# Maximal q-ary Codes and Plotkin's Bound

Conrad Mackenzie and Jennifer Seberry*

Department of Architectural Sciences
University of Sydney
NSW, 2006
Australia

Department of Computer Science
University College
University of New South Wales
Australian Defence Force Academy
Canberra, ACT, 2600
Australia

**Abstract**

The analogue of Plotkin's bound for q-ary codes with high distance relative to length was given by Blake and Mullin as

$$A(n,d) \leq \frac{qd}{qd-n(q-1)}, qd > (q-1)n.$$

Further we show

$$A(n,(q-1)n/q) = qd, qd = (q-1)n.$$

*Generalized Hadamard matrices* are used to obtain q-ary codes which meet these bounds. The q-ary analogue of Levenshtein's construction is discussed and maximal codes constructed.

The codes given are often maximum distance separable, and constructions are given which include the Reed-Solomon codes, but exist for cases when the Reed-Solomon codes cannot exist.

We also study block codes over non-binary alphabets which may prove fruitful for multiple channel encoding.

## 1 The Plotkin Bound

By counting the sum

$$\sum_{u \epsilon G} \sum_{v \epsilon G} dist(u,v)$$

in two ways Blake and Mullin (p.85) show that

**THEOREM 1** *For an alphabet of $q$ symbols, the maximum number of codewords of length $n$ and distance $d$, $A(n,d)$, is*

$$A(n,d) \leq \frac{qd}{qd-(q-1)n} \quad for\ qd > (q-1)n \geq (q-1)d.$$

*The maximum occurs when each symbol occurs $A(n,d/q)$ times in each column which requires $q|A(n,d)$.*

*Research support by a grant from the Australian Computer Research Board.

**LEMMA 2** *(i)* $A(n,d) \leq qA(n-1,d)$; *(ii)* $A(qn,(q-1)n) \leq q^2 n$.

*Proof.* Given a q-ary code, the codewords fall into $q$ classes, those beginning with $0,1,...,(q-1)$. One class must contain at least $1/q$ of the codewords, and so

$$A(n-1,d) \geq A(n,d)/q.$$

Thus, using theorem 1 we have

$$\begin{aligned} A(qn,(q-n)n) &\leq qA(qn-1,(q-1)n) \\ &\leq q\left(\frac{q(q-1)n}{q(q-1)n-(q-1)(qn-1)}\right) \\ &= q^2 n. \end{aligned}$$

We now use generalized Hadamard matrices over groups of size $q$, $GH(n,G)$, to obtain codes which meet these bounds. Although we have discussed the case $q=3$ elsewhere Table 1 revises the knowledge there. This paper considers $q \neq 2,3$.

Remark. We should like to acknowledge that Christiane Engelmann and Michael Kannengann of West Germany have pointed out that our use in a previous paper of

$$A(n,d) \leq 3\left\lfloor \frac{d}{3d-2n} \right\rfloor \quad for \;\; 3d > 2n \geq 2d$$

is incorrect and the correct result is

$$A(n,d) \leq \frac{3d}{3d-2n} \quad for \;\; 3d > 2n \geq 2d.$$

A square matrix of size $n$ with entries from a group $G$ is called a *generalized Hadamard matrix*, $GH(n,G)$, if the inner product of any two distinct rows, $\mathbf{a} = (a_1,...,a_n)$, $\mathbf{b} = b_1,...,b_n)$, $a_i, b_j \epsilon G$, defined by $a \cdot b = \&_{i=1} a_i b_i^{-1}$ is $n/|G|$ copies of $G$. For example, we have

$$GH(5,Z_5) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & a & a^2 & a^3 & a^4 \\ 1 & a^2 & a^4 & a & a^3 \\ 1 & a^3 & a & a^4 & a^2 \\ 1 & a^4 & a^3 & a^2 & a \end{bmatrix}$$

$$GH(6,Z_3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & w & w^2 & w^2 & w \\ 1 & w & 1 & w & w^2 & w^2 \\ 1 & w^2 & w & 1 & w & w^2 \\ 1 & w^2 & w^2 & w & 1 & w \\ 1 & w & w^2 & w^2 & w & 1 \end{bmatrix}.$$

Our constructions will extend the first of these into a code equivalent to a Reed-Solomon code. However our constructions applied to the second example give a maximal code, similar to those of Reed-Solomon, but where Reed-Solomon codes cannot exist because the finite field does not exist, for example for $q = 6$.

The results of de Launey, Drake, Jungnickel, Rajkundlia, Seberry, Seiden, Street and Dawson allow us to say:

**LEMMA 3** *Let $EA(p^i)$ be the elementary abelian group of order $p^i$, where $p$ is a prime. Then the following generalized Hadamard matrices exist:*

(i) $GH(p^{i+j}, EA(p^i))$ for all $i \geq 1, j \geq 0$;

(ii) $GH\left(2^{k+2j}p^{im}, EA(p^i)\right)$ for all $0 \leq k+j \leq m, 0 \leq k, j \leq m$, $m \geq 1, i \geq 1$;

(iii) $GH(2p^i, EA(p^i)), GH(4p^i, EA(p^i))$ for all $1 \geq 1$;

*If $p^t - 1 = r^s$ for some prime $r$, then there exists:*

(iv) $GH\left(p^{tk+l}r^{sj}, EA(p^t)\right)$ for all $1 \leq i \leq t, 1 \leq j \leq k$, $\ell \geq i$ *or* $\ell = 0$;

(v) $GH\left(2^{k+2j}p^{tm}r^{si}, EA(p^t)\right)$ for all $0 \leq i+j+k \leq m, 0 \leq i, j, k \leq m$, $m, r, t \geq 1$;

*If $q$ is a prime power and there exists a $GH(q+1; G)$ for some group $G$, then there exists*

(vi) $GH(q^t(q+1); G)$ for all $t \geq 1$.

For example there exists a $GH(6; Z_3)$ so there exists $GH(5^t.6; Z_3)$.

As well de Launey [1984] surveys the current knowledge on non existence of generalized Hadamard matrices.

Any $GH(n, G)$ is equivalent to a $GH(n, G)$ with its first row and column consisting entirely of the unit element of the group.

**LEMMA 4** *A $GH(n, G), |G| = q$, gives block codes over a $q$-symbol alphabet with parameters, $(n, M, d)$:*

(i) $(n, qn, (q-1)n/q)$,

(ii) $(n-1, qn, (q-1)n/q-1)$,

(iii) $(n-1, n, (q-1)n/q)$,

(iv) $(n-2, n, (q-1)n/q-1)$,

(v) $(q+1, q^2, q)$.

(i), (iii), (v) *are maximal.*

*Proof.* Write A for the normalized $GH(n, G)$ and $G = \{e = a_1, \ldots, a_q\}$. Then the required codes are:

(i)

$$B = \begin{pmatrix} A \\ a_2 A \\ \vdots \\ a_q A \end{pmatrix}$$

where $a_i A$ has the usual meaning of multiplying every element of $A$ by $a_i$;

(ii) $B$ with any column removed;

(iii) $A$ with the first column removed;

(iv) $A$ with the first and any other column removed;

(v) where $n = q$, let $c$ be any column of $A$ except the first, then $C$ is the code

$$C = \begin{pmatrix} Ac \\ a_2 Ac \\ \vdots \\ a_q Ac \end{pmatrix}$$

The result follows as the distance of any two rows of $A$ is $(q - 1)$.

Remark. An interesting paper of Zlotnik deals similarly with extended Reed-Solomon codes but his/her results are for different alphabets.

A number of authors, including de Launey, Lam, Seberry, and Street and Rodger, have studied an extension of generalized Hadamard matrices in which the elements are over a group ring, called Bhaskar Rao designs (BRD). We consider the group ring $\{0\} + G$. A *generalized Bhaskar Rao design* (GBRD) $W = g_1 A_1 + g_2 A_2 + \ldots + g_g A_g$, $g_i \epsilon G$, with parameters $v, b, r, k, \lambda$ satisfies

$$WW^T = rI_v$$

$$\left(\sum_{i=1}^{g} A_i\right)\left(\sum_{i=1}^{g} A_i^T\right) = (r - \lambda)I + \lambda J$$

$$J\sum_{i=1} A_i = kJ$$

$$\left(\sum_{i=1} A_i\right) J = rJ,$$

where $A_i$ are (0,1)-matrices, $\sum_{i=1}^{q} A_i$ is a BIBD $(v, b, r, k, \lambda)$. The GBRD is written GBRD$(v, b, r, k, \lambda; G)$ or GVRD$(v, k, \lambda)$ for brevity. Such designs can be extended to partially balanced and pairwise balanced designs.

In the remainder of this section we use

$$r = \lambda(v-1)/(k-1),\ b = vr/k.$$

**LEMMA 5** *If there exists a GBRD$(v, k, \lambda; G)$, with $|G| = q-1$ then writing $t = 2(r-\lambda) + (q-2)\lambda/(q-1)$ there exists q-ary codes with parameters*

(i) $(b, v, t)$,

(ii) $(b, v+q, min(t, r, b-r))$,

(iii) $(b, qv, min(r, t))$.

*Proof.* Let $M$ be the BRD and $g_1, g_2, \cdots, g_{q-1}$ the group elements. The result follows by considering the rows of

$$M = \begin{bmatrix} 0 & \cdots\cdots & 0 \\ g_1 & \cdots\cdots & g_1 \\ \vdots & & \vdots \\ g_{q-1} & \cdots\cdots & g_{q-1} \\ \cdot & \cdots\ M\ \cdots & \cdot \end{bmatrix}, \quad \begin{bmatrix} M \\ g_1 M \\ \vdots \\ \cdot \\ g_{q-1} M \end{bmatrix},$$

respectively as codewords.

Remark. Codes from BRD over alphabets other than binary should be explored as the zero-nonzero coordinates provide a code in themselves for error correction at one rate while the nonzero coordinates provide a non-binary code with maximum distance separable or near maximum distance separable codewords which could be exploited using phase or frequency variations.

## 2 A property of q-ary codes used to give more codewords

**LEMMA 6** *Let* **a** *and* **b** *be two q-ary vectors. Then with $p = q-1$*

$$\sum_{i=0}^{p} d(\mathbf{a}, \mathbf{b}+1) = 2n$$

$$d(\mathbf{a}+\mathbf{i}, \mathbf{b}+\mathbf{j}) = d(\mathbf{a}+\mathbf{i}+\mathbf{k}, \mathbf{b}+\mathbf{j}+\mathbf{k}), \quad \mathbf{i}, \mathbf{j}, \mathbf{k} \in \{0, 1, \cdots, p\}.$$

*where $d$ is the Hamming distance.*

*Proof.* The second part of the lemma is obviously true for linear codes but we show it is also true for block codes. We write the two codewords as

$$\mathbf{a} = 0 \cdots\cdots\cdots\cdots 0 \cdots p \cdots\cdots\cdots\cdots p$$

$$\mathbf{b} = \underbrace{0 \cdots 0}_{x_{00}} \cdots \underbrace{p \cdots p}_{x_{0p}} \cdots \underbrace{0 \cdots 0}_{x_{p0}} \cdots \underbrace{p \cdots p}_{x_{pp}}.$$

$x_{ij}$ is the number of coordinates which are $i$ in $\mathbf{a}$ and $j$ in $\mathbf{b}$.

Now

$$\begin{aligned} d(\mathbf{a}, \mathbf{b}) &= d(\mathbf{a}+\mathbf{i}, \mathbf{b}+\mathbf{i}) &&= n - \sum_{j=0}^{p} x_{jj} \\ d(\mathbf{a}+\mathbf{i}, \mathbf{b}) &= d(\mathbf{a}+\mathbf{i}, \mathbf{b}+\mathbf{i}-\mathbf{i}) &&= n - \sum_{j=0}^{p} x_{j,j+i} \\ &\vdots \\ d(\mathbf{a}+\mathbf{k}, \mathbf{b}) &= d(\mathbf{a}+\mathbf{i}, \mathbf{b}+\mathbf{i}-\mathbf{k}) &&= n - \sum_{j=0}^{p} x_{j,j+k}. \end{aligned}$$

Further,

$$\sum_{k=0}^{p} d(\mathbf{a}, \mathbf{b}+\mathbf{k}) = q \sum_{i=0}^{p} \sum_{j=0}^{p} x_{ij} = (q-1)n.$$

This allows us to readily test the distance of a constructed code, as in the following:

**LEMMA 7** *Suppose $A$ is a $q$-ary $(p = q-1)$ $(n, M, d)$ -code. Then, writing $A+i$, to denote adding $i$ to each element of $A$ (assumed written on an additively defined alphabet).*

$$\begin{bmatrix} A \\ A+1 \\ \vdots \\ A+p \end{bmatrix}$$

is a q-ary $(n, q, M, d')$-code where

$$d' = min\left[d(\mathbf{a}, \mathbf{b}), d(\mathbf{a}, \mathbf{b}+\mathbf{1}), \cdots, d(\mathbf{a}, \mathbf{b}+\mathbf{p}-\mathbf{1}), (q-1)n - \sum_{j=0}^{p-1} d(\mathbf{a}, \mathbf{b}+\mathbf{j})\right]$$

**a, b** codewords of $A$.

**EXAMPLE 8** Suppose

$$A = \begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 1 & 3 & 2 \\ 0 & 2 & 4 & 0 & 1 & 3 \\ 0 & 3 & 2 & 4 & 0 & 1 \\ 0 & 1 & 3 & 2 & 4 & 0 \\ 0 & 0 & 1 & 3 & 2 & 4 \end{pmatrix}, \quad a\ 5-ary\ (6,6,5)-code,$$

then to find $d'$ we merely need to test $a = (4,0,0,0,0,0)$ with $b = (0,4,0,1,3,2)+\mathbf{i}$ which gives $d = min(4,5) = 4$ and $a = (0,4,0,1,3,2)$ with $b = (0,2,4,0,1,3)+\mathbf{i}$ which gives $d = min(4,5) = 4$. This gives $d' = min[4,5,4,5] = 4$ giving a $(6,30,4)$ 5-ary code.

**THEOREM 9** *Let $A$ be a $q$-ary $(n-1, M, d)$-code. Further define*

$$d_i = \min_{\mathbf{a},\mathbf{b}\in A} d(\mathbf{a}, \mathbf{a}+\mathbf{i}), \quad i = 0, 1, \cdots, q-1.$$

*Then there exists $q$-ary $(n, qM, min(d, d_i+1))$ and $(n-1, qM, min(d_i))$ codes.*

*Proof.* We consider, using the notation of Lemma 7,

$$\begin{pmatrix} 0 & \\ \vdots & A \\ 0 & \\ 1 & \\ \vdots & A+1 \\ 1 & \\ 1 & \\ \vdots & \vdots \\ q-1 & \\ \vdots & A+q-1 \\ q-1 & \end{pmatrix} = \begin{pmatrix} N_0 \\ N_1 \\ \vdots \\ N_{q-1} \end{pmatrix}.$$

This gives the first code. The second follows from Lemma 7.

# 3 Levenshtein's method

Let us suppose that an arbitrary $GF(m, G)$, $M = k|G| = kq$ exists, written on the additive group, whose first column is composed entirely of zero's: denote this matrix $M_m$, and the matrix, when formed by stripping the column of zero's, by $M'_m$.

The theory giving the construction of maximal codes requires matrices of particular orders and distances.

**LEMMA 10** *If there exists an $M_{kq}$ (respectively $M_{q(k+1)}$) then the rows of $M'_{kq}$ (respectively $M'_{q(k+1)}$) form a code with parameters $n = kq-1$, $M = kq$, $d+k(q-1)$ (respectively $n = kq + q - 1$, $M = q(k + 1)$, $d = (k + 1)(q - 1)$).*

Write

$$i = \left\lceil \frac{d}{qd - n(q-1)} \right\rceil .$$

**LEMMA 11** *If $qd > (q - 1)n \geq (q - 1)d$, then there exist integers $a$ and $b$ such that*

$$\left.\begin{aligned} n &= a(qi - 1) + b(qi + q - 1) \\ d &= (q - 1)ai + (q - 1)b(i + 1). \end{aligned}\right\} \tag{1}$$

*Proof.* We can define $i$ in terms of the following inequalities:

$$\left(\frac{d}{qd - n(q-1)}\right) - 1 < i \leq \left(\frac{d}{qd - n(q-1)}\right),$$

that is,

$$\frac{(q-1)(n-d)}{qd - n(q-1)} < i \leq \frac{d}{qd - n(q-1)}.$$

Considering the left inequality gives

$$\frac{(q-1)(i+1)}{qi + (q-1)} < \frac{d}{n}, \tag{2}$$

and the right inequality gives

$$\frac{d}{n} \leq \frac{(q-1)i}{qi - 1}. \tag{3}$$

Combining (2) and (3) we obtain

$$\frac{(q-1)(i+1)}{qi + (q-1)} < \frac{d}{n} \leq \frac{(q-1)i}{qi - 1}. \tag{4}$$

The two inequalities of (4) may be written in determinant form:

$$\begin{vmatrix} d & (q-1)(i+1) \\ n & qi+(q-1) \end{vmatrix} > 0 = A, \quad say \tag{5}$$

$$\begin{vmatrix} n & (qi-1) \\ d & (q-1)i \end{vmatrix} \geq 0 = B, \quad say. \tag{6}$$

Now suppose that both $A$ and $B$ are both divisible by $q-1$. Then let

$$A = (q-1)a$$

$$B = (q-1)b$$

so (5) and (6) become

$$A = (q-1)a = d(qi+q-1) - n(q-1)(i+1) \tag{7}$$

$$B = (q-1)b = (q-1)ni - d(qi-1), \tag{8}$$

and solving (7) and (8) for $n$ and $d$ yields the required results (1).

Note: Requiring that $A$ and $B$ are divisible by $q-1$ imposes only one condition, namely that $d$ is also divisible by $(q-1)$, but in the case of q-ary codes the distance is, in fact, divisible by $(q-1)$ for maximal codes as then $qd = (q-1)n$.

Following Levenshtein, we define the operation of adjunction of the matrices

$$X = (X_{ij}), \quad i = 1,2,\cdots,L_1, \quad j = 1,2,\cdots,n_1$$

$$Y = (Y_{ij}), \quad i = 1,2,\cdots,L_2, \quad j = 1,2,\cdots,n_2$$

as follows:

$$X+Y = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1n_1} & Y_{11} & Y_{12} & \cdots & Y_{1n_2} \\ X_{21} & X_{22} & \cdots & X_{2n_1} & Y_{21} & Y_{22} & \cdots & Y_{2n_2} \\ \vdots & .. & & .. & .. & .. & & .. \\ X_{L_1} & X_{L_2} & \cdots & X_{Ln_1} & Y_{L_1} & Y_{L_2} & \cdots & Y_{Ln_2} \end{pmatrix}$$

where $L = min(L_1, L_2)$.

The operation of extension of a matrix $X$, $r$ times, is defined as the result of the consecutive adjunction of $r$ matrices $X$.

Note: If the rows of the matrix $X$ form a code with the parameters $n_1$, $d_1$ and $M_1$, and the rows of a matrix $Y$ form a code with the parameters $n_2$, $d_2$ and $M_2$, then

the rows of the matrix $aX + bY$, where $a$ and $b$ are integer non-negative numbers, form a code with the parameters

$$n = an_1 + bn_2$$

$$d = ad_1 + bd_2$$

and

$$M = min(M_1, M_2).$$

**THEOREM 12** *If $d$ is divisible by $(q-1)$ and $qd > (q-1)n \geq (q-1)d$, then the following matrix $M$ is maximal in that it meets the bound*

$$\begin{aligned} A(n,d) &= q\left\lfloor \frac{d}{qd-(q-1)n} \right\rfloor = qi \\ M &= aM'_{qi} + bM'_{q(i+1)} \\ a &= d(qi+q-1)/(q-1) - n(i+1) \\ b &= ni - d(qi-1)/(q-1). \end{aligned}$$

*Proof.* For the proof of the theorem, it is sufficient to see,using Lemmas 10 and 11, that the above construction does indeed generate a maximal code.

**EXAMPLE 13** Let

$$A = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & i & i^3 & i^2 \\ 1 & i^2 & 0 & 1 & i & i^3 \\ 1 & i^3 & i^2 & 0 & 1 & i \\ 1 & 1 & i & i^3 & i^2 & 0 \end{bmatrix} \text{ be the } \mathrm{GBRD}(6,5,4;Z_4).$$

Then $A$ is a (6,6,5)-code over a 5-ary alphabet and

$$B = \begin{bmatrix} A \\ iA \\ i^2A \\ i^3A \end{bmatrix}$$

is a (6,24,5)-code over a 5-ary alphabet and

$$\begin{bmatrix} 0 & \cdots & 0 \\ & B & \end{bmatrix}$$

is a (6,25,5) maximal 5-ary code.

**EXAMPLE 14** From Seberry (1980) we have that a $A = \text{GBRD}(p^r+1, p^r, p^r-1; Z_t)$ exists whenever $p^r$ is a prime power, $t$ divides $p^r-1$ and $Z_t$ is a cyclic group. If the elements of the group are $1, g_1, \cdots, g_{t-1}$, then

$$\begin{bmatrix} 0 & \cdots & 0 \\ & A & \\ & g_1 A & \\ & \vdots & \\ & g_{t-1}A & \end{bmatrix}$$

is a $(p^r+1, t(p^r+1)+1, p^r)$-code over a $(t+1)$-ary alphabet. When $t = p^r - 1$ this gives a maximal code.

**COROLLARY 15** *Let $p^r$ be a prime power. Then there exists a $(p^r+1, p^2r, p^r)$ maximal code over a $p^r$-ary alphabet.*

**EXAMPLE 16** From de Launey (1987) a $W = \text{GBRD}\left(\frac{p^t-1}{p-1}, p^{t-1}, p^{t-2}(p-1); Z_{p-1}\right)$ $t \geq 3$, exists whenever $p^t$ is a prime power and $Z_{p-1}$ is a cyclic group. Then proceeding as in Example 14 we have a $((p^t-1)/(p-1), p^{t-1}(p-1)+1, p^{t-2}(p-1))$ - code over a p-ary alphabet.

**EXAMPLE 17** The following are 4-ary codes.

A structured (7,8,6)-code (maximal)

| | |
|---|---|
| aaaaaaa | baceebc |
| eebcbac | cbaceeb |
| ceebcba | bcbacee |
| aceebcb | ebcbace |

A structured (5,16,4)-code (maximal)

aaaaa
aceec
cacee
ecace
eecac
ceeca
abccb
babcc
cbabc
ccbab
bccba
aebbe
eaebb
beaeb
bbeae
ebbea

A (6,8,5)-code

| |
|---|
| cccccc |
| aaaaaa |
| eeabcd |
| beeabc |
| cbeeab |
| bcbeea |
| abcdee |
| eabcbe |

A (10,5,9)-code

| | |
|---|---|
| aabcd | abacd |
| daabc | dabac |
| cdaab | cdaba |
| bcdaa | acdab |
| abcda | bacda |

**EXAMPLE 18** The following are 5-ary codes.

5-ary (7,15,6)-code(maximal)

0 0 0 0 0 0 0
0 2 1 3 3 1 2
2 0 2 1 3 3 1
1 2 0 2 1 3 3
3 1 2 0 2 1 3
3 3 1 2 0 2 1
1 3 3 1 2 0 2
2 1 3 3 1 2 0
4 4 1 4 2 3 0
0 4 4 1 4 2 3
3 0 4 4 1 4 2
2 3 0 4 4 1 4
4 2 3 0 4 4 1
1 4 2 3 0 4 4
4 1 4 2 3 0 4

5-ary (8,10,7)-code

0 0 0 0 0 0 0 0
4 4 4 4 4 4 4 4
0 1 1 2 3 2 4 3
3 0 1 1 2 3 2 4
4 3 0 1 1 2 3 2
2 4 3 0 1 1 2 3
3 2 4 3 0 1 1 2
2 3 2 4 3 0 1 1
1 2 3 2 4 3 0 1
1 1 2 3 2 4 3 0

**Table 1**

**Codes with $3d \geq 2n$, $q = 3$**

| *n* | *M(found)* | *M(max)* | *d* | *Construction or Comment* |
|---|---|---|---|---|
| 3 | 9 | 9 | 9 | GH(3,EA(3)) |
| 4 | 27 | | 2 | Mackenzie and Seberry |
| 5 | 18 | | 3 | From (6,18,4)-code |
| 6 | 27 | | 3 | From (9,27,6)-code |
| 6 | 18 | 18 | 4 | GH(6,EA(3)) |
| 7 | 27 | | 4 | From (8,27,5)-code |
| 8 | 27 | | 5 | From (9,27,6)-code |
| 9 | 27 | 27 | 6 | GH(9,EA(3)) |
| 10 | 54 | | 5 | Mackenzie and Seberry |
| 10 | 36 | | 6 | From (11,36,7)-code |
| 11 | 36 | | 7 | From (12,36,8)-code |
| 12 | 36 | 36 | 8 | GH(12,EA(3)) |
| 13 | 54 | | 7 | From (18,54,12)-code |
| 14 | 54 | | 8 | From (18,54,12)-code |
| 15 | 54 | | 9 | From (18,54,12)-code |
| 15 | 18 | 45 | 10 | (6,18,4) + (9,27,6) |
| 16 | 54 | | 10 | From (17,54,10)-code |
| 17 | 54 | | 11 | From (18,54,12)-code |
| 18 | 54 | 54 | 12 | GH(18,EA(3)) |
| 19 | 57 | | 12 | Corollary 6 |
| 20 | 21 | | 13 | From (21,21,14)-code |
| 21 | 21 | 63 | 14 | Corollary 6 |
| 22 | 72 | | 14 | From (23,72,15)-code |
| 23 | 72 | | 15 | From (24,72,16)-code |
| 24 | 72 | 72 | 16 | GH(24,EA(3)) |
| 25 | 81 | | 16 | From (26,81,17)-code |
| 26 | 81 | | 17 | From (27,81,18)-code |
| 27 | 81 | 81 | 18 | GH(27,EA(3)) |
| 28 | 90 | | 18 | From (29,90,20)-code |
| 29 | 90 | | 19 | From (30,90,20)-code |
| 30 | 90 | 90 | 20 | GH(30,EA(3)) |

**Table 2**

**Codes with $4d \geq 3n \geq 3d$, $q = 4$**

| $n$ | $M$(found) | $M$(max) | $d$ | Construction or Comment |
|---|---|---|---|---|
| 4 | 16 | 16 | 3 | GH(4,EA(4)) |
| 5 | 16 | 16 | 4 | Lemma 4(v), Example 14 |
| 6 | 8 | 10 | 5 | Example 14 |
| 7 | 8 | 8 | 6 | Lemma 4(iii) and GH(8,EA(4)), Example 14 |
| 8 | 32 | 32 | 6 | GH(8,EA(4)) |
| 9 | 16 | 28 | 7 | (4,16,3) + (5,16,4) codes |
| 10 | 16 | 16 | 8 | (5,16,3) + (5,16,4) codes |
| 10 | 5 | 6 | 9 | Example 17 |
| 11 | 12 | 12 | 9 | Lemma 4(iii) and GH(12,EA(4)) |
| 12 | 48 | 48 | 9 | GH(12,EA(4)) |
| 13 | 16 | 40 | 10 | (5,16,4) + (8,32,6) codes |
| 14 | 16 | 22 | 11 | (5,16,4) + (9,28,7) codes |
| 15 | 16 | 16 | 12 | Lemma 4(iii) and GH(12,EA(4)) |
| 16 | 64 | 64 | 12 | GH(16,EA(4)) |
| 17 | 16 | 52 | 13 | (8,32,6) + (9,16,7) codes |
| 18 | 28 | 28 | 14 | (9,28,7) + (9,28,7) codes |
| 19 | 16 | 20 | 15 | (9,28,7) + (10,16,8) codes |
| 20 | 32 | 80 | 15 | (8,32,6) + (12,48,9) codes |
| 21 | 32 | 64 | 16 | (8,32,6) + (13,40,10) codes |
| 22 | 28 | 34 | 17 | (9,29,7) + (13,40,10) codes |
| 23 | 16 | 24 | 18 | (10,16,8) + (13,40,10) codes |
| 24 | 48 | 96 | 18 | (12,48,9) code twice |
| 25 | 16 | 76 | 19 | (9,16,7) + (16,64,12) codes |
| 26 | 28 | 40 | 20 | (8,32,16) + (12,48,9) codes |
| 27 | 28 | 28 | 21 | Lemma 4(iii) |
| 28 | 112 | 112 | 21 | GH(28,EA(4)) |
| 29 | 16 | 88 | 22 | (12,48,9) + (17,16,13) codes |
| 30 | 28 | 46 | 23 | (12,48,9) + (18,28,14) codes |

**Table 3**

**Codes with $5d \geq 4n \geq 4d$, $q = 5$**

| $n$ | $M$(found) | $M$(max) | $d$ | Construction or Comment |
|---|---|---|---|---|
| 4 | 5 | 5 | 4 | Lemma 4(iii) |
| 5 | 25 | 25 | 4 | GH(5,EA(5)) |
| 6 | 25 | 25 | 5 | Lemma 4(v) |
| 7 | 15 | 15 | 6 | Example 15 |
| 8 | 10 | 11 | 7 | Example 15 |
| 9 | 10 | 10 | 8 | Lemma 4(iii) |
| 10 | 50 | 50 | 8 | GH(10,EA(5)) |
| 11 | 25 | 45 | 9 | (5,25,4) + (6,25,5) |
| 12 | 25 | 25 | 10 | (6,25,5) twice |
| 13 | 15 | 18 | 11 | (6,25,5) + (7,15,6) |
| 14 | 15 | 15 | 12 | (7,15,6) twice |
| 15 | 25 | 75 | 12 | GH(15,EA(5)) does not exist |
| 16 | 25 | 65 | 13 | (5,25,4) + (11,25,9) |
| 17 | 25 | 35 | 14 | (6,25,5) + (11,25,9) |
| 18 | 25 | 25 | 15 | (6,25,5) three times |
| 19 | 20 | 20 | 16 | Lemma 4(iii) |
| 20 | 100 | 100 | 16 | GH(20,EA(5)) |
| 21 | 25 | 85 | 17 | (10,50,8) + (11,25,9) |
| 22 | 25 | 45 | 18 | (11,25,9) twice |
| 23 | 25 | 31 | 19 | (11,25,9) + (12,25,10) |
| 24 | 25 | 25 | 20 | Lemma 4(iii) |
| 25 | 125 | 125 | 20 | GH(25,EA(5)) |
| 26 | 25 | 105 | 21 | (10,50,8) + (16,25,13) codes |
| 27 | 25 | 55 | 22 | (12,25,10) + (15,25,12) codes |
| 28 | 25 | 38 | 23 | (12,25,10) + (16,25,13) codes |
| 29 | 25 | 30 | 24 | (12,25,10) + (17,25,14) codes |
| 30 | 125 | 150 | 25 | Corollary 4.7 deLaunay |

## References


[1] Ian F. Blake and Ronald C. Mullin, *An Introduction to Algebraic and Combinatorial Coding Theory*, Academic Press, New York, 1976.

[2] Jeremy E. Dawson, A construction for generalized Hadamard matrices GH(4q,EA(q)), *J. Stat. Planning and Inference*, 11, (1985), 103-110.

[3] Warwick de Launey, Non-existence of generalized Hadamard matrices, *J. Stat. Planning and Inference*, 10, (1984), 385-396.

[4] Warwick de Launey and Jennifer Seberry, Generalized Bhaskar Rao designs with block size four, *Congressus Numerantium*, 41 (1984), 229-294.

[5] D.A. Drake, Partial $\lambda$−geometrics and generalized matrices over groups, *Canad. J. Math.* 31 (1979), 617-627.

[6] Christiane Engelmann and Michael Kannengann, private communication (1985).

[7] D. Jungnickel, On difference matrices, resolving TD's and generalized Hadamard matrices, *Math. Z.* 167 (1979), 49-60.

[8] Clement Lam and Jennifer Seberry, Generalized Bhaskar Rao designs, *J. Stat. Planning and Inference*, 10, (1984), 83-95.

[9] V.I. Levenshtein, Application of the Hadamard matrix to a problem of coding, *Priblemy Kibernetiki*, vol. 5 (1961), 123-136.

[10] Conrad Mackenzie and Jennifer Seberry, Maximal ternary codes and Plotkin's bound, *Ars Combinatoria*, 17A (1984), 251-270.

[11] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Vol. 1, North-Holland, Amsterdam, New York, Oxford, 1977.

[12] D. Rajkundlia, Some techniques for constructing new infinite families or balanced incomplete block designs, *Discrete Math.* 44 (1983), 61-96.

[13] Jennifer Seberry, A construction for generalized Hadamard matrices, *J. Stat. Planning and Inferenece*, 4 (1980), 365-368.

[14] Jennifer Seberry, Regular group divisible designs and Bhaskar Rao designs with block size three, *J. Stat. Planning and Inference*, 10, (1982), 378-386.

[15] Deborah J. Street, Generalized Hadamard matrices, orthogonal arrays and F-squares, *Ars Combinatoria*, 8 (1979), 131-141.

[16] Deborah J. Street and C.A. Rodger, Some results on Bhaskar Rao designs, in *Combinatorial Mathematics III*, Lecture Notes in Mathematics, Vol. 829 (eds. R.W. Robinson, G.W. Southern and W.D. Wallis), Springer-Verlag, Berlin-Heidelberg-New York, 1980, 238-245.

[17] B.M. Zlotnik, Doubly transitive groups of type $p^m(p^m-1)$ and maximal non binary codes generated by them, Translated from *Kibernetika*, No. 3, May-June, 32, (1983) 16-32. Copyright Plenum Publishing Corp.