МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2000
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2000
Proceedings of Twenty Ninth Spring Conference of
the Union of Bulgarian Mathematicians
Lovetch, April 3–6, 2000

BOUNDS FOR CODES OVER SMALL ALPHABETS

Galina T. Bogdanova[1], **Stoian N. Kapralov**[2]

This paper dwells on the problem of finding the values of $A_q(n,d)$: the maximum size of a code of length n and minimum distance d over an alphabet of q elements. All the parameters (n,d) for which $q \le A_q(n,d) < 2q$ are determined. Some new bounds on $A_3(n,d)$ are presented.

1. Introduction. We assume that the reader is familiar with the basic notions and facts of coding theory [6],[7]. The codes to be considered are $(n,M,d)_q$-codes, i.e. codes over an alphabet of q elements, that contain M words of length n at minimum distance d. We denote by $A_q(n,d)$ the maximum of M, for which an $(n,M,d)_q$-code exists.

The first systematic research of the function $A_3(n,d)$ was in [12], where a table of its values was presented for $n \le 16$. Few improvements were made in that table for the next several years. In [4] an updated table was presented. Here we reproduce only a part of the last table.

Table 1. Values of $A_3(n,d)$

n	$d=3$	$d=4$	$d=5$	$d=6$	$d=7$	$d=8$	$d=9$	$d=10$
4	9							
5	18	6						
6	38–48	18	4					
7	99–144	33–46	10	3				
8	243–340	99–138	27	9	3			
9	729–937	243–340	81	27	6	3		
10	2187–2811	729–937	243	81	14–18	6	3	
11	6561–7029	1458–2561	729	243	36–50	12	4	3

2. General bounds on $A_q(n,d)$.

Theorem 2.1.

$$A_q(n,d) \le A_q(n-1,d-1), \qquad A_q(n,d) \le qA_q(n-1,d).$$

[1]This work was partially supported by UVO-ROSTE Contract No 875.630.9.
[2]This work was partially supported by the Bulgarian National Science Fund under Grant I–618/96.

Theorem 2.2. [2]

$$A_q(n,d) = q \quad \Longleftrightarrow \quad \frac{q^2+q-2}{q(q+1)}n < d \le n.$$

Theorem 2.3. [3]

$$A_q(n,d) = q+1 \quad \Longleftrightarrow \quad \frac{q^2+3q-2}{(q+1)(q+2)}n < d \le \frac{q^2+q-2}{q(q+1)}n.$$

Theorem 2.4. (The Plotkin bound) [10], [6]. *If C is an $(n,M,d)_q$-code, then* $(M-1)qd \le M(q-1)n$.

In the recent paper [1], a stronger result is proved:

Theorem 2.5. (The sharpened Plotkin bound) [1] *If C is an $(n,M,d)_q$-code and $M = pq+r,\ 0 \le r \le q-1$, then $(M-1)Md \le (M^2-\sigma)n$, where $\sigma = (q-r)p^2+r(p+1)^2$.*

3. New general result.

Lemma 3.1. *If an $(n,M,d)_q$-code exists and $q \le M \le 2q$ then*

$$d \le \frac{M^2-3M+2q}{M^2-M}n.$$

Proof. Follows from Theorem 2.5.

Some definition and preliminary results are needed for the proof of the next Lemma.

Let $V = \{1,2,\ldots,m\}$. There are $\binom{m}{2}$ distinct unordered pairs of the elements of V.

Definition 3.2. *A Pair Design $PD(m)$ is an arrangement of the pairs in a sequence in such a way that there are at least $\left\lfloor \frac{m-3}{2} \right\rfloor$ pairs between every two pairs with a common element.*

Example 3.3. $PD(7)$

12, 34, 56, 71, 23, 45, 67, 13, 52, 74, 61, 35, 27, 46, 15, 73, 62, 41, 57, 36, 24.

Example 3.4. $PD(8)$

12, 34, 56, 78, 13, 52, 74, 86, 15, 73, 82, 64, 17, 85, 63, 42, 18, 67, 45, 23, 16, 48, 27, 35, 14, 26, 38, 57.

Theorem 3.5 [11], [5]. *A $PD(m)$ exists for all positive integers $m \ge 2$.*

Construction.

a) for odd m the first m pairs are

$$\{1,2\},\{3,4\},\ldots,\{m-2,m-1\},\{m,1\},\{2,3\},\ldots,\{m-1,m\}.$$

Then apply $\dfrac{m-1}{2}-1$ times the permutation:

$$(1)(3,5,7,\ldots,m-4,m-2,m,m-1,m-3,,\ldots,6,4,2)$$

b) for even m the first $\dfrac{m}{2}$ pairs are

$$\{1,2\},\{3,4\},\ldots,\{m-1,m\};$$

Then apply $m-2$ times the permutation:

$$(1)(3,5,7,\ldots,m-3,m-1,m,m-2,m-4,,\ldots,6,4,2).$$

The obtained $PD(m)$ are *cyclic.* Using k times reiteration of $PD(m)$, we obtain the sequence where any pair occurs k times, and with the property that there are at least $\left\lfloor \dfrac{m-3}{2} \right\rfloor$ pairs between two appearances of any one element. We call such a sequence PD-sequence.

Lemma 3.6. *If* $q \le M \le 2q$ *and* $d \le \dfrac{M^2-3M+2q}{M^2-M}n$ *then an* $(n,M,d)_q$*-code exists.*

Construction. If $M=q$ the desired code may be:

$$\begin{array}{cccc}
\overbrace{\begin{array}{cccc} 0 & 0 & \ldots & 0 \\ 1 & 1 & \ldots & 1 \\ 2 & 2 & \ldots & 2 \\ \ldots & & & \\ q-1 & q-1 & \ldots & q-1 \end{array}}^{d} & \overbrace{\begin{array}{cccc} 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \ldots & & & \\ 0 & 0 & \ldots & 0 \end{array}}^{n-d}
\end{array}$$

If $M>q$ let $r=M-q$. First produce a PD-sequence of length $r\times n$.
Cut the sequence into subsequences of length r.
Every subsequence $\{x_0,y_0,\},\{x_1,y_1\},\ldots,\{x_{r-1},y_{r-1}\}$ corresponds to a coordinate of the desired code: for $i=0,1,\ldots,r-1$ set this coordinate of the x_i-th and y_i-th codewords equal to i. If $M<2q$ the nonfilled entries in any position fill with the unused elements of Z_q, i.e. $r,r+1,\ldots,q-1$.

Example 3.7. Construction of a $(28,8,25)_5$ code.
Take three times $PD(8)$ and cut the sequence into parts of length 3
12,34,56; 78,13,52; 74,86,15; 73,82,64; 17,85,63; 42,18,67; 45,23,16;
48,27,35; 14,26,38; 57,12,34; 56,78,13; 52,74,86; 15,73,82; 64,17,85;
63,42,18; 67,45,23; 16,48,27; 35,14,26; 38,57,12; 34,56,78; 13,52,74;
86,15,73; 82,64,17; 85,63,42; 18,67,45; 23,16,48; 27,35,14; 26,38,57.

The code is:
0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3 0 1 2 3
0 2 3 1 3 0 1 1 1 1 3 0 2 3 1 2 2 2 2 4 1 3 0 2 3 0 0 0
1 1 4 0 2 3 1 2 2 2 2 4 1 4 0 2 3 0 0 0 0 2 3 1 4 0 1 1
1 3 0 2 4 0 0 0 0 2 4 1 3 0 1 1 1 1 3 0 2 4 1 2 2 2 2 4
2 2 2 4 1 4 0 2 3 0 0 0 0 2 3 1 4 0 1 1 1 1 4 0 2 3 1 2
2 4 1 2 2 2 2 4 1 3 0 2 4 0 0 0 0 2 4 1 3 0 1 1 1 1 3 0
3 0 0 0 0 2 3 1 4 0 1 1 1 1 4 0 2 3 1 2 2 2 2 4 1 4 0 2
4 0 1 1 1 1 4 0 2 4 1 2 2 2 2 4 1 4 0 2 4 0 0 0 0 2 4 1.

Theorem 3.8. *If* $q \le M < 2q$ *then* $A_q(n,d) = M$ *iff*

$$\frac{(M+1)^2 - 3(M+1) + 2q}{(M+1)^2 - (M+1)} n < d \le \frac{M^2 - 3M + 2q}{M^2 - M} n.$$

Proof. Follows from Lemma 3.1 and Lemma 3.6.

4. New specific results. In [12] a $(6,37,3)_3$ code has been constructed.
In [4] a $(6,38,3)_3$ code has been constructed.
By the Linear Programming bound $(6,49,3)_3$-codes do not exist.
Hence $38 \le A_3(6,3) \le 48$, as it is shown in Table 1.
In this paper we will prove that $38 \le A_3(6,3) \le 39$.

Theorem 4.1. *There are no* $(6,40,3)_3$*-codes.*

Proof. Our approach is similar to that one used in [8] for proving the nonexistence of a $(10,73,3)_2$-code.

Any $(n,M,d)_q$-code contains an $(n-1,M',d)_q$-code with $M' \ge M/q$.

Suppose that C is a $(6,40,3)_3$-code. Then C must contain a subcode C' which is a $(5,M',3)_3$-code with $M' \ge 14$. In Table 1 we see that $M' \le 18$. We have classified (up to equivalence) all codes with parameters $(5,M',3)_3$ for $14 \le M' \le 18$ and all codes with parameters $(4,M'',3)_3$ for $5 \le M'' \le 9$.

Definition 4.2. *Two* q*-ary codes are called equivalent if one can be obtained from the other by a superpossition of operations of the following types:*
a) permutation of the coordinates of the code;
b) permutation of the symbols appearing in a fixed position.

To find out whether two q-ary codes are equivalent the brute-force approach of checking all $n!(q!)^n$ possible permutations of the coordinates and coordinate values is not acceptable even for small values of q and n.

In [9] the complexity of algorithms for determining the code equivalence is studied. A polynomial-time reduction from the Graph Isomorphism problem to Code Equivalence problem was presented. Thus, if one could find an efficient (i.e., polynomial-time) algorithm for the Code Equivalence problem, then one could settle up the long-standing problem of determining whether there is an efficient algorithm for solving the Graph Isomorphism problem.

In [8] we find just the opposite approach: the Code Equivalence problem is transformed into a Graph Isomorphism one.

We use our own specially developed computer program for determining code equivalence.
The results are summarized in the following table:

Table 2. Inequivalent $(4, M, 3)_3$ and $(5, M, 3)_3$-codes

M	# inequivalent $(4, M, 3)_3$-codes	M	# inequivalent $(5, M, 3)_3$-codes
5	5	14	78
6	4	15	10
7	1	16	3
8	1	17	1
9	1	18	1

We checked with a computer that none of the subcodes can be extended to a $(6, 40, 3)_3$-code.

Using the same approach we prove the following theorem:

Theorem 4.3. *There are no* $(10, 16, 7)_3$*-codes.*

From Theorem 4.2, Theorem 4.3 and Theorem 2.1 we obtain the following improvements in Table 1:

Corollary 4.4.
a) $A_3(6, 3) \leq 39$, $A_3(7, 3) \leq 117$, $A_3(7, 4) \leq 39$, $A_3(8, 3) \leq 117$;
b) $A_3(10, 7) \leq 15$, $A_3(11, 7) \leq 45$.

REFERENCES

[1] G. Bogdanova, S. Kapralov. A recursive construction of a family nonlinear codes. *Mathematics and Education in Mathematics*, **28** (1999), 72–75.

[2] G. T. Bogdanova, P. R. J. Östergård. Error-correcting Codes an Alphabet of Four Elements. Intern. Symp. on Inform. Theory, 2000, Toronto, Italy, (submitted).

[3] G. T. Bogdanova, P. R. J. Östergård, S. N. Kapralov. Bounds on Codes over an Alphabet of Five Elements. *Discrete Mathematics*, (submitted).

[4] A. E. Brouwer, H. O. Hämäläinen, P. R. J. Östergård, N. J. A. Sloane, W. D. Smith. Bounds on Mixed Binary/Ternary Codes. *IEEE Trans. Inform. Theory*, **44** (1998), 140–161.

[5] J. H. Dinitz, E. R. Lamken, W. D. Wallis. Scheduling a Tournament, a Chapter in: The CRC Handbook of Combinatorial Designs. (Eds. C. J. Colbourn, J. H. Dinitz), CRC Press, New York, 1996, 565–578.

[6] J. H. van Lint. Introduction to Coding Theory. Springer-Verlag, New York, 1982.

[7] F. J. MacWilliams, N. J. A. Sloanem. The Theory of Error-Correcting Codes, North-Holland. Amsterdam, 1977.

[8] P. R. J. Östergård, T. Baicheva, E. Kolev. Optimal binary one-error-correcting codes of length 10 have 72 codewords. *IEEE Trans. Inform. Theory*, **45** (1999), 1229–1231.

[9] E. Petrank, R. M. Roth. Is code equivalence easy to deside? *IEEE Trans. Inform. Theory*, **43** (1997), 1602–1604.

[10] M. Plotkin. Binary codes with specified minimum distance. *IRE Trans. Inform. Theory*, **6** (1960) 445–450.

[11] G. J. Simmons, J. A. Davis. Pair designs. *Commun. Stat.*, **4** (1975), 255–272.
[12] R. J. M. Vaessens, E. H. L. Aarts, J. H. van Lint. Genetic algorithms in coding theory – a table for $A_3(n,d)$. *Discrete Applied Mathematics*, **45** (1993), 71–87.

Galina T. Bogdanova
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
P.O. Box 323, 5000 V. Tarnovo, Bulgaria
lpmivt@vt.bia-bg.com

Stoian N. Kapralov
Department of Mathematics
Technical University
5300 Gabrovo, Bulgaria
kapralov@tugab.bg

ГРАНИЦИ ЗА КОДОВЕ НАД МАЛКИ АЗБУКИ

Галина Т. Богданова, Стоян Н. Капралов

Статията е посветена на проблема за определяне стойностите на $A_q(n,d)$ – максималния обем на код с дължина n и минимално разстояние d над азбука с q елемента. Определени са всички двойки (n,d), за които $q \leq A_q(n,d) < 2q$. Получени са някои нови граници за $A_3(n,d)$.