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

OPTIMAL QUATERNARY TWO-ERROR-CORRECTING CODES OF LENGTH 7 HAVE 32 CODEWORDS

Kaloyan S. Kapralov*

An $(n,M,d)_q$ code is a q-ary code of length n, with M codewords and minimum distance d. Let $A_q(n,d)$ denote the largest value of M such that there exists an $(n,M,d)_q$ code. We prove the uniqueness of the $(6,9,5)_4$ code and the nonexistence of $(7,33,5)_4$ codes. The latter implies that $A_4(7,5)=32$.

1. Introduction.

An $(n,M,d)_q$ code is a q-ary code of length n, containing M codewords and having minimum distance d. A code with minimum distance d is a $\lfloor (d-1)/2 \rfloor$-error-correcting code. The problem of optimizing one of the parameters n, M, d for given values of the other two is often referred to as *the main coding theory problem.* Its usual version is to find the largest code of given length and given minimum distance. We denote by $A_q(n,d)$ the largest value of M such that there exists a q-ary (n,M,d) code. Codes with parameters $(n, A_q(n,d), d)_q$ are called optimal.

The function $A_2(n,d)$ has been thouroughly studied ever since the early days of coding theory [1],[5],[6],[7]. The first table for $A_3(n,d)$ was presented in [8]. Some research has also been done on the bounds for mixed binary/ternary codes [4].

For the quaternary case, the problem of finding values of $A_4(n,d)$ is considered in [3]. There, it is proved that $A_4(6,5)=9$ and that $32 \le A_4(7,5) \le 36$.

In this paper we improve the latter result by proving that $A_4(7,5)=32$.

First, we prove that there is exactly one (up to equivalence) $(6,9,5)_4$ code. Then the unique $(6,9,5)_4$ code is used in the attempt to construct a $(7,33,5)_4$ code. It turns out, however, that such codes do not exist.

2. The uniqueness of the $(6,9,5)_4$ code.

Definition 2.1. *Two q-ary codes are called equivalent if one can be obtained from the other by superposition of operations of the following types:*

a) permutation of the coordinates of the code;

b) permutation of the symbols appearing in a fixed position.

Theorem 2.2. (The sharpened Plotkin bound) [2].

If C is an $(n,M,d)_q$ code and $M = pq + r$, $0 \le r \le q-1$,

*This work was partially supported by the Aprilov National High School, Gabrovo, Bulgaria.

then $(M-1)Md \leq (M^2-\sigma)n$, *where* $\sigma = (q-r)p^2 + r(p+1)^2$.

Considering any coordinate we denote by M_j the number of codewords with value j in this coordinate, $j = 0, 1, \ldots, q-1$. An equality in Theorem 2.2 implies that the code is equidistant and that for every coordinate the multiset $\{M_0, M_1, \ldots, M_{q-1}\}$ is uniquely determined:

$$\{M_0, M_1, \ldots, M_{q-1}\} = \{ \underbrace{p+1, p+1, \ldots, p+1}_{r}, \ \underbrace{p, p, \ldots, p}_{q-r} \}$$

From Theorem 2.2 we get the following result:

Lemma 2.3. *If* C *is a quaternary code with* $n = 6,\ M = 9,\ d = 5$ *, then*
a) $dist(x, y) = 5$*, for every pair of codewords;*
b) for every coordinate $\{M_0, M_1, M_2, M_3\} = \{3, 2, 2, 2\}$.

Theorem 2.4. *There exists a unique (up to equivalence)* $(6, 9, 5)_4$ *code.*

Proof: Let C be a $(6, 9, 5)_4$ code. Let B be the 9×6 matrix, its rows being the codewords of C. Denote by B_i the i-th row, and by b_{ij} the j-th entry of the i-th row.

We may assume that the rows $B_1, B_2, \ldots, B_9$ are lexicographically ordered. The same is valid for the columns. By Lemma 2.3 we may assume without loss of generality (w.o.l.g.) that the first column is a transpose of (0 0 0 1 1 2 2 3 3). Since the Hamming distance between codewords is exactly 5, the first three rows are w.o.l.g.:

$$\begin{aligned} B_1 &= 0\,0\,0\,0\,0\,0 \\ B_2 &= 0\,1\,1\,1\,1\,1 \\ B_3 &= 0\,2\,2\,2\,2\,2 \end{aligned}$$

Consider the row $B_i,\ i = 4, 5, \ldots, 9$. Since $dist(B_1, B_i) = 5$ exactly one of b_{i2}, b_{i3}, b_{i4}, b_{i5}, b_{i6} equals '0'. Similarly from $dist(B_2, B_i) = 5$ and $dist(B_3, B_i) = 5$ it follows that among $b_{i2}, b_{i3}, b_{i4}, b_{i5}, b_{i6}$, there is exactly one '1' and exactly one '2'. Thus, we get $B_4 = 1\ 0\ 1\ 2\ 3\ 3$.

There are 6 possibilities for the fifth row. The corresponding 5×6 matrices are:

Matrix 1	Matrix 2	Matrix 3	Matrix 4	Matrix 5	Matrix 6
0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0 0 0
0 1 1 1 1 1	0 1 1 1 1 1	0 1 1 1 1 1	0 1 1 1 1 1	0 1 1 1 1 1	0 1 1 1 1 1
0 2 2 2 2 2	0 2 2 2 2 2	0 2 2 2 2 2	0 2 2 2 2 2	0 2 2 2 2 2	0 2 2 2 2 2
1 0 1 2 3 3	1 0 1 2 3 3	1 0 1 2 3 3	1 0 1 2 3 3	1 0 1 2 3 3	1 0 1 2 3 3
1 1 3 3 0 2	1 2 3 3 0 1	1 3 0 3 1 2	1 3 2 3 0 1	1 3 3 0 1 2	1 3 3 1 0 2

These 6 matrices, however, are equivalent. If we apply the permutation (0)(1,2)(3) over the elements of columns 2–6 of Matrix 1 and then rearrange the rows and the columns, we obtain Matrix 2. Similarly applying the permutations (0,1)(2)(3); (0,1,2)(3); (0,2,1)(3); (0,2)(1)(3), we obtain the rest of the matrices.

Thus the rows $B_1, \ldots, B_5$ are uniquely determined up to equivalence and we continue considerations with the Matrix 1.

If for some $i \in \{6, 7, 8, 9\}$ $b_{i2} = 0$, then $b_{i5} \neq 3$ and $b_{i6} \neq 3$, because $dist(B_4, B_i) = 5$. Hence $b_{i3} = 3$ and $b_{i4} = 3$; it follows a contradiction of $dist(B_5, B_i) = 5$.

We similarly deduce that $b_{i2} \neq 1$ for $i = 6, 7, 8, 9$.

Consequently, the second column of B is a tranpose of (0 1 2 0 1 2 3 2 3).

There are five possibilities for B_6 satisfying the conditions $dist(B_i, B_6) = 5$ for $i = 1, 2, \ldots, 5$. The sixth row must be one of:

2 2 0 3 1 3, 2 2 0 3 3 1, 2 2 3 0 1 3, 2 2 3 0 3 1, 2 2 3 1 3 0.

Replacing the first '2' by '3' we obtain all the possibilities for B_8:

3 2 0 3 1 3, 3 2 0 3 3 1, 3 2 3 0 1 3, 3 2 3 0 3 1, 3 2 3 1 3 0.

Applying the permutation (0)(1)(2,3) over the elements of the first column followed by row sorting, we transform the matrix B into an equivalent one without any difference in the first five rows and in the first two columns. These transformations interchange b_{63} and b_{83}, so we may assume that $b_{63} < b_{83}$. Hence $b_{63} = 0$ and $b_{83} = 3$.

Thus we reduce the possibilities
for B_6 to: 2 2 0 3 1 3, 2 2 0 3 3 1,
for B_8 to: 3 2 3 0 1 3, 3 2 3 0 3 1, 3 2 3 1 3 0.

There are only three possibilities for B_7 satisfying the conditions $dist(B_i, B_7) = 5$ for $i = 1, 2, \ldots, 5$, and $b_{73} \neq b_{63} = 0$.

The seventh row must be one of:

2 3 1 3 2 0, 2 3 2 1 0 3, 2 3 3 2 1 0.

Similarly the possibilities for B_9 are:

3 3 0 1 3 2, 3 3 1 3 2 0, 3 3 2 1 0 3.

Now it is easily checked that the only solution for the matrix B is:

0 0 0 0 0 0
0 1 1 1 1 1
0 2 2 2 2 2
1 0 1 2 3 3
1 1 3 3 0 2
2 2 0 3 3 1
2 3 2 1 0 3
3 2 3 0 1 3
3 3 1 3 2 0.

3. The nonexistence of $(7, 33, 5)_4$ codes.

Theorem 3.1 *There are no* $(7, 33, 5)_4$ *codes.*

Proof: Suppose there exists a $(7, 33, 5)_4$ code C. We may assume w.o.l.g. that the codewords are lexicographically sorted. Then the code C has the following structure:

$$
\begin{array}{|c|c|}
\hline
0 & \\
0 & \\
\vdots & C_0 \\
0 & \\
0 & \\
\hline
1 & \\
1 & \\
\vdots & C_1 \\
1 & \\
1 & \\
\hline
2 & \\
2 & \\
\vdots & C_2 \\
2 & \\
2 & \\
\hline
3 & \\
3 & \\
\vdots & C_3 \\
3 & \\
3 & \\
\hline
\end{array}
\begin{array}{l}
\left.\vphantom{\begin{array}{c}0\\0\\\vdots\\0\\0\end{array}}\right\} M_0 \\
\left.\vphantom{\begin{array}{c}0\\0\\\vdots\\0\\0\end{array}}\right\} M_1 \\
\left.\vphantom{\begin{array}{c}0\\0\\\vdots\\0\\0\end{array}}\right\} M_2 \\
\left.\vphantom{\begin{array}{c}0\\0\\\vdots\\0\\0\end{array}}\right\} M_3
\end{array}
$$

where C_i is a $(6, M_i, 5)_4$ code, $i = 0, 1, 2, 3$.

We may assume up to equivalence that $M_0 \geq M_1 \geq M_2 \geq M_3$; see Definition 2.1. Since $M_0 + M_1 + M_2 + M_3 = 33$, we obtain $M_0 \geq 9$. But $A_4(6, 5) = 9$ [3], hence $M_0 = 9$ and C_0 is a $(6, 9, 5)_4$ code. We may assume that C_0 is the unique $(6, 9, 5)_4$ code constructed in the proof of Theorem 2.4:

$$
C_0 = \begin{array}{cccccc}
0&0&0&0&0&0\\
0&1&1&1&1&1\\
0&2&2&2&2&2\\
1&0&1&2&3&3\\
1&1&3&3&0&2\\
2&2&0&3&3&1\\
2&3&2&1&0&3\\
3&2&3&0&1&3\\
3&3&1&3&2&0.
\end{array}
$$

The codewords of C_1, C_2, and C_3 are at distance at least 4 from the words of C_0. We generate the list L of all such vectors and it turns out that they are exactly 298.

Obviously $8 \leq M_1 \leq 9$.

Let $M_1 = 8$. Then $M_2 = M_3 = 8$ and C_1, C_2 and C_3 are $(6, 8, 5)_4$ codes with codewords from L. With a computer program we find out that there are exactly 102 possibilities for C_i, $i = 1, 2, 3$. However, a computer check shows that for every pair C', C'' from these 102 codes, there exist words $x \in C'$, $y \in C''$ for which $dist(x, y) < 4$.

Hence there are no $(7, 33, 5)_4$ codes with $M_1 = 8$.

Let $M_1 = 9$. Then C_1 is a $(6, 9, 5)_4$ code, which according to Lemma 2.3 is equidistant. Then every 8 codewords from C_1 form a $(6, 8, 5)_4$ equidistant code with $d = 5$. A computer check shows that any of the above mentioned 102 $(6, 8, 5)_4$ codes has codewords at distance 6. Hence there are no $(7, 33, 5)_4$ codes with $M_1 = 9$.

Corollary 3.2. $A_4(7, 5) = 32$.

Corollary 3.2 implies some additional improvements of the values of $A_4(n, 5)$.

Corollary 3.3. $A_4(8, 5) \leq 128, \quad A_4(9, 5) \leq 512, \quad A_4(10, 5) \leq 2048$.

Proof: Let C be an $(n, M, d)_q$ code. Considering any coordinate of C we deduce that some symbol of the alphabet appears at least $\lceil \frac{M}{q} \rceil$ times. Let C' be the code comprising the words of C with that symbol in this particular coordinate. By removing this coordinate from all codewords of C' we obtain C'' with parameters $(n-1, \lceil \frac{M}{q} \rceil, d)_q$.

Suppose there exists a $(8, 129, 5)_4$ code. Therefore, there exists a $(8, 33, 5)_4$ code; a contradiction. Hence $A_4(8, 5) \leq 128$.

The rest of the inequalities can be proved in the same way.

REFERENCES

[1] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane. Bounds for binary codes of length less than 25, *IEEE Trans. Inform. Theory*, **24** (1978), 81–93.

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

[3] G. T. Bogdanova, A. E. Brouwer, S. N. Kapralov, P. R. J. Östergård. Error-correcting Codes an Alphabet of Four Elements. *Designs, Codes and Cryptography* , (to appear).

[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] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, W. D. Smith. A new table of constant weight codes. *IEEE Trans. Inform. Theory*, **36** (1990), 1334–1380.

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

[7] 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.

[8] 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.

Kaloyan S. Kapralov
29 Trakia Str.
5300 Gabrovo, Bulgaria
e-mail: kapralov@tugab.bg

ОПТИМАЛНИТЕ КОДОВЕ НАД АЗБУКА С 4 ЕЛЕМЕНТА, С ДЪЛЖИНА 7, КОИТО ПОПРАВЯТ ДВЕ ГРЕШКИ, ИМАТ 32 КОДОВИ ДУМИ

Калоян С. Капралов

Да означим с $A_q(n, d)$ максималния обем на код с дължина n и минимално разстояние d над азбука с q елемента. Доказано е, че съществува единствен (с точност до еквивалентност) $(6, 9, 5)_4$ код, и че не съществуват $(7, 33, 5)_4$ кодове. От това следва, че $A_4(7, 5) = 32$.