МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 1999
MATHEMATICS AND EDUCATION IN MATHEMATICS, 1999
Proceedings of Twenty Eighth Spring Conference of
the Union of Bulgarian Mathematicians
Montana, April 5–8, 1999

A RECURSIVE CONSTRUCTION OF A FAMILY NONLINEAR CODES*

Galina Bogdanova, Stoian Kapralov

A recursive construction of q-ary codes with parameters (n, M, d) for $M = q + 2$, $n = \lfloor M(M-1)/4 \rfloor$ and $d = n - 1$ is presented.

Introduction. Let $H(n, q)$, $q \geq 2$ be the set of all ordered q-ary n-tuples, where the distance between two n-tuples is the number of positions in which they differ.

We call every subset of $H(n, q)$ a q-ary code of length n. The elements of a code are called codewords. If the code contains M words and the minimum distance between two distinct codewords is d, we call C a q-ary (n, M, d)-code or an $(n, M, d)_q$-code.

The next theorem states a necessary condition for the code existence.

Theorem 1 (The Plotkin bound) [1], [2]. *If C is an $(n, M, d)_q$-code, then*

$$(M-1)qd \leq M(q-1)n. \tag{1}$$

In the present paper the following theorem is proved:

Theorem 2 (The Sharpened Plotkin bound). *If C is an $(n, M, d)_q$-code and $M = pq + r$, $0 \leq r \leq q-1$, then*

$$M(M-1)d \leq (M^2 - \sigma)n. \tag{2}$$

where $\sigma = (q-r)p^2 + r(p+1)^2$.

The inequality (1) is weaker than (2). If M is multiple of q then (1) follows from (2).

The largest value of n for which an $(n, q+1, n-1)_q$ code exists was determined in [3].

In this paper the largest value of n for which an $(n, q+2, n-1)_q$ code exists is determined. It is constructively proved that this value is $n = \lfloor (q+2)(q+1)/4 \rfloor$.

New results.

Proof of Theorem 2. The result follows directly by the next two lemmas.

Lemma 3 [2]. *Let C be an $(n, M, d)_q$-code, and let $\sigma = \min \sum_{j=0}^{q-1} m_j^2$, where m_j, $j = 0, 1, \ldots, q-1$ are nonnegative integers with the sum $\sum_{j=0}^{q-1} m_j = M$. Then*

$$M(M-1)d \leq (M^2 - \sigma)n.$$

*This work was partially supported by the Bulgarian National Science Fund under Grant I–618/96.

Lemma 4. *Let m_j, $j = 0, 1, \dots, q-1$ be nonnegative integers with a sum $M = pq+r$, $0 \le r \le q-1$. Then*

$$\sum_{j=0}^{q-1} m_j^2 \ge (q-r)p^2 + r(p+1)^2.$$

Proof. If $r = 0$ it follows from the Cauchy-Buniakovski inequality, that the sum of the squares is the smallest for $m_j = p$, $j = 0, 1, \dots, q-1$ and is equal to qp^2.

Consider the case $r > 0$. Let σ be the smallest possible sum of the squares and let m_j, $j = 0, 1, \dots, q-1$ be numbers, for which σ is attained. Let $\alpha = \max(m_0, m_1, \dots, m_{q-1})$ and $\beta = \min(m_0, m_1, \dots, m_{q-1})$. If $\alpha - \beta > 1$, then replacing α by $\alpha - 1$ and β by $\beta + 1$ we obtain a new set of numbers with a sum M and a sum of the squares

$$\sigma' = \sigma - \alpha^2 - \beta^2 + (\alpha-1)^2 + (\beta-1)^2 = \sigma - 2(\alpha+\beta-1) < \sigma.$$

Therefore $\alpha - \beta \le 1$.

If $\alpha \ge p+2$, then $\beta \ge p+1$ and therefore $m_j \ge p+1$. Then $\sum_{j=0}^{q-1} \ge (p+1)q > M$, which is a contradiction. If $\beta \le p-1$, then $\alpha \ge p$, and hence $m_j \le p$. Then $\sum_{j=0}^{q-1} \le pq < M$ — a contradiction.

Hence $p \le m_j \le p+1, j = 0, 1, \dots, q-1$. Let x be the count of m_j's equal to p, and y — the count of m_j's equal to $p+1$. Then

$$\left| \begin{array}{ccccc} x & + & y & = & q \\ px & + & (p+1)y & = & pq+r \end{array} \right. .$$

In this way we obtain $x = q - r$, $y = r$. Hence $\sigma = (q-r)p^2 + r(p+1)^2$.

Example 5. At the International Mathematical Olympiad in 1998, the following problem was proposed:

In a contest, there are a candidates and b judges, where $b \ge 3$ is an odd number. Each candidate is evaluated by each judge as either pass or fail. Suppose that each pair of judges agrees on at most k candidates. Prove that

$$\frac{k}{a} \ge \frac{b-1}{2b}.$$

Solution. In fact the problem is about a binary $(a, b, a-k)$-code. We apply Theorem 2. Since $b = 2p+1$, then $\sigma = p^2 + (p+1)^2$. Then $b(b-1)(a-k) \le (b^2 - p^2 - (p+1)^2)a$, which is equivalent to the desired result.

Let $q \ge 2$. Suppose there exists a q-ary code C of length n, size $M = q+2$ and minimum distance $d = n-1$. By Theorem 2 we obtain $\sigma = q+6$, hence

$$M(M-1)(n-1) \le (M^2 - q - 6)n.$$

Therefore

$$n \le M(M-1)/4 = (q+2)(q+1)/4.$$

Thus the largest value of n for which an $(n, q+2, n-1)_q$ may exist is

$$n = \lfloor (q+2)(q+1)/4 \rfloor .$$

Denote by $A_q(n,d)$ the largest value of M for which an $(n,M,d)_q$-code exists.

In [3] the function $A_q(n, n-1)$ is investigated and there is proved that if $n \leq (q+1)q/2$ then $A_q(n, n-1) \geq q+1$. In the present paper the result is specified.

Corollary 6. *If* $\lfloor (q+2)(q+1)/4 \rfloor < n \leq (q+1)q/2$ *then* $A_q(n, n-1) = q+1$.

Theorem 7. *For any integer* $q \geq 2$ *there exists an* $(n, M, d)_q$*-code, where* $M = q+2$, $n = \lfloor (q+2)(q+1)/4 \rfloor$ *and* $d = n-1$.

Proof. For small values of q the parameters of these codes are:

q	M	n	d
2	4	3	2
3	5	5	4
4	6	7	6
5	7	10	9

The following codes are solutions of the problem for $q = 2$ and $q = 3$:

$q=2$	$q=3$
000	20011
011	02101
101	01210
110	10120
	11002

From the solutions for $q = 2$ and $q = 3$ we obtain solutions for $q = 4$ and $q = 5$ respectively:

$q=4$	$q=5$
000 0123	20011 01234
011 3012	02101 40123
101 2301	01210 34012
110 1230	10120 23401
	11002 12340
222 0000	
333 1111	33333 00000
	44444 11111

Let C_q be the matrix consisting of the $q+2$ codewords of a solution for given value of q. Combining C_q and C_2 we obtain C_{q+4} in the following way:

C_q		A	A
	000	00...0	
	011	11...1	
	101		00...0
	110		11...1

where

1) every column of the matrix C_{q+4} consists of the numbers

$$0, 0, 1, 1, 2, 3, \ldots, q, q+1, q+2, q+3;$$

2) the positions of the two zeros and the two ones is important, the positions of the other numbers in the column is of no importance;

3) A is a square matrix and $A_{i,i} = 0$, $i = 1, 2, \ldots, q+2$, $A_{i,i+1} = 1$, $i = 1, 2, \ldots, q+1$, $A_{q+2,1} = 1$.

We obtain a matrix of the codewords of a code with parameters $(n', M', d')_{q'}$, where $n' = n + 3 + 2(q+2)$, $M' = M + 4$, $q' = q + 4$. It is easily checked that $d' = n' - 1$. Using that $n = \lfloor (q+2)(q+1)/4 \rfloor$ we obtain $n' = \lfloor (q'+2)(q'+1)/4 \rfloor$.

Acknowledgment. The authors wish to thank the anonymous referee for the helpful comments and suggestions.

REFERENCES

[1] M. Plotkin, Binary Codes with Specified Minimum Distance, *IRE Trans. on Information Theory*, **6**, 1960, 445–450.

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

[3] G. T. Bogdanova, New bounds for the maximum size of nonlinear q-ary codes, *Mathematics and Education in Mathematics*, **26**, Plovdiv, 1997, 82–84.

Stoian Kapralov
Technical University
BG-5300 Gabrovo
E-mail: kapralov@tugab.bg

РЕКУРСИВНА КОНСТРУКЦИЯ НА ФАМИЛИЯ НЕЛИНЕЙНИ КОДОВЕ

Галина Богданова, Стоян Капралов

Представена е рекурсивна конструкция на q-ични кодове с параметри (n, M, d) за $M = q + 2$, $n = \lfloor M(M-1)/4 \rfloor$ и $d = n - 1$.