A LOWER BOUND ON THE SIZE OF BINARY CODES

PETER J. MCNAMARA

ABSTRACT. In this paper, we construct some nonlinear binary codes that give good (but not optimally known) lower bounds on the size of binary codes with fixed length and minimal distance.

COMMENTS

This is a construction that I came up with one day that produces good binary codes. It is not as strong as the work in [1], where the best bounds using this technique that I am aware of are achieved. The construction here is not optimised, the bound can be improved by a factor of 2 by considering $A(q, d)$ for d even instead of d odd.

1. INTRODUCTION

One of the fundamental problems in coding theory is to determine the maximum number of codewords in a code of length n and minimum distance d. For a binary alphabet, which is the only case considered in this paper, this number is customarially denoted by $A(n, d)$.

The purpose of this paper is to prove a lower bound for $A(n, d)$, generalising a technique appearing in [3, Ch 2, Ex 25], where the bound $A(n, 3) \geq 2^{n-1}/n$ is proved. Specifically we prove the following:

Theorem *Suppose that q is a power of a prime p, and $k < p$ is a non-negative integer. Then we have the following inequality:*

$$A(q, 2k + 1) \geq \frac{2^q}{(2k + 1)q^k}.$$

2. THE CONSTRUCTION

Let k be a non-negative integer, and p a prime larger than k. Let $q = p^r$ for some positive integer r, denote the finite field with q elements by $\mathbb{F}_q$, and list these elements as $f_1, f_2, \ldots, f_q$.

Let $X = \{0, 1\}^q$, and equip X with a metric given by $d(x, y) = \sum_{i=1}^{q} |x_i - y_i|$, where here and elsewhere $x = (x_1, x_2, \ldots, x_q)$ and $y = (y_1, y_2, \ldots, y_q)$. Then a code C is a subset of X and its minimal distance is given by $\inf d(x, y)$ where the infimum is taken over all $x, y \in C$ with $x \neq y$.

Let $R = \mathbb{Z}_{2k+1} \times \mathbb{F}_q^k$. Define a function $\phi : X \longrightarrow R$ by

Date: August 2005.

$$\phi(x) = \left(\sum_{i=1}^{q} x_i, \sum_{i=1}^{q} x_i f_i^1, \sum_{i=1}^{q} x_i f_i^2, \ldots, \sum_{i=1}^{q} x_i f_i^k \right).$$

Lemma 2.1. *If $\phi(x) = \phi(y)$, then $x = y$ or $d(x, y) \geq 2k + 1$.*

Proof. Suppose $\phi(x) = \phi(y)$ and $d(x, y) \leq 2k$.

Let $i_1, i_2, \ldots, i_s$ be the indices i for which $x_i = 1$ and $y_i = 0$.

Let $j_1, j_2, \ldots, j_t$ be the indices j for which $x_j = 0$ and $y_j = 1$.

As $\phi(x) = \phi(y)$, $s \equiv t \pmod{2k + 1}$, while we also have $s + t = d(x, y) \leq 2k$. Hence $s = t \leq d$.

Let $a = (f_{i_1}, f_{i_2}, \ldots, f_{i_s})$, $b = (f_{j_1}, f_{j_2}, \ldots, f_{j_s})$.

For a sequence $u = (u_1, u_2, \ldots, u_s)$ define the power sum symmetric function p_n by $p_n(u) = \sum_{i=1}^{s} u_i^n$ and the elementary symmetric function $e_n(u)$ as the coefficient of z^n in the polynomial $\prod_{i=1}^{s}(1 + zu_i)$.

Since $\phi(x) = \phi(y)$, the equality $p_n(a) = p_n(b)$ holds for $n = 1, 2, \ldots, k$.

From [2, §1, Ch 2, Ex 8] we have the identity

$$e_n = \frac{1}{n!} \begin{vmatrix} p_1 & 1 & 0 & \cdots & 0 \\ p_2 & p_1 & 2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{n-1} & p_{n-2} & \cdot & \cdots & n-1 \\ p_n & p_{n-1} & \cdot & \cdots & p_1 \end{vmatrix}.$$

Since $\mathbb{F}_q$ has characteristic greater than k, this implies that $e_n(a) = e_n(b)$ for $n = 1, 2, \ldots, k$.

As $s \leq k$, this imples that the polynomials $\prod_{m=1}^{s}(z - f_{i_m})$ and $\prod_{m=1}^{s}(z - f_{j_m})$ are equal, so have the same roots. But by definition, we must always have $i_m \neq j_n$, so this is a contradiction unless $s = 0$, in which case we have $x = y$ as required. □

We are now ready to prove our main theorem.

Theorem 2.2. *Let k, p and q be non-negative integers such that $k < p$, p is prime and q is a positive power of p. Then the following inequality holds:*

$$A(q, 2k + 1) \geq \frac{2^q}{(2k + 1)q^k}.$$

Proof. By the above lemma, for all $r \in R$, the set $\phi^{-1}(r)$ is a binary code with minimal distance at least $2k+1$. We have $|R| = (2k+1)q^k$, and $\sum_{r \in R} |\phi^{-1}(r)| = |X| = 2^q$, so there must exist $r \in R$ with $|\phi^{-1}(r)| \geq |X|/|R| = \frac{2^q}{(2k+1)q^k}$. Considering this code $\phi^{-1}(r)$ proves our theorem. □

3. Remarks

If we fix j and consider only those $x \in X$ for which the first coordinate of $\phi(x)$ is equal to j, then we obtain the slight improvement:

$$A(q, 2k + 1) \geq \frac{1}{q^k} \sum_{r \equiv j \bmod 2k+1} \binom{q}{r}.$$

It is possible to rewrite this as

$$A(q, 2k+1) \geq \frac{1}{(2k+1)q^k} \sum_{m=0}^{2k} \zeta^{-mj}(1+\zeta^m)^q$$

where ζ is a primitive $2k+1$-th root of unity. From this formulation it is evident that this bound is strongest when $q \equiv 2j \pm 1 \pmod{4k+2}$.

References

[1] H. Derksen, *Error Correcting Codes and B_h sequences*, IEEE Transactions on Information Theory, 2004, Vol 50 (3), 476–485.

[2] I. G. Macdonald, *"Symmetric Functions and Hall Polynomials,"* 2nd edition, Oxford University Press, Oxford 1995.

[3] H. S. Wilf, *"Generatingfunctionology,"* Academic Press, New York 1994.

E-mail address: petermcn@maths.usyd.edu.au