

# MDS Codes

Cary Miller

December 7, 1999

## 1 Linear Codes

Linear codes are defined algebraically. We consider an  $n$ -dimensional vector space over a finite field  $\mathbf{F}$ . If  $\mathbf{C}$  is a linear  $[n, k]$ -code over  $\mathbf{F}$  then the codewords are the vectors of a  $k$ -dimensional subspace. The minimum distance between code words in a linear code is just the minimum weight of a codeword.

A Hamming code is 1-error-correcting linear code with the properties that

- The minimum distance is 3.
- All vectors are within distance 1 of a codeword.
- The sphere-packing bound is achieved.

One of the questions we like to address is for a given  $n$  and  $k$ , what is the linear  $[n, k]$ -code with largest minimum distance between codewords? Section 5.4 answers the question and allows us to make connections between the algebra of vector spaces and the geometry of projective spaces.

The answer to the above question is given by

### **Theorem 5.4.1 (The 'Singleton bound')**

Let  $d$  be the minimum distance of a linear  $[n, n - r]$ -code. Then

$$d \leq r + 1$$

A particularly interesting case occurs when the minimum distance is equal to  $r + 1$ . This brings us to our first definition.

### **Definition: MDS Code**

A linear  $[n, n - r]$ -code is called an MDS code if  $d = r + 1$ . MDS is shorthand for maximum distance separable.

### **Lemma 5.4.2**

Let  $\mathbf{C}$  be a linear code of length  $n$  with parity check matrix  $H$ . Then

$$d(\mathbf{C}) \geq d \iff \text{every set of } d - 1 \text{ columns of } H \text{ is linearly independent.}$$

Notice in particular that the lemma is true in the case of equality.

$$d(\mathbf{C}) = d \iff \text{every set of } d - 1 \text{ columns of } H \text{ is linearly independent.}$$

## 2 Projective Spaces

We continue setting the stage by defining the geometric equivalent of a linear code.

**Definition:**  $(n, s)$ -set

A set of  $n$  points in a projective space  $\mathbf{P}$  is an  $(n, s)$ -set if  $s$  is the largest integer such that every subset of  $s$  points is independent.

Now we make the connection with

**Theorem 5.4.3**

Let  $n$  and  $r$  be positive integers. Then a linear  $[n, n - r]$ -code with minimum distance  $d$  exists if and only if there exists an  $(n, d - 1)$ -set in  $\mathbf{P} = \text{PG}(r - 1, 2)$ .

We continue with more definitions.

**Definition: cap**

A set of points in a projective space is called a cap if no three of its points are collinear.

**Definition: arc,  $k$ -arc**

Consider a  $d$ -dimensional projective space  $\mathbf{P}$ . A set of points is called an arc if any  $d + 1$  of its points are a basis. An arc with  $k$  points is called a  $k$ -arc.

**Definition: oval** (from section 4.3)

A nonempty set  $\mathcal{O}$  of points in a projective **plane** is called an oval if no three points of  $\mathcal{O}$  are collinear and each point of  $\mathcal{O}$  is on exactly one tangent.

**Definition: ovoid** (from section 4.3)

Let  $\mathbf{P}$  be a  $d$ -dimensional projective space. An ovoid is a nonempty set of points  $\mathcal{O}$  with the following properties:

- No three points of  $\mathcal{O}$  are collinear.
- For each point  $P \in \mathcal{O}$  the tangents through  $P$  cover exactly a hyperplane.

Now we make a statement about the existence of MDS codes using geometric language.

**Corollary 5.4.4**

Let  $n$  and  $r$  be positive integers. Then a linear MDS  $[n, n - r]$ -code with minimum distance 4 exists if and only if in  $\text{PG}(r - 1, 2)$  there is a cap with exactly  $n$  points.

Up to this point we have been dealing strictly with codes over  $\{0, 1\}^n$ , an  $n$ -dimensional vector space over the binary field. For the rest of the section we consider the field  $\text{GF}(q)$  where  $q = p^e$ .

Now we are in a position to restate the problem of finding codes with given minimum distance.

**Definition:**  $\max_{d-1}(r, q)$ 

Let  $d$  and  $r$  be positive integers. Determine the largest number  $n$  such that there is an  $(n, d - 1)$ -set in  $\text{PG}(r - 1, q)$ . The maximum  $n$  is denoted  $\max_{d-1}(r, q)$ .

Recall the definition of an  $(n, d - 1)$ -set in the projective space  $\mathbf{P}$ . It is a set of  $n$  points such that  $d - 1$  is the largest number for which every  $d - 1$  subset is independent. Theorem 5.4.3 allows us to associate an  $(n, d - 1)$ -set in  $\text{PG}(r - 1, 2)$  with a linear code  $\mathbf{C}$  with dimension  $n - r$  and minimum distance  $d - 1$  in  $\mathbf{V} = \text{GF}(2)^n$ .

### 3 The Geometry of MDS Codes

The problem of finding the numbers  $\max_2(r, q)$  for all  $r$  and  $q$  is solved because it is merely the trivial problem of finding the largest number of points such that any two distinct points are not the same. This is the number of points in the space  $\text{PG}(r - 1, q)$ . The same question is unsolved if we increase the number of independent points to three. Nevertheless we do have partial results for  $\max_3(r, q)$  as illustrated by the final three theorems of the section.

**Theorem 5.4.5**

(a)  $\max_3(r, 2) = 2^{r-1}$

(b)  $\max_3(3, q) = \begin{cases} q + 1 & \text{if } q \text{ is odd} \\ q - 1 & \text{if } q \text{ is even} \end{cases}$

In order to prove the second half of the theorem 5.4.5(b) we need the proof of

**Theorem 5.4.6** (Qvist 1952)

Let  $\alpha$  be a  $(q + 1)$ -arc in a finite projective **plane** of order  $q$ . If  $q$  is even then there exists a point  $X$  (the **nucleus** of  $\alpha$ ) such that all tangents of  $\alpha$  pass through  $X$ . This means that  $\alpha$  can be extended to a  $(q + 2)$ -arc  $\alpha \cup X$ .

**Definition: hyperoval**

The  $(q + 2)$ -arcs obtained above in theorem 5.4.6 are called hyperovals.

**Theorem 5.4.7**

If  $q > 2$ , then  $\max_3(4, q) = q^2 + 1$