11

MDS codes

§1. Introduction

We come now to one of the most fascinating chapters in all of coding theory: MDS codes. In Theorem 11 of Ch. 1 it was shown that for a linear code over any field, $d \leq n-k+1$. Codes with $d=n-k+1$ are called *maximum distance separable*, or MDS for short. The name comes from the fact that such a code has the *maximum* possible *distance* between codewords, and that the codewords may be *separated* into message symbols and check symbols (i.e. the code has a systematic encoder, using the terminology of §7 of Ch. 10). In fact *any* k symbols may be taken as message symbols, as Corollary 3 shows. MDS codes are also called *optimal*, but we prefer the less ambiguous term.

In this chapter various properties of MDS codes will be derived. We shall also see that the problem of finding the longest possible MDS code with a given dimension is equivalent to a surprising list of combinatorial problems, none of which is completely solved – see Research Problem 11.1a to 11.1f. In Fig. 11.2 and Research Problem 11.4 we state what is conjectured to be the solution to some of these problems.

In §2 of the preceding chapter it was shown that there is an $[n=q-1, k, d=n-k+1]$ Reed–Solomon (or RS) code over GF(q), for all $k=1,\ldots,n$, and that these codes are MDS codes. Furthermore in §3 an overall parity check was added producing $[n+1, k, n-k+2]$ extended RS codes, also MDS. It is natural to ask if more parity checks can be added, while preserving the property of being MDS. The answer seems to be (§§5, 7 below) that one or two further parity checks can be added, but probably no more. More generally, we state the first version of our problem.

Research Problem (11.1a). Given k and q, find the largest value of n for which an $[n, k, n-k+1]$ MDS code exists over GF(q). Let $m(k, q)$ denote this largest value of n.

It will turn out that in all the known cases, when an $[n, k, d]$ MDS code exists, then an $[n, k, d]$ RS or extended RS code with the same parameters also exists. Thus as far as is known at present, RS and extended RS codes are the most important class of MDS codes. For this reason we don't give a separate discussion of decoding MDS codes but refer to §10 of Ch. 10.

Problem. (1) Show that $[n, 1, n]$, $[n, n-1, 2]$ and $[n, n, 1]$ MDS codes exist over any field. These are called *trivial* MDS codes. For a nontrivial code, $2 \leq k \leq n-2$.

§2. Generator and parity check matrices

Let $\mathscr{C}$ be an $[n, k, d]$ code over GF(q) with parity check matrix H and generator matrix G.

Theorem 1. *$\mathscr{C}$ is* MDS *iff every $n-k$ columns of H are linearly independent.*

Proof. $\mathscr{C}$ contains a codeword of weight w iff w columns of H are linearly dependent (Theorem 10 of Ch. 1). Therefore $\mathscr{C}$ has $d = n-k+1$ iff no $n-k$ or fewer columns of H are linearly dependent. Q.E.D.

Theorem 2. *If $\mathscr{C}$ is* MDS *so is the dual code $\mathscr{C}^{\perp}$.*

Proof. H is a generator matrix for $\mathscr{C}^{\perp}$. From Theorem 1, any $n-k$ columns of H are linearly independent, so only the zero codeword is zero on as many as $n-k$ coordinates. Therefore $\mathscr{C}^{\perp}$ has minimum distance at least $k+1$, i.e. it has parameters $[n, n-k, k+1]$. Q.E.D.

Example.

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \beta \end{pmatrix}$$

is the generator matrix for a $[4, 2, 3]$ MDS code $\mathscr{C}$ over GF(4) =

$\{0, 1, \alpha, \beta = \alpha^2\}$. The dual code $\mathscr{C}^\perp$ has generator matrix

$$\begin{pmatrix} 1 & \alpha & 1 & 0 \\ 1 & \beta & 0 & 1 \end{pmatrix}$$

and is also a $[4, 2, 3]$ MDS code.

Corollary 3. *Let* $\mathscr{C}$ *be an* $[n, k, d]$ *code over* GF(q). *The following statements are equivalent*:

(i) $\mathscr{C}$ *is* MDS;

(ii) *every* k *columns of a generator matrix* G *are linearly independent* (*i.e. any* k *symbols of the codewords may be taken as message symbols*);

(iii) *every* $n-k$ *columns of a parity check matrix* H *are linearly independent.*

Proof. From Theorems 1 and 2. Q.E.D.

The open problem can now be restated as

Research Problem (11.1b). Given k and q, find the largest n for which there is a $k \times n$ matrix over GF(q) having every k columns linearly independent.

Equivalently, in vector space terminology:

Research Problem (11.1c). Given a k-dimensional vector space over GF(q), what is the largest number of vectors with the property that any k of them form a basis for the space?

Problems. (2) Show that the only binary MDS codes are the trivial ones.

(3) The Singleton bound for nonlinear codes. If $\mathscr{C}$ is an (n, M, d) code over GF(q), show that $d \leq n - \log_q M + 1$.

§3. The weight distribution of an MDS code

Surprisingly, the Hamming weight distribution of an MDS code is completely determined.

Theorem 4. *Let* $\mathscr{C}$ *be an* $[n, k, d]$ *code over* GF(q). *Then* $\mathscr{C}$ *is* MDS *iff* $\mathscr{C}$ *has a minimum weight codeword in any* d *coordinates.*

Proof. (Only if.) Given any $n-k+1$ coordinates, take one of them together with the complementary $k-1$ coordinates as message symbols (which can be done by Corollary 3). Setting the single coordinate equal to 1 and the $k-1$ to 0 gives a codeword of weight $n-k+1$. The proof of the converse is left to the reader. Q.E.D.

Corollary 5. *The number of codewords in $\mathscr{C}$ of weight $n-k+1$ is*

$$(q-1)\binom{n}{n-k+1}.$$

An MDS code has k distinct nonzero weights, $n-k+1,\ldots,n$, and the dual code has minimum distance $d'=k+1$. Therefore by Theorem 29 of Ch. 6, the codewords of weight d form a t-design, which however by Theorem 4 is just a trivial design. Theorem 4 of Ch. 6 also determines the weight distribution, but in this case it is easier to begin from the MacWilliams identities in the form of Problem (6) of Ch. 5, namely

$$\sum_{i=0}^{n-j}\binom{n-i}{j}A_i=q^{k-j}\sum_{i=0}^{j}\binom{n-i}{j-i}A'_i,\quad j=0,1,\ldots,n.$$

Since $A_i=0$ for $1\leqslant i\leqslant n-k$ and $A'_i=0$ for $1\leqslant i\leqslant k$, this becomes

$$\sum_{i=n-k+1}^{n-j}\binom{n-i}{j}A_i=\binom{n}{j}(q^{k-j}-1),\quad j=0,1,\ldots,k-1.$$

Setting $j=k-1$ and $k-2$ gives

$$A_{n-k+1}=\binom{n}{k-1}(q-1),$$

$$\binom{k-1}{k-2}A_{n-k+1}+A_{n-k+2}=\binom{n}{k-2}(q^2-1),$$

$$A_{n-k+2}=\binom{n}{k-2}[(q^2-1)-(n-k+2)(q-1)].$$

It is not hard to guess (and to verify) that the general solution is

$$A_{n-k+r}=\binom{n}{k-r}\sum_{j=0}^{r-1}(-1)^j\binom{n-k+r}{j}(q^{r-j}-1).$$

Hence we have

Theorem 6. *The number of codewords of weight w in an* $[n,k,d=n-k+1]$

MDS *code over* GF(q) *is*

$$A_w = \binom{n}{w}\sum_{j=0}^{w-d}(-1)^j\binom{w}{j}(q^{w-d+1-j}-1)$$
$$= \binom{n}{w}(q-1)\sum_{j=0}^{w-d}(-1)^j\binom{w-1}{j}q^{w-d-j}.$$

We note that

$$A_{n-k+2} = \binom{n}{k-2}(q-1)(q-n+k-1).$$

This number must be nonnegative, hence

Corollary 7. *Let* $\mathscr{C}$ *be an* $[n, k, n-k+1]$ MDS *code. If* $k \geq 2$, $q \geq n-k+1$. *If* $k \leq n-2$, $q \geq k+1$.

Proof. The second statement follows from examining the weight distribution of $\mathscr{C}^\perp$. Q.E.D.

Problems. (4) Prove the converse part of Theorem 4.

(5) A *real code* consists of all linear combinations with real coefficients of the rows of a generator matrix $G = (q_{ij})$, where the q_{ij} are real numbers. Justify the statement that most real codes are MDS.

Research Problem (11.2). What can be said about the complete weight enumerator (see §6 of Ch. 5) of an MDS code, or even of an RS code?

§4. Matrices with every square submatrix nonsingular

Theorem 8. *An* $[n, k, d]$ *code* $\mathscr{C}$ *with generator matrix* $G = [I \mid A]$, *where* A *is a* $k \times (n-k)$ *matrix, is* MDS *iff every square submatrix* (*formed from any* i *rows and any* i *columns, for any* $i = 1, 2, \ldots,$ $\min\{k, n-k\}$) *of* A *is nonsingular.*

Proof. ($\Rightarrow$) Suppose $\mathscr{C}$ is MDS. By Corollary 3, every k columns of G are linearly independent. The idea of the proof is very simple and we shall just illustrate it by proving that the top right 3×3 submatrix A' of A is nonsingular. Take the matrix B consisting of the last $k-3$ columns of I and the first 3 columns of A:

$$B = \begin{array}{|c|c|}\hline 0 & A' \\ \hline \begin{matrix} 1 & & & \\ & 1 & & \\ & & \cdots & \\ & & & 1 \end{matrix} & \\ \hline \end{array}$$

Then $\det B = \det A' \neq 0$. The general case is handled in the same way. ($\Leftarrow$) The converse is immediate. Q.E.D.

Examples. (1) The $[4, 2, 3]$ code over GF(4) shown in Fig. 10.2 has

$$A = \begin{bmatrix} \beta & \alpha \\ \alpha & \beta \end{bmatrix},$$

and indeed every square submatrix of A (of size 1 and 2) is nonsingular.

(2) The $[5, 2, 4]$ extended RS code over GF(5) has

$$A = \begin{bmatrix} 3 & 4 & 2 \\ 3 & 2 & 4 \end{bmatrix}.$$

From Theorem 8 the next version of our problem is:

Research Problem (11.1d). Given k and q, find the largest r such that there exists a $k \times r$ matrix having entries from GF(q) with the property that every square submatrix is nonsingular.

Problem. (6) (Singleton.) Show that any rectangular submatrix A of the arrays in Fig. 11.1 has the property that any $k \times k$ submatrix of A is nonsingular over GF(q).

$$q = 5 \quad \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & \\ 1 & 4 & & \end{array} \qquad q = 7 \quad \begin{array}{cccccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 6 & 4 & 2 & 5 \\ 1 & 6 & 4 & 2 & 5 & \\ 1 & 4 & 2 & 5 & & \\ 1 & 2 & 5 & & & \\ 1 & 5 & & & & \end{array}$$

Fig. 11.1.

Research Problem (11.3). Generalize Fig. 11.1. for larger q.

Problem. (7) (a) Show that any square submatrix of a Vandermonde matrix with real, positive entries is nonsingular. Show that this is not true for Vandermonde matrices over finite fields.

(b) Given $x_1, \ldots, x_n, y_1, \ldots, y_n$ the matrix $C = (c_{ij})$ where $c_{ij} = 1/(x_i + y_j)$ is called a *Cauchy matrix*. Show that

$$\det(C) = \frac{\prod_{1 \leq i < j \leq n} (x_j - x_i)(y_j - y_i)}{\prod_{1 \leq i, j \leq n} (x_i + y_j)}.$$

Hence, provided the x_i are distinct, the y_i are distinct, and $x_i + y_j \neq 0$ for all i, j, it follows that any square submatrix of a Cauchy matrix is nonsingular over any field.

§5. MDS codes from RS codes

Let $\alpha_1, \ldots, \alpha_{q-1}$ be the nonzero elements of GF(q). The $[q, k, d = q - k + 1]$ extended RS code of §3 of Ch. 10 has parity check matrix

$$H_1 = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ \alpha_1 & \cdots & \alpha_{q-1} & 0 \\ \alpha_1^2 & \cdots & \alpha_{q-1}^2 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{q-k-1} & \cdots & \alpha_{q-1}^{q-k-1} & 0 \end{bmatrix}.$$

One more parity check can always be added, producing a $[q + 1, k, q - k + 2]$ MDS code, by using the parity check matrix

$$H_2 = \begin{bmatrix} 1 & \cdots & 1 & 1 & 0 \\ \alpha_1 & \cdots & \alpha_{q-1} & 0 & 0 \\ \alpha_1^2 & \cdots & \alpha_{q-1}^2 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{q-k} & \cdots & \alpha_{q-1}^{q-k} & 0 & 1 \end{bmatrix}. \tag{1}$$

To show this, we must verify that any $q - k + 1$ columns of H_2 are linearly independent, i.e. form a nonsingular matrix. In fact, any $q - k + 1$ of the first $q - 1$ columns form a Vandermonde matrix (Lemma 17 of Ch. 4) and are nonsingular. Similarly, given any $q - k + 1$ columns which include one or both of the last two columns, we expand about these columns and again obtain a Vandermonde matrix.

In fact, there exist cyclic codes with the same parameters.

Theorem 9. *For any k, $1 \leq k \leq q + 1$, there exists a $[q + 1, k, q - k + 2]$ cyclic* MDS *code over* GF(q).

Proof. We only prove the case $q = 2^m$, the case of odd q being similar. To exclude the trivial cases we assume $2 \leq k \leq q - 1$. Consider the polynomial $x^{2^m+1} + 1$ over GF(2^m). The cyclotomic cosets, under multiplication by 2^m and reduction modulo $2^m + 1$, are

$$\begin{array}{c}
\{0\} \\
\{1, 2^m\} = \{1, -1\} \\
\{2, 2^m - 1\} = \{2, -2\} \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\{2^{m-1}, 2^{m-1} + 1\} = \{2^{m-1}, -2^{m-1}\}.
\end{array}$$

For example, if $2^m + 1 = 33$ we have the cyclotomic cosets

$$\begin{array}{ll}
\{0\} & \\
\{1, 32\} & \{9, 24\} \\
\{2, 31\} & \{10, 23\} \\
\{3, 30\} & \{11, 22\} \\
\{4, 29\} & \{12, 21\} \\
\{5, 28\} & \{13, 20\} \\
\{6, 27\} & \{14, 19\} \\
\{7, 26\} & \{15, 18\} \\
\{8, 25\} & \{16, 17\}
\end{array}$$

Thus $x^{2^m+1} + 1$ has, besides $x + 1$, only quadratic factors over GF(2^m), and these are of the form

$$x^2 + (\alpha^i + \alpha^{-i})x + 1 = (x + \alpha^i)(x + \alpha^{-i}),$$

where α is a primitive ($2^m + 1$)-st root of unity. Now $\alpha \in$ GF(2^{2m}); in fact if ξ is a primitive element of GF(2^{2m}) we may take $\alpha = \xi^{2^m-1}$.

Problem. (8) With this value of α show $\alpha^i + \alpha^{-i}$ is in GF(2^m).

Now consider the $[2^m + 1, 2^m + 1 - 2t - 1]$ cyclic code with generator polynomial

$$(x + 1) \prod_{i=1}^{t} (x^2 + (\alpha^i + \alpha^{-i})x + 1).$$

This has $2t + 1$ consecutive zeros

$$\alpha^{-t}, \alpha^{-t+1}, \ldots, \alpha^{-1}, 1, \alpha, \ldots, \alpha^{t-1}, \alpha^t;$$

thus by the BCH bound the minimum distance is at least $2t + 2$. Since $n = 2^m + 1$, $k = 2^m + 1 - 2t - 1$, $n - k + 1 = 2t + 2$, and the code is MDS. This constructs the desired codes for all even values of k.

Similarly the code with generator polynomial

$$\prod_{i=2^{m-1}-t+1}^{2^{m-1}} (x^2+(\alpha^i+\alpha^{-i})x+1)$$

has the $2t$ consecutive zeros

$$\alpha^{2^{m-1}-t+1}, \ldots, \alpha^{2^{m-1}}, \alpha^{2^{m-1}+1}, \ldots, \alpha^{2^{m-1}+t},$$

and is a $[2^m+1, 2^m+1-2t, 2t+1]$ MDS code. This gives the desired codes for all odd k. Q.E.D.

Example. Codes of length $n=9$ over GF(2^3). Let ξ be a primitive element of GF(2^6), $\beta=\xi^9$ a primitive element of GF(2^3), and $\alpha=\xi^7$ a primitive 9th root of unity. Then from Fig. 4.5, $\beta^3=\beta^2+1$, and

$$\alpha+\alpha^{-1}=\xi^7+\xi^{56}=\beta^5, \qquad \alpha^2+\alpha^{-2}=\xi^{14}+\xi^{49}=\beta^3,$$
$$\alpha^3+\alpha^{-3}=\xi^{21}+\xi^{42}=1, \qquad \alpha^4+\alpha^{-4}=\xi^{28}+\xi^{35}=\beta^6.$$

Therefore

$$x^9+1=(x+1)(x^2+x+1)(x^2+\beta^3x+1)(x^2+\beta^5x+1)(x^2+\beta^6x+1).$$

The code over GF(8) with check polynomial x^2+x+1 is degenerate (for x^2+x+1 divides x^3+1, see Lemma 8 of Chapter 8). It is a $[9,2,6]$ code with idempotent $x+x^2+x^4+x^5+x^7+x^8$, or 011011011 using an obvious notation.

The other three codes of dimension 2 are $[9,2,8]$ codes. Their idempotents are readily found to be:

Idempotent									*Check polynomial*
1	x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	
0	β^3	β^6	1	β^5	β^5	1	β^6	β^3	$x^2+\beta^3x+1$
0	β^5	β^3	1	β^6	β^6	1	β^3	β^5	$x^2+\beta^5x+1$
0	β^6	β^5	1	β^3	β^3	1	β^5	β^6	$x^2+\beta^6x+1$

The codes with these idempotents are minimal codes (§3 of Ch. 8) and consist of the 9 cyclic shifts of the idempotent and their scalar multiples. The code with generator polynomial $x^2+\beta^6x+1$ and zeros α^4, α^{-4} is a $[9,7,3]$ code. The polynomial $(x+1)(x^2+\beta^5x+1)$ has zeros α^{-1}, 1, α and generates a $[9,6,4]$ code; the polynomial $(x^2+x+1)(x^2+\beta^6x+1)$ has zeros α^3, α^4, α^5, α^6 and generates a $[9,5,5]$ code, and so on.

Problem. (9) Find the idempotents and weight distributions of these codes.

The case $k=3$ and q even. There are just two known cases when another parity check can be added: when $q=2^m$ and $k=3$ or $k=q-1$.

Theorem 10. *There exist* $[2^m+2, 3, 2^m]$ *and* $[2^m+2, 2^m-1, 4]$ *triply-extended* RS (*and* MDS) *codes.*

Proof. Use the matrix

$$\begin{bmatrix} 1 & \cdots & 1 & 1 & 0 & 0 \\ \alpha_1 & \cdots & \alpha_{q-1} & 0 & 1 & 0 \\ \alpha_1^2 & \cdots & \alpha_{q-1}^2 & 0 & 0 & 1 \end{bmatrix} \qquad (2)$$

as either generator or parity check matrix. Any 3 columns are linearly independent, since the α_i^2 are all distinct. Q.E.D.

§6. *n*-arcs

There is also a connection between MDS codes and finite geometries. From Corollary 3 we see that the problem of finding an $[n, k, n-k+1]$ MDS code $\mathscr{C}$ can be looked at as the geometric problem of finding a set S of n points in the projective geometry $PG(k-1, q)$ (see Appendix B) such that every k points of S are linearly independent, i.e. such that no k points of S lie on a hyperplane. The coordinates of the points are the columns of a generator matrix of $\mathscr{C}$.

For example, the columns of (2) comprise 2^m+2 points in the projective plane $PG(2, 2^m)$ such that no three points lie on a line.

Definition. An *n-arc* is a set of n points in the geometry $PG(k-1, q)$ such that no k points lie in a hyperplane $PG(k-2, q)$, where $n \geqslant k \geqslant 3$. E.g. (2) shows a (2^m+2)-arc in $PG(2, 2^m)$.

Thus another version of our problem is:

Research Problem (11.1e). Given k and q, find the largest value of n for which there exists an n-arc in $PG(k-1, q)$.

There is an extensive geometrical literature on this problem, but we restrict ourselves to just one theorem.

Theorem 11. *If* $\mathscr{C}$ *is a nontrivial* $[n, k \geqslant 3, n-k+1]$ MDS *code over* GF(q), q *odd, then* $n \leqslant q+k-2$. *Equivalently, for any n-arc in* $PG(k-1, q)$, q *odd,* $n \leqslant q+k-2$.

Proof. Let $G = (g_{ij})$ be a $k \times n$ generator matrix of $\mathscr{C}$, let $r_1, \ldots, r_k$ denote the rows of G, and let C be the 0-chain in PG$(k-1, q)$ consisting of the points whose coordinates are the columns of G. A generic point of PG$(k-1, q)$ will be denoted by $(x_1, \ldots, x_k)$. It is clear that the hyperplane $x_1 = 0$ meets C in those points for which $g_{1i} = 0$. Therefore the weight of the first row, r_1, of G equals n − number of points in which the hyperplane $x_1 = 0$ meets C. Similarly the weight of the codeword $\Sigma_{i=1}^{k} \lambda_i r_i$ of $\mathscr{C}$ equals n − number of points in which the hyperplane $\Sigma_{i=1}^{k} \lambda_i x_i = 0$ meets C.

We know from Corollary 7 that $n \leqslant q + k - 1$. Suppose now $n = q + k - 1$, which implies $A_{n-k+2} = 0$. Then C meets the hyperplanes of PG$(k-1, q)$ in $k-1$, $k-3$, $k-4, \ldots, 1$, or 0 points (but not $k-2$ since there are no codewords of weight $n-k+2$).

Pick a hyperplane which contains $k-3$ points of C, say $P_1, \ldots, P_{k-3}$. Let Σ be a subspace PG$(k-3, q)$ lying in this hyperplane and containing $P_1, \ldots, P_{k-3}$. Any hyperplane through Σ must meet C in 2 or 0 more points. Let r be the number which meet C in 2 more points. The union of all these hyperplanes is PG$(k-1, q)$, so certainly contains all the points of C. Therefore

$$2r + k - 3 = q + k - 1,$$

or $2r = q + 2$, which is a contradiction since q is odd. Q.E.D.

§7. The known results

For $k = 3$ and q odd, Theorem 11 says $n \leqslant q + 1$, and so the codes of Theorem 9 have the largest possible n. Thus one case of Research Problem 11.1a is solved: $m(3, q) = q + 1$ if q is odd.

On the other hand for $k = 3$ and q even, $n \leqslant q + 2$ by Corollary 7, and the codes of Theorem 10 show that $m(3, q) = q + 2$ if q is even.

The results for general k are best shown graphically. Figure 11.2 gives the values of k and r for which an $[n = k + r, k]$ MDS code over GF(q) is known to exist (thus r is the number of parity checks).

By Corollary 2 the figure is symmetric in k and r. Apart from the codes of Theorem 10, no code is known which lies above the broken line $n = k + r = q + 1$ $(r \geqslant 2, k \geqslant 2)$. Codes above the heavy line are forbidden by Corollary 7.

There is good evidence that the broken line is the true upper bound, and we state this as:

Research Problem (11.4). Prove (or disprove) that all MDS codes, with the exception of those given in Theorem 10, lie beneath the line $n = k + r = q + 1$ in Fig. 11.2.

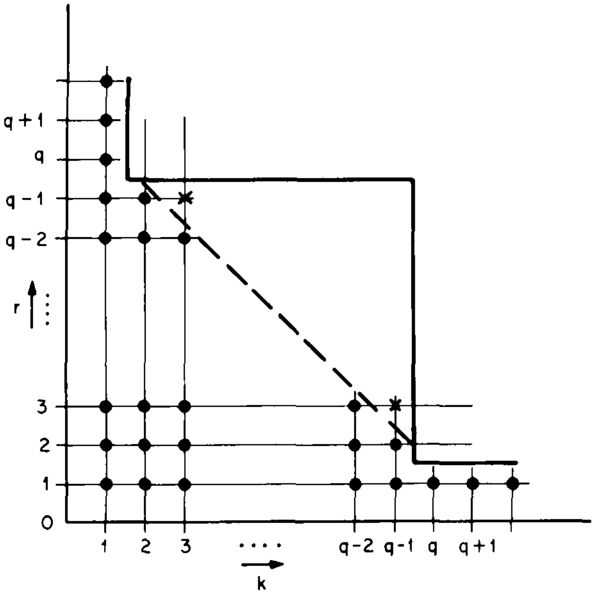

Fig. 11.2. The best $[n = k + r, k]$ MDS codes known. ● means a code exists for all q; × means a code exists iff $q = 2^m$.

This is known to be true for codes with $k \leq 5$, or $q \leq 11$, or $q > (4k - 9)^2$, and in some other cases.

Stated in terms of the function $m(k, q)$ the conjecture is that

$$m(k, q) = \begin{cases} q + 1 \text{ for } & 2 \leq k \leq q, \\ k + 1 \text{ for } & q < k, \end{cases} \tag{3}$$

except for

$$m(3, q) = m(q - 1, q) = q + 2 \quad \text{if} \quad q = 2^m. \tag{4}$$

§8. Orthogonal arrays

Definition. An $M \times n$ matrix A with entries from a set of q elements is called an *orthogonal array* of *size M*, *n constraints*, *q levels*, *strength k*, and *index* λ if any set of k columns of A contains all q^k possible row vectors exactly λ times. Such an array is denoted by (M, n, q, k). Clearly $M = \lambda q^k$. The case $q = 2$ was considered in Theorem 8 of Ch. 5.

Examples. The code $\mathscr{A}_{12}$ of Fig. 2.1 is a (12, 11, 2, 2) (see Theorem 8 of Ch. 5). Fig. 11.3 shows a (4, 3, 2, 2), and the codewords in Fig. 10.1 form a (16, 3, 4, 2) with entries from GF(4).

$$\begin{bmatrix} 1 & 1 & 1 \\ - & 1 & - \\ 1 & - & - \\ - & - & 1 \end{bmatrix}$$

Fig. 11.3. A (4, 3, 2, 2) orthogonal array.

Theorem 12. *The rows of a* (q^k, n, q, k) *linear orthogonal array* A *of index unity and symbols from* GF(q) *are the codewords of an* $[n, k]$ MDS *code over* GF(q), *and conversely.*

Proof. Any $q^k \times k$ submatrix of A contains each k-tuple exactly once $\Leftrightarrow$ the corresponding k coordinates can be taken as message symbols $\Leftrightarrow$ the code is MDS, by Corollary 3. Q.E.D.

Problem. (10) Show that if $H_{4\lambda}$ is a normalized Hadamard matrix of order 4λ (§3 of Ch. 2), then the last $4\lambda - 1$ columns of $H_{4\lambda}$ form a $(4\lambda, 4\lambda - 1, 2, 2)$ orthogonal array of index λ. Fig. 11.3 is the case $\lambda = 1$.

Thus the final version of our problem is:

Research Problem (11.1f). Find the greatest possible n in a (q^k, n, q, k) orthogonal array of index unity.

Notes on Chapter 11

§1. Singleton [1214] seems to have been the first to explicitly study MDS codes. However in 1952 Bush [220] had already discovered Reed–Solomon codes and the extensions given in Theorems 9 and 10, using the language of orthogonal arrays (§8).

Some other redundant residue codes besides RS codes are also MDS – see §9 of Ch. 10.

Assmus and Mattson [41] have shown that MDS codes whose length n is a prime number π are very common, by showing that every cyclic code of length π over GF(p^i) is MDS for all i, for all except a finite number of primes p.

Without giving any details we just mention that an MDS code with $k = 2$ is also equivalent to a set of $n - k$ mutually orthogonal Latin squares of order q (Denes and Keedwell [371, p. 351], Posner [1068], Singleton [1214]). Therefore the more general problem of finding MDS codes over alphabets of size s (i.e. not necessarily over a field) includes the very difficult problem of finding all projective planes! (See Appendix B.)

§3. The weight distribution of MDS codes was found independently by Assmus, Gleason, Mattson and Turyn [50], Forney and Kohlenberg [436], and Kasami, Lin and Peterson [736]. Our derivation follows Goethals [491]. See also [933].

Corollary 7 is due to Bush. It is also given in [1214] and by Borodin [172]. Our proof follows Robillard [1118].

§4. For Problem 7 see Knuth [772, p. 36] and Pólya-Szegö [1067, vol. 2, p. 45].

§5. See the Notes to §3 of Ch. 10.

§6. Segre [1170–1173] and later Thas [1316, 1317], Casse [252], Hirschfeld [655] and many others have studied n-arcs and related problems in finite geometries. Two recent surveys are Barlotti [69, 70]. See also Dowling [385], Gulati et al. [565–569].

Using methods of algebraic geometry Segre [1170; 1173, p. 312] and Casse [252] have improved Theorem 11 as follows:

Theorem 13. *Assume* $q \geqslant k+1$.
(i) *If* $k = 3$, 4 *or* 5 *then* (3) *and* (4) *hold.*
(ii) *If* $k \geqslant 6$ *then* $m(k, q) \leqslant q + k - 4$.

Thas [1316] has shown:

Theorem 14. *For* q *odd and* $q > (4k-9)^2$, $m(k, q) = q + 1$.

Maneri, Silverman, and Jurick ([904, 905, 703]) have shown

Theorem 15. (3) *and* (4) *hold for* $q \leqslant 11$.

Other conditions under which (3) and (4) hold are given by Thas [1318]. It also follows from the geometrical theory that if q is odd then in many (conjecturally all) cases there is an unique $[n = q+1, k, q-k+2]$ MDS code. But if q is even this is known to be false.

In a projective plane of order h, a set C of $h+1$ points no 3 of which are collinear is called an *oval.* Segre [1171; 1173, p. 270] has shown that in a Desarguesian plane of odd order (i.e. $h = q$, an odd prime power) these points form a conic. For example, if we take the columns of the generator matrix ((2)

without the penultimate column) of the $[q+1, 3, q-1]$ MDS code as the points, we see that they satisfy the equation $x_2^2 = x_1 x_3$.

If however $q = 2^m$, all lines which meet the oval C in a single point are concurrent; the point in which they meet is called the *nucleus* or *knot* of C. The points of C together with the nucleus give $2^m + 2$ points no 3 of which are collinear, and give a $[2^m + 2, 3, 2^m]$ MDS code with the same parameters as the code given in Theorem 10.