MTH6018 Coding Theory – Solutions 11

April 15, 2021

1. For which values of $s \geq 0$, if any, is $R(s, s+2)$ an MDS code? What about $R(s, s+3)$?

   An MDS code is precisely an $[n, k, d]$-code such that $n - k + 1 = d$. For $R(s, s+2)$ we have $n = 2^{s+2}$, $k = \sum_{j=0}^{s} \binom{s+2}{j}$, $d = 2^{(s+2)-s} = 4$, so $R(s, s+2)$ is an MDS code if and only if $2^{s+2} - \sum_{j=0}^{s} \binom{s+2}{j} + 1 = 4$. We have $\sum_{j=0}^{s+2} \binom{s+2}{j} = 2^{s+2}$ by Lemma 6.3, so

   $$\sum_{j=0}^{s} \binom{s+2}{j} = 2^{s+2} - \binom{s+2}{s+1} - \binom{s+2}{s+2} = 2^{s+2} - (s+2) - 1.$$

   Thus $R(s, s+2)$ is an MDS code if and only if

   $$2^{s+2} - \big(2^{s+2} - (s+2) - 1\big) + 1 = 4$$

   which is to say if and only if

   $$s + 4 = 4.$$

   Thus $R(0, 2)$ is an MDS code but no other Reed-Muller code of the form $R(s, s+2)$ is an MDS code.

   For $R(s, s+3)$, since

   $$\sum_{j=0}^{s} \binom{s+3}{j} = 2^{s+3} - \binom{s+3}{s+1} - \binom{s+3}{s+2} - \binom{s+3}{s+3} = 2^{s+3} - \frac{(s+3)(s+2)}{2} - (s+3) - 1$$

   and $d(R(s, s+3)) = 2^{s+3-s} = 8$, we can similarly calculate that $R(s, s+3)$ is an MDS code if and only if

   $$2^{s+3} - \left(2^{s+3} - \frac{(s+3)(s+2)}{2} - (s+3) - 1\right) + 1 = 8$$

   which holds if and only if

   $$\frac{(s+3)(s+2)}{2} + (s+3) + 2 = 8,$$

   if and only if $(s+3)(s+4) = 12$. The only non-negative integer solution is $s = 0$.

2. For which values of $r, q \geq 2$ is $\mathrm{Ham}(r, q)$ an MDS code?

   An MDS code is precisely an $[n, k, d]$-code such that $n - k + 1 = d$, or equivalently, a code such that the minimum distance is one plus the redundancy. The redundancy of a linear code is the number of rows in its parity-check matrix, $n - k$. So the redundancy of $\mathrm{Ham}(r, q)$ is precisely the parameter r, which is the number of rows in the parity-check matrix for $\mathrm{Ham}(r, q)$. So $\mathrm{Ham}(r, q)$ is an MDS code when $r + 1 = d(\mathrm{Ham}(r, q))$. But $d(\mathrm{Ham}(r, q)) = 3$, so this happens precisely when $r = 2$. Therefore $\mathrm{Ham}(2, q)$ is an MDS code for every prime power q, but when $r > 2$, $\mathrm{Ham}(r, q)$ is not an MDS code for any prime power q.

3. Find the minimum distances of the codes over $\mathbb{F}_5$ with the following parity-check matrices and decide whether either is an MDS code:

   (a)
$$\begin{pmatrix} 2 & 3 & 0 & 1 & 3 \\ 4 & 4 & 3 & 4 & 4 \\ 0 & 1 & 3 & 1 & 0 \end{pmatrix}$$

   The minimum distance is the smallest number d such that there is a choice of d columns which is linearly dependent. This can be no more than one plus the column rank of the matrix, which is equal to one plus the row rank, which is at most 1+3=4. We can easily see that no two columns are scalar multiples of one another, so this number d is also at least 3. So if every three columns are linearly independent the minimum distance is 4, and if not, it is 3.

   We decide whether or not every three columns are linearly independent by computing determinants, which for this particular matrix turns out to be quite a long process. (For this matrix the calculation is certainly too long for a good exam question!) There are ten ways to choose three columns from the five. We have

$$\det \begin{pmatrix} 2 & 3 & 0 \\ 4 & 4 & 3 \\ 0 & 1 & 3 \end{pmatrix} = -18 = 2 \mod 5,$$

$$\det \begin{pmatrix} 2 & 3 & 1 \\ 4 & 4 & 4 \\ 0 & 1 & 1 \end{pmatrix} = -8 = 2 \mod 5,$$

$$\det \begin{pmatrix} 2 & 3 & 3 \\ 4 & 4 & 4 \\ 0 & 1 & 0 \end{pmatrix} = 4 = 4 \mod 5,$$

$$\det \begin{pmatrix} 2 & 0 & 1 \\ 4 & 3 & 4 \\ 0 & 3 & 1 \end{pmatrix} = -6 = 4 \mod 5,$$

$$\det\begin{pmatrix}2 & 0 & 3\\ 4 & 3 & 4\\ 0 & 3 & 0\end{pmatrix} = 12 = 2 \mod 5,$$

$$\det\begin{pmatrix}2 & 1 & 3\\ 4 & 4 & 4\\ 0 & 1 & 0\end{pmatrix} = 4 \mod 5,$$

$$\det\begin{pmatrix}3 & 0 & 1\\ 4 & 3 & 4\\ 1 & 3 & 1\end{pmatrix} = -18 = 2 \mod 5,$$

$$\det\begin{pmatrix}3 & 0 & 3\\ 4 & 3 & 4\\ 1 & 3 & 0\end{pmatrix} = -9 = 1 \mod 5,$$

$$\det\begin{pmatrix}3 & 1 & 3\\ 4 & 4 & 4\\ 1 & 1 & 0\end{pmatrix} = -8 = 2 \mod 5,$$

but finally

$$\det\begin{pmatrix}0 & 1 & 3\\ 3 & 4 & 4\\ 3 & 1 & 0\end{pmatrix} = -15 = 0 \mod 5$$

so the last three columns are linearly independent. (In fact two times the fourth column, plus the third and fifth columns, is the zero vector.) Therefore the minimum distance is not 4, but must be 3. This code is not an MDS code since its redundancy is 3 and its minimum distance is also 3: for an MDS code the minimum distance must be 1 plus the redundancy.

(b)

$$\begin{pmatrix}4 & 1 & 0 & 0 & 2\\ 1 & 3 & 2 & 2 & 4\\ 0 & 1 & 0 & 3 & 4\end{pmatrix}$$

For this code exactly the same principles apply, but the linearly dependent columns are easier to find:

$$\det\begin{pmatrix}4 & 1 & 0\\ 1 & 3 & 2\\ 0 & 1 & 3\end{pmatrix} = 25 = 0 \mod 5$$

so the first, second and fourth columns form a linearly dependent set. Again the minimum distance is 3 and the code is not MDS.

4. The following 9×10 matrix is *not* the parity-check matrix of an MDS code over $\mathbb{F}_2$. What are *two* reasons why not?

$$H_{\smiley} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$

A parity-check matrix must have all rows linearly independent, but some rows of this matrix are identical. Therefore it is not a parity-check matrix at all! Furthermore, in order to be a parity-check matrix of an MDS code, a $9 \times n$ matrix needs to have the property that every choice of 9 columns is linearly independent. For this matrix there are pairs of columns which are exactly the same, so not even every choice of 2 columns is linearly independent.