Coding Theory

Sheet 8 Solutions

Spring 2014

1. Let $\mathcal{A}_i$ be the set of words of weight i. Then the map from $\mathcal{A}_i$ to $\mathcal{A}_{n-i}$ given by
$$v \mapsto v + u,$$
where $u = (1, 1, \ldots, 1)$, is a bijection, since it is both surjective and injective; it is surjective since $w + y \mapsto w$ and injective since $v_1 + y = v_2 + y$ implies that $v_1 = v_2$. Hence $A_i = A_{n-i}$.

2. If $v \in C$ has weight i, then $\lambda v \in C$ for $\lambda \in \mathbf{F}_q$ also has weight i. So the words of weight $i \neq 0$ come in sets of size $q - 1$. Hence, $q - 1$ divides A_i for $i = 1, 2, \ldots, n$.

3. For $2 \leq r \leq q$, let $\mathbf{F}_q = \{0, t_1, \ldots, t_{q-1}\}$ and let
$$M = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ t_1 & t_2 & \ldots & t_{q-1} \\ & \vdots & \ldots & \vdots \\ t_1^{r-1} & t_2^{r-1} & \ldots & t_{q-1}^{r-1} \end{bmatrix}.$$
Let $M_{i_1 i_2 \ldots i_r}$ be the $r \times r$ matrix formed from columns $i_1, i_2, \ldots, i_r$. Then
$$M_{12\ldots r} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ t_1 & t_2 & \ldots & t_r \\ & \vdots & \ldots & \vdots \\ t_1^{r-1} & t_2^{r-1} & \ldots & t_r^{r-1} \end{bmatrix};$$
so
$$\det M_{12\ldots r} = \prod_{\substack{i > j \\ i,j = 1, \ldots, r}} (t_i - t_j) \neq 0.$$
Similarly, $\det M_{i_1 i_2 \ldots i_r} \neq 0$ for any choice of $i_1, i_2, \ldots, i_r$. So $\mathcal{N}_{q-1}(r, q)$ is MDS.

The codes $\mathcal{N}_q(r, q)$ and $\mathcal{N}_{q+1}(r, q)$ are checked similarly. First,
$$[M \ e_1^T] = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 \\ t_1 & t_2 & \ldots & t_{q-1} & 0 \\ & \vdots & \ldots & & \vdots \\ t_1^{r-1} & t_2^{r-1} & \ldots & t_{q-1}^{r-1} & 0 \end{bmatrix}.$$

Then

$$M' = [M_{12\ldots r-1}\; e_1^T] = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 \\ t_1 & t_2 & \ldots & t_{r-1} & 0 \\ & \vdots & \ldots & & \vdots \\ t_1^{r-1} & t_2^{r-1} & \ldots & t_{r-1}^{r-1} & 0 \end{bmatrix},$$

and

$$\det M' = \pm \det \begin{bmatrix} t_1 & t_2 & \ldots & t_{r-1} \\ & \vdots & \ldots & \vdots \\ t_1^{r-1} & t_2^{r-1} & \ldots & t_{r-1}^{r-1} \end{bmatrix} = \pm t_1 t_2 \ldots t_{r-1} \prod_{\substack{i>j \\ i,j=1,\ldots,r-1}} (t_i - t_j) \neq 0.$$

This shows that every r columns in $[M\; e_1^T]$ are linearly independent; so $\mathcal{N}_q(r,q)$ is MDS. To check that $\mathcal{N}_{q+1}(r,q)$ is MDS, it is now only necessary to consider r columns of the generator matrix $[M\; e_1^T\; e_r^T]$, where either e_r^T is one of them or both e_1^T, e_r^T are included. So. let

$$M'' = [M_{12\ldots r-1}\; e_r^T] = \begin{bmatrix} 1 & 1 & \ldots & 1 & 0 \\ t_1 & t_2 & \ldots & t_{r-1} & 0 \\ & \vdots & \ldots & \vdots & \vdots \\ & & \ldots & & 0 \\ t_1^{r-1} & t_2^{r-1} & \ldots & t_{r-1}^{r-1} & 1 \end{bmatrix};$$

then

$$\det M'' = \pm \prod_{\substack{i>j \\ i,j=1,\ldots,r-1}} (t_i - t_j) \neq 0.$$

Similarly, let

$$M''' = [M_{12\ldots r-2}\; e_1^T\; e_r^T] = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 \\ t_1 & t_2 & \ldots & t_{r-2} & 0 & 0 \\ & \vdots & \ldots & \vdots & \vdots & \vdots \\ & & \ldots & & 0 & 0 \\ t_1^{r-1} & t_2^{r-1} & \ldots & t_{r-2}^{r-1} & 0 & 1 \end{bmatrix};$$

then

$$\det M''' = \pm t_1 t_2 \ldots t_{r-2} \prod_{\substack{i>j \\ i,j=1,\ldots,r-2}} (t_i - t_j) \neq 0.$$

Hence $\mathcal{N}_{q+1}(r,q)$ is MDS as well.

4. The parity-check matrix of $\mathcal{N}_{q+2}(3,q)$ is

$$H = \begin{array}{c} \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 0 & 0 \\ t_1 & t_2 & \ldots & t_{q-1} & 0 & 0 & 1 \\ t_1^2 & t_2^2 & \ldots & t_{q-1}^2 & 0 & 1 & 0 \end{bmatrix} \\ \begin{array}{ccccccc} & & & \phantom{t_{q-1}^2} & c_0 & c_1 & c_2 \end{array} \end{array}.$$

It is necessary to check the determinant D of any three columns of H. If the columns are i_1, i_2, i_3 among the first $q-1$, then $D = (t_{i_3} - t_{i_2})(t_{i_3} - t_{i_1})(t_{i_2} - t_{i_1}) \neq 0$. Taking the first two and c_0 gives $D = t_1 t_2 (t_2 - t_1) \neq 0$. Taking the first two and c_1 gives $D = t_2 - t_1 \neq 0$. Taking the first two and c_2 gives $D = t_2^2 - t_1^2$; so, if q is even, $D \neq 0$. However, if q is odd, then $D = 0$ when $t_2 = -t_1$. So $\mathcal{N}_{q+2}(3, q)$ is not MDS for q odd.

To complete the result for q even, taking either the last three columns or any two of the last three and the first, $D = 1, t_1, t_1^2 \neq 0$. Hence $\mathcal{N}_{q+2}(3, q)$ is MDS for q even.

5. By definition, $\mathcal{N}_5(3,5)^\perp$ is a $[5,3,3]_5$ code and $\mathcal{N}_5(3,5)$ is a $[5,2,4]_5$ code. Then a generator matrix H for $\mathcal{N}_5(3,5)^\perp$ is

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & -2 & -1 & 0 \\ 1 & -1 & -1 & 1 & 0 \end{bmatrix} \rightarrow \begin{bmatrix} 1 & -2 & 1 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 \\ -2 & 1 & 0 & 0 & 1 \end{bmatrix},$$

by row operations. So, a generator matrix G for $\mathcal{N}_5(3,5)$ is

$$G = \begin{bmatrix} 1 & 0 & -1 & -2 & 2 \\ 0 & 1 & 2 & -2 & -1 \end{bmatrix}.$$

For H, the three 2×2 determinants are

$$\begin{vmatrix} 1 & -2 \\ 2 & 2 \end{vmatrix} = 1, \quad \begin{vmatrix} 1 & -2 \\ -2 & 1 \end{vmatrix} = 2, \quad \begin{vmatrix} 2 & 2 \\ -2 & 1 \end{vmatrix} = 1.$$

For G, they have the same values.

6. Let G be a generator matrix for the $[n,k]_q$ MDS code C. Since the first k columns are linearly independent, row operations give the matrix G' in standard form

$$G' = [I_k \; A],$$

which is another generator matrix for C with $a_{i,j} \neq 0$ for all i, j. Hence the number of words of C with 0 in the first $k-1$ positions, and so weight $n - (k-1)$, is $q-1$; these words are just multiples of the last row of G'. However, there is nothing special about these positions. Hence the number of words of weight $n - (k-1)$ is

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

7. Over $\mathbf{F}_2$,

$$\begin{aligned} X^3 + 1 &= (X+1)(X^2+X+1); \\ X^4 + 1 &= (X+1)^4; \\ X^5 + 1 &= (X+1)(X^4+X^3+X^2+X+1); \\ X^6 + 1 &= (X+1)^2(X^2+X+1)^2; \\ X^7 + 1 &= (X+1)(X^3+X+1)(X^3+X^2+1); \\ X^8 + 1 &= (X+1)^8; \\ X^9 + 1 &= (X+1)(X^2+X+1)(X^6+X^3+1). \end{aligned}$$

Note that $X^6 + X^3 + 1$ is irreducible, since if it had a quadratic factor, this would be $X^2 + X + 1$, but

$$X^6 + X^3 + 1 = (X^2 + X + 1)(X^4 + X^3) + 1;$$

if it had a cubic factor, $X^6 + X^3 + 1$ would be the square of $X^3 + X + 1$ or $X^3 + X^2 + 1$ or it would be $(X^3 + X + 1)(X^3 + X^2 + 1)$, none of which hold.

8. In $R_7 = \mathbf{F}_2[X]/(X^7 + 1)$,

$$\begin{aligned} &(1 + X^3 + X^6)(1 + X) \\ &= 1 + X^3 + X^6 + X + X^4 + X^7 \\ &= 1 + X^3 + X^6 + X + X^4 + 1 \\ &= X + X^3 + X^4 + X^6; \end{aligned}$$

$$\begin{aligned} &(1 + X^4 + X^5)(1 + X^3 + X^4) \\ &= 1 + X^4 + X^5 + X^3 + X^7 + X^8 + X^4 + X^8 + X^9 \\ &= 1 + X^4 + X^5 + X^3 + 1 + X + X^4 + X + X^2 \\ &= X^2 + X^3 + X^5. \end{aligned}$$

9. (a) $X^3 + 1 = (X + 1)(X^2 + X + 1)$. So generator polynomials, generator matrices and parameters are as follows:

$$\begin{array}{ccc} 1 & I_3 & k = 3,\ d = 1 \\[1em] 1 + X & \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} & k = 2,\ d = 2 \\[0.5em] 1 + X + X^2 & \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} & k = 1,\ d = 3 \\[1em] 1 + X^3 & \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} & k = 0,\ d = 0 \end{array}$$

(b) $X^4 + 1 = (X + 1)^4$. So generator polynomials, generator matrices and parameters are as follows:

$$\begin{array}{ccc} 1 & I_4 & k = 4,\ d = 1 \\[1em] 1 + X & \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} & k = 3,\ d = 2 \\[0.5em] 1 + X^2 & \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} & k = 2,\ d = 2 \\[0.5em] 1 + X + X^2 + X^3 & \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} & k = 1,\ d = 4 \\[1em] 1 + X^4 & \begin{bmatrix} 0 & 0 & 0 & 0 \end{bmatrix} & k = 0,\ d = 0 \end{array}$$

(c) $X^5+1=(X+1)(X^4+X^3+X^2+X+1)$. So generator polynomials, generator matrices and parameters are as follows:

$$\begin{array}{ccc}
1 & I_5 & k=5,\ d=1 \\[2ex]
1+X & \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} & k=4,\ d=2 \\
1+X+X^2+X^3+X^4 & \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix} & k=1,\ d=5 \\[2ex]
1+X^5 & \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \end{bmatrix} & k=0,\ d=0
\end{array}$$

10. Over $\mathbf{F}_3$,

$$X^5-1=(X-1)(X^4+X^3+X^2+X+1).$$

So generator polynomials, generator matrices and parameters are as follows:

$$\begin{array}{ccc}
1 & I_5 & k=5,\ d=1 \\[2ex]
-1+X & \begin{bmatrix} -1 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & -1 & 1 \end{bmatrix} & k=4,\ d=2 \\
1+X+X^2+X^3+X^4 & \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \end{bmatrix} & k=1,\ d=5 \\[2ex]
-1+X^5 & \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \end{bmatrix} & k=0,\ d=0
\end{array}$$