Homework 7 Solutions

#1: $Q(t) = 2t^3 + 6t + 8$, $R(t) = 4t + 10$, where all coefficients are $\pmod{11}$.

#8: (a) One correct answer is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

You could also rearrange the rows in the last three columns in any other order.

(b) Each row of $\mathbf{C}$ obviously has weight at least 3. The sum of any two rows has two 1's in the first m columns and at least one more 1 in the last k columns, because no two rows of $\mathbf{B}$ are equal. Therefore every sum of two rows has weight at least 3. Finally, the sum of any three or more rows has at least three 1's in the first m columns, so these also have weight at least 3.

#9: The number of code vectors is 2^m. There are n vectors at distance 1 from each code vector, hence $n + 1$ vectors at distance ≤ 1 from each code vector. These sets of $n + 1$ vectors do not overlap for different code vectors, since the code can correct one error. Therefore there are a total of $2^m(n+1)$ vectors at distance ≤ 1 from some code vector. Now $2^m(n + 1) = 2^{(2^k - k - 1)} 2^k = 2^{(2^k - 1)} = 2^n$, which is the total number of vectors of length n. Therefore every vector has distance ≤ 1 from a code vector.

#10: With one message symbol x, the message polynomial $P(t)$ is just the constant $xt^0 = x$, so the corresponding code vector $\begin{bmatrix} P(0) & P(1) & \dots & P(n) \end{bmatrix}$ is $\begin{bmatrix} x & x & \dots & x \end{bmatrix}$.

#11: (a)

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 2 & 2 & 4 & 1 \end{bmatrix}$$

(b)

$$\begin{bmatrix} 2 & 3 & 4 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 4 & 2 & 2 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 3 & 5 & 1 & 5 & 3 \end{bmatrix}$$

#12: The code vector $\mathbf{y} = \mathbf{xC}$ corresponding to a message vector $\mathbf{x}$ has the form $\mathbf{y} = \begin{bmatrix} \mathbf{x} \mid \mathbf{p} \end{bmatrix}$, with $\mathbf{p} = \mathbf{xP}$. Since $\mathbf{x}$ is arbitrary, the code vectors are exactly all vectors of the form $\begin{bmatrix} \mathbf{x} \mid \mathbf{xP} \end{bmatrix}$.

Given a received vector $\mathbf{r}$, let $\mathbf{x}$ be its first m entries and let $\mathbf{q}$ be the rest, so $\mathbf{r} = \begin{bmatrix} \mathbf{x} \mid \mathbf{q} \end{bmatrix}$. From the form of $\mathbf{S}$, we see that the equation $\mathbf{rS} = \mathbf{0}$ is equivalent to $-\mathbf{x} + \mathbf{qP} = \mathbf{0}$, or $\mathbf{q} = \mathbf{xP}$. As we have seen above, this is true precisely when $\mathbf{r}$ is a code vector.