S-72.341 CODING METHODS

Tutorial 4, Solutions

1. This is a straightforward basic problem about linear block codes. Note that the code in this problem is the dual code (with shuffled parity part) of the code in problem 3 of Tutorial 3.

   a) The nonsystematic generator matrix is

$$\mathbf{G}_{\text{nonsyst}} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

   The generator matrix can be put into the systematic form by exchanging the first and the third row:

$$\mathbf{G}_{\text{syst}} = \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{array}\right] = \left[\mathbf{I}_{3\times 3} \mid \mathbf{P}_{3\times 4}\right].$$

   b) Parity-check matrix is

$$\mathbf{H}^T = \left[\frac{\mathbf{P}_{3\times 4}}{\mathbf{I}_{4\times 4}}\right] = \left[\begin{array}{cccc} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right].$$

   Check: now

$$\mathbf{G}_{\text{syst}}\mathbf{H}^T = \left[\mathbf{I}_{3\times 3} \mid \mathbf{P}_{3\times 4}\right]\left[\frac{\mathbf{P}_{3\times 4}}{\mathbf{I}_{4\times 4}}\right] = \mathbf{I}_{3\times 3}\mathbf{P}_{3\times 4} + \mathbf{P}_{3\times 4}\mathbf{I}_{4\times 4} = \mathbf{0}$$

like it should be.

c) This is a $(7,3)$ code so there are eight code words and 16 syndromes. All single-error code words are detected and also some double-error code words. Selection is not unique with double-error error words. Syndromes can be calculated using formula $\mathbf{s} = \mathbf{eH}$, where $\mathbf{e}$ is the error pattern.

Error pattern $\mathbf{e}$	Syndrome $\mathbf{s}$
$\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 0 & 0 & 0\end{bmatrix}$
$\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 0 & 1\end{bmatrix}$	$\begin{bmatrix}0 & 0 & 0 & 1\end{bmatrix}$
$\begin{bmatrix}0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 0 & 1 & 0\end{bmatrix}$
$\begin{bmatrix}0 & 0 & 0 & 0 & 1 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix}$
$\begin{bmatrix}0 & 0 & 0 & 1 & 0 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}$
$\begin{bmatrix}0 & 0 & 1 & 0 & 0 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 1 & 0 & 1\end{bmatrix}$
$\begin{bmatrix}0 & 1 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 1 & 1 & 1\end{bmatrix}$
$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 1 & 1 & 0\end{bmatrix}$
$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}$
$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}$
$\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix}$
$\begin{bmatrix}1 & 0 & 0 & 1 & 0 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}$
$\begin{bmatrix}1 & 0 & 1 & 0 & 0 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}$
$\begin{bmatrix}1 & 1 & 0 & 0 & 0 & 0 & 0\end{bmatrix}$	$\begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}$
$\begin{bmatrix}0 & 1 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$	$\begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}$
$\begin{bmatrix}0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix}$	$\begin{bmatrix}1 & 0 & 1 & 1\end{bmatrix}$

d) By investigating the generator matrix or the weights of the eight code words in the table above we can deduce that the minimum Hamming distance of the code is $d_{\min} = 4$.

e) The code word corresponding to the message is

$$\begin{aligned}\mathbf{c} = \mathbf{mG} &= \begin{bmatrix}1 & 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 1 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 1 & 1 & 1\\ 0 & 0 & 1 & 1 & 1 & 0 & 1\end{bmatrix}\\ &= \begin{bmatrix}1 & 0 & 0 & 1 & 1 & 1 & 0\end{bmatrix} + \begin{bmatrix}0 & 0 & 1 & 1 & 1 & 0 & 1\end{bmatrix}\\ &= \begin{bmatrix}1 & 0 & 1 & 0 & 0 & 1 & 1\end{bmatrix}\end{aligned}$$

Now,

$$\begin{aligned}\mathbf{cH}^T &= \begin{bmatrix}1 & 0 & 1 & 0 & 0 & 1 & 1\end{bmatrix}\left[\begin{array}{cccc}1 & 1 & 1 & 0\\ 0 & 1 & 1 & 1\\ 1 & 1 & 0 & 1\\ \hline 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{array}\right]\\ &= \begin{bmatrix}1 & 1 & 1 & 0\end{bmatrix} + \begin{bmatrix}1 & 1 & 0 & 1\end{bmatrix} + \begin{bmatrix}0 & 0 & 1 & 0\end{bmatrix} + \begin{bmatrix}0 & 0 & 0 & 1\end{bmatrix}\\ &= \begin{bmatrix}0 & 0 & 0 & 0\end{bmatrix},\end{aligned}$$

which confirms that the code word is orthogonal to the parity-check matrix.

2. By Definition 4-9 of the book the code is linear if the sum of any two code words is also a code word. Thus, for even n, we pick two palindromes $\mathbf{x} = \begin{bmatrix}x_1 & x_2 & \dots & x_{\frac{n}{2}} & x_{\frac{n}{2}} & \dots & x_2 & x_1\end{bmatrix}$ and $\mathbf{y} = \begin{bmatrix}y_1 & y_2 & \dots & y_{\frac{n}{2}} & y_{\frac{n}{2}} & \dots & y_2 & y_1\end{bmatrix}$. Since the sum $\mathbf{x} + \mathbf{y}$ is also a palindrome we conclude that the code is linear. For odd n, the result follows by deleting the $\lceil \frac{n}{2} \rceil$th coordinate from $\mathbf{x}$ and $\mathbf{y}$.

For instance, $n = 4$ yields the following linear code.

$$\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{array}$$

The code for $n = 3$ is

$$\begin{array}{cc|c} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{array}$$

The generator matrix of the palindrome code, for even n, is $\mathbf{G} = \left[\mathbf{I}_{\frac{n}{2}} \quad \mathbf{I}^p_{\frac{n}{2}}\right]$, where $\mathbf{I}_{\frac{n}{2}}$ is an $\frac{n}{2} \times \frac{n}{2}$ identity matrix, and

$$\mathbf{I}^p_{\frac{n}{2}} \triangleq \begin{bmatrix} 0 & 0 & \cdots & 1 \\ 0 & 0 & \iddots & 0 \\ \vdots & & & \vdots \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

is the $\frac{n}{2} \times \frac{n}{2}$ permuted "identity" matrix. The parity-check matrix can be obtained in the usual manner from $\mathbf{G}\mathbf{H}^T = \mathbf{0}$ [note that $\left(\mathbf{I}^p_{\frac{n}{2}}\right)^T = \mathbf{I}^p_{\frac{n}{2}}$]:

$$\mathbf{H} = \left[\mathbf{I}^p_{\frac{n}{2}} \quad \mathbf{I}_{\frac{n}{2}}\right].$$

For odd n, the right-hand side of the generator matrix is formed by removing the left-most column of $\mathbf{I}^p_{\frac{n}{2}}$. We denote this $\lceil \frac{n}{2} \rceil \times \lfloor \frac{n}{2} \rfloor$ matrix by $\tilde{\mathbf{I}}^p_{\lceil \frac{n}{2} \rceil \times \lfloor \frac{n}{2} \rfloor}$. The generator matrix for odd n is

$$\mathbf{G} = \left[\mathbf{I}_{\lceil \frac{n}{2} \rceil} \quad \tilde{\mathbf{I}}^p_{\lceil \frac{n}{2} \rceil \times \lfloor \frac{n}{2} \rfloor}\right],$$

and the corresponding parity-check matrix is ($(\cdot)^T$ denotes transpose)

$$\mathbf{H} = \left[\left(\tilde{\mathbf{I}}^p_{\lceil \frac{n}{2} \rceil \times \lfloor \frac{n}{2} \rfloor}\right)^T \quad \mathbf{I}_{\lfloor \frac{n}{2} \rfloor}\right].$$

A code word $\mathbf{x}$ of length n is formed by multiplying the generator matrix from the left by a message word $\mathbf{m}$, a binary row vector of length $\lceil \frac{n}{2} \rceil$: $\mathbf{x} = \mathbf{m}\mathbf{G}$.

The minimum distance of a palindrome code is two for any n, since we can always find two identical columns in a parity-check matrix. Thus, any palindrome code can detect one error in a word.

3. The weight enumerating function for a binary Hamming code of length n is given in equation 4-12 of the book:

$$A(x) = \frac{1}{n+1}\left\{(1+x)^n + n(1-x)\left(1-x^2\right)^{(n-1)/2}\right\}.$$

For the $(7,4)$ Hamming code the weight enumerating function takes form

$$\begin{aligned} A(x) &= \frac{1}{8}\left\{(1+x)^7 + 7(1-x)\left(1-x^2\right)^3\right\} \\ &= 1 + 7x^3 + 7x^4 + x^7. \end{aligned}$$

4. The parity-check matrix of a binary $\left(2^m - 1, 2^m - m - 1\right)$ Hamming code is a matrix whose columns consist of all nonzero binary m-tuples. The parity-check matrix of a nonbinary Hamming code is constructed using the same approach, see page 93 of the book. In our case $\mathbf{H}$ has $\left(3^3 - 1\right)/(3-1) = 13$ columns. We select as columns of $\mathbf{H}$ all distinct 3-ary 3-tuples for which the uppermost element is 1. The parity-check matrix $\mathbf{H}$ is:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 0 & 1 & 1 & 2 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{bmatrix}.$$

5. A basic problem about cyclic codes…

   a) For a cyclic code the parity-check polynomial should satisfy

$$h(x)g(x) = x^n - 1,$$

   where $g(x)$ is a generator polynomial. We get

$$h(x) = \frac{x^{15}+1}{x^5 + x^4 + x^2 + 1} = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1.$$

   b) Since $k = n - r = 15 - 5 = 10$, we have $2^{10} = 1024$ different code words.

c) The code word is message polynomial multiplied with the generator polynomial. The polynomial multiplication can be expressed using matrix multiplication:

$$\begin{aligned} c(x) &= m(x)g(x) \\ &= \left(m_0 + m_1 x + \ldots + m_{n-r-1}x^{n-r-1}\right)g(x) \\ &= m_0 g(x) + m_1 x g(x) + \ldots + m_{n-r-1}x^{n-r-1}g(x) \end{aligned}$$

$$= \begin{bmatrix} m_0 & m_1 & \ldots & m_{n-r-1} \end{bmatrix} \begin{bmatrix} 1 \\ x \\ \vdots \\ x^{n-r-1} \end{bmatrix} g(x).$$

Multiplication with x^i is equal to a i-step shift to the right. This allows us to describe the rows of the generator matrix as shifted versions of the coefficients of the generator polynomial.

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & & & & & & \\ & 1 & 0 & 1 & 0 & 1 & 1 & & & & & \\ & & & & & & & \ddots & & & & \\ & & & & & & & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Similarly the rows of the parity check matrix for a linear cyclic code are shifted versions of the parity check polynomial $h(x)$.

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & & & & & & & & \\ & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & & & & & & & \\ & & & & & & & & & & & & \ddots & & & & & & & & & \\ & & & & & & & & & & & & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

d) The code word is calculated by multiplying the message polynomial with the generator polynomial:

i) $x^2 g(x) = x^2 + x^4 + x^6 + x^7$,

ii) $\left(x^9 + x^4 + x^2 + 1\right)g(x) = 1 + x^4 + x^5 + x^7 + x^8 + x^{11} + x^{13} + x^{14}$.

e) The systematic code polynomial can be calculated using the procedure described on page 107 of the book, repeated below for your convenience.

Step 1: Multiply the message polynomial $m(x)$ by x^{n-k}.

Step 2: Divide the result of Step 1 by the generator polynomial $g(x)$. Let $d(x)$ be the remainder.

Step 3: Set $c(x) = x^{n-k}m(x) - d(x)$

For the given message polynomials we get

i) $c(x) = x^7 + x^3 + x + 1$,

ii) $c(x) = x^{14} + x^9 + x^7 + x^5 + x^4 + x^3 + x^2 + 1$.

6. Syndromes can be computed as $s(x) = r(x)h(x) \bmod \left(x^{15} + 1\right)$, $h(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1$.

   a) Notice that $x^{n+k} \bmod (x^n + 1) = x^k$. Using this we see that

$$\begin{aligned} s(x) &= x^{10}\left(x^{10} + x^9 + x^8 + x^6 + x^5 + x^2 + 1\right) \bmod \left(x^{15} + 1\right) \\ &= x^{12} + x^{10} + x^5 + x^4 + x^3 + x + 1. \end{aligned}$$

   b) $s(x) = x^{13} + x^{10} + x^9 + x^7 + x^5 + x^4 + x^3 + x^2$.

   c) $s(x) = 0$.

   d) $s(x) = x^{13} + x^{12} + x^{10} + x^8 + x^7 + x^6 + x^5 + x$.