

1. (a) We know  $r = \deg g(x) = 5$ , so  $k = n - r = 15 - 5 = 10$ . Hence, there are  $2^{10} = 1024$  code words in  $\mathcal{C}$ .
- (b) For the systematic generator matrix, we fill the  $i$ -th row of  $\mathbf{G}$ , ( $i = 1, 2, \dots, 10$ ), with the coefficients of the polynomial  $c_i(x) = x^{r+i-1} + \text{Rem}\{x^{r+i-1}/g(x)\}$ . Thus, we have

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

For the systematic parity check matrix, we apply the usual conversion trick to  $\mathbf{G}$ , producing

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

- (c) Systematic encoding produces

$$\begin{aligned} c(x) &= x^5(x^9 + x^4 + x^2 + 1) + \text{Rem}\left\{\frac{x^5(x^9 + x^4 + x^2 + 1)}{g(x)}\right\} \\ &= x^{14} + x^9 + x^7 + x^5 + x^4 + x^3 + x^2 + 1. \end{aligned}$$

Hence,  $\bar{c} = (101111010100001)$ .

- (e) Corresponding to the systematic parity check matrix, the syndrome is computed as

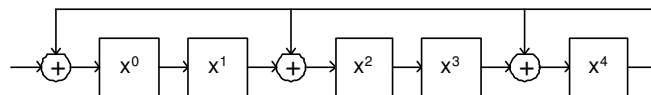
$$s(x) = \text{Rem}\left\{\frac{x^8 + x^7 + x^6 + x^5 + x^3}{x^5 + x^4 + x^2 + 1}\right\}.$$

Since  $x^8 + x^7 + x^6 + x^5 + x^3 = (x^3 + x + 1)g(x) + (x^4 + x^3 + x^2 + x + 1)$ , we have  $s(x) = 1 + x + x^2 + x^3 + x^4$ . From the vector space representation  $\bar{s} = \mathbf{H}\bar{x}^T$ , we see that

$$\bar{s} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix},$$

which agrees with the polynomial computation.

2. (a) The divide-by- $g(x)$  shift register is shown below:



- (b) We input the polynomial  $x^{15} + 1$  into the divide-by- $g(x)$  shift register, beginning with the coefficient of the highest power of  $x$ . The shift register computations are shown in the table below. The entries changed by the feedback are denoted by underlines.

Step	Input	Shift Register Content	
		$x^0x^1x^2x^3x^4$	Feedback
0	1	00000	0
1	0	10000	0
2	0	01000	0
3	0	00100	0
4	0	00010	0
5	0	00001	0
6	0	<u>10101</u>	1
7	0	<u>11111</u>	1
8	0	<u>11010</u>	1
9	0	01101	0
10	0	<u>10011</u>	1
11	0	<u>11100</u>	1
12	0	01110	0
13	0	00111	0
14	0	<u>10110</u>	1
15	1	01011	0
16	-	<u>00000</u>	1

Since the register becomes all-zero once the polynomial  $x^{15} + 1$  has been clocked in, we conclude that  $g(x)$  divides  $x^{15} + 1$  with zero remainder.

- (c) The syndromes for the 1-bit error patterns are easily determined from the shift register computation in part (b). In particular, the contents of the shift register at step  $i + 1$  represents the polynomial

$$s_i(x) = \text{Rem} \left\{ \frac{x^i}{g(x)} \right\},$$

the syndrome for the 1-bit error pattern in which the bit error occurs at position  $x^i$ . Hence, the table computed above *is* in fact the syndrome table we want!

3. Let  $g_{\text{EW}}(x) = (x + 1) \cdot g(x)$ , and let  $\mathcal{C}_{\text{EW}}$  denote the cyclic code it generates. Note that  $g(x)$  and  $x + 1$  are factors of  $x^n + 1$  that have no non-constant factor in common. So their product  $g_{\text{EW}}(x)$  is also a factor of  $x^n + 1$  and hence  $\mathcal{C}_{\text{EW}}$  is cyclic code.

There are two parts to show:

- ( $\Rightarrow$ ) To show: *Every code word in  $\mathcal{C}_{\text{EW}}$  is a code word of  $\mathcal{C}$  of even weight.*

Every code word in  $\mathcal{C}_{\text{EW}}$  is a code word in  $\mathcal{C}$ , since every multiple of  $g_{\text{EW}}(x)$  is also a multiple of  $g(x)$ . Consider any specific code word  $c_{\text{EW}}(x) = m(x)g_{\text{EW}}(x)$ . Using the hint, we find  $\text{wt}(c_{\text{EW}}(x)) = m(1)g_{\text{EW}}(1) = (1 + 1)m(1)g(1) \equiv 0 \pmod{2}$ .

- ( $\Leftarrow$ ) To show: *Every code word in  $\mathcal{C}$  of even weight is a code word of  $\mathcal{C}_{\text{EW}}$ .*

We first claim that every even weight polynomial is a multiple of  $x + 1$ . Suppose  $p(x)$  is of even weight. Dividing  $p(x)$  by  $x + 1$ , we find quotient  $q(x)$  and remainder  $r$  satisfying

$$p(x) = (x + 1)q(x) + r,$$

where  $\deg\{r\} < \deg\{x + 1\}$ , so  $r$  is constant. Then

$$0 = [\text{wt}(p(x))]_{\pmod{2}} = p(1) = (1 + 1)q(1) + r = r.$$

Hence,  $p(x) = (x + 1)q(x)$  is a multiple of  $x + 1$  as claimed.

Now suppose that  $c(x) = m(x)g(x)$  is an even-weight code word of  $\mathcal{C}$ . Then  $c(1) = m(1)g(1) = 0$ . Since  $g(x)$  is not divisible by  $x + 1$ , we have  $g(1) = 1$ . Thus,  $m(1) = 0$ , so  $x + 1$  is a divisor of  $m(x)$ . Let  $m(x) = (x + 1)m_{\text{EW}}(x)$ . Then  $c(x) = (x + 1)m_{\text{EW}}(x)g(x) = m_{\text{EW}}(x)g_{\text{EW}}(x)$  is a code word in  $\mathcal{C}_{\text{EW}}$ .

4. From homework 1 solution (problem 2b), we found that the twenty questions version of the code  $\mathcal{H}_7$  has canonical parity check matrix

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

We have the corresponding canonical generator matrix

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

This is different from but very similar to the canonical generator matrix for the cyclic version of  $\mathcal{H}_7$  produced by the generator polynomial  $g(x) = x^3 + x + 1$ :

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

By inspection, we see that the first information bit (fourth column) of  $\mathbf{G}_{\text{non-cyclic}}$  is the third information bit (sixth column) of  $\mathbf{G}_{\text{cyclic}}$ ; the second information bits are the same; the third information bit of  $\mathbf{G}_{\text{non-cyclic}}$  is the last information bit of  $\mathbf{G}_{\text{cyclic}}$ ; and the last information bit of  $\mathbf{G}_{\text{non-cyclic}}$  is the first information bit of  $\mathbf{G}_{\text{cyclic}}$ . In other words, by interchanging these columns and then rearranging the rows to restore the canonical form, we change  $\mathbf{G}_{\text{non-cyclic}}$  into  $\mathbf{G}_{\text{cyclic}}$ .

5. (a) The reverse of  $g_2(x)$  is

$$\begin{aligned} x^{11} \cdot g_2\left(\frac{1}{x}\right) &= x^{11} \cdot \left[ \frac{1}{x^{11}} + \frac{1}{x^9} + \frac{1}{x^7} + \frac{1}{x^6} + \frac{1}{x^5} + \frac{1}{x} + 1 \right] \\ &= 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}, \end{aligned}$$

which is just  $g_1(x)$ .

- (b) The two versions are NOT the same, because the generator for a cyclic code is ALWAYS unique! But the two versions of  $\mathcal{G}_{23}$  differ only in the order of presentation of the bits—the code words in one version are just written backwards for the other version. Let  $c(x) = m(x)g_1(x)$  be a code word in the version generated by  $g_1(x)$ . Then, written backwards, it becomes

$$\begin{aligned} c_{\text{back}}(x) &= x^{n-1}c\left(\frac{1}{x}\right) \\ &= x^{n-1}m\left(\frac{1}{x}\right)g\left(\frac{1}{x}\right) \\ &= \left[ x^{k-1}m\left(\frac{1}{x}\right) \right] \left[ x^r g\left(\frac{1}{x}\right) \right] \\ &= m_{\text{back}}(x) \cdot g_2(x), \end{aligned}$$

where  $n = 23$ ,  $k = 12$ ,  $r = 11$ , and  $m_{\text{back}}(x)$  is the information polynomial written backwards. This change is a simple permutation of coordinates, so the two versions of the Golay code are equivalent. (*Caution:* Note that “written backwards” is slightly different than “reverse” since in the former case we have a fixed block size independent of the degree of the polynomial.)