

1. Let  $\mathcal{C}$  be the cyclic code of length 15 with generator polynomial  $g(x) = x^5 + x^4 + x^2 + 1$ .
  - (a) Determine the number of code words in  $\mathcal{C}$ .
  - (b) Determine systematic generator and parity check matrices for  $\mathcal{C}$ .
  - (c) Perform systematic encoding of the message polynomial  $m(x) = x^9 + x^4 + x^2 + 1$  using the polynomial representation.
  - (d) Compute the syndrome for the received message polynomial  $r(x) = x^8 + x^7 + x^6 + x^5 + x^3$  using the polynomial representation.
2. Consider again the cyclic code of length 15 with generator polynomial  $g(x) = x^5 + x^4 + x^2 + 1$ .
  - (a) Draw the divide-by- $g(x)$  linear feedback shift register.
  - (b) Use the shift register to verify that  $g(x) \mid x^{15} + 1$ .
  - (c) Use the shift register to *determine* a syndrome table decoder capable of correcting all 1-bit error patterns. (N.B. You do not have to convert the shift register into a decoder—just use it to determine the entries in the syndrome table decoder.)
3. Within a linear code, the set of code words of even Hamming weight form a smaller code that is also linear. It is called the *even weight subcode*. Let  $\mathcal{C}$  be a cyclic code of length  $n$ , dimension  $k$ , and having generator polynomial  $g(x)$ . Assume that  $x + 1$  is not a factor of  $g(x)$ . Show that the cyclic code generated by  $(x + 1)g(x)$  is the even weight subcode of  $\mathcal{C}$ . (*Hint:  $c(x)$  is of even Hamming weight if and only if  $c(1) = 0 \pmod{2}$ .*)
4. Two codes are said to be *equivalent* if one can permute the vector coordinates in such a way that the code words of one code are transformed into the code words of the other code. For example, the codes generated by matrices

$$\mathbf{G}_1 = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad \text{and} \quad \mathbf{G}_2 = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

are equivalent: the first two bits are just swapped. Performance of equivalent codes is the same on memoryless channels such as the BSC. Explain how the cyclic code generated by  $g(x) = x^3 + x + 1$  is equivalent to  $\mathcal{H}_7$  as defined in Homework #1 by demonstrating the permutation that changes one into the other.

5. There are two generator polynomials  $g_1(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$  and  $g_2(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$  that can be used to generate the perfect Golay code  $\mathcal{G}_{23}$ .
  - (a) Show that  $g_1(x)$  and  $g_2(x)$  are reverse polynomials of one another.
  - (b) How are these versions of  $\mathcal{G}_{23}$  related to one another? Are the cyclic codes generated by  $g_1(x)$  and  $g_2(x)$  the same? Are they equivalent? Why?