6.1 Consider the Galois field $GF(2^4)$ given by Table 2.8. The element $\beta = \alpha^7$ is also a primitive element. Let $\mathbf{g}_0(X)$ be the lowest-degree polynomial over $GF(2)$ that has

$$\beta, \beta^2, \beta^3, \beta^4$$

as its roots. This polynomial also generates a double-error-correcting primitive BCH code of length 15.

a. Determine $\mathbf{g}_0(X)$.

b. Find the parity-check matrix for this code.

c. Show that $\mathbf{g}_0(X)$ is the reciprocal polynomial of the polynomial $\mathbf{g}(X)$ that generates the (15, 7) double-error-correcting BCH code given in Example 6.1.

6.2 Determine the generator polynomials of all the primitive BCH codes of length 31. Use the Galois field $GF(2^5)$ generated by $\mathbf{p}(X) = 1 + X^2 + X^5$.

6.3 Suppose that the double-error-correcting BCH code of length 31 constructed in Problem 6.2 is used for error correction on a BSC. Decode the received polynomials $\mathbf{r}_1(X) = X^7 + X^{30}$ and $\mathbf{r}_2(X) = 1 + X^{17} + X^{28}$.

6.4 Consider a t-error-correcting primitive binary BCH code of length $n = 2^m - 1$. If $2t + 1$ is a factor of n, prove that the minimum distance of the code is exactly $2t + 1$. (*Hint*: Let $n = l(2t + 1)$. Show that $(X^n + 1)/(X^l + 1)$ is a code polynomial of weight $2t + 1$.)