1. Show that if $C_{RS}$ is a conventional narrow-sense (meaning $b = 1$) Reed-Solomon code of length $n > 1$ over $K$, then $C_{RS}$ always contains the all-ones word $1 = (1 \ldots 1) \in K^n$. Conclude from this that any narrow-sense BCH code (i.e., a subfield-subcode of $C_{RS}$ as above) of length $n > 1$ contains the all-ones word as a codeword.

2. Let $C$ be the $[15, 5, 7]$ triple-error-correcting (primitive, narrow-sense) binary BCH code with parity-check matrix

$$H_{RS} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{14} \\
1 & \alpha^2 & (\alpha^2)^2 & (\alpha^3)^2 & \cdots & (\alpha^{14})^2 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \alpha^6 & (\alpha^2)^6 & (\alpha^3)^6 & \cdots & (\alpha^{14})^6 \end{bmatrix},$$

where $\alpha \in F_{16}$ is a root of $f(x) = x^4 + x^3 + 1$. Suppose that a codeword from $C$ was transmitted. Use the Peterson-Gorenstein-Zierler decoding algorithm to decode the following received words, if possible:

(a) $0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1$

(b) $1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$

(c) $1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$

3. Let $C$ be the code in Problem 2. Let $s = [s_0 \ s_1 \ s_2 \ s_3 \ s_4]^T \in (F_{16})^6$ be the syndrome arising from a binary received word $y \in F_{15}^2$. In each of the following cases, analyze the operation of the extended Euclidean algorithm decoder to identify all the values of $s_4$ or $s_2$ (as the case may be) for which the decoder is able to produce a codeword from $C$ as output.

(a) $s_0 = 0$, $s_2 = 0$, $s_4 \neq 0$.

(b) $s_0 = 0$, $s_2 \neq 0$, $s_4 = 0$.

4. Consider the $[10, 6, 5]$ Reed-Solomon code over $F_{11}$ defined by the code locators and column multipliers $\alpha_j = v_j = 2^{j-1}$, $j = 1, 2, \ldots, 10$. (It is known that 2 is a primitive element of $F_{11}$.) From a received word $y$, the syndrome polynomial $S(x)$ and error-locator polynomial $\sigma(x)$ are computed to be

$$S(x) = 1 + x^2, \quad \sigma(x) = 1 - x^2.$$

Find, if possible, an error vector $e$ of weight $t \leq 2$ that gives rise to these polynomials.

5. Let $\alpha$ be a primitive element in the field $F_{2^r}$, $r \geq 3$. Set $n = 2^r - 1$, and define the matrix

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\
1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \cdots & \alpha^{-(n-1)} \end{bmatrix}.$$

Consider the binary code $C = \{c \in \{0, 1\}^n : Hc^T = 0\}$. (For $r = 4$, this is the code considered in Problem 4 of Homework Assignment #5.)
(a) Prove that $C$ is a cyclic code by showing that it has a generator polynomial.

(b) Determine the dimension of $C$.

(c) Derive a decoding algorithm for $C$ that attempts to correct binary error patterns with at most two errors. In doing so, prove that $C$ is a double-error-correcting code if and only if $r$ is odd.

[Hint: Approach this in a manner similar to our original approach to deriving a decoding algorithm for the double-error-correcting binary BCH code. In your analysis, you may need to use the fact (which you must also prove) that there exists a $\gamma \in \mathbb{F}_{2^r}$ such that $\gamma^2 + \gamma + 1 = 0$, if and only if $2 \mid r$.]

6. Let $g(x)$ be the generator polynomial of a cyclic $[n, k]$ code $C$ over $\mathbb{F}$, so that $g(x)$ divides $x^n - 1$ in $\mathbb{F}[x]$. Let $h(x) = \sum_{i=0}^{k} h_i x^i$ be such that $g(x)h(x) = x^n - 1$ in $\mathbb{F}[x]$. The polynomial $h(x)$ is called the check polynomial of $C$. Show that the following $(n-k) \times n$ matrix

$$
H = \begin{bmatrix}
    h_k & h_{k-1} & \cdots & h_0 \\
    h_k & h_{k-1} & \cdots & h_0 \\
    \vdots & \vdots & \ddots & \vdots \\
    h_k & h_{k-1} & \cdots & h_0
\end{bmatrix}
$$

is a parity-check matrix for $C$. 