PROBLEMS

7.1 Consider the triple-error-correcting RS code given in Example 7.2. Find the code polynomial for the message

$$\mathbf{a}(X) = 1 + \alpha^5 X + \alpha X^4 + \alpha^7 X^8.$$

7.2 Using the Galois field $GF(2^5)$ given in Appendix A, find the generator polynomials of the double-error-correcting and triple-error-correcting RS codes of length 31.

7.3 Using the Galois field $GF(2^6)$ given in Table 6.2, find the generator polynomials of double-error-correcting and triple-error-correcting RS codes of length 63.

7.4 Consider the triple-error-correcting RS code of length 15 given in Example 7.2. Decode the received polynomial

$$\mathbf{r}(X) = \alpha^4 X^3 + \alpha^9 X^8 + \alpha^3 X^{13}$$

using the Berlekamp algorithm.

7.5 Continue Problem 7.4. Decode the received polynomial with the Euclidean algorithm.

7.6 Consider the triple-error-correcting RS code of length 31 constructed in Problem 7.2. Decode the received polynomial

$$\mathbf{r}(X) = \alpha^2 + \alpha^{21} X^{12} + \alpha^7 X^{20}$$

using the Euclidean algorithm.

7.7 Continue Problem 7.6. Decode the received polynomial in the frequency domain using transform decoding.

7.8 For the same RS code of Problem 7.6, decode the following received polynomial with two erasures:

$$\mathbf{r}(X) = (*)X^3 + \alpha^5 X^7 + (*)X^{18} + \alpha^3 X^{21}$$

with the Euclidean algorithm.

7.9 Prove that the dual code of a RS code is also a RS code.

7.10 Prove that the $(2^m - 1, k)$ RS code with minimum distance d contains the primitive binary BCH code of length $2^m - 1$ with designed distance d as a subcode. This subcode is called a *subfield subcode*.

7.11 Let α be a primitive element in $GF(2^m)$. Consider the $(2^m - 1, k)$ RS code of length of $2^m - 1$ and minimum distance d generated by

$$\mathbf{g}(X) = (X - \alpha)(X - \alpha^2)...(X - \alpha^{d-1}).$$

Prove that extending each codeword $v = (v_0, v_1, \cdots, v_{2^m-2})$ by adding an overall parity-check symbol

$$v_\infty = -\sum_{i=0}^{2^m-2} v_i$$

produces a $(2^m, k)$ code with a minimum distance of $d + 1$.

7.12 Consider a t-symbol error-correcting RS code over $GF(2^m)$ with the following parity-check matrix:

$$\mathbf{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & \alpha^{2t} & (\alpha^{2t})^2 & \cdots & (\alpha^{2t})^{n-1} \end{bmatrix},$$

where $n = 2^m - 1$, and α is a primitive element in $GF(2^m)$. Consider the extended Reed–Solomon code with the following parity-check matrix:

$$\mathbf{H}_1 = \begin{bmatrix} 0 & 1 & \\ 0 & 0 & \\ \vdots & \vdots & \mathbf{H} \\ 0 & 0 & \\ 1 & 0 & \end{bmatrix}$$

Prove that the extended code also has a minimum distance of $2t + 1$.

7.13 Let $\mathbf{a}(X) = a_0 + a_1X + \cdots + a_{k-1}X^{k-1}$ be a polynomial of degree $k - 1$ or less over $GF(2^m)$. There are $(2^m)^k$ such polynomials. Let α be a primitive element in $GF(2^m)$. For each polynomial $\mathbf{a}(X)$, form the following polynomial of degree $2^m - 2$ or less over $GF(2^m)$:

$$\mathbf{v}(X) = \mathbf{a}(1) + \mathbf{a}(\alpha)X + \mathbf{a}(\alpha^2)X^2 + \cdots + \mathbf{a}(\alpha^{2^m-2})X^{2^m-2}.$$

Prove that the set $\{\mathbf{v}(X)\}$ forms the $(2^m - 1, k)$ RS code over $GF(2^m)$. (*Hint:* Show that $\mathbf{v}(X)$ has $\alpha, \alpha^2, \cdots, \alpha^{2^m-k-1}$ as roots). This original definition of a RS code is given by Reed and Solomon [1].