Solutions to Homework Assignment 2

Problem 1.

$$\mathbf{V}_\mu \triangleq (V_0, V_1\alpha^\mu, \ldots, V_{n-1}\alpha^{\mu(n-1)}).$$

Therefore the jth component of its DFT is given by

$$\widehat{V}_{\mu,j} = \sum_{i=0}^{n-1} V_i \alpha^{\mu i}\alpha^{ij} = \sum_{i=0}^{n-1} V_i \alpha^{i(\mu+j)} = \widehat{V}_{(\mu+j)\bmod n}$$

since $\alpha^n = 1$. This is the required result.

Problem 2.

$$\mathbf{V} = (0, \beta^4, \beta^5, 0, \beta^7)$$

where $\beta = \alpha^3$. Therefore the DFT of $\mathbf{V}$ is given by

$$\widehat{V}_j = \sum_{i=0}^{4} V_i \beta^{ij}, \quad j = 0, \ldots, 4.$$

Substituting the values of $\mathbf{V}$ and $\beta = \alpha^3$, we compute the components of $\widehat{\mathbf{V}}$ using arithmetic in the field GF(16) to get

$$\widehat{\mathbf{V}} = (\alpha, \alpha^8, \alpha^5, \alpha^7, \alpha^9).$$

The support set I of the vector V, i.e. the set of indices for which it is nonzero, is $\{1, 2, 4\}$. Therefore the error locator polynomial $\sigma_{\mathbf{V}}(x)$ is given by

$$\sigma_{\mathbf{V}}(x) = \prod_{i\in I}(1-\beta^i x) = (1-\beta x)(1-\beta^2 x)(1-\beta^4 x) = 1 + \alpha^7 x + \alpha^4 x^2 + \alpha^6 x^3.$$

The polynomials $\sigma_{\mathbf{V}}^{(i)}(x)$ are defined as

$$\sigma_{\mathbf{V}}^{(i)}(x) = \prod_{j\in I, j\neq i} (1-\beta^j x).$$

Therefore we have

$$\sigma_{\mathbf{V}}^{(1)}(x) = (1-\beta^2 x)(1-\beta^4 x) = 1+\alpha^4 x + \alpha^3 x^2.$$

$$\sigma_{\mathbf{V}}^{(2)}(x) = (1-\beta x)(1-\beta^4 x) = 1+\alpha^{10} x + x^2.$$

$$\sigma_{\mathbf{V}}^{(3)}(x) = (1-\beta x)(1-\beta^2 x) = 1+\alpha^2 x + \alpha^9 x^2.$$

The evaluator polynomial $\omega_{\mathbf{V}}(x)$ is then defined as

$$\omega_{\mathbf{V}}(x) = \sum_{i\in I} V_i \sigma_{\mathbf{V}}^{(i)}(x) = \beta^4 \sigma_{\mathbf{V}}^{(1)}(x) + \beta^5 \sigma_{\mathbf{V}}^{(2)}(x) + \beta^7 \sigma_{\mathbf{V}}^{(3)}(x) = \alpha + x^2.$$

This completes all the necessary computations.

Problem 3.
We begin by computing a table of powers of α, the primitive root in GF(8) satisfying $\alpha^3 = \alpha + 1$. We get

$$\alpha^3 = \alpha+1,\ \alpha^4 = \alpha^2+\alpha,\ \alpha^5 = \alpha^2+\alpha+1,\ \alpha^6 = \alpha^2+1.$$

Using this table, we perform computations as in the previous problem. We are given

$$\mathbf{V} = (1, \alpha, 0, 0, 0, 0, 0).$$

The jth component of its DFT is given by

$$\widehat{V}_j = \sum_{i=0}^{6} V_i \alpha^{ij} = \alpha + \alpha^j.$$

Computing this for all values of j, we get $\widehat{\mathbf{V}} = (\alpha^3, 0, \alpha^4, 1, \alpha^2, \alpha^6, \alpha^5)$.
The support set I of V is now $\{0,1\}$. The evaluator polynomial $\sigma(x)$ is therefore given by

$$\sigma(x) = (1-x)(1-\alpha x) = 1 + \alpha^3 x + \alpha x^2.$$

Similarly $\sigma^{(0)}(x)$ and $\sigma^{(1)}(x)$ are given by

$$\sigma^{(0)}(x) = 1 + \alpha x, \text{ and } \sigma^{(1)}(x) = 1 + x.$$

The evaluator polynomial $\omega(x)$ is then given by

$$\omega(x) = \alpha(1 + \alpha x) + 1(1 + x) = \alpha^3 + \alpha^6 x.$$

Now, $\widehat{\mathbf{V}}$ is supposed to satisfy the recursion $\widehat{V}_j = \sigma_1 \widehat{V}_{j-1} + \sigma_2 \widehat{V}_{j-2}$. In this case $\sigma_1 = \alpha^3$ and $\sigma_2 = \alpha$. Therefore the RHS of the recursion simplifies to

$$\alpha^3(\alpha + \alpha^{j-1}) + \alpha(\alpha + \alpha^{j-2}) = (\alpha^4 + \alpha^2) + \alpha^{j-1}(1 + \alpha^3) = \alpha + \alpha^j = \widehat{V}_j$$

as required. Therefore the recursion is satisfied.

Problem 4.
The received vector is $\mathbf{R} = (\alpha^3, 1, \alpha, \alpha^2, \alpha^3, \alpha, 1)$. We first compute the syndrome polynomial $S(x)$ of degree $r - 1 = 3$ in which the coefficient of x^{j-1} for $j = 1, \ldots, 4$ is given by

$$S_j = \sum_{i=0}^{n-1} R_i \alpha^{ij}.$$

Carrying out these computations, we get $S(x) = \alpha^2 + \alpha^6 x + \alpha^5 x^2 + \alpha^6 x^3$. Since the syndrome is nonzero, the received vector has errors. Since $r = 4$, we have $t = 2$. We now need to run Euclid's algorithm in order to compute $\sigma(x)$ and $\omega(x)$. We implement the procedure $Euclid[x^r, S(x), t, t-1]$, and this procedure returns the output $v(x) = \alpha^5 + \alpha^3 x + \alpha^3 x^2$ and $r(x) = 1 + x$. Now, we have $\sigma(x) = v(x)/v(0)$ and $\omega(x) = r(x)/v(0)$. Thus we get $\sigma(x) = 1 + \alpha^5 x + \alpha^5 x^2$ and $\omega(x) = \alpha^2 + \alpha^2 x$.
Time domain completion:
Now we compute $\sigma(\alpha^{-i})$ for $0 \leq i \leq 6$ and find that $\sigma(\alpha^{-2}) = \sigma(\alpha^{-3}) = 0$. Thus there are errors in locations 2 and 3. To compute the values of the error vector in these locations, we first need to compute the formal derivative $\sigma'(x)$ of $\sigma(x)$. This is given by $\sigma'(x) = \alpha^5 + 2\alpha^5 x = \alpha^5$, since 2 is the same as 0 in the field we are working in. Now, in the error locations, we have $E_i = -\omega(\alpha^{-i})/\sigma'(\alpha^{-i})$. Carrying out this computation, we get $E_2 = \alpha$ and

$E_3 = \alpha^2$. Thus $\mathbf{E} = (0, 0, \alpha, \alpha^2, 0, 0, 0)$. Subtracting this error vector from the received vector, we get the decoded vector $\widehat{\mathbf{C}}$ as

$$\widehat{\mathbf{C}} = (\alpha^3, 1, 0, 0, \alpha^3, \alpha, 1).$$

Frequency domain completion:
We must now compute the coefficients S_5, S_6, and S_7 of the syndrome vector by the recursion

$$S_j = -\sigma_1 S_{j-1} - \sigma_2 S_{j-2} = \alpha^5 S_{j-1} + \alpha^5 S_{j-2}$$

and thus we get the full syndrome vector to be $\mathbf{S} = (\alpha^4, \alpha^2, \alpha^6, \alpha^5, \alpha^6, \alpha^6, 0)$. The error vector $\mathbf{E}$ is now given by the inverse DFT of $\mathbf{S}$ and works out to be $(0, 0, \alpha, \alpha^2, 0, 0, 0)$ again. Therefore we get again

$$\widehat{\mathbf{C}} = (\alpha^3, 1, 0, 0, \alpha^3, \alpha, 1).$$

Problem 5.
The received vector this time is $\mathbf{R} = (1, \alpha, \alpha^2, *, *, *, *)$ where the $*$'s denote erasures. The erasures are in positions 3,4,5 and 6, and therefore the erasure locator polynomial is given by

$$\sigma_0(x) = (1 - \alpha^3 x)(1 - \alpha^4 x)(1 - \alpha^5 x)(1 - \alpha^6 x) = 1 + \alpha^5 x + \alpha^4 x^2 + x^3 + \alpha^4 x^4.$$

We now replace the erasures by 0's and then compute the syndrome of this modified received vector. $S(x)$ works out to be $\alpha^3 + \alpha^5 x^2 + \alpha^6 x^2 + \alpha^6 x^3$. Now we compute $S_0(x) = \sigma_0(x)S(x) \bmod x^r$ which works out to be $\alpha^3 + \alpha^6 x + \alpha^5 x^2 + \alpha^2 x^3$. Now in this case, since we have 3 erasures, we know that we can correct no errors, i.e. we assume that no errors were made, therefore we get $\sigma_1(x) = 1$ and $\omega(x) = S_0(x) = \alpha^3 + \alpha^6 x + \alpha^5 x^2 + \alpha^2 x^3$. Euclid's algorithm would also return the same answer at the first step. Also we now get $\sigma(x) = \sigma_0(x)\sigma_1(x) = \sigma_0(x)$. Its formal derivative $\sigma'(x)$ is now given by $\alpha^5 + 2\alpha^4 x + 3x^2 + 4\alpha^4 x^3 = \alpha^5 + x^2$. Now we compute $\sigma(\alpha^{-i})$ for each i and as expected it is zero for $i = 3, 4, 5$ and 6. We compute $E_i = -\omega(\alpha^{-i})/\sigma'(\alpha^{-i})$ for these values of i and get the error vector $\mathbf{E}$ to be $(0, 0, 0, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$. Therefore the decoded codeword is given by

$$\widehat{\mathbf{C}} = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6).$$