EE/Ma 127b Error-Correcting Codes - Homework Assignment 2

Ling Li, ling@cs.caltech.edu

February 1, 2001

2.1 *DFT of phase-shifted vector.* Let $\mathbf{W} = \mathbf{V}_\mu = (V_0, V_1\alpha^\mu, \ldots, V_{n-1}\alpha^{\mu(n-1)})$, i.e., $W_i = V_i\alpha^{i\mu}$. From

$$\widehat{V}_j = \sum_{i=0}^{n-1} V_i\alpha^{ij},$$

and

$$\widehat{W}_j = \sum_{i=0}^{n-1} W_i\alpha^{ij} = \sum_{i=0}^{n-1} V_i\alpha^{i(\mu+j)},$$

we find that $\widehat{W}_j = \widehat{V}_{\mu+j}$, since the subscripts are taken mod n, and $\mathrm{ord}(\alpha)$ is also n. Thus

$$\widehat{\mathbf{V}}_\mu = \widehat{\mathbf{W}} = (\widehat{W}_0, \widehat{W}_1, \ldots, \widehat{W}_{n-1}) = (\widehat{V}_\mu, \widehat{V}_{\mu+1}, \ldots, \widehat{V}_{\mu+n-1}).$$

2.2 $\beta = \alpha^3$, $\mathbf{V} = (0, \beta^4, \beta^5, 0, \beta^7) = (0, \beta^4, 1, 0, \beta^2)$. The polynomial $V(x)$ is

$$V(x) = \beta^4 x + x^2 + \beta^2 x^4.$$

Using $\widehat{V}_j = V(\beta^j)$, we can calculate the DFT of $\mathbf{V}$:

$$\begin{aligned}
\widehat{V}_0 &= \beta^4 + 1 + \beta^2 = [0010] = \alpha, \\
\widehat{V}_1 &= \beta^5 + \beta^2 + \beta^6 = [0101] = \alpha^8, \\
\widehat{V}_2 &= \beta^6 + \beta^4 + \beta^{10} = [0110] = \alpha^5, \\
\widehat{V}_3 &= \beta^7 + \beta^6 + \beta^{14} = [1011] = \alpha^7, \\
\widehat{V}_4 &= \beta^8 + \beta^8 + \beta^{18} = \beta^3 = \alpha^9,
\end{aligned}$$

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

The support set of $\mathbf{V}$ is $I = \{1, 2, 4\}$, so the locator polynomial for $\mathbf{V}$ is

$$\sigma_{\mathbf{V}}(x) = (1+\beta x)(1+\beta^2 x)(1+\beta^4 x) = 1 + \alpha^7 x + \alpha^4 x^2 + \alpha^6 x^3,$$

and the polynomials $\sigma_{\mathbf{V}}^{(i)}(x)$ for $i = 1, 2, 4$ are

$$\begin{aligned}
\sigma_{\mathbf{V}}^{(1)}(x) &= (1+\beta^2 x)(1+\beta^4 x) = 1 + \alpha^4 x + \alpha^3 x^2, \\
\sigma_{\mathbf{V}}^{(2)}(x) &= (1+\beta x)(1+\beta^4 x) = 1 + \alpha^{10} x + x^2, \\
\sigma_{\mathbf{V}}^{(4)}(x) &= (1+\beta x)(1+\beta^2 x) = 1 + \alpha^2 x + \alpha^9 x^2.
\end{aligned}$$

The evaluator polynomial is

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

We can calculate

$$\sigma_{\mathbf{V}}(x)\widehat{V}(x) = \alpha + x^2 + \alpha x^5 + x^7,$$

and (here $n = \mathrm{ord}(\beta) = 5$)

$$\omega_{\mathbf{V}}(x)(1 - x^n) = \alpha + x^2 + \alpha x^5 + x^7.$$

Thus the key equation $\sigma_{\mathbf{V}}(x)\widehat{V}(x) = \omega_{\mathbf{V}}(x)(1 - x^n)$ also holds here.

2.3 Let α be a primitive root in GF(8) satisfying $\alpha^3 = \alpha + 1$, and let $\mathbf{V} = (\alpha, 1, 0, 0, 0, 0, 0)$. The support set of $\mathbf{V}$ is $I = \{0, 1\}$. Thus the locator polynomial is

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

and the evaluator polynomial is

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

The component of $\widehat{\mathbf{V}}$ is $\widehat{V}_j = \alpha + \alpha^j$, so

$$\widehat{\mathbf{V}} = (\alpha^3, 0, \alpha^4, 1, \alpha^2, \alpha^6, \alpha^5).$$

Since

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

we verified that

$$\widehat{V}_j = -\sum_{i=1}^{2} \sigma_i \widehat{V}_{j-i} = \alpha^3 \widehat{V}_{j-1} + \alpha \widehat{V}_{j-2}.$$

2.4 *R-S Decoding.* $n = 7$, $r = 4$, $\mathbf{R} = (\alpha^3, 1, \alpha, \alpha^2, \alpha^3, \alpha, 1)$. The syndrome polynomial is

$$S(x) = \alpha^2 + \alpha^6 x + \alpha^5 x^2 + \alpha^6 x^3.$$

The $\gcd(x^r, S(x))$ gives

i	u_i	v_i	r_i	q_i
-1	1	0	x^4	-
0	0	1	$\alpha^2 + \alpha^6 x + \alpha^5 x^2 + \alpha^6 x^3$	-
1	1	$1 + \alpha x$	$\alpha^2 + \alpha^4 x + \alpha^4 x^2$	$1 + \alpha x$
2	$\alpha^4 + \alpha^2 x$	$\alpha^5 + \alpha^3 x + \alpha^3 x^2$	$1 + x$	$\alpha^4 + \alpha^2 x$

By $\deg \sigma(x) \leq 2$ and $\deg \omega(x) \leq 1$, we get

$$\sigma(x) = v_2(x)/\alpha^5 = 1 + \alpha^5 x + \alpha^5 x^2, \quad \omega(x) = r_2/\alpha^5 = \alpha^2 + \alpha^2 x.$$

Then we can use either frequency domain or time domain to complete the decoding.

(a) *Frequency domain.* Using $S_i = -(\sigma_1 S_{i-1} + \sigma_2 S_{i-2}) = \alpha^5(S_{i-1} + S_{i-2})$, we have $\widehat{\mathbf{E}} = \mathbf{S} = (\alpha^4, \alpha^2, \alpha^6, \alpha^5, \alpha^6, \alpha^6, 0)$. So $\mathbf{E} = (0, 0, \alpha, \alpha^2, 0, 0, 0)$ and the codeword is

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

(b) *Time domain.* Since $\sigma(x) = 1 + \alpha^5 x + \alpha^5 x^2 = (1 + \alpha^2 x)(1 + \alpha^3 x)$, we have $\sigma(\alpha^{-2}) = \sigma(\alpha^{-3}) = 0$ and

$$E_2 = -\frac{\omega(\alpha^{-2})}{\sigma'(\alpha^{-2})} = \frac{1+\alpha^2}{\alpha^5} = \alpha, \quad E_3 = -\frac{\omega(\alpha^{-3})}{\sigma'(\alpha^{-3})} = \frac{1+\alpha^6}{\alpha^5} = \alpha^2.$$

Thus we also get $\mathbf{C} = \mathbf{R} - \mathbf{E} = (\alpha^3, 1, 0, 0, \alpha^3, \alpha, 1)$.

2.5 $\mathbf{R} = (1, \alpha, \alpha^2, *, *, *, *)$, $r = 4$. The erasure locator polynomial is

$$\sigma_0(x) = (1 + \alpha^3 x)(1 + \alpha^4 x)(1 + \alpha^5 x)(1 + \alpha^6 x) = 1 + \alpha^5 x + \alpha^4 x^2 + x^3 + \alpha^4 x^4, \tag{1}$$

and the modified received vector $\mathbf{R}' = (1, \alpha, \alpha^2, 0, 0, 0, 0)$. Using $\mathbf{R}'$, we have $S(x) = \alpha^3 + \alpha^5 x + \alpha^6 x^2 + \alpha^6 x^3$. Thus

$$S_0(x) = S(x)\sigma_0(x) \bmod x^4 = \alpha^3 + \alpha^6 x + \alpha^5 x^2 + \alpha^2 x^3.$$

Since the number of erasures is 4 and $r = 4$, we have in the key equation

$$\sigma_1(x) S_0(x) \equiv \omega(x) \pmod{x^r},$$

$\deg \sigma_1(x) \leq 0$ and $\deg \omega(x) \leq 3$. Thus $\sigma_1(x) = 1$ and $\omega(x) = S_0(x)$, and finally

$$\sigma(x) = \sigma_0(x)\sigma_1(x) = \sigma_0(x). \tag{2}$$

Then we can use either frequency domain or time domain to complete the decoding.

(a) *Frequency domain.* Using $S_i = \alpha^5 S_{i-1} + \alpha^4 S_{i-2} + S_{i-3} + \alpha^4 S_{i-4}$, we have $\widehat{\mathbf{E}} = \mathbf{S} = (\alpha^5, \alpha^3, \alpha^5, \alpha^6, \alpha^6, \alpha^3, 0)$. So $\mathbf{E} = (0, 0, 0, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$ and the codeword is

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

(b) *Time domain.* From (1) and (2), we have for $i \in \{3, 4, 5, 6\}$, $\sigma(\alpha^{-i}) = 0$. Note that $\sigma'(x) = \alpha^5 + x^2$, so

$$E_3 = -\frac{\omega(\alpha^{-3})}{\sigma'(\alpha^{-3})} = \frac{\alpha^2}{\alpha^6} = \alpha^3, \quad E_4 = -\frac{\omega(\alpha^{-4})}{\sigma'(\alpha^{-4})} = \frac{\alpha^5}{\alpha} = \alpha^4,$$

$$E_5 = -\frac{\omega(\alpha^{-5})}{\sigma'(\alpha^{-5})} = \frac{\alpha^5}{1} = \alpha^5, \quad E_6 = -\frac{\omega(\alpha^{-6})}{\sigma'(\alpha^{-6})} = \frac{\alpha^2}{\alpha^3} = \alpha^6.$$

Thus we also get $\mathbf{C} = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6)$.