Problem 1

1)

Power	Polynomial	2 tuple vector
0	0	$(0,0)$
1	1	$(1,0)$
ω	ω	$(0,1)$
ω^2	$1+\omega$	$(1,1)$

2)

$+$	0	1	ω	ω^2
0	0	1	ω	ω^2
1	1	0	ω^2	ω
ω	ω	ω^2	0	1
ω^2	ω^2	ω	1	0

$\cdot$	0	1	ω	ω^2
0	0	0	0	0
1	0	1	ω	ω^2
ω	0	ω	ω^2	1
ω^2	0	ω^2	1	ω

Problem 2

1) $P(X) = X^2 + X + \omega$ is irreducible since if not then it is divisible by $X - a$ for some element a in $GF(4)$, i.e, it has a root in $GF(4)$. However,

$P(0) = 0 + 0 + \omega = \omega \neq 0$

$P(1) = 1 + 1 + \omega = \omega \neq 0$

$P(\omega) = \omega^2 + \omega + \omega = \omega^2 \neq 0$

$P(\omega^2) = \omega + \omega^2 + \omega = \omega^2 \neq 0$

Hence, $P(X)$ is irreducible.

2)

power	polynomial	2-tuple vector
0	0	$(0,0)$
1	1	$(1,0)$
α	α	$(0,1)$
α^2	$\omega + \alpha$	$(\omega,1)$
α^3	$\omega + \omega^2\alpha$	(ω,ω^2)
α^4	$1 + \alpha$	$(1,1)$
α^5	ω	$(\omega,0)$
α^6	$\omega\alpha$	$(0,\omega)$
α^7	$\omega^2 + \omega\alpha$	(ω^2,ω)
α^8	$\omega^2 + \alpha$	$(\omega^2,1)$
α^9	$\omega + \omega\alpha$	(ω,ω)
α^{10}	ω^2	$(\omega^2,0)$
α^{11}	$\omega^2\alpha$	$(0,\omega^2)$
α^{12}	$1 + \omega^2\alpha$	$(1,\omega^2)$
α^{13}	$1 + \omega\alpha$	$(1,\omega)$
α^{14}	$\omega^2 + \omega^2\alpha$	(ω^2,ω^2)

Problem 2 (cont.)

3)

element	minimal polynomial
1	$X+1$
α	$(X+\alpha)(X+\alpha^4) = X^2+X+\omega$
α^2	$(X+\alpha^2)(X+\alpha^8) = X^2+X+\omega^2$
α^3	$(X+\alpha^3)(X+\alpha^{12}) = X^2+\omega^2X+1$
α^4	$(X+\alpha^4)(X+\alpha) = X^2+X+\omega$
α^5	$X+\alpha^5 = X+\omega$
α^6	$(X+\alpha^6)(X+\alpha^9) = X^2+\omega X+1$
α^7	$(X+\alpha^7)(X+\alpha^{13}) = X^2+\omega X+\omega$
α^8	$(X+\alpha^8)(X+\alpha^2) = X^2+X+\omega^2$
α^9	$(X+\alpha^9)(X+\alpha^6) = X^2+\omega X+1$
α^{10}	$X+\alpha^{10} = X+\omega^2$
α^{11}	$(X+\alpha^{11})(X+\alpha^{14}) = X^2+\omega^2X+\omega^2$
α^{12}	$(X+\alpha^{12})(X+\alpha^3) = X^2+\omega^2X+1$
α^{13}	$(X+\alpha^{13})(X+\alpha^7) = X^2+\omega X+\omega$
α^{14}	$(X+\alpha^{14})(X+\alpha^{11}) = X^2+\omega^2X+\omega^2$

Problem 3

1) $g(X) = LCM\{\phi_1(X), \phi_2(X), \phi_3(X), \phi_4(X)\}$

where $\phi_i(X)$ is the minimal polynomial of α^i

$$g(X) = LCM\{X^2+X+\omega, X^2+X+\omega^2, X^2+\omega^2X+1, X^2+X+\omega\}$$

$$= (X^2+X+\omega)(X^2+X+\omega^2)(X^2+\omega^2X+1) = X^6+\omega^2X^5+X^4+X^3+\omega X^2+\omega X+1$$

2) Dimension $= 15 - \text{degree of } g(X)$

$= 15 - 6 = 9$

Number of codewords $= 4^9 = 262{,}144$

Problem 4

$r(X) = \omega^2 X^9 + \omega X^8 + X^3 + X$

Syndrome Computation: $S_1 = r(\alpha) = \alpha^2$, $S_2 = r(\alpha^2) = \alpha^{14}$, $S_3 = r(\alpha^3) = 0$, $S_4 = r(\alpha^4) = \alpha^8$.

Berlekamp-Massey Algorithm:

μ	$\sigma^{(\mu)}(x)$	d_μ	l_μ	ρ
-1	1	1	0	–
0	1	α^2	0	–
1	$1 + \alpha^2 X$	α^9	1	-1
2	$1 + \alpha^{12} X$	α^{11}	1	0
3	$1 + \alpha^{12} X + \alpha^9 X^2$	0	2	0
4	$1 + \alpha^{12} X + \alpha^9 X^2$	–	2	–

$\sigma(X) = \alpha^9 X^2 + \alpha^{12} X + 1$

$\sigma(X)$ has roots α^8 and α^{13}. Hence, $\beta_1 = \alpha^{-13} = \alpha^2$, $\beta_2 = \alpha^{-8} = \alpha^7$.

Error Evaluation:

$$Z_0 = S_1 + (S_2 + \sigma_1 S_1) X = \alpha^2 + (\alpha^{14} + \alpha^{12} \cdot \alpha^2) X = \alpha^2$$

$$\delta_k = -\frac{Z_0(\beta_k^{-1})}{\sigma'(\beta_k^{-1})} \quad \text{where} \quad \sigma'(X) = \alpha^{12}.$$

$$\delta_1 = -\frac{\alpha^2}{\alpha^{12}} = \alpha^5 = \omega, \qquad \delta_2 = -\frac{\alpha^2}{\alpha^{12}} = \alpha^5 = \omega.$$

$$e(X) = \omega X^2 + \omega X^7$$

$$v(X) = r(X) - e(X)$$

$$= \omega^2 X^9 + \omega X^8 + \omega X^7 + X^3 + \omega X^2 + X.$$