ECC 2020 HW 2

Prob. 1

(a) This number is $\leq (M-1)V_{d-1}$

(b) # of codes in which the i^{th} point is bad

$$\leq q^{n(M-1)} \cdot (M-1) V_{d-1} \qquad (1)$$

(c) There are M points in the code, and for each the number of ways to be bad is given in (1), so:

$$\#(\text{Bad codes}) \leq M(M-1) V_{d-1} q^{n(M-1)} \qquad (2)$$

If $M(M-1) V_{d-1} q^{n(M-1)} < q^{nM}$ ← # of all codes

then there is a good code. We obtain for M

$$M(M-1) < \frac{q^n}{V_{d-1}} \qquad (\text{asymptotically } 2R = 1 - h_q(\delta))$$

(d) Note that, from (1), the i^{th} point is bad in $\leq (M-1) q^{n(M-1)} V_{d-1}$ codes, and there are M points altogether, so the average # of bad points per code is

$$\leq \frac{M(M-1) V_{d-1} q^{n(M-1)}}{q^{nM}} = \frac{M(M-1) V_{d-1}}{q^n} \qquad (3)$$

Thus, there is a code with at most (3) bad points; let us discard them. For this, let us adjust the value of M so that, after the discarding, there are $\geq \frac{M}{2}$ points left.

Namely, take:

$$M \le \frac{q^n}{2V_{d-1}} + 1 < M+1,$$

then the right-hand side of (3) is $\le \frac{M}{2}$, and

then the remaining number of points in the code after discarding is $> \frac{M}{2} > \frac{q^n}{4V_{d-1}}$.

Moreover, the obtained code is good!

Prob. 2

(a) $x^4+x^3+1 = x^4(1+x^{-1}+x^{-4})$. The polynomial in the parentheses has zeros $\alpha^{-1}, \alpha^{-2}, \alpha^{-4}, \alpha^{-8}$, where $\alpha^4 = \alpha+1$. Ans: 4 zeros

(If you are wondering what is α^{-i}, it is $1\cdot\alpha^{-i} = \alpha^{15-i}$.)

For x^4+x^2+x we have

$$x^4+x^2+x = (x^3+x+1)x$$

The polynomial $f(x)=x^3+x+1$ generates $\mathbb{F}_8$ over $\mathbb{F}_2$, so its roots have order 7 (i.e., $a^7=1$ for all a such that $f(a)=0$). Since $\mathbb{F}_{16}$ does not contains elements of order 7 ($7 \nmid 15$), $f(x)$ has only one root $x=0$.

(b) Let β be a root of x^4+x^3+1. Per part (a) we have $\beta = \alpha^{-1}$ where α is such that $\alpha^4+\alpha+1=0$. Thus we have

$$\mathbb{F}_{16} = \begin{matrix} 0 & 1 & \beta & \beta^2 & \cdots & \beta^{14} \\ 0 & 1 & \alpha^{-1} & \alpha^{-2} & \cdots & \alpha^{-14} \\ & & \| & \| & & \| \\ & & \alpha^{14} & \alpha^{13} & & \alpha \end{matrix}$$

(c) Let $\alpha^4 = \alpha + 1$ be a primitive element of $\mathbb{F}_{16}$, and let $\beta = \alpha^3$. (using β instead of ξ)

We have

$$f(\beta) = \beta^4 + \beta^3 + \beta^2 + \beta + 1 = \frac{\beta^5 - 1}{\beta - 1} = \frac{(\alpha^3)^5 - 1}{\beta - 1} = 0$$

since $\beta \neq 0$ and $\alpha^{15} = 1$.

We can also take $\beta = \alpha^6$, α^9, or α^{12}. This yields isomorphic realizations.

Since $f(\beta^2) = (f(\beta))^2$, we obtain that $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ are roots of $f(x)$, i.e.,

$$f(x) = \prod_{i=0}^{3} (x - \beta^{2^i})$$

For the sake of contradiction, suppose that $f(x)$ is reducible over $\mathbb{F}_2$. It cannot have linear factors since $\beta^{2^i} \notin \mathbb{F}_2$ for $i = 0, 1, 2, 3$, so it must split into two quadratic factors, g_1 and g_2. The coefficients of g_1 (and g_2) must be 0 or 1, including the constant terms, but no 2 elements of the form β^{2^i} multiply to 0 or 1, contradiction.

$f(x)$ is not primitive, so the powers of β do not generate $\mathbb{F}_{16}$. Nevertheless, $\mathbb{F}_{16}$ can be obtained as a 4-dimensional linear space over $\mathbb{F}_2$

β^3	β^2	β	1		α^3	α^2	α	1	
0	0	0	0	0	0	0	0	0	0
0	0	0	1	β	1	0	0	0	α^3
0	0	1	0	β^2	1	1	0	0	α^6
0	1	0	0	β^3	1	0	1	0	α^9
1	0	0	0	$\beta+1$	1	0	0	1	α^{14}
0	0	1	1	β^2+1	1	1	0	1	α^{13}
0	1	0	1	$\beta^2+\beta$	0	1	0	0	α^2
0	1	1	0	β^3+1	1	0	1	1	α^7
1	0	0	1	$\beta^3+\beta$	0	0	1	0	α
1	0	1	0	$\beta^3+\beta^2$	0	1	1	0	α^5
1	1	0	0	$\beta^2+\beta+1$	0	1	0	1	α^8
0	1	1	1	$\beta^3+\beta+1$	0	0	1	1	α^4
1	0	1	1	$\beta^3+\beta^2+1$	0	1	1	1	α^{10}
1	1	0	1	$\beta^3+\beta^2+\beta$	1	1	1	0	α^{11}
1	1	1	0	$\beta^3+\beta^2+\beta+1$	1	1	1	1	α^{12}
1	1	1	1	$1 = \beta^0$	0	0	0	1	$1 = \alpha^0$
0	0	0	1						

To show that $1+\beta$ is primitive (in the problem statement $\beta = \xi$), we just note that $1+\beta = \alpha^{14}$. Since $\gcd(14,15)=1$, consecutive powers of $(1+\beta)$ exhaust all the elements in $\mathbb{F}_{16}\setminus\{0\}$, so it is primitive.

(d) The elements $a \in \mathbb{F}_{p^\ell}$ satisfy $a^{p^\ell - 1} = 1$, and the elements $b \in \mathbb{F}_{p^m}$ satisfy $b^{p^m - 1} = 1$.

Thus $\mathbb{F}_{p^\ell}$ is a subfield of $\mathbb{F}_{p^m}$ if and only if $(x^{p^\ell - 1} - 1) \mid (x^{p^m - 1} - 1)$, which happens if and only if $(p^\ell - 1) \mid (p^m - 1)$ (long division of polynomials), which in turn happens if and only if $\ell \mid m$ (long division).

Take $f(x) = x^6 + x + 1$; let α be a root of $f(x)$

The elements $(0, 1, \alpha^{21}, \alpha^{42})$ form $\mathbb{F}_4$ and the elements $(0, 1, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54})$ form $\mathbb{F}_8$.

Finally $$\alpha^{21} + \alpha^{42} = (\alpha^4 + \alpha^3 + \alpha^2 + \alpha) + (\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) = 1 \in \mathbb{F}_4$$

A more clever way of showing that $\alpha^{21} + \alpha^{42} \in \mathbb{F}_4$ is:

$$\alpha^{21} + \alpha^{42} = \alpha^{21} + (\alpha^{21})^2 = \gamma + \gamma^2 ; \text{ since } \gamma, \gamma^2 \in \mathbb{F}_4$$

and $\mathbb{F}_4$ is generated by $\varphi(x) = x^2 + x + 1$, we have $\varphi(\gamma) = 0$, i.e., $\gamma^2 + \gamma + 1 = 0$, or $\gamma^2 + \gamma = 1$.

Problem 3

1. Yes: all the consecutive powers of 2 mod 13 are distinct:

i	0	1	2	3	4	5	6	7	8	9	10	11
2^i	1	2	4	8	3	6	12	11	9	5	10	7

2. The parity check matrix can be written in the form

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^{2\cdot 2} & \dots & \alpha^{2(n-1)} \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \dots & \alpha^{(n-k)(n-1)} \end{bmatrix} = \text{rixForm=}$$

$$\begin{pmatrix} 1 & 2 & 4 & 8 & 3 & 6 & 12 & 11 & 9 & 5 & 10 & 7 \\ 1 & 4 & 3 & 12 & 9 & 10 & 1 & 4 & 3 & 12 & 9 & 10 \\ 1 & 8 & 12 & 5 & 1 & 8 & 12 & 5 & 1 & 8 & 12 & 5 \\ 1 & 3 & 9 & 1 & 3 & 9 & 1 & 3 & 9 & 1 & 3 & 9 \end{pmatrix}$$

3. Set up a system of linear equations for the coefficients of $Q(X,Y)$ using the conditions

$$Q(\alpha_i, y_i) = 0 \quad \text{(lec. 9, p. 7)}$$

There are 12 equations for 13 unknowns, so the system always has a nonzero solution. The matrix of the system has the form

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 2 & 4 & 8 & 3 & 6 & 12 & 11 & 9 & 5 & 0 & 0 & 0 \\ 1 & 4 & 3 & 12 & 9 & 10 & 1 & 4 & 3 & 12 & 10 & 1 & 4 \\ 1 & 8 & 12 & 5 & 1 & 8 & 12 & 5 & 1 & 8 & 3 & 11 & 10 \\ 1 & 3 & 9 & 1 & 3 & 9 & 1 & 3 & 9 & 1 & 10 & 4 & 12 \\ 1 & 6 & 10 & 8 & 9 & 2 & 12 & 7 & 3 & 5 & 2 & 12 & 7 \\ 1 & 12 & 1 & 12 & 1 & 12 & 1 & 12 & 1 & 12 & 4 & 9 & 4 \\ 1 & 11 & 4 & 5 & 3 & 7 & 12 & 2 & 9 & 8 & 12 & 2 & 9 \\ 1 & 9 & 3 & 1 & 9 & 3 & 1 & 9 & 3 & 1 & 0 & 0 & 0 \\ 1 & 5 & 12 & 8 & 1 & 5 & 12 & 8 & 1 & 5 & 8 & 1 & 5 \\ 1 & 10 & 9 & 12 & 3 & 4 & 1 & 10 & 9 & 12 & 9 & 12 & 3 \\ 1 & 7 & 10 & 5 & 9 & 11 & 12 & 6 & 3 & 8 & 6 & 3 & 8 \end{pmatrix}$$

and we obtain the error locator polynomial and $N(X)$ in the form

$$E(X) = 12 + X^2$$

$$N(X) = -(11 + 12X + 6X^2 + 7X^3 + 9X^4 + 8X^6 + 12X^7 + 5X^8 + 8X^9)$$

Then compute

$$f(X) = \frac{N(X)}{E(X)} = 11 + 12X + 4X^2 + 6X^3 + 6X^5 + 8X^6 + 5X^7$$

Evaluating $f(X)$ at α^i, $i = 0, \dots, 11$, we find the codeword

$$c = (0, 0, 10, 3, 10, 2, 7, 12, 0, 8, 9, 6)$$

There were 2 errors in locations $\alpha^0 = 1$, $\alpha^6 = 12$, and indeed

$$E(X) = 12 + X^2 = (X-1)(X-12).$$

(instead of computing $f(X)$, we could have found the roots of $E(X)$ and then found the error values at these two locations).

Problem 4.

(a) We write $c_i = f(\alpha^i)$ for some polynomial $f \in \mathbb{F}_q[x]$, $\deg f \le k-1$

$$x \cdot c(x) = x \sum_{i=0}^{n-1} f(\alpha^i) x^i = \sum_{i=0}^{n-1} f(\alpha^i) x^{i+1}$$

Let $f(x) = \sum_{i=0}^{k-1} f_i x^i$, and consider the polynomial

$$f^*(x) = f_0 + \sum_{i=1}^{k-1} (\alpha^{-1} f_i) x^i$$

We have $f^*(\alpha^i) = f(\alpha^{i-1})$, so upon evaluating $f^*(x)$ at $(1, \alpha, \dots, \alpha^{n-1})$ and noticing that $\alpha^{-1} = \alpha^{n-1}$, we obtain the codeword $c^* = (c_0^*, c_1^*, \dots, c_{n-1}^*)$, where $c_0^* = f(\alpha^{n-1}) = c_{n-1}$, $c_1^* = c_0$, $\dots$, $c_{n-1}^* = c_{n-2}$.

Since $\deg f^* \le k-1$, the vector $c^* \in RS$ (is a valid codeword)

We have shown that cyclic shift by one preserves the code, and by induction the same is true for any

cyclic shift to the left (or to the right).
Note that the above argument works because $\alpha^n = 1$,
so having $n = q-1$ is an essential assumption.
If $n < q-1$ (and n is not a divisor of $q-1$), RS codes of length n are not cyclic.

(b) This is a description of the RS code in cyclic form.
The dimension = the dimension of the linear space of polynomials $a(x) = \kappa$ (the number of coefficients)
The distance is d because the parity-check matrix of $\mathbb{D}$ has the form

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^{2\cdot 2} & \dots & \alpha^{2(n-1)} \\ \vdots & & & & \\ 1 & \alpha^{n-\kappa} & \alpha^{2(n-\kappa)} & \dots & \alpha^{(n-1)(n-\kappa)} \end{bmatrix}$$

and every submatrix formed of $n-\kappa$ columns has full rank
$\Rightarrow$ distance $d = n-\kappa+1$.

(c) The polynomial $g(x)$ represents a codeword in $\mathbb{D}$ and it has $n-\kappa+1$ coefficients, which must be nonzero to conform with the condition $d = n-\kappa+1$

(d) $d = 13$, $n = 15$, so $k = n-d+1 = 3$. We obtain

$$g(x) = \prod_{i=1}^{n-\kappa} (x - \alpha^i) = \sum_{i=0}^{12} g_i x^i, \text{ where}$$

$$g_0^{12} = (\alpha^3 \alpha^{13} \alpha^6 \alpha^2 \alpha^{14} \alpha^{13} \alpha^2 \,|\, \alpha^3 \alpha^8 \alpha^{14} \alpha^8 \,|\, 1)$$

(using GAP)

The generator matrix can be written in the form

$$\begin{bmatrix} g(x) \\ x\,g(x) \\ x^2 g(x) \end{bmatrix} = \begin{bmatrix} g_0 & \cdots & g_{12} & 0 & 0 & 0 \\ 0 & g_0 & \cdots & g_{12} & 0 & 0 \\ 0 & 0 & g_0 & \cdots & g_{12} & 0 \end{bmatrix}$$

Note that another form of the parity-check matrix is

$$n-k \begin{bmatrix} & & & h_{k-1} & \cdots & h_1 & h_0 \\ & & h_{k-1} & \cdots & h_1 & h_0 & \\ & & & \vdots & & & \\ h_{k-1} & \cdots & h_1 & h_0 & & & \end{bmatrix}$$

$\longleftarrow n \longrightarrow$

(in the example $k-1=2$)

where the polynomial $h(x) = \sum_{i=0}^{k-1} h_i x^i$ is given by

$$h(x) = \frac{x^n - 1}{g(x)} = \prod_{i=n-k+1}^{n} (x - \alpha^i)$$