Coding Theory: Practice Exam Solutions

1.

a)

0	1	α	α^2	α^3	α^4	α^5	α^6
000	001	010	100	011	110	111	101

b) i)

$$H_{3,1} = \begin{pmatrix} \alpha^6 & \alpha^5 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

ii) Note that $H_{3,1}v = \big(v(\alpha)\big)$, so $v(X)$ is a codeword if and only if $v(\alpha) = 0$. Since $v(X) \in \mathbb{B}[X]$, we know that $v(\alpha) = 0$ if and only if the minimal polynomial of α divides $v(X)$. Clearly, the minimal polynomial of α is $X^3 + X + 1$ so the generator polynomial of $\mathrm{Ham}(3)$ is $X^3 + X + 1$.

To show $\mathrm{Ham}(3)$ is cyclic, we need to show that the generator polynomial $X^3 + X + 1$ divides $X^7 - 1$. Indeed, by Fermat's little theorem, α is a zero of $X^7 - 1$, so its minimal polynomial $X^3 + X + 1$ divides $X^7 - 1$.

c) i) The standard choice of check matrix is

$$V_{3,2} = \begin{pmatrix} \alpha^6 & \cdots & \alpha^2 & \alpha & 1 \\ (\alpha^6)^2 & \cdots & (\alpha^2)^2 & \alpha^2 & 1 \\ (\alpha^6)^3 & \cdots & (\alpha^2)^3 & \alpha^3 & 1 \\ (\alpha^6)^4 & \cdots & (\alpha^2)^4 & \alpha^4 & 1 \end{pmatrix}.$$

The corresponding generator polynomial is $g^{\mathrm{RS}}_{3,2}(X) = (X-\alpha)(X-\alpha^2)(X-\alpha^3)(X-\alpha^4)$. We show that the F-linear code defined by the check matrix $V_{3,2}$ and the cyclic code defined by the generator polynomial $g^{\mathrm{RS}}_{3,2}(X)$ as follows. We identify, as usual, $v := (v_6, \cdots, v_0) \in F^7$ with $v(X) := v_6X^6 + \cdots + v_0 \in F[X]$. Then the equation $V_{3,2}v = 0$ translates to $v(\alpha) = \cdots = v(\alpha^4) = 0$; i.e. $(X-\alpha)|v(X), \cdots, (X-\alpha^4)|v(X)$, which is equivalent to requiring $g_{3,2}(X)|v(X)$.

To show $\mathrm{RS}(3,2)$ is cyclic, one needs to show that the generator polynomial divides $X^7 - 1$. Indeed, by Fermat's little theorem, we know that $X - \alpha^i$ divides $X^7 - 1$ for any i.

ii) Since the dimension of $\mathrm{RS}(3,2)$ is precisely $2^3 - 1 - 2\cdot 2 = 3$, the generator matrix is a 7×3-matrix with entries in F, and giving a generator matrix is equivalent to giving an injective F-linear map $F^3 \to F^7$.

The systematic encoding sends $u(X)$ to $u(X)\cdot X^4 - \Big(u(X)X^4 \bmod g^{\mathrm{RS}}_{3,2}(X)\Big)$, where $u(X) \in F[X]$ is of degree $\leqslant 2$ and $u(X)X^4 \bmod g^{\mathrm{RS}}_{3,2}(X)$ is the remainder of $u(X)X^4$ after long division by $g^{\mathrm{RS}}_{3,2}(X)$. (Note that what you obtain is a polynomial with degree $\leqslant 6$ with coefficients in F.) Under the usual identification[1], the systematic encoding gives an injective F-linear map $F^3 \to F^7$. (So far, we have not done anything but recalled various definitions.)

To find the 7×3 matrix corresponding to the systematic encoding, we plug in the "standard basis" of F^3; i.e. $(1,0,0)^\top, (0,1,0)^\top, (0,0,1)^\top \in F^3$. Note that they correspond to $X^2, X, 1 \in F[X]$, respectively. To proceed, we need to expand the generator polynomial.

$$\begin{aligned} g_{3,2}^{\mathrm{RS}}(X) &= X^4 + (\alpha + \alpha^2 + \alpha^3 + \alpha^4)X^3 \\ &\quad + (\alpha\alpha^2 + \alpha\alpha^3 + \alpha\alpha^4 + \alpha^2\alpha^3 + \alpha^2\alpha^4 + \alpha^3\alpha^4)X^2 \\ &\quad + (\alpha\alpha^2\alpha^3 + \alpha\alpha^2\alpha^4 + \alpha\alpha^3\alpha^4 + \alpha^2\alpha^3\alpha^4)X + \alpha\alpha^2\alpha^3\alpha^4 \\ &= X^4 + \alpha^3 X^3 + X^2 + \alpha X + \alpha^3 \end{aligned}$$

For the computation, use table in a) above.

We perform long division:

$$\begin{aligned} X^2 \cdot X^4 &= (X^2 + \alpha^3 X + \alpha^2) g_{3,2}^{\mathrm{RS}}(X) + \alpha^4 X^3 + X^2 + \alpha^4 X + \alpha^5 \\ X \cdot X^4 &= (X + \alpha^3) g_{3,2}^{\mathrm{RS}}(X) + \alpha^2 X^3 + X^2 + \alpha^6 X + \alpha^6 \\ 1 \cdot X^4 &= g_{3,2}^{\mathrm{RS}}(X) + \alpha^3 X^3 + X^2 + \alpha X + \alpha^3 \end{aligned}$$

So the systematic encoding produces:

$$\begin{aligned} X^2 &\mapsto X^6 + \alpha^4 X^3 + X^2 + \alpha^4 X + \alpha^5 \\ X &\mapsto X^5 + \alpha^2 X^3 + X^2 + \alpha^6 X + \alpha^6 \\ 1 &\mapsto X^4 + \alpha^3 X^3 + X^2 + \alpha X + \alpha^3 \end{aligned}$$

and if we rewrite this in vector form

$$\begin{aligned} (1,0,0)^\top &\mapsto (1,0,0,\alpha^4,1,\alpha^4,\alpha^5)^\top \\ (0,1,0)^\top &\mapsto (0,1,0,\alpha^2,1,\alpha^6,\alpha^6)^\top \\ (0,0,1)^\top &\mapsto (0,0,1,\alpha^3,1,\alpha,\alpha^3)^\top \end{aligned}$$

So the corresponding generator matrix is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha^4 & \alpha^2 & \alpha^3 \\ 1 & 1 & 1 \\ \alpha^4 & \alpha^6 & \alpha \\ \alpha^5 & \alpha^6 & \alpha^3 \end{pmatrix}$$

[1] We identify a vector $u \in F^3$ with a polynomial $u(X) \in F[X]$ with degree $\leqslant 2$, and a vector $v \in F^7$ with a polynomial $v(X) \in F[X]$ with degree $\leqslant 6$.

2. a) $$V_{k,t} = \begin{pmatrix} \alpha^{q-2} & \cdots & \alpha^2 & \alpha & 1 \\ (\alpha^{q-2})^2 & \cdots & (\alpha^2)^2 & \alpha^2 & 1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ (\alpha^{q-2})^{2t} & \cdots & (\alpha^2)^{2t} & \alpha^{2t} & 1 \end{pmatrix}.$$

b) $g^{\mathrm{RS}}_{k,t}(X) = \prod_{i=1}^{2t}(X-\alpha^i)$. This divides $X^{q-1}-1$ because by Fermat's little theorem $X-\alpha^i$ divides $X^{2^k-1}-1$ for any i.

Identify $v = (v_{q-2}, \cdots, v_0) \in F^{q-1}$ with $v(X) := v_{q-2}X^{q-2} + \cdots + v_0 \in F[X]$ Then $V_{k,t}v = 0$ can be rewritten as

$$\begin{aligned} v_{q-2}\alpha^{q-2} + \cdots + v_1\alpha + v_0 &= 0 \\ v_{q-2}(\alpha^2)^{q-2} + \cdots + v_1\alpha^2 + v_0 &= 0 \\ &\vdots \\ v_{q-2}(\alpha^{2t})^{q-2} + \cdots + v_1\alpha^{2t} + v_0 &= 0, \end{aligned}$$

i.e., $v(\alpha) = v(\alpha^2) = \cdots = v(\alpha^{2t}) = 0$. This shows that $v(X)$ is a $\mathrm{RS}(k,t)$-codeword if and only if $g^{\mathrm{RS}}_{k,t}(X)$ divides $v(X)$.

c) i) Let $v = (v_{q-2}, \cdots, v_0) \in F^{q-1}$ be a codeword such that $v_j = 0$ for any $j \neq i_1, \cdots i_{2t}$. we want to show that $v = 0$. Clearly,

$$0 = V_{k,t}v = \begin{pmatrix} \alpha^{i_{2t}} & & \alpha^{i_1} \\ \vdots & \cdots & \vdots \\ \alpha^{(2t)i_{2t}} & & \alpha^{(2t)i_1} \end{pmatrix} \begin{pmatrix} v_{i_{2t}} \\ \vdots \\ v_{i_1} \end{pmatrix}$$

But because the determinant of the square matrix is non-zero, it is invertible. Therefore,

$$\begin{pmatrix} v_{i_{2t}} \\ \vdots \\ v_{i_1} \end{pmatrix} = \begin{pmatrix} \alpha^{i_{2t}} & & \alpha^{i_1} \\ \vdots & \cdots & \vdots \\ \alpha^{(2t)i_{2t}} & & \alpha^{(2t)i_1} \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Therefore $v_{i_1} = \cdots = v_{i_{2t}} = 0$. But because $v_j = 0$ for all $j \neq i_1, \cdots, i_{2t}$, we conclude that $v = 0$.

ii) Any $2t+1$ vectors in F^{2t} are linearly dependent over F.Therefore, there exists an F-linear dependence relation

$$v_{2t}(\alpha^{2t}, \cdots, (\alpha^{2t})^{2t})^\top + \cdots + v_1(\alpha, \cdots, \alpha^{2t})^\top + v_0(1, \cdots, 1)^\top = 0, \tag{2.1}$$

where $v_0, v_1 \cdots, v_{2t} \in F$ and not all of them are zero. Now, take $v := (0, \cdots, 0, v_{2t}, \cdots, v_1, v_0) \in F^{q-1}$. Then we see

$$V_{k,t}v = v_{2t}(\alpha^{2t}, \cdots, (\alpha^{2t})^{2t})^\top + \cdots + v_1(\alpha, \cdots, \alpha^{2t})^\top + v_0(1, \cdots, 1)^\top = 0,$$

so v is a codeword of $\mathrm{RS}(k,t)$. This shows that the minimal distance of $\mathrm{RS}(k,t)$ is at most $2t+1$. On the other hand, part i) shows that the minimal distance of $\mathrm{RS}(k,t)$ is at least $2t+1$. So the minimal distance has to be exactly $2t+1$.

iii) Even though $V_{k,t}$ is a check matrix for $\mathrm{BCH}(k,t)$ the solution to part ii) does not work because $v_0, \cdots v_{2t}$ in equation ii) does not have to be elements of $\mathbb{B}$. In order to produce a codeword $v \in \mathbb{B}^{q-1}$ with $d(v,0) = 2t+1$ one has to find a linear dependence relation <u>over $\mathbb{B}$</u> of some $2t+1$ column vectors of $V_{k,t}$, but this is not always possible. Indeed any $2t+1$ vectors in F^{2t} are linearly dependent <u>over F</u> but the linear dependence relation doesn't need to have all coefficients in $\mathbb{B}$.

3. a) i) To show F_β is closed under addition and multiplication, consider two elements $\gamma := \sum_{n\geqslant 0} a_n\beta^n$ and $\delta := \sum_{n\geqslant 0} b_n\beta^n$. Now, one can obtain by direct computation that

$$\begin{aligned}\gamma+\delta &= \sum_{n\geqslant 0}(a_n+b_n)\beta^n \\ \gamma\cdot\delta &= \sum_{n\geqslant 0}\Big(\sum_{m=0}^{n} a_m b_{n-m}\Big)\beta^n.\end{aligned}$$

Clearly, $\gamma+\delta$ and $\gamma\cdot\delta$ satisfy the requirement for being elements in F_β.

To show F_β is a subfield, one needs to note:

- Note that $0,1 \in F_\beta$ (by taking $a_i = 0$ for all i, or $a_0 = 1$ and $a_i = 0$ for all $i > 0$).
- For $\gamma \in F_\beta$, $-\gamma \in F_\beta$ because $-\gamma = \gamma$ (i.e., $\gamma+\gamma = 0$).
- For any nonzero $\gamma \in F_\beta$, $\gamma^{-1} \in F_\beta$ because by Fermat's little theorem $\gamma^{-1} = \gamma^{2^k-2}$ and F_β is closed under multiplication.

ii) We need to show that any subfield $F' \subset F$ containing β also contains F_β. Indeed, F' is necessarily closed under addition and multiplication, so it has to contain all the elements of the form $\sum_{n\geqslant 0} a_n\beta^n$ for $a_n \in \mathbb{B}$.

b) Note that $\beta^2 = \alpha^2+\alpha+1 = \beta+1$ and $\beta^3 = 1$. Therefore, any element in F_β can be written as $a_0 + a_1\beta$ for $a_0, a_1 \in \mathbb{B}$; i.e., $F_\beta = \{0, 1, \beta, 1+\beta\}$.

Note that the smallest field containing α is F_α, but it is clear from the definition that any element $\gamma \in F$ also belongs to F_α; i.e., $F_\alpha = F$.

c) i) To check $F_{q'}$ is a subfield, we need to check the following:

- $0,1 \in F_{q'}$; this is obvious from the definition of $F_{q'}$.
- For any $\gamma \in F_{q'}$, we have $-\gamma, \gamma^{-1} \in F_{q'}$; indeed, $-\gamma = \gamma$, and $(\gamma^{-1})^{q'} = (\gamma^{q'})^{-1} = \gamma^{-1}$.
- $F_{q'}$ is closed under addition and multiplication; consider $\gamma, \delta \in F_{q'}$, in other words, $\gamma^{q'} = \gamma$ and $\delta^{q'} = \delta$. We have

$$\begin{aligned}(\gamma\delta)^{q'} &= \gamma^{q'}\delta^{q'} = \gamma\delta \\ (\gamma+\delta)^{q'} &= \gamma^{q'}+\delta^{q'} = \gamma+\delta.\end{aligned}$$

Note that the second line is obtained from iterating $(\gamma+\delta)^2 = \gamma+\delta$ using that $q' = 2^{k'}$.

Now we check that $|F_{q'}| = q'$. One can do this by writing down all the nonzero elements of $F_{q'}$ as powers of a (chosen) primitive element of F. We present an alternative solution. Note that elements of $F_{q'}$ are exactly zeroes of $X^{q'} - X = X(X^{q'-1}-1)$. So it is enough to show that

$X^{q'-1}-1$ has $q'-1$ zeroes in F. Note that $(q'-1)|(q-1)$; indeed, we have $\frac{q-1}{q'-1} = 1+q'+\cdots+(q')^{k/k'-1}$. (Recall that $q=2^k$, $q'=2^{k'}$ and $k'|k$.) Therefore $X^{q-1}-1 = (X^{q'-1}-1)(1+X^{q'-1}+\cdots+X^{\frac{q-1}{q'-1}-1})$. Now, by Fermat's little theorem, $X^{q-1}-1$ has exactly $q-1$ simple (i.e., distinct) zeroes in F, so it follows that its factor $X^{q'-1}-1$ has $q'-1$ zeroes.

ii) Since $F_{q'}$ is a subfield of F, F is a vector space over $F_{q'}$. In other words, there exists an $F_{q'}$-linear isomorphism $F \cong F_{q'}^n$ for a suitable n. By counting both sides, one obtain that $q=(q')^n$, so we have $k=k'n$.

iii) By the previous part, for any subfield $F' \subset F$ we have $|F'| = 2^{k'}$ for some $k'|k$. By Fermat's little theorem, any subfield $F' \subset F$ with $|F'| = q'$ should equal to $F_{q'}$. This shows that all the possible subfields of F are of the form $F_{q'}$ for some $q'=2^{k'}$ with $k'|k$.

Set $q'=2^{k'}$ for some $k'|k$. We will write down all the non-zero elements of $F_{q'}$ in terms of α. Indeed, $\beta := \alpha^{(q-1)/(q'-1)} \in F_{q'}$. Furthermore, $\beta^i \in F_{q'}$ for any i. Since α is a primitive element, it follows that $1,\beta,\beta^2,\cdots,\beta^{q'-2}$ are all distinct. So we have found $q'-1$ nonzero elements of $F_{q'}$. Hence,

$$F_{q'} = \{0,1,\beta,\beta^2,\cdots,\beta^{q'-2}\},$$

where $\beta := \alpha^{(q-1)/(q'-1)}$. We have any shown that any subfield of F is of this form for $q'=2^{k'}$ with $k'|k$.

iv) Let $k=4$. Then possible k' are 1, 2, and 4. Clearly, $F_2 = \mathbb{B}$, and $F_{16} = F$. It remains to find F_4.

Using the previous part $\beta = \alpha^{15/3} = \alpha^5 = \alpha^2+\alpha$, and $F_4 = \{0,1,\beta,\beta^2 = \beta+1\}$. This is the subfield found in b).

4. a) We present two solutions. Note that the check matrix $V_{4,2}$ for $\mathrm{RS}(4,2)$ is obtained by deleting the last two rows from the check matrix $V_{4,3}$ for $\mathrm{RS}(4,3)$. Therefore any $v \in F^{15}$ such that $V_{4,3}v = 0$ should also satisfy $V_{4,2}v=0$.

Alternatively, we may use the cyclic code description of $\mathrm{RS}(4,t)$, Let $g^{\mathrm{RS}}_{4,2}(X)$ and $g^{\mathrm{RS}}_{4,3}(X)$ denote the generator polynomials of $\mathrm{RS}(4,2)$ and $\mathrm{RS}(4,3)$, respectively. Observe that $g^{\mathrm{RS}}_{4,2}(X)$ divides $g^{\mathrm{RS}}_{4,3}(X)$ (which is clear from the formula). If $v(X)$ is a codeword of $\mathrm{RS}(4,3)$, then $g^{\mathrm{RS}}_{4,3}(X)$ divides $v(X)$, so clearly $g^{\mathrm{RS}}_{4,2}(X)$ also divides $v(X)$.

b) i) $s(z) = \alpha^3z^3+\alpha^4z^2+\alpha^3z+\alpha^5$. Since $s(z)\neq 0$, $d(X)$ is not a codeword and some error has occurred during transmission.

ii) We apply Euclid's algorithm for $s(z)$ and z^4:

Step 1 $\quad z^4 = (\alpha^{12}z+\alpha^{13})s(z)+r_1(z)$ where $r_1(z) = \alpha^8z^2+\alpha^5z+\alpha^3$.

Step 2 $\quad s(z) = (\alpha^{10}z+\alpha^8)r_1(z)+r_2(z)$ where $r_2(z) = \alpha^3z+\alpha^3$.

We stop the process since $\deg(r_2(z)) < 2$. Putting this all thgether, we get

$$\begin{aligned} r_2(z) &= s(z)+(\alpha^{10}z+\alpha^8)r_1(z) && \ldots\text{Step2} \\ &= s(z)+(\alpha^{10}z+\alpha^8)\Big((\alpha^{12}z+\alpha^{13})s(z)+z^4\Big) && \ldots\text{Step1} \\ &\equiv (\alpha^7z^2+\alpha^4z+\alpha^{13})s(z) \bmod z^4 \end{aligned}$$

Therefore we get

$$\begin{aligned} l(z) &= \alpha^2(\alpha^7 z^2+\alpha^4 z+\alpha^{13}) = \alpha^9 z^2+\alpha^6 z+1 \\ w(z) &= \alpha^2 r_2(z) = \alpha^5 z+\alpha^5. \end{aligned}$$

By exhaustive search, One can see that $l(z)$ has no roots in F; i.e., $l(z) \in F[z]$ is irreducible. (Mode B3) This cannot occur if there were at most 2 error symbols, so we conclude that there are at least 3 error symbols in the received word.

c) i) $s(z) = \alpha^3 z^3+\alpha^4 z^2+\alpha^3 z+\alpha^5$. Since $s(z) \neq 0$, $d(X)$ is not a codeword and some error has occurred during transmission.
Remark. It is a *mere coincidence* that the syndrome polynomial for the $\mathrm{RS}(4,3)$-decoding and the syndrome polynomial for $\mathrm{RS}(4,2)$-decoding, which was found in part b) i) coincide – in general, this is not the case. Note that in our message we have $d(\alpha^5) = d(\alpha^6) = 0$, which caused such a coincidence.

ii) We apply Euclid's algorithm for $s(z)$ and z^6:

Step 1 $z^6 = (\alpha^{12} z^3+\alpha^{13} z^2+\alpha^5 z+\alpha^3)s(z)+r_1(z)$ where

$$r_1(z) = \alpha^5 z^2+\alpha^7 z+\alpha^8.$$

We stop the process since $\deg(r_1(z)) < 3$.So

$$r_1(z) \equiv (\alpha^{12} z^3+\alpha^{13} z^2+\alpha^5 z+\alpha^3)s(z) \bmod z^6$$

Therefore we get

$$\begin{aligned} l(z) &= \alpha^{12}(\alpha^{12} z^3+\alpha^{13} z^2+\alpha^5 z+\alpha^3) = \alpha^9 z^3+\alpha^{10} z^2+\alpha^2 z+1 \\ w(z) &= \alpha^{12} r_1(z) = \alpha^2 z^2+\alpha^4 z+\alpha^5. \end{aligned}$$

By exhaustive search, we find the roots of $l(z)$ are $\alpha^{-7}, \alpha^{-8}, \alpha^{-9}$, so the error positions are $\{7,8,9\}$. We briefly explain how to find the roots of $l(z)$. (See the handout *Examples: Decoding Algorithm* for more details.) By plugging in $z = 1, \alpha^{-1}, \alpha^{-2}, \cdots$, we find α^{-7} is the first root of $l(z)$ (and is a simple root because it is not a root of $\frac{d}{dz} l(z) = \alpha^9 z^2+\alpha^2$). So $(1+\alpha^7 z)$ is a factor of $l(z)$ and its quotient is $\alpha^2 z^2+\alpha^{12} z+1$. Continuing the search, we see that α^{-8} is another root, so we have $\alpha^2 z^2+\alpha^{12} z+1 = (1-\alpha^8 z)(1-\alpha^s z)$ for some s. By comparing the coefficients of z^2 , we obtain $s = 9$.

So the error polynomial is of the form $e(X) = e_9 X^9+e_8 X^8+e_7 X^7$, where

$$\begin{aligned} e_9 &= w(\alpha^{-9})(\alpha^{-9}(1-\alpha^7\alpha^{-9})^{-1}(1-\alpha^8\alpha^{-9})^{-1} = 1 \\ e_8 &= w(\alpha^{-8})\alpha^{-8}(1-\alpha^7\alpha^{-8})^{-1}(1-\alpha^9\alpha^{-8})^{-1} = \alpha^9 \\ e_7 &= w(\alpha^{-7})\alpha^{-7}(1-\alpha^8\alpha^{-7})^{-1}(1-\alpha^9\alpha^{-7})^{-1} = \alpha^{11} \end{aligned}$$

So $e(X) = X^9+\alpha^9 X^8+\alpha^{11} X^7$

iii) Assume that the correction via $\mathrm{RS}(4,3)$-decoding algorithm is correct. Then the transmitted codeword $c(X) = d(X)+e(X)$ is an $\mathrm{RS}(4,3)$-codeword and three symbols are transmitted incorrectly during transmission. But since $c(X)$ is also a $\mathrm{RS}(4,2)$-codeword by part a), you may try the $\mathrm{RS}(4,2)$-decoding algorithm. This will not work because $\mathrm{RS}(4,2)$-decoding algorithm can correct at most two error symbols in a block, and there are three error symbols.

Remark. In the remark, I ask you to re-do this question for the following syndromes:

$$d(\alpha) = d(\alpha^2) = 0, \quad d(\alpha^3) = \alpha^{13}, \quad d(\alpha^4) = \alpha^{11}, \quad d(\alpha^5) = \alpha^7, \quad d(\alpha^6) = \alpha^6.$$

The "interesting and instructive" feature here is that both the $\mathrm{RS}(4,2)$- and $\mathrm{RS}(4,3)$- decoding algorithms work, but produce different error polynomials. The $\mathrm{RS}(4,2)$-decoding algorithm should produce $X^4 + \alpha^{13}X^3$ as the error polynomial, while $\mathrm{RS}(4,3)$-decoding algorithm should produce $\alpha^6X^2 + \alpha^3X + \alpha^{10}$. This indicates that even when there are more than 2 error symbols, the $\mathrm{RS}(4,2)$-decoding algorithm might work but it produces a wrong error polynomial.

Here is a more detailed explanation to this phenomenon. One can observe that both error polynomials produce the *same* syndromes for $i = 1,2,3,4$; i.e. when evaluated at $X = \alpha, \alpha^2, \alpha^3, \alpha^4$ they produce the same values as above. But when evaluated at $X = \alpha^5, \alpha^6$, the former one (produced by the $\mathrm{RS}(4,2)$-decoding algorithm) gives wrong syndromes while the latter one (produced by the $\mathrm{RS}(4,3)$-decoding algorithm) gives the right syndromes. Roughly speaking what the $\mathrm{RS}(4,2)$-decoding algorithm does is to find an error polynomial with at most two non-zero terms which has the same syndromes for $i = 1,2,3,4$ as given. And as we have seen above it is possible that an error polynomial with more than two non-zero terms have exactly the same syndromes for $i = 1,2,3,4$ as a polynomial with at most two non-zero terms. In that case, the $\mathrm{RS}(4,2)$-decoding algorithm produces a wrong error polynomial (the one with at most two non-zero terms). So in practice, in order for the $\mathrm{RS}(4,t)$-decoding algorithm to be completely reliable, the chance of having more than t error symbols in a single block should be negligible.

For the next set of syndromes:

$$d(\alpha) = d(\alpha^2) = 0, \quad d(\alpha^3) = \alpha^{13}, \quad d(\alpha^4) = \alpha^{11}, \quad d(\alpha^5) = \alpha^7, \quad d(\alpha^6) = \alpha^6$$

the $\mathrm{RS}(4,3)$-decoding algorithm should produce the error polynomial $\alpha^4X^5 + \alpha^9X^4 + \alpha^7X^3$. If you run the $\mathrm{RS}(4,2)$-decoding algorithm, you will run into the failure mode A since the syndrome polynomial is divisible by z^2.

For the last set of syndromes:

$$d(\alpha) = \alpha^6, \quad d(\alpha^2) = (\alpha^3) = 0, \quad d(\alpha^4) = \alpha^3, \quad d(\alpha^5) = \alpha, \quad d(\alpha^6) = \alpha^{12}$$

the $\mathrm{RS}(4,3)$-decoding algorithm should produce the error polynomial $\alpha^4X^5 + \alpha^{10}X^4 + \alpha^9X^3$. If you run the $\mathrm{RS}(4,2)$-decoding algorithm, you will run into the failure mode B1 since Euclid's algorithm terminates in step 1 and produces $r_1(z) = \alpha^3 z$ which has $z = 0$ as a root.