#20

a)

Il peut corriger 7 erreurs s'il y a seulement une erreur dans chaque groupe de 3 bits.
2 erreurs ne peuvent pas se retrouver dans un même 3 bits.

b)

D'abord, ne parlons pas des bits, mais des caractères (éléments de $\mathbb{F}_{2^3}$).
Le principe de Reed-Solomon $C(7,3)$ est de prendre tous les groupes de 3 equations possibles (sur 7) et regarder quel résultat $u = (u_0, u_1, u_2)$ revient le plus souvent.
On veut que la vraie réponse revienne le plus souvent. Alors, en référence à la p. 200 du manuel, on veut :

$$\binom{2^m - s - 1}{k} > \binom{s + k - 1}{k}$$

nombre de façons de choisir k équations sans erreur

↳ nb façons max de retomber sur la même erreur.

ici, $m=3$, $k=3$. s est le nb d'erreurs.

$$\binom{2^m - s - 1}{k} > \binom{s + k - 1}{k} \xrightarrow{\text{ici}} \binom{8 - s - 1}{3} > \binom{s + 3 - 1}{3}$$

$\Leftrightarrow 7 - s > s + 2 \Leftrightarrow s < \frac{5}{2} \Rightarrow s \leq 2.$

Le nb d'erreurs de caractères max est de 2.

Puis, ces caractères sont mis en bits :

$$\begin{matrix} V_0 & V_1 & \cdots & V_7 \\ b_0 b_1 b_2 & c_0 c_1 c_2 & & \end{matrix}$$

on peut corriger 2 v_i, c'est-à-dire corriger 2 groupes de $b_0 b_1 b_2$ ou $c_0 c_1 c_2$ ... On peut alors corriger au max 6 bits, à condition qu'ils se retrouvent dans les mêmes groupes de 3 bits.

23

$\mathbb{F}_8 = \mathbb{F}_2[x]/P(x)$ où $P(x)$ doit être un poly. irréd de deg 3.
(car $\mathbb{F}_8 = \mathbb{F}_{2^3}$.)

on prend $P(x) = x^3 + x + 1$, irréduc.
on trouve une racine primitive α
tq $\mathbb{F}_8 = (0, \alpha, \alpha^2, \dots, \alpha^7 = 1)$

$$\boxed{\alpha = x.}$$

$$\boxed{\alpha^2 = x^2}$$

$$\boxed{\alpha^3} = x^3 + x^3 + x + 1 = \boxed{x+1}$$

$$\alpha^4 = \alpha^3 \cdot \alpha = (x+1)x = \boxed{x^2 + x}$$

$$\alpha^5 = \alpha^2 \cdot \alpha^3 = x^2(x+1) = x^3 + x^2$$
$$= x^3 + x^2 + x^3 + x + 1$$
$$= \boxed{x^2 + x + 1}$$

$$\alpha^6 = \alpha^3 \cdot \alpha^3 = (x+1)(x+1) = x^2 + 2x + 1 = \boxed{x^2 + 1}$$

$$\alpha^7 = \alpha^4 \cdot \alpha^3 = (x^2 + x)(x+1) = x^3 + x^2 + x^2 + x$$
$$= x^3 + x$$
$$= x^3 + x + x^3 + x + 1$$
$$= \boxed{1}$$

a) comme au 20 b).

b) on a le message $u=(u_0,u_1,u_2)=(0,1,\alpha)$

on encode alors le message avec le polynôme $q(x)=u_0+u_1x+u_2x^2$

$$=0+x+\alpha x^2$$

encoder:

$V_0=q(\alpha^0=1)=1+\alpha=1+x=\alpha^3$

$V_1=q(\alpha)=\alpha+\alpha^3=x+x+1=1$

$V_2=q(\alpha^2)=\alpha^2+\alpha^5=x^2+x^2+x+1=x+1=\alpha^3$

$V_3=q(\alpha^3)=\alpha^3+\alpha^7=x+1+1=x=\alpha$

$V_4=q(\alpha^4)=\alpha^4+\alpha^9=\alpha^4+\alpha^7\cdot\alpha^2=x^2+\cancel{x^2}=0$

$V_5=q(\alpha^5)=\alpha^5+\alpha^{11}=\alpha^5+\alpha^4=x^2+x+1+x^2+x=1$

$V_6=q(\alpha^6)=\alpha^6+\alpha^{13}=\alpha^6+\alpha^6=0$

Le mot encodé est alors:

$(\alpha^3,1,\alpha^3,\alpha,0,1,0)$

c) $P \in \mathbb{F}_{2^m}^{2^m-1}$, $u \in \mathbb{F}_{2^m}^{k}$, $C \in \mathbb{F}_{2^m}^{(2^m-1)\times k}$

P : mot encodé $\quad$ u : mot $\quad$ C : matrice ici 7×3.

$u = (u_0, u_1, u_2)$, $P(x) = u_0 + u_1 x + u_2 x^2$

$v_0 = P(1) = u_0 + u_1 + u_2$

$v_1 = P(\alpha) = u_0 + u_1\alpha + u_2\alpha^2$

$v_2 = P(\alpha^2) = u_0 + u_1\alpha^2 + u_2\alpha^4$

$v_3 = P(\alpha^3) = u_0 + u_1\alpha^3 + u_2\alpha^6$

$\vdots$

$v_6 = P(\alpha^6) = u_0 + u_1\alpha^6 + u_2\alpha^5$

$$C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \\ 1 & \alpha^3 & \alpha^6 \\ 1 & \alpha^4 & \alpha \\ 1 & \alpha^5 & \alpha^3 \\ 1 & \alpha^6 & \alpha^5 \end{pmatrix}, \quad u = \begin{pmatrix} u_0 \\ u_1 \\ u_2 \end{pmatrix}$$

Table d'addition pour nous aider avec les calculs

+	0	α	α^2	α^3	α^4	α^5	α^6	1
0	0							
α	α	0						
α^2	α^2	α^4	0					
α^3	α^3	1	α^5	0				
α^4	α^4	α^2	α	α^6	0			
α^5	α^5	α^6	α^3	α^2	1	0		
α^6	α^6	α^5	1	α^4	α^3	α	0	
$\alpha^7 = 1$	1	α^3	α^6	α	α^5	α^4	α^2	0

d) 0^e, 1^e et 4^e ligne de ma matrice C :

$$D = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^4 & \alpha \end{pmatrix}, \quad W = Du$$

$$w = (1, \alpha^4, \alpha^2, \alpha^4, \alpha^2, \alpha^4, \alpha^2).$$

$$D u = \bar{w} \Rightarrow \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \\ 1 & \alpha^4 & \alpha \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha^4 \\ \alpha^2 \end{pmatrix}$$

$$\sim \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^2 \end{array}\right) \underset{L_{31}(-1)}{\overset{L_{21}(-1)}{\sim}} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha^5 \\ 0 & \alpha^5 & \alpha^3 & \alpha^6 \end{array}\right)$$

$$\overset{L_{21}(-\alpha^2)}{\sim} \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & \alpha^3 & \alpha^6 & \alpha^5 \\ 0 & 0 & \alpha^2 & \alpha^4 \end{array}\right) \Rightarrow \alpha^2 u_2 = \alpha^4$$

$$\Rightarrow u_2 = \alpha^2$$

(2) $\alpha^3 u_1 + \alpha^6 \cdot u_2 = \alpha^5$

$$\Rightarrow \alpha^3 u_1 = \alpha^5 - \alpha^8 = \alpha^5 - \alpha = x^2 + x + 1 + x$$

$$= x^2 + 1 = \alpha^6$$

$$\Rightarrow u_1 = \alpha^3$$

(1) $u_0 + u_1 + u_2 = 1$

$$\Rightarrow u_0 = 1 - \alpha^3 - \alpha^2$$

$$= 1 - x - 1 - x^2 = -x^2 - x$$

$$= x^2 + x = \alpha^4$$

$$\Rightarrow (u_0, u_1, u_2) = (\alpha^4, \alpha^3, \alpha^2)$$

e)*changement de question:

Sachant qu'il y a au plus 2 erreurs, combien de systèmes devra-t-on résoudre pour être sûr de n'avoir aucune erreur?

il faut en évaluer plus de

$\binom{s+k-1}{k}$ où ici, $k=3$ → nombre de caractères dans notre message.

$s=2$ → nb d'erreurs.

$=\binom{4}{3}=4$

Il faudra alors obtenir 5 fois le même résultat de (u_0, u_1, u_2) avec différents systèmes pour être sûr que c'est la bonne réponse.

Exercice D

1.

On a $\mathbb{F}_2[x]/_{x^2+x+1}$

$\alpha = x$. On se demande si $\mathbb{F}_4 = \{0, \alpha, \alpha^2, \alpha^3 = 1\}$

$\alpha = x$

$\alpha^2 = x^2 = x^2 + x^2 + x + 1 = 2x^2 + x + 1 = x + 1$

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

$= 2x^2 + 2x + 1$

$= 1$

Aidons-nous d'une table d'addition :

+	0	α	α^2	$\alpha^3 = 1$
0	0	α	α^2	α^3
α	α	0	1	α^2
α^2	α^2	1	0	α
α^3	α^3	α^2	α	0

2.

$u \in (\mathbb{F}_4)^2$, c'est-à-dire qu'il y a dans chaque message u 2 éléments de $\mathbb{F}_4$.

$u = (u_0, u_1)$, $u_0, u_1 \in \mathbb{F}_4$.

Dans chacun de ces éléments on a 2 bits:

$(0,0), (0,1), (1,0)$ ou $(1,1)$.

on a alors 4 bits dans un message u.

3.

On cherche un message $u=(u_0, u_1) \in \mathbb{F}_4^2$ en recevant un message de 3 caractères $w \in \mathbb{F}_4^3$ $w=(w_0, w_1, w_2)$.

on a alors 3 choix de 2 équations à résoudre.

$\bar{u}_1 \rightsquigarrow$ résultat en utilisant w_0 et w_1.

$\bar{u}_2 \rightsquigarrow$ " " " " " " " w_1 et w_2

$\bar{u}_3 \rightsquigarrow$ " " " " " " w_0 et w_2.

supposons qu'il y a une erreur dans w_0. alors, $\bar{u}_1 \neq \bar{u}_2$ et $\bar{u}_3 \neq \bar{u}_2$ et $\bar{u}_1 \neq \bar{u}_3$ (Parfois $\bar{u}_1 = \bar{u}_3$, mais pas nécessairement)

Il n'y a pas moyen de savoir lequel de $\bar{u}_1, \bar{u}_2$ ou $\bar{u}_3$ est le bon (mais on peut détecter l'erreur).

4.

$(1,1)$

$(0,0)$ $(1,0)$

on a $(1,1,0,0,1,0) \longrightarrow (0, 1, \alpha^2)$

on cherche $u = (u_0, u_1)$ ~~avec Reed~~

Posons $q(x) = u_0 + u_1 x$.

$q(1) = u_0 + u_1$, $q(\alpha) = u_0 + u_1 \alpha$, $q(\alpha^2) = u_0 + u_1 \alpha^2$.

on a alors le système

$$\begin{pmatrix} 1 & 1 \\ 1 & \alpha \\ 1 & \alpha^2 \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ \alpha^2 \end{pmatrix}$$

Je choisis deux lignes pour résoudre le système.

$$\begin{pmatrix} 1 & 1 \\ 1 & \alpha \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \sim \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 1 & \alpha & 1 \end{array}\right)$$

$$\overset{L_2, (-1)}{\sim} \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & \alpha^2 & 1 \end{array}\right)$$

De la 2^e ligne: $\alpha^2 u_1 = \overset{= \alpha^3}{1} \Rightarrow u_1 = \alpha$.

De la $1^{ère}$ ligne: $u_0 + u_1 = 0 \Rightarrow u_0 + \alpha = 0 \Rightarrow u_0 = \alpha$

Le mot cherché est alors $u = (\alpha, \alpha)$.