1 Comparaison de différents codes correcteurs

1.

a. *$\delta(C)$ est le minimum des poids : $Min(w(x); x \neq [0\dots0]) = m$.*

b. Il faut $m = 2*2+1 = 5$. Donc $(5,1)$ convient. $(5k,k)$ aussi.

c. *$(5k,k)$, est de rendement $\frac{k}{5k} = 0.2$.*

2.

a. *On construit $\mathbb{F}_8$ comme étant $\mathbb{Z}/_{2\mathbb{Z}}[Y]/Q$. Soit aY^2+bY+c un résidu modulo Q; on le note: $[a,b,c]$. On a $\mathbb{F}_8^\star = \{[010]^i \mod Q; i = 0,\dots,6\}$.*

b. $[010]^3 = Y^3 = 1+Y = [011]$, $[010]^4 = Y^4 = Y(1+Y) = Y+Y^2 = [110]$.
NB: Pour vérifier que Q est primitif il suffit d'exhiber toutes les puissances de Y pour montrer que Y est générateur de $\mathbb{F}_8^*$:
$[010]^5 = Y(Y^4) = Y(Y+Y^2) = Y^2+1+Y = [111]$, $[010]^6 = Y(Y^5) = Y^3+Y+Y^2 = Y^2+1 = [101]$ et $[010]^7 = Y(Y^7) = Y^3+Y = 1 = [001]$.

c. $n = q-1 = 8-1 = 7$.

d. Avec b., il suffit de prendre $g = (X-[010])*(X-[010]^2)*(X-[010]^3)*(X-[010]^4)$ soit $g = (X-[010])*(X-[100])*(X-[011])*(X-[110])$. Les racines de g sont une suite de 4 puissances successives d'une racine primitive. Donc g donne un code de distance 5, 4-détecteur et 2-correcteur.

e. *Le code est $(7,3)$ car g est de degré 3. Donc le rendement est $\frac{3}{7} = \frac{9}{21} \approx 0,43$ en terme de bits ou d'éléments.*

3.

a. *Le code sera $(15,11,5)$.*

b. rendement de $\frac{11}{15} \approx 0.73$; taux de correction de $\frac{2}{15} \approx 0.13 \approx 13\%$.

c. *rendement de $\frac{44}{60} \approx 0.73$; taux de correction de $\frac{2}{60} \approx 0.033 \approx 3\%$. Mais, on peut corriger jusqu'à 8 erreurs de bits si les erreurs de bits portent uniquement sur 2 chiffres hexadécimaux (les 13 autres étant corrects).*

4. *On choisit $k > 0.75n$ et on veut $t \geq 2$. Donc $m \leq \frac{n-k}{2} < 0.125n$. On choisit n plus petite puissance de 2 telle que $log_2 n < 0.125n$. $n = 64 = 2^6$ convient. On prend $k = 64 \times 0.75 = 48$
On obtient un code $(64,48)$ qui est $\frac{16}{6} \approx 2.67 > 2$ correcteur.
Le rendement est de 75% et le taux de correction $\frac{2}{64} \approx 3.1\%$.*

Construction d'un code de Reed-Solomon adapté

1. $p_8 = 1 - 0.999^8 = 0.00797$

Rappel.

2.

a. *Comme on envoie des octets, on choisit $\mathbb{F}_{256}$, qui a $q = 256 = 2^8$ éléments, comme corps de base. Un code de Reed-Solomon impose alors de choisir $n = q - 1 = 255$.*

b. Pour corriger au moins $0.0079n = 2.03$ erreurs, il faut avoir pouvoir corriger 3 erreurs, donc choisir un code de distance $\delta \geq 2 * 3 + 1 = 7$. Avec un code de Reed-Solomon, le polynôme générateur est de degré $r = \delta - 1 = 6$.

c. *Le nombre maximal d'erreurs détectées est 6.*

d. Soit $g = \sum_{i=0}^{6} g_i X^i$ le polynôme générateur. La matrice génératrice a 248 lignes et 255 colonnes. Elle s'écrit sous la forme

$$\begin{bmatrix} g_0 & g_1 & \dots & g_6 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_6 & \dots & 0 \\ & & & \dots & & & \end{bmatrix}$$

e. *On choisit donc $P = 1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^8$ pour implémenter $\mathbb{F}_{256} = \mathbb{F}_2[\alpha]/P$. Soit $X = \sum_{i=0}^{7} x_i \alpha^i$ avec $x_i \in \{0, 1\}$; X est représenté par l'octet $(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7)$.*
Soit $Y = \sum_{i=0}^{7} y_i \alpha^i$ avec $y_i \in \{0, 1\}$ un autre élément du corps.
$X + Y$ est alors représenté par l'octet $(x_0 + y_0, \dots x_7 + y_7)$.
Pour $X.Y$, on calcule le produit de polynômes $X.Y$ mod P; les coefficients de ce polynôme permettent d'obtenir le codage de XY sous forme d'octet.

f. Comme P est primitif, α un élément générateur de $\mathbb{F}_{256}^{\star}$ (une racine primitive 255-ième de l'unité). Il suffit donc de choisir comme polynôme générateur $g = \prod_{i=1..6}(X - \alpha^i)$ mod $P = X^6 + \sum_{i=0}^{5} g_i X^i$, où chaque g_i est un élément de $\mathbb{F}_{256}$ représenté par un octet (cf question précédente).

3. *La capacité du canal binaire symétrique de probabilité d'erreur $q = 0.001$ est $C = 1 + q \log_2 q + (1 - q) \log_2 (1 - q) = 0.98859$.*
Le rendement du code ne dépasse pas la capacité du canal (deuxième théorème de Shannon).