1 Comparaison de différents codes correcteurs

On veut comparer le rendement en terme de bits de différents codes 2-correcteurs.

1. Nous considérons tout d'abord un code de répétition sur $V = \{0, 1\}$, c'est à dire un code (mk, k) où chaque groupe de k bits est simplement répété m fois.

a. Quelle est la distance minimale entre deux mots de code ?

b. Proposer un code de répétition qui soit 2-correcteur

c. Quel est son rendement ?

2. Soit un code de Reed-Solomon 2-correcteur sur $\mathbb{F}_8$ et son rendement en terme de bits.

a. On admet que $Q = 1 + Y + Y^3$ est un polynôme primitif de $\mathbb{F}_2[Y]$. En déduire une construction possible de $\mathbb{F}_8$.

b. Que valent $[010]^3$, $[010]^4$ dans cette construction ?

c. Nous construisons maintenant un code de Reed-Solomon sur $\mathbb{F}_8$. Quelle doit être la taille n des mots de code ?

d. Expliciter un polynôme générateur d'un code 2-correcteur. Combien d'erreurs peut-il détecter ?

e. Quel est le rendement de ce code en terme d'éléments de $\mathbb{F}_8$? en terme de bits totaux ?

3. On admet que $1 + Y + Y^4$ est un polynôme primitif de degré 4 sur $\mathbb{Z}/_{2\mathbb{Z}}[Y]$.

a. Donner les caractéristiques (n, k, d) d'un code de Reed-Solomon 2-correcteur sur $\mathbb{F}_{16}$.

b. On implémente ce code sur un canal hexadécimal : quel est le rendement de ce code ? quel est le taux de correction (i.e. le pourcentage d'erreurs corrigées) ?

c. On implémente ce code sur un canal binaire : quel est le rendement de ce code ? quel est le taux de correction ?

4. Soit $n = 2^m$; un code de Goppa (n, k) sur $\mathbb{F}_2$ est un code linéaire qui est $t = \frac{n-k}{m}$ correcteur. Donner un choix de n et k qui permet d'obtenir un code de Goppa 2-correcteur avec un rendement supérieur à 75%.

Construction d'un code de Reed-Solomon adapté

On considère une liaison infrarouge modélisée par un canal binaire symétrique de probabilité d'erreur 0.001. On désire ici assurer des transmissions fiables sur ce canal.

1. Quelle est la probabilité p d'erreur lorsqu'on envoie un octet ?

Rappel. Soit α un élément primitif du corps $V = \mathbb{F}_q$.
On rappelle que les codes de Reed-Solomon sont des codes cycliques sur V de de longueur $n = q - 1$ dont le polynôme générateur g de degré r est de la forme :

$$g(X) = \prod_{i=s}^{s+r-1} (X - \alpha^i) .$$

Le code de Reed-Solomon ainsi obtenu est donc un code $(n = q-1, k = n-r = q-1-r)$ avec r arbitraire. Ce code est de distance $r+1$ [cf polycopié].
En choisissant r, on peut donc construire un code de distance arbitraire, donc de taux de correction arbitraire.

2. Pour remédier aux erreurs dues au canal, lorsqu'on envoie n octets, on veut garantir de corriger jusqu'à $p \times n$ erreurs. Expliquer comment construire un code correcteur de type Reed-Solomon en précisant :

a. le corps de base et la valeur choisie pour n;

b. le degré du polynôme générateur et le rendement du code.

c. le nombre maximal d'erreurs détectées;

d. la dimension d'une matrice génératrice du code. Comment s'écrit cette matrice à partir des coefficients du polynôme générateur ?

Pour $d = 3, .., 10$, les polynômes suivants à coefficients dans $\mathbb{F}_2$ sont primitifs :

degré d	Polynôme primitif
3	$1 + \alpha + \alpha^3$
4	$1 + \alpha + \alpha^4$
5	$1 + \alpha^2 + \alpha^5$
6	$1 + \alpha + \alpha^6$

degré d	Polynôme primitif
7	$1 + \alpha^3 + \alpha^7$
8	$1 + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^8$
9	$1 + \alpha^4 + \alpha^9$
10	$1 + \alpha^3 + \alpha^{10}$

e. donner le polynôme utilisé pour implémenter le corps de base et expliquer brièvement comment réaliser les opérations d'addition et de multiplication;

f. donner l'expression du polynôme générateur en fonction de α.

3. Calculer la capacité du canal. Comparer au rendement du code proposé.