**Feuille TD 5 - Codes cycliques**

On suppose que le vocabulaire $V$ du canal $V$ est un corps fini (i.e. possède $q = p^m$ chiffres). Soit l'application linéaire $\sigma$ de $V^n$, appelée *opération de décalage*, définie par $\sigma([u_0, \ldots, u_{n-1}]) = [u_{n-1}, u_0, \ldots, u_{n-2}]$ .. Un code linéaire $C$ sur $V$ est *cyclique* ssi $\forall x \in C : \sigma(x) \in C$ .
Les codes cycliques ont un double intérêt : d'une part [exercice 1], le codage et le décodage/correction sont rapides, en $O(n \log n)$; d'autre part, il est possible de construire des codes cycliques, tels les codes de Reed-Solomon [exercice 2] de distance maximale, atteignant la borne de Singleton.

# 1 Caractérisation d'un code cyclique

Dans toute la suite, $C$ désigne un code cyclique $(n, k)$ quelconque (sous forme systématique).

1. Montrer que le code binaire de parité $(n, n-1, 2)$ est un code cyclique.

2. Expliciter $\sigma^{-1}$. En déduire que si $x \in C$, alors $\sigma^{-1}(x) \in C$.

3. Montrer que $C$ admet une matrice génératrice $G_C$ de la forme :

$$G_C = \begin{bmatrix} m \\ \sigma(m) \\ \ldots \\ \sigma^{k-1}(m) \end{bmatrix}$$

avec $m = [a_0, a_1, \ldots, a_{n-k} = 1, 0, \ldots, 0]$.
**Indication:** on pourra considérer $\sigma^{1-k}(u)$ où $u$ est la dernière ligne de la matrice génératrice normalisée de $C$.

4. Tout élément $U = [u_0, \ldots, u_{n-1}]$ de $V^n$ peut être représenté par le polynôme $P_U$ de degré $n$ de $V[X]$ défini par : $P_U = \sum_{i=0}^{n-1} u_i X^i$. Montrer que

$$P_{\sigma(U)} = X.P_U \bmod (X^n - 1) .$$

*Remarque: Comme $X^n - 1$ est un polynôme de degré n, $V^n \equiv V[X]/(X^n - 1)$ (l'anneau des restes dans la division euclidienne modulo $X^n - 1$). Ainsi, cette question montre que $P_{\sigma(U)} = X.P_U$ dans l'anneau $V[X]/(X^n - 1)$.*

5. Dans toute la suite, $g$ désigne le polynôme $g(X) = P_m = \sum_{i=0}^{n-k} a_i X^i$, appelé *polynôme générateur* de $C$.
Soit $x \in C$; montrer que $P_x$ est multiple de $g$ modulo $(X^n - 1)$.
Autrement dit, $P_x \bmod g = 0$ dans l'anneau $V[X]/(X^n - 1)$.

6. Montrer que $g$ est un diviseur de $X^n - 1$.

7. Montrer que l'opération de codage se ramène à un produit de polynômes modulo $X^n - 1$ que l'on explicitera.
*Remarque: Le codage est donc une multiplication de polynômes qui se ramène à une FFT, soit de coût $O(n \log n)$.*

8. Montrer que $x \in C$ si et seulement si $P_x$ est multiple de $g$. En déduire que la détection d'erreur se ramène à une division polynomiale que l'on explicitera.
*Remarque: La détection d'erreurs est donc une division de polynômes, qui se ramène aussi à une multiplication de polynômes de coût $O(n \log n)$. L'algorithme de Berlekamp-Massey permet de réaliser la correction pour un code cyclique avec un coût similaire.*

9. En résumé, on a montré que tout code cyclique est caractérisé par la donnée d'un polynôme générateur qui est un diviseur unitaire de degré $r = n - k$ de $X^n - 1$.
Le code $C$ est donc caractérisé par la donnée de seulement $r = n - k$ coefficients : $g_0, \ldots, g_{n-k-1}$.
Justifier que réciproquement, la donnée d'un polynôme $g$ diviseur unitaire de degré $n-k$ de $X^n - 1$ définit un unique code cyclique $(n, k)$.

# 2 Application: codes de Reed-Solomon

Soit $\alpha$ un élément primitif du corps $V = \mathbb{F}_q$.
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.

1. Montrer qu'un code de Reed-Solomon est de distance maximale parmi les codes linéaires sur $V$.

2. Le satellite d'exploration de Jupiter *Galileo* utilise le code de Reed-Solomon sur $V = \mathbb{F}_{256}$ de polynôme générateur

$$g = \prod_{j=12}^{43} (X - \alpha^{11j})$$

où $\alpha$ est un élément primitif de $\mathbb{F}_{2^8}$. Quels sont les caractéristiques de ce code sur $\mathbb{F}_{2^8}$ ? Quelle est sa distance ? Combien d'erreurs sur $V$ peut-il corriger ? Quel est son rendement et son taux de correction sur $V$ ?

3. Un code de Reed-Solomon sur $V = \mathbb{F}_{2^m}$ avec $r$ chiffres de redondance peut être vu comme un code binaire $C$ sur $\{0, 1\}$.
Donner les caractéristiques de ce code binaire $C$ : longueur, nombre de bits de redondance, distance.

4. Quel est le nombre maximal de bits consécutifs erronés (on parle de *paquet d'erreurs*) que le code binaire $C$ garantit pouvoir corriger ?

5. *Application 1: Code Galileo pour comunications spatiales.* Donner les caractéristiques du code Galileo en tant que code binaire, son rendement et son taux de correction. Quelle taille de paquet d'erreurs permet-il de corriger ?

6. *Application 2 : Construction d'un code de Reed-Solomon de taux de correction arbitraire.*
On communique sur un réseau qui transmet des bits avec un taux d'erreur de 1%.
Pour y remédier, lorsqu'on envoie $n$ octets, on veut détecter et corriger $0.01 \times n$ 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 son écriture;
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?