**Feuille TD 5 - Codes cycliques**

# 1 Caractérisation d'un code cyclique

1. *Le code est linéaire et* $x = [x_1, \ldots, x_n] \in C \Longleftrightarrow \sum_{i=1}^{n} x_i \Longleftrightarrow [x_n, x_1, \ldots, x_{n-1}] \in C$.

2. *On a* $\sigma^n = Id$ *d'où* $\sigma^{-1} = \sigma^{n-1}$. *Soit* $x \in C$; *comme* $\sigma$ *est stable dans* $C$, $\sigma^{-1}(x) = \sigma^{n-1}(x) \in C$.

3. *Soit* $u = [0, \ldots, 0, 1, u_1, \ldots, u_r]$ *la dernière ligne de la matrice génératrice normalisée* $G_1$ *de* $C$. *Comme* $C$ *est cyclique, d'après la question précédente,* $v = \sigma^{-k+1}(u) = [1, u_1, \ldots, u_r, 0, \ldots, 0] \in C$.
*Montrons que* $u_r \neq 0$. *Comme* $C$ *est cyclique,* $\sigma^i(v) \in C$ *pour* $i = 0, \ldots, k-1$. *Ces* $k$ *vecteurs étant indépendants, il forment une matrice génératrice* $G_2$ *du code* $C$. *Par l'absurde, supposons* $u_r = 0$; *alors la dernière colonne de* $G_2$ *est nulle: donc tous les mots de* $C$ *ont leur dernière composante nulle: ce qui est absurde puisque, comme* $C$ *est cyclique,* $\sigma^{-1}(v) \in C$ *et a sa dernière composante égale à 1. On en déduit que* $u_r \neq 0$.
*Soit alors* $m = \frac{1}{u_r}.v$ *qui appartient à* $C$ *car* $C$ *est linéaire;* $m$ *est de la forme* $m = [a_0, a_1, \ldots, a_{n-k} = 1, 0, \ldots, 0]$.
*Comme* $C$ *est cyclique,* $\sigma^i(m) \in C$ *pour* $i = 0, \ldots, k-1$. *Ces* $k$ *vecteurs étant indépendants, il forment une matrice génératrice* $G_C$ *du code* $C$ *de la forme demandée, qed.*

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

5. $x$ *est une combinaison linéaire des lignes* $\sigma^i(m)$ *de* $G_C$; *donc* $P_x$ *est une combinaison linéaire des polynômes* $P_{\sigma^i(m)}$. *Or, d'après la question précédente,* $P_{\sigma^i(m)} = X^i.P_m$ *dans l'anneau* $V[X]/(X^n - 1)$. *Donc, dans l'anneau* $V[X]/(X^n - 1)$, $P_x$ *est une combinaison linéaire des polynômes* $X^i P_m$, *tous multiples de* $P_m = g$. *Donc* $P_x$ *est multiple de* $g$.

6. $P_{\sigma^k(m)} = X^k.g \ mod\ X^n - 1$. *Comme* $C$ *est cyclique et* $m \in C$, $\sigma^k(m)$ *appartient à* $C$; *donc* $P_{\sigma^k(m)}$ *est combinaison linéaire des* $P_{\sigma^i(m)} = X^i.g$ *pour* $i = 0, \ldots, k-1$.
*Ainsi, il existe* $(\alpha_0, \ldots, \alpha_{k-1})$ : $X^k.g = \sum_{i=0}^{k-1} \alpha_i.X^i.g \ mod\ X^n - 1$. *Soit* $(X^k - \sum_{i=0}^{k-1} \alpha_i.X^i).g = 0 \ mod\ X^n - 1$, .
*Comme* $(X^k - \sum_{i=0}^{k-1} \alpha_i.X^i)$ *est unitaire de degré* $k$, $g$ *est unitaire de degré* $n-k$ *et* $X^n - 1$ *est unitaire de degré* $n$, *on en déduit que* $(X^k - \sum_{i=0}^{k-1} \alpha_i.X^i).g = (X^n - 1)$. *Donc* $g$ *est un diviseur de* $X^n - 1$.

7. *Soit* $u = [u_0, \ldots, u_{k-1}] \in V^k$ *un mot source et* $P_u = \sum_{i=0}^{k-1} u_i X^i$ *son polynôme associé. Le mot de code associé à* $u$ *est* $\phi(u) = u.G_C$ *de polynôme associé* $P_{u.G_C}$. *De part l'écriture de* $G_C$ *à partir des coefficients de* $g(X)$, *on a :*

$$\begin{aligned} P_{u.G_C} &= \sum_{i=0}^{k-1} u_i (X^i g(X) \ mod\ X^n - 1) \\ &= [g(X)(\sum_{i=0}^{k-1} u_i X^i)] \ mod\ X^n - 1 \\ &= [g(X).P_u(X)] \ mod\ X^n - 1\ . \end{aligned}$$

*Le codage correspond donc à un produit de polynômes par* $g$, *les degrés des monômes étant pris modulo* $n$ : *en effet, calculer* $X^n - 1$ *revient à considérer que* $X^n = 1 = X^0$.

8. *On a déja vu que tout mot de code est multiple de $g$ modulo $X^n - 1$. Or, comme $g$ est de degré $r = n - k$ et diviseur de $X^n - 1$, il y a exactement $|V|^k$ multiples de $g$ modulo $X^n - 1$, qui sont obtenus en multipliant $g$ par un polynôme de degré inférieur ou égal à $k-1$. Comme Card$(C) = |V|^k$, on en déduit que tout multiple correspond nécessairement à l'un des $|V|^k$ mots de code.*
*Détection d'erreurs: pour chaque mot $y$ reçu, on considère le polynôme $P_y$ associé. On calcule $P_y \mod g$ : si $= 0$, $y \in C$ et on ne détecte pas d'erreur. Sinon, on a détecté une erreur.*

9. *La donnée des $r = n - k$ coefficients de $g$ définit une matrice $G_C$ unique et donc un code linéaire unique. Or $g$ étant un diviseur de $X^n - 1$, $C$ est stable par $\sigma$ donc cyclique.*

# 2 Application: codes de Reed-Solomon

1. *La borne de Singleton montre que $\delta \leq n - k + 1 = r + 1$; ainsi, la distance $\delta = r + 1$ du code de Reed-Solomon atteint la borne de Singleton pour un code linéaire.*

2. *Le code est de longueur 256-1=255. $g$ est de degré $r = 43 - 12 + 1 = 32$; c'est donc un code (255,223, 33).*
*Distance = 255-223+1=33. Il est 16-correcteur.*
*Rendement* $= 223/255 \simeq 87\%$. *Taux de correction* $= 16/255 \simeq 6\%$.

3. *Chaque élément de $\mathbb{F}_{2^m}$ est codé sur $m$ bits. La distance est inchangée. Le code binaire $C$ est un code $(2^m - m, (2^m - 1 - r).m, r + 1)$.*

4. *Le code de Reed-Solomon peut corriger au maximum jusqu'à $t = \left\lfloor \frac{r-1}{2} \right\rfloor$ chiffres de $m$ bits consécutifs, donc tout paquet qui ne perturbe pas plus de $t$ chiffres de $V$ consécutifs (chacun comportant $m$ bits). Donc $C$ corrige tout paquet de longueur inférieure ou égale à à $\left(\left\lfloor \frac{r-1}{2} \right\rfloor - 1\right).m + 1$.*

5. *On a $m = 8$ et $r = 32$. En temps que code binaire, c'est un code* $(8\times255 = 2040, 8\times223 = 1784, 33)$.
*Le rendement=223/255=87% est inchangé.*
*Mais le taux de correction de bits n'est plus que de 16/2040* $\simeq 0.78\%$.
*Le code permet de corriger tout paquet d'erreurs de longueur inférieure à 121 bits.*

6.