TD 11 : Algorithme de Guruswami et Sudan

On s'intéresse dans ce TD à l'algorithme de V. Guruswami et M. Sudan pour le décodage en liste des codes de Reed-Solomon, qui permet de corriger une fraction $1 - \sqrt{R}$ d'erreurs, où R est le ratio du code. Cet algorithme suit le même schéma général que l'algorithme de décodage en liste vu en cours qui peut corriger une fraction $1 - \sqrt{2R}$ d'erreurs. Dans toute la suite, $\mathbb{K}$ désigne un corps fini.

Définition Soit $Q(X,Y) = \sum_{k=0}^{d} \sum_{\ell=0}^{d_k} c_{k,\ell} X^k Y^\ell \in \mathbb{K}[X,Y]$. Sa *dérivée de Hasse* d'ordre (i,j) est

$$Q^{[i,j]}(X,Y) = \sum_{k=i}^{d} \sum_{\ell=j}^{d_k} \binom{k}{i} \binom{\ell}{j} c_{k,\ell} X^{k-i} Y^{\ell-j}.$$

Un couple $(\alpha,\beta) \in \mathbb{K}^2$ est une *racine de multiplicité* r si $Q^{[i,j]}(\alpha,\beta) = 0$ pour tout (i,j) tel que $i + j < r$.

1. **(a)** Soit $Q \in \mathbb{K}[X,Y]$ et $(\alpha,\beta) \in \mathbb{K}^2$. Notons $Q(X+\alpha, Y+\beta) = \sum_{i,j} b_{i,j} X^i Y^j$. Montrer que pour tout i, j, $b_{i,j} = Q^{[i,j]}(\alpha,\beta)$.
   (b) En déduire que si (α,β) est une racine de multiplicité r de Q et si $P \in \mathbb{K}[X]$ vérifie $P(\alpha) = \beta$, alors α est une racine de multiplicité r de $Q(X, P(X))$ (au sens usuel, *i.e.* $(X-\alpha)^r$ divise $Q(X,P(X))$).
2. Soit D, t et r des entiers tels que $t > D/r$. Supposons que $Q \in \mathbb{K}[X,Y]$ est de $(1,k-1)$-degré[1] D, et $(\alpha_1,y_1), \ldots, (\alpha_t,y_t)$ des racines de multiplicité r de Q. Soit $P \in \mathbb{K}[X]$ de degré $< k$ tel que $P(\alpha_i) = y_i$ pour $1 \leq i \leq t$. Montrer que $Y - P(X)$ divise Q.
3. Soit $(\alpha_1,y_1), \ldots, (\alpha_n,y_n) \in \mathbb{K}^2$. Montrer que si D vérifie l'inégalité

$$\frac{D(D+2)}{2(k-1)} > n\binom{r+1}{2},$$

   alors il existe un polynôme $Q \in \mathbb{K}[X,Y]$ de $(1,k-1)$-degré au plus D tel que chaque couple (α_i,y_i) soit une racine de multiplicité r de Q. *Indication. Penser à l'algèbre linéaire.*
4. **(a)** Montrer que l'inégalité de la question 3. est satisfaite si $D = \left\lfloor \sqrt{(k-1)nr(r+1)} \right\rfloor$.
   (b) On pose $r = 2(k-1)n$. Montrer que si t est un entier strictement supérieur à $\sqrt{(k-1)n}$, alors $t > D/r$. *Indication. On admettra*[2] *l'inégalité* $1 + \lfloor\sqrt{m}\rfloor > \sqrt{m+1/2}$ *valable pour tout* $m \in \mathbb{N}$.
5. Déduire des questions précédentes qu'il existe un algorithme polynomial de décodage en liste pour les codes de Reed-Solomon de paramètres k et n, capable de corriger $\lceil n - \sqrt{(k-1)n} - 1 \rceil$ erreurs.

1. Rappel : le $(1,k-1)$-degré de X^iY^j est $i + (k-1)j$.
2. Il est autorisé de la démontrer !