Université Bordeaux 1 — **Algèbre et calcul formel – Master**
Mathématiques — Année 2012–2013

FEUILLE D'EXERCICES n° 6

Exercice 1 – (FFT itérative) – Nous considérons ici des polynômes de $A[X]$ où A est un anneau commutatif unitaire. Soit n une puissance de 2 différente de 1 : $n = 2^k$ avec $k > 0$. Soit $\omega \in A$ une racine primitive n-ième de l'unité (on a $\omega^n = 1$ et $\omega^d - 1$ n'est diviseur de zéro pour aucun $1 \leqslant d < n$). On admettra que l'anneau considéré possède une telle racine. On appelle *transformée de Fourier discrète* d'un polynôme $R \in A[X]$ de degré $< n$, identifié au n-uplet $(R_0, \ldots, R_{n-1})$ le n-uplet

$$DFT_\omega(R) = (R(1), R(\omega), \ldots, R(\omega^{n-1})).$$

On pose $m = n/2 = 2^{k-1}$. Alors, pour $0 \leqslant p < m$, on a

$$R(\omega^p) = \sum_{j=0}^{m-1} R_{2j}\omega^{2jp} + \omega^p \sum_{j=0}^{m-1} R_{2j+1}\omega^{2jp}$$

et

$$R(\omega^{p+m}) = \sum_{j=0}^{m-1} R_{2j}\omega^{2jp} - \omega^p \sum_{j=0}^{m-1} R_{2j+1}\omega^{2jp}.$$

Les formules précédentes permettent de ramener le calcul d'une DFT de degré $< n$ à deux DFT de degrés $< m$. En cours, vous avez vu un algorithme récursif qui utilise ce fait.

1) Soit $A = \mathbb{F}_{29}$. Trouver une racine primitive quatrième de l'unité ω dans $\mathbb{F}_{29}$. Soit $P = x^3 + x - 1$ dans $\mathbb{F}_{29}$. Exécuter l'algorithme pour calculer $DFT_\omega(P)$.

2) Écrire l'arbre de récursivité de l'algorithme pour $n = 8$ et

$$P = \sum_{i=0}^{7} a_i x^i.$$

Vérifier que si $b_0, \ldots, b_7$ est la liste des coefficients obtenus, alors pour tout i dans $\{0, \ldots, 7\}$, $b_i = a_{M(3,i)}$, où M est l'application "miroir" définie comme suit : si $t = \sum_{i=0}^{k-1} t_i 2^i$, où les t_i appartiennent à $\{0, 1\}$, alors

$$M(k, t) = \sum_{i=0}^{k-1} t_{k-i-1} 2^i$$

(on inverse l'écriture binaire de t). Ainsi, $M(k, t)$ n'est défini que si t appartient à $\{0, \ldots, 2^k - 1\}$.

3) Montrer que si $n = 2^k$, la suite des coefficients obtenus $b_0, \ldots, b_{n-1}$ par récursivité sont tels que pour tout i,

$$b_i = a_{M(k,i)}.$$

4) Soit P un polynôme de degré strictement inférieur à n. Montrer qu'on peut écrire P de façon unique

$$P = P_0(x^2) + xP_1(x^2).$$

Soit T le tableau indicé de 0 à $n-1$ tel que si $0 \leqslant i \leqslant n/2-1$, alors $T[i] = P_0(\omega^{2i})$ et $T[i+m] = P_1(\omega^{2i})$. Comment obtient-on la transformée de Fourier discrète de P à partir de T ?

5) En déduire un algorithme itératif de transformée de Fourier rapide.

Exercice 2 – (FFT sur un exemple)

1) Montrer que 2 est une racine primitive 8ème de l'unité dans $\mathbb{F}_{17}$.

2) Soit dans $\mathbb{F}_{17}[x]$ le polynôme.

$$P(x) = \sum_{i=0}^{7} ix^i.$$

Exécuter l'algorithme récursif de la FFT vu en cours sur P, avec $n = 8$ et en prenant 2 comme racine de l'unité.

Exercice 3 – (Fast negative wrapped convolution) – On se propose ici de décrire une variante que l'on peut mettre en œuvre lorsque A n'admet pas nécessairement de racine primitive n-ième de l'unité. On supposera que 2 est une unité de A et si d est une puissance de 2 on posera

$$D_d = A[X]/\langle X^d + 1\rangle,$$

et

$$\omega_d = X \mod (X^d + 1) \in D_d.$$

1) Montrer que ω_d est une racine primitive $2d$-ième de l'unité de D_d.

2) Soient P et Q deux polynômes de degrés $< n = 2^k$ où $k \geqslant 1$, vérifiant en outre $\deg(PQ) < n$. Posons

$$m = 2^{\lfloor \frac{k}{2} \rfloor} \text{ et } t = \frac{n}{m},$$

et partitionnons P et Q en t blocs de dimension m :

$$P = \sum_{j=0}^{t-1} P_j X^{mj} \quad \text{et} \quad Q = \sum_{j=0}^{t-1} Q_j X^{mj},$$

où les P_j et Q_j sont des polynômes de $A[X]$ de degré $< m$. Posons

$$P' = \sum_{j=0}^{t-1} P_j Y^j \in A[X,Y] \quad \text{et} \quad Q' = \sum_{j=0}^{t-1} Q_j Y^j \in A[X,Y].$$

3) Montrer que pour déterminer PQ il suffit de déterminer $P'Q'$ modulo $(Y^t + 1)$.

4) Se ramener à la détermination de $P"Q"$ modulo $(Y^t + 1)$ dans $D_{2m}[Y]$ où $P" = P' \mod (Y^t + 1)$ et $Q" = Q' \mod (Y^t + 1)$.

5) Observer qu'il y a dans D_{2m} des racines primitives $2t$-ièmes de l'unité et utiliser la FFT pour calculer PQ.