UPS – Centre d'Orsay
Mathématiques

MAO – Maîtrise
Année 2003–2004

Examen (la transformation de Fourier rapide)

Notes de cours et documents distribués au cours des séances sont autorisés

Toutes les questions peuvent être illustrées par des programmes et des exemples judicieux. Plus généralement, ne pas hésiter à conjecturer, commenter, comparer, bref élargir.

Soit $n > 1$ un entier, et K un corps commutatif contenant une racine primitive n-ième de l'unité ω, c'est-à-dire que ω est d'ordre exactement n dans $(K^*, \times)$. On pose par définition $\omega^0 = 1$.

1. Exemples

1) Proposer des exemples d'une telle situation pour différents corps K raisonnables.

2) En particulier, si $K = \mathbb{F}_q$ est un corps fini, pour quels n existe-t-il un tel ω ?

3) Trouver un tel ω pour $q = 100000000000000006363$ $(= 10^{20} + 6363)$ et $n = 101$.

4) Trouver un tel ω pour $q = 101^2$ et $n = 85$. [*Commencer par trouver une représentation concrète des éléments de* $\mathbb{F}_{101^2}$.]

2. Transformée de Fourier

On note $(a_i \colon 0 \leqslant i < n)$ pour $(a_0, \ldots, a_{n-1})$. Soit $(a_i \colon 0 \leqslant i < n) \in K^n$, que l'on considère comme donnant les coefficients du polynôme $f = \sum_{i=0}^{n-1} a_i X^i$ de $K[X]$. Par définition, la Transformée de Fourier de (a_i) relativement à ω est le vecteur

$$\mathrm{FT}((a_i), \omega) = \mathrm{FT}(f, \omega) = (b_j \colon 0 \leqslant j < n) \in K^n, \quad \text{où} \quad b_j = f(\omega^j).$$

1) Soit $k \in \mathbb{Z}$. Montrer que $\sum_{i=0}^{n-1} \omega^{ik} = 0$ si $n \nmid k$ et vaut n sinon.

2) Montrer que $\mathrm{FT}((b_j \colon 0 \leqslant j < n), \omega^{-1}) = (na_i \colon 0 \leqslant i < n)$.

3) Donner un algorithme simple pour calculer la transformée de Fourier de (a_i) en $O(n^2)$ opérations dans K (additions et multiplications).

3. « Fast Fourier Transform » (FFT)

On suppose dorénavant que $n = 2^k$, pour un entier $k \geqslant 1$.

1) Soit

$$f = \sum_{i=0}^{n-1} a_i X^i = f_{\text{pair}}(X^2) + X f_{\text{impair}}(X^2).$$

Expliciter f_{pair} et f_{impair}.

2) Soient

$$(u_i\colon 0 \leqslant i < n/2) = \mathrm{FT}(f_{\mathrm{pair}}, \omega^2),$$
$$(v_i\colon 0 \leqslant i < n/2) = \mathrm{FT}(f_{\mathrm{impair}}, \omega^2).$$

Par abus de language, u_j et v_j sont prolongés par périodicité modulo $n/2$. Montrer que $f(\omega^j) = u_j + \omega^j v_j$ pour tout $j \geqslant 0$.

3) En déduire un algorithme de calcul récursif de $\mathrm{FT}(f, \omega)$.

4) On note $y(k)$ le nombre d'opérations dans K utilisées par cet algorithme pour calculer la transformée de Fourier $\mathrm{FT}((a_i\colon 0 \leqslant i < n), \omega)$ d'un vecteur de longueur $n = 2^k$. Montrer que

$$y(k) = 2y(k-1) + O(2^k).$$

En déduire que $y(k) = O(k2^k) = O(n \log n)$.

4. Une application

Soient $f, g \in \mathbb{Z}[X]$ deux polynômes de degrés inférieurs à $n = 2^k$, de norme infinie inférieure à M.

1) Rappeler la complexité binaire du calcul naïf de $f \times g$.

2) Expliquer comment trouver un nombre premier $p > 2(n+1)M^2$, tel que $\mathbb{F}_p$ contienne une racine primitive $2n$-ième de l'unité ω.

3) Préciser et commenter l'algorithme suivant du calcul de $f \times g$:

- Calculer $(u_i) = \mathrm{FT}(f, \omega)$ et $(v_i) = \mathrm{FT}(g, \omega)$.
- $f \times g$ est un relèvement à $\mathbb{Z}[X]$ convenable de

$$\frac{1}{2n}\mathrm{FT}\big((u_i v_i\colon 0 \leqslant i < 2n), \omega^{-1}\big).$$

On pourra en particulier remarquer que les coefficients de $f \times g$ sont de valeur absolue inférieure à $(n+1)M^2$, et que $2n$ est nécessairement inversible modulo p sauf dans un cas trivial.

4) Discuter le choix du corps $\mathbb{F}_p$ pour exécuter l'algorithme abstrait de la FFT. Autres possibilités ? Imaginer une solution utilisant le Lemme Chinois.