École normale supérieure **2010-2011**
Département d'informatique

Algorithmique et Programmation
TD n° 8 : FFT

Exercice 1. Quand on veut calculer une convolution, on a besoin d'un calcul exact et non approché comme le donne la FFT. On va utiliser l'anneau $\mathbb{Z}/m\mathbb{Z}$ des entiers modulo m, où $m = \omega^{n/2} + 1$ si n et ω sont des puissances de 2, $n = 2^k$, $k \geq 1$. On remarque que si les composantes de la convolution sont plus grandes que $\omega^{n/2}$, le calcul sera réduit modulo m.

1. Montrer que pour tout $a \in \mathbb{Z}/m\mathbb{Z}$, $\sum_{i=0}^{n-1} a^i = \prod_{i=0}^{k-1}(1 + a^{2^i})$.
2. Montrer que pour tout $1 \leq p < n$, on a $\sum_{i=0}^{n-1} \omega^{ip} = 0 \bmod m$.
3. Montrer que n est inversible modulo m et que ω est une racine principale n-ième de l'unité.
4. Soit $m = \omega^p + 1$ pour un entier p et $a = \sum_{i=0}^{\ell-1} a_i \omega^{pi}$, où $0 \leq a_i < \omega^p$ pour chaque i. Alors, $a = \sum_{i=0}^{\ell-1} a_i(-1)^i \bmod m$. En déduire le coût de la réduction modulaire quand ℓ est une constante.
5. Montrer que la FFT d'un vecteur de taille n et son inverse, et la convolution de deux vecteurs de taille n est exacte si les composantes de la convolution sont dans l'ensemble $\omega^{n/2}$, et que ces calculs demandent $O(n^2 \log n \log \omega)$ opérations binaires.

Exercice 2. Le but de l'exercice est d'étudier des stratégies de calcul d'une transformée de Fourier dont la taille n'est pas nécessairement une puissance de deux. Soit N un entier positif. On note $\omega = e^{-2i\pi/N}$. La transformée de Fourier prend en entrée un vecteur $x_0, \ldots, x_{N-1}$ et calcule un vecteur $\hat{x}_0, \ldots, \hat{x}_{N-1}$ par la formule :

$$\hat{x}_k = \sum_{n=0}^{N-1} x_n \omega^{nk}$$

1. Rappelez le nombre de multiplications complexes quand N est une puissance de 2. (On pourra supposer les coefficients ω^{nk} précalculés.)
2. Expliquer pourquoi la FFT en prenant une puissance de deux supérieure ne calculent pas le bon résultat. En fait, ce n'est pas forcément grave pour calculer une convolution ou un produit de polynômes car on calcule l'évaluation et sa réciproque. Cependant, il existe un algorithme en $O(N \log^2 N)$ pour évaluer un polynôme en N points arbitraires.
3. A combien de multiplications l'application naïve de la formule ci-dessus conduit-elle ?
4. Montrer qu'on peut en fait calculer une FFT de taille 2 sans aucune multiplication et une FFT de taille 4 avec une seule multiplication. On ignorera les multiplications par 1 ou -1 mais on comptera les multiplications par i. Proposer un calcul d'une FFT de taille 3 avec un nombre minimal de multiplications. On admettra qu'il existe une FFT de taille 5 avec 5 multiplications.
5. On considère maintenant le cas où la taille est un nombre premier impair p. On note que $\hat{x}_0$ est une simple sommation et on s'intéresse aux autres coefficients. Soit g un générateur du groupe multiplicatif cyclique des entiers $\{1, \ldots, p-1\}$, modulo p. On peut donc remplacer les indices $n > 0$ et $k > 0$ par des variables $g^u \bmod p$ et $g^v \bmod p$, avec $u = 0, \ldots, p-2$ et $v = 0, \ldots, p-2$. On obtient :

$$\bar{x}_{g^v} = x_0 + \sum_{u=0}^{p-2} x_{g^u} \omega^{g^{u+v}}$$

   (a) Interpréter la sommation de la formule ci-dessus comme une convolution cyclique. Expliciter complètement ces deux vecteurs dans le cas particulier où $p = 17$ et $g = 3$.

   (b) En déduire une stratégie de calcul d'une FFT de taille p basée sur une FFT de taille $p - 1$.

(c) Évaluer le nombre de multiplications pour un nombre premier p de la forme $2^\ell + 1$. On ne tiendra pas compte du calcul des constantes qui sont des puissances de ω. La stratégie est-elle appropriée pour $p = 5$, $p = 17$?

6. On considère maintenant le cas où la taille est une puissance d'un nombre premier impair p, soit $N = p^e$. On note G le groupe multiplicatif cyclique des entiers modulo N et on pose $\omega = e^{-2i\pi/N}$. Chaque coefficient de Fourier

$$\hat{x}_k = \sum_{n=0}^{N-1} x_n \omega^{nk}$$

peut être considéré comme la somme de deux termes :

$$\bar{x}_k = \sum_{n \in G} x_n \omega^{nk} \text{ et } \tilde{x}_k = \sum_{n \notin G} x_n \omega^{nk}.$$

(a) En généralisant la méthode de la première question, donner une stratégie pour calculer les coefficients de Fourier partiels $\bar{x}_k$ dont l'indice k n'est pas divisible par p.

(b) Montrer que les coefficients $\hat{x}_k$ d'indice multiple de p sont calculés par une transformée de Fourier de taille p^{e-1}. On pourra utiliser un changement de variable $n = p^{e-1}n_1 + n_2$, $n_1 = 0, \ldots, p-1$, $n_2 = 0, \ldots, p^{e-1} - 1$.

(c) Montrer que les coefficients de Fourier partiels $\tilde{x}_k$, pour $k \in G$ sont aussi calculés par une transformée de Fourier de taille p^{e-1}.

7. On s'intéresse maintenant au cas d'une transformée de Fourier de taille N, où N est le produit N_1N_2 de deux entiers premiers entre eux. On pose $\omega = e^{-2i\pi/N}$, $\omega_1 = e^{-2i\pi/N_1}$ et $\omega_2 = e^{-2i\pi/N_2}$. On note $t_1 = (N_1)^{-1} \bmod N_2$ et $t_2 = (N_2)^{-1} \bmod N_1$.

(a) Montrer que les deux applications respectivement définies pour $n_1 = 0, \ldots, N_1 - 1$ et $n_2 = 0, \ldots, N_2 - 1$ par :

$$\begin{aligned} (n_1, n_2) &\rightarrow n_2N_1 + n_1N_2 \bmod N \\ (n_1, n_2) &\rightarrow n_2N_1t_1 + n_1N_2t_2 \bmod N \end{aligned}$$

sont des bijections sur $\{0, \ldots, N-1\}$.

(b) Par des changements de variables sur n et k, vérifier que le calcul de $\hat{x}_k$,

$$\hat{x}_k = \sum_{n=0}^{N-1} x_n \omega^{nk}$$

se ramène à celui du tableau d'entiers indicés par (k_1, k_2), où on considère k_1 comme un indice "ligne" et k_2 comme un indice "colonne" :

$$\sum_{n_1=0}^{N_1-1} \sum_{n_2=0}^{N_2-1} x_{n_2N_1+n_1N_2} \omega_1^{n_1k_1} \omega_2^{n_2k_2}.$$

Montrer que le tableau $\hat{T}$ ainsi défini peut être calculé par un programme qui prend en entrée le tableau T de taille $N_1 \times N_2$, dont l'élément d'indice "ligne" n_1 et d'indice "colonne" n_2 est $x_{n_2N_1+n_1N_2}$. Montrer que ce programme fait :
- N_1 appels à un programme de calcul d'une FFT de taille N_2
- N_2 appels à un programme de calcul d'une FFT de taille N_1

On explicitera la stratégie du programme en termes des lignes et des colonnes des tableaux T et $\hat{T}$ manipulés.

8. Outre les résultats sur la FFT de taille une puissance de 2 et ceux de la question 2, on admettra qu'il existe une FFT de taille 7 avec 8 multiplications et une FFT de taille 9 avec 10 multiplications (en ignorant comme plus haut les multiplications triviales). En utilisant les stratégies proposées dans les questions précédentes, proposer des algorithmes de calcul de FFT pour les tailles $N = 85$, $N = 153$, $N = 289$ et évaluer le nombre de multiplications que la méthode nécessite. Comparer à l'algorithme naïf.