

TD 4 : Produit médian et inversion

Soit F et G deux polynômes, de tailles respectives n et $2n - 1$, et $H = \sum_{i=0}^{3n-3} h_i X^i$ leur produit. Le *produit médian* de F et G est le polynôme $M(F, G) = \sum_{i=0}^{n-1} h_{i+n-1} X^i$, de taille n . Il peut servir de brique de base dans le calcul d'inverse d'une série formelle.

Toutes les complexités sont exprimées en **nombre de multiplications** dans l'anneau des coefficients.

1.
 - i. Donner un algorithme naïf de calcul du produit médian, et comparer sa complexité à celle du produit (naïf) de deux polynômes de taille n .
 - ii. Montrer que si l'on dispose d'un algorithme de complexité $M(n)$ pour multiplier deux polynômes de taille n , on peut calculer un produit médian en complexité $2M(n)$.

On souhaite utiliser le produit médian dans l'algorithme d'inversion de série formelle. Dans toute la suite, n est supposé être une puissance de 2.

2.
 - i. Écrire une version itérative de l'algorithme d'inversion de série formelle, en faisant appel au produit médian.
 - ii. On suppose que le produit médian de deux polynômes de tailles n et $2n - 1$ peut s'effectuer avec la même complexité $M(n)$ que le produit de deux polynômes de taille n . Exprimer la complexité obtenue, en fonction de $M(n/2^k)$ pour diverses valeurs de k .
 - iii. On note $K(n)$ la complexité de l'algorithme de Karatsuba. Montrer que l'inversion de série en précision n peut s'effectuer en temps précisément $K(n)$ (sans $O(\cdot)$!).
 - iv. On note $F(n)$ la complexité de l'algorithme de multiplication par FFT. Montrer que l'inversion de série en précision n peut s'effectuer en temps $2F(n)$.

On cherche maintenant à montrer qu'on peut calculer un produit médian de tailles n et $2n - 1$ en temps $M(n)$, plutôt que $2M(n)$, où $M(n)$ est la complexité du produit standard. On le fait dans les cas particuliers de l'algorithme de Karatsuba et de la transformée de Fourier rapide.

3. On cherche à adapter l'algorithme de Karatsuba au cas du produit médian.
 - i. Soit $F = f_0 + f_1 X$ et $G = g_0 + g_1 X + g_2 X^2$. Donner l'expression de $M(F, G)$.
 - ii. Donner un algorithme effectuant 3 multiplications pour calculer $M(F, G)$. Indication : une des multiplications est $(f_1 - f_0)g_1$.
 - iii. En déduire un algorithme de type « diviser pour régner » pour le produit médian, dans le cas où n est une puissance de 2.
 - iv. Comparer la complexité obtenue avec celle de l'algorithme de Karatsuba pour deux polynômes de degré n .
4. On cherche maintenant à adapter l'algorithme de multiplication par FFT au cas du produit médian. On note ω une racine primitive $(2n - 1)$ ème de l'unité. On note $H = H_0 + X^{n-1} H_1 + X^{2n-1} H_2$, où H_0 et H_2 sont de taille $n - 1$ et H_1 est de taille n .
 - i. Calculer $H^* = H \bmod (X^{2n-1} - 1)$.
 - ii. Montrer que pour tout $i \geq 0$, $H(\omega^i) = H^*(\omega^i)$.
 - iii. En déduire qu'on peut calculer H^* à l'aide de trois calculs de FFT. En déduire un algorithme pour le produit médian.
 - iv. Comparer la complexité obtenue avec celle de l'algorithme de multiplication par FFT de deux polynômes de taille n .

De manière générale, si on dispose d'un algorithme de calcul du produit standard de complexité $M(n)$, on peut en déduire un algorithme de même complexité pour le produit médian. Ce résultat est un cas particulier du « théorème de transposition » en calcul formel, qui dépasse du cadre de ce cours.