

## TD 4

**Exercice 1.***Décalage de polynôme*

On souhaite calculer, étant donné un polynôme  $P$  de taille<sup>1</sup>  $n$  et un point  $a$ , le polynôme  $P(X + a)$ .

1. Montrer qu'on peut calculer l'évaluation  $P(a)$  en  $(n - 1)$  multiplications dans l'anneau des coefficients.
2. En déduire un algorithme effectuant  $n(n - 1)/2$  multiplications pour le calcul de  $P(X + a)$ .
3. Décrire un algorithme de type « diviser pour régner » pour le calcul de  $P(X + a)$  lorsque la taille est une puissance de 2, de complexité  $O(M(n) \log n)$  où  $M(n)$  est la complexité de la multiplication de deux polynômes de taille  $n$ . *Indications. Découper  $P$  en deux polynômes de taille moitié et pré-calculer les  $(X + a)^{2^k}$ .*

**Exercice 2.***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  $n$ .

Toutes les complexités dans cet exercice sont comptées en nombre de multiplications dans l'anneau des coefficients.

1. Donner un algorithme naïf de calcul du produit médian, et comparer sa complexité à celle du produit (naïf) de deux polynômes de taille  $n$ .
2. 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  $2M(n)$ .
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  $\omega$  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  $n$ .
5. On souhaite utiliser le produit médian dans l'algorithme d'inversion de série. On suppose que le produit médian de polynômes de tailles  $n$  et  $2n - 1$  peut s'effectuer avec la même complexité  $M(n)$  que le produit de deux polynômes de taille  $n$ . On s'intéresse au cas où  $n$  est une puissance de 2.
  - i. Quel produit de l'algorithme peut être remplacé par un produit médian ?
  - ii. 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  $K(n)$  (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  $2F(n)$ .

1. Rappel : un polynôme est de taille  $n$  s'il est de degré  $< n$ .