UFR Sciences
M2 Calcul Formel

Martin WEIMANN

TP 7 : Polynômes univariés

Exercice 1 (Evaluation de Hörner) Soit $P \in K[X]$ et $a \in K$.

1. Ecrire une procédure qui calcule $P(a)$ selon la métode de Hörner. Comparer les temps avec l'évaluation naïve sur des polynômes de tailles significatives.
2. Modifier votre algorithme pour qu'il retourne aussi la quotient $Q = P \mod (X - a)$.
3. En déduire un algorithme qui calcule le développement de Taylor de P au point a.

Exercice 2 (Evaluation multipoints) Programmer un algorithme d'évaluation multipoints : étant donnés $P \in K[x]$ de degré $< n$ et $a_1, \ldots, a_n$, on retournera la liste des $P(a_i)$. On supposera que n est une puissance de 2 et on s'appuiera sur une procédure intermédiaire qui pré-calcule l'arbre des sous-produits. Tester votre procédure sur quelques exemples.

Exercice 3 (Interpolation rapide) Soit $A = [a_1, \ldots, a_n]$ et $B = [b_1, \ldots, b_n]$ des listes d'éléments d'un corps K avec n une puissance de 2 et les a_i deux à deux distincts.

1. Ecrire une procédure qui calcule le polynôme d'interpolation aux noeuds (a_i, b_i) selon la formule d'interpolation de Lagrange.
2. Ecrire une procédure qui calcule le polynôme d'interpolation aux noeuds (a_i, b_i) selon la méthode diviser pour régner.
3. Comparer les temps de vos procédures. Comparer également avec la procédure d'interpolation de Sage (on pourra regarder `R.lagrange_polynomial(Noeuds)` où R désigne l'anneau $K[X]$). Faire un graphique permettant de visualiser les exposants de complexité des différentes approches.

Exercice 4 (Multiplication rapide par FFT)

1. Programmer un algorithme de multiplication rapide par FFT (Fast Fourier Transform).
2. Soit $p = 29.2^{57} + 1$. Si $n \leq 2^{57}$ est une puissance de 2, comment produire facilement une racine n-ème de l'unité dans $\mathbb{F}_p$ à partir d'un élément primitif a de $\mathbb{F}_p$?
3. Tester votre procédure FFT dans $\mathbb{F}_p[X]$ en vous aidant de la question 2. Jusqu'à quel degré peut-on utiliser la multiplication rapide dans cet anneau ?

Exercice 5 (Localisation de racines par l'algorithme de Sturm) On testera les procédures sur un polynôme P aléatoire de $\mathbb{R}[X]$ de degré 10 (Sage utilise par défaut la loi gaussienne centrée réduite).

1. Ecrire une procédure qui calcule la suite de Sturm d'un polynôme $P \in \mathbb{R}[X]$.
2. En déduire une procédure qui calcule le nombre de racines réelles de P dans un intervalle donné $]a, b]$. Quel choix de a et b assure de trouver toutes les racines réelles de P ? Tester.
3. Ecrire une procédure dichotomique qui retourne les racines réelles de P calculées à précision e (en supposant que cette précision suffit à isoler les racines). Tester. Combien de temps pour $e = 10^{-11}$?
4. Ecrire une procédure qui calcule les racines réelles de P à précision donnée 10^{-11}, en utilisant cette fois l'itération de Newton en relais dès lors que toutes les racines sont isolées par l'algorithme de la question 3. Comparer les temps des deux approches.