Factorisation des polynômes

Préparation agrégation 2006, option C

Révision : 4/05/07

Ce texte discute plusieurs méthodes de localisation de racines réelles ou/et complexes d'un polynôme $P(X)$ de degré n.

Ce texte est très largement inspiré d'idées de M. Eisermann

1 Introduction

Si P est à coefficients entiers (ou rationnels, ou entiers de Gauss), on peut toujours se ramener au cas où P n'a pas de racines multiples (par calcul de PGCD, c'est la factorisation "square-free"), on peut aussi décider d'appliquer un algorithme de factorisation exact (par exemple Berlekamp, Cantor-Zassenhaus) pour si possible diminuer le degré du polynôme dont on cherche à localiser les racines.

On supposera dans tout ce qui suit que l'on cherche à localiser les racines d'un polynôme dont toutes les racines sont simples.

On présente ici principalement deux méthodes :

- la méthode de Newton et des améliorations pour éviter le problème de la recherche de la valeur initiale de la suite itérative
- la généralisation des suites de Sturm aux racines complexes

2 La méthode de Newton.

La méthode de Newton est une méthode fréquemment implémentée par les logiciels de calcul scientifique et formel. Dans sa forme la plus simple, on cherche une racine r de P, on élimine la racine trouvée en prenant le quotient Q de P par $X - r$, on recommence alors avec Q. Cette méthode présente plusieurs inconvénients :

- si le point de départ de la recherche est éloigné d'une racine, la méthode de Newton n'a pas de raison de converger (en tous cas en un nombre raisonnable d'itérations)
- les erreurs d'arrondis se cumulent à chaque élimination de racine

On peut remédier au premier inconvénient par exemple par des algorithmes d'algèbre linéaire. Ainsi en appliquant quelques itérations de la méthode de la puissance à la matrice companion M du polynôme P

$$v_{n+1} = Mv_n, \quad v_0 \text{ aléatoire}$$

on peut obtenir une estimation de la plus grande racine complexe en module du polynôme (si P est á coefficients réels il peut être nécessaire de faire des itérations sur $M + \alpha i$, pour découpler une paire de racines complexes conjuguées), puis on affine en prenant cette estimation comme valeur initiale de la méthode de Newton. Pour atténuer le problème des erreurs d'arrondi à chaque élimintation de racine, on peut effecter quelques itérations de Newton supplémentaires sur les racines approchées de Q avec le polynôme initial P. On peut aussi utiliser la factorisation de Schur de la matrice companion pour avoir une estimation simultanée de toutes les racines

du polynôme (méthode utilisée par Xcas), on peut aussi utiliser la méthode d'Aberth, qui consiste à faire pour $k \in [1, n]$ une itération de Newton sur l'estimation z_k d'une des racines en prenant comme fonction :

$$\frac{P(x)}{\prod_{1 \leq j \leq n, j \neq k}(x - z_j)}$$

Lorsqu'on a trouvé une racine approchée z d'un polynôme P de degré n, on peut en déduire que le disque du plan complexe de centre z et de rayon $n|P(z)/P'(z)|$ contient au moins une racine, en effet :

$$\frac{P'}{P} = \sum_{k=1}^{n} \frac{1}{z - z_j}$$

si toutes les racines z_j sont en-dehors du disque, on peut minorer $|z - z_j|$ et donc majorer $|P'(z)/P(z)|$. Pour certifier l'existence d'une racine dans un disque, on prendra une racine approchée $z \in \mathbb{Q}[i]$ pour calculer le rayon exact du disque.

3 Par homotopie

On présente dans cette section une autre méthode qui détermine simultanément les racines de P. L'idée est de construire un chemin de polynômes reliant un polynôme dont les racines sont connues au polynôme P, en suivant les racines le long du chemin. Soit donc :

$$P_t = tP + (1 - t)(x^n - 1), \quad P_0 = x^n - 1,\ P_1 = P$$

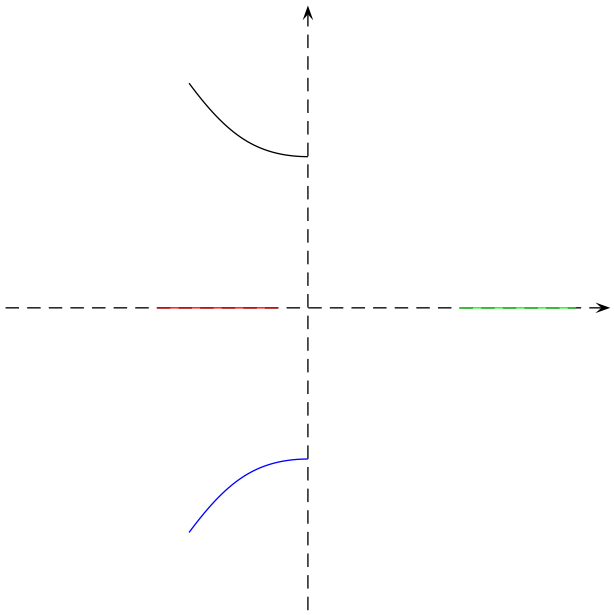
Pour passer de $t = 0$ à $t = 1$, il faut trouver un chemin dans le plan complexe tel que les racines de P_t restent simples, afin de pouvoir suivre les racines mais aussi pour pouvoir appliquer la méthode de Newton : pour trouver les racines de $P_{t+\Delta t}$ ($\Delta t << 1$) on appliquera quelques itérations de la méthode de Newton en prenant les racines de P_t comme valeurs initiales. De proche en proche, on arrivera à calculer simultanément toutes les racines de P.

Soit R le résultant de P_t et de sa dérivée. Comme le but de l'algorithme est de calculer les valeurs approchés de racines d'un polynome, on ne peut pas utiliser un algorithme de recherche de racines approchées de R pour savoir quel chemin utiliser pour relier $t = 0$ et $t = 1$. Mais R est un polynôme à coefficients entiers, on peut donc calculer sa suite de Sturm et localiser les racines réelles de R. Si R n'a pas de racine réelles dans $[0, 1]$, alors on peut rester dans l'intervalle $[0, 1]$. Dans le cas contraire (par exemple si $R(t = 0)$ et $R(t = 1)$ ne sont pas de même signe), il faut passer dans le complexe. On peut par exemple utiliser une ligne polygonale $[0, 1/2(1 + i * k)] \cup [1/2(1 + i * k), 1]$, il existe forcément un k entier tel que la ligne polygonale ne contient pas de racines du résultant. Pour déterminer une valeur de k qui convient, on paramètre chaque segment à l'aide d'un paramètre réel, par exemple pour le premier segment :

$$t = \frac{u}{2}(1 + ik), \quad u \in [0, 1]$$

puis on remplace dans R, qui devient un polynôme $R_1(u)$ à coefficients complexes. Pour savoir s'il a des racines réelles $u \in [0, 1]$, on utilise les suites de Sturm sur le polynôme $|R_1|^2(u)$ qui est à coefficients réels.

Exemple : on prend le polynôme $P = x^4 - 5x - 1$, on vérifie facilement que R ne s'annule pas sur $[0, 1]$, les racines suivent les chemins représentés sur la figure suivante :



4 Les suites de Sturm complexes

Il s'agit ici de généraliser le résultat de localisation de racines réelles d'un polynôme à coefficients réels. On compte les racines à l'intérieur d'un rectangle γ du plan complexe et on effectue une dichotomie pour diminuer la taille du rectangle s'il contient des racines, jusqu'à la précision souhaitée.

On suppose que P ne s'annule pas sur le rectangle γ. Pour compter les racines, on calcule le nombre de tours que fait $P(z)$ autour de 0 lorsque z parcourt le rectangle γ. Plus précisément, on calcule un indice que l'on incrémente ou décrémente lorsque $P(z)$ traverse l'axe réel ($\Im P(z) = 0$) en tenant compte du sens de traversée et du signe de $\Re P(z)$ lorsque $\Im P(z) = 0$: si $\Re P(z) > 0$ et $\Im P(z)$ croit ou si $\Re P(z) < 0$ et $\Im P(z)$ décroit, on augmente l'indice de 1 (car on tourne autour de 0 dans le sens trigonométrique), sinon on diminue l'indice de 1. Le nombre de racines de P dans γ est alors égal au nombre de tours autour de 0 c'est-à-dire à l'indice divisé par 2.

Calcul de l'indice de manière exacte

On utilise une généralisation des suites de Sturm. Sur un segment $[a, b]$ du rectangle γ, on définit :

$$Q(t) = P(a + t(b - a)), \quad t \in [0, 1]$$

Posons $S(t) = \Im Q(t)$ et $R(t) = \Re Q(t)$ et supposons que S et R sont premiers entre eux. On forme alors la suite des opposés des restes des divisions euclidiennes comme pour les suites de Sturm réelles avec P et P' et on compte le nombre de changements de signes en $t = 0$ et $t = 1$. On montre que la différence entre ces 2 nombres est égal à la variation de l'indice sur le segment $[a, b]$:

- on vérifie que le nombre de changements de signes ne varie pas lorsque t augmente sauf si S s'annule.
- Si S s'annule en croissant avec R positif, alors ce nombre diminue de 1 de même que l'indice, on regarde les 3 autres cas et on conclut.

Pour calculer l'indice sur γ, il suffit de sommer les 4 indices sur chaque coté. On divise ensuite par 2 pour obtenir le nombre de racines.

Traitement des cas particuliers :

- Si S s'annule en un sommet de γ, cela ne pose pas de problèmes, car pour le nombre de changements de signe, tout se passe comme si S était du signe de R en ce sommet (ce qui revient à déformer un peu γ). Il

faut néanmoins s'assurer que P ne s'annule pas sur un sommet de rectangle, ce que l'on fait en éliminant les racines rationnelles complexes de P au préalable.

– Si S et R ne sont pas premiers entre eux. Si leur pgcd G est de degré inférieur strict au degré de P, alors on peut utiliser G pour factoriser P en 2 polynômes de degré strictement plus petit et recommencer avec ces 2 polynômes. Si leur pgcd est de degré maximal, alors P est à une constante complexe c près un multiple du pgcd G de R et S, et G est un polynôme à coefficients réels. En multipliant P par une constante complexe adéquate, on peut supposer que la constante c est réelle. On peut compter les racines de P sur le segment $[a, b]$ par isolation des racines de G. On montre ensuite que sur un segment parallèle à $[a, b]$ situé à l'intérieur au rectangle à distance ϵ, on a $S(t) = \epsilon Q'(t) + O(\epsilon^2)$ et $R(t) = Q(t) + O(\epsilon)$, le calcul de l'indice sur le segment parallèle à $[a, b]$ infiniment proche est alors égal à celui obtenu en prenant la suites de Sturm réelle de Q et $-Q'$ entre $t = 0$ et $t = 1$.

Exemple :

Nombre de racines complexes de $x^3 + ix + 1$ dans le rectangle de sommets opposés 0 et $1 + i$.

– Sur le segment $[0, 1]$, $Q(t) = P(t)$ donc $S(t) = t$ et $R(t) = t^3 + 1$. La suite de Sturm est formée de $t, t^3 + 1, -t, -1$, en 0 un changement de signe, en 1 1 changement de signe, contribution à l'indice de 0.
– Sur $[1, 1 + i]$, on trouve $S(t) = -t^3 + 3t + 1$ et $R(t) = -3t^2 - t + 2$. La suite de Sturm est formée de $S, R, (-20t - 11)/9, -657/400$. En 0, un changement de signe, en 1, aussi, indice 0.
– Sur $[1 + i, i]$, $S = 3t^2 - 7t + 3$, $R = -t^3 + 3t^2 - 2$, on trouve que la contribution à l'indice est de 1
– Sur $[i, 0]$, $S = t^3 - 3t^2 + 3t - 1$, $R = t$, la suite est donc $S, R, 1$, en $t = 0$ on a un changement de signe et en $t = 1$ 0 changements de signe, la contribution à l'indice est de 1.

On obtient donc un indice de 2, donc 1 racine complexe dans le rectangle.

Remarque

Pour l'implémentation de cette méthode, on utilise l'algorithme du sous-résultant pour calculer la suite de Sturm et on conserve la liste des quotients au lieu de la liste des restes, car il est plus efficace d'évaluer un quotient en $t = 0$ et $t = 1$ qu'un reste puisque un quotient de la suite est génériquement de degré 1.

5 Suggestions

– Certification des racines renvoyées par la commande de recherche de racines approchées de votre logiciel (`proot` en Xcas).
– Mise en oeuvre de la méthode de la puissance pour déterminer une valeur approchée d'une racine de module maximal d'un polynôme.
– Calcul des racines par la méthode de Newton avec élimination (en utilisant uniquement l'algorithme de Horner), illustration des problèmes évoqués pour cette méthode. Bassins d'attraction des racines pour une suite récurrente définie par la méthode de Newton.
– Interactions entre factorisation exacte et approchée.
– Représentation de la variation des racines en fonction de t dans la méthode d'homotopie. Cas où deux racines se croisent.
– Localisation des racines réelles par les suites de Sturm.
– En utilisant le résultant des polynômes $\Re P(x + iy)$ et $\Im P(x + iy)$ pour $x, y \in \mathbb{R}$, montrer qu'on peut localiser la partie réelle et la partie imaginaire d'un polynôme à l'aide de suites de Sturm réelles. Discuter l'efficacité de cette méthode en fonction du degré.
– Expliquer la méthode des suites de Sturm complexes en complétant certaines esquisses de démonstrations du texte. Illustrer cette méthode.
– Que peut-on dire du point de vue efficacité des algorithmes nécessaire au calcul des suites de Sturm complexe ? (changement d'origine $Q(t) = P(a + t(b - a))$, algorithme d'Euclide, ...)
– Connaissez-vous des méthodes de calculs de racines rationnelles d'un polynôme ? Peuvent-elles se généraliser à la recherche de racines rationnelles complexes ?