19

La recherche des racines complexes d'un polynôme selon Schönhage

Xavier Gourdon
École Polytechnique, Palaiseau

[résumé par Xavier Gourdon]

Le but de l'exposé est de présenter une méthode due à Schönhage qui recherche les racines complexes d'un polynôme à coefficients complexes [5, 6]. L'avantage de cette dernière est qu'elle permet *dans tous les cas* d'approcher les racines d'un polynôme. Ce n'est pas le cas avec les méthodes existantes. Des tests montrent par exemple que la méthode de Traub et Jenkins [3] qui est implantée en MAPLE et MATHEMATICA échoue lorsque le polynôme est mal conditionné (par exemple à racines multiples ou proches, ou à racines régulièrement réparties) ou lorsqu'il est de degré trop élevé (variant de 25 à 100 selon les polynômes et les programmes). (La méthode de Traub et Jenkins était jusque là reconnue comme étant la plus efficace). Une implantation soignée de l'algorithme de Schönhage en MAPLE donne sur tous les polynômes d'excellents résultats (pour une étude complète de l'algorithme, voir [2]).

1 Position du problème

Notation 1 *On définit la norme* $|\cdot|$. *Si* $P = a_0 + a_1 X + \cdots + a_n X^n$, *on pose :*

$$|P| = |a_0| + |a_1| + \cdots + |a_n|.$$

Si tant d'algorithmes échouent, c'est que la recherche des racines d'un polynôme est un problème extrêmement mal conditionné. Le théorème de perturbation qui suit confirme ce fait.

Théorème 1 (Ostrowski) *Soit* P *et* Q *deux polynômes unitaires de degré* $n > 0$, *avec* $Q = (X - v_1)\cdots(X - v_n)$. *Alors si* $\epsilon = |P - Q|$, *on peut écrire* $P = (X - u_1)\cdots(X - u_n)$ *avec*

$$\forall i, \quad |u_i - v_i| < 4\rho\epsilon^{1/n}, \qquad \text{où } \rho = \sup\{1, |u_i|\}.$$

Autrement dit, les racines d'un polynôme bougent en $\epsilon^{1/n}$ lorsque ses coefficients bougent en ϵ (un exemple facile où le phénomène se produit est le cas de $P = X^n - \epsilon$ et $Q = X^n$). Ce résultat est en fait très pessimiste dans le cas général. De manière intuitive, lorsqu'un polynôme est perturbé à ϵ près, une racine u d'ordre p (i.e. p racines du polynôme sont proches de u, les autres sont éloignées de u) se déplace avec une erreur de l'ordre de $\epsilon^{1/p}$.
Le théorème justifie le choix fait par Schönhage. Un polynôme P unitaire de degré $n > 1$ et un entier $s > 0$ étant donnés, son algorithme détermine n nombres complexes $u_1, \ldots, u_n$ tels que :

$$|P - (X - u_1)\cdots(X - u_n)| < 2^{-s} \tag{1}$$

en un temps d'exécution

$$O\left[(n^3 \log n + sn^2)\log(ns)\log(\log(ns))\right]. \tag{2}$$

C'est donc au sens de (1) que l'algorithme donne des approximations des racines de P. En généralisant le théorème donné plus haut, on peut alors donner *a posteriori* pour chaque racine trouvée une borne d'erreur proche de l'imprécision réelle. Quant à (2), ce résultat est surtout théorique. Il est obtenu en utilisant des méthodes de F.F.T. pour le calcul de produit et de division de polynômes, et la constante devant (2) est énorme. Dans la pratique, c'est surtout le fait que les racines soient trouvées dans *tous les cas* qui est intéressant.

2 Principe de la méthode de Schönhage

Soit P un polynôme à coefficients complexes de degré $n > 1$. L'idée est non pas de calculer directement une racine de P (comme le font en général les autres méthodes), mais de factoriser P en deux polynômes : $P = FG$. En réitérant ainsi le procédé sur F et G, on saura écrire P comme produit de facteurs du premier degré.
L'algorithme détermine d'abord un cercle Γ contenant une partie des racines de P (voir figure 1), par exemple

$$u_1, u_2, \ldots, u_k \qquad \text{avec} \qquad 1 \leq k < n.$$

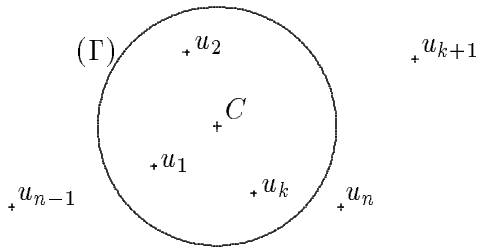

Figure 1. Les racines de P et le cercle de séparation.

Par intégration le long de ce cercle (appelé cercle de séparation), on peut ensuite déterminer le polynôme unitaire dont les racines sont $u_1, u_2, \ldots, u_k$. On a en effet :

$$\forall p, \qquad S_p = u_1^p + u_2^p + \cdots + u_k^p = \oint_{(\Gamma)} \frac{P'(z)}{P(z)} z^p \, dz \tag{3}$$

d'où les coefficients de $F(z) = (z - u_1)\cdots(z - u_k)$ par les formules de Newton. Si G est le quotient de la division euclidienne de P par F, on a donc factorisé P en un produit de deux facteurs. Ceci dit, l'approximation numérique de (3) par discrétisation de Γ sera plus ou moins précise selon le choix de Γ. On sent bien que s'il se trouve près de Γ une racine de P, le calcul numérique de (3) sera mauvais. Dans cette optique, le cercle de séparation Γ sera choisi de sorte que les racines de P s'en éloignent le plus possible.

3 Recherche du cercle de séparation

Notation 2 *Si P est un polynôme complexe de degré $n > 0$, on note $r_1(P), \cdots, r_n(P)$ les modules de ses racines rangés dans l'ordre croissant.*

On veut un cercle de séparation pour P, i.e. un cercle contenant une partie non vide de ses racines et ne les contenant pas toutes. Si $\Delta = \log(r_n(P)/r_1(P)) > 0$, alors $\exists j$ tel que $\log(r_{j+1}(P)/r_j(P)) > \Delta/(n-1)$. On a alors trouvé un candidat pour notre cercle de séparation : le cercle de centre 0 de rayon $\sqrt{r_j r_{j+1}}$. Ceci n'est malheureusement possible que si $\Delta \neq 0$; de toutes façons, même si $\Delta \neq 0$ il se peut que Δ soit faible et alors notre cercle de séparation n'est pas intéressant puisqu'il est trop près des racines. Nous allons pallier à ce problème en changeant d'origine.

3.1 Recherche du centre du cercle de séparation

On se ramène d'abord au cas où le barycentre des racines de P est l'origine (pour cela, si $P = X^n + a_{n-1}X^{n-1} + \cdots$, considérer $P(X - a_{n-1}/n)$). On se ramène ensuite au cas où le plus grand des rayons des racines de P est égal à 1 (voir le paragraphe suivant pour le calcul de $r_n(P)$). Le dessin suivant montre alors que si $v_0 = 2, v_1 = 2i, v_2 = -2, v_3 = -2i$, alors $\exists j$ tel que $\Delta_j = \log(r_n(P_j)/r_1(P_j)) > 0.30$ (où $P_j = P(X + v_j)$). En calculant Δ_j pour $j = 0 \ldots 3$, puis en choisissant j maximisant Δ_j, on s'est ainsi ramené au cas où $\Delta > 0.30$.

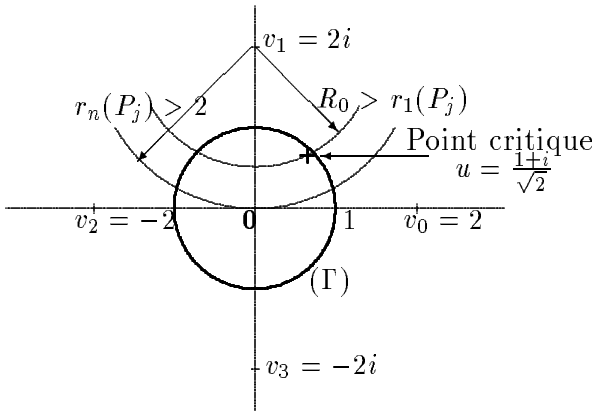

Figure 2. Les centres v_i pour obtenir l'écartement $\Delta = \log(r_n/r_1) > 0.30$.

3.2 Recherche du rayon du cercle de séparation

Il nous faut savoir calculer les modules $r_i(P)$ des racines de P. Comme $\Delta = \log(r_n/r_1)$ n'est pas trop petit, on saura ensuite trouver un cercle de séparation dont les racines ne soient pas trop proches. Ceci est permis grâce à la méthode de Graeffe dont nous rappelons les grandes lignes.
L'idée est que les racines du polynôme Q défini par $Q(X^2) = P(X)P(-X)$ sont les carrés des racines de P. On note Q =Graeffe(P). On pose $P_0 = P$ puis P_m =Graeffe(P_{m-1}), de sorte que $r_k(P_m) = r_k(P)^{2^m}$, et donc, si $r_1(P) < \cdots < r_n(P)$, en notant $P_m = a_n^{(m)}X^n + a_{n-1}^{(m)}X^{n-1} + \cdots$:

$$\lim_{m\to\infty} \left| \frac{a_{k-1}^{(m)}}{a_k^{(m)}} \right|^{2^{-m}} = r_k(P).$$

L'utilisation directe de ce procédé est difficile pour deux raisons.

- La convergence n'est assurée que si $r_1 < \cdots < r_n$. Par ailleurs, même si cette dernière condition est réalisée, la convergence peut être très lente (c'est le cas si pour un k, r_{k+1}/r_k est proche de 1).
- Les coefficients de P_m divergent très rapidement en module.

Schönhage contourne ces difficultés en utilisant une approche modifiée du problème (pour plus de détails, voir [2, 3.1].

4 Calcul d'un facteur à partir du cercle de séparation

Quitte à effectuer des transformations simples, on peut supposer que le cercle de séparation est le cercle unité. Sa recherche nous permet même de connaître le nombre k des racines se trouvant à l'intérieur du cercle et un paramètre $\delta > 0$ tel qu'aucune des racines de P ne se trouve dans la couronne $\{e^{-\delta} < |z| < e^{\delta}\}$.
Les coefficients du polynôme F dont les racines se trouvent à l'intérieur du cercle de séparation sont donnés par calcul de (3) suivi des formules de Newton. On approxime les valeurs S_p de (3) pour $1 \leq p \leq k$ par discrétisation du cercle unité en N points régulièrement répartis. On montre qu'après calculs, l'approximation F_0 de F vérifie

$$|F_0 - F| < |F| k n e^{-\delta(N-k)}.$$

C'est cette majoration qui permet de déterminer la valeur de N qu'il faut choisir pour être sûr que F_0 est déterminé avec suffisamment de précision. Seulement ce calcul peut devenir très coûteux si l'on désire avoir une bonne précision sur F_0. L'algorithme de Schönhage s'en sort comme suit. Il détermine d'abord par cette méthode une approximation F_0 de F suffisamment bonne puis il lance une méthode dite de Newton-Schönhage qui permet d'obtenir rapidement à partir de F_0 une bonne approximation de F.

4.1 La méthode de Newton Schönhage

Hypothèses. $P = FG$ où les racines de F sont à l'intérieur du cercle unité, celles de G en dehors. On connaît une approximation F_0 de F, une approximation G_0 de G (déterminée par division euclidienne de P par F_0).
Problème. On veut trouver deux termes correcteurs f et g tels que $F_1 = F_0 + f$ et $G_1 = G_0 + g$ approchent F et G mieux que F_0 et G_0.

On a $F_1 G_1 = (F_0 + f)(G_0 + g) = F_0 G_0 + f G_0 + g F_0 + fg$. Le terme fg étant du second ordre, si on choisit f et g tels que

$$P = F_0 G_0 + f G_0 + g F_0 \quad \Longleftrightarrow \quad \frac{P - F_0 G_0}{F_0 G_0} = \frac{f}{F_0} + \frac{g}{G_0}, \tag{4}$$

on aura $|P - F_1 G_1| = |fg| \leq |f| \cdot |g|$, donc du second ordre. F_0 et G_0 sont premiers entre eux et f et g dans (4) sont donc uniques. On peut les déterminer par exemple grâce à l'algorithme d'Euclide. Sans rentrer dans les détails, disons que le problème est que cette méthode est peu stable numériquement et Schönhage s'en sort autrement à partir d'une représentation intégrale de f, conséquence du théorème des résidus.

4.2 Description complète de la factorisation à partir du cercle de séparation

On se demande maintenant avec quelle précision on doit calculer F_0 pour assurer une convergence rapide de la méthode de Newton-Schönhage. On montre que le nombre de points N pris sur le cercle unité pour approximer F_0 doit vérifier :

$$N \geq k + \frac{1}{\delta}\left(\log(100) + \log(k^3(n-k)^{3/2}n) + \frac{5}{2}\log(\gamma) + \log\left(\frac{1}{\mu}\right) + 3\log(|F|\cdot|G|)\right),$$

où $\gamma = \frac{1}{2\pi}\oint |dt/P(t)|$ et $\mu = \inf_{|z|=1}|P(z)|$. Le calcul de γ et μ est réglé par approximation numérique. Il faut donner une majoration de $|F|\cdot|G|$. Schönhage utilise la majoration $|F|\cdot|G| < 2^n|P|$, donnée par Mignotte dans [4]. En fait, on peut donner une inégalité beaucoup plus fine :

$$|F|\cdot|G| < 2^{n/2}\sqrt{\binom{n}{k}}\,[P]_2, \quad \text{où} \quad [P]_2 = \left(\sum_{i=0}^{n}\frac{|a_i|^2}{\binom{n}{i}}\right)^{1/2}.$$

Cette inégalité est une conséquence d'un résultat démontré dans [1]. Cette étape d'intégration numérique est la plus coûteuse de l'algorithme de Schönhage. Son coût est déjà considérablement diminué en utilisant une F.F.T partielle. Il est également important de diminuer le plus possible la valeur de N. Celle donnée plus haut améliore déjà celle donnée par Schönhage lui-même dans [5]. On peut encore l'améliorer en augmentant la valeur de δ, ce qui est rendu possible par une transformation homographique préalable : $z \mapsto (z-a)/(\bar{a}z-1)$.

Conclusion

Les optimisations données à l'algorithme de Schönhage dans [2] permettent de gagner par rapport à l'algorithme initial un facteur temps de l'ordre de 10. Le programme écrit en MAPLE fait 1500 lignes. Il donne de bons résultats numériques sur *tous les polynômes* (même mal conditionnés), en un temps cependant plus élevé que les algorithmes déjà existants.
Les bornes d'erreur données *a posteriori* sur les approximations des racines sont garanties et autorisent l'introduction de moyens numériques dans le calcul formel. Cette idée est nouvelle et permettrait parfois de diminuer considérablement le coût de certaines opérations formelles.

Références

[1] B. Beauzamy. Products of polynomials and a priori estimates for coefficients in poynomial decompositions. *Journal of Symbolic Computation*, 1992. To appear.

[2] X. Gourdon. Algorithmique du théorème fondamental de l'algèbre. Rapport de recherche, Institut National de Recherche en Informatique et en Automatique, 1992. À paraître.

[3] M. A. Jenkins and J. F. Traub. A three-stage variable-shift iteration for polynomial zeros and its relation to generalized Rayleigh iteration. *Numer. Math.*, 14:252–263, 1970.

[4] M. Mignotte. An inequality about factors of polynomials. *Math. Comp.*, 28(128), 1974.

[5] A. Schönhage. The fundamental theorem of algebra in terms of computational complexity. Technical report, Mathematisches Institut der Universität Tübingen, 1982.

[6] A. Schönhage. Equation solving in terms of computational complexity. In *Proceedings of the International Congress of Mathematicians*, pages 131–153, 1987. Berkeley, California, 1986.