SUR LE CALCUL DES RACINES DES POLYNOMES

Jean-Pierre DEDIEU
Laboratoire d'Analyse Numérique
118 route de Narbonne
Université Paul Sabatier
31062 Toulouse CEDEX

C'est pourquoi je me contenterai ici de vous avertir que pourvu qu'en démêlant ces équations on ne manque pas de se servir de toutes les divisions qui seront possibles, on aura infailliblement les plus simples termes auxquels la question puisse être résolue.
René Descartes

0 - INTRODUCTION

Donnons-nous un nombre algébrique, c'est-à-dire une racine d'un polynôme à coefficients entiers. Se le donner qu'est-ce à dire ? De quels moyens dispose-t-on pour décrire un tel nombre, pour le coder ...Le procédé le plus ancien est purement géométrique : $\sqrt{2}$ est défini comme la longueur de la diagonale d'un carré de côté unité. On lui associe alors une suite de valeurs approchées : citons le procédé d'Héron d'Alexandrie qui raffine l'approximation a de $\sqrt{A}$ par la formule $(a + A/a)/2$, ou bien les valeurs approchées de $\sqrt{2}$:

$1 + \frac{25}{60}$ et $1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3}$ trouvées sur des tablettes babyloniennes. A côté de ces méthodes géométriques et numériques figurent la localisation et le codage par les signes. Dans le premier cas on décrit un nombre algébrique par un polynôme dont-il est racine et un intervalle à extrémités rationnelles contenant ce nombre à l'exclusion de toute autre racine. Dans le second cas notre nombre a est donné par l'équation qu'il satisfait $P(a) = 0$ et par les signes des dérivées successives de $P(x)$ en a.

La localisation suppose avant tout de connaître un intervalle contenant les éventuelles racines réelles de $P(x)$. D'où un premier problème : estimer

$$\rho(P) = \max \{ |r|, P(r) = 0 \}$$

Puis, si l'on procède par dichotomie, on a besoin d'un test d'arrêt qui sera fondé soit sur le nombre

$$\mathrm{sep}(P) = \min \{ |r_i - r_j|, \quad P(r_i) = P(r_j) = 0 \text{ et } r_i \neq r_j \}$$

(tout intervalle de longueur $m \leq \mathrm{sep}(P)$ contient au plus une racine), soit sur le calcul du nombre de racines réelles contenues dans un intervalle donné (méthode de Sturm).

Nous exposons dans le premier paragraphe des résultats classiques concernant $\rho(P)$ et $\mathrm{sep}(P)$, ainsi que des estimations des modules des racines fondées sur la méthode de Dandelin-Graeffe et les inégalités d'Ostrowski.

Les techniques de codage par les signes des dérivées sont exposées au cours du second paragraphe. Elles sont baties à partir du lemme de Thom d'une part (on peut le faire) et des suites de Sturm d'autre part (comment le faire).

Nous ne donnons de démonstrations que des résultats que nous n'avons pu (ou su) trouver dans la littérature idoine. Quant aux autres ... nous renvoyons le lecteur à la bibliographie ci-jointe.

1 - LE CALCUL DU PLUS GRAND DES MODULES ET SES CONSEQUENCES

1. Introduction

Considérons un polynôme $P(x) = \sum_{i=0}^{n} a_i \, x^{n-i}$ à coefficients réels et de degré n,

dont les racines sont rangées par module décroissant : $|r_1| \geq |r_2| \geq \ldots \geq |r_n|$.

Notons $\rho(P) = \max_{1 \leq i \leq n} |r_i|$. Nous allons décrire diverses méthodes qui permettent d'estimer ou de calculer ce nombre en toute généralité. Le maximum des modules est relié à de nombreuses questions sur les racines d'un polynôme. Par exemple le calcul du minimum des modules des racines ou du minimum des distances des racines. On peut aussi, connaissant $\rho(P)$, calculer le diviseur de $P(x)$ dont les zéros ont un module égal à $\rho(P)$. On obtient ainsi la factorisation équimodulaire de $P(x)$ (c'est-à-dire dont les facteurs ont des racines de même module).

Nous n'avons pas ici cherché à être exhaustif. Notamment, nous ne présentons que des résultats que l'on peut prouver sans faire d'hypothèses sur les racines de $P(x)$. par exemple réelles, ou de modules distincts, ou déjà localisées.

2. Des inégalités classiques

Les inégalités suivantes sont aussi satisfaites pour des polynômes à coefficients complexes. Leur démonstration figure dans le livre de Marden ou l'article de Mignotte.

Cauchy (1829) :

$$(1) \qquad \rho(P) < 1 + \max_{1 \leq i \leq n} \frac{|a_i|}{|a_0|} \, .$$

Montel (1931) : pour $p > 1$, $q > 1$, $p^{-1} + q^{-1} = 1$:

$$(2) \qquad \rho(P) < \left(1 + \left(\sum_{i=1}^{n} \left|\frac{a_i}{a_0}\right|^p\right)^{q/p}\right)^{1/q} .$$

Landau :

$$(3) \qquad |a_0| \prod_{i=1}^{n} \max\{1, |r_i|\} \leq \left(\sum_{i=0}^{n} |a_i|^2\right)^{1/2} .$$

L'inégalité suivante (M. Mignotte, 1982) relie les coefficients d'un diviseur $Q(x) = \sum_{i=0}^{m} b_i x^{m-i}$ de degré m de $P(x)$ à ceux de $P(x)$:

$$(4) \qquad \sum_{i=0}^{m} |b_i| \leq |b_0/a_0| \, 2^m \left(\sum_{i=0}^{n} |a_i|^2\right)^{1/2} .$$

La double inégalité suivante est due à Birkhoff (1914).

Notons $|P|(x) = |a_0| x^n - \sum_{i=1}^{n} |a_i| x^{n-i}$. Ce polynôme est à coefficients réels et par la règle des signes de Descartes on peut voir qu'il possède un seul zéro $r(P) > 0$. On a :

$$(5) \qquad (2^{1/n} - 1)\, r(P) \leq r(P) \leq r(P) .$$

Il existe des polynômes pour lesquels les bornes de ces inégalités sont atteintes.

3. Le minimum des modules des racines

Supposons que 0 ne soit pas racine de P(x) et notons $\sigma(P) = \min_{1 \leq i \leq n} |r_i|$.

Le polynôme $Q(x) = x^n P(1/x)$ a pour racines $r_1^{-1}, \ldots, r_n^{-1}$ de sorte que $\sigma(P) = \rho(Q)^{-1}$.

4. Calcul de $\rho(P)$ lorsque c'est une racine de $P(x)$.

Ce qui revient à dire que la (ou une) racine de plus grand module est réelle. Supposons que $a_0 > 0$. Toutes les racines de P(x) sont dans le demi-plan complexe $\mathrm{Re}(z) \leq \rho(P)$. Le théorème de Lucas nous dit qu'alors les zéros de $P'(x)$ et $P''(x)$ sont aussi dans ce demi-plan, et ceci prouve que pour $x \geq \rho(P)$, $P(x)$ est positive, croissante et convexe. L'itération de Newton partant de $x_0 > \rho(P)$ fournit alors une suite décroissante et qui converge vers $\rho(P)$ (Figure 1).

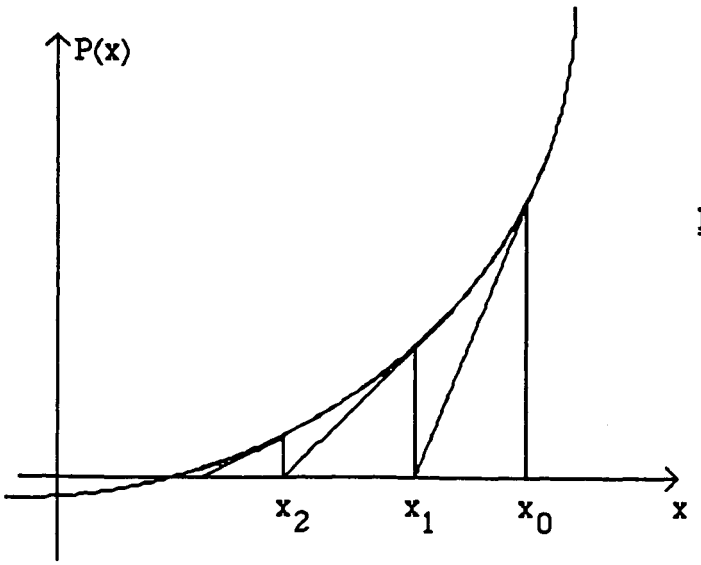

Figure 1

Proposition 1 - *Lorsque* $\rho(P)$ *est racine de* $P(x)$ *l'itération*

$$x_0 = 1 + \max_{1 \le i \le n} \left| \frac{a_i}{a_0} \right| \quad (\text{ou } x_0 > \rho(P)),$$

$$x_{n+1} = x_n - \frac{P(x_n)}{P'(x_n)},$$

est décroissante et converge vers $\rho(P)$.

Ce résultat permet de calculer ou de majorer $r(P)$ dans l'inégalité de Birkhoff (§ 2.2.). En effet, si l'on applique cette inégalité à $|P|$, on obtient $\rho(|P|) \le r(|P|) = r(P)$ de sorte que $\rho(|P|) = r(P)$ et c'est une racine de $|P|$. D'où le corollaire :

Corollaire 1 - *Pour* $|P|(x) = |a_0| x^n - \sum_{i=1}^{n} |a_i| x^{n-i}$ *et* $r(P)$ *sa racine* >0, *l'itération*

$$x_0 = 1 + \max_{1 \le i \le n} \left| \frac{a_i}{a_0} \right|$$

$$x_{n+1} = x_n - \frac{|P|(x_n)}{|P|'(x_n)}$$

est décroissante et converge vers $r(P)$.

5. Calcul de $\rho(P)$ dans le cas général.

Supposons que $P(0) \neq 0$ et soit $R(y) = \text{res}_x(P(x), x^n P(y/x))$ le résultant en x de ces deux polynômes. Les racines de $R(y)$ sont les produits $r_i r_j$, $1 \le i, j \le n$, des racines $P(x)$

(Davenport - I.4. proposition 3). On a bien sûr $\rho(R) = \rho(P)^2$. Soit r une racine de plus grand module pour $P(x)$. Comme ce polynôme est à coefficients réels, la conjuguée $\bar{r}$ de r est aussi racine de plus grand module et ceci prouve que $r \cdot \bar{r} = \rho(P)^2 = \rho(R)$ est racine de $R(y)$. La proposition 1 du paragraphe précédent nous donne :

Proposition 2 - *Supposons* $P(0) \neq 0$ *et soit*

$$R(y) = \mathrm{res}_x(P(x), x^n P(y/x)) .$$

L'itération

$$y_0 = (1 + \max_{1 \leq i \leq n} |\frac{a_i}{a_0}|)^2 \qquad (\text{ou } y_0 > \rho(P)^2) ,$$

$$y_{n+1} = y_n - \frac{R(y_n)}{R'(Y_n)}$$

est décroissante et converge vers $\rho(P)^2$.

6. La méthode de Dandelin-Graeffe

Il s'agit de construire une suite de polynômes $P_k(x) = \sum_{i=0}^{n} a_{i,k}\, x^{n-i}$, de même degré que P(x), et dont les racines sont les puissances k-ièmes de celles de $P(x)$: $r_1^k, \ldots, r_n^k$. Les coefficients $a_{i,k}$ sont des fonctions symétriques des racines, en particulier :

$$a_{1,k}/a_{0,k} = -(r_1^k + \ldots + r_n^k) = -r_1^k(1 + \sum_{i=2}^{n} (r_i r_1^{-1})^k) .$$

Si l'on suppose que $\rho(P) = |r_1| > |r_2| \geq \ldots \geq |r_n|$, on obtient asymptotiquement :

$$\rho(P) = |r_1| \sim |a_{1,k} / a_{0,k}|^{1/k} .$$

Le cas où il existe p racines de plus grand module se traite de façon identique mais en considérant $a_{p,k}$ au lieu de $a_{1,k}$.

Cette méthode a été inventée par Dandelin (1826) et popularisée par Graeffe (1833) et Encke (1841). Elle est aussi citée par Lobachevsky (1834). Ces auteurs ne considéraient que la sous-suite $P_k(x)$, $k = 2^s$, et obtenaient ρ(P) par extractions de racines carrées.

6.1. Le calcul de P_2

Supposons que $P(x) = a_0 \prod_{i=1}^{n} (x - r_i)$, on a

$$P(\sqrt{x})\, P(-\sqrt{x}) = a_0^2 \prod_{i=1}^{n} (\sqrt{x} - r_i)(-\sqrt{x} - r_i) = a_0^2 (-1)^n \prod_{i=1}^{n} (x - r_i^2),$$

ce qui conduit à la formule suivante :

$$(6) \qquad P_2(x) = P(\sqrt{x})\, P(-\sqrt{x}) .$$

Les coefficients de $P_2(x)$ sont donnés par :

$$(7) \qquad a_{i,2} = \sum_{j=0}^{n} (-1)^{n-i-j} \cdot a_{i+j} \cdot a_{i-j}$$

en convenant que $a_k = 0$ pour $k < 0$ et $k > n$.

Une autre façon de calculer $P_2(x)$ est la suivante. Séparons dans $P(x)$ les termes en x^{2i} et ceux en x^{2i+1} :

$$P(x) = A(x^2) + x\, B(x^2).$$

Si $P(r) = 0$ on a $A(r^2) = -r\, B(r^2)$ et en élevant au carré $A(r^2)^2 = r^2 B(r^2)$, ce qui prouve que r^2 est racine de

$$(8) \qquad P_2(x) = A(x)^2 - x\, B(x)^2 .$$

Connaissant P on construit par ces formules la suite P_k, $k = 2^s$.

6.2. Le calcul de P_k .

Les résultats précédents s'étentent ainsi pour k quelconque :

$$(9) \qquad P_k(x) = P(wx^{1/k})\, P(w^2 x^{1/k}) \ldots P(w^k x^{1/k})$$

où w est une racine primitive k-ième de l'unité.

Pour $k = k_1 k_2$ et $\omega_2^{k_2} = 1$ on a :

$$(10) \qquad P_k(x) = P_{k_1}(\omega_2 x^{1/k_2}) \ldots P_{k_1}(\omega_2^{k_2} x^{1/k_2}) .$$

Une autre possibilité de calcul est obtenue en regroupant dans $P(x)$ les monômes de même congruence modulo k.

Proposition 3 - *Si* $P(x) = \sum_{i=0}^{k-1} x^i \, A_i(x^k)$ alors

$$(11) \qquad P_k(x) = \begin{vmatrix} A_0(x) & A_1(x) & \dots & A_{k-2}(x) & A_{k-1}(x) \\ x A_{k-1}(x) & A_0(x) & \dots & A_{k-3}(x) & A_{k-2}(x) \\ \dots & \dots & \dots & \dots & \dots \\ x A_1(x) & x A_2(x) & \dots & x A_{k-1}(x) & A_0(x) \end{vmatrix}$$

Démonstration : Notons $Q(x)$ la matrice dont les entrées sont celles du déterminant ci-dessus, fixons une valeur de x et considérons d'une part le polynôme :

$$R(y) = \sum_{i=0}^{k-1} y^i \, A_i(x) ,$$

d'autre part la matrice $k \times k$ suivante :

$$B = \begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \\ x & 0 & 0 & \dots & 0 \end{vmatrix} .$$

Il est connu que $\det R(B) = R(\lambda_1) \dots R(\lambda_k)$ où les λ_j sont les valeurs propres de B, c'est-à-dire ici $\lambda_j = w^j x^{1/k}$, $j = 1 \dots k$, $w^k = 1$. On obtient :

$$R(\lambda_j) = \sum_{i=0}^{k-1} (\omega^j x^{1/k})^i \, A_i(x) = P(\omega^j x^{1/k}) .$$

Comme par ailleurs $R(B) = Q(x)$ on a :

$$\det Q(x) = P(w x^{1/k}) \dots P(w^k x^{1/k}) = P_k(x) ,$$

d'après la formule (9).

Remarquons que pour $k \geq n$ les entrées de $Q(x)$ ne sont plus polynomiales mais scalaires. Pour $k = 2$ on retrouve la formule (8).

7. Raffinements de l'inégalité de Birkhoff.

L'inégalité de Birkhoff (6) appliquée aux itérées de Graeffe $P_k(x)$ de $P(x)$ nous donne une estimation de $\rho(P_k) = \rho(P)^k$.

$$(2^{1/n}-1)^{1/k} \leq \frac{\rho(P)}{r(P_k)^{1/k}} \leq 1$$

Cette estimation permet de prévoir indépendamment du polynôme $P(x)$, le nombre d'itérées de Graeffe que l'on aura besoin de calculer pour obtenir une précision donnée.

8. Les inégalités d'Ostrowski sur les modules des racines

Dans un long mémoire consacré à la méthode de Dandelin-Graeffe, Ostrowski (1940) donne des estimations des modules des racines à l'aide des inclinaisons numériques du polygone de Newton associé à P. Le polygone décrit ici diffère de celui introduit par Newton dans sa "méthode des fluxions" : il s'agit de la version donnée par J. Hadamard (1892) pour l'étude de la croissance des fonctions entières.

On suppose ici que $a_n \neq 0$, c'est-à-dire que $P(0) \neq 0$.

Notons :

$$M_i = (i, -\text{Log}\,|a_i|)\,,$$

$$D_i = \{\,(i,\lambda) \mid -Log\,|a_i| \leq \lambda\,\}\,,$$

avec $i = 0 \ldots n$ est en convenant que $D_i = \emptyset$ lorsque $a_i = 0$. Le polygone de Newton $\mathcal{N}_P$ de $P(x)$ est l'enveloppe convexe de la réunion des D_i.

Notons :

$$y_i = \min\,\{\lambda \mid (i,\lambda) \in \mathcal{N}_P\}\,,$$

$$b_i = \exp(-y_i)\,, \quad i = 0 \mid n\,.$$

La majorante newtonnienne de $P(x)$ est :

$$N_P(x) = \sum_{i=0}^{n} b_i\, x^{n-i}$$

et les inclinaisons numériques du polygone de Newton sont :

$$v_i = b_i/b_{i-1}\,, \quad i = 1 \ldots n\,.$$

Donnons un exemple de cette construction :

$$P(x) = x^6 + 4x^5 - 8x^4 - 8x^3 + 32x^2 + 32x + 1\,.$$

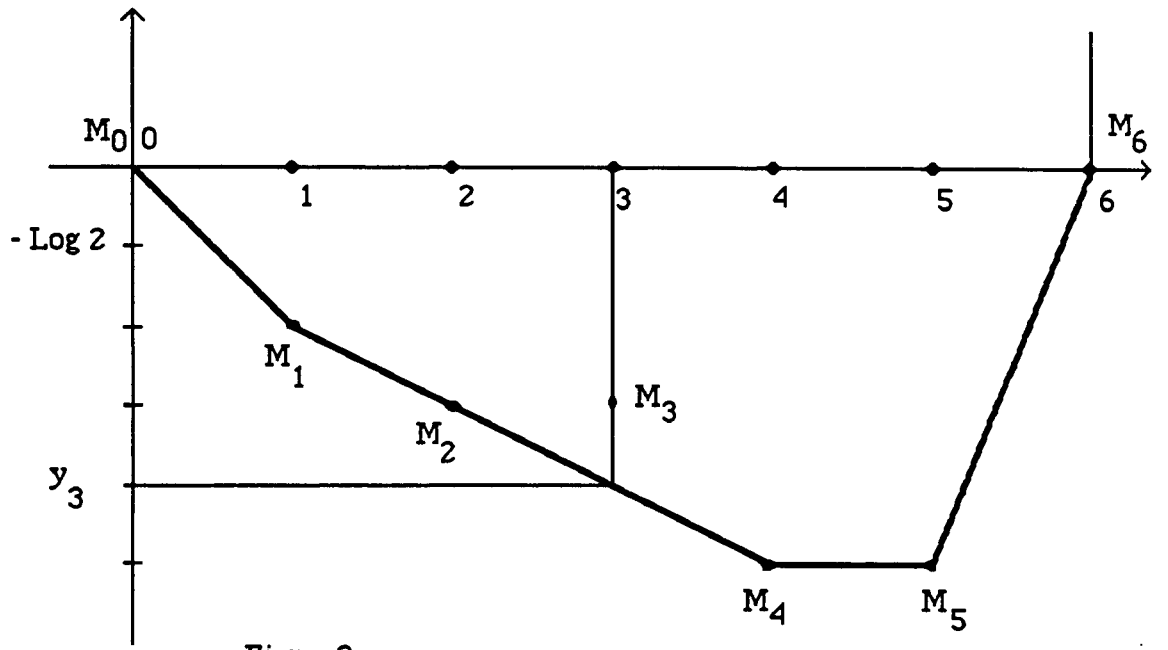

Figure 2

On a ici :

$$Np(x) = x^6 + 4\,x^5 + 8\,x^4 + 16\,x^3 + 32\,x^2 + 32\,x + 1\ ,$$

$$v_1 = 4, \quad v_2 = v_3 = v_4 = 2\ , \quad v_5 = 1, \quad v_6 = 0{,}03125$$

Remarquons que les inclinaisons numériques v_i sont décroissantes et > 0. De plus, si les a_i sont rationnels ou algébriques, les b_i (et donc les v_i) sont aussi algébriques. Les inégalités d'Ostrowski sont les suivantes :

Théorème 4 - *On a :*

$$\frac{1}{n} \le \frac{|r_1|}{v_1} < 2, \quad \frac{1}{2} < \frac{|r_n|}{v_n} \le n\ ,$$

$$1 - (\frac{1}{2})^{1/(n-i+1)} < \frac{|r_i|}{v_i} < (1 - (\frac{1}{2})^{1/i})^{-1}$$

lorsque $i = 2 \ldots n-1$.

Corollaire 1 - *Notons* $v_{i,k}$ *les inclinaisons numériques du polygone de Newton de l'itérée de Graeffe* $P_k(x)$ *de* $P(x)$. *On a :*

$$\frac{1}{n^{1/k}} \le \frac{|r_1|}{v_{1,k}^{1/k}} < 2^{1/k}, \quad \frac{1}{2^{1/k}} < \frac{|r_n|}{v_{n,k}^{1/k}} \le n^{1/k},$$

$$(1 - (\frac{1}{2})^{1/(n-i+1)})^{1/k} < \frac{|r_i|}{v_{i,k}^{1/k}} < (1 - (\frac{1}{2})^{1/i})^{-1/k},$$

lorsque $i = 2 \ldots n-1$.

9. Le minimum des distances des racines

Définissons :

$$\text{sep}(P) = \min \{|r_i - r_j| \ |r_i \neq r_j|\} .$$

On obtient si l'on connaît un minorant de sep(P) une limite inférieure pour la longueur des intervalles lorsque l'on cherche à isoler les racines réelles de $P(x)$ par dichotomie.

Pour des polynômes sans racines multiples on a (Mignotte) :

$$\text{sep(P)} > |3D|^{1/2} n^{-(n+1)/2} (\sum_{i=0}^{n} a_i^2)^{(1-n)/2},$$

où l'on désigne par

$$D = \text{discriminant } (P) = \text{res } (P,P').$$

Une autre façon de minorer sep(P) est la suivante :

$$T(x) = \text{res}_y(P(y-x), P(x))$$

est un polynôme de degré n^2 en x qui possède pour racines $r_i - r_j$, $1 \le i, j \le n$, (Davenport, I, Prop.2). C'est-à-dire :

$$0 \quad \text{si} \quad r_i = r_j$$

$$r_i - r_j \quad \text{et} \quad r_j - r_i \quad \text{si} \quad r_i \neq r_j \text{ et } i < j .$$

Aussi on obtient la factorisation

$$T(x) = c.x^m . \Pi(x^2 - (r_i - r_j)^2)$$

où le produit est pris pour $i < j$ et $r_i \neq r_j$. Considérons :

$$U(x^2) = x^{-m} T(x), \qquad d = \text{degré } (U),$$
$$V(x) = x^d \ U(1/x) .$$

Les racines de $V(x)$ sont $(r_i - r_j)^{-2}$, pour $r_i \neq r_j$ et $1 \le i < j \le n$, de sorte que

$$\text{sep}(P) = \rho(V)^{-1/2} .$$

Le calcul de sep(P) est ainsi ramené à celui d'un plus grand module.

10. Séparation des racines réelles par dichotomie.

Soit $P(x)$ un polynôme ne possédant que des racines simples et supposons donnés des nombres M et m tels que $0 < m \leq \text{sep}(P)$, $\rho(P) \leq M$.

Le shéma suivant permet de trouver pour chaque racine réelle de $P(x)$ un intervalle la contenant et n'en contenant pas d'autre :

- diviser l'intervalle $[-M,M]$ en sous-intervalles $[a_i,a_{i+1}]$ de longueur $\leq m$,
- calculer $P(a_i)$ (en fait : signe $(P(a_i))$),
- si $P(a_i) \neq 0$, calculer le signe de $P(a_i)\ P(a_{i+1})$,
- si $P(a_i)\,P(a_{i+1}) > 0$ il n'y a pas de racine dans $[a_i, a_{i+1}]$,
- si $P(a_i)\,P(a_{i+1}) < 0$ il y a une racine de $P(x)$ dans $]a_i, a_{i+1}[$ et une seule.

Le coût de cet algorithme dépend de la qualité des bornes m et M.

11. Calcul des facteurs équimodulaires

Posons $\rho = \rho(P)$ et supposons que $a_n \neq 0$, c'est-à-dire que $P(0) \neq 0$. Les racines de P étant rangées par module décroissant, on peut supposer que

$$\rho = |r_1| = \ldots = |r_p| > |r_{p+1}| \geq \ldots \geq |r_n| .$$

Les racines du polynôme $x^n\,P(\rho^2/x)$ sont ρ^2/r_i, $i = 1 \ldots n$. Lorsque $i = 1 \ldots p$, on a $r^2/r_i = \overline{r_i}$ (le conjugué de r_i) et c'est une racine de $P(x)$. Lorsque $i = p+1 \ldots n$, on a $|\rho^2/r_i| > \rho$ et ce n'est pas une racine de $P(x)$. D'où le résultat suivant :

Proposition 5 - *Si* $P(0) \neq 0$ et $\rho = \rho(P)$, *le polynôme*

$$\text{pgcd}\,(P(x), x^n P(\rho^2/x))$$

a pour racines celles de $P(x)$ *dont le module est égal à* $\rho(P)$. *C'est un facteur équimodulaire de* $P(x)$.

Corollaire 1 - *Le nombre de racines réelles ou complexes de* $P(x)$*ayant pour module* $\rho(P)$ *est égal à*

$$\text{degré}\,(\text{pgdc}(P(x), x^n P(\rho^2/x))$$

lorsque chacune est comptée avec sa multiplicité.

12. De la factorisation équimodulaire au calcul des racines.

Supposons que l'on sache calculer pour un polynôme $P(x)$ sa factorisation équimodulaire : $P(x) = P^1(x) \mid P^m(x)$, c'est-à-dire où les zéros de $P^j(x)$ ont le même module. Comment en déduire les racines de $P(x)$? En considérant un des facteurs $P^j(x)$ à la

place de $P(x)$, on se ramène au cas où $P(x)$ est équimodulaire ; notons ρ le module commun.

Dans une première étape on teste si ρ ou $-\rho$ annule $P(x)$. Les autres racines sont complexes et conjuguées, de module ρ, d'où la factorisation :

$$P(x) = a_0(x - \rho)^{n_1}(x + \rho)^{n_2} \prod_{i=1}^{m} (x - r_i)(x - r_i)$$

$$= a_0(x - \rho)^{n_1}(x + \rho)^{n_2} x^m \prod_{i=1}^{m} (y - 2\,\mathrm{Re}(r_i))$$

avec $y = x + \rho^2/x$, $n_1 + n_2 + 2m = n$.

On est ainsi conduit à l'étude d'un polynôme $Q(y)$ de degré $m \leq n/2$ pour lequel on réitère ce processus. Les racines r_i, r_i de $P(x)$ se déduisent de celles de $Q(y)$ par la résolution des équations :

$$x^2 - xy + \rho^2 = 0 .$$

Par exemple pour $P(x) = x^7 - 1$ dont les racines sont de module $\rho = 1$ on a

$$P(x) = (x - 1) \sum_{i=0}^{6} x^i = (x - 1)\,x^3(y^3 + y^2 - 2y - 1)$$

avec $x^2 - xy + 1 = 0$. On a ramené la factorisation de $x^7 - 1$ à celle de $y^3 + y^2 - 2y - 1$.