Polytech'Lille — PEIP — Calcul Scientifique
Un Algorithme d'Isolation de Racines Réelles — François Boulier — 2017

---

1 Introduction

Ce cours présente un algorithme d'isolation de racines réelles. L'algorithme dont il s'agit prend en entrée un polynôme $P(x)$ en une indéterminée x, à coefficients réels et de degré quelconque. Il retourne un ensemble d'intervalles avec la garantie que chaque intervalle retourné contient une et une seule racine réelle de $P(x)$. Un algorithme de ce type est implanté dans la fonction MAPLE `realroot` [6].

Dans ce cours, on suppose que toutes les racines de $P(x)$ sont simples. C'est une condition essentielle pour garantir l'arrêt de la méthode. Ce n'est pas une vraie restriction parce qu'il est toujours possible de transformer un polynôme $P_0(x)$ quelconque en un polynôme $P(x)$ ayant exactement les mêmes racines que $P_0(x)$, mais n'ayant que des racines simples : il suffit de diviser $P_0(x)$ (division euclidienne de polynômes, algorithmique) par le plus grand diviseur commun de $P_0(x)$ et de sa dérivée (le pgcd de deux polynômes peut se calculer par l'algorithme d'Euclide, qui n'est rien d'autre qu'une suite de divisions euclidiennes).

Le fait que les intervalles retournés isolent des racines *simples* d'un polynôme donné $P(x)$ présente un avantage très important : le polynôme $P(x)$ s'évalue en deux nombres de signes différents aux deux bornes de l'intervalle, ce qui permet de raffiner indéfiniment chaque intervalle d'isolation, après exécution de l'algorithme, grâce à la méthode dichotomique.

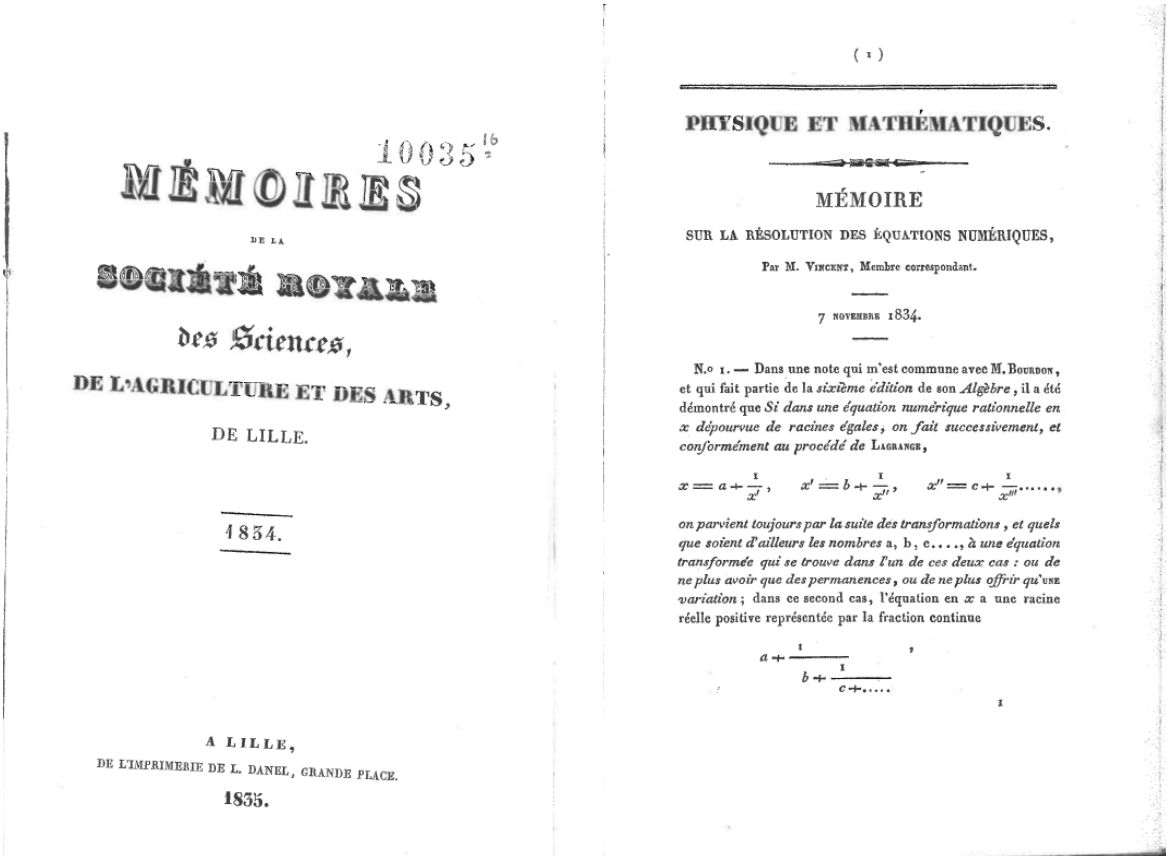
L'algorithme que nous allons donner n'isole que les racines réelles strictement positives de $P(x)$. Là non plus, ce n'est pas une vraie restriction puisque les racines réelles strictement négatives sont les racines réelles strictement positives de $P(-x)$.

La seule vraie restriction réside dans le fait que l'algorithme doit être capable de déterminer avec certitude si un coefficient de $P(x)$ est nul et, s'il ne l'est pas, de déterminer son signe. Concrètement, les coefficients peuvent être des nombres rationnels ou des nombres réels α, eux-mêmes présentés sous la forme d'un intervalle d'isolation et d'un polynôme $A(x)$ tel que $A(\alpha) = 0$. Cette dernière possibilité est utilisée dans le cadre d'algorithmes d'analyse topologique de courbes algébriques planes, par exemple.

La preuve d'un algorithme se décompose normalement en deux parties : la preuve que le résultat retourné est correct (preuve de correction) ; et la preuve que les calculs ne se poursuivent jamais indéfiniment (preuve d'arrêt). La preuve de correction repose essentiellement sur la *règle des signes* de Descartes [7].

C'est la preuve d'arrêt qui est compliquée. Comme de nombreuses versions d'algorithmes d'isolation ont été mises au point, il existe plusieurs preuves d'arrêt différentes. Autant que je sache, elles revêtent toutes un caractère commun. Tout d'abord, elles consistent à raisonner sur les racines complexes de $P(x)$ (ce qui est surprenant pour un algorithme d'isolation de racines réelles). Ensuite, elles utilisent toutes l'argument que l'algorithme a pour effet de « zoomer » sur certaines régions du plan complexe, « écartant » les racines complexes les unes des autres. Toutes ces preuves se concluent enfin par un argument qui montre que, si toutes les racines complexes sont suffisamment éloignées les unes des autres, alors un certain phénomène se produit qui arrête les calculs.

Il est remarquable que le premier (semble-t-il) à avoir eu cette idée, l'ait publiée dans les *Mémoires de la Société royale des sciences, de l'agriculture et des arts de Lille*, en 1834 (voir figure 1).



10035 (16)

MÉMOIRES

DE LA

SOCIÉTÉ ROYALE

des Sciences,

DE L'AGRICULTURE ET DES ARTS,

DE LILLE.

1834.

A LILLE,

DE L'IMPRIMERIE DE L. DANEL, GRANDE PLACE.

1835.

(1)

PHYSIQUE ET MATHÉMATIQUES.

MÉMOIRE

SUR LA RÉSOLUTION DES ÉQUATIONS NUMÉRIQUES,

Par M. Vincent, Membre correspondant.

7 novembre 1834.

N.o 1. — Dans une note qui m'est commune avec M. Bourdon, et qui fait partie de la *sixième édition* de son *Algèbre*, il a été démontré que *Si dans une équation numérique rationnelle en x dépourvue de racines égales, on fait successivement, et conformément au procédé de* Lagrange,

$$x = a + \frac{1}{x'}, \quad x' = b + \frac{1}{x''}, \quad x'' = c + \frac{1}{x'''} \ldots\ldots,$$

on parvient toujours par la suite des transformations, et quels que soient d'ailleurs les nombres a, b, c...., *à une équation transformée qui se trouve dans l'un de ces deux cas : ou de ne plus avoir que des permanences, ou de ne plus offrir qu'une variation*; dans ce second cas, l'équation en x a une racine réelle positive représentée par la fraction continue

$$a + \cfrac{1}{b + \cfrac{1}{c + \ldots\ldots}}$$

,

1

FIGURE 1 – La page de garde des *mémoires* de 1834 ainsi que la première page de l'article de Vincent [11]. Photocopie prise aux Archives Départementales du Nord, à Lille. La Société existe toujours en 2017 (son nom a un peu évolué). Il s'agit d'une des plus anciennes sociétés savantes françaises toujours en activité.

Il s'agit d'Alexandre Joseph Hidulphe Vincent, membre correspondant de la société lilloise [1]. Citons [4, page 264] : *Vincent's theorem can be used to show [5] that if an interval contains a single root and the remaining roots are sufficiently far away, a single variation will be obtained.*

L'algorithme que nous allons décrire est donc une variation sur une idée de Vincent, due à George Edwin Collins et Alkiviadis Akritas [3]. Je l'ai donc appelé algorithme de Vincent-Collins-Akritas. Il est parfois connu sous le nom d'algorithme d'Uspensky [10] mais cette appellation semble trompeuse [2]. La preuve d'arrêt décrite dans ce document (le théorème des deux cercles) est due à [4]. J'en ai eu connaissance via [3] [8].

1. À ma connaissance, c'est le texte le plus ancien qui lie la ville de Lille à l'informatique et, en particulier, à des algorithmes qui sont utilisés (et même de plus en plus utilisés) aujourd'hui.

2. James Victor Uspensky a mis au point un algorithme nettement moins efficace en s'inspirant des idées de Vincent. Après une longue enquête historique menée par Alkiviadis Akritas, à laquelle j'ai un peu participé, et où on a même pu suspecter un comportement répréhensible de la part d'Uspensky [1], il apparaît (discussion entre A. Akritas et une personne ayant connu Uspensky) qu'en toute bonne foi, Uspensky n'a eu accès qu'à des informations très succintes sur les travaux de Vincent, via le livre de Joseph Alfred Serret (voir Figure 7).

3. J'en profite pour remercier Fabrice Rouillier pour ses notes de cours ainsi que ses interventions dans le cours de DEUG *Systèmes polynomiaux, que signifie : résoudre ?*, créé à l'université Lille 1 et assuré plusieurs années, à la

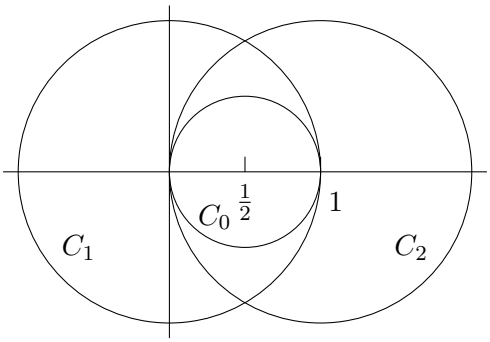


FIGURE 2 – Le cercle C_0 mentionné dans le théorème 2 et les deux cercles C_1 et C_2 mentionnés dans le théorème 3. Les trois cercles appartiennent au plan complexe.

2 La règle des signes

La règle des signes est publiée (sous une forme un peu plus faible) pour la première fois en 1636 dans [7]. Elle fut généralisée dans les années 1820 par Budan et Fourier dans le théorème qui porte aujourd'hui leur nom [2].

Théorème 1 *(règle des signes)*
Soient $P(x) \in \mathbb{R}[x]$ un polynôme non nul, $v(P)$ le nombre de variations de signe dans la liste des coefficients non nuls de $P(x)$ et $r(P)$ le nombre de racines réelles positives de $P(x)$ comptées avec multiplicités. Alors $v(P) \geq r(P)$.

Preuve Par récurrence sur le degré de $P(x)$.
Initialisation. si le degré est nul on a $v(P) = 0$ et $r(P) = 0$. Le théorème est donc vérifié.
Hérédité : On considère un polynôme

$$P(x) \quad = \quad a_d\, x^d + \cdots + a_1\, x + a_0\,.$$

de degré $d > 0$ et on suppose (hypothèse de récurrence) que le théorème est vérifié pour tout polynôme de degré strictement inférieur à d. On peut supposer $a_0 > 0$ (on ne change ni $r(P)$ ni $v(P)$ en divisant le polynôme par une puissance de x dans le cas $a_0 = 0$ ou en le multipliant par -1 si $a_0 < 0$). La dérivée de $P(x)$ s'écrit $P'(x) = d\, a_d\, x^{d-1} + \cdots + a_1$. On peut supposer $a_1 \neq 0$ (on ne change ni $r(P')$ ni $v(P')$ en divisant la dérivée par une puissance de x dans le cas $a_1 = 0$). Comme $\deg P' < \deg P$, l'hypothèse de récurrence s'applique et $v(P') \geq r(P')$. Entre deux racines réelles distinctes de $P(x)$ il existe au moins une racine de $P'(x)$ (cette remarque se généralise aux racines de $P(x)$ de multiplicité $k > 1$ en se rappelant que ce sont des racines de $P'(x)$ de multiplicité $k-1$). On voit donc que

$$r(P') + 1 \quad \geq \quad r(P)\,. \tag{1}$$

On distingue deux cas.

---

suite de la conférence ISSAC 2002.

Premier cas : $a_1 > 0$. Comme $a_0 > 0$, on voit que $v(P) = v(P')$. En $x = 0$, on a $P(0) = a_0 > 0$ et $P'(0) = a_1 > 0$. Comme a_1 est la pente de la tangente au graphe, en $x = 0$, on voit qu'entre 0 et $+\infty$, le graphe de $P(x)$ démarre avec une valeur positive et une pente positive. Donc $P'(x)$ a nécessairement au moins une racine positive strictement inférieure à la plus petite racine réelle positive de $P(x)$ et donc $r(P') \geq r(P)$. Par conséquent, $v(P) = v(P') \geq r(P') \geq r(P)$ (la première inégalité est due à l'hypothèse de récurrence et la seconde vient juste d'être établie) et le théorème est prouvé dans le cas $a_1 > 0$.
Second cas : $a_1 < 0$. Comme $a_0 > 0$, il y a dans la suite des coefficients de P, une variation de signe qui n'apparaît plus dans la suite des coefficients de P' et donc $v(P) = v(P') + 1$. Par conséquent, $v(P) = v(P') + 1 \geq r(P') + 1 \geq r(P)$ (la première inégalité est due à l'hypothèse de récurrence et la seconde à (1)) et le théorème est prouvé dans tous les cas. □

Corollaire 1 *Si $v(P) = 0$ alors $P(x)$ n'a aucune racine réelle strictement positive.*

Corollaire 2 *Si $v(P) = 1$ alors $P(x)$ a exactement une racine réelle strictement positive.*

Preuve La règle des signes implique que $r(P) \leq 1$. Comme $v(P) = 1$, les coefficients de tête et de queue de $P(x)$ sont de signes différents, ce qui implique que $P(x)$ s'annule au moins une fois sur $]0, +\infty[$ et donc que $r(P) \geq 1$. □

3 Appliquer la règle des signes sur l'intervalle $]0, 1[$

À tout réel $x \in]0, 1[$, on peut faire correspondre un réel $y \in]1, +\infty[$ en posant $x = \frac{1}{y}$. On peut même lui faire correspondre un réel $z \in]0, +\infty[$ en posant $y = z + 1$ (et donc $x = \frac{1}{z+1}$). Cette correspondance établit une bijection de l'intervalle $]0, 1[$ sur l'intervalle $]0, +\infty[$.

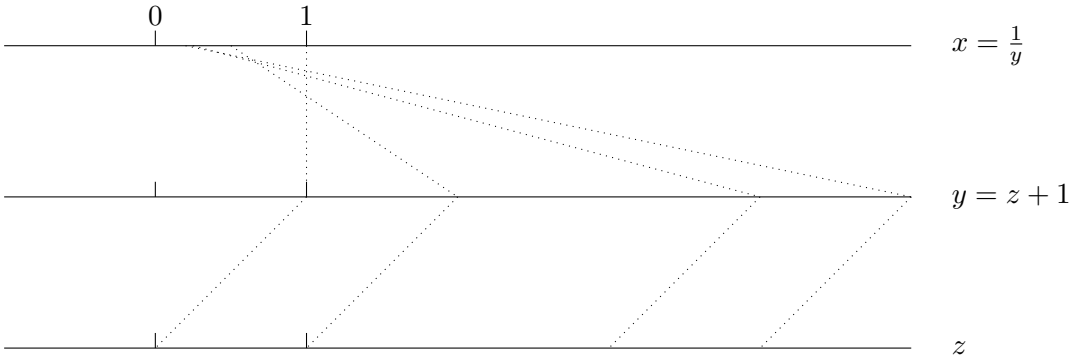


FIGURE 3 – Bijection entre $]0, 1[$ et $]0, +\infty[$. Soit $P(x)$ un polynôme quelconque de degré d. Les racines de $P(x)$ appartenant à $]0, 1[$ sont en bijection avec les racines de $R(z)$ appartenant à $]0, +\infty[$ où $R(z)$ est défini par : $R(z) = Q(z + 1)$ et $Q(y) = y^d\, P(\frac{1}{y})$.

Soit $P(x)$ un polynôme de degré d. À toute racine $x \in]0, 1[$ de $P(x)$, on peut faire correspondre une racine $y \in]1, +\infty[$ du polynôme $Q(y)$ défini par $Q(y) = y^d\, P(1/y)$ (la multiplication par y^d a uniquement pour but d'éviter l'introduction de fractions rationnelles). On peut même lui faire correspondre une racine $z \in]0, +\infty[$ du polynôme $R(z)$ défini par $R(z) = Q(z+1)$. Là encore, cette

correspondance établit une bijection de l'ensemble des racines de $P(x)$ appartenant à l'intervalle $]0,1[$ sur l'ensemble des racines réelles strictement positives de $R(z)$. Voir Figure 3.

Par conséquent, le nombre $v(R)$ de variations de signe dans la suite des coefficients non nuls de $R(z)$, qui borne le nombre de racines réelles strictement positives de $R(z)$, borne aussi le nombre de racines de $P(x)$ appartenant à l'intervalle $]0,1[$.

La définition et la proposition suivante synthétisent ces observations.

Définition 1 *Soient $P(x)$ un polynôme de degré d et $R(z) = Q(z+1)$ où $Q(y) = y^d\, P(\frac{1}{y})$. On note $v_{01}(P) = v(R)$.*

Proposition 1 *Le nombre de racines de $P(x)$ appartenant à l'intervalle $]0,1[$ est inférieur ou égal à $v_{01}(P)$.*

4 Ramener toutes les racines dans $]0,1[$

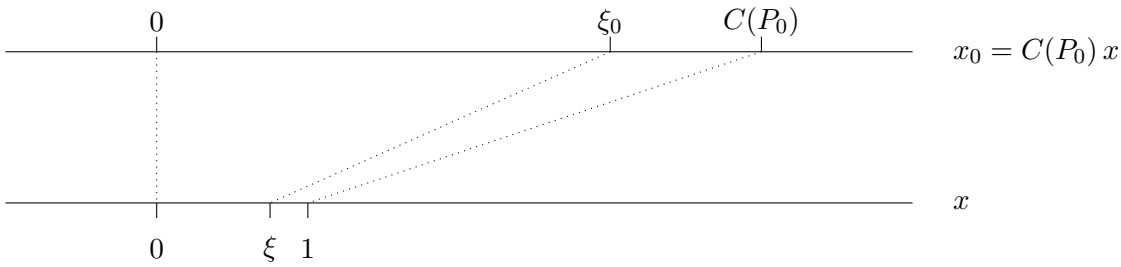


FIGURE 4 – Bijection entre $]0, C(P_0)[$ et $]0,1[$. Soient $P_0(x_0)$ un polynôme quelconque et $P(x) = P_0(C(P_0)\, x)$. Les racines réelles strictement positives de $P_0(x_0)$ sont en bijection avec les racines de $P(x)$ appartenant à $]0,1[$.

La borne suivante n'est pas optimale mais sa preuve a l'avantage d'être simple.

Proposition 2 *(Cauchy, 1829)*
Soient $P(x) \in \mathbb{C}[x]$ un polynôme à coefficients complexes et $\alpha \in \mathbb{C}$ une de ses racines. Notons

$$C(P) \;=\; \sum_{i=0}^{d} \left| \frac{a_i}{a_d} \right| .$$

Alors $|\alpha| < C(P)$.

Preuve Comme $C(P) \geq 1$, il suffit de considérer une racine α de $P(x)$ de valeur absolue (ou module pour les complexes) supérieure à 1. On a

$$a_d\, \alpha^d \;=\; -(a_{d-1}\, \alpha^{d-1} + \cdots + a_1\, \alpha + a_0)\, .$$

D'après l'inégalité triangulaire

$$|a_d|\, |\alpha|^d \;\leq\; |a_{d-1}|\, |\alpha|^{d-1} + \cdots + |a_1|\, |\alpha| + |a_0|\, .$$

Comme $|\alpha| \geq 1$, on peut majorer chaque terme de la somme en le multipliant par une puissance appropriée de $|\alpha|$ pour obtenir

$$|a_d|\,|\alpha|^d \;\leq\; (|a_{d-1}| + \cdots + |a_0|)\,|\alpha|^{d-1}\,.$$

Une borne valable pour le cas $|\alpha| \geq 1$ s'obtient en divisant les deux membres de l'inégalité par $|a_d|\,|\alpha|^{d-1}$. On ajoute un terme supplémentaire (valant 1) à la somme, pour obtenir une borne valable dans tous les cas. □

La proposition suivante est illustrée Figure 4.

Proposition 3 *Soient $P_0(x_0)$ un polynôme à coefficients réels et $P(x) = P_0(C(P_0)\,x)$. Il y a bijection entre les racines réelles strictement positives ξ_0 de $P_0(x_0)$ et les racines ξ de $P(x)$ appartenant à l'intervalle $]0,1[$. La bijection est donnée par $\xi_0 = C(P_0)\,\xi$.*

Preuve C'est un corollaire de la proposition 2. □

5 Cas de deux variations de signe (ou plus)

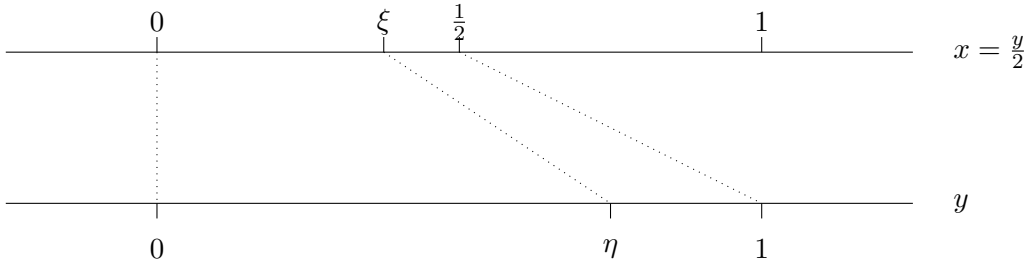


FIGURE 5 – Bijection entre $]0, \frac{1}{2}[$ et $]0,1[$. Soient $P(x)$ un polynôme quelconque et $Q(y) = P(\frac{y}{2})$. Les racines ξ de $P(x)$ appartenant à $]0, \frac{1}{2}[$ sont en bijection avec les racines η de $Q(y)$ appartenant à $]0,1[$.

Les deux propositions suivantes sont illustrées Figures 5 et 6.

Proposition 4 *Soient $P(x)$ un polynôme à coefficients réels et $Q(y) = P(\frac{y}{2})$. Il y a bijection entre les racines ξ de $P(x)$ appartenant à l'intervalle $]0, \frac{1}{2}[$ et les racines η de $Q(y)$ appartenant à l'intervalle $]0,1[$. La bijection est donnée par $\xi = \frac{\eta}{2}$.*

Proposition 5 *Soient $P(x)$ un polynôme à coefficients réels et $Q(y) = P(\frac{y+1}{2})$. Il y a bijection entre les racines ξ de $P(x)$ appartenant à l'intervalle $]\frac{1}{2}, 1[$ et les racines η de $Q(y)$ appartenant à l'intervalle $]0,1[$. La bijection est donnée par $\xi = \frac{\eta+1}{2}$.*

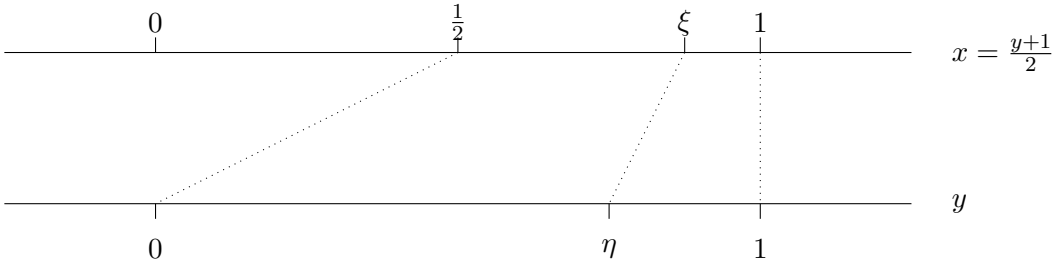


FIGURE 6 – Bijection entre $]\frac{1}{2}, 1[$ et $]0, 1[$. Soient $P(x)$ un polynôme quelconque et $Q(y) = P(\frac{y+1}{2})$. Les racines ξ de $P(x)$ appartenant à $]\frac{1}{2}, 1[$ sont en bijection avec les racines η de $Q(y)$ appartenant à $]0, 1[$.

6 L'algorithme de Vincent-Collins-Akritas

Il applique les propositions précédentes en faisant attention à ne pas perdre de racine, dans le cas où $\frac{1}{2}$ serait racine de $P(x)$.

```
function Vincent_Collins_Akritas (P_0(x_0))
Retourne une liste d'intervalles isolant les racines réelles strictement positives de P_0(x_0)
Les intervalles sont soit ouverts soit réduits à un point
begin
  P(x) := P_0(C(P_0) x)
  return isole_01 (P(x), ]0, C(P_0)[)
end

function isole_01 (P(x), ]a, b[)
Sous–fonction de Vincent_Collins_Akritas.
Toute racine ξ ∈ ]0, 1[ de P(x) correspond à une racine ξ_0 = a + ξ (b − a) ∈ ]a, b[ de P_0(x_0).
begin
  n := v_01 (P)
  if n = 0 then
    return ∅
  elif n = 1 then
    return {]a, b[}
  else
    Q(x) := P(x/2)
    R(x) := P((x+1)/2)
    m := (a+b)/2
    if P(1/2) ≠ 0 then
      return isole_01 (Q, ]a, m[) ∪ isole_01 (R, ]m, b[)
    else
      return isole_01 (Q, ]a, m[) ∪ isole_01 (R, ]m, b[) ∪ {[m, m]}
    fi
  fi
end
```

7 La preuve d'arrêt

À chaque appel récursif, l'algorithme isole_{01} est amené à considérer un polynôme dont les racines sont de plus en plus éloignées les unes des autres (à condition bien sûr que toutes les racines soient simples). Cette observation vaut pour les racines réelles du polynôme $P(x)$, comme le montrent les figures 5 et 6. Elle vaut aussi pour les racines complexes.

Pour montrer l'arrêt de l'algorithme, il suffit donc de montrer que, si toutes les racines complexes de $P(x)$ sont « suffisamment éloignées », alors $v_{01}(P)$ vaut soit zéro, soit un.

La fonction v_{01} retourne le nombre de variations de signe d'un polynôme $R(z)$ dont les racines sont liées à celles du polynôme $P(x)$ par le changement de variable suivant :

$$x \;=\; \tfrac{1}{z+1} \qquad z \;=\; \tfrac{1}{x} - 1\,.$$

Lemme 1 *Si $x = a + i\,b$ est un nombre complexe situé à l'extérieur du cercle C_0 de rayon $\frac{1}{2}$, centré en $(\frac{1}{2}, 0)$ (voir Figure 2), alors $z = \frac{1}{x} - 1$ est à partie réelle strictement négative.*

Preuve Les coordonnées de x satisfont donc à (la formule de gauche donne le carré de la distance au centre de C_0) :

$$\begin{aligned} \left(a - \frac{1}{2}\right)^2 + b^2 &> \left(\frac{1}{2}\right)^2, \\ a^2 + b^2 &> a\,. \end{aligned} \tag{2}$$

On a (l'inégalité étant due à (2)) :

$$\frac{1}{x} \;=\; \frac{a - i\,b}{a^2 + b^2} \qquad \text{et donc} \quad \Re\left(\frac{1}{x}\right) \;=\; \frac{a}{a^2 + b^2} \;\leq\; \frac{a^2 + b^2}{a^2 + b^2} \;=\; 1\,.$$

La partie réelle de z est donc strictement négative. □

Le lemme ci-dessus a pour corollaire le théorème suivant, repris de [4, Theorem 2, page 267]. Noter que sa preuve nécessite la prise en compte des racines complexes de $P(x)$, pas seulement les réelles.

Théorème 2 *Soit $P(x)$ un polynôme à coefficients réels n'ayant aucune racine dans le cercle C_0 de rayon $\frac{1}{2}$, centré en $(\frac{1}{2}, 0)$. Alors $v_{01}(P) = 0$.*

Preuve Notons $d = \deg P$ et $R(z) = z^d\,P(1/(z+1))$ de telle sorte que $v_{01}(P) = v(R)$. Le polynôme $R(z)$ n'a que des racines à partie réelle négative. Le polynôme $R(z)$ est donc un produit de facteurs de la forme soit $z - a$, soit $(z - a - i\,b)(z - a + i\,b) = z^2 - 2\,a\,z + a^2 + b^2$ avec $a < 0$, c'est-à-dire un produit de facteurs dont tous les coefficients sont positifs. Par conséquent, tous les facteurs de $R(z)$ ont même signe et $v(R) = 0$. □

Le théorème suivant est repris de [4, Theorem 1, page 267].

Théorème 3 *(théorème des deux cercles)*
Soit $P(x)$ un polynôme à coefficients réels ayant exactement une racine réelle dans l'intervalle $]0, 1[$ et toutes ses racines non réelles à l'extérieur de $C_1 \cup C_2$ où C_1 et C_2 sont les deux cercles de rayon 1, centrés en $(0, 0)$ et $(1, 0)$. Alors $v_{01}(P) = 1$.

Preuve Notons $d = \deg P$ et $R(z) = z^d\, P(1/(z+1))$ de telle sorte que $v_{01}(P) = v(R)$. Le polynôme $R(z)$ a exactement une racine réelle a strictement positive. Toutes les autres racines de $R(z)$ sont à partie réelle strictement négative (voir le lemme ci-dessus). Le polynôme $R(z)$ peut se construire en incorporant ses racines les unes après les autres. Plus précisément, il existe un indice j tel que $R(z) = R_j(z)$ où :

$$\left\{\begin{array}{rcll} R_0(z) & = & z-a\,, & \\ R_{i+1}(z) & = & R_i(z)\,(z-\gamma) & \text{si } \gamma \text{ est une racine réelle} \\ & = & R_i(z)\,(z-\gamma)\,(z-\bar{\gamma}) & \text{si } \gamma \text{ est une racine non réelle}\,. \end{array}\right.$$

Pour montrer le théorème, il suffit de montrer que $v(R_i) = 1$ pour tout $i \geq 0$. Cette propriété est vérifiée pour $R_0(z)$. On suppose qu'elle est vérifiée pour $R_i(z)$ et on montre qu'elle est vraie pour $R_{i+1}(z)$.
Le cas où γ est réelle. Le facteur $z-\gamma$ a tous ses coefficients strictement positifs. Soient $e = \deg R_i$ et

$$R_i(z) \;=\; a_e\, z^e + a_{e-1}\, z^{e-1} + \cdots + a_j\, z^j - a_{j-1}\, z^{j-1} - \cdots - a_1\, z - a_0\,.$$

On suppose le coefficient dominant a_e positif pour simplifier, tous les a_k positifs ou nuls, et l'unique changement de signe entre les coefficients a_j et a_{j-1}. Notons $\lambda = -\gamma$ de telle sorte que $R_{i+1}(z) = R_i(z)\,(z+\lambda)$ avec $\lambda > 0$. On obtient :

$$\begin{array}{rcl} R_{i+1}(z) & = & \underbrace{a_e\, z^e + (a_{e-1} + \lambda\, a_e)\, z^{e-1} + \cdots + (a_j + \lambda\, a_{j+1})\, z^j}_{\text{coefficients}\geq 0} + (-a_{j-1} + \lambda\, a_j)\, z^{j-1} \\ & & + \underbrace{(-a_{j-2} - \lambda\, a_{j-1})\, z^{j-2} + \cdots + (-a_0 - \lambda\, a_1)\, z - \lambda\, a_0}_{\text{coefficients}\leq 0}\,. \end{array}$$

Le nombre de variations de signes de $R_{i+1}(z)$ est donc égal à 1, quel que soit le signe de $-a_{j-1} + \lambda\, a_j$.
Le cas où γ est non réelle. Le nombre γ est de la forme $\gamma = 1/\beta - 1$ où le nombre complexe $\beta = a + i\, b$ est une racine de $P(x)$ à l'extérieur de $C_1 \cup C_2$. Les coordonnées de β vérifient donc $a^2 + b^2 > 1$ et $(a-1)^2 + b^2 > 1$. Le polynôme $R_{i+1}(z)$ est de la forme $R_i(z)\, F(z)$ où

$$F(z) \;=\; (z-\gamma)\,(z-\bar{\gamma}) \;=\; z^2 + \underbrace{\left(\frac{(a^2+b^2) + (a^2 - 2\,a + b^2)}{a^2+b^2}\right)}_{s}\, z + \underbrace{\frac{1 + (a^2 - 2\,a + b^2)}{a^2+b^2}}_{t}.$$

On a $s > t$ puisque $a^2 + b^2 > 1$ (β à l'extérieur de C_1). Le numérateur de t s'écrit aussi $(a-1)^2 + b^2$. On a donc d'une part $t > 0$, d'autre part $s > 1$ puisque $(a-1)^2 + b^2 > 1$ (β à l'extérieur de C_2).

Le polynôme $R_{i+1}(z) = R_i(z)\,(z^2 + s\, z + t)$ est de la forme :

$$\begin{array}{rcl} R_{i+1}(z) & = & \underbrace{a_e\, z^e + (a_{e-1} + s\, a_e)\, z^{e-1} + (a_{e-2} + s\, a_{e-1} + t\, a_e)\, z^{e-2} + \cdots + (a_j + s\, a_{j+1} + t\, a_{j+2})\, z^j}_{\text{coefficients}\geq 0} \\ & & + (-a_{j-1} + s\, a_j + t\, a_{j+1})\, z^{j-1} + (-a_{j-2} - s\, a_{j-1} + t\, a_j)\, z^{j-2} \\ & & \underbrace{+ (-a_{j-3} - s\, a_{j-2} - t\, a_{j-1})\, z^{j-3} + \cdots + (-a_0 - s\, a_1 - t\, a_2)\, z^2 + -s\, a_0 - t\, a_1\, z - t\, a_0}_{\text{coefficients}\leq 0} \end{array}$$

Le nombre de variations de signes de $R_{i+1}(z)$ est donc supérieur ou égal à 1. Pour montrer qu'il est égal à 1, il suffit de montrer que

$$-a_{j-1} + s\,a_j + t\,a_{j+1} \quad > \quad -a_{j-2} - s\,a_{j-1} + t\,a_j$$

La différence entre les deux membres de l'inégalité est égale à $a_{j-2} + (s-1)\,a_{j-1} + (s-t)\,a_j + t\,a_{j+1}$. Comme $s > 1$ et $s > t$, cette différence est toujours positive ou nulle.

On a donc montré que $v(R_i) = 1$ pour tout i et donc que $v_{01}(P) = 1$. □

Références

[1] Alkiviadis G. Akritas. There is no Uspensky's method. In *proceedings of ISSAC 1986*, 1986.

[2] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer Verlag, 2003.

[3] George Edwin Collins and Alkiviadis G. Akritas. Polynomial real root isolation using Descartes'rule of signs. In *Proceedings of ISSAC 1976*, pages 272–275, Yorktown Heights NY, 1976.

[4] George Edwin Collins and Jeremy R. Johnson. Quantifier Elimination and the Sign Variation Method for Real Root Isolation. In *Proceedings of ISSAC 1989*, pages 264–271, 1989.

[5] George Edwin Collins and Rüdiger Georg Konrad Loos. *Real zeros of polynomials*, pages 83–94. Springer Verlag, Wien–New York, 1982.

[6] The MapleSoft Company. Help page of the realroot function. `http://www.maplesoft.com/support/help/Maple/view.aspx?path=realroot&L=F`.

[7] René Descartes. *Géométrie*. 1636.

[8] Fabrice Rouillier. La méthode de Uspensky, 2002. Note de cours, communication privée.

[9] Joseph Alfred Serret. *Cours d'Algèbre Supérieure*. Gauthier-Villars, quatrième edition, 1877.

[10] James Victor Uspensky. *Theory of Equations*. McGraw – Hill Co., New–York, 1948.

[11] Alexandre Joseph Hidulphe Vincent. Mémoire sur la résolution des équations numériques. *Mémoires de la Société royale des sciences, de l'agriculture et des arts de Lille*, pages 1–34, 1834. L'article est daté de 1834 mais le volume de 1835. Il est republié dans le Journal de Mathématiques Pures et Appliquées, 1836.

et l'on pourra faire

$$\frac{G_{k+1}+E_{k+1}}{G_k+E_k}=\frac{G_{k+1}}{G_k}+e_{k+1}=\frac{m}{k+1}-1+e_{k+1},$$

e_{k+1} étant un nombre réel qui peut devenir moindre que toute quantité donnée en prenant n suffisamment grand. Désignons maintenant par $(\lambda-1)g$ la racine positive de notre transformée; il est évident que cette transformée s'obtiendra en égalant à zéro le produit du polynôme (6) par $x-(\lambda-1)g$; on a, à cause de $G_0=1$,

$$(7)\quad \begin{cases} x^m+\left(\frac{m}{1}+e_1-\lambda\right)G_0 g x^{m-1}+\left(\frac{m}{2}+e_2-\lambda\right)(G_1+E_1)g^2x^{m-2}+\dots \\ \quad+\left(\frac{m}{m-1}+e_{m-1}-\lambda\right)(G_{m-2}+E_{m-2})g^{m-1}x \\ \qquad -(\lambda-1)(G_{m-1}+E_{m-1})g^m=0. \end{cases}$$

Le premier terme de cette équation a le signe + et le dernier terme a le signe —; d'ailleurs, les quantités e_1, e_2, ..., E_1, E_2, ... peuvent être supposées aussi petites que l'on voudra, et, si le coefficient de l'un des termes compris entre le premier et le dernier est nul ou négatif, il est évident que tous les coefficients qui suivent seront négatifs. L'équation (7) n'a donc qu'une seule variation, ce qui achève la démonstration du théorème énoncé.

Ainsi que l'a montré Vincent, le théorème précédent suffit pour opérer la séparation des racines, sans que l'on soit obligé d'en déterminer le nombre *a priori*, ou de leur assigner des limites, pourvu qu'afin de s'épargner des essais inutiles on fasse un usage convenable du théorème de Budan; mais nous renverrons au Mémoire de l'auteur, pour le développement de cette méthode.

FIGURE 7 – Victor Uspensky aurait eu connaissance des travaux de Vincent via le livre de Serret [9]. L'unique référence à Vincent se trouve page 368.