1. Racines Réelles de polynômes de $\mathbb{Z}[X]$

Si on se donne un polynôme sans facteurs carrés à coefficients dans $\mathbb{R}$ et un intervalle suffisamment petit autour de l'une de ses racines réelles, alors le polynôme prend des valeurs opposées aux bornes de l'intervalle. Le plus ancien algorithme d'isolation de zéros réels à coefficients réels est certainement dû à Kronecker et est basé sur ce principe élémentaire:

- on définit un intervalle $[A, B]$ contenant toutes les racines de P,
- on découpe cet intervalle en petits intervalles dont le longueur est inférieure à la distance minimale entre deux racines de P.
- on calcule alors le signe de P aux bornes de ces intervalles (supposant P sans facteurs multiples) pour détecter les intervalles contenant 1 racine.

Cette méthode est d'une inefficacité notoire puisque l'utilisation exclusive de bornes rend le nombre de calculs (evaluations du signe de P) exponentiel en le degré du polynôme. Un remède simple à ce comportement est d'effectuer une dichotomie de $[A, B]$, à condition toutefois de pouvoir borner ou calculer le nombre de zéros dans un intervalle donné.

1.1. Rappels utiles.

$P, Q \in \mathbb{R}[X], \alpha = (\alpha_1, ..., \alpha_p)$ et $\beta = (\beta_1, ..., \beta_q)$ racines de P, Q.

Théorème 1. $\mathrm{res}(P,\ Q) = \mathrm{lc}(P)^{d_q}\ \mathrm{lc}(Q)^{d_p} \prod_{i=1}^{d_p} \prod_{j=1}^{d_q} (\alpha_i - \beta_j) = \mathrm{lc}(P)^{d_q} \prod_{i=1}^{d_p} Q(\alpha_i) = \mathrm{lc}(Q)^{d_p} \prod_{i=1}^{d_q} P(\beta_i)$

Démonstration. $\mathrm{Res}(P, Q\,(X-\alpha)) = P(\alpha)\mathrm{Res}(P, Q)$ (essentiellement ...) □

Définition 2. *Discriminant de $P \in \mathbb{D}[X]$ avec $\mathbb{D}$ anneau intègre (en général factoriel)*
$\mathrm{Discriminant}(P) = \mathrm{lc}(P)^{2d_p-2} \prod_{1 \leqslant i < j \leqslant d_p} (\alpha_i - \alpha_j)^2 \in \mathbb{D}$

Proposition 3. $\mathrm{lc}(P)\,\mathrm{Dis}(P) = (-1)^{\frac{p(p-1)}{2}}\,\mathrm{Res}(P, P')$

1.2. Borner les racines réelles

Un certain nombre de méthodes pour l'isolation des zéros réels de polynômes en une variables sont à caractère dichotomique. Précisément, il s'agit en général d'isoler les racines d'un polynôme étant donné un intervalle de départ qui sera découpé en intervalles plus petits. Pour être sûrs d'isoler toutes les racines d'un polynôme donné, il faut être en mesure de fournir un intervalle les contenant toutes. Nous donnons ici une collection de bornes utiles. Dans toute cette partie, on suppose que $P(X) = \sum_{i=0}^{n} a_i X^i$ est un polynôme de $\mathbb{R}[X]$. La borne la plus simple à calculer est certainement la suivante :

Proposition 4. *Si α est une racine complexe de P et que $a_n = 1$, alors $|\alpha| < 1 + \max_{i=0}^{n}(|a_i|)$.*

Démonstration. Supposons $A = \max_{i=0}^{n-1}(|a_i|)$. Pour tout $x \in \mathbb{R}$ tel que $|x| \geq A + 1$,

$$|P(x)| \geq |x|^n - A\,(|x|^{n-1} + ... + 1) = |x|^n - \frac{A(|x|^n) - 1}{|x| - 1}.$$

Comme $|x| \geq A + 1$, alors $1 \geq A\,/\,(|x| - 1)$ et donc $|x|^n \geq A|x|^n\,/\,(|x| - 1)$, ce qui implique $|P(x)| \geq A/(|x| - 1) > 0$. □

Note : il y a beaucoup d'autres bornes connues pour majorer le module des racines complexes et/ou réelles d'un polynôme en une variable, certaines seront vues en TD.

1.3. Séparation des racines

Pour appliquer la méthode (simpliste) de Kronecker résumée plus haut à un polynôme à coefficients entiers (par exemple), il faut être en mesure de déterminer *a priori* la distance entre les racines réelles du polynôme étudié. Cette information peut être calculée directement à partir des coefficients du polynôme.

PROPOSITION 5. *Soit $P \in \mathbb{Z}[X]$ de degré d, sans facteur carré, ne s'annulant pas en 0, sans facteurs carrés, et dont les racines sont notées $\alpha_1, \dots \alpha_d$.*

$$\mathrm{sep}(P) \geq \sqrt{\frac{3}{d^d+2}} \cdot \frac{1}{M(P)^{d-1}}$$

où $M(P) = |a_n| \prod_{k=1}^{d} \max(1, |\alpha_k|)$.

Remarque : on impose $\mathbb{Z}[X]$ par facilité (utilisation de Discriminant $\neq 0 \Rightarrow$ Discriminant $\geqslant 1$) mais le résultat reste vrai car on peut montrer que $M(P) \leqslant \|P\|_2$ (résultat un peu plus long à montrer)

Démonstration. Notons $\alpha_1, \dots \alpha_d$ les racines de P. Rappelons que la matrice suivante est dite de Vandermonde :

$$P_d = \begin{bmatrix} 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_d \\ \vdots & & \vdots \\ \alpha_1^{d-1} & \dots & \alpha_d^{d-1} \end{bmatrix}$$

Remarquons que $\det(P_d)^2 = (\prod_{i<j} (\alpha_i - \alpha_j)^2) = \frac{\mathrm{Discrim}(P)}{a_d^{2d-2}}$. On ordonne les racines de P de telle sorte que
$|\alpha_1| \geq \dots \geq |\alpha_m| \geq 1 \geq |\alpha_{m+1}| \geq \dots |\alpha_d|$.

En retranchant la j-ième colonne de P_d à la $i$ième, on peut voir que $(\alpha_i - \alpha_j)$ divise $\det(P_d)$ et que

$$\frac{\det(P_d)}{(\alpha_i - \alpha_j)} = \begin{vmatrix} 1 & \dots & 1 & 0 & 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_{i-1} & q_2 & \alpha_{i+1} & \dots & \alpha_d \\ \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{d-1} & \dots & \alpha_{i-1}^{d-1} & q_{d-1} & \alpha_{i-1}^{d+1} & \dots & \alpha_d^{d-1} \end{vmatrix}$$

avec $q_l = \alpha_i^{l-1} + \alpha_i^{l-2}\alpha_j + \dots + \alpha_i \alpha_j^{l-2} + \alpha_j^{l-1}$.

En divisant les m premières colonnes par α_i^{d-1} $i = 1 \dots m$ de sorte à avoir des entrées de valeur absolue inférieure à 1 sauf peut-être à la i-ième colonne, on peut voir que :

$$\left| \frac{\det(P_d)}{(\alpha_i - \alpha_j) \prod_{i=1\dots m} \alpha_i^{d-1}} \right|^2 \leq \prod_{j=1}^{d} |C_j|^2 \leq d^{d-1} \underbrace{\sum_{i=0}^{d-1} i^2}_{|C_l|}$$

et donc que

$$\frac{\mathrm{Discrim}(P_d)}{a_d^{2d-2} |(\alpha_i - \alpha_j) \prod_{i=1\dots m} \alpha_i^{d-1}|^2} \leq \frac{d^{d-1}\, d\,(d-1)\,(2\,d-1)}{6}.$$

Ainsi, $|\alpha_i - \alpha_j|^2 \geq \frac{\mathrm{Discrim}(P)}{|a_d^{d-1} \prod_{i=1\dots m} \alpha_i^{d-1}|^2} \cdot \frac{3}{d^{d+2}}$. Comme $\mathrm{Discrim}(P) \in \mathbb{Z}^{*+}$, alors $|\alpha_i - \alpha_j|^2 \geq \frac{1}{|a_d^{d-1} \prod_{i=1\dots m} \alpha_i^{d-1}|^2} \cdot \frac{3}{d^{d+2}}$, ce qui montre l'inégalité :

$$\mathrm{sep}(P)^2 \geq \frac{3}{(M(P)^{d-1})^2} \cdot \frac{1}{d^{d+2}}.$$

□

La borne ci-dessus n'est pas directement exploitable pour le calcul. Le corollaire suivant fournit une méthode pour minorer le séparateur des racines :

Corollaire 6. *Soit $P \in \mathbb{Z}[X]$ de degré d, ne s'annulant pas en 0, sans facteurs carrés, et dont les racines sont notées $\alpha_1, \dots \alpha_d$.*

$$\operatorname{sep}(P) \geq \sqrt{\frac{3}{d^d+2}} \cdot \frac{1}{||P||_2^{d-1}}$$

où $||P||_2 = \sqrt{\sum_{i=0}^{d} a_i^2}$.

Pour montrer ce résultat, il suffit de montrer que $M(P) \leq ||P||_2$. Pour ce faire, on a besoin d'un petit lemme technique :

Lemme 7. *Pour tout $z \in \mathbb{C}^*$, $||(\overline{z}x-1)P(x)||_2 = ||(x-z)P(x)||_2$.*

Démonstration. On pose $a_{-1} = 0 = a_{d+1}$.

$$\begin{aligned}
||(\overline{z}x-1)P(x)||_2^2 &= \sum_{k=0}^{d+1} |\overline{z}\,a_{k-1} - a_k|^2 = \sum_{k=0}^{d+1} (\overline{z}\,a_{k-1} - a_k)\,\overline{(\overline{z}\,a_{k-1} - a_k)} \\
&= \sum_{k=0}^{d+1} |z|^2 a_{k-1}^2 + |a_k|^2 - 2\operatorname{Re}(z\overline{a_{k-1}}a_k) \\
&= (|z|^2+1)||P||_2^2 - \sum_{k=0}^{d+1} 2\operatorname{Re}(z\overline{a_{k-1}}a_k)
\end{aligned}$$

□

$$\begin{aligned}
||(x-z)P(x)||_2^2 &= \sum_{k=0}^{d+1} |a_{k-1} - z\,a_k|^2 = \sum_{k=0}^{d+1} (a_{k-1} - z\,a_k)\,\overline{(a_{k-1} - z\,a_k)} \\
&= \sum_{k=0}^{d+1} a_{k-1}^2 + |z|^2|a_k|^2 - 2\operatorname{Re}(z\overline{a_{k-1}}a_k) \\
&= (|z|^2+1)||P||_2^2 - \sum_{k=0}^{d+1} 2\operatorname{Re}(z\overline{a_{k-1}}a_k)
\end{aligned}$$

Démonstration. (du corollaire) On suppose que $P(x) = a_n \prod_{i=1}^{d} (X - \alpha_i)$.

Pour $d > m \geqslant 0$, on pose $Q(X) = a_n \prod_{i=1}^{m} (\bar{\alpha_i}X - 1) \prod_{i=m+1}^{d} (x - \alpha_i)$.

D'après le lemme précédent, $||Q(x)||_2 = ||P(x)||_2$.

Le terme de tête de $Q(x)$ s'écrit $a_n \prod_{i=1}^{m} (\bar{\alpha_i})$ et le terme constant de $Q(x)$ s'écrit $a_n \prod_{i=m+1}^{d} (\alpha_i)$.

En particulier $||Q||_2^2 \geq |a_n|^2 \prod_{i=1}^{m} |\bar{\alpha_i}|^2 + |a_n|^2 \prod_{i=m+1}^{d} |\alpha_i|^2$.

On peut choisir m tel que $|\alpha_i| \geq 1$, $\forall i > m$.

Dans ce cas, $M(P)^2 = |a_n|^2 \prod_{i=m+1}^{d} |\alpha_i|^2$ et donc $||Q||_2^2 \geq M(P)^2$. □

1.4. Nombre de racines réelles d'un polynôme.

La plupart des méthodes exposées dans cette partie utilisent la notion de variations de signes dans une suite de scalaires, en particulier dans la suite des coefficients de polynomes :

Définition 8. *On définit le signe, sign(a), d'un élément $a \in \mathbb{R}$ par un entier vallant 0 si $a = 0$, 1 si $a > 0$ et -1 si $a < 0$. Le nombre de changements de signes* Var(a)*, dans une suite, $a = a_1, \cdots, a_k$, d'éléments de $\mathcal{R} \setminus \{0\}$ est définie par induction sur k par:*

$$\begin{aligned}
&\operatorname{Var}(a_1) = 0 \\
&\operatorname{Var}(a_1, \cdots, a_k) = \begin{cases} \operatorname{Var}(a_1, \cdots, a_{k-1}) + 1 & \text{si} \quad \operatorname{sign}(a_{k-1}\,a_k) = -1 \\ \operatorname{Var}(a_1, \cdots, a_{k-1}) & \text{sinon} \end{cases}
\end{aligned}$$

Cette définition s'étend à une suite a d'éléments de $\mathcal{R}$ non tous nuls: on note b la suite obtenue en supprimant les zéros dans la suite a et on définit Var$(a) =$ Var(b)*. Par exemple* Var $(1, -1, 2, 0, 0, 3, 4, -5, -2, 0, 3) =$ Var$(1, -1, 2, 3, 4, -5, -2, 3) = 4$.

Enfin, pour $P = \sum_{i=0}^{p} \in \mathcal{R}[X]$, on définit Var$(P) =$ Var$(a_0, ..., a_p)$.

DÉFINITION 9. *Soit $P \in \mathbb{R}[X]$. Une suite de Sturm associée à P pour un intervalle donné $[a,b] \in \mathbb{R}$ est une suite de polynômes de $\mathbb{R}[X]$ $[f_0(X), \dots f_s(X)]$ tels que :*

- *(i) $f_0 = P$*
- *(ii) f_s n'a aucune racine réelle dans $[a,b]$;*
- *(iii) pour $0 < i < s$, si $\alpha \in [a,b]$ est tel que $f_i(\alpha) = 0$, alors $f_{i-1}(\alpha)\, f_{i+1}(\alpha) < 0$:*
- *(iv) si $\alpha \in [a,b]$ est tel que $f_0(\alpha) = 0$, alors*

$$\begin{cases} f_0\, f_1\,(\alpha - \epsilon) < 0 \\ f_0\, f_1\,(\alpha + \epsilon) > 0 \end{cases}$$

pour toute valeur de ϵ suffisamment petite ($f_0\, f_1$ est une fonction croissante en α).

PROPOSITION 10. *Soit $P \in \mathbb{R}[X]$ et $[f_0(X), \dots f_s(X)]$ une suite de Sturm associée à P sur un intervalle borné $[a,b]$.*
$\mathrm{Var}(f_0(a), \dots, f_s(a)) - V_{\mathrm{ar}}(f_0(b), \dots, f_s(b))$ est égal au nombre de racines réelles de P dans $]a,b]$.

Démonstration. Soit $\alpha \in [a,b]$.
Si $f_i(\alpha) \neq 0$ pour $0 \leq i \leq s$, alors $V_{stu}(P(c))$ est constant sur un voisinage de α.
Supposons que $\exists i > 0$ tq $f_i(\alpha) = 0$

- Alors $f_{i-1}(\alpha)\, f_{i+1}(\alpha) < 0$ (pt iii) et donc $V(f_{i-1}, f_i, f_{i+1}) = \mathrm{cte}$
- Donc $V_{stu}(P(c))$ ne varie pas lorsque c varie dans un voisinage de α.

Supposons que $f_0(\alpha) = 0$. $V_{stu}(P(c))$ décroit de 1 lorsque c varie de $\alpha - \epsilon$ à $\alpha + \epsilon$ pour ϵ petit (pt iv) □

COROLLAIRE 11. *Soit $P \in \mathbb{R}[X]$ et $[f_0(X), \dots f_s(X)]$ une suite de Sturm associée à P sur $\mathbb{R}$. L'entier $\mathrm{Var}(f_0(-\infty), \dots, f_s(-\infty)) - \mathrm{Var}(f_0(+\infty), \dots, f_s(+\infty))$ est égal au nombre de racines réelles de P dans $\mathbb{R}$.*

Démonstration. Toutes les racines sont strictement contenues dans un intervalle]a,b[et $\mathrm{Var}(f_0(+\infty), \dots, f_s(+\infty)) = \mathrm{Var}(f_0(b), \dots, f_s(b))$, $V_{\mathrm{stu}}(P(f_0(-\infty), \dots, f_s(-\infty))) = \mathrm{Var}(f_0(a), \dots, f_s(a))$ □

Remarque 12.
$\mathrm{Var}(f_0(+\infty), \dots, f_s(+\infty)) = \mathrm{Var}(\mathrm{sign}(\mathrm{lc}(f_0)), \dots, \mathrm{sign}(\mathrm{lc}(f_s)))$
et
$\mathrm{Var}(f_0(-\infty), \dots, f_s(-\infty)) = \mathrm{Var}(\mathrm{sign}(\mathrm{lc}(f_0)), \dots, (-1)^s \mathrm{sign}(\mathrm{lc}(f_s)))$

PROPOSITION 13. *Soit $P \in \mathbb{R}[X]$* ***sans racince réelle multiple*** *dans $[a,b]$.*

- *$f_0 = P$, $f_1 = P'$*
- *$f_{i-2} = f_{i-1}\, g_i - f_i$*
- *f_s tq f_s n'a pas de racine réelle dans $]a,b[$*

$(f_i)_{i=0,\dots,s}$ est la ***suite de Sturm associée à P***

Démonstration. Preuve. Il suffit de vérifier que la suite définie vérifie les propriétés de la définition. □

Le corolaire suivant (théorème de Sturm) montre que l'on peut se passer simplement de la condition *P est sans facteurs carrés* :

COROLLAIRE 14. *[Théorème de Sturm] Soit $P \in \mathbb{R}[X]$.*

- *$f_0 = P$, $f_1 = P'$*
- *$f_{i-2} = f_{i-1}\, g_i - f_i$ avec $\deg(f_i) < \deg(f_{i-1})$ (opposé du reste)*
- *$f_{s-2} = f_{s-1}\, g_s$ avec $g_s = \gcd(P, P')$ (dernier reste non nul)*

La suite ainsi construite avec a, b tels que $P(a)\,P(b) \neq 0$ vérifie $\mathrm{Var}(f_i(a), i=0...s) - \mathrm{Var}(f_i(b), i=0...s)$ = *nombre de racines réelles de P dans (a,b).*

Démonstration. $g_s = \gcd(P, P') \Rightarrow$ g_s divise $f_0, ..., f_s$

On pose $\forall i = 0 \dots s$, $f_i = g_s \bar{f}_i$ et on remarque que $V_{\mathrm{stu}}(f_i(c)) = V_{\mathrm{stu}}(\overline{f_i}(c))$

On vérifie que $(\overline{f_0})_{i=0...s}$ est une suite de Sturm pour $\overline{f_0}$

- (i) et $(i\,i)$ sont immédiats
- $\bar{f}_{i-2} = \bar{f}_{i-1}\, g_i - \bar{f}_i$ donc soit $\overline{f}_i(\alpha) = \bar{f}_{i+1}(\alpha) = 0$ et donc $\overline{f}_{i+k}(\alpha) = 0, \forall k > 0$ et donc $i > s$ (impossible) soit iii est vrai.
- Supposons que α soit une racine de f_0 de multiplicité $k > 0$. On peut alors écrire $f_0 = (X-\alpha)^k\, h$ et $g_s = (X-\alpha)^{k-1}\, Q$ avec $h(\alpha) \neq 0$ et $Q(\alpha) \neq 0$. Il en découle que $\bar{f}_0 = (X-\alpha)\, h(X)/Q(X), \bar{f}_1 = k\, h(X)/Q(X) + (X-\alpha)\, h'(X)/Q(X)$ et donc que :

$$\bar{f}_0\, \bar{f}_1(X) = (X-\alpha)/Q^2(X)\,(h(X)^2 + (X-\alpha)\, h(X)\, h'(X)).$$

Ainsi, au voisinage de α, $\bar{f}_0\, \bar{f}_1$ a le même signe que $(X-\alpha)$, ce qui vérifie le point $(i\,v)$ de la définition. □

1.5. Suites de Sturm généralisées

On veut compter le nombre de racines reelles c de P telles que $Q(c) > 0$. Pour cela on peut généraliser la notion de suite de Sturm en prenant $f_0 = P$, $f_1 = PQ$ puis en calculant la liste des restes signés comme précédemment. On obtient alors la suite de Sturm de P et $P'\,Q$ que l'on note $f_0, \dots f_s$. En posant $V_{stu}(P, Q, a) = V(f_0(a), \dots f_s(a))$, on a alors le résultat suivant :

Théorème 15. *Soient a et b deux nombres réels tels que $a < b$ et n'annulant pas P. L'entier $V_{stu}(P, Q, a) - V_{stu}(P, Q, b)$ est alors Égal au nombre de racines de P dans $]a, b[$ telles que $Q > 0$ moins le nombre de racines de P dans $]a, b[$ telles que $Q < 0$.*

Démonstration. La preuve est similaire au cas $Q = 1$. □

2. Procédé dichotomique de recherche de racines

Regardons comment les résultats précédents permettent de concevoir des algorithmes simples et corrects pour l'isolation des racines réelles des polynômes en une variable.

Nous avons vu dans la section précedente que l'on peut calculer une borne sur la distance minimale entre 2 racines de P en fonction des coefficients de P.

Nous avons également vu qu'il est facile de calculer une borne sur la valeur absolue des racines réelles de P.

Supposons que P admet toutes ses racines dans un intervalle $[A, B]$. En subdivisant $[A, B]$ en intervalles de largeur au plus $\mathrm{sep}(P)$, et en supposant P sans racines multiples, l'étude du signe de P aux bornes de ces intervalles suffit à déterminer ceux qui contiennent une unique racine de P. On peut facilement lever la condition "P sans racines multiples" en remplaçant P par $P/\gcd(P, P')$.

Le problème d'une telle stratégie est que le nombre d'intervalles à considérer est exponentiel en le degré de P.

Soit $P = \sum_{i=0}^{d} a_i x^i$ avec $a_0 \neq 0$ et $a_n = 1$. Les racines de P sont dans l'intervalle $[A, B]$ avec $B = 2 \cdot \max_{i=0}^{d-1} |a_i|^{1/(d-i)} = -A$. La distance minimale entre 2 racines est minorée par $\mathrm{sep}(P) = \sqrt{\frac{3}{d^d+2}} \cdot \frac{1}{||P||_2^{d-1}}$.

Le nombre d'intervalles à construire sera donc de l'ordre de $2 \cdot \max_{i=0}^{d-1} |a_i|^{1/(d-i)} \frac{1}{\mathrm{sep}(P)} = \max_{i=0}^{d-1} |a_i|^{1/(d-i)} ||P||_2^{d-1} \sqrt{d^{d+2}}$.

Un moyen simple d'éviter ce comportement exponentiel est d'introduire une stratégie de bissection : en calculant une borne A sur les racines de P et en effectuant un changement de variable de la forme $X \to A\,X$, on peut supposer que toutes les racines de P sont dans $]0,1[$.

La stratégie de bissection peut être décrite comme suit :

Algorithme Bissection

- on commence avec $k=0$ et $c=0$
- liste $=[0,1]$
- resultat $=[]$
- tant que liste $\neq\emptyset$ faire
  - retirer $[c/2^k,(c+1)/2^k]$ de liste
  - Si P admet exactement une racine dans $[c/2^k,(c+1)/2^k]$, ajouter $[c/2^k,(c+1)/2^k]$ à resultat;
  - Si P admet (éventuellement) plus d'une racine dans $[c/2^k,(c+1)/2^k]$, ajouter $[2\,c/2^{k+1},(2\,c+1)/2^{k+1}]$ et $[(2\,c+1)/2^{k+1},(2\,c+2)/2^{k+1}]$ à liste;

Si on utilise par exemple des suites de Sturm pour calculer le nombre de de zéros réels dans chaque intervalle, on peut aisément voir que la valeur maximale atteinte pour k est de l'ordre de $\log_2(1/\mathrm{sep}(P))$ et le nombre d'intervalles visités pour k fixé ne peut éxéder le nombre de zéros réels de P qui est bien sur majoré par le degre de P. Moralité, le nombre d'intervalles visités ne peut jamais dépasser quelque chose qui est de l'ordre de $d\log_2(1/\mathrm{sep}(P))$ ce qui est nettement meilleur que l'algorithme de Kronecker.

3. Règle des signes de Descartes

La règle des signes de Descartes est un instrument d'une incroyable efficacité pratique pour calculer des bornes sur le nombre de zéros réels positifs de polynÙmes de $\mathbb{R}[X]$. En effet, elle ne réclame aucun calcul ! :

Proposition 16. *[Lemme de Descartes] Soit $P=\sum_{i=0}^{n}a_n\,X^n\in\mathbb{R}[X]$. Le nombre $Z_{\mathbb{R}^{+*}}(P)$ de racines strictement positives de P est égal à $V(P)$ modulo 2.*

Remarquons en particulier que si $V(P)=0$, P n'admet aucune racine réelle strictement positive et si $V(P)=1$, P admet exactement une racine réelle strictement positive.

La démonstration de la proposition 16 est simplfiée dès lors que le lemme suivant est connu :

Lemme 17. *Soit $P\in\mathbb{R}[X]$, $P\neq 0$. $V(P)\geq r=\sharp\,Z_{\mathbb{R}^{+*}}(P)$.*

Démonstration. Par récurrence sur le degré de P.

Si $n=0$, le résultat est trivial. Supposons donc $n>0$.

Si $a_0=0$, alors $V(P)=V(P/X)$

On peut également supposer $a_0<0$ puisque $V(P)=V(-P)$.

Supposons donc $a_0<0$.

Si P n'a pas de racines réelles, le résultat est trivial.

Notons $0<\alpha_1<\ldots<\alpha_s$, $s>0$ les racines réelles de P strictement positives ayant les multiplicités respectives $\mu_1,\ldots\mu_s$ et notons r' le nombre de racines réelles strictement positives de P'.

Par hypothèse de récurrence, $V(P')>r'$.

Remarquons alors que $V(P)=V(P')$ ou $V(P)=V(P')+1$.

Le théorème de Rolle nous dit alors que $r'\geq r-1$.

Si $V(P)=V(P')+1$ alors on a bien $V(P)\geq r$.

Supposons que $V(P)=V(P')$.

Comme $a_0 < 0$, alors le coefficient de la plus petite puissance de X dans P' est nécessairement négatif (sinon $V(P) = V(P') + 1$)

Pour u assez petit, on a $P(u) < 0$ et $P'(u) < 0$, ce qui implique que P' admet au moins une racine réelle positive strictement plus petite que α_1, donc que $r' \geq r$, ce qui entraine $V(P) = V(P') \geq r' \geq r$. □

Démonstration. (Lemme de Descartes) Le théorème des valeurs intermédiaires induit immédiatement que le nombre de racines réelles strictement positives de P est pair si et seulement si les signes des coefficients de la plus petite puissance et de la plus grande puissance de X apparaissant dans P sont les mêmes.

D'un autre coté, $V(P)$ est pair si et seulement si si et seulement si les signes des coefficients de la plus petite puissance et de la plus grande puissance de X apparaissant dans P sont les mêmes.

Le lemme 17 permet alors de conclure. □

Introduisons quelques nouvelles notations. On suppose que $P = \sum_{i=0}^{d} a_i\, x^i$ est un polynôme sans facteurs carrés à coefficients dans $\mathbb{Z}$ et ayant toutes ses racines dans $]0, 1[$.

Notation 18. *Soient k et c 2 entiers positifs tels que $c < 2^k$, et $\lambda \in \mathcal{R}$. On définit :*

$$I_{k,c} =]\frac{c}{2^k}, \frac{c+1}{2^k}[, \quad P_{k,c} = 2^{kn}\, P(\frac{x+c}{2^k}),$$
$$R(P(x)) = x^n\, P(\frac{1}{x}), \quad H_\lambda(P(x)) = P(\lambda\, x), \quad T_\lambda(P(x)) = P(x + \lambda).$$

Les intervalles $I_{k,c}$ sont appelés intervalles standard.

Clairement, étudier les racines réelles de P dans $I_{k,c}$ revient exatement à étudier les racines réelles de $P_{k,c}$ dans $I_{0,0} =]0, 1]$.

Le lemme suivant se déduit immédiatement de la règle de Descartes :

Lemme 19. *Soit $P = \sum_{i=0}^{d} a_i\, x^i$ est un polynôme sans facteurs carrés à coefficients dans $\mathbb{Z}$ et ayant toutes ses racines dans $]0, 1[$. $\mathrm{Var}\,(T_1\, R(P_{k,c}))$ majore le nombre de racines réelles de P dans $I_{k,c}$ et est égal à celui-ci modulo 2.*

Démonstration. Il suffit de remarquer que les racines reelles strictement positives de $T_1\, R(P_{k,c})$ sont en bijection avec les racines réelles de P dans $I_{k,c}$. □

Introduisons quelques nouvelles notations. On suppose que $P = \sum_{i=0}^{d} a_i\, x^i$ est un polynôme sans facteurs carrés à coefficients dans $\mathbb{Z}$ et ayant toutes ses racines dans $]0, 1[$.

Notation 20. *Soient k et c 2 entiers positifs tels que $c < 2^k$, et $\lambda \in \mathcal{R}$. On définit :*

$$I_{k,c} =]\frac{c}{2^k}, \frac{c+1}{2^k}[, \quad P_{k,c} = 2^{kn}\, P(\frac{x+c}{2^k}),$$
$$R(P(x)) = x^n\, P(\frac{1}{x}), \quad H_\lambda(P(x)) = P(\lambda\, x), \quad T_\lambda(P(x)) = P(x + \lambda).$$

Les intervalles $I_{k,c}$ sont appelés intervalles standard.

Clairement, étudier les racines réelles de P dans $I_{k,c}$ revient exatement à étudier les racines réelles de $P_{k,c}$ dans $I_{0,0} =]0, 1]$.

Le lemme suivant se déduit immédiatement de la règle de Descartes :

Lemme 21. *Soit $P = \sum_{i=0}^{d} a_i\, x^i$ est un polynôme sans facteurs carrés à coefficients dans $\mathbb{Z}$ et ayant toutes ses racines dans $]0, 1[$. $\mathrm{Var}\,(T_1\, R(P_{k,c}))$ majore le nombre de racines réelles de P dans $I_{k,c}$ et est égal à celui-ci modulo 2.*

Démonstration. Il suffit de remarquer que les racines reelles strictement positives de $T_1\, R(P_{k,c})$ sont en bijection avec les racines réelles de P dans $I_{k,c}$. □

3.1. Réciproque de la règle de Descartes : application à l'isolation des racines réelles de polynômes de $\mathbb{R}[X]$

Si on se donne un intervalle $I_{k,c}$ et que la règle proposée dans le lemme 21 donne 0 (resp. 1), alors on est sûr que P n'admet aucune racine (resp. admet exactement une racine) dans $I_{k,c}$.

Pour pouvoir utiliser cette règle dans le procédé dichotomique et assurer que l'algorithme termine, il faut maintenant montrer qu'il existe un entier k suffisamment grand tel que pour tout entier c tel que $0 \leq c \leq 2^k$, $\mathrm{Var}\,(T_1\,R(P_{k,c}))$ est égal à 0 ou 1.

On a vu que si P n'a aucune racine complexe de partie réelle strictement positive, alors $\mathrm{Var}(P) = 0$. On peut bien sûr appliquer cette règle au polynôme $T_1\,R(P_{k,c})$.

Rappelons que les transformations du type $x -> \frac{a*x+b}{c*x+c}$ transforment des cercles en d'autres cercles ou en droites (pour définir complètement l'image d'un cercle, il suffit donc de calculer l'image de 3 points).

En remarquant que les racines complexes de partie réelle positive de $T_1\,R(P_{k,c})$ correspondent bijectivement aux racines complexes de P dans le disque de centre $(0, (2*c+1)/2^k)$ et de rayon $1/2^k$, on peut simplement énoncer le corollaire suivant :

Corollaire 22. *Soit $P = \sum_{i=0}^{n} a_n\,X^n \in \mathbb{R}[X]$, sans racine multiple. Si P n'a aucune racine complexe dans le disque de centre $(0, (2*c+1)/2^k)$ et de rayon $1/2^k$, alors* $\mathrm{Var}\,(T_1\,R(P_{k,c})) = 0$.

En particulier, si $1/2^k$ est plus petit que $\mathrm{sep}(P)$ *et que $I_{k,c}$ ne contient pas de racines de P, alors $Var\,(T_1\,R(P_{k,c})) = 0$.*

Il reste maintenant à trouver un résultat analogue pour $\mathrm{Var}\,(T_1\,R(P_{k,c})) = 1$

Théorème 23. *Soit $P = \sum_{i=0}^{n} a_n\,X^n \in \mathbb{R}[X]$, sans racine multiple avec une unique racine (réelle) dans $]0,1[$ et aucune racine non réelle dans les disques D_0 (centre $(0,0)$ rayon 1) et D_1 (centre $(1,0)$ et rayon 1). Alors* $\mathrm{Var}\,(T_1\,R(P)) = 1$.

Démonstration. La factorisation de P dans $\mathbb{R}[X]$ donne un produit de facteurs linéaires et quadratiques, il en est clairement de même pour $T_1\,R(P)$.

D'après les hypothèses, il existe un unique facteur linéaire de P s'annulant dans $]0,1[$ ou autrement dit, il existe un unique facteur linéaire de $T_1\,R(P)$ s'annulant dans $\mathbb{R}^{+*}$.

Si A est un polynôme de $\mathbb{R}[x]$ tel que $\mathrm{Var}(A) = 1$, alors pour tout $b \in \mathbb{R}^{+*}$, $\mathrm{Var}\,(A \cdot (x+b)) = 1$.

En effet, si on pose $A = \sum_{j=0}^{d} a_i\,X^i$ et on suppose sans perte de généralité que $a_k < 0$ pour $k = 0, \ldots i-1$ et que $a_k > 0$ pour $k = i, \ldots d$.

Comme $A \cdot (x+b) = \sum_{k=0}^{d+1} c_k\,x^k = b\,a_0 + \sum_{k=1}^{d} (a_{k-1} + b\,a_k)\,x^k + a_d\,x^{d+1}$ et que $b > 0$, alors $c_k < 0$ $k = 0 \ldots i-1$ et $c_k > 0$ $k = i+1 \ldots d+1$. Ainsi, quel que soit le signe de c_i, $\mathrm{Var}\,(A \cdot (x+b)) = 1$.

Par récurrence, on peut donc voir que si L est le produit des facteurs linéaires de $T_1\,R(P)$, alors $\mathrm{Var}(L) = 1$.

Montrons maintenant que les facteurs quadratiques apparaissant dans la factorisation de $T_1\,R(P)$ sont tous de la forme $(x^2 + b\,x + c)$ avec $b > 1$ et $b > c > 0$. Les facteurs quadratiques de P s'écrivent $(x-\alpha)\,(x-\bar{\alpha})$, pour α en dehors de l'intersection des disques D_0 et D_1.

Dire que $\alpha \notin D_1$ revient à dire que $1/\alpha - 1$ est dans le demi-plan $\mathrm{Re}(z) < -1/2$ et donc $b = -2\,Re\,(1/\alpha - 1) > 1$.

Dire que $\alpha \notin D_0$ revient à dire que $1/\alpha \in D_0$ et donc que $1/\alpha - 1$ est dans le disque D_{-1} (de centre $(-1,0)$ et de rayon 1).

Comme $c = ((1/\alpha - 1)\,\overline{(1/\alpha - 1)})$, en posant $(1/\alpha - 1) = e + i\,f$, on peut alors remarquer que $c = e^2 + f^2$. Comme $1/\alpha \in D_0$ alors $(e+1)^2 + f^2 < 1$ et donc $c = e^2 + f^2 < -2\,e$. Enfin, comme $b = -2\,e > 1$, on a bien $b > 1 > c > 0$.

On termine en montrant comme plus haut que si A est un polynôme de $\mathbb{R}[x]$ tel que $\mathrm{Var}(A) = 1$, alors pour tout $(b,c) \in \mathbb{R}^{+*} \times \mathbb{R}^{+*}$ tel que $b > 1 > c > 0$, $\mathrm{Var}\,(A \cdot (x^2 + b\,x + c)) = 1$. □

On peut maintenant étendre le résultat précédent :

Corollaire 24. *Soit* $P = \sum_{i=0}^{n} a_n\, X^n \in \mathbb{R}[X]$, *sans racine multiple avec une unique racine (réelle) dans* $]c/2^k, (c+1)/2^k[$ *et aucune racine non réelle dans les disques* $D_{c,k}$ *(centre* $(c/2^k, 0)$ *rayon* $1/2^k$*) et* $D_{c+1,k}$ *(centre* $((c+1)/2^k, 0)$ *et rayon* $1/2^k$*). Alors* $\mathrm{Var}\,(T_1\, R(P_{k,c})) = 1$.

Ainsi, pour tout k tel que $1/2^{k+1} < \mathrm{sep}(P)$ soit $\mathrm{Var}\,(T_1\, R(P_{k,c})) = 0$ soit $\mathrm{Var}\,(T_1\, R(P_{k,c})) = 1$.