1. Theoreme de Sturm pour un polynôme quelconque

Soit $P \in \mathbb{R}[X]$. On pose :

- $f_0 = P,\ f_1 = P'$
- pour $i = 1 \ldots s-1$, $f_{i+1} = -\text{Reste}(f_{i-1}, f_i)$ avec $0 < \deg(f_{i+1}) < \deg(f_i) < \deg(f_{i-1})$
- $f_s = -\text{Reste}(f_{s-2}, f_{s-1}) \approx \text{GCD}(P, P')$

1. Montrer que $\forall i = 0 \ldots s\ \overline{f_i} = f_i / f_s \in \mathbb{R}[X]$

   Ceci est une conséquence directe des propriétés de la suite des restes associée à 2 polynômes f et g : $\gcd(f, g) \sim \gcd(r_i, r_{i+1}) \sim r_s$. En particulier, r_s divise chaque r_i.

2. Montrer que la suite $\overline{f_i}$ ainsi construite avec a, b tels que $P(a)\ P(b) \neq 0$ vérifie $\text{Var}(f_i(a), i = 0 \ldots s) - \text{Var}(f_i(b), i = 0 \ldots s) =$ nombre de racines réelles de P dans (a, b).

   On pose $\forall i = 0 \ldots s$, $f_i = f_s\ \bar{f}_i$ et on remarque que $\text{Var}(f_i(c), i = 0 \ldots s) = \text{Var}(\overline{f_i}(c), o = 0 \ldots s)$

   On vérifie que $(\overline{f_0})_{i=0\ldots s}$ 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 que $\bar{f}_0\, \bar{f}_1(X) = (X - \alpha) / Q^2(X)\, (h(X)^2 + (X - \alpha)\, h(X)\, h'(X))$

     Ainsi, pour X voisin de α, comme $h(X)^2 > 0$, alors $h(X)^2 + (X - \alpha)\, h(X)\, h'(X) > 0$ et $\bar{f}_0\, \bar{f}_1(X)$ a le même signe que $(X - \alpha)$, ce qui vérifie le point $(i\,v)$ de la définition.

2. « Reciproque » de la Règle de Descartes

Notation 1. *Soit $P = \sum_{i=0}^{n} a_i\, x^i \in \mathbb{R}[X]$ et soient k et c 2 entiers positifs tels que $c < 2^k$, $\lambda \in \mathbb{R}$. 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.

1. Supposons que $P = \sum_{i=0}^{n} a_i\, x^i$ soit un polynôme sans facteurs carrés à coefficients dans $\mathbb{Z}$ et ayant toutes ses racines dans $]0, 1[$. Montrer que

   a) $\text{Var}\,(T_1\, R(P_{k,c}))$ majore le nombre de racines réelles de P dans $I_{k,c}$ et est égal à celui-ci modulo 2.

      Il suffit de remarquer que les racines de $P_{k,c}$ dans $I_{k,c}$ sont en bijection avec celles de P dans $(0, 1)$ puis de remarquer que les racines de Q dans $(0, 1)$ sont en bijection avec les racines positives de $T_1\, R(Q)$.

   b) 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 $\text{Var}\,(T_1\, R(P_{k,c})) = 0$.

      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 $1 / 2^k$, il suffit simplement d'adapter à $T_1\, R(P_{k,c})$ le théorème du cours : "Si P n'a aucune racine complexe de partie réelle strictement positive, alors $V(P) = 0$"

2. On suppose $P=\sum_{i=0}^{n} a_n X^n \in \mathbb{R}[X]$, 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).

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

   Si on pose $A=\sum_{j=0}^{d} a_j X^j$ et on suppose sans perte de généralité que $a_k<0$ pour $k=0,\dots,i-1$ et que $a_k>0$ pour $k=i,\dots,d$.

   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 $c_k<0$ $k=0\dots i-1$ et $c_k>0$ $k=i+1\dots d+1$. 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 $\mathrm{Var}(L)=1$.

   b) Montrer 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 $b=-2\,\mathrm{Re}\,(1/\alpha-1)>1$.

   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 $b>1>c>0$.

   c) Montrer que $\mathrm{Var}\,(T_1\, R(P))=1$

   On montre comme en 2)a) que si $T_1\, R(P)=(x^2+b\,x+c)\,A$ avec $\mathrm{Var}\,(T_1\, R(P))=1$, alors Var(A)=1 et on conclut en factorisant $T_1\, R(P)$ dans $\mathbb{R}$.

3. Donner un algorithme complet d'isolation basé sur la règle de Descartes et utilisant le même procédé dichotomique que celui basé sur le théorème de Sturm en prouvant qu'il termine. Argumenter sur son efficacité probable

3. Paramétrisation rationnelle de solutions de systèmes algébriques en 2 variables

Soient $P,Q\in\mathbb{Q}[X,Y]$ sans facteurs communs dans $\mathbb{Q}[X,Y]$ avec $\deg_Y(P)>\deg_Y(Q)$. En outre $\mathrm{Res}_Y(P,Q)\neq 0$ dans $\mathbb{Q}[X]$. Soit $(\alpha,\beta)\in\mathbb{C}^2$ tel que $P(\alpha,\beta)=Q(\alpha,\beta)=0$.

1. Soit $\alpha\in\mathbb{C}$ tel que $\mathrm{lc}_Y(P)(\alpha)\mathrm{lc}_Y(Q)(\alpha)\neq 0$. On définit l'entier k_α par $k_\alpha=\inf\,(j,\mathrm{sres}_j(P,Q)(\alpha)\neq 0)$. Montrer que $\mathrm{Sres}_{k_\alpha}(P,Q)(\alpha,Y)\sim\mathrm{PGCD}(P(\alpha,Y),Q(\alpha,Y))$.

   Comme $\mathrm{lc}_Y(P)(\alpha)\mathrm{lc}_Y(Q)(\alpha)\neq 0$, la propriété de spécialisation des sous-résultants appliquée au morphisme d'anneaux $X\to\alpha$ implique $\mathrm{sres}_{k_\alpha}(P,Q)(\alpha)=\mathrm{sres}_{k_\alpha}(P(\alpha,Y),Q(\alpha,Y))$.

   Dire que $\mathrm{sres}_{k_\alpha}(P(\alpha,Y),Q(\alpha,Y))\neq 0$, implique qu'il existe un reste normalisé $r_{n_{k_\alpha}}$ dans la suite des restes associée à $P(\alpha,Y),Q(\alpha,Y)$ tel que $\mathrm{degre}(r_{n_{k_\alpha}})=k_\alpha$ et deux polynômes $s_{n_{k_\alpha}}$ et $t_{n_{k_\alpha}}$ consituant la relation de Bezout $s_{n_{k_\alpha}}\,P+t_{n_{k_\alpha}}\,Q=r_{n_{k_\alpha}}$.

   Par construction de k_α, il n'existe pas d'entier plus petit que k_α dans la suite des degrés des restes r_i, ce qui implique que $r_{k_{k_\alpha}}$ est un pgcd de $P(\alpha,Y),Q(\alpha,Y)$.

   Enfin k_α existe puisque le fait de supposer que $0\neq\mathrm{lc}_Y(P)(\alpha)\mathrm{lc}_Y(Q)(\alpha)$ implique au moins que le sous-resultant de degré $\deg(Q(\alpha,Y))$ est non identiquement nul.

2. Montrer que l'on peut alors décomposer le système $\{(\alpha,\beta)\in\mathbb{C}^2, P(\alpha,\beta)=0, Q(\alpha,\beta)=0\}$ en une union finie de systèmes disjoints de la forme $\cup_{i=1}^{s}\{(\alpha,\beta)\in\mathbb{C}^2, R_i(\alpha)=0, B_i(\alpha,\beta)=0\}$ tels que $R_i\in\mathbb{Q}[X]$, $B_i\in\mathbb{Q}[X,Y]$ et $\forall\alpha\in\mathbb{C}, R_i(\alpha)=0, B_i(\alpha,Y)\sim\mathrm{PGCD}(P(\alpha,Y),Q(\alpha,Y))$.

   Pour tout α non racine de $\mathrm{lc}_Y(P)\,\mathrm{lc}_Y(Q)\mathrm{Res}(P,Q,Y), \gcd(P(\alpha,Y),Q(\alpha,Y))\sim 1$, donc (α,β) vérifie $P(\alpha,\beta)=0=Q(\alpha,\beta)$ si α est racine de $\mathrm{lc}_Y(P)\,\mathrm{lc}_Y(Q)\mathrm{Res}_Y(P,Q)$.

D'après le 1) $\deg(\gcd(P(\alpha,Y),Q(\alpha,Y)))>0 \Rightarrow \alpha$ annule $\mathrm{lc}_Y(P)\,\mathrm{lc}_Y(Q)\mathrm{Res}_Y(P,Q)$.
Posons $R_0=\frac{\mathrm{Res}_Y(P,Q)}{\gcd(\mathrm{Res}_Y(P,Q),\mathrm{lc}_Y(P)\,\mathrm{lc}_Y(Q))}$.

On définit alors $G_1=\gcd(\mathrm{sres}_1(P,Q),R_0)$ et $R_1=\frac{R_0}{G_1}$. D'après 1), $\mathrm{Sres}_1(P,Q)(\alpha)=\gcd(P(\alpha,Y),Q(\alpha,Y))$ pour tout α racine de R_1.

On construit ainsi $(R_i,B_i=\mathrm{Sres}_i)_{i=1}^{\deg_Y(Q)}$ avec la propriété : si $P(\alpha,\beta)=0, Q(\alpha,\beta)=0$, alors soit (α,β) appartient à l'un des ensembles disjoints $((\alpha,\beta)\in\mathbb{C}^2, R_i(\alpha)=0, B_i(\alpha,\beta)=0)_{i=1}^{\deg_Y(Q)}$ soit α annule $\mathrm{lc}_Y(P)\ \mathrm{lc}_Y(Q)$. On réalise alors la même construction en considérant Q (ou P quitte éventuellement à inverser le rôle des polynômes) privé de son terme de tête et en remplaçant R_0 par $\gcd(R_0,\mathrm{Lc}_Y(Q))$.

3. Si on suppose que $(\alpha,\beta)\neq(\alpha',\beta')\Rightarrow\alpha\neq\alpha'$ pour tous couples (α,β), (α',β') tels que $P(\alpha,\beta)=Q(\alpha,\beta)=P(\alpha',\beta')=Q(\alpha',\beta')=0$, montrer que l'on peut alors décomposer le système $\{(\alpha,\beta)\in\mathbb{C}^2, P(\alpha,\beta)=0, Q(\alpha,\beta)=0\}$ en une union finie de systèmes disjoints de la forme $\cup_{i=1}^s\{(\alpha,\beta)\in\mathbb{C}^2, R_i(\alpha)=0, \beta=C_i(\alpha)\}$ avec $R_i,C_i\in\mathbb{Q}[X]$.

   Dire que $(\alpha,\beta)\neq(\alpha',\beta')\Rightarrow\alpha\neq\alpha'$ pour tous couples (α,β), (α',β') tels que $P(\alpha,\beta)=Q(\alpha,\beta)=P(\alpha',\beta')=Q(\alpha',\beta')=0$ implique que pour tout α tel que $\exists\beta$ tel que $P(\alpha,\beta)=Q(\alpha,\beta)=0$, $\mathrm{pgcd}(P(\alpha,Y)Q(\alpha,Y))$ n'admet qu'une seule racine β et s'écrit donc, une fois normalisé, $(Y-\beta)^k$ avec $k\in\mathbb{N}^\star$.

   Si $\{R_i(X),B_i(X,Y)\}$ est le couples de polynômes calculé en 3) tels que $R_i(\alpha)=B_i(\alpha,\beta)=0$, alors $B_i(\alpha,Y)=\gcd(P(\alpha,Y),Q(\alpha,Y))$ et il existe $a_1(X)$ et $b_1(X)$ tels que $B_i(X,Y)=(b_1(X)+Y\,a_1(X))^{k_i}\bmod R_i(X)$. On on peut alors remplacer $B_i(X,Y)$ par $Ya_i(X)+b_i(X)$ dans la décomposition en posant $a_1(X)=\mathrm{lc}_Y(B_i)$ et $b_1(X)=\frac{1}{k_1}\mathrm{coeff}_Y(B_i,k_1-1)$.

   Par construction, $\gcd(a_1,R_i)\sim 1$ ce qui fait que $a_1(X)$ est inversible modulo $R_i(X)$, inverse que l'on peut calculer en appliquant l'algorithme d'Euclide étendu (si $s\,a_1+t\,R_i=1$ alors $s=a_1^{-1}\bmod R_i$) et conclure en posant $C_i=-(\mathrm{lc}_Y(B_i))^{-1}\frac{1}{k_1}\mathrm{coeff}_Y(B_i,k_1-1)\bmod R_i$.

4. Pour tout $a\in\mathbb{Z}$, on définit $T_a=X+a\,Y$. Montrer que sauf pour un nombre fini de valeurs de a , pour tous couples $(\alpha,\beta),(\alpha',\beta')$ tels que $P(\alpha,\beta)=Q(\alpha,\beta)=P(\alpha',\beta')=Q(\alpha',\beta')=0$, $t_a(\alpha,\beta)\neq t_a(\alpha',\beta')$. On dit alors que T_a sépare les racines du système $\{P=0,Q=0\}$.

   On note (α_i,β_i) $i=1...D$ les racines distinctes communes de P,Q. Soit T une nouvelle variable. Le polynôme $\prod_{i=1}^d\prod_{i<j\leqslant d}((\alpha_i-\alpha_j)+T\ (\beta_i-\beta_j))$ est un polynôme non identiquement nul de $\mathbb{C}[T]$ de degré $\leqslant d^2$. Il admet donc au plus d^2 racines.

5. Trouver un algorithme permettant de calculer $a\in\mathbb{Z}$ tq T_a sépare les racines du système $\{P=0,Q=0\}$.

   On remarque que lorsque l'on fait un changement de variabe du type $P(T-a\,Y,Y)$ on construit un polynôme de $\mathbb{Q}[T,Y]$ tel que $\mathrm{lc}_Y(P)\in\mathbb{Q}$. Ainsi, tout (γ,β) racine de $P_a=P(T-a\,Y,Y)$ et $Q_a=Q(T-a\,Y,Y)$ si et seulement si γ est racine de $\mathrm{Res}_Y(P_T,Q_T)=0$. Ainsi, T_a sépare les racines de P et Q si et seulement si $\deg_Y(\mathrm{Res}_Y(P_a,Q_a))$ est maximal.

6. Montrer que l'on peut alors décomposer le système $\{(\alpha,\beta)\in\mathbb{C}^2, P(\alpha,\beta)=0, Q(\alpha,\beta)=0\}$ en une union finie de systèmes disjoints de la forme $\cup_{i=1}^s\{(\alpha,\beta)\in\mathbb{C}^2, R_i(\gamma)=0, \alpha=C_{X,i}(\gamma), \beta=C_{Y,i}(\gamma)\}$avec $R_i,C_{X,i},C_{Y,i}\in\mathbb{Q}[T]$.

   Il suffit de faire le changement de variable idoine pour se ramener à un systeme en T, Y , appliquer les résultats précédents et puis se souvenir que $X=T-a\,Y$