Stage de Licence 3

Rémy Garnier et Mathieu Huot

Introduction

Dans le cadre de l'étude des PolITA, Polynomial Interrupt Timed Automata, c'est à dire des automates temporisés polynomiaux que nous verrons ci-après, nous étudions le *problème de l'accessibilité*. Ce problème est le problème de décision consistant à déterminer si un état donné de l'automate peut être atteint, partant de la configuration initiale.

Première partie

PolITA

1 Position du problème

1.1 Définitions

On note $\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{Z}$ l'ensemble des entiers relatifs, $\mathbb{Q}$ l'ensemble des rationnels, $\mathbb{R}$ l'ensemble des réels, $\mathbb{C}$ l'ensemble des nombres complexes, $\mathbb{D}$ un anneau intègre quelconque, et $\mathbb{K}_{\mathbb{D}}$ son corps de fraction.

Soit $X = \{x_1, ...x_n\}$ un ensemble fini de n variables, appelées horloges. On note $\mathbb{Q}[x_1, ...x_n]$ l'ensemble des polynômes à n variables à coefficients dans $\mathbb{Q}$.

On note $\bowtie \in \{<, \leq, =, \geq, >\}$. On appelle *contrainte polynomiale* la conjonction de contraintes de la forme $P \bowtie 0$, et on note $C(X)$ l'ensemble des contraintes polynomiales.

On définit également l'ensemble des *mises à jour polynomiales* sur X :

$$U(X) = \{ \bigwedge_{x \in X} x := P_x | P_x \in \mathbb{Q}[x_1, ...x_n] \}$$

Une valuation pour X est une fonction $v \in \mathbb{R}^X$, qu'on peut identifier au vecteur $(v(x_1), ...v(x_n)) \in \mathbb{R}^n$. On note 0 la valuation où $v(x) = 0$ pour tout $x \in X$. Pour $P \in \mathbb{Q}[x_1, ...x_n]$ et une valuation v, la valeur de P en v est $P(v) = P(v(x_1), ...v(x_n))$. Une valuation v satisfait la contrainte $P \bowtie 0$, noté $v \models P \bowtie 0$, si $P(v) \bowtie 0$. La notation est naturellement étendue à une contrainte polynomiale : $v \models \varphi$ avec $\varphi = \bigwedge_i P_i \bowtie_i 0$ si $v \models P_i \bowtie_i 0$ pour tout i.

Une mise à jour de valuation v par $u = \bigwedge_{x \in X} x := P_x \in U(X)$ est la valuation $v[u]$ définie par $v[u](x) = P_x(v)$ pour tout $x \in X$.

Pour une valuation v et un délai $d \in \mathbb{R}_{\geq 0}$, la valuation $v' = v +_k d$ correspondant au *temps écoulé pour l'horloge* x_k, est définie par $v'(x_k) = v(x_k) + detv'(x) = v(x)$ pour tout autre horloge x.

Un PolITA est un tuple $A = \langle \Sigma, Q, q_0, F, X, \lambda, \Delta \rangle$, où :

Σ est un alphabet fini

Q est un nombre fini d'états, q_0 est l'état initial, $F \subseteq Q$ est l'ensemble des états finals

$X = \{x_1, ...x_n\}$ un ensemble de n horloges

La fonction $\lambda : Q \longrightarrow \{1, ...n\}$ associe à chaque état son niveau et nous appelons $x_{\lambda(q)}$ l'horloge active dans l'état q

$\Delta \subseteq Q \times C(X) \times (\Sigma \cup \{\epsilon\}) \times U(X) \times Q$ est l'ensemble des transitions. Soit $q \rightarrow^{\varphi,a,u} q'$ une transition avec $k = \lambda(q)$ et $k' = \lambda(q')$. La formule φ est une conjonction de contraintes de la forme $P \bowtie 0$ avec $P \in \mathbb{Q}[x_1, ...x_{k-1}]$ (P est un polynôme sur les horloges de niveau inférieur ou égal à k). La mise à jour u est de la forme $\bigwedge_{i=1}^{n} x_i := C_i$ avec :

Si $k > k'$, c'est à dire si la transition fait décroître le niveau, alors pour $1 \leq i \leq k'$, $C_i = x_i$ et pour $i > k'$, $C_i = 0$.

Si $k \leq k'$, alors pour tout $i \leq i < k$, $C_i = x_i$, $C_k = P$ pour $P \in \mathbb{Q}[x_1, ...x_{k-1}]$ ou $C_k = x_k$, et pour $i > k$, $C_i = 0$.

La *sémantique* d'un ITA A est définie par le système de transition (temporisé) $T_A = (S, s_0, \rightarrow)$, où $S = \{(q, v) | q \in Q, v \in \mathbb{R}^X\}$ est l'ensemble des configurations, d'état initial $s_0 = (q_0, 0)$. La relation $\rightarrow$ est définie par deux étapes :

Étapes temporisées : Seulement l'horloge active d'un état peut évoluer, toutes les autres sont suspendues. Pour un état q d'horloge active $x_{\lambda(q)}$, une étape temporisée d'une durée de $d >$ est définie par $(q, v) \rightarrow^d (q', v')$ avec $v' = v +_{\lambda(q)} v$. Une étape de durée 0 laisse le système T_A dans la même configuration.

Étapes discrètes : Une étape discrète $(q, v) \rightarrow^a (q', v')$ peut se produire s'il existe une transition $q \longrightarrow^{\varphi,a,u} q'$ de Δ telle que $v \models \varphi$ et $v' = v[u]$.

1.2 Le problème de l'accessibilité

Le *problème d'accessibilité* est un problème de décision où l'on se demande si un état donné peut être atteint partant de la configuration initiale.

Formellement, le problème de l'accessibilité demande, étant donné un état q, s'il existe une valuation v et un chemin de $(q_0, 0)$ à (q, v) dans le système de transition T_A.

Puisque le système de transition T_A est infini, une recherche exhaustive n'est pas possible, et l'algorithme repose sur une abstraction dudit système.Ces techniques ont été largement utilisées dans la configuration de systèmes linéaires temporisés, où ils sont définis comme des polygones de $\mathbb{R}^X$. Ces abstractions ont besoin d'être suffisamment raffinées afin

de capturer à la fois l'écoulement temporel et les sauts discrets au passage d'une transition. A savoir, deux configurations dans la même classe d'abstraction devraient atteindre la même classe de successeur lorsque le temps s'écoule ou lorsqu'une mise à jour est effectuée.

Les travaux précédents sur les ITA ont construit une telle abstraction en se basant sur un ensemble d'*expressions*. Ces expressions contenaient des formes linéaires en lien avec les gardes et les mises à jour, avec l'horloge active du niveau. De plus, puisque l'ordre de deux expressions d'un niveau donné peut dépendre de la valeur des horloges de plus bas niveau, certaines expressions sont nécessaires à des niveaux inférieures. Les régions où furent alors définis comme des sous-ensembles de $\mathbb{R}^n$ où l'ordre des expressions était constant.

Le procédé précédent est adapté au contexte des PolITA, où les contraintes sont algébriques plutôt que linéaires, et donc donnent des régions qui ne sont pas des polygones mais des cellules définies par la dite *décomposition cylindrique algébrique*.

2 Une décomposition cylindrique pour la théorie des réels du premier ordre

On considère des formules qui expriment des propriétés des réels. Elles sont définies de manière inductive comme suit. UNe expression arithmétique est :

Soit une constante entière, une variable

Soit $e_1 + e_2$, $e_1 * e_2$ où e_1 et e_2 sont des expressions arithmétiques.

Une formule est :

Une formule basique : $e \sim 0$ où $\sim \in \{<, =\}$ et e est une expression arithmétique

Ou $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$, $\neg\varphi_1$, $\forall x\varphi_1$, $\exists x\varphi_1$ où φ_1 et φ_2 sont des formules et x est une variable

Une phrase est une formule sans variables libres. UNe phrase a une valeur de vérité lorsqu'elle est interprétée sur $\mathbb{R}$ et l'on cherche à décider de la valeur d'une formule. Ce problème a été résolu la première fois par Tarski[10] à l'aide d'une procédure non élémentaire. Plus tard une procédure en 2EXPTIME fut trouvée par Collins[9] basée sur une technique appelée *décomposition cylindrique*. Finalement, une procédure en EXPSPACE fut établie. La meilleure borne inférieure actuellement connue pour ce problème est $\mathrm{STA}(*, 2^{nO(1)}, n)$ (une classe de complexité définie par des machins alternantes limitées et se situant entre EXPTIME et EXPSPACE).

Pour nos objectifs, nous allons adapter la décomposition cylindrique. Nous développons alors dans cette section les outils nécessaires. Ici nous décrivons seulement les principes généraux et expliquons comment l'on peut les utiliser pour décider de la valeur d'une formule. Le premier concept que nous introduisons est la *cellule*.

Définition : Une cellule de niveau n est un sous ensemble de $\mathbb{R}^n$ définit de façon inductive comme suit :

Lorsque $n = 1$, c'est un point ou un intervalle ouvert.

Une cellule C de niveau $n+1$ est définie à partir d'une cellule C' de niveau n et a l'une

des formes suivantes :

$C = C' \times \mathbb{R}$;

$C = \{(x, f(x))|x \in C'\}$ où f est une fonction continue de C' dans $\mathbb{R}$;

$C = \{(x, y)|x \in C' \wedge y \sim f(x)\}$ où f est une fonction continue de C' dans $\mathbb{R}$ et $\sim \in \{<, >\}$;

$C = \{(x, y)|x \in C' \wedge l(x) < y < u(x)\}$ où $l < u$ sont deux fonctions continues de C' dans $\mathbb{R}$.

Par convention l'unique cellule de niveau 0 est $\mathbb{R}^0$.

Soit $P = \{P_i\}_{1 \leq i \leq n}$ une famille de d'ensemble de polynômes telle que pour tout P$\in P_i$, P$\in \mathbb{R}[X_1, ..., X_i]$. Par convention, on étend P avec $P_0 = \emptyset$. Nous introduisons maintenant le concept d'*invariance de signe* d'une cellule par rapport à P.

Définition : Soit $P = \{P_i\}_{1 \leq i \leq n}$. Une cellule C de niveau i est P-invariante si :

$\forall \leq i, \forall$P$\in P_j, \forall x, y \in C$, signe(P$(x)$)=signe(P$(y)$).

Lorsque $i < n$,

Soit $C \times \mathbb{R}$ est P-invariant ;

Soit il existe $f_1 < ... < f_k$ des fonctions continues de C dans $\mathbb{R}$ telles que les cellules suivantes sont P-invariantes :

$\forall i \leq i \leq k, \{(x, f_i(x))|x \in C\}$

$\{(x, y|x \in C \wedge y < f_1(x)\}$

$\{(x, y|x \in C \wedge y > f_k(x)\}$

$\forall i \leq i < k, \{(x, y|x \in C \wedge f_i(x) < y < f_{i+1}(x)\}$

On observe que si $\mathbb{R}^0$ est P-invariant, on peut définir de façon inductive un arbre de cellules P-invariantes comme suit :

La racine est $\mathbb{R}^0$;

Soit C une cellule P-invariante de niveau $i < n$ de l'arbre. Alors selon le type d'invariance :

Soit C a un unique enfant $C \times \mathbb{R}$;

Soit pour un certain $k > 0$, C a $2k + 1$ enfants ordonnés $\{(x, y|x \in C \wedge y < f_1(x)\}$, $\{(x, f(x))|x \in C\}$, $\forall i \leq i < k, \{(x, y|x \in C \wedge f_1(x) < y < f_2(x)\}$,...,$\{(x, y|x \in C \wedge y > f_k(x)\}$.

Cet arbre est également appelé *décomposition cylindrique*.

Voyons maintenant comment une décomposition cylindrique est utile en théorie des réels du premier ordre. Toute proposition peut-être transformée en une formule équivalente par la mise en forme prénèxe (tous les quantificateurs au début). On construit alors, par analyse syntaxique, la famille P des polynômes apparaissant dans la formule. Supposons que nous ayons produit une décomposition cylindrique pour P. Alors l'algorithme suivant résout le problème de décision avec l'appel $Check(\varphi, 0, \mathbb{R}^0, \emptyset$.

Deuxième partie

Programmer une décomposition cylindrique

3 Calcul des sous résultants

3.1 Position du problème

Dans toute la suite, $\mathbb{D}$ désigne un anneau représentable en machine et $\mathbb{D}[X]$ l'anneau des polynômes associé, avec $\mathbb{D} \subset \mathbb{R}$

On suppose qu'on peut additionner et multiplier des éléments de $\mathbb{D}$. On suppose également qu'on dispose d'une fonction *sign* tel que : $\forall x \in \mathbb{D}, sign(x) = 1$ pour $x > 0$, $sign(x) = -1$ pour $x < 0$, $sign(x) = 0$ si $x = 0$.

De même, la permutation de i éléments a un signe de $\epsilon_i = (-1)^{\frac{i(i-1)}{2}}$.

Enfin, si $P, Q \in \mathbb{D}[X]$, de degrés respectif p et q avec $p \geq q$, on note *Rem(P,Q)* l'unique polynôme de degré strictement inférieur à q tel qu'il existe $C \in \mathbb{D}[X]$ tel que :

$$P = CQ + Rem(P, Q)$$

3.2 Matrices de Sylvester-Habicht

Soit $P, Q \in \mathbb{D}[X]$, de degré respectifs p et q (on suppose que l'on a p > q). On cherche à connaître le degré de leur pgcd. Pour cela, on introduit les matrices de Sylvester-Habitch associés à ces polynômes

Définition : Matrices de Sylvester-Habicht Pour tout $j < max(p-1, q)$ on définit la j-ième matrice de Sylvester-Habicht comme la matrice de taille $(p+q-2j, p+q-j)$ la famille $(X^{q-j-1}P, ...XP, P, Q, ..., X^{p-j-1}Q)$ dans la base canonique de $\mathbb{D}[X]$. Cette matrice est notée $SyHa_j(P, Q)$.

Définition : Sous-Résultants La matrice $SyHa_{j,j}(P, Q)$ est la matrice $SyHa_j(P, Q)$ privée de ses j dernières colonnes. Cette matrice est carrée (de taille $p + q - 2j$), on peut donc considérer son déterminant $sRes_j(P, Q) = det(SyHa_{j,j}(P, Q)$. C'est le j-ième sous résultant de P et Q.

Exemple : Si $P = \sum a_i X^i$ et $Q = \sum b_i X^i$, on a

$$\begin{bmatrix}
a_p & a_{p-1} & ... & a_1 & a_0 & 0 & ... & ... & 0 \\
0 & a_p & ... & ... & a_1 & a_0 & 0 & ... & \vdots \\
\vdots & \ddots & \ddots & ... & ... & ... & \ddots & \ddots & \vdots \\
\vdots & ... & \ddots & \ddots & ... & ... & ... & \ddots & 0 \\
0 & ... & ... & 0 & a_p & ... & ... & ... & a_0 \\
0 & ... & ... & ... & ... & 0 & b_q & ... & b_0 \\
\vdots & ... & ... & ... & \iddots & \iddots & ... & \iddots & 0 \\
\vdots & ... & ... & \iddots & \iddots & ... & \iddots & \iddots & \vdots \\
\vdots & ... & \iddots & \iddots & ... & \iddots & \iddots & ... & \vdots \\
\vdots & \iddots & \iddots & ... & \iddots & \iddots & ... & ... & \vdots \\
0 & b_q & ... & b_0 & 0 & ... & ... & ... & \vdots \\
b_q & ... & b_0 & 0 & ... & ... & ... & ... & 0
\end{bmatrix}$$

Proposition Pour $P, Q \in \mathbb{D}[X]$, on a $deg(pgcd(P,Q)) = j$ si et seulement si $\forall i \in [0; j-1], sRes_i(P,Q) = 0$ et $sRes_j(P,Q) \neq 0$

Démonstration On remarque que $sRes_j(P,Q) = 0$ si et seulement il existe une famille (λ_i) de $\mathbb{D}$ telle que $\lambda_1 X^{q-j-1}P + ... + \lambda_{p+q-2j}X^{p-j-1}Q$ soit un polynôme de degré inférieur à j.

3.3 Calcul des sous résultants

Définition : P-Matrices Pour (P_i) famille de m polynômes de degré inférieur à n tel que $\forall i \in [1; m] P_i = \sum a_{i,j}X^j$, on définit la P-matrice $Pmat(P_i)$ comme la matrice de taille $m * m$ de coefficients $m_{i,j}$ tels que

— $\forall i \leq m \forall j < m, m_{i,j} = a_{i,j}$
— $\forall i \leq m, m_{i,j} = P_i$

Proposition : Sous résultants Pour $P, Q \in \mathbb{D}[X]$, on note $sResP_j(P,Q) = det(Pmat(X^{q-j-1}P, X^{q-j}$
Le coefficient dominant de $sResP_j(P,Q)$ est $S_Resj(P,Q)$.

Démonstration Notre matrice s'écrit :

$$\begin{bmatrix}
a_p & a_{p-1} & ... & ... & a_j & ... & a_0 & ... & ... & X^{q-j-1}P \\
0 & a_p & ... & ... & ... & a_j & ... & a_0 & ... & X^{q-j-2}P \\
\vdots & \ddots & \ddots & ... & ... & ... & \ddots & ... & \ddots & \vdots \\
\vdots & ... & \ddots & \ddots & ... & ... & ... & \ddots & ... & \vdots \\
\vdots & ... & ... & \ddots & \ddots & ... & ... & ... & \ddots & \vdots \\
0 & ... & ... & ... & 0 & a_p & ... & ... & ... & P \\
0 & ... & ... & ... & ... & 0 & b_q & ... & ... & Q \\
\vdots & ... & ... & ... & \iddots & \iddots & ... & ... & \iddots & \vdots \\
\vdots & ... & ... & \iddots & \iddots & ... & ... & \iddots & ... & \vdots \\
\vdots & ... & \iddots & \iddots & ... & ... & \iddots & ... & ... & \vdots \\
\vdots & \iddots & \iddots & ... & ... & \iddots & ... & ... & ... & \vdots \\
0 & b_q & ... & ... & b_j & ... & ... & \iddots & ... & X^{p-j-2}Q \\
b_q & ... & ... & b_j & ... & ... & ... & ... & ... & X^{p-j-1}P
\end{bmatrix}$$

Pour calculer son déterminant, on peut faire un développement par rapport à la dernière colonne (et en particulier en fonction des coefficients X^k). Or pour tour $k < p+q-2*j$, la k-ième colonne est la colonne des coefficients des polynômes $(X^{q-j-1}P, ...XP, P, Q, ..., X^{p-j-1}Q)$ de degré p+q-j-k, et est donc identique à la dernière colonne lors du développement pour ce degré. Le plus grand degré non nul du déterminant est donc $p+q-j-(p+q-2*j) = j$, et le déterminant associé est $S_Resj(P,Q)$.

Théorème Pour $P, Q \in \mathbb{D}[X]$, de degré respectif p et q tels que $p > q$, notant pour $j < p, s_j = S_Resj(P,Q)$ et t_j le coefficient dominant de $S_ResPj(P,Q)$ et $s_p = t_p = 1$, il existe une suite d'indice $(i_k)_{0<k<J+1}$ tels que :

— $\forall 1 < j < J, deg(S_Resi_j(P,Q)) = i_j$ et $deg(S_Resi_j - 1(P,Q)) = i_{j+1}$

— $\forall j < i_J, S_ResPj(P,Q) = 0$

— $\forall j < J, \forall i_j - 1 > k > i_{j+1}, S_ResPk(P,Q) = 0$ et $t_{i_j-1}S_ResPi_{j+1}(P,Q) = s_{i_{j+1}}S_ResPi_j - 1(P,Q)$

—

Ce théorème donne une méthode de calcul des sous-résultants. On se référera à l'annexe pour une démonstration.

Lemme $\epsilon_{p+q-2j}(-1)^{q-j} = \epsilon_{p-q}$

Démonstration $\epsilon_{p+q-2j}(-1)^{q-j} = \epsilon_{p-q} \leftrightarrow \epsilon_{p+q-2j}\epsilon_{p-q} = (-1)^{q-j} = (-1)^{q+j}$

Or $\frac{1}{2}(p+q-2j)(p+q-2j+1) + \frac{1}{2}(p-q)(p-q-1) = \frac{1}{2}(p^2+pq-2pj-p+pq+q^2-2qj-q-2pj-2qj+4j^4+2j+p^2-2pq+q^2-p+q) \equiv \frac{1}{2}(2p^2+2q^2-2p+2j)[2] \equiv (p(p-1)+j+q^2)[2] \equiv j+q^2[2] \equiv j+q[2]$ d'où le résultat.

Dans la suite P et Q sont deux polynômes de $\mathbb{D}[X]$ de degré respectivement p et q. On précisera quand nécessaire l'ordre voulu entre p et q, et on note $P = \sum_{i \leq p} a_i X^i$ et $Q = \sum_{i \leq q} b_i X^i$

4 Calcul du signe de Q sur les zéros de P

Le but va être de calculer le nombres de racines de P en lesquelles Q est positif, négatif, nul. On définit ainsi :

$$nb_P(Q)[-1] = |\{z \in Zer(P) | Q(z) < 0\}|$$
$$nb_P(Q)[0] = |\{z \in Zer(P) | Q(z) = 0\}|$$
$$nb_P(Q)[1] = |\{z \in Zer(P) | Q(z) > 0\}|$$

Pour calculer ces nombres, nous allons passer par plusieurs étapes intermédiaires. Nous allons partir des sous résultants que l'on vient de voir, puis calculer le PmV, puis l'index de Cauchy et enfin la question de Tarski, qui permettra alors enfin de trouver rapidement le résultat voulu. Nous allons définir puis voir comment la question de Tarski résout le problème , puis comment cette dernière est résolue par l'indice de Cauchy, ...

4.1 La question de Tarski

Définition

$$TaQ(Q, P) = \sum_{z \in Zer(P)} sign(Q(z))$$

Proposition La question de Tarski permet de retrouver les compteurs de racines.

Démonstration

$$TaQ(1, P) = \sum_{z \in Zer(P)} sign(1(z)) = nb_P(Q)[1] + nb_P(Q)[-1] + nb_P(Q)[0]$$
$$TaQ(Q, P) = \sum_{z \in Zer(P)} sign(Q(z)) = nb_P(Q)[1] - nb_P(Q)[-1]$$
$$TaQ(Q^2, P) = \sum_{z \in Zer(P)} sign(Q^2(z)) = nb_P(Q)[1] + nb_P(Q)[-1]$$

En notant a, b et c les nombres des lignes respectivement 1, 2 et 3 on obtient :

$$nb_P(Q)[0] = a - b$$
$$nb_P(Q)[1] = \frac{b + c}{2}$$
$$nb_P(Q)[-1] = \frac{b - c}{2}$$

4.2 L'indice de Cauchy

Définition

$$Ind(Q/P) = \frac{1}{2} \sum_{z \in Pole(Q/P)} sign((Q/P)(z^+)) - sign((Q/P)(z^-))$$

Lemme On peut toujours supposer $q < p$ pour calculer l'indice de Cauchy.

Démonstration Soit a_p le coefficient dominant de P, et supposons que $q = p$. Alors la division euclidienne de $a_p^{2\lceil \frac{q-p+1}{2} \rceil}Q$ par P donne deux polynômes D et R tel que $a_p^{2\lceil \frac{q-p+1}{2} \rceil}Q = PD + R$. Alors, puisque D n'a pas de pôle, on a : $Ind(Q/P) = Ind(R/P)$. La multiplication par une puissance paire de a_p préserve le signe et R est obtenu par multiplications, additions et soustractions, de sorte que l'on peut l'obtenir en restant dans l'anneau $\mathbb{D}$.

Proposition

$$TaQ(Q, P) = Ind(P'Q/P)$$

Démonstration Soit z une racine de P d'ordre de multiplicité μ. Alors $P'Q/P = Q(\frac{\mu}{X-z} + R)$ où R est une fraction rationnelle sans pôle en z.

Si $Q(z) = 0$ alors $P'Q/P$ n'a pas de pôle en z. Sinon $sign((P'Q/P)(z^+)) = sign(Q(z))$ et $sign((P'Q/P)(z^-)) = -sign(Q(z))$. On en déduit le résultat.

4.3 Le PmV ou permanence minus variations

Définition Soit $s = (s_p, ..., s_0)$ une liste de réels de premier terme non nul. On définit s' comme étant la plus petite liste vérifiant $s = (s_p, 0, ..., 0) \cdot s'$. Alors :

$$PmV(s) = \begin{cases} 0 \text{ si s' } = \emptyset \\ PmV(s') + \epsilon_{p-q} sign(s_p s_q) \text{ si } s' = (s_q, ...s_0) \text{ et que } p - q \text{ est pair} \\ PmV(s') \text{ sinon} \end{cases} \quad (1)$$

Propriété D'après la définition, il est immédiat que si $(x_p, ...x_0)$ est tel que $sign(x_p) = ... = sign(x_0) \neq 0$, alors $PmV(x_p s_p, ..., x_0 s_0) = PmV(s_p, ..., s_0)$.

On note $sRes = (sRes_p, ..., sRes_0)$.

Proposition Si $p > q$ alors $PmV(sRes(P, Q)) = Ind(Q/P)$.

Démonstration Soit $R = Rem(P, Q)$ et C le quotient de P par Q. Si $R = 0$ alors

4.4 L'encodage de Thom

Définition Si $p > 0$ et $x \in \mathbb{R}$, on définit le $P - encodage$ de x comme le vecteur

$$\sigma_P(x) = (sign(P(x)), sign(P'(x)), ...sign(P^{(p)}(x)))$$

Un $P-code$ est alors défini comme un vecteur de signes ayant pour support $\{0, ..., deg(P)\}$.

Proposition Soit σ un $P-code$. Alors :

1. $\sigma_P^{-1}(\sigma)$ est soit vide, soit un point, soit un intervalle.
2. Si $x \neq x'$ sont deux racines de P, alors $\sigma_P(x) \neq \sigma_P(x')$.
3. Soit $x \neq x'$ tel que $\sigma_P(x) \neq \sigma_P(x')$. Alors $x < x'$ si et seulement si, en notant k le plus grand indice tel que $\sigma_P(x)[k] \neq \sigma_P(x')[k]$:

4.5 Les systèmes triangulaires

Jusqu'à présent nous n'avons vu dans les parties précédentes que des propriétés effectives d'une représentation de $\mathbb{D}$. Nous allons maintenant considérer des représentations spécifiques à des sous-anneaux réels de la forme $\mathbb{D} = \mathbb{Q}[\alpha_1, ...\alpha_l]$ où les α_i sont des nombres algébriques. De telles représentations sont appelées systèmes triangulaires et nous allons voir en quoi elles sont de signe effectif. Nous noterons $lcof(P)$ le coefficient dominant d'un polynôme $P \in \mathbb{D}[X]$

Définition : Système Triangulaire Soit $\{(n_i, P_i)\}_{i=1}^{l}$ tel que pour tout i, $n_i \in \mathbb{N}^*$ et $P_i \in \mathbb{Q}[X_1, ...X_{i-i}][X_i]$ de degré $p_i > 0$? Soit $(\alpha_1, ...\alpha_l)$ des réels. Alors $\{(n_i, P_i)\}_{i=1}^{l}$ est un système triangulaire de niveau l pour $(\alpha_1, ...\alpha_l)$ si :

— a_1 est la n_1^e racine de P_1 ;
— Pour tout $1 \leq i \leq l$, $P_{i+1}[p_{i+1}](\alpha_1, ...\alpha_l) \neq 0$ et α_{i+1} est la n_{i+1}^e racine du polynôme $P_{i+1}(\alpha_1, ...\alpha_l) \in \mathbb{Q}[\alpha_1, ...\alpha_i][X_{i+1}]$.

Par convention, un système triangulaire de niveau 0 est l'ensemble vide . On remarque qu'on ne sait pas *a priori* dire si un système $\{(n_i, P_i)\}_{i=1}^{l}$ est triangulaire pour une séquence de réels $(\alpha_1, ...\alpha_l)$. Étant donné un système triangulaire $\{(n_i, P_i)\}_{i=1}^{l}$, une représentation d'un élément de $\mathbb{Q}[\alpha_1, ...\alpha_l]$ n'est rien d'autre qu'un polynôme $P \in \mathbb{Q}[X_1, ...X_l]$ qui dénote $P(\alpha_1, ...\alpha_l)$.