JOCELYNE ROUYER

Preuves de terminaison de systèmes de réécriture fondées sur les interprétations polynomiales. Une méthode basée sur le théorème de Sturm

Informatique théorique et applications, tome 25, nº 2 (1991), p. 157-169.

<http://www.numdam.org/item?id=ITA_1991__25_2_157_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 25, n° 2, 1991, p. 157 à 169)

PREUVES DE TERMINAISON DE SYSTÈMES DE RÉÉCRITURE FONDÉES SUR LES INTERPRÉTATIONS POLYNOMIALES. UNE MÉTHODE BASÉE SUR LE THÉORÈME DE STURM (*)

par Jocelyne ROUYER [1]

Communiqué par Jean-Éric PIN

Résumé. – *Cet article fournit une méthode pour prouver automatiquement des inégalités sur des polynômes à coefficients entiers. Cette méthode est fondée sur un théorème dû à Sturm et s'applique aux preuves de terminaison des systèmes de réécriture.*

Abstract. – *This paper provides a method to mechanically prove inequalities on polynomials with integer coefficients. This method is founded on a theorem due to Sturm and applies to termination of rewriting systems.*

1. INTERPRÉTATION POLYNOMIALE POUR PROUVER LA TERMINAISON D'UN SYSTÈME DE RÉÉCRITURE

Nous rappelons dans ce paragraphe les résultats sur les preuves de terminaison de systèmes de réécriture qui ont motivé notre étude (*voir* [5] pour une présentation plus complète).

Soit F un ensemble de symboles de fonctions, $\{x_1, \ldots, x_m\}$ un ensemble de variables, $T(F, \{x_1, \ldots, x_m\})$ l'ensemble des termes sur $\{x_1, \ldots, x_m\}$ et $(W, >)$ un ensemble bien ordonné.

Si on associe à chaque fonction f de F, d'arité k, une fonction f_τ: $W^k \to W$ vérifiant la propriété:

$$\forall (w, w') \in W^2, \quad w > w' \quad \Rightarrow \quad f_\tau(\ldots w \ldots) > f_\tau(\ldots w' \ldots) \tag{1}$$

(*) Reçu Juin 1988, revisé Juillet 1989.
[1] CRIN, B.P. n° 239, 54506 Vandœuvre-lès-Nancy.

0988-3754/91/02 157 13/$3.30/© AFCET-Gauthier-Villars

et si on pose, pour tout terme $f(t_1, \ldots, t_k)$ de $T(F, \{x_1, \ldots, x_m\})$

$$\tau(f(t_1, \ldots, t_k)) = f_\tau(\tau(t_1), \ldots, \tau(t_k))$$

on dit que l'application $\tau: T(F, \{x_1, \ldots, x_m\}) \rightarrow W$ ainsi définie est une fonction de terminaison.

THÉORÈME 1 (Manna-Ness) : *Un système de réécriture R sur $T(F, \{x_1, \ldots, x_m\})$ termine si et seulement s'il existe un ensemble bien ordonné $(W, >)$ et une fonction de terminaison $\tau: T(F, \{x_1, \ldots, x_m\}) \rightarrow W$ telle que :*

$$\tau(\sigma(g)) > \tau(\sigma(d))$$

pour toute règle $g \rightarrow d$ de R et toute substitution σ.

On peut en particulier prendre pour W l'ensemble des fonctions de N^m dans N muni de l'ordre bien fondé suivant :

$$u < v \iff \forall (a_1, \ldots, a_m) \in N^m, u(a_1, \ldots, a_m) < v(a_1, \ldots, a_m).$$

Si on associe à chaque fonction f de F, d'arité k, une fonction polynomiale de k variables notée $[f](X_1, \ldots, X_k)$ à coefficients entiers naturels, on peut lui associer une fonction f_τ de W^k dans W en posant, pour toutes fonctions $h_1, \ldots, h_k$ de N^m dans N:

$$f_\tau(h_1, \ldots, h_k)(X_1, \ldots, X_m) = [f](h_1(X_1, \ldots, X_m), \ldots, h_k(X_1, \ldots, X_m)).$$

$[f]$ ayant des coefficients entiers naturels, f_τ vérifiera la propriété (1). On pourra donc définir une fonction de terminaison τ de $T(F, \{x_1, \ldots, x_m\})$ dans W en posant :

$$[x_i](X_1, \ldots, X_m) = X_i \qquad \textit{pour} \quad 1 \leqq i \leqq m$$
$$\tau(f(t_1, \ldots, t_k))(X_1, \ldots, X_m) = [f](\tau(t_1)(X_1, \ldots, X_m), \ldots, \tau(t_k)(X_1, \ldots, X_m)).$$

Pour prouver qu'un système R de réécriture termine en utilisant des interprétations polynomiales, il suffira de prouver que l'on a, pour toute règle $g \rightarrow d$ de R et toute substitution σ :

$$\tau(\sigma(g)) > \tau(\sigma(d))$$

ce qui équivaut par définition à :

$$\forall (X_1, \ldots, X_m) \in N^m, \quad \tau(\sigma(g))(X_1, \ldots, X_m) > \tau(\sigma(d))(X_1, \ldots, X_m)$$

ou encore à :

$$\forall (X_1, \ldots, X_m) \in N^m, \quad [g](\sigma(X_1), \ldots, \sigma(X_m)) > [d](\sigma(X_1), \ldots, \sigma(X_m)).$$

Ceci sera vérifié si on a :

$$[g] > [d].$$

On est donc ramené à prouver qu'un polynôme est plus grand qu'un autre sur les entiers, ce qui revient à démontrer des inégalités de la forme :

$$P(X_1, \ldots, X_m) > 0$$

où P est un polynôme à coefficients entiers.

Ce problème ne peut pas être résolu sur les entiers car il est équivalent au dixième problème de Hilbert [3]. Pour résoudre des inégalités de ce type sur les réels, Tarski [8] a donné une méthode basée sur l'élimination des quantificateurs. Collins [2] a amélioré cette méthode en introduisant la décomposition cylindrique algébrique et l'a implantée mais le temps de calcul est encore important.

Poursuivant le travail de Lankford [7], A. Ben Chérifa et P. Lescanne [1], nous cherchons une méthode de calcul efficace, non pour résoudre complètement des inégalités de la forme $P(X_1, \ldots, X_m) > 0$, mais pour déterminer si elles sont vraies ou non sur un ensemble de la forme $[d, +\infty[^m$, dans lequel restent les interprétations des termes. La méthode que nous proposons dans la suite de cet article pour prouver la positivité de polynômes à m variables sur des ensembles de la forme $[d, +\infty[^m$ est basée sur le théorème de Sturm.

2. THÉORÈME DE STURM

Soit P une fonction polynôme de la variable x, de degré n, on définit la suite de Sturm associée à P de la façon suivante [6] :

P_0 est égale à P

P_1 est la dérivée de P

P_2 est l'opposée du reste de la division euclidienne de P_0 par P_1

P_3 est l'opposée du reste de la division euclidienne de P_1 par P_2

et ainsi de suite jusqu'à P_n.

THÉORÈME 1 (Sturm) : *Soit a et b deux réels tels que $a<b$, $N_P(a)$ et $N_P(b)$ les nombres de changements de signes de la suite $P_0(x), \ldots, P_n(x)$ pour $x=a$*

et $x=b$, *le nombre de racines réelles de* P *comprises entre* a *et* b *est* $N_P(a)-N_P(b)$, *si* P *ne s'annule ni en* a, *ni en* b.

Remarque : Si $P_i(a)$ est nul, il n'intervient pas dans le décompte du nombre de changements de signes de la suite $P_0(a), \ldots, P_n(a)$.

Calculs pratiques

On peut obtenir, sans faire de divisions, une suite de fonctions polynômes dont les signes sont les mêmes que ceux de la suite de Sturm.

Soit $P_0(x)=\sum_{i=0}^{n} a_i x^{n-i}$ et $P_1(x)=\sum_{i=0}^{n-1} b_i x^{n-1-i}$, P_1 étant la dérivée de P_0, on écrit les deux lignes suivantes:

$$\begin{array}{c|l} P_0 & a_0\ a_1\ \ldots\ a_{n-1}\ a_n \\ P_1 & b_0\ b_1\ \ldots\ b_{n-1} \end{array}$$

A partir de ces deux lignes on en calcule une troisième en faisant des produits en croix:

$$\forall i, \quad 0 \leqq i \leqq n-1, \qquad c_i=b_0 a_{i+1}-a_0 b_{i+1}$$

puis on calcule de la même façon $d_i=c_0 b_{i+1}-b_0 c_{i+1}$ pour $0 \leqq i \leqq n-2$.

On obtient ainsi, en quatrième ligne, les coefficients de P_2 à un coefficient multiplicatif positif près. On continue de la même façon à calculer P_{i+1} en fonction de P_i et P_{i-1} en créant une nouvelle ligne de calcul intermédiaire, mais en ne réutilisant pas la précédente.

Exemple :

$$P_0(x)=x^3-2x^2+x+1$$

$$P_1(x)=3x^2-4x+1$$

$$\begin{array}{c|rrrr} P_0 & 1 & -2 & 1 & 1 \\ P_1 & 3 & -4 & 1 & \\ & -2 & 2 & 3 & \\ P_2 & 2 & -11 & & \\ & 25 & 2 & & \\ P_3 & -279 & & & \end{array}$$

On a donc:

$$P_2(x)=2x-11$$

$$P_3(x)=-279.$$

Remarque : Le terme qui manque dans la ligne précédente lorsqu'on calcule une ligne intermédiaire est prix égal à 0.

Pour trouver le nombre de racines réelles supérieures à 1, on calcule les nombres de changements de signes dans la suite $P_0(x)$, $P_1(x)$, $P_2(x)$, $P_3(x)$ en 1 et en $+\infty$. Le signe de $P_i(+\infty)$ est celui du coefficient du terme de plus haut degré de P_i. Le signe de $P_i(1)$ est celui de la somme des coefficients de P_i.

	1	$+\infty$
0	+	+
1	0	+
2	−	+
3	−	−
N_P	1	1

On obtient $N_P(1)-N_P(+\infty)=0$. Le polynôme P_0 n'admet donc aucune racine réelle supérieure à 1.

3. ÉTUDE DE LA POSITIVITÉ D'UN POLYNÔME

Bien que le théorème de Sturm porte sur les polynômes à une variable, nous nous proposons de l'utiliser pour déterminer si une inégalité de la forme $P(X_1, \ldots, X_m)>0$ ou $P(X_1, \ldots, X_m)<0$ est vraie ou non sur un ensemble du type $[d, +\infty[^m$, P étant un polynôme en $X_1, \ldots, X_m$.

On peut dire que cette inégalité est vraie si et seulement si, pour $(X_2, \ldots, X_m)$ fixé quelconque dans $[d, +\infty[^{m-1}$, on a :

$$P_0(X_1)>0 \quad sur \ [d, +\infty[\tag{2}$$

en posant $P_0(X_1)=P(X_1, \ldots, X_m)$.

Or, un polynôme à une variable qui ne s'annule pas reste du signe du coefficient de son terme de plus haut degré, donc si $a_{0,0}$ est le coefficient du terme de plus haut degré de P_0, on a :

$$(2) \quad \Leftrightarrow \quad \begin{cases} \text{(i) } a_{0,0}>0 \\ \text{(ii) } P_0 \textit{ ne s'annule pas sur } [d, +\infty[\end{cases}$$

D'après le théorème de Sturm, P_0 ne s'annule pas sur $[d, +\infty[$ si et seulement si le nombre de changements de signes de la suite de Sturm associée à P_0 est le même en d qu'en $+\infty$. Il faut donc déterminer les signes de $P_i(d)$ et $P_i(+\infty)$ pour les polynômes P_i de la suite de Sturm associée à P_0.

Le signe de $P_i(+\infty)$ est celui du coefficient $a_{i,0}$ du terme de plus haut degré de P_i, qui est un polynôme en $X_2, \ldots, X_m$. Les polynômes P_i sont des polynômes en X_1 dont les coefficients sont des polynômes en $X_2, \ldots, X_m$, de même que $a_{i,0}$. Ces polynômes peuvent être considérés comme des polynômes en X_2, dont les coefficients sont des polynômes en $X_3, \ldots, X_m$.

S'ils ne s'annulent pas pour $X_2 \in [d, +\infty[$, c'est-à-dire si la condition déterminée par le théorème de Sturm est vérifiée, leur signe est celui du coefficient de leur terme de plus haut degré qui est un polynôme en $X_3, \ldots, X_m$, dont on peut donc chercher à déterminer le signe de manière analogue.

Remarque : Si un de ces polynômes, autre que P_n, si n est le degré de P_0, s'annule en d mais que le nombre de changements de signes de la suite de Sturm qui lui est associée est le même en d qu'en $+\infty$, on peut affirmer qu'il ne s'annule pas sur l'intervalle ouvert $]d, +\infty[$, et par conséquent, qu'il reste du signe du coefficient de son terme de plus haut degré. Par contre, si l'on obtient $N(d)-N(+\infty)=1$, on ne peut pas conclure, la racine comptabilisée pouvant être d ou une racine appartenant à $]d, +\infty[$.

La méthode appliquée récursivement à tous les polynômes de la suite de Sturm associée à P_0 permettra de déterminer le signe de ces polynômes en d et en $+\infty$, si ces polynômes ne s'annulent pas pour des valeurs des variables supérieures ou égales à d, et même strictement supérieures à d pour les polynômes de la suite autres que P_n.

On pourra alors déterminer le nombre de changements de signes de la suite de Sturm associée à P_0 en d et en $+\infty$ et savoir si le polynôme P étudié garde ou non un signe constant sur $[d, +\infty[^m$.

Exemple 1 : Soit $P(X, Y)=X^2+Y^2-2XY+1$.

Cet exemple d'école montre que la méthode que nous proposons peut réussir dans des cas où la méthode proposée par A. Ben Chérifa et P. Lescanne échoue. L'inégalité $P(X, Y)>0$ ne peut en effet être démontrée ni pour X, Y entiers supérieurs ou égaux à 1, ni même pour X, Y strictement supérieurs à 1, par la méthode proposée dans [1], qui consiste à majorer les monômes négatifs du polynôme considéré par des monômes positifs, car on ne peut majorer le monôme $-2XY$ ni par X^2, ni par Y^2.

Appliquons la méthode proposée précédemment avec $d=1$.

On a : $a_{0,0}=1$ donc $a_{0,0}>0$. La condition (i) est donc vérifiée. Pour démontrer la condition (ii), on pose $P_0(X)=X^2-2YX+Y^2+1$. On a alors $P_1(X)=2X-2Y$, et on calcule, par la méthode décrite précédemment, la suite de Sturm associée à P_0. On obtient :

$$\begin{array}{c|lll} P_0 & 1 & -2Y & Y^2+1 \\ P_1 & 2 & -2Y & \\ & -2Y & 2Y^2+2 & \\ P_2 & -4 & & \end{array}$$

et :

$$\begin{array}{c|cc} & 1 & +\infty \\ \hline 0 & sg(Y^2-2Y+2) & + \\ 1 & sg(-2Y+2) & + \\ 2 & - & - \end{array} \tag{1}$$

Si le polynôme Y^2-2Y+2 ne s'annule pas pour $Y\in[1, +\infty[$, son signe est le même que celui du coefficient de son terme de plus haut degré.

Cherchons si la condition déterminée par le théorème de Sturm est vérifiée pour le polynôme $Q_0(Y)=Y^2-2Y+2$.

On a $Q_1(Y)=2Y-2$, d'où les tableaux :

$$\begin{array}{c|lll} Q_0 & 1 & -2 & 2 \\ Q_1 & 2 & -2 & \\ & -2 & 4 & \\ Q_2 & -4 & & \end{array}$$

et :

$$\begin{array}{c|cc} & 1 & +\infty \\ \hline 0 & + & + \\ 1 & 0 & + \\ 2 & - & - \\ \hline N_Q & 1 & 1 \end{array}$$

On a bien $N_Q(1)-N_Q(+\infty)=0$ et par suite $sg(Y^2-2Y+2)=+$.

Le polynôme $-2Y+2$ s'annule pour $Y=1$, mais pas pour $Y>1$. On a en effet, en posant $R_0(Y)=-2Y+2$:

$$R_1(Y)=-2$$

donc :

	1	$+\infty$
0	0	$-$
1	$-$	$-$
N_R	0	0

et $N_R(1)-N_R(+\infty)=0$, ce qui prouve que R_0 ne s'annule pas sur l'intervalle ouvert $]1, +\infty[$, d'après la remarque précédente. Le polynôme $-2Y+2$ est donc du signe du coefficient de son terme de plus haut degré, c'est-à-dire négatif (au sens large) sur l'intervalle $[1, +\infty[$.

On peut à présent reprendre le tableau (1) et le compléter. On obtient :

	1	$+\infty$
P_0	$+$	$+$
P_1	$-$	$+$
P_2	$-$	$-$
N_P	1	1

On a $N_P(1)-N_P(+\infty)=0$. La condition (ii) est donc vérifiée. On en conclut que l'inégalité $P(X, Y)>0$ est vraie sur $[1, +\infty[^2$.

Exemple 2 : Considérons le système de réécriture sur la dérivation symbolique par rapport à x défini par :

$$\begin{aligned}
&D_x x \to 1\\
&D_x a \to 0 \quad \textit{a étant un symbole de constante}\\
&D_x(y+z) \to D_x y + D_x z\\
&D_x(y^*z) \to z^*D_x y + y^*D_x z\\
&D_x(y-z) \to D_x y - D_x z\\
&D_x(-y) \to -D_x y\\
&D_x(y/z) \to D_x y/z - y^*D_x z/z^2\\
&D_x(ln(y)) \to D_x y/y\\
&D_x(y^z) \to z^*y^{z-1*}D_x y + y^{z*}(ln(y))^*D_x z
\end{aligned} \tag{I}$$

et les interprétations des symboles de fonctions suivantes, données dans [5]:

$$[+](Y, Z) = [Y] + [Z]$$
$$[*](Y, Z) = [Y] + [Z]$$
$$[-](Y, Z) = [Y] + [Z]$$
$$[-Y] = [Y] + 1$$
$$[/](Y, Z) = [Y] + [Z]$$
$$[ln Y] = [Y] + 1$$
$$[\wedge](Y, Z) = [Y] + [Z]$$
$$[D_x Y] = [Y]^2$$

Dershowitz a donné dans [5] une démonstration de la terminaison de ce système de réécriture, corrigée dans [4], qui ne précisait pas sur quel ensemble on pouvait se placer pour faire cette preuve. Nous allons exhiber, grâce à notre méthode, le plus petit entier c tel qu'en posant $[a] = c$, on puisse prouver la terminaison du système de réécriture. Il faut que, pour toute valeur des variables supérieure ou égale à c, les inégalités suivantes soient vraies:

$$X^2 > c \tag{1}$$
$$c^2 > c \tag{2}$$
$$(X_1 + X_2)^2 > X_1^2 + X_2^2 \tag{3}$$
$$(X_1 + X_2)^2 > X_1^2 + X_2^2 + X_1 + X_2 \tag{4}$$
$$(X_1 + X_2)^2 > X_1^2 + X_2^2 \tag{5}$$
$$(X_1 + 1)^2 > X_1^2 + 1 \tag{6}$$
$$(X_1 + X_2)^2 > X_1^2 + X_2^2 + X_1 + 2 X_2 + c \tag{7}$$
$$(X_1 + 1)^2 > X_1^2 + X_1 \tag{8}$$
$$(X_1 + X_2)^2 > X_1^2 + X_2^2 + 3 X_1 + 3 X_2 + c + 1 \tag{9}$$

Les inégalités (1) et (2) sont vraies si c est strictement supérieur à 1.

Nous supposerons donc dans la suite $c \geqq 2$.

Les inégalités (3) et (5) se ramènent à $2 X_1 X_2 > 0$ qui est vraie.

L'inégalité (4) s'écrit $2 X_1 X_2 - X_1 - X_2 > 0$. Démontrons cette inégalité par la méthode proposée précédemment.

On pose:

$$P_0(X_1) = (2 X_2 - 1) X_1 - X_2$$

d'où :

$$P_1(X_1)=2X_2-1$$

On en déduit le tableau :

	c	$+\infty$
P_0	$sg((2c-1)X_2-c)$	$sg(2X_2-1)$
P_1	$sg(2X_2-1)$	$sg(2X_2-1)$

Le polynôme $(2c-1)X_2-c$ est strictement positif pour $X_2>c/(2c-1)$ donc pour $X_2\geqq c$. Le polynôme $2X_2-1$ est aussi strictement positif sur $[c, +\infty[$. Il n'y a donc pas de changement de signe dans la suite de Sturm associée à P_0 en c et en $+\infty$. P_0 reste du signe du coefficient de son terme de plus haut degré $2X_2-1$, c'est-à-dire strictement positif, sur l'intervalle $[c, +\infty[$, ce qui prouve l'inégalité (4).

L'inégalité (6) se ramène à $2X_1>0$ qui est vraie.

L'inégalité (7) s'écrit $2X_1X_2-X_1-2X_2-c>0$. Pour démontrer cette inégalité posons :

$$P_0(X_1)=(2X_2-1)X_1-2X_2-c.$$

On a :

$$P_1(X_1)=2X_2-1$$

d'où le tableau :

	c	$+\infty$
P_0	$sg(2(c-1)X_2-2c)$	$sg(2X_2-1)$
P_1	$sg(2X_2-1)$	$sg(2X_2-1)$

Le polynôme $2(c-1)X_2-2c$ est strictement positif pour $X_2>c/(c-1)$ donc pour $X_2\geqq c$, à condition de prendre c strictement supérieur à 2. Le polynôme $2X_2-1$ étant aussi strictement positif sur $[c, +\infty[$, il n'y a aucun changement de signe dans la suite de Sturm associée à P_0 en c et en $+\infty$. P_0 reste donc du signe du coefficient de son terme de plus haut degré $2X_2-1$, c'est-à-dire strictement positif, sur $[c, +\infty[^2$ et l'inégalité (7) est vérifiée.

L'inégalité (8) se ramenant à $X_1+1>0$ ne pose pas de problème.

La dernière inégalité s'écrit $2X_1X_2-3X_1-3X_2-c-1>0$.

On pose:

$$Q_0(X_1) = (2X_2-3)X_1 - 3X_2 - c - 1$$

d'où:

$$Q_1(X_1) = 2X_2 - 3$$

et le tableau:

	c	$+\infty$
Q_0	$sg((2c-3)X_2-4c-1)$	$sg(2X_2-3)$
Q_1	$sg(2X_2-3)$	$sg(2X_2-3)$

Le polynôme $(2c-3)X_2-4c-1$ est strictement positif pour X_2 strictement supérieur à $(4c+1)/(2c-3)$. Il le sera donc pour tout X_2 supérieur ou égal à c si et seulement si on a:

$$c > \frac{4c+1}{2c-3}$$

ce qui équivaut à $2c^2-7c-1>0$ et par un calcul élémentaire nous donne comme solution $c \geqq 4$.

On peut donc démontrer que l'interprétation du membre gauche de la dernière règle du système (I) est strictement supérieure à celle du membre droit en utilisant les interprétations polynomiales sur l'ensemble des entiers supérieurs ou égaux à 4 définies plus haut et en posant $[a]=4$.

Les autres inégalités étant vraies pour toutes les valeurs des variables supérieures ou égales à c si c est strictement supérieur à 2, on prouve ainsi que le système de réécriture (I) termine.

4. EXTENSION DE LA MÉTHODE DANS UN CAS PARTICULIER

On ne peut pas déterminer le signe d'un polynôme par la méthode précédente, si un des polynômes de la suite de Sturm associée, appelons le R, s'annule sur l'intervalle $]d, +\infty[$. Si le polynôme R est à une seule variable, on peut aller plus loin en déterminant la multiplicité de la (ou des) racine(s).

1[er] *cas*: Si le polynôme R est de degré n et si, dans la suite de Sturm associée, R_n n'est pas nul, le polynôme R n'admet que des racines simples. Il change donc de signe sur l'intervalle $]d, +\infty[$.

2[e] *cas*: Si R_n est nul et si R n'adment qu'une seule racine dans l'intervalle $]d, +\infty[$, c'est-à-dire si $N(d)-N(+\infty)=1$ et $R(d)\neq 0$, on peut déterminer la multiplicité de cette racine.

Si k est le rang à partir duquel les polynômes R_i de la suite de Sturm associée à R sont nuls, la racine est d'ordre $n-k+2$.

Si la racine est d'ordre pair, donc si $n-k$ est pair, le polynôme R reste du signe du coefficient de son terme de plus haut degré sur l'intervalle $]d, +\infty[$.

Si $n-k$ est impair, R change de signe sur cet intervalle.

3[e] *cas*: Si R_n est nul et si R admet plusieurs racines dans l'intervalle $]d, +\infty[$, R changera de signe si et seulement si au moins une de ses racines est d'ordre impair.

Soit $Q_1 = pgcd(R, R')$, les racines de Q_1 sont les racines x_i de R à l'ordre $n_i - 1$, si n_i est la multiplicité de la racine x_i dans R.

Soit $Q_2 = pgcd(Q_1, Q_1')$, les racines de Q_2 sont les racines x_i de R à l'ordre $n_i - 2$.

Si l'on réitère le procédé jusqu'à ce que l'on obtienne un polynôme constant, le polynôme Q_j obtenu au rang précédent n'aura que des racines simples et ces racines seront des racines de R d'ordre $j+1$.

Si $j+1$ est impair, on peut affirmer que le polynôme R change de signe et s'arrêter.

Dans le cas contraire, les racines de R de plus grand ordre sont d'ordre pair, il faut étudier les autres racines. Pour cela il suffit d'utiliser le même procédé en partant du polynôme R/Q_j^{j+1}.

Si le polynôme R/Q_j^{j+1} est constant, c'est que R n'a que des racines d'ordre pair, on peut donc affirmer qu'il garde un signe constant (au sens large) et s'arrêter.

5. CONCLUSION

La méthode présentée dans cet article, avec l'amélioration ci-dessus, a été implantée dans un langage adapté au calcul symbolique: Maple. Elle nous a donné des résultats rapides dans les différents exemples classiques de preuve de terminaison de systèmes de réécriture testés, notamment ceux cités dans [1].

Cette méthode ne permet pas de conclure lorsqu'un des polynômes de la suite de Sturm, autre que P_0, change de signe sur l'intervalle considéré. Nous sommes en train d'étudier une méthode plus générale, mais dont le temps de calcul risque d'être supérieur.

BIBLIOGRAPHIE

1. A. Ben Cherifa and P. Lescanne, Termination of Rewriting by Polynomial Interpetretations and its Implementation, *Sci. Comput. Programming*, October 1987, Vol. *9*(2), pp. 137-160.
2. G. Collins, Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition, *Proceedings 2nd GI Conference on Automata and Formal Languages*, Springer Verlag, *Lectures Notes in Computer Science*, 1975.
3. M. Davis, Y. Matijasevic and J. Robinson. Hilbert's Tenth Problem: Positive Aspects of a Negative Solution, *in* F. E. Browder Ed., *Mathematical Developments Arising from Hilbert Problems*, American Mathematical Society, 1976, pp. 323-378.
4. N. Dershowitz, Corrigendum to Termination of Rewriting, *J. Symbolic Comput.*, 1987, Vol. *4*, pp. 409-410.
5. N. Dershowitz, Termination of Rewriting, *J. Symbolic Comput.*, 1987, Vol. *3*(1 et 2), pp. 69-116.
6. D. Knuth, *The Art of Computer Programming*, Vol. *2*, Addison Wesley, Reading Massachusetts, 2nd edition, 1981.
7. D. S. Lankford, *On Proving Term Rewriting Systems are Noetherian*, Technical Report, Louisiana Tech. University, Mathematics Dept., Ruston LA, 1979.
8. Tarski, *A Decision Method for Elementary Algebra and Geometry*, University of California Press, Berkeley, 2nd edition, 1951.