BULLETIN DE LA S. M. F.

JOOS HEINTZ
MARIE-FRANÇOISE ROY
PABLO SOLERNÓ

# Sur la complexité du principe de Tarski-Seidenberg

*Bulletin de la S. M. F.*, tome 118, n° 1 (1990), p. 101-126
<http://www.numdam.org/item?id=BSMF_1990__118_1_101_0>

*Bull. Soc. math. France,*
118, 1990, p. 101–126.

# SUR LA COMPLEXITÉ DU PRINCIPE DE TARSKI-SEIDENBERG

PAR

JOOS HEINTZ, MARIE-FRANÇOISE ROY, PABLO SOLERNÓ (*)

RÉSUMÉ. — Cet article est consacré à un algorithme d'élimination des quantificateurs dans les corps réels clos dont la complexité est simplement exponentielle en séquentiel (et polynomiale en parallèle) en le nombre de variables dès lors que le nombre d'alternances de quantificateurs est fixé.

ABSTRACT. — This paper is devoted to an algorithm for quantifier elimination in the real closed case which is of complexity single exponential in the number of variables in the sequential model (and polynomial in the parallel model) as soon as the number of alternations of quantifiers is fixed.

## 1. Introduction

*Nous remercions* Teresa KRICK *et* Henri LOMBARDI *pour l'aide qu'ils nous ont apportée et leurs nombreuses suggestions utiles concernant ce travail.*

Avant d'énoncer plus précisément notre résultat, il est nécessaire de faire quelques rappels sur la géométrie algébrique réelle et la complexité d'algorithmes.

### 1.1. Rappels sur la géométrie algébrique réelle.

Pour les notions et preuves résumées dans ce paragraphe on peut voir [3].

*Définition.* — Un *corps réel clos* est un corps ordonné où tout élément positif a une racine carrée et où tout polynôme de degré impair a une racine.

(*) Texte reçu le 31 octobre 1989, révisé le 3 avril 1990.
J. HEINTZ et P. SOLERNÓ, Intituto Argentino de Matematica, CONICET, Viamonte 1636, 1055 Buenos-Aires, Argentine.
M.-F. ROY, IRMAR, Université de Rennes I, 35042 Rennes Cedex, France.

BULLETIN DE LA SOCIÉTÉ MATHÉMATIQUE DE FRANCE 0037-9484/1990/101/$ 5.00

Dans tout l'article **A** désigne un anneau intègre et **R** un corps réel clos contenant **A**.

*Définition.* — Un *ensemble semi-algébrique* $S$ de $\mathbf{R}^n$ défini sur **A** est un ensemble défini par une combinaison booléenne d'inégalités polynomiales à coefficients dans **A**.

Beaucoup de constructions restent à l'intérieur du domaine semi-algébrique et on a les résultats suivants :

THÉORÈME (théorème de projection). — *La projection d'un ensemble semi-algébrique de* $\mathbf{R}^{n+1}$ *défini sur* **A** *sur* $\mathbf{R}^n$ *est un ensemble semi-algébrique défini sur* **A**.

THÉORÈME (composantes semi-algébriquement connexes). — *Les composantes (semi-algébriquement) connexes d'un ensemble semi-algébrique défini sur* **A** *sont en nombre fini. Ce sont des ensembles semi-algébriques définis sur* **A**.

Le théorème de projection peut se reformuler en termes logiques. On doit pour cela introduire la définition suivante.

*Définition.* — Une *formule du langage des corps ordonnés à paramètres dans* **A** est construite en un nombre fini d'étapes à partir des formules atomiques qui sont des égalités et inégalités portant sur des polynômes à coefficients dans **A**, à l'aide des connecteurs logiques (ou, et, non) et de quantificateurs ($\exists$, $\forall$) portant sur les éléments du corps. Une *formule prénexe* est une formule où tous les quantificateurs apparaissent au début de la formule. Toute formule est équivalente à une formule prénexe.

*Exemple.* — Si $S$ est un ensemble semi-algébrique de $\mathbf{R}^n$, son adhérence peut-être décrite par la formule suivante

$$\Big\{(x_1,\ldots,x_n)\in\mathbf{R}^n \mid \forall\varepsilon\geq 0\ \exists\,(y_1,\ldots,y_n)\in S \sum_{i=1,\ldots,n}(x_i-y_i)^2\leq\varepsilon^2\Big\}.$$

Le théorème de projection admet l'importante conséquence suivante qu'on démontre par induction sur le nombre de quantificateurs :

THÉORÈME (principe de Tarski-Seidenberg ou élimination des quantificateurs). — *Un sous-ensemble de* $\mathbf{R}^n$ *défini par une formule du langage des corps ordonnés à paramètres dans* **A** *est un ensemble semi-algébrique défini sur* **A**.

On en déduit le corollaire suivant.

THÉORÈME (principe de transfert). — *Soient* $\mathbf{R}'$ *un corps réel clos contenant* $\mathbf{R}$ *et* $\Phi$ *une formule du langage des corps ordonnés à paramètres dans* $\mathbf{A}$. *La formule* $\Phi$ *est vraie dans* $\mathbf{R}$ *si et seulement si elle est vraie dans* $\mathbf{R}'$.

*Notation.* — Si $\mathbf{R}'$ est un corps réel clos contenant $\mathbf{R}$ et $S$ est un ensemble semi-algébrique de $\mathbf{R}^n$ on note $S(\mathbf{R}')$ le sous-ensemble de $\mathbf{R}'^n$ défini par la même formule sans quantificateurs que $S$. Le fait que cette notation ait un sens est une conséquence facile du principe de transfert.

### 1.2. Notions de complexité d'algorithme.

Les polynômes que nous considérons sont à coefficients dans $\mathbf{A}$. Les opérations arithmétiques considérées sur $\mathbf{A}$ sont les additions, multiplications, divisions exactes (lorsqu'on sait d'avance que le rapport est encore dans $\mathbf{A}$) et déterminations du signe d'un élément de $\mathbf{A}$ (dans $\mathbf{R}$).

On évaluera la complexité des algorithmes en considérant les paramètres suivants :

- $d$ le degré total des polynômes ;
- $t$ la taille des coefficients (dans le cas où $\mathbf{A} = \mathbb{Z}$) ;
- $s$ le nombre des polynômes ;
- $n$ le nombre de variables ;
- $m$ le nombre d'alternances de quantificateurs dans une formule prénexe.

Les algorithmes sont décrits par une famille de réseaux arithmétiques sur $\mathbf{A}$ dépendant de ces divers paramètres (voir [12]).

*Définition.* — La *complexité séquentielle* (sur $\mathbf{A}$) d'un algorithme est la fonction des paramètres qui mesure la taille du réseau arithmétique donc compte le nombre (maximal) d'opérations arithmétiques sur $\mathbf{A}$ nécessaires pour l'algorithme. La *complexité séquentielle binaire* (lorsque $\mathbf{A} = \mathbb{Z}$) d'un algorithme est la fonction des paramètres qui évalue le nombre (maximal) d'opérations binaires nécessaires pour l'algorithme. La *complexité parallèle* (sur $\mathbf{A}$) est la fonction des paramètres qui mesure la la profondeur du réseau arithmétique.

Nous nous intéresserons aussi à la parallélisation des algorithmes.

*Définition.* — On dit qu'un algorithme de complexité séquentielle polynomiale (resp. simplement exponentielle, resp. doublement exponentielle) est *bien parallélisable* si sa complexité paralèle est polylog (*i.e.* polynomiale dans le log) (resp. polynomiale, resp. simplement exponentielle). La largeur du réseau arithmétique qui définit l'algorithme est alors polynomiale (resp. simplement exponentielle, resp. doublement exponentielle).

*Exemple.* — Les calculs de déterminants sont bien parallélisables : on connaît un algorithme pour le le calcul des déterminants d'une matrice à coefficients dans $\mathbf{A}$ de taille $x$ de complexité parallèle $\log^2 x$ et de complexité séquentielle polynomiale en $x$ (voir [2]).

Ce résultat permet de bien paralléliser tous les calculs à base d'algèbre linéaire.

### 1.3. Nos résultats.

Le résultat essentiel de cet article est le suivant :

*La réponse au problème de l'élimination des quantificateurs (principe de Tarski-Seidenberg) est donnée par un algorithme de complexité doublement exponentielle en m bien parallélisable.*

Ce résultat a déjà été annoncé dans [19] (voir aussi [28] et [24]). La preuve repose sur une nouvelle démonstration du résultat suivant :

*On peut décider si S est vide en complexité séquentielle simplement exponentielle, en complexité parallèle polynomiale en n (voir* [4], *et* [23], [28] [18]).

Cet énoncé d'élimination des quantificateurs est similaire à un résultat récent dans le cas algébriquement clos (voir [7], [11]).

Les problèmes mathématiquement significatifs ont un petit nombre d'alternances de quantificateurs. Les résultats ci-dessus signifient qu'ils sont résolubles en complexité simplement exponentielle (polynomiale en parallèle). C'est le cas par exemple du calcul de l'adhérence ou de l'intérieur d'un ensemble semi-algébrique, de la distance entre entre deux ensembles semi-algébriques, *etc.*

### 1.4. Historique du sujet.

Le théorème d'élimination des quantificateurs est dû à TARSKI et SEIDENBERG et a été publié au début des années 50 (voir [31], [26]). La complexité des algorithmes qu'on peut déduire de leurs démonstrations est hyperexponentielle.

Dans les travaux de COLLINS datant des années 70 on utilise les progrès du calcul formel pour obtenir un algorithme séquentiel (mais qui n'est pas bien parallélisable) polynomial en $d, s, t$ doublement exponentiel en $n$ (voir [6]).

Les résultats de BEN-OR, KOZEN et REIF [1], complétés par FITCHAS, GALLIGO et MORGENSTERN [10] donnent un algorithme doublement exponentiel en $n$, bien parallélisable.