Une généralisation du Positivstellensatz pour les corps valués algébriquement clos

Henri Lombardi *

Janvier 2000

Résumé

Nous donnons une forme généralisée du Positivstellensatz pour les corps valués algébriquement clos

English abstract

We give a generalized form of the Positivstellensatz for algebraically closed valued fields : there is an algebraic certificate when a "basic semialgebraic subset" of L^n is empty (where L is an agebraically closed valued field). Here a basic semialgebraic subset of L^n is given by a finite system of "valued sign conditions" on polynomials : being of valuation > 0, ≤ 0, $= 0$, < 0, ≥ 0, $= \infty$ or $\neq \infty$. Moreover, we give a formal abstract version of the same theorem.

Classification AMS : 12J10, 12J20, 12L05, 03F65

Mots clés : Positivstellensatz, Corps valués algébriquement clos, Mathématiques constructives.

1 Introduction

Dans [1] est donné un Positivstellensatz pour les corps valués algébriquement clos, qui généralise un résultat de Prestel et Ripoli [3]. Dans [2] une autre forme apparaît, ou du moins est suggérée. Nous expliquons dans cette note comment obtenir un Positivstellensatz qui les généralise tous.

Rappelons le Positivstellensatz de Stengle pour le cas des corps ordonnés.

Théorème 1.1 (Positivstellensatz concret) *Soit K un corps ordonné, R sa cloture réelle, et $R_{=0}, R_{\geq 0}, R_{>0}$ trois familles finies dans $K[x] = K[x_1, x_2, \cdots, x_n]$. Soit $\mathcal{M}_{>0}$ le monoïde engendré par $R_{>0}$, $\mathcal{C}_{\geq 0}$ le cone de $K[x]$ engendré par $R_{>0} \cup R_{\geq 0} \cup K^{>0}$ et $\mathcal{I}_{=0}$ l'idéal de $K[x]$ engendré par $R_{=0}$. Si le système de conditions de signe $[u(x) > 0,\ q(x) \geq 0,\ j(x) = 0]$ pour $u \in R_{>0}$, $q \in R_{\geq 0}$, $j \in R_{=0}$ est impossible dans R^n alors on peut construire une identité algébrique*

$$m + p + i = 0$$

où $m \in \mathcal{M}_{>0}$, $p \in \mathcal{C}_{\geq 0}$ et $i \in \mathcal{I}_{=0}$

*Equipe de Mathématiques, CNRS UMR 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25 030 BESANCON cedex, FRANCE, lombardi@math.univ-fcomte.fr

Dans [1] ce résultat est démontré constructivement en utilisant la notion de "présentation d'un corps ordonné" (on donne un ensemble de générateurs G et on spécifie des éléments de $\mathbb{Z}[G]$ qui doivent être nuls, strictement positifs ou positifs). On dit qu'une telle présentation *collapse* dans la théorie des corps réels clos lorsque cette théorie appliquée avec la présentation considérée est incohérente. Le Positivstellensatz de Stengle est alors une conséquence assez facile du résultat plus formel suivant.

Proposition 1.2 (Caractérisation algébrique du collapsus) *Soit $\mathcal{K} = (G; R_{=0}, R_{\geq 0}, R_{>0})$ une présentation de corps ordonné. Soit $\mathcal{I}_{=0}$ l'idéal de $\mathbb{Z}[G]$ engendré par $R_{=0}$, $\mathcal{M}_{>0}$ le monoïde engendré par $R_{>0}$, $\mathcal{C}_{\geq 0}$ le cone engendré par $R_{\geq 0} \cup R_{>0}$. Un collapsus de la presentation $\mathcal{K}$ dans la théorie des corps réels clos produit une égalité dans $\mathbb{Z}[G]$ de la forme suivante :*

$$m + q + i = 0$$

avec $m \in \mathcal{M}_{>0}$, $q \in \mathcal{C}_{\geq 0}$ et $i \in \mathcal{I}_{=0}$.

2 Présentation des résultats

Nous montrons dans la section suivante comment obtenir des résultats analogues au théorème 1.1 et à la proposition 1.2 dans le cas des corps valués.

2.1 Notations

Nous voulons parler d'un anneau de valuation V d'un corps K.

Nous considérons les prédicats $\mathrm{Vr}(x)$, $\mathrm{Rn}(x)$, $\mathrm{U}(x)$, $\mathrm{Nvr}(x)$ et $\mathrm{Nrn}(x)$, correspondant respectivement aux éléments de V, à ceux de l'idéal maximal (les "infiniment petits"), aux unités, aux éléments du corps qui ne sont pas dans V (les "infiniment grands") et à ceux qui ne sont pas dans l'idéal maximal.

Si la structure (K, V) n'est pas complètement spécifiée, elle peut être "présentée" au moyen d'un ensemble G de générateurs de K et de parties $R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}}, R_{\mathrm{Nvr}}, R_{\mathrm{Nrn}}$ de $\mathbb{Z}[G]$, qui sont des éléments x vérifiant respectivement les prédicats $x = 0$, $x \neq 0$, $\mathrm{Vr}(x)$, $\mathrm{Rn}(x)$, $\mathrm{U}(x)$, $\mathrm{Nvr}(x)$, $\mathrm{Nrn}(x)$. Cette présentation est notée $(G; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}}, R_{\mathrm{Nvr}}, R_{\mathrm{Nrn}})$.

Par rapport à l'article [1], l'élément nouveau est l'introduction des deux prédicats supplémentaires $\mathrm{Nvr}(x)$ et $\mathrm{Nrn}(x)$.

2.2 Résultats

Nous démontrons le Positivstellensatz formel et le Positivstellensatz concret suivants pour les corps valués algébriquement clos.

Théorème 2.1 (Positivstellensatz formel généralisé pour les corps valués) *Soit B un anneau et $(R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}}, R_{\mathrm{Nvr}}, R_{\mathrm{Nrn}})$ des parties de B. Soit $\mathcal{I}_{=0}$ l'idéal de B engendré par $R_{=0}$, $\mathcal{M}_{\neq 0}$ le monoïde (multiplicatif) engendré par $R_{\neq 0}$, $\mathcal{V}_{\mathrm{Vr}}$ le sous-anneau de B engendré par $R_{\mathrm{Vr}} \cup R_{\mathrm{Rn}} \cup R_{\mathrm{U}}$, $\mathcal{I}_{\mathrm{Rn}}$ l'idéal de $\mathcal{V}_{\mathrm{Vr}}$ engendré par R_{Rn}, $\mathcal{M}_{\mathrm{U}}$ le monoïde engendré par R_{U}. Les propriétés suivantes sont équivalentes :*

(1) *On a une égalité du type suivant dans B*

$$s(up_1^{\mu_1} \cdots p_k^{\mu_k} q_1^{\nu_1} \cdots q_\ell^{\nu_\ell} + j(p, q) + a(p)) + i = 0$$

avec $i \in \mathcal{I}_{=0}$, $s \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j(p,q) = j(p_1,\ldots,p_k,q_1,\ldots,q_\ell)$ *est un polynome à coefficients dans* $\mathcal{I}_{\mathrm{Rn}}$ *dans lequel les multiexposants sont tous* $\leq (\mu_1,\ldots,\mu_k,\nu_1,\ldots,\nu_\ell)$ *(pour l'ordre produit) et* $a(p) = a(p_1,\ldots,p_k)$ *est un polynome à coefficients dans* $\mathcal{V}_{\mathrm{Vr}}$ *dans lequel les multiexposants sont tous* $< (\mu_1,\ldots,\mu_k)$.

(2) *Il n'existe pas d'homomorphisme* $\phi : B \to L$ *avec* L *corps valué, son anneau de valuation* A *ayant* I_A *pour idéal maximal et* U_A *comme groupe d'unités, et* $\phi(n) = 0$ *pour* $n \in R_{=0}$, $\phi(t) \neq 0$ *pour* $t \in R_{\neq 0}$, $\phi(c) \in A$ *pour* $c \in R_{\mathrm{Vr}}$, $\phi(k) \in I_A$ *pour* $k \in R_{\mathrm{Rn}}$, $\phi(v) \in U_A$ *pour* $v \in R_{\mathrm{U}}$, $\phi(p) \notin A$ *pour* $p \in R_{\mathrm{Nvr}}$, $\phi(q) \notin I_A$ *pour* $q \in R_{\mathrm{Nrn}}$.

NB : Dans [2] est suggéré un Positivstellensatz formel du même style que le théorème 2.1, mais où interviennent seulement les deux prédicats Vr et Nvr.

Théorème 2.2 (Positivstellensatz généralisé pour les corps valués algébriquement clos) *Soit* (K, A) *un corps valué,* U_A *les unités de* A, I_A *son idéal maximal. Supposons que* (K', A') *soit une extension valuée algébriquement close de* K *(donc* $A = A' \cap K$*). Notons* $U_{A'}$ *les unités de* A' *et* $I_{A'}$ *son idéal maximal. Considérons sept familles finies* $(R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}}, R_{\mathrm{Nvr}}, R_{\mathrm{Nrn}})$ *dans l'anneau* $K[x_1, x_2, \cdots, x_m] = K[x]$. *Soit* $\mathcal{I}_{=0}$ *l'idéal de* $K[x]$ *engendré par* $R_{=0}$, $\mathcal{M}_{\neq 0}$ *le monoïde engendré par* $R_{\neq 0}$, $\mathcal{V}_{\mathrm{Vr}}$ *le sous-anneau de* $K[x]$ *engendré par* $R_{\mathrm{Vr}} \cup R_{\mathrm{Rn}} \cup R_{\mathrm{U}} \cup A$, $\mathcal{I}_{\mathrm{Rn}}$ *l'idéal de* $\mathcal{V}_{\mathrm{Vr}}$ *engendré par* $R_{\mathrm{Rn}} \cup I_A$, $\mathcal{M}_{\mathrm{U}}$ *le monoïde engendré par* $R_{\mathrm{U}} \cup U_A$.
Soit $\mathcal{S} \subset K'^m$ *l'ensemble des points* x *satisfaisant les conditions :* $n(x) = 0$ *pour* $n \in R_{=0}$, $t(x) \neq 0$ *pour* $t \in R_{\neq 0}$, $c(x) \in A'$ *pour* $c \in R_{\mathrm{Vr}}$, $v(x) \in U_{A'}$ *pour* $v \in R_{\mathrm{U}}$, $k(x) \in I_{A'}$ *pour* $k \in R_{\mathrm{Rn}}$, $p(x) \notin A'$ *pour* $p \in R_{\mathrm{Nvr}}$, $q(x) \notin I_{A'}$ *pour* $q \in R_{\mathrm{Nrn}}$.
L'ensemble $\mathcal{S}$ *est vide si et seulement si on a une identité algébrique*

$$s(up_1^{\mu_1}\cdots p_k^{\mu_k} q_1^{\nu_1}\cdots q_\ell^{\nu_\ell} + j(p,q) + a(p)) + i = 0$$

avec $i \in \mathcal{I}_{=0}$, $s \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j(p,q) = j(p_1,\ldots,p_k,q_1,\ldots,q_\ell)$ *est un polynome à coefficients dans* $\mathcal{I}_{\mathrm{Rn}}$ *dans lequel les multiexposants sont tous* $\leq (\mu_1,\ldots,\mu_k,\nu_1,\ldots,\nu_\ell)$ *(pour l'ordre produit) et* $a(p) = a(p_1,\ldots,p_k)$ *est un polynome à coefficients dans* $\mathcal{V}_{\mathrm{Vr}}$ *dans lequel les multiexposants sont tous* $< (\mu_1,\ldots,\mu_k)$.

3 Démonstration

La théorie des corps valués algébriquement clos admet une description axiomatique dont la structure est très simple. Avec les prédicats que nous avons envisagé on peut par exemple prendre pour axiomes

	$\vdash \mathrm{Vr}(-1)$	$D(1)$	$(x \neq 0,\ y \neq 0)$	$\vdash xy \neq 0$	$D(15)$
$(x = 0,\ \mathrm{Vr}(y))$	$\vdash \mathrm{Vr}(x+y)$	$D(2)$	$\mathrm{U}(x)$	$\vdash \mathrm{Vr}(x)$	$D(16)$
$(\mathrm{Vr}(x),\ \mathrm{Vr}(y))$	$\vdash \mathrm{Vr}(xy)$	$D(3)$	$\mathrm{Rn}(x)$	$\vdash \mathrm{Vr}(x)$	$D(17)$
$(\mathrm{Vr}(x),\ \mathrm{Vr}(y))$	$\vdash \mathrm{Vr}(x+y)$	$D(4)$	$(0 \neq 0)$	$\vdash \bot$	*Collapsus*
	$\vdash \mathrm{Rn}(0)$	$D(5)$	$xu = 1$	$\vdash x \neq 0$	$S(1)$
$(x = 0,\ \mathrm{Rn}(y))$	$\vdash \mathrm{Rn}(x+y)$	$D(6)$	$(\mathrm{Vr}(xy),\ \mathrm{U}(x))$	$\vdash \mathrm{Vr}(y)$	$S(2)$
$(\mathrm{Rn}(x),\ \mathrm{Vr}(y))$	$\vdash \mathrm{Rn}(xy)$	$D(7)$	$(xu = 1,\ \mathrm{Vr}(x))$	$\vdash \mathrm{Nrn}(u)$	$S(4)$
$(\mathrm{Rn}(x),\ \mathrm{Rn}(y))$	$\vdash \mathrm{Rn}(x+y)$	$D(8)$	$(xu = 1,\ \mathrm{Rn}(x))$	$\vdash \mathrm{Nvr}(u)$	$S(5)$
	$\vdash \mathrm{U}(1)$	$D(9)$	$x \neq 0$	$\vdash \exists u\ xu = 1$	$Dy(1)$
$(x = 0,\ \mathrm{U}(y))$	$\vdash \mathrm{U}(x+y)$	$D(10)$		$\vdash x = 0 \ \vee\ x \neq 0$	$Dy(2)$
$(\mathrm{U}(x),\ \mathrm{U}(y))$	$\vdash \mathrm{U}(xy)$	$D(11)$	$xy = 1$	$\vdash (\mathrm{Vr}(x) \ \vee\ \mathrm{Vr}(y))$	$Dy(3)$
$(\mathrm{Rn}(x),\ \mathrm{U}(y))$	$\vdash \mathrm{U}(x+y)$	$D(12)$	$\mathrm{Vr}(x)$	$\vdash (\mathrm{U}(x) \ \vee\ \mathrm{Rn}(x))$	$Dy(4)$
$\mathrm{U}(x)$	$\vdash x \neq 0$	$D(13)$	$\mathrm{Nrn}(x)$	$\vdash \exists u\ (xu = 1,\ \mathrm{Vr}(u))$	$Dy(5)$
$(x = 0,\ y \neq 0)$	$\vdash x + y \neq 0$	$D(14)$	$\mathrm{Nvr}(x)$	$\vdash \exists u\ (xu = 1,\ \mathrm{Rn}(u))$	$Dy(6)$

sans oublier les axiomes de cloture algébrique

$$\vdash \ \exists y \quad y^n + x_{n-1}y^{n-1} + \cdots + x_1 y + x_0 = 0 \qquad\qquad Dy_n(7)$$

Ceci nous permet de donner une définition précise du collapsus d'une présentation.

Définition 1 *Une présentation* $(G; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}}, R_{\mathrm{Nvr}}, R_{\mathrm{Nrn}})$ *de corps valué* collapse *dans la théorie des corps valués algébriquement clos si la présentation considérée prouve* $\perp$ *lorsqu'on utilise les axiomes ci-dessus.*

Dans [1], il est démontré que, pour toute structure algébrique ayant des axiomes *dynamiques* (i.e., du même style très simple que ceux ci-dessus) le collapsus, s'il a lieu, peut être obtenu au moyen d'une preuve très élémentaire (appelée évaluation dynamique). Ce résultat est à la base de la production systématique de théorèmes du style Nullstellensatz.

En particulier, il est démontré dans [1] le théorème suivant qui caractérise le collapsus au moyen d'une identité algébrique (mais sans les prédicats Nvr et Nrn), analogue à la proposition 1.2.

Théorème 3.1 *Soit* $(G; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}})$ *une présentation de corps valué. Soit* $\mathcal{I}_{=0}$ *l'idéal de* $\mathbb{Z}[G]$ *engendré par* $R_{=0}$*,* $\mathcal{M}_{\neq 0}$ *le monoïde (multiplicatif) de* $\mathbb{Z}[G]$ *engendré par* $R_{\neq 0}$*,* $\mathcal{V}_{\mathrm{Vr}}$ *le sous-anneau de* $\mathbb{Z}[G]$ *engendré par* $R_{\mathrm{Vr}} \cup R_{\mathrm{Rn}} \cup R_{\mathrm{U}}$*,* $\mathcal{I}_{\mathrm{Rn}}$ *l'idéal de* $\mathcal{V}_{\mathrm{Vr}}$ *engendré par* R_{Rn}*,* $\mathcal{M}_{\mathrm{U}}$ *le monoïde engendré par* R_{U}*.*
Cette présentation collapse comme corps valué si et seulement si elle collapse comme corps valué algébriquement clos si et seulement si on a une identité algébrique dans $\mathbb{Z}[G]$

$$s(u + j) + i = 0$$

avec $i \in \mathcal{I}_{=0}$*,* $s \in \mathcal{M}_{\neq 0}$*,* $u \in \mathcal{M}_{\mathrm{U}}$ *et* $j \in \mathcal{I}_{\mathrm{Rn}}$ *(ce qui est le collapsus de la structure répondant aux seuls axiomes :* $D(1) \to D(17)$ *et Collapsus).*

En rajoutant les deux prédicats Nvr et Nrn on en déduit facilement l'énoncé suivant.

Théorème 3.2 *Soit* $(G; R_{=0}, R_{\neq 0}, R_{\mathrm{Vr}}, R_{\mathrm{Rn}}, R_{\mathrm{U}}, R_{\mathrm{Nvr}}, R_{\mathrm{Nrn}})$ *une présentation de corps valué. Soit* $\mathcal{I}_{=0}$ *l'idéal de* $\mathbb{Z}[G]$ *engendré par* $R_{=0}$*,* $\mathcal{M}_{\neq 0}$ *le monoïde (multiplicatif) engendré par* $R_{\neq 0}$*,* $\mathcal{V}_{\mathrm{Vr}}$ *le sous-anneau de* $\mathbb{Z}[G]$ *engendré par* $R_{\mathrm{Vr}} \cup R_{\mathrm{Rn}} \cup R_{\mathrm{U}}$*,* $\mathcal{I}_{\mathrm{Rn}}$ *l'idéal de* $\mathcal{V}_{\mathrm{Vr}}$ *engendré par* R_{Rn}*,* $\mathcal{M}_{\mathrm{U}}$ *le monoïde engendré par* R_{U}*.*
Cette présentation collapse comme corps valué si et seulement si elle collapse comme corps valué algébriquement clos si et seulement si on a une identité algébrique dans $\mathbb{Z}[G]$

$$s(up_1^{\mu_1} \cdots p_k^{\mu_k} q_1^{\nu_1} \cdots q_\ell^{\nu_\ell} + j(p,q) + a(p)) + i = 0$$

avec $i \in \mathcal{I}_{=0}$*,* $s \in \mathcal{M}_{\neq 0}$*,* $u \in \mathcal{M}_{\mathrm{U}}$*,* $j(p,q) = j(p_1, \ldots, p_k, q_1, \ldots, q_\ell)$ *est un polynome à coefficients dans* $\mathcal{I}_{\mathrm{Rn}}$ *dans lequel les multiexposants sont tous* $\leq (\mu_1, \ldots, \mu_k, \nu_1, \ldots, \nu_\ell)$ *(pour l'ordre produit) et* $a(p) = a(p_1, \ldots, p_k)$ *est un polynome à coefficients dans* $\mathcal{V}_{\mathrm{Vr}}$ *dans lequel les multiexposants sont tous* $< (\mu_1, \ldots, \mu_k)$*.*

Preuve Nous supposons sans perte de généralité que les p_h et q_r sont non identiquement nuls, car le collapsus est alors évident.

Comme $\mathrm{Nvr}(x)$ signifie $\mathrm{Rn}(1/x)$ et $\mathrm{Nrn}(x)$ signifie $\mathrm{Vr}(1/x)$ on peut remplacer chaque élément p_h de R_{Nvr} par un générateur t_h, une équation $t_h p_h - 1 = 0$ et une relation $\mathrm{Rn}(t_h)$, et de même, on peut remplacer chaque élément q_r de R_{Nvr} par un générateur v_r, une équation $v_r q_r - 1 = 0$

et une relation $\mathrm{Vr}(v_r)$. On se retrouve avec une présentation où ne figurent plus R_{Nvr} ni R_{Nrn} et on peut appliquer le théorème 3.1 puisque la deuxième présentation collapse si et seulement si la première collapse. Le collapsus est donné par une identité algébrique

$$s(u + j_1(t,v) + t_1a_1(t,v) + \cdots + t_ka_k(t,v)) + i_1(t,v) = \\ (t_1p_1 - 1)b_1(t,v) + \cdots + (t_kp_k - 1)b_k(t,v) + (v_1q_1 - 1)c_1(t,v) + \cdots + (v_\ell q_\ell - 1)c_\ell(t,v)$$

avec $s \in \mathcal{M}_{\neq 0}$, $u \in \mathcal{M}_{\mathrm{U}}$, $j_1(t,v) \in \mathcal{I}_{\mathrm{Rn}}[t_1,\ldots,t_h,v_1,\ldots,v_\ell] = \mathcal{I}_{\mathrm{Rn}}[t,v]$, $i_1(t,v) \in \mathcal{I}_{=0}[t,v]$, les $a_j(t,v) \in \mathcal{V}_{\mathrm{Vr}}[t,v]$, les b_j et les c_j dans $\mathbb{Z}[G][t,v]$. On multiplie par $p_1^{\mu_1}\cdots p_k^{\mu_k}q_1^{\nu_1}\cdots q_\ell^{\nu_\ell}$ où les exposants sont suffisamment grands pour qu'on puisse chasser dans la deuxième ligne tous les t_h et v_h qui interviennent dans la première ligne de l'identité ($t_h^m p_h^{m+m'}$ est remplacé par $p_h^{m'}$ modulo $(t_hp_h - 1)$). On obtient l'identité voulue car la deuxième ligne est alors nécessairement nulle. □

Les théorèmes 2.1 et 2.2 se déduisent du théorème précédent de la même manière que dans [1]. Pour démontrer le théorème 2.2 on peut utiliser le théorème formel, mais alors la preuve n'est pas constructive. Si on suit la méthode donnée dans [1] on obtient par contre un moyen explicite de construire l'identité algébrique voulue. On part d'une preuve que $\mathcal{S}$ est vide, obtenue par un algorithme de décision, et on applique le théorème 3.2.

Références

[1] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze* Annals of Pure and Applied Logic (à paraître).

[2] Coquand T., Persson H. *Valuations and Dedekind's Prague Theorem* Journal of Pure and Applied Algebra **155** (2001) 121–129.

[3] Prestel A., Ripoli C.: Integral valued rational functions on valued fields. Manuscripta Math. 73, 437–452 (1991)