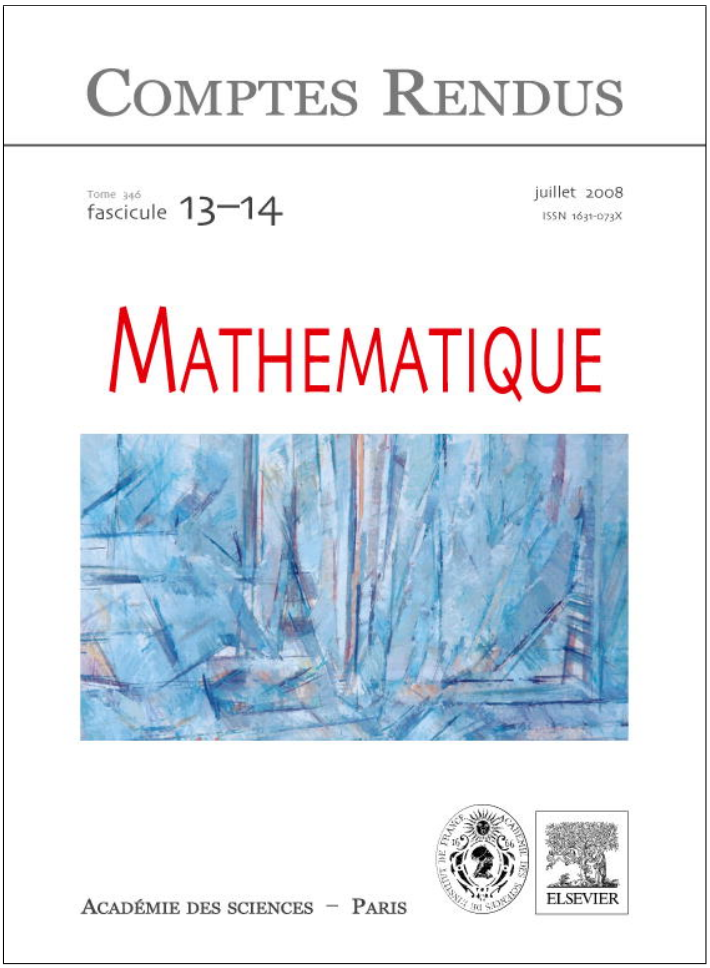

Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 346 (2008) 703–706
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Logique

Élimination des quantificateurs dans les équations aux différences linéaires sur les vecteurs de Witt

Luc Bélair [a], Françoise Point [b]

[a] *Département de mathématiques, Université du Québec – UQAM, C.P. 8888 succ. Centre-ville, Montréal, Québec, H3C 3P8, Canada*
[b] *F.N.R.S., Institut de mathématique, Université de Mons-Hainaut, Le Pentagone, 6, avenue du Champ de Mars, B-700 Mons, Belgique*

Reçu le 3 mai 2007 ; accepté après révision le 26 mai 2008

Disponible sur Internet le 20 juin 2008

Présenté par Jean-Yves Girard

Résumé

On donne un algorithme d'élimination des quantificateurs dans les vecteurs de Witt sur un corps algébriquement clos (ou encore dans les séries formelles), vus comme module valué sur l'anneau de Ore des polynômes de Frobenius. On obtient alors que ces structures n'ont pas la propriété d'indépendance. ***Pour citer cet article : L. Bélair, F. Point, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Abstract

Quantifier elimination in linear difference equations over Witt vectors. We prove quantifier elimination in Witt vectors over an algebraically closed fields (or in power series), considered as a valued module over the Ore ring of Frobenius polynomials. We get that these structures do not have the independence property. ***To cite this article: L. Bélair, F. Point, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

1. Introduction

Soit $W[E]$ l'anneau des vecteurs de Witt sur E, un corps parfait de caractéristique $p > 0$. Soit $\rho : E \to W[E]$ le système multiplicatif de représentants. Tout $x \in W[E]$ a une représentation unique $x = \sum_{i=0}^{\infty} \rho(\alpha_i) p^i$, et on a l'automorphisme $\sigma_p : W[E] \to W[E]$ défini par $\sigma_p(\sum_{i=0}^{\infty} \rho(\alpha_i) p^i) = \sum_{i=0}^{\infty} \rho(\alpha_i)^p p^i$ (voir [7]). Soit $W(E)$ le corps des fractions de $W[E]$ et v_p sa valuation p-adique. On note aussi σ_p le prolongement à $W(E)$. Il y a une élimination des quantificateurs dans la structure $(W(E), +, \cdot, v_p, \sigma_p)$ comme dans les corps valués (voir [1,6]). Dans cette Note, on considère $W(E)$ dans un formalisme plus faible, où n'apparaissent que les équations aux différences linéaires, comme $c_n \sigma_p^n(X) + \cdots + c_1 \sigma_p(X) + c_0 X = b$. On fait alors de $W(E)$ un module sur un anneau approprié. Le cas qui nous intéresse est $E = \tilde{\mathbb{F}}_p$, la clôture algébrique du corps premier. Le résultat principal de cette Note est un algorithme

Adresses e-mail : belair.luc@uqam.ca (L. Bélair), point@logique.jussieu.fr (F. Point).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.05.011

d'élimination des quantificateurs (Théorème 3.3) dans un langage à deux sortes de module valué analogue à [8].[1] On remarque qu'on a les mêmes résultats en remplaçant $W(E)$ par le corps de séries formelles $E((X))$ en la variable X avec sa valuation X-adique et l'automorphisme $\varphi_p(\sum a_i X^i) = \sum a_i^p X^i$. On peut alors déduire l'équivalence élémentaire dans ce formalisme d'un ultraproduit non-principal des $(W(\tilde{\mathbb{F}}_p), \sigma_p)$ avec l'ultraproduit des $(\tilde{\mathbb{F}}_p((X)), \varphi_p)$ (déjà conséquence de [1,6]).

Dans cette Note, tous les modules sont des modules à droite. Pour la théorie des modèles des modules, on renvoie à [4]. On note $\mathbf{x}$ le n-uplet $(x_1, \ldots, x_n)$, et nous abuserons parfois de cette notation. Pour un corps valué (K, v), $\mathcal{O}_K$ désigne son anneau de valuation et vK son groupe de valuation. On appelle *isométrie* un automorphisme σ d'un corps valué (K, v) tel que $v(\sigma(x)) = v(x)$ (voir [3]). On notera (K, v, σ) un corps valué muni d'une isométrie. Pour un tel (K, v, σ), soit $A = K[t; \sigma]$ l'anneau de polynômes non commutatifs déterminé par la règle $kt = t\sigma(k), k \in K$ (voir [2], chap. 2), introduit par O. Ore. Si σ n'est pas l' identité, alors l'anneau A n'est pas commutatif, il n'a pas de diviseur de zéro et est euclidien à droite et à gauche. Il y a sur A une valuation qui prolonge la valuation de K, que nous noterons aussi v, et qui est définie par $v(\sum_{i=0}^n t^i k_i) = \min_i\{v(k_i)\}$ (voir [2], chap. 9). On pose $A_0 = \mathcal{O}_K[t; \sigma]$, c'est un sous-anneau de A. Le corps K a une structure naturelle de A-module par l'action $k.(\sum_{i=0}^n t^i k_i) = \sum_{i=0}^n \sigma^i(k) k_i$.

2. Le module sur l'anneau de Ore des polynômes de Frobenius

Pour le reste de la Note, on fixe (K, v, σ) un corps valué muni d'une isométrie et $A = K[t; \sigma]$.

Définition 2.1. Soit L_A le langage du premier ordre des A-modules, et T_A les axiomes de A-modules. Soit T_{Ore} la théorie de A-modules obtenue de T_A en ajoutant les axiomes suivants :

(1) $\forall m \exists n (m = n.t) \& \forall m (m.t = 0 \to m = 0)$;
(2) $\forall m \exists n (n.q(t) = m)$, où $q(t) \in A$ est irréductible et $q(0) \neq 0$;
(3) $\exists n (n \neq 0 \& n.q(t) = 0)$, où $q(t) \in A$ est irréductible et $q(0) \neq 0$.

Notons que cette axiomatisation équivaut à celle où l'on requiert la divisibilité pour les polynômes non divisibles par t. Un corps de caractéristique $p > 0$ est dit p-clos s'il ne possède aucune d'extension finie de degré divisible par p. Le corps $\tilde{\mathbb{F}}_p$ est p-clos. Le lemme suivant découle d'un procédé d'approximation du genre Newton–Raphson (cf. [6,1]). Le théorème s'ensuit de façon standard (cf. [4]).

Lemme 2.2. *Soit E un corps p-clos, $K = W(E)$ et $\sigma = \sigma_p$. Alors $W[E]$ est un A_0-module divisible, et $W(E)$ est un A-module divisible.*

Théorème 2.3. *Soit E un corps algébriquement clos, $K = W(E)$ et $\sigma = \sigma_p$. Alors $W(E)$ est un modèle de la théorie T_{Ore} et cette théorie est complète et admet l'élimination des quantificateurs.*

3. Le module valué

Définition 3.1. (Cf. [8].) Un A-module valué est une structure $(M, \Delta, \leqslant, +, w, \infty)$ où M est un A-module, $\infty \in \Delta$, $(\Delta, \leqslant)$ est un ensemble totalement ordonné dont ∞ est le maximum, $+$ est une action de vK sur $(\Delta, \leqslant)$ et w est une fonction surjective $w : M \to \Delta$ tels que : (1) $\forall \delta_1, \delta_2 \in \Delta, \forall \gamma_1, \gamma_2 \in vK$, $\delta_1 \leqslant \delta_2$ et $\gamma_1 \leqslant \gamma_2$ entraîne $\delta_1 + \gamma_1 \leqslant \delta_2 + \gamma_2$; (2) $w(m) = \infty$ ssi $m = 0$ et $\forall m_1, m_2 \in M, w(m_1 + m_2) \geqslant \min\{w(m_1), w(m_2)\}$; (3) $\forall m \in M, w(m.t) = w(m)$; (4) $\forall m \in M, \forall \lambda \in K, \lambda \neq 0, w(m.\lambda) = w(m) + v(\lambda)$.

Définition 3.2.

(1) Le langage L_w est le langage à deux sortes des A-modules valués obtenu de L_A, avec une sorte M pour l'ensemble sous-jacent du module, une sorte Δ pour l'ensemble ordonné des valuations, une constante ∞ de sorte Δ et des

[1] Citons [5] pour l'automorphisme de Frobenius $x \mapsto x^p$ en caractéristique p dans ce contexte de modules valués.

opérations unaires de sorte Δ pour chacun des $\gamma \in vK$. Dans L_w, m, n, x, y, z désigneront les variables de sorte M, et α, δ désigneront les variables de sorte Δ.

(2) Soit $T_{Ore,w}$ la L_w-théorie de A-modules valués obtenue de T_{Ore} en ajoutant les axiomes suivants : soient $a_0, \ldots, a_n \in A_0$ tels que a_0 est de terme constant non nul, $v(a_0) = \cdots = v(a_n) = 0$, alors pour tout δ et pour tous $m_0, \ldots, m_n$: (DG) il existe x tel que $x.a_0 = m_0$ et $w(x) = w(m_0)$; (IR) il existe $x \neq 0$ tel que si $w(m_i) \geqslant \delta, i = 1, \ldots, n$, alors $w(x) = w(x.a_i + m_i) = \delta, i = 1, \ldots, n$.

Le même procédé Newton–Raphson que pour T_{Ore}, assure que si E est algébriquement clos, $K = W(E)$ et $\sigma = \sigma_p$, alors $W(E)$ est un modèle de $T_{Ore,w}$. Pour $\nu \in \mathbb{N}$ et $a \in A_0$ on note $\mathrm{Ind}_{\nu,a}(\delta)$ la formule $\exists x_1, \ldots, x_\nu (\bigwedge_{i=1}^{\nu} (w(x_i.a) > \delta \,\&\, w(x_i) = \delta \,\&\, \bigwedge_{i \neq j} w(x_i - x_j) = \delta))$.

Théorème 3.3. *Pour toute formule $\varphi(x, \mathbf{y}, \boldsymbol{\alpha})$ du langage L_w qui soit sans quantificateur dans la sorte M, la formule $\exists x \varphi(x, \mathbf{y}, \boldsymbol{\alpha})$ est équivalente dans $T_{Ore,w}$ à une formule $\Phi(\mathbf{y}, \boldsymbol{\alpha})$ qui est sans quantificateur dans la sorte M, sauf peut-être pour des sous-formules de la forme* $\mathrm{Ind}_{\nu,a}(\alpha_i)$.

Preuve. On peut supposer que φ est une conjonction de formules atomiques et de négations de formules atomiques. En remplaçant chaque inéquation $x.r \neq u$ par $w(x.r - u) \neq \infty$, on peut toujours supposer qu'il n'y a pas de telles inéquations. On remplace ensuite chaque inéquation où apparaît un terme de la forme $w(x.r + u)$, où $r \in A$ et u est un terme où x n'apparaît pas, par une formule $\exists \delta (w(x.r + u) = \delta \,\&\, \psi)$, où ψ est obtenu de l'inéquation en remplaçant $w(x.r + u)$ par δ. De proche en proche, cela permet de supposer que les termes de la forme $w(x.r + u)$ n'apparaissent que dans des équations $w(x.r + u) = \delta$ (cf. [9], §.2). (Par inéquation, nous entendons une formule de base de la forme $t_1 \neq t_2$, ou $t_1 \leqslant t_2$ ou $t_1 < t_2$, où t_1 et t_2 sont des termes ; la négation d'une inéquation est une inéquation ou une équation). Comme A est euclidien, il suffit de considérer des formules où il n'y a qu'une seule équation du type $x.r = u$. Grâce à ces manipulations, on se ramène à une formule de la forme : $\bigwedge_{i=1}^{n} w(x.r_i + u_i(\mathbf{y})) = \delta_i \,\&\, x.r_0 = u_0(\mathbf{y}) \,\&\, \theta(\mathbf{y}, \boldsymbol{\delta})$, où $r_i \in A$, $\theta(\mathbf{y}, \boldsymbol{\delta})$ est une formule sans quantificateur dans la sorte M où x n'apparaît pas, les u_i sont des termes du langage L_A, $\delta_i \in \Delta, \infty \neq \delta_1 \geqslant \delta_2 \geqslant \cdots \geqslant \delta_n$. Il suffit de montrer que toute formule $\exists x (\bigwedge_{i=1}^{n} w(x.r_i + u_i(\mathbf{y})) = \delta_i \,\&\, x.r_0 = u_0(\mathbf{y}))$ est équivalente à une formule sans quantificateur dans la sorte M, modulo les formules $\mathrm{Ind}_{\nu,a}(\delta)$.

Notons qu'il existe pour les $r_i \neq 0$ des $\lambda_i \in K$ tels que $r_i \lambda_i \in A_0$ et $v(r_i \lambda_i) = 0$. On peut donc toujours supposer que $r_i \in A_0$ et $v(r_i) = 0$. Notons aussi qu'on peut toujours se ramener au cas où $\deg(r_0) > \deg(r_i), i = 1, \ldots, n$. On effet, si $\deg(r_0) \leqslant \deg(r_i)$, disons $i = 1$, alors par la division euclidienne à droite généralisée on a $\lambda \in \mathcal{O}_K$ et $r, r_1' \in A_0$ tels que $r_1 \lambda = r_0 r + r_1'$, $\deg(r_1') < \deg(r_0)$. On remplace alors $w(x.r_1 + u_1) = \delta_1$ par $w(x.r_1' + u_1.\lambda + u_0.r) = \delta_1 + v(\lambda)$.

Considérons le cas crucial suivant, où l'on a un système

$$(1) : x.r_0 = u_0, w(x.r_1 + u_1) = \delta_1, \ldots, w(x.r_n + u_n) = \delta_n$$

où $\deg(r_0) > \deg(r_i), r_i \in A_0, v(r_i) = 0, i = 1, \ldots, n$. Par la division euclidienne à droite généralisée, il existe $\lambda \in \mathcal{O}_K$ et $s, s_1 \in A_0$ tel que $r_0 \lambda = r_1 s + s_1$ et $\deg(s_1) < \deg(r_1)$. Soit ℓ tel que $\delta_1 = \delta_2 = \cdots = \delta_\ell > \delta_{\ell+1} \geqslant \cdots \geqslant \delta_n, 1 \leqslant \ell \leqslant n$.

Je dis que le système (1) est équivalent aux systèmes (2a) ou (2b) :

$$(2a) : x.r_0 = u_0, w(x.s_1 - u_0.\lambda - u_1.s) = \delta_1, \quad w(x.r_1 + u_1) \geqslant \delta_1, \quad \bigwedge_{i=2}^{\ell} w(x.r_i + u_i) = \delta_1, \quad \bigwedge_{i=\ell+1}^{n} w(x.r_i + u_i) = \delta_i.$$

$$(2b) : x.r_0 = u_0, w(x.s_1 - u_0.\lambda - u_1.s) > \delta_1, \quad \bigwedge_{i=1}^{\ell} w(x.r_i + u_i) = \delta_1, \quad \bigwedge_{i=\ell+1}^{n} w(x.r_i + u_i) = \delta_i.$$

Ainsi, la présence d'une équation dans la formule sans quantificateur nous permet d'abaisser le degré du coefficient de la variable x dans les expressions $w(x.s - u) \,\square\, \delta$, où $\square$ désigne $>, \geqslant$ ou $=$. Supposons x une solution de (1). On a $w(x.r_1 + u_1) = \delta_1$, de sorte que $w(x.r_1.s + u_1.s) \geqslant \delta_1$. Si $w(x.r_1.s + u_1.s) = \delta_1$, on obtient $x.r_1.s = u_0.\lambda - x.s_1$ et

$w(x.s_1 - u_0.\lambda - u_1.s) = \delta_1$, et x est solution de (2a). De même, si $w(x.r_1.s + u_1.s) > \delta_1$ on obtient $w(x.s_1 - u_0.\lambda - u_1.s) > \delta_1$, et x est solution de (2b).

Réciproquement, soit x une solution de (2a). On a $w(x.r_1.s + u_1.s) \geqslant w(x.r_1 + u_1)$ et $w(x.r_1.s + u_1.s) = w(x.s_1 - u_0.\lambda - u_1.s) = \delta_1$, de sorte qu'on ne peut avoir $w(x.r_1 + u_1) > \delta_1$, d'où $w(x.r_1 + u_1) = \delta_1$ et x est solution de (1). Notons qu'une solution de (2b) est immédiatement une solution de (1).

Cette réduction illustre les manipulations de base de l'algorithme. En itérant ce procédé, deux cas de figure se produisent : dans une division euclidienne donnée le reste est non nul et de degré plus petit que celui du diviseur, ou alors le reste est nul et on a un multiple du diviseur. Le premier cas de figure mène, de proche en proche, à un système où on conserve une équation $x.r_0 = u_0$ mais où on a réduit la complexité des relations valuationnelles au maximum en n'ayant que des relations de la forme $w(x - u') = \delta_1$ ou encore une relation $w(x - u') > \delta_1$. C'est alors que les formules $\mathrm{Ind}_{v,a}(\delta_1)$ et l'axiome (DG) interviennent et permettent l'élimination. Notons qu'en présence de $w(x - u') > \delta_1$, l'axiome (DG) suffit. Le deuxième cas de figure mène à considérer la situation où tous les r_i divisent r_0. On peut alors se ramener à des cas déjà traités.

Dans le cas où $r_0 = 0$ (on n'a pas d'équation), à savoir $(1')$: $\bigwedge_{i=1}^{n} w(x.r_i + u_i) = \delta_i$. Soit de nouveau ℓ tel que $\delta_1 = \cdots = \delta_\ell > \delta_{\ell+1} \geqslant \cdots$. Je dis que $(1')$ est équivalent au système $(1'')$: $x.r_1 = -u_1$, $\bigwedge_{i=2}^{\ell} w(x.r_i + u_i) \geqslant \delta_1 \& \bigwedge_{i=\ell+1}^{n} w(x.r_i + u_i) = \delta_i$. En effet, supposons x une solution de $(1')$. Par l'axiome (DG), soit y tel que $y.r_1 = -x.r_1 - u_1$, $w(y) = \delta_1$, alors $x + y$ est une solution de $(1'')$. Réciproquement, soit x une solution de $(1'')$. Par l'axiome (IR), soit y tel que $w(y) = \delta_1$, $w(y.r_1) = \delta_1$, $w(y.r_i + x.r_i + u_i) = \delta_1$, $i = 2, \ldots, \ell$. Alors $x + y$ est une solution de $(1')$. On est maintenant ramené au cas déjà traité. □

Théorème 3.4. *Si $M = K = W(\tilde{\mathbb{F}}_p)$, $w = v = v_p$, $\sigma = \sigma_p$, alors $W(\tilde{\mathbb{F}}_p)$ admet l'élimination des quantificateurs dans L_w, et ne possède pas la propriété d'indépendance.*

Preuve. Pour la propriété d'indépendance, on raisonne directement sur les formules sans quantificateur. Un argument combinatoire permet de se ramener au cas d'une formule atomique, et on utilise que ni la théorie des chaînes ni celle des modules n'ont la propriété d'indépendance. □

Soit L_V le langage obtenu de L_A en fixant l'ensemble Δ et en ajoutant pour chaque $\delta \in \Delta$ un prédicat unaire V_δ, avec $V_\delta = \{m \in M\colon\ w(m) \geqslant \delta\}$ (cf. [5]). On a un résultat d'élimination analogue dans L_V.

Remerciements

Nous remercions le rapporteur pour sa lecture attentive.

Références

[1] L. Bélair, A. Macintyre, T. Scanlon, Model theory of the Frobenius on the Witt vectors, Amer. J. Math. 129 (2007) 665–721.
[2] P.M. Cohn, Skew Fields, Cambridge Univ. Press, 1995.
[3] A. Duval, Lemmes de Hensel et factorisation formelle pour les opérateurs aux différences, Funkcialaj Ekvacioj 26 (1983) 349–368.
[4] M. Prest, Model Theory and Modules, Cambridge Univ. Press, 1988.
[5] T. Rohwer, Valued difference fields as modules over twisted polynomial rings, thèse de PhD, University of Illinois at Urbana-Champaign, 2003.
[6] T. Scanlon, Quantifier elimination for the relative Frobenius, in : F.-V. Kuhlmann, et al. (Eds.), Valuation Theory and Its Applications, vol. II, Amer. Math. Soc., 2003, pp. 323–352.
[7] J.-P. Serre, Corps locaux, Hermann, 1968.
[8] L. van den Dries, Quantifier elimination for linear formulas over ordered and valued fields, Bull. Soc. Math. Belgique, Série B 33 (1981) 19–31.
[9] V. Weispfenning, Quantifier elimination and decision procedures for valued fields, in: Models and Sets, Aachen, 1983, in: Lecture Notes in Math., vol. 1103, Springer, 1984, pp. 419–472.