MONOMIALIZATION OF MORPHISMS AND P-ADIC QUANTIFIER ELIMINATION

JAN DENEFF

(Communicated by Lev Borisov)

Dedicated to the memory of Professor Patrick Sargos

ABSTRACT. We give a short proof of Macintyre’s Theorem on Quantifier Elimination for p -adic numbers, using a version of monomialization that follows directly from the Weak Toroidalization Theorem of Abramovich and Karu (extended to non-closed fields).

1. WEAK MONOMIALIZATION OF MORPHISMS

Definition 1.1. Let $f : X \rightarrow Y$ be a dominant morphism of non-singular schemes of finite type over a field K of characteristic zero, and let D be a closed subset of X . The morphism f is called *monomial with respect to D at a K -rational point a of X* if there exist an étale morphism $U \rightarrow X$, a K -rational point a' on U mapping to a , uniformizing parameters $x_1, \dots, x_n$ on U , uniformizing parameters $y_1, \dots, y_m$ on a Zariski open neighborhood of $f(a)$ in Y , and a matrix $(a_{i,j})_{i,j}$ of non-negative integers (which necessarily has rank m) such that

$$\begin{aligned} y_1 &= x_1^{a_{11}} \cdots x_n^{a_{1n}}, \\ &\vdots \\ y_m &= x_1^{a_{m1}} \cdots x_n^{a_{mn}}, \end{aligned} \tag{*}$$

and such that the preimage of D in U is contained in the locus of $\prod_i x_i$.

The morphism f is called *monomial with respect to D* if, for each field extension L of K , the morphism $f \otimes_K L : X \otimes_K L \rightarrow Y \otimes_K L$ is monomial with respect to the preimage of D at each L -rational point of $X \otimes_K L$. The morphism f is called *monomial* if it is monomial with respect to the empty set.

With *uniformizing parameters on a scheme Z over K* , we mean a sequence of regular functions on Z that induces an étale morphism from Z to an affine space over K . When A is a local ring containing its residue field, we will call elements $a_1, \dots, a_r \in A$ *uniformizing parameters for A* if these elements minus their residues are regular parameters for A .

Remark 1.2. The definition of a monomial morphism as stated above is slightly different from Definition 1.2 in Cutkosky’s paper [5], but is what we need for the present paper.

Received by the editors September 1, 2011.

2010 *Mathematics Subject Classification.* Primary 11S05, 11G25, 14G20; Secondary 03C10.

The author thanks Dan Abramovich, Steven Dale Cutkosky, and Kalle Karu for stimulating conversations and information.

Next we state a version of monomialization that follows directly from the Weak Toroidalization Theorem in [2], which is an extension to non-closed fields of the Weak Toroidalization Theorem of Abramovich and Karu [1]. Instead of [2] one could use the more recent stronger version of weak toroidalization in Illusie and Temkin [11, Theorem 3.9].

Theorem 1.3 (Weak monomialization). *Let $f : X \rightarrow Y$ be a dominant morphism of integral separated schemes of finite type over a field K of characteristic zero. Let S be a proper closed subset of X . Then there exist non-singular integral separated schemes X_1 and Y_1 of finite type over K , birational proper morphisms $\alpha : X_1 \rightarrow X$, $\beta : Y_1 \rightarrow Y$, and a morphism $g : X_1 \rightarrow Y_1$ which is monomial with respect to $\alpha^{-1}(S)$ such that the following diagram commutes:*

$$\begin{array}{ccc} X_1 & \xrightarrow{\alpha} & X \\ \downarrow g & & \downarrow f \\ Y_1 & \xrightarrow{\beta} & Y \end{array}$$

and such that $\alpha^{-1}(S)$ is a strict normal crossings divisor on X_1 .

This version of monomialization is also related to (but not implied by) Cutkosky's Theorem on Local Monomialization of Morphisms (Theorem 1.3 in [5]).

It is conjectured that we can take α and β to be compositions of blow-ups of non-singular subvarieties. This conjecture is a weakening of the Conjecture on (Strong) Toroidalization of Morphisms [1, 6].

Remark 1.4. To see that the Weak Toroidalization Theorem [2] implies Theorem 1.3, note that a dominant morphism $f : X \rightarrow Y$ of non-singular varieties over K , which is toroidal with respect to strict toroidal embeddings $U_X \subset X$, $U_Y \subset Y$ (as defined in [2]), is also monomial with respect to $D_X = X \setminus U_X$. Indeed this follows from Proposition 3.1 in section 3 and the remark below it.

2. QUANTIFIER ELIMINATION FOR $\mathbb{Q}_p$

Let p be a prime number. We denote the field of p -adic numbers by $\mathbb{Q}_p$.

Let X be a scheme of finite type over $\mathbb{Q}_p$. A subset A of $X(\mathbb{Q}_p)$ is called *semi-algebraic* if X can be covered by affine open subschemes Y such that $A \cap Y(\mathbb{Q}_p)$ is a finite boolean combination of subsets of $Y(\mathbb{Q}_p)$ determined by conditions of the form $f(y) = 0$ or of the form $\exists z \in \mathbb{Q}_p : f(y) = z^m$, with f any regular function on Y and m any positive integer.

It is well known that any subset of $\mathbb{Q}_p^n$ of the form $C = \{y \in \mathbb{Q}_p^n \mid \text{ord}_p f(y) \leq \text{ord}_p g(y)\}$, with f, g polynomials over $\mathbb{Q}_p$, is semi-algebraic. Indeed, for $p \neq 2$, $y \in C$ if and only if $(f(y))^2 + p(g(y))^2$ is a square in $\mathbb{Q}_p$, and for $p = 2$, $y \in C$ if and only if $(f(y))^2 + 8(g(y))^2$ is a square in $\mathbb{Q}_p$.

If U is an open subscheme of X , then any semi-algebraic subset B of $U(\mathbb{Q}_p)$ is a semi-algebraic subset of $X(\mathbb{Q}_p)$. Moreover, if X is affine, then B is expressible with regular functions on X , meaning that B is expressible by a finite boolean combination of conditions of the form $f(y) = 0$ or $\exists z \in \mathbb{Q}_p : f(y) = z^m$, with f any regular function on X . To verify this, note that this is evident when X is affine, U is the complement of the locus of a regular function on X , and B is expressible with regular functions U .

For any semi-algebraic subset A of $X(\mathbb{Q}_p)$, there exist an affine reduced scheme Z of finite type over $\mathbb{Q}_p$ and a morphism $h : Z \rightarrow X$ such that $A = h(Z(\mathbb{Q}_p))$.

Indeed, this follows easily from the observation that the complement of a coset of the subgroup of m -th powers in $\mathbb{Q}_p^\times$ is a finite union of such cosets.

We are now ready to state Macintyre's Theorem [12] on Quantifier Elimination for $\mathbb{Q}_p$, slightly reformulated.

Theorem 2.1 (Macintyre [12]). *Let $f : X \rightarrow Y$ be a morphism of schemes of finite type over $\mathbb{Q}_p$. Let A be a semi-algebraic subset of $X(\mathbb{Q}_p)$. Then $f(A)$ is a semi-algebraic subset of $Y(\mathbb{Q}_p)$.*

Macintyre's proof is based on methods from mathematical logic and the work of Ax and Kochen [3] and of Eršov [10]. An elementary but rather convoluted proof has been given in [8], based on p -adic cell decomposition which goes back to P. Cohen [4]. For some applications to number theory we refer to [7]. We will now derive Macintyre's Theorem from Theorem 1.3 (weak monomialization) in a straightforward way.

Proof of Theorem 2.1. Clearly it suffices to prove the theorem when X, Y are affine and integral and when $A = X(\mathbb{Q}_p)$. Let $\tilde{X}, \tilde{Y}$ be projective closures of X, Y . Replacing Y by $\tilde{Y}$, X by the closure of the graph of f in $\tilde{X} \times \tilde{Y}$, and f by the projection morphism to $\tilde{Y}$, we see that it suffices to prove the theorem when X, Y are proper and integral and when $A = X(\mathbb{Q}_p) \setminus S(\mathbb{Q}_p)$, where S is a proper closed subset of X . Moreover we may assume that f is dominant. Using Theorem 1.3, Lemma 2.2 below, and induction on $\dim X$, we see that it is sufficient to prove the theorem when X and Y are proper, integral, and non-singular, f is dominant and *monomial* with respect to a closed subset D of X of pure codimension 1, and $A = X(\mathbb{Q}_p) \setminus D(\mathbb{Q}_p)$. Then $X(\mathbb{Q}_p)$ is compact, and working locally, we reduce easily to the case that $X = \mathbb{A}^n, Y = \mathbb{A}^m$, f is dominant and given by monomials in the standard coordinates, and A is a p -adic ball minus the coordinate hyperplanes. Indeed, each point $a \in X(\mathbb{Q}_p)$ has arbitrary small p -adic neighborhoods that are balls in the local coordinates making f monomial at a , and, using induction on $\dim X$, we can cut out the coordinate hyperplanes. The theorem now follows from Lemma 2.4 below. $\square$

Lemma 2.2. *Consider the following commutative diagram of morphisms of integral schemes of finite type over $\mathbb{Q}_p$:*

$$\begin{array}{ccc} X_1 & \xrightarrow{\alpha} & X \\ \downarrow g & & \downarrow f \\ Y_1 & \xrightarrow{\beta} & Y \end{array}$$

with f dominant and with α and β birational. Let $X_0 \subsetneq X, Y_0 \subsetneq Y$ be reduced closed subschemes with $f^{-1}(Y_0) \subset X_0$ such that α and β are isomorphisms above $X \setminus X_0, Y \setminus Y_0$. Let A be a subset of $X(\mathbb{Q}_p)$. If $f(X_0(\mathbb{Q}_p) \cap A)$ and $g(X_1(\mathbb{Q}_p) \cap \alpha^{-1}(A))$ are semi-algebraic, then $f(A)$ is semi-algebraic.

Proof.

$$f(A) = \beta(g(X_1(\mathbb{Q}_p) \cap \alpha^{-1}(A))) \cup f(X_0(\mathbb{Q}_p) \cap A),$$

because α is an isomorphism above $X \setminus X_0$. Thus

$$f(A) = [\beta(g(X_1(\mathbb{Q}_p) \cap \alpha^{-1}(A))) \setminus Y_0(\mathbb{Q}_p)] \cup f(X_0(\mathbb{Q}_p) \cap A),$$

because $f^{-1}(Y_0) \subset X_0$. The lemma now follows from the fact that for any semi-algebraic subset B of $Y_1(\mathbb{Q}_p)$ we have that $\beta(B) \setminus Y_0(\mathbb{Q}_p)$ is semi-algebraic, because

$\beta^{-1}(y)$ is given by rational functions in the coordinates of $y \in Y(\mathbb{Q}_p) \setminus Y_0(\mathbb{Q}_p)$, with no poles on $Y \setminus Y_0$. $\square$

Lemma 2.3. *Let K be a Henselian valued field. Fix elements $y_1, \dots, y_m$ in $K^\times$, and consider the system of equations*

$$(*) \quad \begin{aligned} y_1 &= x_1^{a_{11}} \cdots x_n^{a_{1n}}, \\ &\vdots \\ y_m &= x_1^{a_{m1}} \cdots x_n^{a_{mn}}, \end{aligned}$$

in the unknowns $x_1, \dots, x_n$, with $m \leq n$, and $A := (a_{i,j})_{i,j}$ a matrix of non-negative integers with rank equal to m . Let d be the absolute value of the determinant of some (m, m) -minor of A with rank m . Let I be any proper ideal of the valuation ring of K . Then any solution of $(*)$ in the group $K^\times / 1 + dI$ which can be lifted to a solution in $K^\times / 1 + d^2I$ can be lifted to a solution of $(*)$ in the group $K^\times$.

Proof. Let $x_1, \dots, x_n \in K^\times$ be a solution of $(*)$ in $K^\times / 1 + d^2I$. Thus there exist $u_1, \dots, u_m \in 1 + d^2I$ such that the right side of $(*)$ equals $y_1 u_1^{-1}, \dots, y_m u_m^{-1}$. We have to find $\varepsilon_1, \dots, \varepsilon_n \in 1 + dI$ such that $x_1 \varepsilon_1, \dots, x_n \varepsilon_n$ is an exact solution of $(*)$. This is equivalent to the system of equations

$$(**) \quad \begin{aligned} u_1 &= \varepsilon_1^{a_{11}} \cdots \varepsilon_n^{a_{1n}}, \\ &\vdots \\ u_m &= \varepsilon_1^{a_{m1}} \cdots \varepsilon_n^{a_{mn}}. \end{aligned}$$

We may assume that $d = \det A_0$, where A_0 is the minor of A consisting of the first m columns of A . We choose $\varepsilon_{m+1} = \cdots = \varepsilon_n = 1$. Let u be the column vector with components $u_1, \dots, u_m$, and let ε be the column vector with components $\varepsilon_1, \dots, \varepsilon_m$. We have to find $\varepsilon \in (1 + dI)^m$ such that $u = \varepsilon^{A_0}$. A necessary condition is that $u^{B_0} = \varepsilon^{B_0 A_0}$, where $B_0 = dA_0^{-1}$ has integral coefficients; hence $u^{B_0} = \varepsilon^d$. Since $u \in (1 + d^2I)^m$, we can indeed choose $\varepsilon \in (1 + dI)^m$ such that $u^{B_0} = \varepsilon^d$. This implies $u^d = \varepsilon^{dA_0}$; hence $u = \varepsilon^{A_0}$, because the components of both sides belong to $1 + dI$ and have equal d -th powers. This concludes the proof of the lemma. $\square$

Lemma 2.4. *Let $f : \mathbb{Q}_p^n \rightarrow \mathbb{Q}_p^m : (x_1, \dots, x_n) \mapsto (y_1, \dots, y_m)$ be given by the formula $(*)$ in Lemma 2.3, with $(a_{i,j})_{i,j}$ a matrix of non-negative integers having rank m . Let $A \subset \mathbb{Q}_p^n$ be a p -adic ball minus the coordinate hyperplanes. Then $f(A)$ is semi-algebraic.*

Proof. By covering and scaling, we may suppose that $A = (\mathbb{Z}_p \setminus \{0\})^k \times (1 + I)^{n-k}$, with I a proper ideal in $\mathbb{Z}_p$. By Lemma 2.3, an element $y \in \mathbb{Q}_p^m$ belongs to $f(A)$ if and only if $(*)$ is solvable in $\mathbb{Q}_p^\times / 1 + d^2I$ with side requirements $x_1, \dots, x_k \in \mathbb{Z}_p$, and $x_{k+1}, \dots, x_n \in 1 + I$. Clearly, this solvability condition on y depends only on $\text{ord}_p y_1, \dots, \text{ord}_p y_m$ and on the angular components modulo d^2I of $y_1, \dots, y_m$. The angular component of a p -adic number z is defined as $zp^{-\text{ord}_p z}$. Moreover, the condition on $\text{ord}_p y_i$ is independent of the condition on the angular components. Since there are a priori only a finite number of possibilities for the angular component modulo d^2I , the condition on the angular components modulo d^2I of $y_1, \dots, y_m$ is semi-algebraic. Indeed, it is easy to verify that the subset of $\mathbb{Q}_p$ consisting of all p -adic numbers with a fixed angular component modulo d^2I is semi-algebraic

(see e.g. [8]). Finally, by Presburger elimination for linear equations over $\mathbb{N}$, the condition on $\text{ord}_p y_1, \dots, \text{ord}_p y_m$ is equivalent to a boolean combination of linear equations, linear inequalities, and linear congruences modulo fixed moduli. Again it is easy to verify that these are semi-algebraic; see e.g. [8]. This concludes the proof of the lemma. $\square$

Remark 2.5. In the same way one can easily prove Tarski's elimination of quantifiers for the field of real numbers. The above proof uses the local compactness of $\mathbb{Q}_p$ in an essential way. By a different argument we also obtained alternative proofs [9] of the Ax-Kochen-Eršov transfer principle and all classical results in the model theory of henselian valued fields of characteristic zero (except those on subanalytic sets). These alternative proofs are based on the Weak Toroidalization Theorem [2] and are purely algebraic geometric. To treat the theory of real and p -adic subanalytic sets in the same way, we would need a version of weak monomialization for analytic morphisms of analytic varieties.

3. TOROIDAL MORPHISMS

In this section we prove a property of toroidal morphisms that we need in order to see that Theorem 1.3 is a direct consequence of the Weak Toroidalization Theorem [2].

Proposition 3.1. *Let $f : X \rightarrow Y$ be a dominant morphism of non-singular integral separated schemes of finite type over a field K of characteristic zero. Assume that f is toroidal with respect to strict toroidal embeddings $U_X \subset X$, $U_Y \subset Y$ (as defined in [2]). Then for each K -rational point a of X , there exist uniformizing parameters $\tilde{x}_1, \dots, \tilde{x}_n$ for the henselization $\mathcal{O}_{X,a}^h$ of $\mathcal{O}_{X,a}$, uniformizing parameters $y_1, \dots, y_m$ for $\mathcal{O}_{Y,f(a)}$, and non-negative integers $e_{j,i}$ such that f is given by $y_j = \prod_i \tilde{x}_i^{e_{j,i}}$, the ideal of $D_X := X \setminus U_X$ in $\mathcal{O}_{X,a}^h$ is generated by $\prod_i \tilde{x}_i$, and the ideal of $D_Y := Y \setminus U_Y$ in $\mathcal{O}_{Y,f(a)}$ is generated by $\prod_j y_j$.*

Proof. Let $\bar{K}$ be an algebraic closure of K , and let $\bar{X}, \bar{Y}$ be the base change to $\bar{K}$ of X, Y . There exist uniformizing parameters $\bar{x}_i$, $i = 1, \dots, n$, for the completion of $\mathcal{O}_{\bar{X},a}$, and uniformizing parameters $\bar{y}_j$, $j = 1, \dots, m$, for the completion of $\mathcal{O}_{\bar{Y},f(a)}$, such that $\bar{y}_j = \prod_{i=1}^n \bar{x}_i^{e_{j,i}}$, with the $e_{j,i}$ forming a matrix of maximal rank $m \leq n$. Moreover, because D_X and D_Y are strict normal crossings divisors over K , there are uniformizing parameters x_i , $i = 1, \dots, n$, for $\mathcal{O}_{X,a}$, and uniformizing parameters y_j , $j = 1, \dots, m$, for $\mathcal{O}_{Y,f(a)}$, such that $\bar{x}_i/x_i$, $\bar{y}_j/y_j$ are units, the ideal of D_X in $\mathcal{O}_{X,a}$ is generated by $\prod_{i=1}^n x_i$, and the ideal of D_Y in $\mathcal{O}_{Y,f(a)}$ is generated by $\prod_{j=1}^m y_j$. Hence there exist units u_j , $j = 1, \dots, m$, in $\mathcal{O}_{X,a}$ such that $y_j = u_j \prod_{i=1}^n x_i^{e_{j,i}}$. Changing y_j we may assume that u_j has residue 1.

For $j = m + 1, \dots, n$, define $u_j := 1$ and $y_j = u_j \prod_{i=1}^n x_i^{e_{j,i}}$, with $e_{j,i}$ any non-negative integers, such that the matrices

$$[e_{j,i}]_{j,i=1,\dots,n} \quad \text{and} \quad [(\partial \log y_j / \partial \log x_i)(a)]_{j,i=1,\dots,n}$$

have maximal rank n . Such non-negative integers exist because the first m rows of the second matrix form a matrix with maximal rank m , since the same is true for x_i, y_j replaced by $\bar{x}_i, \bar{y}_j$, for $j = 1, \dots, m$, and because the components of the other rows of the second matrix are the $e_{j,i}$, with $j > m$.

By Hensel's Lemma there exist units $\epsilon_i \in \mathcal{O}_{X,a}^h$, with residue 1, for $i = 1, \dots, n$, such that $u_j = \prod_{i=1}^n \epsilon_i^{e_{j,i}}$, for $j = 1, \dots, n$. Put $\tilde{x}_i = \epsilon_i x_i \in \mathcal{O}_{X,a}^h$, for $i = 1, \dots, n$; then $y_j = \prod_{i=1}^n \tilde{x}_i^{e_{j,i}}$, for $j = 1, \dots, n$. It remains to prove that the $\tilde{x}_i$ are uniformizing parameters for $\mathcal{O}_{X,a}^h$. Thus we have to show that the jacobian $\partial \tilde{x} / \partial x$ has maximal rank n at a . But this follows directly from the formula $\partial \log y / \partial \log x = \partial \log y / \partial \log \tilde{x} \cdot \partial \log \tilde{x} / \partial \log x$, because the left side has maximal rank n at a and $\det \partial \log \tilde{x} / \partial \log x = (\prod_i \epsilon_i^{-1}) \det \partial \tilde{x} / \partial x$. This terminates the proof of the proposition. $\square$

Remark 3.2. From the above proof it follows that in the definition of toroidal morphisms with respect to non-singular strict toroidal embeddings (over fields of characteristic zero), as defined in [2], we can replace the completions by henselizations. Using this fact, it is easy to verify that if f is toroidal, then also $f \otimes_K L$ is toroidal for any field extension L of K . See also Remark 2.2.1 in [2].

REFERENCES

- [1] D. Abramovich and K. Karu, *Weak semistable reduction in characteristic 0*, Invent. Math. **139** (2000), no. 2, 241–273, DOI 10.1007/s002229900024. MR1738451 (2001f:14021)
- [2] Dan Abramovich, Jan Denef, and Kalle Karu, *Weak toroidalization over non-closed fields*, Manuscripta Mathematica (2013), DOI:10.1007/s00229-013-0610-5
- [3] James Ax and Simon Kochen, *Diophantine problems over local fields. I*, Amer. J. Math. **87** (1965), 605–630. MR0184930 (32 #2401)
- [4] Paul J. Cohen, *Decision procedures for real and p -adic fields*, Comm. Pure Appl. Math. **22** (1969), 131–151. MR0244025 (39 #5342)
- [5] Steven Dale Cutkosky, *Local monomialization of transcendental extensions*, Ann. Inst. Fourier (Grenoble) **55** (2005), no. 5, 1517–1586 (English, with English and French summaries). MR2172273 (2007i:14016)
- [6] Steven Dale Cutkosky, *Toroidalization of dominant morphisms of 3-folds*, Mem. Amer. Math. Soc. **190** (2007), no. 890, vi+222. MR2356202 (2008k:14028)
- [7] J. Denef, *The rationality of the Poincaré series associated to the p -adic points on a variety*, Invent. Math. **77** (1984), no. 1, 1–23, DOI 10.1007/BF01389133. MR751129 (86c:11043)
- [8] Jan Denef, *p -adic semi-algebraic sets and cell decomposition*, J. Reine Angew. Math. **369** (1986), 154–166, DOI 10.1515/crll.1986.369.154. MR850632 (88d:11030)
- [9] Jan Denef, *Algebraic geometric proof of theorems of Ax-Kochen and Eršov*, 2011, <http://perswww.kuleuven.be/~u0009256/Denef-Mathematics>
- [10] Ju. L. Eršov, *On elementary theories of local fields*, Algebra i Logika Sem. **4** (1965), no. 2, 5–30 (Russian). MR0207686 (34 #7501)
- [11] Luc Illusie and Michael Temkin, *Gabber's modification theorem (log smooth case)*, 2012, Exposé 10 in: Travaux de Gabber sur l'uniformisation locale et la cohomologie étale des schémas quasi-excellents (Séminaire à l'École Polytechnique 2006–2008). Luc Illusie, Yves Laszlo, Fabrice Orgogozo, editors, arXiv:1207.3648.
- [12] Angus Macintyre, *On definable subsets of p -adic fields*, J. Symbolic Logic **41** (1976), no. 3, 605–610. MR0485335 (58 #5182)

DEPARTMENT OF MATHEMATICS, KU LEUVEN, CELESTIJNENLAAN 200B, BUS 2400, 3001 LEUVEN, BELGIUM

E-mail address: Jan.Denef@wis.kuleuven.be