On the decidability of the p-adic exponential ring.

Nathanaël Mariaule

Seconda Università degli Studi di Napoli

Model Theory of Fields
(Interaction between Model Theory and Field Theory)
UMons, Mons, November 18, 2013

Introduction

Theorem (A. Macintyre, A. Wilkie)

If Schanuel's conjecture is true, $Th(\mathbb{R}_{\mathsf{exp}})$ is decidable.

On the other hand, $Th(\mathbb{C}_{exp})$ is undecidable.

Problem

Is the theory of $\mathbb{Q}_{p,exp}$ decidable?

Plan

Plan

p-adic numbers

Let p be a prime number. Consider the map:

$$\begin{array}{rrcl} v_p: & \mathbb{Z}^* & \longrightarrow & \mathbb{Z} \\ & x = p^n m & \longmapsto & n. \end{array}$$

We define $v_p(0) = +\infty$ and extend the map to the set $\mathbb{Q}$:

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

To the map v_p corresponds a distance $|x|_p := p^{-v_p(x)}$.
The field of p-adic number $\mathbb{Q}_p$ is defined as the completion of $\mathbb{Q}$ with respect to the distance $|\cdot|_p$.

p-adic numbers

$|\cdot|_p$ is an absolute value on the field $\mathbb{Q}_p$. i.e. for all $x, y \in \mathbb{Q}_p$

1. $|x|_p = 0$ iff $x = 0$;
2. $|xy|_p = |x|_p \, |y|_p$;
3. $|x + y|_p \leq \max\{|x|_p \, , |y|_p\}$ (ultrametric inequality).

p-adic numbers

$(\mathbb{Q}_p, v_p)$ is a valued field.

- the valuation ring: $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \ v_p(x) \geq 0\}$;
- its maximal ideal: $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \ v_p(x) > 0\}$.

The field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ is called *residue field* of $\mathbb{Q}_p$.
$Res : \mathbb{Z}_p \longrightarrow \mathbb{F}_p$ is called the residue map.

p-adic exponential function

Fix a sequence $\{a_n\} \subset \mathbb{Q}_p$.
The series $\sum a_n$ is convergent in $\mathbb{Q}_p$ iff $|a_n|_p \to 0$ iff $v_p(a_n) \to \infty$.

The exponential function defined by the usual power series $exp(x) = \sum \frac{x^n}{n!}$ is convergent iff

$$v_p(x) > \frac{1}{p-1}.$$

p-adic exponential ring

We define the function

$$\begin{array}{rcl} E_p : (\mathbb{Z}_p, +, 0) & \longrightarrow & (\mathbb{Z}_p^\times, \cdot, 1) \\ x & \longmapsto & \begin{cases} exp(p \cdot x) & \text{if } p \neq 2 \\ exp(4 \cdot x) & \text{otherwise.} \end{cases} \end{array}$$

$$\mathcal{L}_{\text{exp}} = (+, \cdot, 0, 1, E_p, P_n; n \in \mathbb{N}),$$

$\mathbb{Z}_{p,\text{exp}}$ denotes the structure $\mathbb{Z}_p$ in the language $\mathcal{L}_{\text{exp}}$.

Problem

Is $Th(\mathbb{Z}_{p,\text{exp}})$ decidable?

Let us remark that it is not difficult to generalise the results of this talk to the structure $(\mathcal{O}_K, +, \cdot, 0, 1, E_p, P_k)$ where $\mathcal{O}_K$ is the valuation ring of a finite algebraic extension K of $\mathbb{Q}_p$.

Plan

Model-completeness

Theorem (A. Macintyre [2], see also [3])

$\mathrm{Th}(\mathbb{Z}_{p,\mathrm{exp}})$ is model-complete in the language $\mathcal{L}_{\mathrm{exp}}$ expanded by 'trigonometric' functions.

Theorem (J. Denef, L. van den Dries [1])

The theory of $\mathbb{Z}_p$ admits elimination of quantifiers in $\mathcal{L}_{an}^D$.

Weierstrass Preparation theorem

Definition

Let $f \in \mathbb{Z}_p\{\overline{X}, Y\}$, $f = \sum f_i(\overline{X})Y^i$. We say that f has order d in Y if

$$Res(f) = A_0(\overline{X}) + \cdots + A_{d-1}(\overline{X})Y^{d-1} + Y^d$$

where $A_i(\overline{X}) \in \mathbb{F}_p[\overline{X}]$.

Weierstrass Preparation Theorem

Let $f(\overline{X}, Y) \in \mathbb{Z}_p\{\overline{X}, Y\}$ of order d in Y. Then, there are $a_0(\overline{X}), \cdots, a_{d-1}(\overline{X}) \in \mathbb{Z}_p\{\overline{X}\}$ and $u(\overline{X}, Y) \in \mathbb{Z}_p\{\overline{X}, Y\}$ a unit such that

$$f(\overline{X}, Y) = u(\overline{X}, Y) \cdot \left[Y^d + a_{d-1}(\overline{X})Y^{d-1} + \cdots + a_0(\overline{X})\right].$$

Weierstrass system

A *Weierstrass system* over $\mathbb{Z}_p$ is a family of rings $\mathbb{Z}_p[\![X_1, \cdots, X_n]\!]$, $n \in \mathbb{N}$, such that for all n, the following conditions hold:

1. $\mathbb{Z}[\overline{X}] \subseteq \mathbb{Z}_p[\![\overline{X}]\!] \subseteq \mathbb{Z}_p\{\overline{X}\}$ where $\overline{X} = (X_1, \cdots, X_n)$;
2. $\mathbb{Z}_p[\![X_1, \cdots, X_n]\!]$ is closed under permutation of the variables, inverses and division by integers (whenever it is well-defined in $\mathbb{Z}_p\{\overline{X}\}$);
3. (Weierstrass division) If $f \in \mathbb{Z}_p[\![X_1, \cdots, X_n, Y]\!]$ and f is regular of order d in Y, then, for all $g \in \mathbb{Z}_p[\![\overline{X}, Y]\!]$, there are $a_0, \cdots, a_{d-1} \in \mathbb{Z}_p[\![\overline{X}]\!]$ and $q \in \mathbb{Z}_p[\![\overline{X}]\!]$ such that

$$g(\overline{X}, Y) = q(\overline{X}, Y) \cdot f(\overline{X}, Y) + \Big(Y^{d-1} a_{d-1}(\overline{X}) + \cdots + a_0(\overline{X})\Big).$$

Weierstrass system

Corollary

Let W be a Weirestrass system, then Th$(\mathbb{Z}_p)$ admits quantifier elimination in $\mathcal{L}_W^D$.
Th$(\mathbb{Z}_p)$ is model-complete in $\mathcal{L}_W$.

Let $\mathcal{L}_{pEC}$ be the expansion of $\mathcal{L}_{exp}$ by the trigonometric functions.
We define *the Weierstrass system generated by the $\mathcal{L}_{pEC}$-terms* by:
For each n, let $W_n^{(0)}$ be the set of $\mathcal{L}_{pEC}$-terms with n variables.
We define $W_n^{(m+1)}$ by induction on m.
$W_n^{(m+1)}$ is the ring generated by:

1. $W_n^{(m)} \subset W_n^{(m+1)}$;
2. For all $f \in W_n^{(m)}$, if g is obtained from f using a permutation of the variables, inversion or division by an integer (when it makes sense in $\mathbb{Z}_p\{\overline{X}\}$), then $g \in W_n^{(m+1)}$;
3. For each $f \in W_{n+1}^{(m)}$ of order d in X_{n+1}, for each $g \in W_{n+1}^{(m)}$, the functions $a_0, \cdots, a_{d-1} \in \mathbb{Z}_p\{\overline{X}\}$ and $q \in \mathbb{Z}_p\{\overline{X}, Y\}$ given by the Weierstrass division and their partial derivatives belong to $W_n^{(m+1)}$ and $W_{n+1}^{(m+1)}$ respectively.

Let $W_n := \bigcup_m W_n^{(m)}$. It determines a Weierstrass system W_{exp}.

Weierstrass system generated by $\mathcal{L}_{pEC}$

Then, $Th(\mathbb{Z}_p)$ is model-complete in $\mathcal{L}_{W_{exp}}$.

Lemma

Let $f \in W^{(m+1)} = \bigcup_n W_n^{(m+1)}$. Then, f is $\mathcal{L}_{W^{(m)}}$-existentially definable.

So, by induction, any function in W_{exp} is existentially definable in $\mathcal{L}_{pEC}$.
The hard case is when f is obtained using the Weierstrass division theorem.

Existential definition of the Weierstrass coefficients

Let $f(\overline{X}, Y) \in \mathbb{Z}_p\{\overline{X}, Y\}$ of order d in Y. Let $a_0(\overline{X}), \cdots, a_{d-1}(\overline{X})$ be the power series like in the Weierstrass preparation theorem.
Fix $\overline{x} \in \mathbb{Z}_p^m$.
Let $\alpha_1, \cdots, \alpha_d$ roots of $f(\overline{x}, Y)$ in $\widetilde{\mathbb{Q}_p}$ with nonnegative valuation. Assume $\alpha_i \neq \alpha_j$ for all $i \neq j$. Then,

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ \vdots & & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \cdot \begin{pmatrix} a_0(\overline{x}) \\ \vdots \\ a_{d-1}(\overline{x}) \end{pmatrix} = \begin{pmatrix} \alpha_1^d \\ \vdots \\ \alpha_d^d \end{pmatrix} . (*)$$

determines uniquely $a_0(\overline{x}), \cdots, a_{d-1}(\overline{x})$. We can also define the coefficients $a_i(\overline{x})$ when the roots are singular.

Existential definition of the Weierstrass coefficients

We define (K_n) a family of finite algebraic extensions of $\mathbb{Q}_p$ such that:

- $K_m \subset K_n$ for all $m < n$;
- K_n is the splitting field of P_n polynomial with coefficients in $\mathbb{Q}$ and is generated by β_n any root of P_n;
- $V_n = \mathbb{Z}_p[\beta_n]$;
- any extension of degree n is contained in K_n.

Then, $\alpha_1, \cdots, \alpha_d \in V_d$ (for all choice of $\overline{x}$).

Existential definition of the Weierstrass coefficients

As $\alpha_1, \cdots, \alpha_d \in V_d$ (for all choice of $\overline{x}$), the graphs of $a_0, \cdots, a_{d-1}$ are determined by an existential formula of the type:

$$\Gamma(\overline{x}, a_0, \cdots, a_{d-1}) \equiv \exists \alpha_1 \cdots \alpha_d \in V_d \ \wedge_i f(\overline{x}, \alpha_i) = 0 \wedge \bigwedge_l \Big(\wedge_{i \neq j} \alpha_i \neq \alpha_j \rightarrow T_l(\overline{\alpha}, \overline{a}) = 0 \Big),$$

where l varies over all possibilities for the multiplicities of the roots and the terms T_l are polynomials like (*).
Note that the formula Γ quantifies over V_d. If we are able to define the structure $(V_d, +, \cdot, 0, 1, P_k, E_p)$ in $\mathbb{Z}_{p,\mathrm{exp}}$, then Γ would be equivalent to an existential formula over $\mathbb{Z}_p$. Therefore the graphs of a_i's would be existentially definable in $\mathbb{Z}_{p,\mathrm{exp}}$ and so we would have model-completeness (as any function in $\mathcal{L}_{W_{exp}}$ would be existentially definable in $\mathcal{L}_{exp}$).

Existential definition of the Weierstrass coefficients

The structure $(V_n, +, \cdot, 0, 1)$ is definable in $\mathbb{Z}_{p,\mathrm{exp}}$.
However, the structure $(V_n, +, \cdot, 0, 1, E_p)$ may not be interpretable in $\mathbb{Z}_{p,\mathrm{exp}}$.
We will add in our language symbols for functions such that the above structure is definable in the expanded language.

Existential definition of the Weierstrass coefficients

Let $V_n = \mathbb{Z}_p[\beta_n]$ as before.
We decompose $E_p(\beta_n^k x)$, $k < d_n$, in the basis of V_n over $\mathbb{Z}_p$:

$$E_p(\beta_n^k x) = c_{0,k,n}(x) + c_{1,k,n}(x)\beta_n + \cdots + c_{d_n-1,k,n}(x)\beta_n^{d_n-1}.$$

We define the language $\mathcal{L}_{pEC}$ the expansion of $\mathcal{L}_{\exp}$ by symbols for the functions $c_{i,k,n}$ determined by the extensions K_n.

Lemma

$(V_n, +, \cdot, 0, 1, P_k, E_p, c_{ijl})$ is definable in $(\mathbb{Z}_p, +, \cdot, 0, 1, P_k, E_p, c_{ijl})$.

Effective model-completeness

Theorem (A. Macintyre)

The theory of $\mathbb{Z}_p$ is model-complete in the language $\mathcal{L}_{pEC}$.

Furthermore,

Lemma

The above model-completeness is effective i.e. given $\psi(\overline{x})$ a $\mathcal{L}_{pEC}$-formula, one can compute an existential formula equivalent to $\psi(\overline{x})$.

Plan

1. p-adic exponential
2. Effective model-completeness
3. Decidability

Existential sentences

Any sentence is (effectively) equivalent to a disjunction of sentences of the type:

$$\exists \overline{x} f(\overline{x}) = 0 \wedge g(\overline{x}) \neq 0, \ (*)$$

where f, g are $\mathcal{L}_{pEC}$-terms.
It is sufficient to give an algorithm that stops if $(*)$ is true (and may never stop otherwise).
For simplicity, I will assume that f, g are $\mathcal{L}_{\mathrm{exp}}$-terms of the form:
$F_P(\overline{X}) = P(x_1, \cdots, x_n, E_p(x_1), \cdots, E_p(x_n))$ where $P \in \mathbb{Z}[\overline{X}, \overline{Y}]$.

Analytic Hensel's lemma

Analytic Hensel's lemma

Let $\mathbf{f} = (f_1, \cdots, f_n)$, $f_i \in \mathbb{Z}_p\{X_1, \cdots, X_n\}$ and $r \in \mathbb{N}$.
Assume there exists $\overline{a} \in \mathbb{Z}_p^n$ such that

$$det\ J_{\mathbf{f}}(\overline{a}) \neq 0 \text{ and } v\Big(\mathbf{f}(\overline{a})\Big) > 2 \cdot v\Big(det\ J_{\mathbf{f}}(\overline{a})\Big) + r.$$

Then, there exists a unique $\overline{b} \in \mathbb{Z}_p^n$ such that

$$\mathbf{f}(\overline{b}) = 0 \text{ and } v(\overline{b} - \overline{a}) > v\Big(det\ J_{\mathbf{f}}(\overline{a})\Big) + r.$$

Nonsingular case

Fix $\mathbf{f} = (F_{P_1}, \cdots, F_{P_n})$, $P_i \in \mathbb{Z}[X_1, \cdots, X_n, Y_1, \cdots, Y_n]$.
We can determine if the sentence:

$$\exists \overline{x}\ \overline{x} \in V^{ns}(\mathbf{f}) \equiv \exists \overline{x}\ F_{P_1}(\overline{x}) = \cdots = F_{P_n}(\overline{x}) = 0 \neq det\ J_{\mathbf{f}}(\overline{x}).$$

is true in $\mathbb{Z}_p$:

Algorithm

Fix $\overline{a}_0, \overline{a}_1, \cdots$, an enumeration of $\mathbb{Z}^n$.
For each i, if

$$det\ J_{\mathbf{f}}(\overline{a}_i) \neq 0 \text{ and } v\Big(\mathbf{f}(\overline{a}_i)\Big) > 2 \cdot v\Big(det\ J_{\mathbf{f}}(\overline{a}_i)\Big)$$

return true. Otherwise, go to $i+1$.

Desingularization theorem

Theorem (see [3])

Let $F_P \in \mathbb{Z}[X_1, \cdots, X_n, E_p(X_1), \cdots, E_p(X_n)]$, $V(F_P) \neq \varnothing$. Then, there exist $F_{P_1}, \cdots, F_{P_n} \in \mathbb{Z}[\overline{X}, E_p(\overline{X})]$ such that

$$V(F_P) \cap V^{ns}(F_{P_1}, \cdots, F_{P_n}) \neq \varnothing.$$

Lemma

Let $m, r \in \mathbb{N}$, I *prime ideal of* $\mathbb{Z}[X_1, \cdots, X_m]$, $I \cap \mathbb{Z} = \{0\}$ *such that*

$$trdeg_{\mathbb{Q}}\ Frac\Big(\mathbb{Z}[\overline{X}]/I\Big) = r.$$

Then, there exists $Q \in \mathbb{Z}[\overline{X}] \setminus I$ *such that* $Q \cdot I$ *is generated by* $(m-r)$ *elements.*

Let $\overline{b} \in V(F_P) \cap V^{ns}(F_{P_1}, \cdots F_{P_n})$ like in the last theorem. We want to apply the lemma with

$$I := \{h \in \mathbb{Z}[\overline{X}, \overline{Y}] \mid h(b_1, \cdots, b_n, E_p(b_1), \cdots E_p(b_n)) = 0\}.$$

We have that:

$$trdeg_{\mathbb{Q}}\ Frac\Big(\mathbb{Z}[\overline{X}]/I\Big) = trdeg_{\mathbb{Q}}(b_1, \cdots, b_n, E_p(b_1), \cdots E_p(b_n)).$$

As $\overline{b} \in V^{ns}(F_{P_1}, \cdots F_{P_n})$,

$$trdeg_{\mathbb{Q}}(b_1, \cdots, b_n, E_p(b_1), \cdots E_p(b_n)) \leq n.$$

In order to obtain the equality, we use a p-adic version of Schanuel's conjecture.

Schanuel's conjecture

p-adic Schanuel's conjecture

Let $\beta_1, \cdots, \beta_n \in \mathbb{C}_p$, $\mathbb{Q}$-linearly independent such that $v(\beta_i) > 1/(p-1)$. Then,

$$trdeg_{\mathbb{Q}}\mathbb{Q}(\beta_1, \cdots, \beta_n, exp(\beta_1), \cdots, exp(\beta_n)) \geq n.$$

Let $F_P(\overline{X}) = P(\overline{X}, E_p(\overline{X}))$. Assume that $F_P(\overline{a}) = 0$ for some $\overline{a} \in \mathbb{Z}_p^n$.
Let $F_{P_1}, \cdots, F_{P_n}$ like in the last theorem.
Let $\overline{b} \in V(F_P) \cap V^{ns}(F_{P_1}, \cdots, F_{P_n})$.
Assume that Schanuel's conjecture is true. Then if $b_1, \cdots, b_n$ are $\mathbb{Q}$-linearly independent,

$$trdeg_{\mathbb{Q}} \mathbb{Q}(b_1, \cdots, b_n, E_p(b_1), \cdots, E_p(b_n)) = n.$$

So, by the lemma, there exist $Q, Q_1, \cdots, Q_n, S_1, \cdots, S_n$ such that

$$QP = \sum S_i Q_i.$$

Furthermore, $\overline{b} \in V^{ns}(F_{Q_1}, \cdots, F_{Q_n})$.

Decidability

Theorem (see [3])

If the p-adic Schanuel's conjecture is true, $Th(\mathbb{Z}_{p,\mathsf{exp}})$ and $Th(\mathbb{Z}_{pEC})$ are decidable.

Let $\Psi \equiv \exists \overline{x} F_P(\overline{x}) = 0 \wedge F_R(\overline{x}) \neq 0$.
Assume that the formula is realised by $\overline{\alpha} \in \mathbb{Z}_p$ where $\alpha_1, \cdots, \alpha_n$ are $\mathbb{Q}$-linearly independent. Then, the following algorithm stops and returns true.

Algorithm

Enumerate all

- $\overline{a} + p^k \mathbb{Z}_p^n$ where $\overline{a}$ runs over $\mathbb{Z}^n$ and k over $\mathbb{N}$;
- $m \in \mathbb{N}$, $m > k$;
- $Q, Q_1, \cdots, Q_n, S_1, \cdots, S_n \in \mathbb{Z}[X_1, \cdots, X_n, Y_1, \cdots, Y_n]$.

If

- $QP = \sum S_i Q_i$;
- $detJ_{\mathbf{f}}(\overline{a}) \neq 0$ and $v\Big(\mathbf{f}(\overline{a})\Big) > 2 \cdot v\Big(detJ_{\mathbf{f}}(\overline{a})\Big) + k$;
- for all $\overline{b} \in (\mathbb{Z}/p^m\mathbb{Z})^n$ such that $\overline{b} \equiv \overline{a} \mod p^k$, $F_Q(\overline{b}) \not\equiv 0 \mod p^m$ and $F_R(\overline{b}) \not\equiv 0 \mod p^m$;

return true. Otherwise, go to the next step.

Bibliography

[1] J. Denef and L. van den Dries.
p-adic and Real Subanalytic Sets.
The Annals of Mathematics, Second Series, Vol. 128, No.1, pages 79–138, 1988.

[2] A. Macintyre.
The elementary theory of p-adic exponentiation.
Unpublished.

[3] N. Mariaule.
On the decidability of the p-adic exponential ring.
PhD thesis, University of Manchester, 2013.