ON THE DECIDABILITY OF THE P-ADIC EXPONENTIAL RING.

A thesis submitted to the University of Manchester
for the degree of Doctor of Philosophy
in the Faculty of Engineering and Physical Sciences

2013

Nathanaël Mariaule
School of Mathematics

Contents

Word count 24812

The University of Manchester

Nathanaël Mariaule
Doctor of Philosophy
On the decidability of the p-adic exponential ring.
October 4, 2013

Let E_p be the map $x \longmapsto exp(px)$ where exp denotes the exponential map determined by the usual power series. It defines an exponential ring $(\mathbb{Z}_p, +, \cdot, 0, 1, E_p)$. The goal of the thesis is to study the model theory of this structure. In particular, we are interested by the question of the decidability of this theory.
The main theorem of the thesis is:

Theorem. *If the p-adic Schanuel's conjecture is true, then the theory of* $(\mathbb{Z}_p, +, \cdot, 0, 1, E_p)$ *is decidable.*

The proof involves:

- A result of effective model-completeness (chapters 3 and 4): If F is a family of restricted analytic functions (i.e. power series with coefficients in the valuation ring and convergent on $\mathbb{Z}_p$) closed under decomposition functions and such that the set of terms in the language $\mathcal{L}_F = (+, \cdot, 0, 1, f; f \in F)$ is closed under derivation, then we prove that the theory of $\mathbb{Z}_p$ in the language $\mathcal{L}_F$ is model-complete. And furthermore, if each term of $\mathcal{L}_F$ has an effective Weierstrass bound, then the model-completeness is effective.

- A resolution of the decision problem for existential formulas (assuming Schanuel's conjecture) in chapter 5.

We also consider the problem of the decidability of the structure $(\mathcal{O}_p, +, \cdot, 0, 1, |, E_p)$ where $\mathcal{O}_p$ denotes the valuation ring of $\mathbb{C}_p$. We give a positive answer to this question assuming the p-adic Schanuel's conjecture.

Declaration

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

Copyright Statement

Acknowledgements

First, I would like to thanks my supervisor Alex Wilkie for its mathematical and moral support. I am also very grateful to Angus Macintyre who kindly made available its unpublished notes on the p-adic exponential.

I also thank my family and my friends for their support in many ways.

Index of Notation

$\overline{x}$	a tuple $(x_1, \cdots, x_n)$
$\lvert I\rvert = i_1 + \cdots + i_n$	where $I \in \mathbb{N}^n$
K^*, R^*	The set of nonzero elements of a field K (resp. a ring R)
$R^\times$	The set of invertible elements of a ring R
K^{alg}	The algebraic closure of K
$Gal(L/K)$	The Galois group of L over K
$\mathbb{N}$	The set of nonnegative integers
$\mathbb{N}_0$	The set of positive integers
$\mathbb{Z}$	The set of integers
$\mathbb{Q}$	The set of rational numbers
$\mathbb{R}$	The set of real numbers
$\mathbb{R}_{>0}, \mathbb{R}_{\geq 0}$	The set of positive (resp. nonnegative) real numbers
$\mathbb{Q}_p$	The field of p-adic numbers
$\mathbb{Z}_p$	The ring of p-adic integers
$\mathbb{C}_p$	The completion of $\mathbb{Q}_p^{alg}$
$\mathbb{F}_p$	Finite field with p elements
v_p, v	The p-adic valuation

$\|.\|_p, \|.\|$	The p-adic distance
$\mathcal{O}_K$	The valuation ring K
$\mathfrak{M}_K$	The maximal ideal of $\mathcal{O}_K$
$\overline{K}$	The residue field of a valued field K
$\mathcal{O}_p$	The valuation ring of $\mathbb{C}_p$
$\mathfrak{M}_p$	The maximal ideal of $\mathcal{O}_p$
$N_{K\|\mathbb{Q}_p}$	The norm from K over $\mathbb{Q}_p$, page 17
$R[[\overline{X}]]$	The ring of formal power series with coefficients in R
$R\{\overline{X}\}$	The ring of restricted analytic functions, page 20
$R[\overline{X}]^E$	The ring of exponential polynomials, page 29
$\mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$	The ring of separated power series, page 103
$\mathbb{Z}_p[\![X_1, \cdots, X_n]\!]$	A Weierstrass system, page 36
$\mathcal{O}_p[\![X_1, \cdots, X_n, \rho_1, \cdots, \rho_m]\!]_s$	A separated Weierstrass system, page 105
$\|\|f\|\|$	The Gauss norm of f , page 20
$V_K(f), V(f)$	The set of zeros of f in K
$Trop(f)$	The tropicalization of f, page 123
$\mathcal{L}_P$	The language of p-adic fields, page 26
$\mathcal{L}_{an}$	The language of restricted analytic functions, page 27
$\mathcal{L}_{an}^D$	The expansion of $\mathcal{L}_{an}$ by a division symbol
$\mathbb{Z}_{p,an}$	The structure $(\mathbb{Z}_p, f(f \in \mathbb{Z}_p\{\overline{X}\}), D, P_n(n \in \mathbb{N}_0))$, page 27
$\mathcal{L}_{exp}$	The language of p-adic exponential rings, page 28
$\mathbb{Z}_{p,exp}$	The structure $(\mathbb{Z}_p, +, \cdot, E_p, 0, 1, P_n; n \in \mathbb{N})$, page 28

$\mathcal{L}_{pEC}$ The language of p-adic exponential rings expanded by the trigonometric functions, page 66

$\mathbb{Z}_{pEC}$ The structure with underlying set $\mathbb{Z}_p$ and natural interpretations for the symbols in the language $\mathcal{L}_{pEC}$

$\mathcal{L}_F$ The language $(+, \cdot, 0, 1, f(f \in F), P_n(n \in \mathbb{N}))$ where F is a family of restricted analytic functions

$\mathbb{Z}_{p,F}$ The structure with underlying set $\mathbb{Z}_p$ and natural interpretations for the symbols in the language $\mathcal{L}_F$

Chapter 1

Introduction

Let E_p be the map $x \longmapsto exp(px)$ where $exp(x)$ denotes the power series $\sum x^n/n!$. This map is well-defined on $\mathbb{Z}_p$. It determines an exponential ring $(\mathbb{Z}_p, +, \cdot, 0, 1, E_p)$ i.e. a ring R together with a morphism from the additive group $(R, +, 0)$ to the multiplicative group $(R^\times, \cdot, 1)$. The goal of the thesis is to study the model theory of this exponential ring.
We define $\mathcal{L}_{exp}$, the language of p-adic exponential rings, as the expansion of the language of p-adically closed fields $\mathcal{L}_P = (+, \cdot, 0, 1, P_n; n \in \mathbb{N})$ by a function symbol for E_p. Let $\mathbb{Z}_{p,exp}$ denote the structure with underlying set $\mathbb{Z}_p$ and natural interpretations for the elements of the language $\mathcal{L}_{exp}$. This should be thought as the p-adic equivalent of the structure $\mathbb{R}_{exp}$ where we restrict the exponential to a compact interval.

The main goal of the thesis is to prove:

Theorem. *If the p-adic Schanuel's conjecture is true, then the theory of $\mathbb{Z}_{p,exp}$ is decidable.*

The proof is split in two main parts: first, in chapters 3 and 4, we prove a result of effective model-completeness. Then in chapter 5, assuming Schanuel's conjecture, we show the decidability of the existential part of the theory.

In chapter 3, we prove a result of strong model-completeness based on the quantifier elimination in $\mathbb{Z}_{p,an}$. $\mathbb{Z}_{p,an}$ denotes the structure with underlying set $\mathbb{Z}_p$ in $\mathcal{L}_{an}$, the language $\mathcal{L}_P$ expanded by all restricted analytic functions (in the sense of J. Denef, L.

van den Dries [4]). In [4], it is proved that the theory of $\mathbb{Z}_{p,an}$ eliminates the quantifiers in the language $\mathcal{L}_{an}$ expanded by a division symbol D.
Let $\mathcal{L}_F$ be a reduction of this language i.e. we consider a family of restricted analytic functions F and $\mathcal{L}_F$ is the expansion of $\mathcal{L}_P$ by the elements of F. It is immediate from the proof of the quantifier elimination in $\mathcal{L}_{an}^D$ that $\mathbb{Z}_p$ admits the elimination of quantifiers in $\mathcal{L}_{W_F}^D$ where W_F denotes the *Weierstrass system generated by the $\mathcal{L}_F$-terms.*
In chapter 3, we show that the functions in W_F are strongly definable in $\mathcal{L}_F$. For this, we require that the set of $\mathcal{L}_F$-terms is closed under derivation and that the structure $(V, +, \cdot, 0, 1, f; f \in F)$ is existentially definably interpretable in our structure (where V could be the valuation ring of any finite algebraic extension of $\mathbb{Q}_p$). The last assumption is not true for general F. So, we will expand F by a family of *decomposition functions* (i.e. functions so that the above structure becomes existentially definably interpretable in the expanded language). Under these hypotheses, we can prove the main result of the chapter:

Theorem 3.4.2. *Let F be a family of restricted analytic functions. Assume that the set of $\mathcal{L}_F$-terms is closed under derivation. Let $\widetilde{F}$ be the extension of F by the decomposition functions of each $f \in F$. Then, $\mathbb{Z}_{p,\widetilde{F}}$ is strongly model-complete in $\mathcal{L}_{\widetilde{F}}$.*

In chapter 4, we study the effectivity of the above theorem. The main issue is that in the proof of 3.4.2 some steps use Noetherian properties and so may not be effective. We show in theorem 4.3.1 that under the assumption that each $\mathcal{L}_{\widetilde{F}}$-term has *an effective Weierstrass bound* (i.e. the Noetherian property is effective for the terms in the language), $\mathbb{Z}_{p,\widetilde{F}}$ is effectively model-complete in the language $\mathcal{L}_{\widetilde{F}}$. This part of the proof involves results of tropical analytic geometry. As the reader may not be familiar with these results, we include in appendix A an introduction to this topic.

In section 4.4 as a particular case of the above results, we consider $F = \{E_p\}$. In that case, let $\mathcal{L}_{pEC}$ denote the expansion of $\mathcal{L}_F$ by the decomposition functions. In this section, we will give a proof due to A. Macintyre in [8] that any $\mathcal{L}_{pEC}$-term has an effective Weierstrass bound. And therefore,

Theorem 4.4.5. *The theory of $\mathbb{Z}_p$ in the language $\mathcal{L}_{pEC}$ is effectively strongly model-complete.*

Let us remark that these results can be easily generalised to any finite algebraic extension.

By theorem 4.4.5, the decidability of $\mathbb{Z}_{p,exp}$ can be reduced to the decidability of the $\mathcal{L}_{pEC}$-existential formulas in $\mathbb{Z}_p$. We consider this problem in chapter 5. We follow the same strategy that the one proposed in [11] to solve the equivalent problem in $\mathbb{R}$. Let $(f_1, \cdots, f_n)$ be a system of $\mathcal{L}_{pEC}$-terms in n variables. Let Ψ be the formula

$$\exists x_1, \cdots, x_n f_1(\overline{x}) = \cdots = f_n(\overline{x}) = 0 \neq \det\ J(\overline{x}),$$

where J denotes the Jacobian of the system. Then, assuming that the formula is true in $\mathbb{Z}_p$, it is not hard to check this property. Indeed, by the analytic Hensel's lemma 2.1.7, Ψ is true in $\mathbb{Z}_p$ iff there is $\overline{t} \in \mathbb{Z}^n$ such that for all i

$$v(f_i(\overline{t})) > 2v(\ \det\ J(\overline{t})).$$

So, if we want to check that Ψ is true, we just have to enumerate all tuples in $\mathbb{Z}^n$ and find one that satisfies the above inequality.
We reduce the general case to this nonsingular case via a desingularization theorem: let f be a $\mathcal{L}_{pEC}$-term. We prove in theorem 5.1.5 that if $f(\overline{X})$ has a root in $\mathbb{Z}_p^n$, then there are $\mathcal{L}_{pEC}$-terms $f_1, \cdots, f_n$ and $\overline{a} \in \mathbb{Z}_p^n$ such that

$$f(\overline{a}) = f_1(\overline{a}) = \cdots = f_n(\overline{a}) = 0 \neq \det\ J(\overline{a}).$$

Then, in lemma 5.2.1, assuming the p-adic Schanuel's conjecture and that f is a $\mathcal{L}_{exp}$-term, we show that there is such a system $(f_1, \cdots, f_n)$ of $\mathcal{L}_{exp}$-terms such that any nonsingular solution $\overline{b}$ is a root of f. In fact, roughly speaking, f is almost in the ideal generated by $f_1, \cdots, f_n$ (note that we can check effectively this property). So, the existence of such a $\overline{b}$ implies $\mathbb{Z}_p \models \exists \overline{x} f(\overline{x}) = 0$. This implies that the positive existential theory of $\mathbb{Z}_{p,exp}$ is decidable if Schanuel's conjecture is true (Proposition 5.2.3).
The general case leads to some difficulties: First, we have to deal with inequalities (lemma 5.2.2). Second, we have to generalise our results to $\mathcal{L}_{pEC}$-terms. In particular,

lemma 5.2.1 is generalised in lemma 5.2.4. In the same section 5.2.2, we prove the main theorem of the thesis:

Theorem 5.2.5. *Assume that the p-adic version of Schanuel's conjecture holds. Then, the theory of $\mathbb{Z}_p$ in the language $\mathcal{L}_{pEC}$ is decidable.*

Finally, in chapter 6, we consider the problem of the decidability of the theory of $\mathcal{O}_p$, the valuation ring of $\mathbb{C}_p$, in the language $\mathcal{L}_{exp} = (+, -, \cdot, 0, 1, |, E_p)$. We use the same techniques that for $\mathbb{Z}_{p,exp}$. First, we prove the effective model-completeness of the theory. Here, we use the quantifier elimination result due to Lipshitz [7]. Instead of restricted power series, we consider Weierstrass system composed by separated power series (in the sense of Lipshitz). The model-compleness (theorem 6.2.11) is here rather immediate if we assume the set of $\mathcal{L}_F$-terms closed under derivation (since we don't need to add decomposition functions as our field is algebraically closed). Once again, we can prove the effectivity of the model-completeness using the results of tropical analytic geometry (theorem 6.3.6).
Then, we prove that the existential part of the theory is decidable. We show that any existential formula realised in our structure is realised in the valuation ring of some finite algebraic extension (proposition 6.4.1). So, as we can enumerate all finite algebraic extensions and by the main result of the thesis,

Theorem 6.4.2. *Assume that the p-adic Schanuel's conjecture is true. Then, the theory of $(\mathcal{O}_{p,exp}, +, -, \cdot, 0, 1, |, E_p)$ in the language of exponential ring is decidable.*

Chapter 2

Preliminaries

2.1 Background

In the first part of this chapter, we introduce some background on the notions of p-adic numbers and p-adic analysis. We will also fix some notations that will be used throughout the thesis. We refer to the index for an overview of the main notations.

2.1.1 p-adic numbers

We will denote by v_p (or when the context is clear by v) the p-adic valuation. Let us recall that this map is defined by:

$$\begin{aligned} v_p : \mathbb{Z} \setminus \{0\} &\longrightarrow \mathbb{Z} \\ m = p^n k &\longmapsto n \text{ where } (p,k) = 1. \end{aligned}$$

We set $v_p(0) = \infty$. We can extend v_p to $\mathbb{Q}$ via the relation

$$v_p(a/b) = v_p(a) - v_p(b).$$

This map is a valuation. In general,

Definition 2.1.1. *Let R be a commutative ring with unity, let $(\Gamma, <)$ be an abelian ordered group and let ∞ be an element such that $a < \infty$ for all $a \in \Gamma$. A* valuation *is a map $v : R \to \Gamma \cup \{\infty\}$ such that for all $a, b \in R$:*

(i) $v(a \cdot b) = v(a) + v(b)$;

(ii) $v(a) = \infty$ *iff* $a = 0$;

(iii) $v(a+b) \geq \min\{v(a), v(b)\}$.

A field K (resp. a ring) equipped with a valuation is called *valued field* (resp. *valued ring*). The group Γ is called *value group*. A valued ring R determines a local ring $\mathcal{O}_R$ defined by

$$\mathcal{O}_R = \{x \mid \ v(x) \geq 0\}.$$

We call this ring the *valuation ring*. Its maximal ideal is

$$\mathfrak{M}_R = \{x \mid \ v(x) > 0\}.$$

The quotient field $\mathcal{O}_R/\mathfrak{M}_R$ is called the *residue field*. We will denote this field by $\overline{R}$ and we denote by $\overline{}$ the canonical map $R \to \overline{R}$. We use the same notation for canonical extensions of the residue map (to polynomial rings for instance).

Let us remark that the p-adic valuation determines a distance on $\mathbb{Q}$:

$$d(x,y) = |x-y|_p := p^{-v_p(x-y)}.$$

We call this distance *p-adic distance* (*p-adic norm* or *p-adic absolute value*) and denote it by $|\cdot|$ when the context is clear. It is not hard to see that the p-adic distance satisfies all the properties of an absolute value (non-negativity, positive-definiteness, multiplicativeness and the triangle inequality). Actually, it satisfies a stronger property than the triangle inequality: by property (iii) in the definition of a valuation, this distance satisfies the *ultrametric property*:

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}.$$

The field of *p-adic numbers* is the completion of $\mathbb{Q}$ with respect to this distance (i.e. is the quotient of the ring of Cauchy sequences in $\mathbb{Q}$ (with respect to $|.|_p$) by the ideal of the null sequences). We denote this field by $\mathbb{Q}_p$. Note that v_p extends uniquely to $\mathbb{Q}_p$. Therefore, $(\mathbb{Q}_p, v_p)$ is a valued field. Its value group is $\mathbb{Z}$. The valuation ring of $\mathbb{Q}_p$ is denoted by $\mathbb{Z}_p$ and is called the ring of *p-adic integers*. Let us remark that this ring is the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$. The maximal ideal of $\mathbb{Q}_p$ is $p\mathbb{Z}_p$ and its residue field is isomorphic to $\mathbb{F}_p$.

Alternatively, we could have defined $\mathbb{Z}_p$ as the inverse limit of the projective system $(\mathbb{Z}/p^n\mathbb{Z}, \pi_n, n \in \mathbb{N}_0)$ (where $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the canonical projection) and set

$\mathbb{Q}_p = Frac\ \mathbb{Z}_p$. The two definitions determine isomorphic, homeomorphic topological fields.

A crucial property of $\mathbb{Q}_p$ is that the field is henselian:

Definition 2.1.2. *A valued field (K, v) is called* henselian *if the valuation extends uniquely to any finite Galois extension.*

Note that if (K, v) is a valued field and L is an extension of K (not necessarily algebraic), then v can always be extended to a valuation on L. The henselian property claims the uniqueness of this extension (when L is an algebraic extension of K).

Equivalently, we may define an henselian field by any of the below properties:

Proposition 2.1.3. *Let (K, v) be a valued field. Then, the following assertions are equivalent:*

(i) K is henselian;

(ii) For all $f \in K[X]$, if there exists $a \in K$ such that $\overline{f}(\overline{a}) = 0 \neq \overline{f'}(\overline{a})$, then there exists a unique $b \in K$ such that $f(b) = 0$ and $\overline{b-a} = 0$;

(iii) For all $f \in K[X]$, if there exists $a \in K$ such that $v(f(a)) > 2v(f'(a))$, then there exists a unique $b \in K$ such that $f(b) = 0$ and $v(a - b) > v(f'(a))$.

In the case of $\mathbb{Q}_p$, condition (ii) is the famous Hensel's lemma. Condition (iii) is sometimes called in the litterature Hensel-Rychlik lemma (or just Hensel's lemma).

Let $K = \mathbb{Q}_p(\alpha)$ be a finite algebraic extension of $\mathbb{Q}_p$ of degree n. As $\mathbb{Q}_p$ is henselian, the valuation v_p extends uniquely to K. We will also denote by v_p this extension. We can describe precisely the valuation of an element of K:

Let $P(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbb{Q}_p[X]$ be the minimal polynomial of α. The *norm from K over $\mathbb{Q}_p$* is

$$N_{K|\mathbb{Q}_p}(\alpha) := (-1)^n a_n.$$

Equivalently, $N_{K|\mathbb{Q}_p}(\alpha) = \prod \alpha_i$ where α_i are the conjugates of α over $\mathbb{Q}_p$ or $N_{K|\mathbb{Q}_p}(\alpha) = det\ A_\alpha$ where A_α is the matrix of the $\mathbb{Q}_p$-linear map determined by the multiplication by α in K. If $\beta \in K$, then

$$N_{K|\mathbb{Q}_p}(\beta) := \left(N_{\mathbb{Q}_p(\beta)|\mathbb{Q}_p}(\beta)\right)^{[K:\mathbb{Q}_p(\beta)]}.$$

Then, the unique absolute value on K extending $|\cdot|_p$ is (up to equivalence of absolute value):

$$|\beta|_p = |N_{K|\mathbb{Q}_p}(\beta)|_p^{1/n}.$$

This determines the unique extension of v_p to K:

$$v_p(\beta) := -\log_p|\beta|_p.$$

Let us note that K is complete with respect to this distance. Also, let us remark that the value group of K is $\frac{1}{e}\mathbb{Z}$ for some $e \in \mathbb{N}$ (called the *ramification index*) while its residue field is a finite algebraic extension of $\mathbb{F}_p$ (say of degree p^f). Then, one can show that $n = e \cdot f$. We call an element with smallest positive valuation *prime element.* Such an element generates the maximal ideal of the valuation ring.

The algebraic closure of $\mathbb{Q}_p$ (denoted $\mathbb{Q}_p^{alg}$) is an extension of infinite degree. This field is not complete with respect to the (unique extension of the) valuation v_p. We denote its completion by $\mathbb{C}_p$. Note that $\mathbb{C}_p$ is an algebraically closed field. This field is the p-adic analogue of the complex field for the real numbers (i.e. is both complete and algebraically closed). Both $\mathbb{C}_p$ and $\mathbb{Q}_p^{alg}$ have for value group $\mathbb{Q}$ and for residue field $\mathbb{F}_p^{alg}$. Note that $\mathbb{Z}_p$ (or the valuation ring of any finite extension of $\mathbb{Q}_p$) is a compact ring. But, this is not the case of the valuation ring of $\mathbb{C}_p$. Actually, this ring is not even locally compact.

We can learn a bit more on the structure of the finite algebraic extensions using Krasner's lemma:

Proposition 2.1.4 (Krasner's lemma)**.** *Let $a, b \in \mathbb{Q}_p^{alg}$. Let $a_1, \cdots, a_n$ be the conjugates of a over $\mathbb{Q}_p$. Assume that for all $1 \leq i \leq n$*

$$v_p(b - a) > v_p(a_i - a).$$

Then, $\mathbb{Q}_p(a) \subseteq \mathbb{Q}_p(b)$.

This lemma can be used to prove that any finite algebraic extension K is contained in an extension of the type $\mathbb{Q}_p(\beta)$ where β is algebraic over $\mathbb{Q}$. It also implies that there are finitely many extensions of a given degree n.

Finally, we fix some notations: we will denote by $\mathcal{O}_p$ the valuation ring of $\mathbb{C}_p$ and by $\mathfrak{M}_p$ its maximal ideal.

2.1.2 p-adic analysis

We are mainly interested by analytic functions and their properties. In particular, we are interested by the zeros of such a function. For the rest of this section, K will be a finite algebraic extension of $\mathbb{Q}_p$ with prime element π_K. We denote by $K[[\overline{X}]]$ the set of formal power series in the variables $\overline{X} = (X_1, \cdots, X_n)$ with coefficients in K.
Let $\sum a_n$ be a series with coefficients in K. Let us recall that, by the ultrametric property, $\sum a_n$ is convergent in K iff $v(a_n) \to \infty$. It implies that a power series $f = \sum a_I \overline{X}^I$ is well-defined at $\overline{x}$ iff $v(a_I \overline{x}^I) \to \infty$ when $I \to \infty$.

Example.

- The series $exp(X) := \sum \frac{X^n}{n!}$ is well-defined at x iff $v(x) > 1/(p-1)$;
- $\log(1+x) = \sum (-1)^{n+1} \frac{x^n}{n}$ is well-defined iff $v(x) > 0$.

Definition 2.1.5. *Let U be an open subset of K^n. We say that a function $f : U \to \mathbb{Q}_p$ is* analytic *on U if for all $\overline{a} \in U$, there exists a neighbourhood $V_{\overline{a}} = \{\overline{x} \mid v(x_i - a_i) > \pi_k^h\}$ of $\overline{a}$ in U and $F(\overline{X}) \in K[[\overline{X}]]$ such that for all $\overline{x} \in \mathcal{O}_K^n$,*

$$f(\overline{a} + \pi_K^h \overline{x}) = F(\overline{x}).$$

For instance, $exp(X)$ and $\log(X)$ are analytic functions on $p^{\frac{1}{p-1}}\mathcal{O}_K$ (the set of element in K with valuation greater than $1/(p-1)$) and $1 + \pi_K \mathcal{O}_K$ respectively. Note that exp determines a bijection between $p^{\frac{1}{p-1}}\mathcal{O}_K$ and $1 + p^{\frac{1}{p-1}}\mathcal{O}_K$. The inverse is given by the restriction of log. However, there is no global analytic exponentiation on $\mathbb{Q}_p$ (though as a morphism of groups, exp can be extended to $\mathbb{C}_p$ but this extension is not unique and there is no canonical choice for such an extension).
Let us remark that the function

$$f : \mathbb{Z}_p \to \mathbb{Z}_p : x \longmapsto \begin{cases} 1 & \text{if } x \in p\mathbb{Z}_p \\ 0 & \text{otherwise} \end{cases}$$

is analytic. There is no notion of analytic continuation in K. For our purpose, this is an issue in the case of non-locally compact valued field. In $\mathbb{C}_p$, we say that a function is analytic on U if in the above definition $F(\overline{x}) = f(\overline{x})$ is defined everywhere on U. Note that in K, the sets of analytic functions on a bounded open set in the sense of the above definition and in the sense of $\mathbb{C}_p$ are morally the same: a function analytic on a compact set in K^n is completely determined by finitely many power series.

We will denote by $K\{\overline{X}\}$ the ring of analytic functions on $\mathcal{O}_K^n$ defined by a single power series. We have that

$$K\{\overline{X}\} = \left\{ \sum f_I \overline{X}^I \in K[[\overline{X}]] : \ v(f_I) \to \infty \right\}.$$

This ring is sometimes called Tate ring. It comes with a norm (called *Gauss norm*) defined by

$$\|f\| = \left\| \sum f_I \overline{X}^I \right\| = \sup_I |f_I|.$$

As $v(f_I) \to \infty$, the supremum is actually a maximum in the above definition. We denote by $\mathcal{O}_K\{\overline{X}\}$ the subset of elements with Gauss norm less than 1. Note that it coincides with the ring of elements in $K\{\overline{X}\}$ with coefficients in $\mathcal{O}_K$. We call this ring *the ring of restricted analytic functions.* We are interested by the functions in this ring; in particular, by the zeros of these functions in $\mathcal{O}_p$. Let us remark that we can extend canonically the residue map to $\mathcal{O}_p\{\overline{X}\}$. It determines a map $\overline{} : \mathcal{O}_p\{\overline{X}\} \longrightarrow \mathbb{F}_p[\overline{X}]$. First, we present an analytic version of Hensel's lemma. It allows to lift non-singular solutions of a system of equations from the residue field to the valuation ring.

We will take the following notations:

Let $\overline{b}$ be a tuple. Then, $v(\overline{b})$ denotes the minimal valuation among the coordinates of $\overline{b}$. Given a system of analytic functions $f = (f_1, \cdots, f_n)$, by $f(\overline{b}) = 0$, we mean that $f_i(\overline{b}) = 0$ for all i. We take similar notations for congruence, multiplication of matrix by vectors, etc

We define the differential of an analytic map as usual by:

Definition 2.1.6. *Let $f : U \longrightarrow K^m$ where U is an open subset of K^n. Let $\overline{a}$ in U. We set $|\overline{a}|_p := \max\{|a_i|_p\}$. If there exists a linear map A between K^n and K^m such that*

$$\lim_{|\overline{h}|_p \to 0} \frac{|f(\overline{a}+\overline{h}) - f(\overline{a}) - A\overline{h}|_p}{|\overline{h}|_p} = 0,$$

then we say that f is differentiable at *$\overline{a}$ and we note $A = Df(\overline{x})$.*

Assume $f = (f_1, \cdots, f_m) : U \longrightarrow K^m$ differentiable at $\overline{a}$, the matrix associated to $Df(\overline{a})$ is the Jacobian matrix given by

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(\overline{a}) & \cdots & \frac{\partial f_1}{\partial x_n}(\overline{a}) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_1}(\overline{a}) & \cdots & \frac{\partial f_m}{\partial x_n}(\overline{a}) \end{pmatrix}.$$

Here is the extension of Hensel's lemma for systems of analytic functions:

Theorem 2.1.7 (Analytic Hensel's lemma)**.** *Let $f = (f_1, \cdots, f_t)$ be a system of elements in $\mathbb{Z}_p\{X_1, \cdots, X_t\}$. Let $J_f(\overline{X})$ denote the Jacobian matrix of the system. Assume that there is $\overline{a} \in \mathbb{Z}_p^t$ such that*

$$det\ J_f(\overline{a}) \neq 0 \text{ and } v(f(\overline{a})) > 2v(det\ J_f(\overline{a})) + r,$$

where r is any nonnegative integer. Then, there is a unique $\overline{b} \in \mathbb{Z}_p^n$ such that

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

As it seems that this version does not appear exactly in the litterature, we include a proof for the sake of completeness:

Proof. (1) If $v(\text{ det } J_f(\overline{a})) = 0$:

We will construct by induction a sequence $(\overline{b}_n)_{n\in\mathbb{N}}$ of tuple of integers such that each $\overline{b_n}$ is uniquely determined and:

(a) $f(\overline{b}_n) \equiv 0 \mod p^{n+r+1}$;

(b) $\overline{b}_n \equiv \overline{b}_{n-1} \mod p^{n+r}$;

(c) $0 \leq \overline{b}_n < p^{n+r+1}$.

Clearly, choosing $\overline{b}_0$ carefully, such a sequence admits a limit $\overline{b}$ with $f(\overline{b}) = 0$ and $v(\overline{b} - \overline{a}) > r$.

Let $\overline{b}_0$ be the unique element in $\{0, \cdots, p^{r+1} - 1\}^t$ such that $\overline{b}_0 \equiv \overline{a} \mod p^{r+1}$. Then, $f(\overline{b}_0) \equiv f(\overline{a}) \equiv 0 \mod p^{r+1}$: the initial conditions are satisfied.

Assume that we have defined $\overline{b}_0 \cdots, \overline{b}_n$. We want to find $\overline{b}_{n+1}$ satisfying the above conditions. By conditions (b) and (c), such an element has to be of the form: $\overline{b}_{n+1} = \overline{b}_n + \overline{c}p^{n+r+1}$ with $\overline{c} \in \{0, \ldots, p-1\}^t$. Consider the local Taylor expansion around $\overline{b}_n$:

$$\begin{aligned} f(\overline{b}_{n+1}) = f(\overline{b}_n + \overline{c}p^{n+r+1}) &= f(\overline{b}_n) + J_f(\overline{b}_n)\overline{c}p^{n+r+1} + p^{n+r+2}(...) \\ &\equiv f(\overline{b}_n) + J_f(\overline{b}_n)\overline{c}p^{n+r+1} \mod p^{n+r+2}, \end{aligned}$$

where $J_f(\overline{b}_n)\overline{c}$ denotes the product of matrices.

Indeed, as the f_i's have coefficients in $\mathbb{Z}_p$, for all α multi-index greater than 1, the valuation of the element $\frac{\partial^\alpha f_i}{\partial x^\alpha}(\overline{b}_n).\frac{1}{\alpha!}.(c_i p)^{\alpha.(n+r+1)}$ is at least $n+r+2$. In fact, the partial derivative and the factorial term correspond to the αth coefficient of f (which belongs to $\mathbb{Z}_p$) and the other part of the element has clearly valuation greater than $n+r+2$.

As $f(\overline{b}_n) \equiv 0 \mod p^{n+r+1}$, $f(\overline{b}_n) \equiv \overline{e}p^{n+r+1} \mod p^{n+r+2}$ for some $\overline{e} \in \{0,\dots,p-1\}^t$. Therefore, condition (a) would implies that:

$$f(\overline{b_{n+1}}) \equiv \overline{e}p^{n+r+1} + J_f(\overline{b}_n)\overline{c}p^{n+r+1} \equiv 0 \mod p^{n+r+2}$$

or equivalently

$$\overline{e} + J_f(\overline{b}_n)\overline{c} \equiv 0 \mod p.$$

But, $J_f(\overline{b}_n) \equiv J_f(\overline{b}_0) \equiv J_f(\overline{a}) \mod p$. So, det $J_f(\overline{b}_n) \not\equiv 0 \mod p$. Therefore, $J_f(\overline{b}_n) \mod p$ is invertible as a matrix with coefficients in $\mathbb{F}_p$. It means that $\overline{c}$ is uniquely determined by the above equation and the condition $\overline{c} \in \{0,\dots,p-1\}^t$. The first case is done.

(2) We will deduce the general case from the first:

From the Taylor expansion of f_i, we obtain the formal relation:

$$f_i(\overline{X}+\overline{Y}) = f_i(\overline{X}) + J_{f_i}(\overline{X})\overline{Y} + \sum_{j,k} g_{ijk}(\overline{X},\overline{Y})Y_jY_k.$$

Let V be an element of valuation $v(\det\ J_f(\overline{a}))$. In the above expression, we set $\overline{X} = \overline{a}$ and $\overline{Y} = V\overline{Z}$, i.e. we obtain the system

$$\begin{pmatrix} f_1(\overline{a}+V\overline{Z}) \\ \vdots \\ f_t(\overline{a}+V\overline{Z}) \end{pmatrix} = \begin{pmatrix} f_1(\overline{a}) \\ \vdots \\ f_t(\overline{a}) \end{pmatrix} + V \cdot J_f(\overline{a}) \cdot \overline{Z} + V^2 \begin{pmatrix} R_1(\overline{Z}) \\ \vdots \\ R_t(\overline{Z}) \end{pmatrix},$$

where $R_1,\cdots,R_n \in (\overline{Z})^2\mathbb{Z}_p\{\overline{Z}\}$. We define a new system $h = (h_1,\cdots,h_t) \in (\mathbb{Z}_p\{\overline{Z}\})^t$ by

$$\begin{pmatrix} h_1(\overline{Z}) \\ \vdots \\ h_t(\overline{Z}) \end{pmatrix} := V^{-1}J_f(\overline{a})^{-1} \cdot \begin{pmatrix} f_1(\overline{a}+V\overline{Z}) \\ \vdots \\ f_t(\overline{a}+V\overline{Z}) \end{pmatrix}$$

$$= \begin{pmatrix} c_1 \\ \vdots \\ c_t \end{pmatrix} + \overline{Z} + (\cdots)$$

where by hypothesis, $v(\overline{c}) > r$. So, we have that $v(h(\overline{0})) > r$ and $v(\det\ J_h(\overline{0})) = 0$. By the first case, there exists a unique $\overline{d}$ such that $h(\overline{d}) = 0$ and $v(\overline{d}) > r$. Let $\overline{b} = \overline{a} + V\overline{d}$. It is immediate from the above equations that $f(\overline{b}) = 0$ and $v(\overline{a} - \overline{b}) > v(V) + r = v(\det\ J_f(\overline{a})) + r$. The uniqueness of $\overline{b}$ is an immediate consequence of the uniqueness of $\overline{d}$.

This concludes the proof of the theorem. □

Corollary 2.1.8. *The same result holds for power series with coefficients in the valuation ring of K a finite algebraic extension of $\mathbb{Q}_p$.*

For this, we just have to replace in the proof of theorem 2.1.7 p by π_K and $\mathbb{F}_p$ by the residue field $\overline{K}$.

Let $f \in \mathcal{O}_K\{X\}$ nonzero. Then, the coefficients of f contain a lot of informations on the roots of f.

For instance, one can see that f has finitely many roots in $\mathcal{O}_K$:

Theorem 2.1.9 (Strassmann's theorem). *Let $f = \sum a_n X^n \in \mathcal{O}_K\{X\}$ nonzero. Let N be the largest index among the indexes i such that $|a_i| = \max_n |a_n|$. Then, f has at most N zeros in $\mathcal{O}_K$.*

We can actually say more:

Theorem 2.1.10 (Weierstrass preparation theorem). *Let $f = \sum a_n X^n \in \mathcal{O}_K\{X\}$ nonzero. Let N be the largest index among the indexes i such that $|a_i| = \max_n |a_n|$. Then, there exist $k \in \mathbb{N}$, a monic polynomial P of degree N and $h(X) \in \mathcal{O}_K\{X\}$ invertible (i.e. is in $1 + \pi_K \mathcal{O}_K\{\overline{X}\}$) such that*

$$f(X) = \pi_K^k P(X) h(X).$$

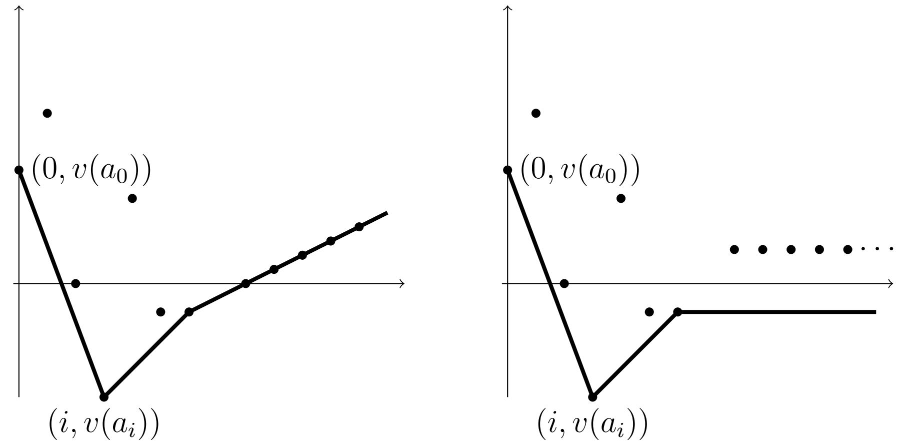
It implies that f has exactly N roots in $\mathcal{O}_p$ (counting multiplicities).

We can do better: the coefficients of f actually determine the valuation of the roots of f. For this, we need to introduce the notion of Newton polygons.

Let $f(x)$ be a power series with coefficients in $\mathcal{O}_p$. Assume that the coefficient of degree 0 is nonzero (if this not the case, divide by x^n for an suitable n). The

Newton polygon of a polynomial f is defined as the lower convex closure of $A := \{P_i = (i, v(a_i)) \mid i \in \mathbb{N}\}$. If $a_i = 0$, we consider P_i as a point to "infinity".

In general, the Newton polygon of f is obtained as follow: we consider the set of points A as above. Rotate the y-axis counterclockwise. If it hits a point $P_i \in A$, break the line and keep going. When the line hits infinitely many points in A (see figure 2.1 (a)) or when the line cannot continue to rotate without missing points in A (see figure 2.1 (b)), stop. The Newton polygon of f is the line obtained after this operation.



(a) The line hits infinitely many points.

(b) The line cannot rotate without missing points.

Figure 2.1: The Newton polygon of two series.

Theorem 2.1.11. *Let $f(X) = \sum a_i X^i \in K[[X]]$ be a power series such that $a_0 \neq 0$. Then,*

1. *Let λ be the least upper bound of all slopes of the Newton polygon, then the radius of convergence of f is p^λ (or all K if λ is not finite). Note that the series may only converge on the open ball of radius p^λ (and not on the closed ball)!*

2. *Let $(i, v(a_i))$ and $(j, v(a_j))$ be two consecutive points where the line breaks, then f has exactly $j - i$ roots of valuation $\frac{v(a_j)-v(a_i)}{i-j}$ in the algebraic closure of K (counting multiplicities).*

3. *If $f \in \mathcal{O}_K\{X\}$, let P be the polynomial given in the Weierstrass preparation theorem (say, this polynomial has degree N). Then, the Newton polygon of P coincides with the Newton polygon of f until the point of coordinates $(N, v(a_N))$.*

The goal of appendix A 'tropical analytic geometry' is to present a generalisation of this result to systems of restricted analytic functions with several variables.
To conclude this part, we give a generalisation of the Weirstrass preparation theorem to power series with several variables.

Definition 2.1.12. *Let $f \in \mathcal{O}_K\{\overline{X}, Y\}$. We say that f is* regular of order d in Y *if*

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

where $a_i(\overline{X}) \in \overline{K}[\overline{X}]$ and $\overline{f}$ denotes the image of f under the residue map.

Theorem 2.1.13. *Let $f \in \mathcal{O}_K\{\overline{X}, Y\}$ regular of order d in Y. Then,*

- *(Weierstrass division theorem) for every $g \in \mathcal{O}_K\{\overline{X}, Y\}$, there exist a (unique) $Q \in \mathcal{O}_K\{\overline{X}, Y\}$ and (unique) $A_0, \cdots, A_{d-1} \in \mathcal{O}_K\{\overline{X}\}$ such that*

$$g = Qf + (A_{d-1}Y^{d-1} + \cdots + A_0).$$

- *(Weierstrass preparation theorem) there exist a (unique) unit $U \in \mathcal{O}_K\{\overline{X}, Y\}$ and (unique) $A_0, \cdots, A_{d-1} \in \mathcal{O}_K\{\overline{X}\}$ such that*

$$f = U(Y^d + A_{d-1}Y^{d-1} + \cdots + A_0).$$

2.2 Model theory of the p-adic numbers

2.2.1 p-adically closed fields

In this text, we will consider the theory of the p-adic numbers in the language of valued rings

$$\mathcal{L}_v = (+, -, \cdot, 0, 1, V),$$

where V is a predicate for the valuation ring. We will not consider the case of multi-sorted languages like in [1].

A model of the theory of $\mathbb{Q}_p$ in the language $\mathcal{L}_v$ is called a p-adically closed field.

Definition 2.2.1. *We say that a valued field (K, v) is* p-adically closed *if it satisfies the following scheme of axioms:*

- *(K, v) is a valued field of characteristic zero;*
- *$v(K^*)$ is a $\mathbb{Z}$-group, i.e. is an abelian ordered group such that for all $n \in \mathbb{N}_0$, for all $x \in K^*$, there exists $y \in K^*$ such that $v(x) = nv(y) + i$ for some $0 \leq i < n$;*
- *$\overline{K} = \mathbb{F}_p$ and $v(p) = 1$;*
- *K is henselian.*

It should be clear how one can write the above properties in the language of valued fields. Indeed, the relation $v(x) \geq v(y)$ is equivalent to $xy^{-1} \in V$. So, for instance, the axiom $v(p) = 1$ can be written formally as

$$p \in V \wedge p^{-1} \notin V \wedge \big(\forall x (x \in V \wedge x^{-1} \notin V) \rightarrow xp^{-1} \in V\big) .$$

Note that the value group is not a definable group in our theory. However, it is interpretable because $v(K^*) \cong K^*/U$ where U is the set of elements in V with zero valuation. Similarly, the residue field is V/pV.

Clearly, $\mathbb{Q}_p$ is a p-adically closed field. Also, it is known since [1], that the above scheme of formulas axiomatizes a complete theory.

Note that in some texts, p-adically closed fields hold for models of the theory of a finite algebraic extension L of $\mathbb{Q}_p$. In this case, we need to replace the third axiom by $\overline{K} = \overline{L}$ and $v(p) = e$ (the ramification index of K over $\mathbb{Q}_p$).

The theory of p-adically closed fields is model-complete and decidable (see [1]) but does not admit quantifier elimination in the language of valued fields. We consider the following expansion of language:

$$\mathcal{L}_P = (+, -, \cdot, 0, 1, V, P_n; n \in \mathbb{N}_0),$$

where P_n are unary predicates interpreted in $\mathbb{Q}_p$ by

$$P_n(x) \equiv \exists y \; x = y^n$$

i.e. P_n is the group of nth powers (together with zero). We call $\mathcal{L}_P$ the *language of p-adically closed fields (or rings)*. Let us remark that the predicate V is not necessary in this language. Indeed,

$$\mathbb{Q}_p \models v(x) \geq 0 \leftrightarrow P_2(1 + px^2)$$

if $p \neq 2$ or

$$\mathbb{Q}_p \vDash v(x) \geq 0 \leftrightarrow P_3(1 + px^3)$$

if $p = 3$. It turns out that the groups of nth-powers are the only obstruction to quantifier elimination:

Theorem 2.2.2 (A. Macintyre [9]). *The theory $Th(\mathbb{Q}_p, +, -, \cdot, 0, 1, V, P_n)$ admits elimination of quantifiers.*

Let us remark that if K is a finite algebraic extension of $\mathbb{Q}_p$, then
$Th(K, +, -, \cdot, 0, 1, V, P_n)$ also admits elimination of quantifiers (see [13] for instance). Also, note that by decidability of the theory, the above quantifier elimination is effective: given a $\mathcal{L}_P$-formula, one can compute an equivalent quantifier-free $\mathcal{L}_P$-formula.

The goal of this thesis is to study the theory of $\mathbb{Z}_p$ in the language $\mathcal{L}_P$ expanded by a symbol for an exponential function. This language can be seen as a reduction of a well-known expansion of the language $\mathcal{L}_P$: the expansion by all restricted analytic functions. The model theory of $\mathbb{Z}_p$ in this language was first studied by J. Denef and L. van den Dries in [4].
We denote by $\mathcal{L}_{an}$ the language

$$\mathcal{L}_{an} := \mathcal{L}_P \cup \Big\{ f; f \in \mathbb{Z}_p\{X_1, \cdots, X_n\}, n \in \mathbb{N}_0 \Big\},$$

where $f \in \mathbb{Z}_p\{\overline{X}\}$ is interpreted in $\mathbb{Q}_p$ by

$$\begin{cases} f(\overline{x}) & \text{if } \overline{x} \in \mathbb{Z}_p^n \\ 0 & \text{otherwise .} \end{cases}$$

The theory of $\mathbb{Z}_p$ does not admit elimination of quantifier in this language. But it is the case for the expansion

$$\mathcal{L}_{an}^D := \mathcal{L}_{an} \cup \{D\}$$

where D is a binary function interpreted in $\mathbb{Q}_p$ by

$$D(x, y) = \begin{cases} xy^{-1} & \text{if } v(x) \geq v(y) \\ 0 & \text{otherwise.} \end{cases}$$

We denote by $\mathbb{Q}_{p,\mathrm{an}}$ (resp. $\mathbb{Z}_{p,an}$) the structure $(\mathbb{Q}_p, f\ (f \in \mathbb{Z}_p\{\overline{X}\}), D, P_n(n \in \mathbb{N}_0))$ (resp. $(\mathbb{Z}_p, f\ (f \in \mathbb{Z}_p\{\overline{X}\}), D, P_n(n \in \mathbb{N}_0))$). The main theorem of [4] is

Theorem 2.2.3 (J. Denef, L. van den Dries)**.** *$Th(\mathbb{Z}_{p,an})$ admits elimination of quantifiers.*

Note that once again this result can be extended to finite algebraic extensions. Also, this theory is the main (non-trivial) example of a P-minimal theory. This notion of P-minimality was introduced in [5] as an equivalent of o-minimality for the field of real numbers.

Definition 2.2.4. *Let $\mathcal{L}$ be an expansion of $\mathcal{L}_P$ and let $\mathcal{M}$ be an $\mathcal{L}$-structure. We say that $\mathcal{M} = (M, \cdots)$ is P-minimal if for all $\mathcal{M}' = (M', \cdots)$ elementary equivalent to $\mathcal{M}$, any definable subset of M' is quantifier-free definable by a $\mathcal{L}_P$-formula.*

It is proved in [6] that

Theorem 2.2.5 (D. Haskell, D. Macpherson, L. van den Dries)**.** *$\mathbb{Q}_{p,an}$ is P-mimimal.*

2.2.2 p-adic exponential rings

Finally, we introduce the structure that will be studied in this thesis: the p-adic exponential rings. We also give in this section some well-known properties of this structure.

As we have seen in section 2.1.2, there is no global analytic exponential function defined on $\mathbb{Q}_p$. The power series $exp(x) = \sum x^n/n!$ is only convergent for x such that $v(x) > 1/(p-1)$. Therefore, the function $x \longmapsto exp(px)$ is well-defined on $\mathbb{Z}_p$ (if $p \neq 2$). We call *p-adic exponential ring* a model of the theory of $\mathbb{Z}_p$ in the language of p-adically closed rings together with a function symbol E_p interpreted in $\mathbb{Z}_p$ by

$$E_p(x) = \begin{cases} exp(px) & \text{if } p \neq 2 \\ exp(p^2x) & \text{otherwise.} \end{cases}$$

We denote the language of this theory by $\mathcal{L}_{exp}$ and the structure $(\mathbb{Z}_p, +, \cdot, E_p, 0, 1, P_n)$ is denoted by $\mathbb{Z}_{p,exp}$. Note that in our proofs we will not discuss the case $p = 2$. Yet, our results remain true if $p = 2$. It should be obvious how one can extend our proofs to this case (usually, it is sufficient to replace p by 4).

Note also that this structure is an exponential ring in the sense of [15].

We will denote by $\mathbb{Z}_p[\overline{X}]^{E_p}$ the *ring of exponential polynomials* (or E_p-polynomials) as defined in [15]. As it will be useful later, let us recall the construction of this ring:

Let (R, E) be an exponential ring i.e. a commutative ring R with unity and a morphism E between $(R, +)$ and $(R^{\times}, \cdot)$. We want to define $R[\overline{X}]^E$ the ring of E-polynomials. We define by induction a ring R_k and an ideal A_k. We also define E_k a morphism of groups between the additive group of R_k and the group of units of R_{k+1}. If $k = -1$, we set $R_{-1} = R$. If $k = 0$, we set $R_0 = R[\overline{X}]$ and $A_0 = (X_1, \cdots, X_n)$. Then, $R_0 = R_{-1} \oplus A_0$ and we define E_{-1} as the composition $R \xrightarrow{E} R \hookrightarrow R_0$.

Assume that we have defined $E_{k-1}, R_{k-1}, R_k, A_k$ such that we have $R_k = R_{k-1} \oplus A_k$ and E_{k-1} is a morphism of groups between R_{k-1} and the group of units of R_k. Then, let $exp(A_k)$ be a multiplicative copy of $(A_k, +)$ (i.e. $exp(A_k)$ is a multiplicative group and we are given an isomorphism $exp : A_k \to exp(A_k)$). We set $R_{k+1} := R_k[exp(A_k)]$ and $A_{k+1} :=$ the R_k-submodule of R_{k+1} generated by the elements of the type $exp(a)$ for $a \in A_k \setminus \{0\}$. Finally, we define E_k: Let $x \in R_k$. Then, $x = x' + a$ for some $x' \in R_{k-1}$ and $a \in A_k$. We define $E_k(x) := E_{k-1}(x') \cdot exp(a)$.

We set

$$R[\overline{X}]^E := \varinjlim R_k.$$

Let us remark that the functions E_k determine an exponential map on $R[\overline{X}]^E$ (given by $E(x) = E_k(x)$ if $x \in R_k$).

Let $r \in R$. Then it is proved in [15] that there exists a unique derivation on $R[X]^E$, trivial on R such that $X' = 1$ and $E(Q)' = rQ'E(Q)$ for all $Q \in R[X]^E$. Note that this derivation maps R_k to itself.

Furthermore, we can define a degree on the elements of $R[X]^E$:

Let $P \in A_k$ (where $k > 0$). We can write $P(X)$ as $\sum_{i=1}^{h} r_i E_p(a_i)$ for some $a_1, \cdots, a_h$ distinct nonzero elements of A_{k-1}. Then, we set $t(P) := h$.

If $P \in R_0 = R[X]$, we put $t(P) = 0$ if $P = 0$ and $t(P) = d + 1$ where d is the degree of P as a polynomial otherwise.

Let $P \in R[X]^E$. Let us remark that we can uniquely decompose P as $P = P_0 + \cdots + P_s$ where $P_0 \in R_0$ and $P_i \in A_i$ for all $0 < i \leq s$. We can now define the degree of P (denoted $d(P)$) as the ordinal

$$d(P) := t(P_s)\omega^s + \cdots + t(P_1)\omega + t(P).$$

Note that $d(P) = 0$ iff $P = 0$. The following well-known lemma will be useful later:

Lemma 2.2.6. *Let $P \in R[X]^E$ nonzero. Then, there exists $Q \in R[X]^E$ such that $d(Q) < d(P)$ and $d((E(-Q)P)') < d(P)$ (where $'$ denotes a natural derivative like above).*

Proof. Let $P = P_0 + \cdots + P_s$ like above.

- If P_0 is nonzero, take $Q = 0$. Then,
$$d(Q) = 0 < d(P)$$
by definitions. And, as R_k is closed under $'$ for all k,
$$d(P_0') < d(P_0) \qquad \text{and} \qquad t(P_i') \leq t(P_i) \text{ for all } i > 0.$$
Note also that $P_i' \in A_i$. So, as $d(S) = \sum_i d(S_i)$ for all $S \in R[X]^E$,
$$d((E(-Q)P)') = d(P') < d(P).$$
- Otherwise, let $i > 0$ such that P_i is nonzero and $P_j = 0$ for all $j < i$. Let $P_i = \sum_{j \leq h} r_j E(a_j)$ like before. Take $Q = a_1$. Then,
$$d(Q) \leq \omega^{i-1} t(Q) < \omega^i \leq d(P).$$
And,
$$\begin{aligned} d((E(-a_i)P)') &= d\left(\left(r_1 + \sum_{j=2}^{h} r_j E(a_j - a_i) + \sum_{k=i+1}^{s} P_k\right)'\right) \\ &= d(r_1') + \sum_{j=2}^{h} d(r(r_j(a_j - a_i)' + r_j')E(a_j - a_i)) + \sum_{k=i+1}^{s} d(P_k') \\ &\leq t(r_1')\omega^{i-1} + (h-1)\omega^i + \sum_k t(P_k')\omega^k \\ &< d(P). \end{aligned}$$

□

The p-adic exponential rings were first introduced by A. Macintyre in [10]. Let us remark that in this paper, the author considers the function $(1+p)^x$ instead of E_p. As observed in this paper, our exponential ring is closed under derivation (in the sense of p-adic analysis). Therefore, proposition (4.1) of [15] holds for our ring: there is one-to-one correspondence between $\mathcal{L}_{exp}$-terms (the E_p-polynomials) and their interpretation in the model (the E_p-polynomial functions). Also (remark (4.6) of [15]),

Proposition 2.2.7. *Identities in the language $\mathcal{L}_{exp}$ which hold in $\mathbb{Z}_p$ are derivable from the axioms of E-rings and the positive diagram of $(\mathbb{Z}_p, E_p)$.*

The main question of this thesis is the following:

Problem 1. Is the theory of $\mathbb{Z}_{p,exp}$ decidable?

First, let us remark that we cannot expect to answer this question via quantifier elimination in the natural language:

Proposition 2.2.8. *In the language $\mathcal{L}_{exp}$, the theory of $\mathbb{Z}_{p,exp}$ does not admit quantifier elimination.*

The proof is the same that for the theory of $\mathbb{Z}_p$ in the language $\mathcal{L}_{an}$:

Proof. First, let us remark that the graph of D is a definable set in the language $\mathcal{L}_{exp}$: $D(x,y) = z$ iff $(v(x) \geq v(y) \wedge y \neq 0 \wedge x = z \cdot y) \vee ((v(x) < v(y) \vee y = 0) \wedge z = 0)$. We claim now that we cannot eliminate the quantifier in the formula:

$$\Psi(x,y,z) \equiv \exists t (D(x,y) = t \wedge z = yE_p(t)).$$

Let us remark that the definable set corresponding to the formula Ψ is given by the graph of the (definable) function

$$f(x,y) = \begin{cases} yE_p(x/y) & \text{if } v(x) \geq v(y) \text{ and } y \neq 0 \\ y & \text{otherwise.} \end{cases}$$

We denote by $\Gamma(f)$ this graph. We remark two important properties of this function:

1. f is not an *algebraic* function i.e. there is no polynomial $P(X,Y,Z)$ with coefficients in $\mathbb{Z}_p$ such that $P(x,y,f(x,y)) = 0$ for all $x, y \in \mathbb{Z}_p$.

2. For all $t \in \mathbb{Z}_p$, $f(tx,ty) = tf(x,y)$.

Consider $(F_1, \cdots, F_k)$, where F_i's are p-adic analytic functions from U (an open neighborhood of 0 in $\mathbb{Z}_p^3$) to $\mathbb{Z}_p$. If we show that $\Gamma(f) \cap U$ doesn't belong to the boolean algebra generated by sets of the types $\{F_i = 0\}$, $\{P_k(F_i)\}$ then we have finished because this algebra contains the collection of all sets definable by a quantifier-free formula in our language.

We argue by contradiction: suppose that $\Gamma(f) \cap U$ is a boolean combination of such sets.

Claim 1. *We can assume that for some i, F_i vanishes on $\Gamma(f) \cap U$.*

Proof. Otherwise, there is a c such that for all i, $F_i(c) \neq 0$. This means that we can find a subset of $\Gamma(f) \cap U$ defined by finite unions and intersections of sets of the form: $\{F_i \neq 0\}, \{P_k(F_i)\}$ and $\{\neg P_k(F_i)\}$. But all these sets contain an open ball in $\mathbb{Z}_p^3$:

- $\{F_i \neq 0\}$ is open.
- $\{P_k(F_i)\}$: $\{P_k(x)\} = \{P_k(x) \wedge x \neq 0\} \cup \{0\}$. The left part is open by Hensel's lemma. As F_i is continuous, $\{P_k(F_i)\}$ contains a open set.
- $\{\neg P_k(F_i)\}$: $\{\neg P_k(x)\} = \{P_k(x)\}^c = \{P_k(x) \wedge x \neq 0\}^c \cap \{x \neq 0\}$. The left part is open as a closed subgroup of $\mathbb{Z}_p^*$. The right part is the complement of a closed set.

So, $\Gamma(f) \cap U$ contains a open subset which gives a contradiction. □

Without loss of generality, we may assume that $i = 1$. We now write $F_1 = P_0 + P_1 + \cdots$ where P_r are homogeneous polynomials of degree r. As for all $t \in \mathbb{Z}_p$, $f(tx, ty) = tf(x, y)$, for all $x, y \in U$, we have:

$$0 = F_1(tx, ty, tz) = P_0(x, y, z) + tP_1(x, y, z) + t^2 P_2(x, y, z) + \cdots .$$

So, $P_r(X, Y, Z)$ vanishes on $\Gamma(f) \cap U$ for all r. Let r with $P_r \not\equiv 0$. Then, $P_r(x, y, f(x, y)) = 0$ for all $x, y \in \mathbb{Z}_p$. This gives a contradiction with the fact that f is not an algebraic function. □

An other approach to solve the decidability problem is to prove the effective model-completeness:

Problem 2. Is the theory of $\mathbb{Z}_{p,exp}$ model-complete?

We will answer to this question in chapter 3 and 4. We will see that in some nice expansion of our language the theory is effectively model-complete.

Chapter 5 will give a (conditional) solution to the problem of the decidability:

We will prove that one can determine the truth value of existential sentences in our expansion of the language $\mathcal{L}_{exp}$. Our proof relies on the p-adic Schanuel's conjecture. We obtain the decidability of the theory only under the condition that this conjecture is true.

Finally, let us remark that $\mathcal{L}_{exp}$ is a sublanguage of $\mathcal{L}_{an}$. Therefore, by theorem 2.2.5,

Corollary 2.2.9. *$\mathbb{Z}_{p,exp}$ is P-minimal.*

It means that all properties of P-minimal theories hold for $Th(\mathbb{Z}_{p,exp})$. For instance, our theory does not have the independence property.

Remark. Note that the function E_p is well-defined on $\mathcal{O}_K$ where K is any algebraic extension of $\mathbb{Q}_p$. Therefore, we may ask the same questions for the theory of $\mathcal{O}_K$ in the language of p-adic exponential ring. It turns out that our results can be generalised to any finite algebraic extension. We shall not discuss this case in details as it should be clear from the case $\mathbb{Z}_{p,exp}$ how one can prove the general case.

Chapter 3

Strong model-completeness

Let $\mathcal{L}_{an}$ be the expansion of the language of p-adically closed rings by all restricted analytic functions. In 1988, J. Denef and L. van den Dries showed in [4] that the theory of $\mathbb{Z}_p$ in this language expanded by a division symbol admits the elimination of quantifiers. Now, let F be any family of restricted analytic functions. We denote by $\mathcal{L}_F$ the language of p-adically closed rings expanded by symbols for elements of F. Let $\mathbb{Z}_{p,F}$ be the $\mathcal{L}_F$-structure with underlying set $\mathbb{Z}_p$ and natural interpretations for the symbols of the language. One may not expect anymore that the theory of $\mathbb{Z}_{p,F}$ admits quantifier elimination (even if we expand the language by the division symbol). However, in this chapter, we will show that under the assumption that the set of $\mathcal{L}_F$-terms is closed under derivation and *decomposition functions* (to be defined later), the theory of $\mathbb{Z}_{p,F}$ is strongly model-complete:

Definition 3.0.1. *Let $\mathcal{M}$ be a $\mathcal{L}$-structure with underlying set M. We say that $\mathcal{M}$ is* strongly model-complete *if for any $\mathcal{L}$-formula $\Psi(\overline{y})$, there is an existential $\mathcal{L}$-formula $\exists\overline{x}\Phi(\overline{x},\overline{y})$, where Φ is quantifier-free, such that for all $\overline{a} \in M^n$,*

$$\mathcal{M} \models \Psi(\overline{a}) \leftrightarrow \exists\overline{x}\Phi(\overline{x},\overline{a}),$$

and furthermore, for each $\overline{a}$ such that $M \models \Psi(\overline{a})$, there is a unique tuple $\overline{b}$ in M^m such that $M \models \Phi(\overline{b},\overline{a})$.

A set X is strongly definable *if*

$$X = \{\overline{a} \in M^n \mid \ \mathcal{M} \models \exists\overline{y}\Phi(\overline{a},\overline{b},\overline{y})\},$$

and, for each $\overline{a} \in X$, there is a unique tuple $\overline{c}$ in M^m such that $M \models \Phi(\overline{a},\overline{b},\overline{c})$. A *function is strongly definable if its graph and the complement of its domain are strongly definable.*

We will denote a formula of the type $\exists\overline{y}\Phi(\overline{x},\overline{y}) \wedge \forall\overline{z}\Big(\Phi(\overline{x},\overline{z}) \rightarrow \overline{z} = \overline{y}\Big)$ by $\exists!\overline{y}\Phi(\overline{x},\overline{y})$. Let us remark that a structure is strongly model-complete iff any formula is equivalent in this structure to a formula of the type $\exists!\overline{y}\Phi(\overline{x},\overline{y})$.
Also, note that any theory that admits elimination of quantifiers is strongly model-complete.

The proof of the main theorem of this chapter is due to A. Macintyre in the special case $F = \{E_p\}$ ([8], unpublished). We expand here the ideas of the proof to a more general family of functions. The case $F = \{E_p\}$ leads to some simplifications which will be discussed at the end of the next chapter.
Actually, the proof uses the same strategy that the main theorem of [16]. In this paper, L. van den Dries shows that the structure with underlying set $\mathbb{R}$ in the language of fields expanded by symbols for the functions exp, sin and cos (restricted to the interval $[0,1]$) is strongly model-complete. His proof relies on two main points:

First, we observe that in the proof of the quantifier elimination of $\mathbb{Z}_{p,an}$ in [4], we do not need all analytic functions. It is actually sufficient to consider a family closed under Weierstrass division (i.e. a Weierstrass system, to be defined later). We will recall this fact in the next section.

Second, L. van den Dries shows that the set of strong existential definable functions in his language forms a Weierstrass system. The central argument is that one can interpret the structure $(\mathbb{C}, +, \cdot, exp, \sin, \cos)$ (where the functions are restricted to the unit box). The proof does not work in the language of (restricted) exponential fields.

We adapt this strategy in the p-adic setting. In this case, we need to add functions so that the structure with underlying set V and natural interpretations for the symbols of $\mathcal{L}_F$ is definably interpretable (here V can be any valuation ring of a finite algebraic extension of $\mathbb{Q}_p$). We will develop this point in section 3.3. Finally, in section 3.4, we will prove that if the set of $\mathcal{L}_F$-terms is closed under derivation and if $\widetilde{F}$ denotes the expansion of F defined in section 3.3, then the theory of $\mathbb{Z}_{p,\widetilde{F}}$ is strongly model-complete.

3.1 Quantifier elimination and Weierstrass system

Definition 3.1.1. *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. *For all permutations σ of $\{1,\cdots,n\}$, if $f(\overline{X})\in\mathbb{Z}_p[\![\overline{X}]\!]$, then $f(X_{\sigma(1)},\cdots,X_{\sigma(n)})\in\mathbb{Z}_p[\![\overline{X}]\!]$;*
3. *If $f\in\mathbb{Z}_p[\![\overline{X}]\!]$ has an inverse g in $\mathbb{Z}_p\{\overline{X}\}$, then $g\in\mathbb{Z}_p[\![\overline{X}]\!]$;*
4. *Let $k\in\mathbb{Z}$. If $f\in\mathbb{Z}_p[\![\overline{X}]\!]$ is divisible by k in $\mathbb{Z}_p\{\overline{X}\}$, then $f/k\in\mathbb{Z}_p[\![\overline{X}]\!]$;*
5. *(Weierstrass division) If $f\in\mathbb{Z}_p[\![X_1,\cdots,X_{n+1}]\!]$ and f is regular of order d in X_{n+1}, then, for all $g\in\mathbb{Z}_p[\![X_1,\cdots,X_{n+1}]\!]$, there are $A_0,\cdots,A_{d-1}\in\mathbb{Z}_p[\![\overline{X'}]\!]$ (where $\overline{X'}=(X_1,\cdots,X_n)$)and $Q\in\mathbb{Z}_p[\![\overline{X}]\!]$ such that*

$$g(\overline{X})=Q(\overline{X})\cdot f(\overline{X})+\Big(X_{n+1}^{d-1}A_{d-1}(\overline{X'})+\cdots+A_0(\overline{X'})\Big).$$

It is well-known that

Lemma 3.1.2. *Let $(\mathbb{Z}_p[\![X_1,\cdots,X_n]\!])_n$ be a Weierstrass system. Then,*

(a) for all $f(\overline{X},\overline{Y})\in\mathbb{Z}_p[\![\overline{X},\overline{Y}]\!]$, for all $g_1,\cdots,g_m\in\mathbb{Z}_p[\![\overline{X}]\!]$, $f(\overline{X},g_1(\overline{X}),\cdots,g_m(\overline{X}))\in\mathbb{Z}_p[\![\overline{X}]\!]$;

(b) for all $f(\overline{X})\in\mathbb{Z}_p[\![\overline{X}]\!]$, for all i, $\frac{\partial f}{\partial X_i}(\overline{X})\in\mathbb{Z}_p[\![\overline{X}]\!]$.

Proof. (a) By Weierstrass division,

$$f(\overline{X},\overline{Y})=U_1(\overline{X},\overline{Y})(Y_1-g_1(\overline{X}))+R_1(\overline{X},Y_2,\cdots,Y_m),$$

where $R_1\in\mathbb{Z}_p[\![\overline{X},Y_2,\cdots,Y_m]\!]$. So, by induction,

$$f(\overline{X},\overline{Y})=U_1(\overline{X},\overline{Y})(Y_1-g_1(\overline{X}))+\cdots+U_m(\overline{X},\overline{Y})(Y_m-g_m(\overline{X}))+R_m(\overline{X}),$$

where $R_m\in\mathbb{Z}_p[\![\overline{X}]\!]$. And, clearly, $f(\overline{X},g_1(\overline{X}),\cdots,g_m(\overline{X}))=R_m(\overline{X})$.

(b) We may assume $i = 1$. By Weierstrass division,

$$f(X_1 + H, X_2, \cdots, X_n) - f(\overline{X}) = U(\overline{X}, H)H^2 + R_1(\overline{X})H + R_0(\overline{X}),$$

where $R_0, R_1 \in \mathbb{Z}_p[\![\overline{X}]\!]$. It is not hard to see that $R_0 = 0$ and $R_1 = \frac{\partial f}{\partial X_1}(\overline{X})$.

□

Actually, $(\mathbb{Z}_p[\![X_1, \cdots, X_n]\!])_n$ contains all the analytic functions that we need to carry on the proof of the quantifier elimination in [4]. The crucial construction of the proof is the following:
Given $f(\overline{X}, \overline{Y}) = \sum a_I(\overline{X})\overline{Y}^I \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}$, there exists $\widetilde{f} \in \mathbb{Z}_p\{\overline{X}, \overline{V}, \overline{Y}\}$ such that

- for all $\overline{x}, \overline{v}(\overline{x}) \subset \mathbb{Z}_p$ which satisfy a first-order condition (depending on f only),

$$f(\overline{x}, \overline{Y}) = a_I(\overline{x})\widetilde{f}(\overline{x}, \overline{v}(\overline{x}), \overline{Y}).$$

- $\widetilde{f}(\overline{X}, \overline{V}, \overline{Y})$ is preregular of order I.

Definition 3.1.3. *Let $f(\overline{X}) = \sum a_I\overline{X}^I \in \mathbb{Z}_p\{\overline{X}\}$. We say that f is* preregular of order I *if $|a_I| = 1$ and $|a_J| < 1$ for all $J > I$ (we use the lexicographical order). We say that f is* preregular *if it is preregular of some order.*

It is well known that

Lemma 3.1.4. *Let $f(\overline{X}) = \sum a_I\overline{X}^I \in \mathbb{Z}_p\{\overline{X}\}$ preregular of order I. Then, there exists an automorphism $T : \mathbb{Z}_p\{\overline{X}\} \longrightarrow \mathbb{Z}_p\{\overline{Z}\}$ such that $T(f)$ is regular in Z_n*

Actually, the automorphism T is a composition of a permutation of the variables and of a function of the type:

$$\begin{cases} X_i & \longmapsto Z_i - Z_n^{e_i} \quad \text{if } i < n, \\ X_n & \longmapsto Z_n. \end{cases}$$

So, in particular, if $f \in \mathbb{Z}_p[\![\overline{X}]\!]$, then $T(f) \in \mathbb{Z}_p[\![\overline{Z}]\!]$. Also,

Lemma 3.1.5. *Let $f(\overline{X}, \overline{Y}) = \sum a_I(\overline{X})\overline{Y}^I \in \mathbb{Z}_p[\![\overline{X}, \overline{Y}]\!]$. Then, the above function $\widetilde{f}$ belongs to $\mathbb{Z}_p[\![\overline{X}, \overline{V}, \overline{Y}]\!]$.*

Proof. First, we recall the construction of the function $\widetilde{f}$:

Let $\overline{x} \in \mathbb{Z}_p^k$. Assume that the following formula is satisfied in $\mathbb{Z}_p$:

$$\mu_I(\overline{x}) \equiv \Big(a_I(\overline{x}) \neq 0\Big) \wedge \bigwedge_{J<I} \Big(|a_J(\overline{x})| \leq |a_I(\overline{x})|\Big) \wedge \bigwedge_{\substack{I<J\\|J|<d}} \Big(|a_J(\overline{x})| < |a_I(\overline{x})|\Big),$$

where $I \in \mathbb{N}^n$, $|I| = i_1 + \cdots + i_n$ and d is like in the following lemma:

Lemma 3.1.6 (lemma 1.4 in [4]). *Let $f(\overline{X},\overline{Y}) = \sum a_I(\overline{X})\overline{Y}^I \in \mathbb{Z}_p\{\overline{X},\overline{Y}\}$. Then, there is $d \in \mathbb{N}$ such that for all I with $|I| \geq d$,*

$$a_I(\overline{X}) = \sum_{|J|<d} b_{IJ}(\overline{X})a_J(\overline{X}),$$

where $b_{IJ} \in \mathbb{Z}_p\{\overline{X}\}$ with $\|b_{IJ}\| < 1$.

Then, assuming that $\mathbb{Z}_p \vDash \mu_I(\overline{x})$, $a_I(\overline{x})^{-1}f(\overline{x},\overline{Y})$ is preregular of order I and

$$\begin{aligned} a_I^{-1}(\overline{x})f(\overline{x},\overline{Y}) = &\sum_{J<I} \Big(a_J(\overline{x})/a_I(\overline{x})\Big)\overline{Y}^J + \overline{Y}^I + \sum_{I<J,|J|<d} \Big(a_J(\overline{x})/a_I(\overline{x})\Big)\overline{Y}^J \\ &+ \sum_{|K|\geq d} \Big\{ \sum_{J<I} \Big(a_J(\overline{x})/a_I(\overline{x})\Big) b_{KJ}(\overline{x}) + b_{KI}(\overline{x}) \\ &+ \sum_{I<J,|J|<d} b_{KJ}(\overline{x}) \Big(a_J(\overline{x})/a_I(\overline{x})\Big) \Big\}\overline{Y}^K. \end{aligned}$$

We define:

$$\begin{aligned} \widetilde{f}(\overline{X},\overline{V},\overline{Y}) = &\sum_{J<I} V_J\overline{Y}^J + \overline{Y}^I + \sum_{I<J,|J|<d} pV_J\overline{Y}^J \\ &+ \sum_{|K|\geq d} \left(\sum_{J<I} V_J b_{KJ}(\overline{X}) + b_{KI}(\overline{X}) + \sum_{I<J,|J|<d} pV_J b_{KJ}(\overline{X}) \right) \overline{Y}^K. \end{aligned}$$

Then, $\widetilde{f}(\overline{X},\overline{V},\overline{Y})$ is preregular of order I and for all $\overline{x}$ such that $\mu_I(\overline{x})$ holds and for

$$v_J(\overline{x}) := \begin{cases} a_J(\overline{x})/a_I(\overline{x}) & \text{if } J < I \\ a_J(\overline{x})/pa_I(\overline{x}) & \text{otherwise,} \end{cases}$$

we have

$$f(\overline{x},\overline{Y}) = a_I(\overline{x})\widetilde{f}(\overline{x},\overline{v}(\overline{x}),\overline{Y}).$$

Now, we have to prove that $\widetilde{f} \in \mathbb{Z}_p[\![\overline{X},\overline{V},\overline{Y}]\!]$.

For all $|J| < d$, we define:

$$f_J(\overline{X},\overline{Y}) = \sum_{|K|\geq d} b_{KJ}(\overline{X})\overline{Y}^K.$$

Then,

$$f(\overline{X},\overline{Y}) = \sum_{|J|<d} a_J(\overline{X})\overline{Y}^J + \sum_{|J|<d} a_J(\overline{X}) f_J(\overline{X},\overline{Y})$$

and

$$\widetilde{f}(\overline{X},\overline{V},\overline{Y}) = \sum_{J<I} V_J(\overline{Y}^J + f_J(\overline{X},\overline{Y})) + \overline{Y}^I + f_I(\overline{X},\overline{Y}) + \sum_{I<J,|J|<d} pV_J(\overline{Y}^J + f_J(\overline{X},\overline{Y})).$$

So, as a Weierstrass system is closed under derivation and composition, if $f_J(\overline{X},\overline{Y}) \in \mathbb{Z}_p[\![\overline{X},\overline{Y}]\!]$ for all J, we are done.

Let $g(\overline{X},\overline{Y}) := f(\overline{X},\overline{Y}) - \sum_{|J|<d} a_J(\overline{X})\overline{Y}$. Let us remark that $g \in \mathbb{Z}_p[\![\overline{X},\overline{Y}]\!]$.

Let $\{I_1, \cdots, I_k\}$ be an enumeration of all $|J| < d$. By induction on k, we will define (uniquely determined) functions $U_1, \cdots, U_k, R_k \in \mathbb{Z}_p[\![\overline{X},\overline{Y}]\!]$ such that

$$g = a_{I_1}U_1 + \cdots + a_{I_k}U_k + R_k.$$

Let I be an index such that $\|a_I(\overline{X})\| = \max_{|J|<d}\{\|a_J(\overline{X})\|\}$. Without loss of generality, we can assume that $I_1 = I$. Let $t \in \mathbb{N}$ such that $p^{-t} = \|a_I(\overline{X})\|$. Then, $p^{-t}g, p^{-t}a_J(\overline{X}) \in \mathbb{Z}_p[\![\overline{X},\overline{Y}]\!]$ for all J and a_{I_1} is preregular. So, there exists an automorphism T_1 like in lemma 3.1.4 such that $T_1(p^{-t}a_{I_1}(\overline{X}))$ is regular in Z_n. So, by the Weierstrass division theorem, there exists a unique $U'_1(\overline{Z},\overline{Y}) \in \mathbb{Z}_p[\![\overline{Z},\overline{Y}]\!]$ and a unique $R'_1 \in \mathbb{Z}_p[\![\overline{Z},\overline{Y}]\!]$ (polynomial in Z_n) such that

$$T_1(p^{-t}g) = U'_1 T_1(p^{-t}a_{I_1}(\overline{X})) + R'_1.$$

So, if we apply T_1^{-1} and multiply by p^t the above equality, we obtain (unique) $U_1, R_1 \in \mathbb{Z}_p[\![\overline{X},\overline{Y}]\!]$ such that

$$g(\overline{X},\overline{Y}) = a_{I_1}(\overline{X})U_1(\overline{X}) + R_1(\overline{X},\overline{Y})$$

where $T_1(p^{-t}R_1)$ is polynomial in Z_n.

We carry on by induction with $\widetilde{g} := g - a_{I_1}U_1$ and we obtain $U_2 \cdots, U_k, R_k \in \mathbb{Z}_p[\![\overline{Z},\overline{Y}]\!]$ with the required properties and such that for some automorphism T, $T(R_k)$ is polynomial in Z_n.

But, as

$$g = a_{I_1}f_{I_1} + \cdots + a_{I_k}f_{I_k} + 0,$$

by uniqueness (note that the functions are actually unique in $\mathbb{Z}_p\{\overline{X},\overline{Y}\}$), $U_i = f_{I_i}$ and therefore $f_{I_i} \in \mathbb{Z}_p[\![\overline{X},\overline{Y}]\!]$. □

Now, it should be clear how we can adapt the proof of the elimination in [4] to prove quantifier elimination in the following language:

Fix a Weierstrass system $W = (\mathbb{Z}_p[\![X_1, \cdots, X_n]\!])_{n\in\mathbb{N}}$. Let $\mathcal{L}_W^D$ be the extension of the language $(+, -, \cdot, 0, 1, P_n; n \in \mathbb{N})$ by symbols f for each $f \in \mathbb{Z}_p[\![X_1, \cdots, X_n]\!]$ and D, a division symbol, interpreted in $\mathbb{Z}_p$ by:

$$D(x, y) = \begin{cases} x/y & \text{if } v(x) \geq v(y) \text{ and } y \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Let $\mathbb{Z}_{p,W}$ be the structure with underlying set $\mathbb{Z}_p$ and natural interpretations for the symbol of $\mathcal{L}_W^D$. Then, it is straightforward from [4] that

Proposition 3.1.7. *The theory $\mathbb{Z}_{p,W}$ admits elimination of quantifiers in $\mathcal{L}_W^D$.*

Note that the graph of the function D is strongly definable in $\mathcal{L}_W$. So, as an immediate corollary of the above proposition, we have

Corollary 3.1.8. *The theory $\mathbb{Z}_{p,W}$ is strongly model-complete in $\mathcal{L}_W$.*

3.2 Weiestrass system generated by a family of functions

Let F be a a family of restricted analytic functions. As before, we denote by $\mathcal{L}_F$ the expansion of the language of p-adically closed rings by the elements of F.
Surely, if W is a Weierstrass system that contains F, the theory of $\mathbb{Z}_p$ eliminates the quantifiers in the language $\mathcal{L}_W^D$. However, it may be hard to give an explicit description of the functions in W. In this section, we will define W_F, the Weierstrass system generated by the $\mathcal{L}_F$-terms. The construction of this system gives us a control on the functions in W_F. In particular, for all $f \in W_F$, there exists a finite collection of functions $f_1, \cdots, f_k \in F$ from which one can construct f using polynomial combinations, Weiestrass divisions, permutations of the variables and inverses. Using this system, we will obtain a result of strong model-completeness: we will see that any function in W_F is actually strongly definable (under some assumptions on F). Furthermore, in the next chapter, we will see that under further conditions on F the model-completeness

is actually effective.

We define *the Weierstrass system generated by the $\mathcal{L}_F$-terms* by:
For each n, let $W_{F,n}^{(0)}$ be the set of $\mathcal{L}_F$-terms with n variables.
We define $W_{F,n}^{(m+1)}$ by induction on m. Assume that we have defined $W_{F,n}^{(k)}$ for each $n \in \mathbb{N}$ and for each $k \leq m$. Then, $W_{F,n}^{(m+1)}$ is the ring generated by:

(a) $W_{F,n}^{(m)} \subset W_{F,n}^{(m+1)}$;

(b) For all $f \in W_{F,n}^{(m)}$, for all permutations σ, $f(X_{\sigma(1)}, \cdots, X_{\sigma(n)}) \in W_{F,n}^{(m+1)}$;

(c) For all $f \in W_{F,n}^{(m)}$, if f is invertible in $\mathbb{Z}_p\{\overline{X}\}$, then $f^{-1} \in W_{F,n}^{(m+1)}$;

(d) For all $f \in W_{F,n}^{(m)}$ and for all $k \in \mathbb{Z}$, if f is divisible by k in $\mathbb{Z}_p\{\overline{X}\}$, then $f/k \in W_{F,n}^{(m+1)}$;

(e) For each $f \in W_{F,n+1}^{(m)}$ of order d in X_{n+1}, for each $g \in W_{F,n+1}^{(m)}$, the functions $A_0, \cdots, A_{d-1} \in \mathbb{Z}_p\{X_1, \cdots, X_n\}$ and $Q \in \mathbb{Z}_p\{X_1, \cdots, X_{n+1}\}$ given by the Weierstrass division and their partial derivatives belong to $W_{F,n}^{(m+1)}$ and $W_{F,n+1}^{(m+1)}$ respectively.

Let $W_{F,n} := \bigcup_m W_{F,n}^{(m)}$. It is clear that these sets determine a Weierstrass system over $\mathbb{Z}_p$. We denote this system by W_F. Then, by proposition 3.1.7, the theory of $\mathbb{Z}_{p,W_F}$ admits elimination of quantifiers in $\mathcal{L}_{W_F}^D$. We will show that each function of W_F is strongly definable in $\mathcal{L}_F$ (under extra assumptions on F).
Also, note that by definition, for all $f \in W_{F,n}^{(m+1)}$, there exists, $g_1, \cdots, g_k \in W_{F,n+1}^{(m)}$ such that f is obtained from $g_1, \cdots, g_k$ using one of the above operations and polynomial combinations. We denote this property by $f \in \langle g_1, \cdots, g_k \rangle$. Now, it is clear that there exist $\mathcal{L}_F$-terms $f_1, \cdots, f_k$ such that $f \in \langle f_1, \cdots, f_k \rangle$. Indeed, by induction, we find a (finite) collection of functions $g_{0,1}, \cdots, g_{m,k_m}$ such that for all i, j, $g_{i,j} \in W_{F,s(i,j)}^{(i)}$ and $g_{i+1,j} \in \langle g_{i,1}, \cdots, g_{i,k_i} \rangle$. As, $W_{F,n}^{(0)}$ is, by definition, the set of $\mathcal{L}_F$-terms with n variables, we have that $f \in \langle f_1, \cdots, f_k \rangle$ for some $\mathcal{L}_F$-terms $f_1, \cdots, f_k$.
Furthermore,

Lemma 3.2.1. *Let $\Psi(\overline{X}) \equiv \exists Y_1, \cdots, Y_n \phi(\overline{X}, \overline{Y})$ be a $\mathcal{L}_F$-formula where ϕ is quantifier-free. Then, there exists ϕ' a $\mathcal{L}_{W_F}^D$-formula such that*

$$\mathbb{Z}_p \models \forall \overline{X} \Big(\Psi(\overline{X}) \leftrightarrow \exists Z_1, \cdots, Z_{n-1} \phi'(\overline{X}, \overline{Z}) \Big).$$

Furthermore, for any subterm f in ϕ' (not involving D), there exists a subterm g in ϕ and $P_1, \cdots, P_m$ polynomials with coefficients in $\mathbb{Z}$ such that $f \in \langle g, P_1, \cdots, P_m \rangle$

This follows immediately from the proof of proposition 3.1.7. Furthermore, by induction, there exists a quantifier-free $\mathcal{L}^D_{W_F}$-formula $\varphi(\overline{X})$ equivalent to Ψ such that for any term f in φ, $f \in \langle g_1, \cdots, g_l, P_1, \cdots, P_s \rangle$ where $g_1, \cdots, g_l$ are the $\mathcal{L}_F$-terms in Ψ and $P_1, \cdots, P_s$ are polynomials with coefficients in $\mathbb{Z}$.

3.3 Interpretation of finite algebraic extensions

Let F be a family of restricted analytic functions and W_F be the Weierstrass system generated by the $\mathcal{L}_F$-terms. The goal for the rest of this chapter is to prove that the functions in W_F are strongly existentially definable in $\mathcal{L}_F$.

First, we illustrate the main idea of the existential definition on a simple example:

Let f be a $\mathcal{L}_F$-term of order d in X_{n+1}. Then, by the Weierstrass preparation theorem, there are $A_0, \cdots, A_{d-1} \in W^{(1)}_{F,n}$ and a unit $U \in W^{(1)}_{F,n+1}$ such that:

$$f(X_1, \cdots, X_{n+1}) = \left[X^d_{n+1} + A_{d-1}(\overline{X'})X^{d-1}_{n+1} + \cdots + A_0(\overline{X'})\right] \cdot U(\overline{X}),$$

where $\overline{X'} = (X_1, \cdots, X_n)$. We want to give an existential definition of the functions $A_0, \cdots, A_{d-1}, U$.

Fix $\overline{x'} = (x_1, \cdots, x_n) \in \mathbb{Z}_p^n$. It is rather clear that $U(\overline{x'}, X)$ is strongly definable in terms of f and $A_0(\overline{x'}), \cdots, A_{d-1}(\overline{x'})$. We will give the explicit definition of the graph of U later and focus now on the definition of the coefficients A_i.

Let $\alpha_1, \cdots, \alpha_d$ be the roots of $P(X) := \sum A_i(\overline{x'})X^i + X^d$ in $\widetilde{\mathbb{Q}_p}$ (note that these are exactly the roots of $f(\overline{x'}, X)$ in $\widetilde{\mathbb{Q}_p}$ with nonnegative valuation). Then, the coefficients $A_i(\overline{x'})$ are uniquely determined by $\alpha_1, \cdots, \alpha_d$. For instance, if the roots are non-singular (i.e. if $\alpha_i \neq \alpha_j$ for all $i \neq j$), the coefficients $A_i(\overline{x'})$ are uniquely determined by the system:

$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \cdot \begin{pmatrix} A_0(\overline{x'}) \\ \vdots \\ A_{d-1}(\overline{x'}) \end{pmatrix} = \begin{pmatrix} \alpha_1^d \\ \vdots \\ \alpha_d^d \end{pmatrix}.$$

Other systems determine the coefficients in the case where the roots are singular (we will give these definitions later). The above relation leads to an existential formula which determines the graphs of the functions A_i. However, the existential quantifiers in this formula quantify over elements in $\widetilde{\mathbb{Q}_p}$ (the α_i's). We want a definition in $\mathbb{Z}_p$. In order to obtain such a definition, we first show that we can actually quantify over a finite algebraic extension of $\mathbb{Q}_p$ (which depends only on f). Then, we will see how one can interpret such an extension in $\mathbb{Z}_p$.

It is well known that the p-adic field $\mathbb{Q}_p$ has finitely many algebraic extensions of a given degree (see proposition 2.1.4). So, we can construct a sequence of finite algebraic extensions $K_1 \subseteq K_2 \subseteq \cdots$ such that:

- K_n is the splitting field of $Q_n(X)$ polynomial of degree N_n with coefficients in $\mathbb{Q}$;
- $K_n = \mathbb{Q}_p(\beta_n)$ and $V_n := \mathcal{O}_{K_n} = \mathbb{Z}_p(\beta_n)$ for all β_n root of Q_n;
- any extension of degree n is contained in K_n.

Let us remark that for any choice of $\overline{x'} \in \mathbb{Z}_p^n$, $\alpha_1, \cdots, \alpha_d \in K_d$. Also, it is well-known that the structure of ring is interpretable in $\mathbb{Z}_p$:

Lemma 3.3.1. *For all d, the structure* $(V_d, +, \cdot, 0, 1, P_n; n \in \mathbb{N})$ *is existentially definably interpretable in* $(\mathbb{Z}_p, +, \cdot, 0, 1, P_n; n \in \mathbb{N})$.

Proof. For this, we identify V_d with its structure of $\mathbb{Z}_p$-module. Let Q be the minimal polynomial of β_d over $\mathbb{Q}_p$. We know that this polynomial have coefficients in $\mathbb{Q}$ (with nonnegative valuation). Let D be the degree of Q. Then, V_d is isomorphic to $\mathbb{Z}_p^D$ where the addition is the addition componentwise and the multiplication is defined by

$$(x_1, \cdots, x_D) \cdot_{V_d} (y_1, \cdots, y_D) = \left(\sum_{1 \le i,j \le D} x_i y_j t_{ij1}, \cdots, \sum_{1 \le i,j \le D} x_i y_j t_{ijD} \right),$$

where the $t_{ijk} \in \mathbb{Q} \cap \mathbb{Z}_p$ are determined by

$$\beta_d^{i+j} = \sum_k t_{ijk} \beta_d^k.$$

□

Let $f \in F$. Then, f defines an analytic function on V_d. So, we can consider the structure $(V_d, +, \cdot, 0, 1, P_n \ (n \in \mathbb{N}), f; f \in F)$. We want that this structure is existentially definably interpretable in $\mathbb{Z}_{p,F}$. In general, this does not seem to be the case. So, we will add function symbols in our language so that the latter structure is interpretable in our expansion of language. For this, it is actually sufficient to describe the decomposition of f in the basis of V_d over $\mathbb{Z}_p$. Fix $f \in F$ and $y = \sum y_i \beta_d^i \in V_d^k$ (where $y_i \in \mathbb{Z}_p^k$). We decompose $f(y)$ in the basis of V_d over $\mathbb{Z}_p$:

$$f(y) = f\left(\sum y_i \beta_d^i\right) = c_{0,f,d}(\overline{y}) + c_{1,f,d}(\overline{y})\beta_d + \cdots + c_{N_d-1,f,d}(\overline{y})\beta_d^{N_d-1},$$

where $\overline{y} = (y_1, \cdots, y_{N_d})$. It determines functions $c_{i,f,d}$ from $\mathbb{Z}_p^{kN_d}$ to $\mathbb{Z}_p$. We call these functions *the decomposition functions of f in K_d*. Note that these functions are independent of the choice of β_d. Indeed, for all σ in the Galois group of K_d over $\mathbb{Q}_p$ (denoted by $Gal(K_d/\mathbb{Q}_p)$),

$$f(y^\sigma) = f\left(\sum y_i \beta_d^{\sigma i}\right) = c_{0,f,d}(\overline{y}) + c_{1,f,d}(\overline{y})\beta_d^\sigma + \cdots + c_{N_d-1,f,d}(\overline{y})\beta_n^{\sigma N_d-1},$$

by continuity of σ. Let $\widetilde{F} := F \cup \{c_{i,f,d} \mid \ f \in F, \ d \in \mathbb{N} \text{ and } i \leq N_d\}$. Then, by definition,

Lemma 3.3.2. *For all d, the structure $(V_d, +, \cdot, 0, 1, P_n \ (n \in \mathbb{N}), f; f \in F)$ is existentially definably interpretable in $\mathbb{Z}_{p,\widetilde{F}}$.*

One may wonder if we need to add more functions to interpret the structure $(V_d, +, \cdot, 0, 1, P_n \ (n \in \mathbb{N}), f; f \in \widetilde{F})$ in $\mathbb{Z}_{p,\widetilde{F}}$. However this is not the case. Indeed, let us remark that the $c_{i,f,d}(\overline{y})$ are linear combinations of the $f(y^\sigma)$:

$$\begin{pmatrix} c_{0,f,d}(\overline{y}) \\ \vdots \\ c_{N_d-1,f,d}(\overline{y}) \end{pmatrix} = V^{-1} \begin{pmatrix} f(y^{\sigma_1}) \\ \vdots \\ f(y^{\sigma_{N_d}}) \end{pmatrix},$$

where V is the Vandermonde matrix of the roots of Q_d and σ_i are the elements of $Gal(K_d/\mathbb{Q}_p)$. So, as power series,

$$c_{i,f,d}(\overline{y}) = \sum a_i \beta_d^i f\left(\sum R_i(\overline{y})\beta_d^i\right),$$

where $a_i \in \mathbb{Q} \cap \mathbb{Z}_p$ and R_i is a polynomial with coefficients in $\mathbb{Z}_p \cap \mathbb{Q}$. Therefore, the above relation holds for all $\overline{y} \in V_l^{kN_d}$. So,

Proposition 3.3.3. *For all d, the structure $(V_d, +, \cdot, 0, 1, P_n \ (n \in \mathbb{N}), f; f \in \widetilde{F})$ is existentially definably interpretable in $\mathbb{Z}_{p,\widetilde{F}}$.*

To conclude this section, we observe that if the set of $\mathcal{L}_F$-terms is closed under derivation, so is the set of $\mathcal{L}_{\widetilde{F}}$-terms. This follows immediately from the above equalities.

3.4 Existential definition of the $\mathcal{L}_{W_{\widetilde{F}}}$-terms

Now that we can interpret finite algebraic extensions in our structure, we are able to formalise the existential definition given at the beginning of section 3.3. Let us remark that in order to get the existential definitions, we will need to express that a function has a root of higher multiplicity. For this, we use the partial derivatives of the function. That is why we assume that the set of $\mathcal{L}_F$-terms is closed under derivation in the next proposition.

Proposition 3.4.1. *Let F be a family of functions in $\mathbb{Z}_p\{\overline{X}\}$. Assume that the set of $\mathcal{L}_F$-terms is closed under derivation. Let $\widetilde{F}$ be the extension of F by the decomposition functions in K_d of each $f \in F$ (for all $d \in \mathbb{N}$). Let $g \in W_{\widetilde{F}}$. Then,*

- *g is strongly definable in $\mathcal{L}_{\widetilde{F}}$.*
- *For all d, the structure (V_d, g) is (strongly definably) interpretable in $\mathbb{Z}_{p,\widetilde{F}}$.*

Given a function $f \in \mathbb{Z}_p\{X_1, \cdots, X_n\}$, we denote the set $\left\{\frac{\partial^k f}{\partial X_i^k}; 1 \leq i \leq n, k \in \mathbb{N}\right\}$ by $[f]$.

Proof. The proof is very similar to the corresponding results in [16]. The definitions given in the below claims are roughly the same that in the real case.
Recall that for all $f \in W^{(m+1)}_{\widetilde{F},n}$, there exist $g_1, \cdots, g_k \in W^{(m)}_{\widetilde{F},n+1}$ such that $f \in \langle g_1, \cdots, g_k\rangle$. So, it is sufficient to prove by induction on m that

1. For all $f \in W^{(m+1)}_{\widetilde{F},n}$, f and its derivatives are strongly definable in terms of functions in $W^{(m)}_{\widetilde{F},n+1}$ (and their derivatives);
2. The definitions remain true uniformly over the algebraic extensions V_d i.e. the graphs of the extension $f : V_d^k \to V_d$ and of its derivatives are strongly definably interpretable in terms of functions in $W^{(m)}_{\widetilde{F},n+1}$ (and their derivatives).

By definition of the language $\mathcal{L}_{\widetilde{F}}$ and by proposition 3.3.3, it is clear that the extensions of the functions in $W^{(0)}_{\widetilde{F},n}$ to V_d are interpretable. So, we assume by induction that the graph of the extension to V_d of any function in $W^{(k)}_{\widetilde{F},n}$ (or one of its derivative) is strongly definably interpretable in our structure for all d, for all n and for all $k \leq m$.

Let $f \in W^{(m+1)}_{\widetilde{F},n}$. Then, $f = P(f_1, \cdots, f_k)$ where $P \in \mathbb{Z}[\overline{Y}]$ and $f_1, \cdots, f_k$ are functions of the type (a)-(e) in the definition of Weierstrass system generated by the $\mathcal{L}_F$-terms. If the functions $f_1, \cdots, f_k$ satisfy properties 1. and 2., then f also satisfies these properties. Indeed, the graph of f is strongly definable in terms of $f_1, \cdots, f_k$ as $(\overline{x}, y)$ is a point of the graph of f iff

$$\mathbb{Z}_p \models \exists t_1 \cdots \exists t_k \bigwedge t_i = f_i(\overline{x}) \wedge y = P(t_1, \cdots, t_k).$$

So, we can assume that f is a function of the type (a)-(e).

The cases where f is obtained as the division by k of a function $g \in W^{(m)}_{\widetilde{F},n}$ or is a function in $W^{(m)}_{\widetilde{F},n}$ are obvious.

If $f(\overline{X}) = g(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$ where σ is a permutation of $\{1, \cdots, n\}$ then the tuple $(\overline{x}, y)$ belongs to the graph of f iff

$$\mathbb{Z}_p \models \exists \overline{t} \;\; \wedge_i \, t_i = x_{\sigma(i)} \wedge y = g(\overline{t}).$$

Therefore, both the graphs of f, of its derivatives and their extensions to V_d are existentially definable in terms of $[g]$.

If f is the inverse of a function g, then $(\overline{x}, y)$ belongs to the graph of f iff

$$yg(\overline{x}) = 1.$$

So, we are reduced to the following case:

Let $f, g \in W^{(m)}_{\widetilde{F},n+1}$ where f has order d in X_{n+1}. Then, there are $A_0, \cdots, A_{d-1} \in W^{(m+1)}_{\widetilde{F},n}$ and $Q \in W^{(m+1)}_{\widetilde{F},n+1}$ such that

$$g = Qf + \Big(A_{d-1}X^{d-1}_{n+1} + \cdots + A_0\Big).$$

We have to prove that $A_0, \cdots, A_{d-1}, Q$ (and their derivatives) are strongly definable in $\mathbb{Z}_p$ and that the definitions work uniformly over the algebraic extensions V_d.

Claim 2. *$A_0, \cdots, A_{d-1}$ are strongly definable in terms of $[f, g]$.*

Proof. Fix $\overline{x} \in \mathbb{Z}_p^n$.

Let $\alpha_1, \cdots, \alpha_d$ be the roots of $f(\overline{x}, X_{n+1})$ in V_d (we take in account multiplicities). Then, $A_0(\overline{x}), \cdots, A_{d-1}(\overline{x})$ are uniquely determined by these roots.

Indeed, first assume that the roots are distinct. In this case, $A_0(\overline{x}), \cdots, A_{d-1}(\overline{x})$ are determined by the relations:

$$\alpha_i \neq \alpha_j \text{ for all } i, j$$
$$f(\overline{x}, \alpha_i) = 0 \text{ for all } i$$
$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} A_0(\overline{x}) \\ \vdots \\ A_{d-1}(\overline{x}) \end{pmatrix} = \begin{pmatrix} g(\overline{x}, \alpha_1) \\ \vdots \\ g(\overline{x}, \alpha_d) \end{pmatrix}.$$

If $f(\overline{x}, X_{n+1})$ admits singular roots, say $\alpha_1 = \alpha_2$ and $\alpha_i \neq \alpha_j$ for all $i \neq j$, $i, j \neq 2$ for instance, then we replace the d equations $f(\overline{x}, \alpha_1) = \cdots = f(\overline{x}, \alpha_d) = 0$ by $f(\overline{x}, \alpha_1) = \frac{\partial f}{\partial X_{n+1}}(\overline{x}, \alpha_1) = f(\overline{x}, \alpha_3) = \cdots = f(\overline{x}, \alpha_d) = 0$. The functions A_i are determined in this case by the relations:

$$\alpha_i \neq \alpha_j \text{ for all } i \neq j,\ j \neq 2$$
$$f(\overline{x}, \alpha_i) = 0 \text{ for all } i \neq 2$$
$$\tfrac{\partial f}{\partial X_{n+1}}(\overline{x}, \alpha_1) = 0$$
$$\begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ 0 & 1 & \cdots & (d-1)\alpha_1^{d-2} \\ 1 & \alpha_3 & \cdots & \alpha_3^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \begin{pmatrix} A_0(\overline{x}) \\ A_1(\overline{x}) \\ A_2(\overline{x}) \\ \vdots \\ A_{d-1}(\overline{x}) \end{pmatrix} = \begin{pmatrix} g(\overline{x}, \alpha_1) \\ \frac{\partial g}{\partial X_{n+1}}(\overline{x}, \alpha_1) \\ g(\overline{x}, \alpha_3) \\ \vdots \\ g(\overline{x}, \alpha_d) \end{pmatrix}.$$

For each configuration of multiplicities of the roots of $f(\overline{x}, X_{n+1})$, the coefficients A_i are completely determined by a system like above. We proceed to a disjunction over all possible cases to define the graphs of $A_0, \cdots, A_{d-1}$ on $\mathbb{Z}_p^n$:

Let $\Psi(\overline{x}, A_0(\overline{x}), \cdots, A_{d-1}(\overline{x}), \overline{\alpha})$ be the disjunction of all possible system like above. Then, the following formula gives an existential definition of the graphs of $A_0, \cdots, A_{d-1}$:

$$\exists \alpha_1 \cdots \alpha_d \in V_d \ \Psi(\overline{x}, A_0(\overline{x}), \cdots, A_{d-1}(\overline{x}), \overline{\alpha}).$$

Let us remark that the above definitions are existential definitions in V_d. We interpret this formulas in $\mathbb{Z}_p$. So, formally, the α_i's are replaced by tuples, the additions, multiplications (in V_d in Ψ) are replaced by their interpretation in $\mathbb{Z}_p$. Similarly, the functions f, g, their derivatives are also replaced by their interpretations in $\mathbb{Z}_p$ (which exists by inductive hypothesis).

Note also that the α_i's are only unique up to permutation. It means that so far, we have only existentially defined the graphs of the A_i's. We transform this existential definition into a strong existential formula using [3]. In this paper, J. Denef gives a formula of definable selection for finite sets i.e. a quantifier free formula $D(x, X)$ (where X is a new predicate) such that for all $X(\overline{v})$ a predicate corresponding to a finite set in $\mathbb{Q}_p$:

$$\begin{aligned}\mathbb{Q}_p \models \exists v_1, \cdots, v_s \quad & \Big[\textstyle\bigwedge_i X(v_i) \wedge \bigwedge_{i,j} v_i \neq v_j\Big] \\ & \to \exists ! v_1, \cdots \exists ! v_s \Big[\textstyle\bigwedge_i X(v_i) \wedge \bigwedge_i D(v_i, X) \wedge \bigwedge_{i,j} v_i \neq v_j\Big].\end{aligned}$$

We use this formula with X equals to the set $\{\alpha_1, \cdots, \alpha_d\}$ to get a strong definition of the graphs of the A_i's. □

Note that the above formula works uniformly over the algebraic extensions. Therefore, the graphs of the $A_i's$ as functions from V_d^n to V_d are also strongly definably interpretable.

Claim 3. *Q and its derivatives (with respect to X_{n+1}) are strongly definable in terms of $[f, g], A_0, \cdots, A_{d-1}$.*

Proof. Let $\widetilde{g} := g - \sum A_i X_{n+1}^i$. Then, $\widetilde{g} = Q \cdot f$. Fix $\overline{x} \in \mathbb{Z}_p^n$.

- If $f(\overline{x}) \neq 0$, then
$$Q(\overline{x}) = \widetilde{g}(\overline{x}) \Big/ f(\overline{x}).$$

- If $f(\overline{x}) = 0 \neq \frac{\partial f}{\partial X_{n+1}}(\overline{x})$, as $\frac{\partial \widetilde{g}}{\partial X_{n+1}}(\overline{x}) = Q(\overline{x}) \cdot \frac{\partial f}{\partial X_{n+1}}(\overline{x}) + \frac{\partial Q}{\partial X_{n+1}}(\overline{x}) \cdot f(\overline{x})$,
$$Q(\overline{x}) = \frac{\partial \widetilde{g}}{\partial X_{n+1}}(\overline{x}) \Big/ \frac{\partial f}{\partial X_{n+1}}(\overline{x}).$$

- We proceed similarly for the other cases. Let us remark that if $f(\overline{x}) = \cdots = \frac{\partial^{d-1} f}{\partial X_{n+1}^{d-1}}(\overline{x}) = 0$, then necessarily, $\frac{\partial^d f}{\partial X_{n+1}^d}(\overline{x}) \neq 0$. In this case, we have that:
$$Q(\overline{x}) = \frac{\partial^d \widetilde{g}}{\partial X_{n+1}^d}(\overline{x}) \Big/ \frac{\partial^d f}{\partial X_{n+1}^d}(\overline{x}).$$

A disjunction over all above cases gives a definition of the graph of Q.
Also, we can define $\frac{\partial Q}{\partial X_{n+1}}$:
If $f(\overline{x}) \neq 0$, as $\frac{\partial \widetilde{g}}{\partial X_n} = Q \cdot \frac{\partial f}{\partial X_{n+1}} + \frac{\partial Q}{\partial X_{n+1}} \cdot f$,

$$\frac{\partial Q}{\partial X_{n+1}} = \Big(\frac{\partial \widetilde{g}}{\partial X_{n+1}} - Q \cdot \frac{\partial f}{\partial X_{n+1}}\Big)\Big/ f.$$

We have a similar equality in the case where $f(\overline{x}) = 0 \neq \frac{\partial f}{\partial X_{n+1}}(\overline{x})$. Again, we have to do a disjunction over all $i \leq d$ such that $\frac{\partial^i f}{\partial X_{n+1}^i}(\overline{x}) \neq 0$ and $\frac{\partial^k f}{\partial X_{n+1}^k}(\overline{x}) = 0$ for all $k < i$. By induction on j, we can define $\frac{\partial^j Q}{\partial X_{n+1}^j}$ similarly. □

Again, the above formula works uniformly over finite algebraic extensions. So, the graphs of Q and its derivative with respect to X_{n+1} as functions from V_d^{n+1} to V_d are strongly existentially definably interpretable.

In the next claim, we will use the following notations: let $I = (i_1, \cdots, i_l)$ where $i_k \in \{1, \cdots, n\}$, then

$$\frac{\partial^I A_i}{\partial X_I} = \frac{\partial}{\partial X_{i_1}} \cdots \frac{\partial}{\partial X_{i_l}} A_i$$
$$\frac{\partial^{I,j} Q}{\partial X_I \partial X_{n+1}^j} = \frac{\partial}{\partial X_{i_1}} \cdots \frac{\partial}{\partial X_{i_l}} \frac{\partial^j}{\partial X_{n+1}^j} Q.$$

Claim 4. *For all $I = (i_1, \cdots, i_l)$ and for all j, $\frac{\partial^I A_i}{\partial X_I}$ and $\frac{\partial^{I,j} Q}{\partial X_I \partial X_{n+1}^j}$ are strongly definable in terms of $[f, g]$.*

Proof. We prove the claim by induction on the length of I. First, we prove that $\frac{\partial R_0}{\partial X_i}, \cdots, \frac{\partial R_{d-1}}{\partial X_i}, \frac{\partial^{(i),j} Q}{\partial X_i \partial X_{n+1}^j}$ are strongly definable in terms of $[f, g]$ for all $i \leq n$ and for all j.

Let $g_i := \frac{\partial g}{\partial X_i} - Q \cdot \frac{\partial f}{\partial X_i}$ (where $i \leq n$). Let us remark that by claim 3, g_i is strongly definable in terms of $[f, g]$. We derive the equality $g = Qf + \sum_k A_k X_{n+1}^k + X_{n+1}^d$ with respect to X_i and obtain that

$$g_i = \frac{\partial Q}{\partial X_i} f + \sum_k \frac{\partial A_k}{\partial X_i} X_{n+1}^k.$$

We apply claims 2 and 3 with this equality to get the strong definitions of $\frac{\partial A_0}{\partial X_i}, \cdots, \frac{\partial A_{d-1}}{\partial X_i}$, $\frac{\partial^{(i),j} Q}{\partial X_i \partial X_n^j}$.

Let $I = (i_1, \cdots, i_l)$. Let $i \in \{1, \cdots, n\}$ and $I' = (i, i_1, \cdots, i_l)$. Assume that the claim is proved for the derivatives with respect to I. Let $g_{I'} := \frac{\partial g_I}{\partial X_i} - Q \cdot \frac{\partial f}{\partial X_i}$ (where g_I is defined by induction on the length of I). As (by induction),

$$g_I = \frac{\partial^I Q}{\partial X_I} f + \sum_k \frac{\partial^I A_k}{\partial X_I} X_{n+1}^k,$$

we derive this equality with respect to X_i and get that

$$g_{I'} = \frac{\partial^{I'} Q}{\partial X_{I'}} f + \sum_k \frac{\partial^{I'} A_k}{\partial X_{I'}} X_{n+1}^k.$$

Again, we apply claims 2 and 3 with this equality to get the strong definitions of $\frac{\partial^{I'} A_0}{\partial X_{I'}}, \cdots, \frac{\partial^{I'} A_{d-1}}{\partial X_{I'}}, \frac{\partial^{I',j} Q}{\partial X_{I'} \partial X_n^j}$.
This completes the proof of the claim 4. □

This proves that $A_0, \cdots, A_{d-1}, Q$ and their derivatives are strongly definable functions in terms of functions in $W^{(m)}_{\widetilde{F},n+1}$ and therefore completes the proof of the proposition.

□

The main theorem of this section follows immediately from propositions 3.1.7 and 3.4.1

Theorem 3.4.2. *Let F be a family of restricted analytic functions. Assume that the set of $\mathcal{L}_F$-terms is closed under derivation. Let $\widetilde{F}$ be the extension of F by the decomposition functions of each $f \in F$. Then, $\mathbb{Z}_{p,\widetilde{F}}$ is strongly model-complete in $\mathcal{L}_{\widetilde{F}}$.*

Chapter 4

Effective model-completeness

In this chapter, we are interested by the effectivity of the theorem 3.4.2 i.e. is there an algorithm which takes for entry a $\mathcal{L}_{\widetilde{F}}$-formula $\Psi(\overline{x})$ and returns a strong existential formula $\varphi(\overline{x})$ equivalent to $\Psi(\overline{x})$?

In chapter 3, we have given an explicit description of φ except for the use of proposition 3.1.7. So, if we can prove that this step can be done effectively, we are done. This proposition relies on the elimination of quantifiers in [4]. In the proof of this theorem, most of the steps are either clearly effective or the effectivity is already well understood (e.g. elimination of quantifier in $\mathbb{Z}_p$, lemma 3.1.5). We will focus our attention to the most awkward step with respect to the effectivity: the use of lemma 1.4 in [4]. First, let us recall this lemma.

Lemma 4.0.1 (lemma 1.4 in [4]). *Let $f(\overline{X},\overline{Y}) = \sum a_I(\overline{Y})\overline{X}^I \in \mathbb{Z}_p\{\overline{X},\overline{Y}\}$. Then, there is $d \in \mathbb{N}$ such that, for all I with $|I| \geq d$,*

$$a_I(\overline{Y}) = \sum_{|J|<d} b_{IJ}(\overline{Y})a_J(\overline{Y}),$$

where $b_{IJ} \in \mathbb{Z}_p\{\overline{Y}\}$ with $\|b_{IJ}\| < 1$.

The existence of d follows from the Noetherian property of the ring $\mathbb{Z}_p\{\overline{Y}\}$. It is a priori not obvious that one can compute effectively such a bound.

Definition 4.0.2. *Let $f \in \mathbb{Z}_p\{\overline{X},\overline{Y}\}$. We say that f has* an effective Weierstrass bound *if one can compute $d(f)$ a upper bound for the smallest integer d like in lemma 4.0.1.*

A Weierstrass system for which there is an algorithm which compute $d(f)$ for each function f of the system is called an *effective Weierstrass system.*
The main theorem of this chapter is that under the assumptions of theorem 3.4.2 and assuming that we can compute the above d for any $\mathcal{L}_{\widetilde{F}}$-term, the Weierstrass system $W_{\widetilde{F}}$ is effective. And therefore, the theory of $\mathbb{Z}_{p,\widetilde{F}}$ is effectively model-complete.
This follows from an induction on the complexity of the functions in the Weierstrass system. We will develop this in section 4.1. In sections 4.2 and 4.3, we prove the main theorem of this chapter. In section 4.2, we compute an effective bound of the mixed volume of a system of analytic equations with effective Weierstrass bound. This notion of mixed volume comes from tropical analytic geometry and will allow us in section 4.3 to compute the effective Weierstrass bound of any function in the Weierstrass system generated by the $\mathcal{L}_{\widetilde{F}}$-terms (under the above assumptions).
Finally, in the last section, we discuss the special case of $\mathbb{Z}_{p,exp}$. In particular, we apply our main result to show that the Weierstrass system generated by the closure under decomposition functions of the $\mathcal{L}_{exp}$-terms is effective. Therefore, this shows that the theory of $\mathbb{Z}_p$ in the language of p-adic exponential rings expanded by the decomposition functions is effectively model-complete.

4.1 Effective Weierstrass system

For the rest of this chapter, we fix F a family of restricted analytic functions. We assume that the set of $\mathcal{L}_F$-terms is closed under derivation. We also assume that this family is an *effective family of restricted analytic functions* i.e. that F is recursively enumerable and that, for all I, there exists some algorithm $\mathcal{D}$ which takes for entries functions f in F and returns a $\mathcal{L}_F$-term g such that $\frac{\partial^I f}{\partial X^I} = g$.

Definition 4.1.1. *A Weierstrass system* $(\mathbb{Z}_p[\![X_1, \cdots, X_n]\!])_{n\in\mathbb{N}}$ *is called* effective *if there exists an algorithm which takes for entries functions f of the system and returns an integer $d(f)$ such that, for all I with $|I| \geq d(f)$,*

$$a_I(\overline{Y}) = \sum_{|J|<d(f)} b_{IJ}(\overline{Y})a_J(\overline{Y}),$$

where $f(\overline{X}, \overline{Y}) = \sum a_I(\overline{Y})\overline{X}^I$ *and* $b_{IJ} \in \mathbb{Z}_p\{\overline{Y}\}$ *with* $\|b_{IJ}\| < 1$.

It should be clear from chapter 3 that if the Weierstrass system generated by the $\mathcal{L}_{\widetilde{F}}$-terms is effective then the strong model-completeness in theorem 3.4.2 is effective. We will now assume that F satisfies:

Hypothesis (W). *Let $f(X,\overline{Y})$ be a $\mathcal{L}_F$-term. Then, f has an effective Weierstrass bound.*

Let W_F be the Weierstrass system generated by the $\mathcal{L}_F$-terms. We will show that, under the hypothesis (W), W_F is an effective Weierstrass system. Therefore, the theorem 3.4.2 is effective assuming that $\widetilde{F}$ (the expansion of F by the decomposition functions) satisfies hypothesis (W): under these hypotheses, $W_{\widetilde{F}}$ is an effective Weierstrass system which implies the effective model-completeness of the theory of $\mathbb{Z}_{p,\widetilde{F}}$. First, we show that the integer $d(f)$ can be computed for each term in our language (for any length of the variable $\overline{X}$). This proposition is due to A. Macintyre in [8].

Proposition 4.1.2. *Let F be any effective family of restricted analytic functions. Assume that F satisfies hypothesis (W). Then, there exists a computable function D from the set of $\mathcal{L}_F$-terms to $\mathbb{N}$ such that for all $\mathcal{L}_F$-term $f(\overline{X},\overline{Y})$, if d is the smallest integer like in lemma 4.0.1, then $d \leq D(f)$.*

Proof. Let $f(\overline{X},\overline{Y}) = \sum a_I(\overline{Y})\overline{X}^I$. Let d be the smallest integer like in lemma 4.0.1. Then, for all $\overline{y} \in \mathbb{Z}_p^m$, one of the following formulas is satisfied in $\mathbb{Z}_p$:

$$Z(\overline{Y}) \equiv \bigwedge_{|J|<d} a_J(\overline{Y}) = 0,$$

or, for some $|I| < d$,

$$\mu_{I,f}(\overline{Y}) \equiv \bigwedge_{J<I} v(a_I(\overline{Y})) \leq v(a_J(\overline{Y})) \wedge \bigwedge_{I<J,\ |J|<d} v(a_I(\overline{Y})) < v(a_J(\overline{Y})).$$

Fix $\overline{y} \in \mathbb{Z}_p^m$ and assume $\mu_{I,f}(\overline{y})$ where $i_1 \neq 0$ (unless $Z(\overline{y})$ is satisfied, we can assume that this is the case). Then,

$$\begin{aligned} a_I^{-1}(\overline{y})f(\overline{X},\overline{y}) = & \sum_{J<I} \Big(a_J(\overline{y})/a_I(\overline{y})\Big)\overline{X}^J + \overline{X}^I + \sum_{I<J,\ |J|<d} \Big(a_J(\overline{y})/a_I(\overline{y})\Big)\overline{X}^J \\ & + \sum_{|K|\geq d} \Big\{ \sum_{J<I} \Big(a_J(\overline{y})/a_I(\overline{y})\Big) b_{KJ}(\overline{y}) + b_{KI}(\overline{y}) \\ & + \sum_{I<J,\ |J|<d} \Big(a_J(\overline{y})/a_I(\overline{y})\Big) b_{KJ}(\overline{y}) \Big\} \overline{X}^K. \end{aligned}$$

We introduce new variables V_J and replace the quotients a_J/a_I by V_J or pV_J according if $J < I$ or $I < J$, $|J| < d$. It defines a function:

$$\widetilde{f}(\overline{X},\overline{V},\overline{Y}) = \sum_{J<I} V_J\overline{X}^J + \overline{X}^I + \sum_{I<J,\ |J|<d} pV_J\overline{X}^J$$
$$+\sum_K \left(\sum_{J<I} V_J b_{KJ} + b_{KI} + \sum_{I<J,\ |J|<d} pV_J b_{KJ} \right) \overline{X}^K.$$

Then, $f(\overline{X},\overline{y}) = a_I(\overline{y})\tilde{f}(\overline{X},\overline{v},\overline{y})$ where $v_J = a_J(\overline{y})/a_I(\overline{y})$ or $a_J(\overline{y})/pa_I(\overline{y})$. And, if we proceed to change of variables

$$\begin{cases} X_i \longrightarrow Z_i - Z_n^{d^{n-i}} \text{if i<n} \\ X_n \longrightarrow Z_n, \end{cases}$$

the function $\tilde{f}(\overline{Z},\overline{v},\overline{y})$ has order $S = i_n + i_{n-1}d + \cdots + i_1 d^{n-1}$ in Z_n (where $I = (i_1, \cdots, i_n)$). By the Weierstrass preparation theorem,

$$\tilde{f}(\overline{Z},\overline{V},\overline{y}) = \Big(Z_n^S + A_{S-1}(Z_1,\cdots,Z_{n-1},\overline{V},\overline{y}) + \cdots + A_0(Z_1,\cdots,Z_{n-1},\overline{V},\overline{y})\Big)U(\overline{Z},\overline{V},\overline{y}).$$

And ,

$$f(\overline{Z},\overline{y}) = a_I(\overline{y})\tilde{f}(\overline{Z},\overline{v},\overline{y}).$$

So, for any $z_1, \cdots, z_{n-1} \in \mathbb{Z}_p$, $f(Z_n, \overline{z'}, \overline{y})$ has exactly S roots (counting multiplicities) in $\mathcal{O}_p$. By Strassmann theorem 2.1.9, the integer $d(f)$ given by hypothesis (W) determines an effective upper bound of S and therefore of d (unless $I = (0, \cdots, 0)$ for all $\overline{y}$, in which case, we can take $D(f) = 1$). □

As we have seen in this proof, if we want to prove that W_F is an effective Weierstrass system, it is actually sufficient to prove the following:
Let $f(X, \overline{Y})$ be a $\mathcal{L}_{W_F}$-term. Then, one can compute an upper bound $S(f)$ on the number of roots (counting multiplicities) of the function $f(X, \overline{y})$ in $\mathcal{O}_p$ (if this number is finite). We want that this bound does not depend on the choice of the parameters $\overline{y} \in \mathbb{Z}_p^n$.
In that case, f has an effective Weierstrass bound given by $S(f) + 1$.
Let f be a function in our Weierstrass system. Then, there are integers n and $m+1$ such that $f \in W_{F,n}^{(m+1)}$. Also, f has an existential definition in terms of functions in $W_{F,n+1}^{(m)}$: as we have seen in chapter 3, there exist $g_1, \cdots, g_k \in W_{F,n+1}^{(m)}$ such that $f \in \langle g_1, \cdots, g_k \rangle$.

So, we proceed by induction: assuming that we can compute $d(g_1), \cdots, d(g_k)$, we will show that we can effectively bound the number of solutions in $\mathcal{O}_p$ of $f(X, \overline{x'}) = 0$ (uniformly over $\overline{x'} \in \mathbb{Z}_p^{n-1}$). And therefore, we will find an effective bound of $S(f)$ in terms of $d(g_1), \cdots, d(g_k)$.
The basic step of the induction is given by proposition 4.1.2. The cases where f is obtained from a function $g \in W_{F,n}^{(m)}$ by inversion, permutation of the variables or division by an integer are rather easy. The main difficulty is the case where f is obtained using Weierstrass division. In this case, by the definitions given in the claims 2 to 4 in proposition 3.4.1, we see that zeros of such a function correspond to zeros of systems of n' equations in $W_{F,n'}^{(m)}$ (with t parameters) .
We will now bound the number of solutions in $(\mathcal{O}_p^*)^n$ of a general system of n analytic functions with n variables (uniformly over some parameters). For this, we will use results of tropical analytic geometry (see appendix A).

4.2 Effective bound for the mixed volume of a system with effective Weierstrass bound.

In this section, we will use results of tropical analytic geometry due to J. Rabinoff (see [14]). We refer to appendix A for an overview of the results and notions that we need for this section.

Let $f = \sum a_I \overline{X}^I \in \mathbb{Z}_p\{\overline{X}\}$. First, note that $f \in \mathbb{Q}_p\langle [0,\infty)^n \rangle := \mathbb{Q}_p\{\overline{X}\}$. So, it makes sense to apply the results of appendix A in our setting. We recall some notations:

$$vert_v(f) := \{(I, v_p(a_I)) \mid \ a_I \neq 0 \text{ and } v_p(a_I) + \langle I, v \rangle \leq v_p(a_J) + \langle J, v \rangle \ \forall J\},$$

where $\langle \cdot, \cdot \rangle$ denotes the scalar product, $v \in [0, +\infty)^n$.
And, the Newton complex of f, denoted by $New(f)$, is the set of cells

$$\check{\gamma}_v = \check{\gamma}_v(f) := \pi(conv(vert_v(f))),$$

where π denotes the projection along the n first coordinates and $v \in [0, \infty)^n$. Let us recall that the polyhedron $\check{\gamma}_v$ is the convex closure of a finite subset of $\mathbb{R}^n$. Finally,

$$Trop(f) = \{v \in (\mathbb{R} \cup \{\infty\})^n \mid \quad v = (v_p(x_1), \cdots, v_p(x_n)) \text{ for some } \overline{x} \in \mathcal{O}_p \text{ such that } f(\overline{x}) = 0\}.$$

Let $f = (f_1, \cdots, f_n)$ be a system of functions in $\mathbb{Z}_p\{X_1, \cdots, X_n, \overline{Y}\}$. We assume that each f_i satisfies our inductive hypothesis. It means that each f_i has an effective Weierstrass bound $d(f_i)$. We will also assume that any derivative of f_i has an effective Weierstrass bound (this will be our actual inductive hypothesis).

We want to bound the number of solutions of the system uniformly over the parameters $\overline{Y}$ (whenever there is finitely many solutions for this choice of parameters). Fix $\overline{y} \in \mathbb{Z}_p^k$ and assume that the number of solutions of the system in $\mathcal{O}_p^n$ is finite for this choice of parameters. We recall the main results of [14]: there is a relation between the number of solutions of the system and the Newton complex:

If $\overline{x}$ is a solution of the system in $\mathcal{O}_p^n$ with non-zero coordinates such that $trop(\overline{x}) := (v(x_1), \cdots, v(x_n)) \in \mathbb{R}^n$ is an isolated point of $\bigcap_i Trop(f_i)$, then the number of solutions in $\mathcal{O}_p^n$ with valuation $trop(\overline{x})$ is exactly (counting multiplicity) the mixed volume of the polyhedrons

$$\pi(conv(vert_{trop(\overline{x})}(f_1))), \cdots, \pi(conv(vert_{trop(\overline{x})}(f_n))).$$

We denote this volume by

$$MV(\check{\gamma}_v(f_1), \cdots, \check{\gamma}_v(f_n)).$$

On the other hand, if $v := trop(\overline{x})$ is not isolated in $\bigcap Trop(f_i)$. Let $C = \bigcap_i \gamma_v(f_i) = \{v' \in \bigcap Trop(f_i) \mid \ vert_{v'}(f_i) \supseteq vert_v(f_i) \text{ for all } i\}$. Then, C is a Γ-affine polyhedron contained in $\bigcap_i Trop(f_i)$ and which contains v. We want to apply theorem A.4.4 to determine the maximal number of roots with valuation in this component. Assume that all the hypothesis of this theorem are satisfied. Then, the number of solutions in $\mathcal{O}_p^n$ with valuation in $\overline{C}$ (the compactification of C) is (counting multiplicities):

$$i(C, Trop(f_1), \cdots, Trop(f_n)) := \sum_{\nu \in \widetilde{P}} i(\nu, Trop(f_1) + \varepsilon\widetilde{v}_1, \cdots, Trop(f_n) + \varepsilon\widetilde{v}'_n),$$

for any suitable perturbation of the system $\widetilde{P}$ ($\widetilde{P}$ is a finite set).

We will now prove that one can compute integers D_1 and D_2 such that

- $MV(\check{\gamma}_v(f_1), \cdots, \check{\gamma}_v(f_n))$ and $i(\nu, Trop(f_1) + \varepsilon\widetilde{v}_1, \cdots, Trop(f_n) + \varepsilon\widetilde{v}'_n))$ are both less than D_1 (independently on the choice of $\overline{x}, \overline{y}, \nu$ and $\widetilde{v}$); and,
- $\bigcap Trop(f_i)$ can obtained as the union of less than D_2 isolated points and connected components C like above. Furtermore, D_2 is a bound for the cardinality of $\widetilde{P}$.

With this, we will be able to bound the number of solutions of our system with non-zero coordinates.

The crucial point of the proof is that under our inductive hypothesis, we are able to compute a box such that the (support of the) Newton complex of f_i is contained in this box:

Lemma 4.2.1. *Let $f \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}$ such that f and all its derivatives have an effective Weierstrass bound. Then, we can effectively find an integer $E(f)$ such that for all $\overline{y} \in \mathbb{Z}_p$, either $f_{\overline{y}}(\overline{X}) := f(\overline{X}, \overline{y})$ is identically zero or $New(f_{\overline{y}}) \subseteq B_{\max}(E(f))$.*

In this lemma, $B_{\max}(E)$ denotes the set $\{I \in \mathbb{R}^n \mid \max_k\{|i_k|\} \leq E\}$. Note also that we have identify $New(f)$ and its support.

Proof. Let us recall that an element of $New(f)$ is the projection of a set $vert_\nu(f)$ (for $\nu \in \mathbb{R}^n$, $\nu = trop(\overline{x})$ for some $\overline{x} \in (\mathcal{O}_p^*)^n$) i.e. is the set of indexes J such that $v(a_J(\overline{y})) + \langle \nu, J\rangle$ reaches the minimum of the set $\{v(a_I(\overline{y})) + \langle \nu, I\rangle;\ I \in \mathbb{N}^n\}$ for some $\nu \in [0, \infty)^n$. So, it is sufficient to show that for all $\nu \in [0, \infty)^n$ the projection of the set $vert_\nu(f)$ is contained in $B_{\max}(E(f))$ for suitable (computable) $E(f)$.

As f has an effective Weierstrass bound, we know that there exists $d(f)$ (computable) such that for all $|I| \geq d(f)$,

$$a_I(\overline{Y}) = \sum_{|J|<d(f)} b_{IJ}(\overline{Y}) a_J(\overline{Y}),$$

where $b_{IJ} \in \mathbb{Z}_p\{\overline{Y}\}$ with $\|b_{IJ}\| < 1$. Fix $\overline{y} \in \mathbb{Z}_p$ and assume $f_{\overline{y}} \not\equiv 0$ i.e. $a_I(\overline{y}) \neq 0$ for some $|I| < d(f)$. First, let us remark that for all I such that $i_1, \cdots, i_n \geq d(f)$, for all $\overline{x} \in (\mathcal{O}_p^*)^n$, we can find J with $|J| < d(f)$ such that

$$\begin{aligned} v(a_I(\overline{y})) + \langle I, trop(\overline{x})\rangle &\geq \min_{|K|<d(f)} \{v(b_{IK}(\overline{y})) + v(a_K(\overline{y})) + \langle K, trop(\overline{x})\rangle\} \\ &> v(a_J(\overline{y})) + \langle J, trop(\overline{x})\rangle. \end{aligned}$$

If $n = 1$, take $E(f) = d(f)$ and we are done by the above inequality.

In the general case, we already know by the above inequality that no index I that satisfies $i_1, \cdots, i_n \geq d(f)$ can be a point of $vert_\nu(f)$. It remains to bound indexes in $vert_\nu(f)$ with at least one coordinate less than $d(f)$.

Fix $1 \leq k \leq n$ and $1 \leq s \leq d(f)$. Fix a coefficient I whose kth coordinate is s. Then, $a_I(\overline{y})\overline{X}^I$ is the $(i_1, \cdots, i_{k-1}, s, i_{k+1}, \cdots, i_n)$th coefficient of the function $f_{s,k}(\overline{X}, \overline{y})X_k^s$ where

$$f_{s,k}(\overline{X}, \overline{y}) = (1/s!)\frac{\partial^s f}{\partial x_k^s}(X_1, \ldots, X_{k-1}, 0, X_{k+1}, \cdots, X_n, \overline{y}).$$

Then, as $f_{s,k}$ has an effective Weierstrass bound, there is $d(f, s, k) := d(f_{s,k})$ such that for all I with $\max_{j \neq k}\{i_j\} \geq d(f, s, k)$,

$$v(a_I(\overline{y})) + \sum_{l \neq k} i_l v(x_l) > \min\{v(a_{(j_1, \cdots, j_{k-1}, s, j_{k+1}, \cdots, j_n)}(\overline{y})) + \sum_{l \neq k} j_l v(x_l)\}.$$

where the min is taken in $\{J' : |J'| = |(j_1, \cdots, j_{k-1}, j_{k+1}, \cdots, j_n)| < d(f, s, k)\}$. We set:

$$E'(f) = \max_{k \leq n} \max_{s \leq d(f)} \{d(f, k, s), d(f)\}.$$

If $n = 2$, we can take $E(f) = E'(f)$. Otherwise, we can compute $E(f_{s,k})$ for all $s \leq d(f)$ and $k \leq n$ by induction: we proceed like above with $f = f_{s,k}$. Then, we take $E(f) = \max_{s,k}\{E(f_{s,k}), E'(f)\}$. □

We can now bound effectively the number of roots (counting multiplity) of the system f with isolated tropicalization.

Lemma 4.2.2. *Let $f = (f_1, \cdots, f_n) \in (\mathbb{Z}_p\{\overline{X}, \overline{Y}\})^n$ such that f_i and all its derivatives have an effective Weierstrass bound for all i. Then, one can compute integers D_1 and D_2 (depending only on f) such that for all $\overline{y} \in \mathbb{Z}_p^m$, either $\bigcap V(f_i(\overline{X}, \overline{y}))$ is infinite, or $\bigcap Trop(f_i(\overline{X}, \overline{y}))$ has less than D_1 isolated points and for each such a point the tropical intersection multiplicity of f at this point is less than D_2.*

In particular, under these hypotheses, whenever the system f has finitely may solutions in $(\mathcal{O}_p)^n$, it has less than $D_1 \cdot D_2$ solutions in $(\mathcal{O}_p^*)^n$ with isolated tropicalization (counting multiplicities).

Proof. Assume that we have choosen $\overline{y}$ such that the number of solutions of the system is nonzero and finite. Then, by lemma 4.2.1, $New(f_i)$ is contained in $B_{\max}(E(f_i))$.

Let us remark that the number of polygons with integral coordinates for the vertices contained in $B_{\max}(E(f_i))$ is finite. Let D_2 be the maximum of the mixed volumes $MV(P_1, \cdots, P_n)$ where each P_i runs accross the different polygons contained in $B_{\max}(E(f_i))$. Then, by theorem A.3.3, D_2 satisfies the conditions of our lemma.

Let us recall that the points of $\bigcap Trop(f_i(\overline{X}, \overline{y}))$ are determined by a system of linear equations. Each equation corresponds to an half-hyperplane contained in $Trop(f_i(\overline{X}, \overline{y}))$ (determined by some γ_v in the notation of appendix A). As these half-hyperplanes are in bijection with the faces of $New(f_i)$ (the $\check{\gamma}_v$'s, see proposition A.2.4), we can bound the number of systems:

Consider the polygon contained in $B_{\max}(E(f_i))$ with the maximal number of faces (say this polygon has d_i faces). Note that d_i is computable. Then, $Trop(f_i(\overline{X}, \overline{y}))$ has at most d_i half-hyperplanes. So, the number of isolated points contained in the intersection of all $Trop(f_j(\overline{X}, \overline{y}))$ is no more than $\prod_i d_i$. We define D_1 to be the product of all d_i's. □

We will now determine a bound for the number of roots such that the tropicalization lies on a non-proper intersection of $\bigcap Trop(f_i)$.

First, we recall some facts from appendix A:

Let $f_1, \cdots, f_n \in \mathbb{Z}_p\{\overline{X}\}$, $f_i = \sum f_{i,I}\overline{X}^I$. Let C be a connected component of $\bigcap Trop(f_i) \cap P$ where $P = [0, \infty)^n$. Then, there exist $v_1, \cdots, v_n \in \mathbb{N}^n$ and T such that, for all $\varepsilon \in (0, T]$, the intersection

$$\widetilde{P} := \bigcap (Trop(f_i) + \varepsilon v_i) \cap (P + \varepsilon v_i)$$

is a finite set of points.

Assume that C is a Γ-affine polyhedron and that the polyhedron $\bigcap_i conv(\{I \mid f_{i,I} \neq 0\})$ is pointed (i.e. has dimension n). Then, by theorem A.4.4, the number of solutions of our system with valuation in the compactification of the component C is equal to the tropical intersection multiplicity along C. And, by definition, this number is equal to the sum of tropical intersection multiplicities after pertubation of the system by ε i.e.

$$i(C, Trop(f_1), \cdots, Trop(f_n)) = \sum_{\nu \in \widetilde{P}} i(\nu, Trop(f_1) + \varepsilon v_1, \cdots, Trop(f_n) + \varepsilon v_n).$$

Let us remark now that, like in lemma 4.2.2, as the half-hyperplanes of $Trop(f_i)$ are in bijection with the faces of the Newton complex, one can compute effectively a bound for the number of connected components of the type $C = \bigcap \gamma_v(f_i)$ (which actually cover $\bigcap Trop(f_i)$).

On the other hand, let $f = \sum a_I \overline{X}^I \in \mathbb{Z}_p\{\overline{X}\}$ and $f'(\overline{X}) = \sum a'_I \overline{X}^I := f(\overline{X_i t^{-v_i}})$ (so, $Trop(f'_i) = Trop(f_i) + \varepsilon v_i$). Let $\overline{x} \in \mathcal{O}_p^n$ and $t \in \mathcal{O}_p$ with valuation ε and $I \in \mathbb{N}^n$ such that

$$v(a_I \overline{x}^I) = \min_J \{v(a_J \overline{x}^J)\}.$$

Then, for $\overline{x}' = \overline{xt^{v_i}}$,

$$v(a'_I \overline{x}') = v(a_I \overline{x}'^I t^{-\langle I, \overline{v} \rangle}) = \min_J \{v(a_J \overline{x'}^J t^{-\langle J, \overline{v} \rangle})\} = \min_J \{v(a'_J \overline{x'}^J)\}.$$

Therefore, $New(f)$ and $New(f')$ are both contained in the box given in lemma 4.2.1. It means that we can find an effective bound for $i(\nu, Trop(f_1) + \varepsilon v_1, \cdots, Trop(f_n) + \varepsilon v_n)$ for all $\nu \in \widetilde{P}$ and for the cardinality of $\widetilde{P}$ like in lemmas 4.2.1 and 4.2.2.

The above paragraph shows that we can compute a bound for the number of connected components $C = \bigcap \gamma_v(f_i)$ that cover $Trop(f_i)$ and that, for each such a C, we can bound the number of solutions of our system with tropicalization in $\overline{C}$. This shows that we can give a bound for the number of solutions $(\mathcal{O}_p^*)^n$ of the system assuming that $\bigcap_i conv(\{I \mid f_{i,I} \neq 0\})$ is pointed.

We are now ready to prove:

Theorem 4.2.3. *Let $f = (f_1, \cdots, f_n) \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}^n$ such that f_i and all its derivatives have an effective Weierstrass bound for each i. Then, there exists $S(f)$ computable in terms of the f_i's such that for all $\overline{y} \in \mathbb{Z}_p^n$, either the system $f_{\overline{y}}$ has infinitely many roots or it has less than $S(f)$ roots in $(\mathcal{O}_p^*)^n$.*

Proof. Lemma 4.2.2 gives us a bound $N(f)$ for the number of roots with isolated tropicalization. It remains to count the roots with non-isolated tropicalization.

If $\bigcap_i conv(\{I \mid f_{i,I} \neq 0\})$ is pointed, we are done by the above paragraph. Let us remark that in this case, the number $S(f)$ is determined using only the effective Weierstrass bound of the f_i's (and their derivatives).

In order to guarantee that the above polyhedron is pointed, we apply the following transformations to our system:

- If the variable X_i does not occur in f_j, we set ${f'}_j := f_j \cdot (1 + p^s X_i)$. We apply this transformation for all i, j when necessary.

  Then, the number of solutions of the system $({f'}_1, \cdots, {f'}_n)$ in $\mathcal{O}_p^n$ is the same that the number of solutions of the system $(f_1, \cdots, f_n)$ (indeed, the polynomial $(1 + p^s X_i)$ has no root in $\mathcal{O}_p$, and more generally no root with valuation greater than $-s$). Also, f'_j has the same effective Weierstrass bound that the Weierstrass bound of f_j. Note that the box $B_{\max}(E(f'_i))$ in which lies the Newton complex of f'_i does not depend on the choice of s.

- Let $(\widetilde{f_1}, \cdots, \widetilde{f_n})$ be the system obtained after the change of variables $X_i \longmapsto X_i - p^t Z_i$ applied to the system $({f'}_1, \cdots, {f'}_n)$ (where $\overline{Z}$ is a new parameter). Then, for t large enough (take t at least $\|f_j\|$), $\widetilde{f_j}$ has the same effective Weierstrass bound that f_j. Also, for a suitable choice of $\overline{z} \in \mathbb{Z}_p^n$, the number of non-zero solutions of the system $(\widetilde{f_1}, \cdots, \widetilde{f_n})$ is finite and is an upper bound for the number of non-zero solutions of the system $(f_1, \cdots, f_n)$. Furtermore, for the same choice of $\overline{z}$, we have that $\bigcap_i conv(\{I \mid \widetilde{f_{i,I}} \neq 0\})$ is pointed.

As, $\bigcap_i conv(\{I \mid \widetilde{f_{i,I}} \neq 0\})$ is pointed, we can compute a bound $S(\widetilde{f})$ on the number of non-zero solutions of the system $(\widetilde{f_1}, \cdots, \widetilde{f_n})$. Indeed, this number is determined by the effective Weierstrass bound of the $\widetilde{f_i}$'s (which are computable as we have discussed above). Note that, $S(\widetilde{f})$ does not depend on our choices of s, t. We set $S(f) := S(\widetilde{f}) + N(f)$. □

Remark. Let $f_1, \cdots, f_n \in \mathbb{Z}_p\{X_1, \cdots, X_n, \overline{Y}\}$ and
$g_1 \cdots, g_m \in \mathbb{Z}_p[X_1, \cdots, X_n, X_{n+1}, \cdots, X_{n+m}, \overline{Y}]$. Then, we can find an effective bound like in theorem 4.2.3 for the number of solutions of the system
$(f_1, \cdots, f_n, g_1, \cdots, g_m)$ in $(\mathcal{O}_p^*)^n \times (\mathbb{C}_p^*)^m$.
In fact, we can apply the results of appendix A in $K\langle P\rangle$ where $P = [0, \infty) \times [r_i, \infty)$. It allows us to bound the number of solutions in $(\mathcal{O}_p^*)^n \times (\mathbb{C}_p^*)^m$ with valuation at least r_i (for the last coordinates). Indeed, it is easy to see that we can compute a box in which lies $New(g_i)$. It implies that we can compute the bound with the same method that in theorem 4.2.3. Furthermore, let us remark that the box does not depend on the choice of r_i. Therefore, the bound for the number of solutions obtained is independent on the choice of r_i. It means that we have actually computed a bound for the number

of solutions in $(\mathcal{O}_p^*)^n \times (\mathbb{C}_p^*)^m$.

4.3 Proof of the main theorem

We can now prove the main theorem of this chapter:

Theorem 4.3.1. *Let F be an effective family of restricted analytic functions such that the set of $\mathcal{L}_F$-terms is closed under derivation. Let $\widetilde{F}$ be the extension of F by all decomposition functions of elements in F. Assume that $\widetilde{F}$ satisfies hypothesis (W). Then, the theory of $\mathbb{Z}_{p,\widetilde{F}}$ is effectively strongly model-complete in the language $\mathcal{L}_{\widetilde{F}}$.*

Proof. For this, as we have seen, it is actually sufficent to prove that $W_{\widetilde{F}}$ is an effective Weierstrass system. Let $f \in W_{\widetilde{F},n}^{(k)}$. We have to show that f has an effective Weierstrass bound. We proceed by induction on k and we show that for any $f \in W_{\widetilde{F},n}^{(k)}$, f and each of its derivatives admit an effective Weierstrass bound. The basic step of the induction is proposition 4.1.2.

So assume that for all n, for all $k \leq m$ and for all $g \in W_{\widetilde{F},n}^{(k)}$, g and all its derivatives have an effective Weierstrass bound. Let $H \in W_{\widetilde{F},n}^{(m+1)}$. We want to compute $d(H)$ (or more generaly, $d(G)$ where G denotes a derivatives of H). By definition of the Weierstrass system generated by the $\mathcal{L}_{\widetilde{F}}$-terms, H is a polynomial combination one of the following possibilities:

(a) $h \in W_{\widetilde{F},n}^{(m)}$. In that case, we can compute $d(h)$ by inductive hypothesis.

(b) There are $f \in W_{\widetilde{F},n}^{(m)}$ and a permutation σ such that $h(\overline{X}) = f(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$. In that case, we can compute $d(f)$ by inductive hypothesis and $d(h) = d(f)$. The same holds for any derivative of h.

(c) There is $f \in W_{\widetilde{F},n}^{(m)}$ such that f is invertible in $\mathbb{Z}_p\{\overline{X}\}$ and $h = f^{-1}$. In that case, $d(f) = d(h) = 1$. Also, $d\left(\frac{\partial h}{\partial X_i}\right) = d\left(-\frac{\partial f}{\partial X_i} h^2\right) = d\left(\frac{\partial f}{\partial X_i}\right)$ and similarly for the higher derivatives.

(d) There are $f \in W_{\widetilde{F},n}^{(m)}$ and $k \in \mathbb{Z}$ such that $h = f/k$. In that case, we can compute $d(f)$ by inductive hypothesis and $d(h) = d(f)$. The same holds for any derivative of h.

(e) There are $f \in W^{(m)}_{\widetilde{F},n+1}$ of order d in X_{n+1} and $g \in W^{(m)}_{\widetilde{F},n+1}$ such that h is one of the functions $a_0, \cdots, a_{d-1} \in \mathbb{Z}_p\{X_1, \cdots, X_n\}$ or $Q \in \mathbb{Z}_p\{X_1, \cdots, X_{n+1}\}$ given by the Weierstrass division.

In the last case, h (or any of its derivatives) is actually determined by a system of equations (see claims 2 to 4 in proposition 3.4.1). Let us remark that by inductive hypothesis, we can compute $d(f)$ and $d(g)$. More generally, let $h(\overline{X}) = P(\overline{X}, a_0(\overline{X}), \cdots, a_s(\overline{X}))$ where P is any polynomial with coefficients in $\mathbb{Z}$. Then,

Claim 5. *h and all its derivatives have an effective Weierstrass bound.*

Proof. Let $d(h)$ be the smallest integer like in lemma 4.0.1. We want to compute a bound of $d(h)$. For this, it is sufficient to bound $S(h)$, the number of roots in $\mathcal{O}_p$ of $h(Z, \overline{y}) = P(Z, a_0(z, \overline{y}), \cdots, a_s(z, \overline{y}), \overline{y})$, for any $\overline{y} \subset \mathbb{Z}_p^{n+k-1}$ such that this number is finite (where $Z = X_1$ and $\overline{y}$ denotes now $(x_2, \cdots, x_{n-1}, y_1, \cdots, y_k)$). Fix $\overline{y}$ such that the number of roots is finite. Let us remark that z is a solution of $h(Z, \overline{y})$ if $z, t_0, \cdots, t_s, a_0, \cdots a_s$ are solutions of the system of equations:

$$\begin{cases} f(t_0, z, \overline{y}) = 0 \\ \vdots \\ f(t_s, z, \overline{y}) = 0 \\ \begin{pmatrix} 1 & t_0 & \cdots & t_0^s \\ \vdots & \vdots & & \vdots \\ 1 & t_s & \cdots & t_s^s \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_s \end{pmatrix} = \begin{pmatrix} g(t_0, \overline{y}) \\ \vdots \\ g(t_s, \overline{y}) \end{pmatrix} \\ P(z, a_0, \cdots, a_s, \overline{y}) = 0 \end{cases}$$

if $t_i \neq t_j$ for all $i \neq j$. To make sure that this last condition is satisfied, we introduce the variables t_{ij} $0 \leq i < j \leq s$ and add to the system the equations:

$$t_{ij} \cdot (t_i - t_j) - 1 = 0.$$

Note that this system has finitely many solutions in $(\mathcal{O}_p)^{2s+3} \times (\mathbb{C}_p)^{(s^2+s)/2}$ if $h(Z, \overline{y})$ has finitely many solutions in $\mathcal{O}_p$. By theorem 4.2.3 and the remark after, one can compute a bound for the number of solutions of the system in $(\mathcal{O}_p^*)^{2s+3} \times (\mathbb{C}_p^*)^{(s^2+s)/2}$. It remains to count the number of solutions with at least one zero coordinate.

Clearly, for all z, the a_i's are uniquely determined and the t_j's are unique up to permutation. So, the system have less than $(s + 1)!$ solutions with $z = 0$.

We proceed now by induction on the number of non-zero variables a_i and t_j involved. If all a_i and t_j are zeros, let us remark that one of the equations $P(z, 0, \cdots, 0, \overline{y}) = 0$ or $f(0, z, \overline{y}) = 0$ has a finite number of solutions (otherwise, the system has infinitely many solutions). Then, the number of solutions of the system with $a_i = t_j = 0$ for all i, j is no more than the minimum between the (computable) bounds on the number of solutions of these two equations.
If $t_j = 0$, there is two cases:

1. The equation $f(0, Z, \overline{y}) = 0$ has a finite number of solutions. In this case, there is a computable bound $S(f)$ of this number (determined by $d(f)$ by Strassmann theorem). Also, as remarked before, for z fixed, the a_i's are uniquely determined and the t_i's are unique up to permutation. So, number of solutions of the system with t_j is no more than $S(f) \cdot (s+1)!$ in this case.

2. If the equation $f(0, Z, \overline{y}) = 0$ has infinitely many solutions, then any $z \in \mathcal{O}_p$ is solution of this equation. So, the number of solutions of our system with $t_j = 0$ is the same that the number of solutions of the subsystem where one removes the equation $f(t_j, Z, \overline{y}) = 0$ and fix $t_j = 0$ in the others. This number is computable by inductive hypothesis and theorem 4.2.3.

As a bound for the number of solutions when $t_j = 0$, we take the maximum of the bounds obtained in each case.
Similarly, if $a_i = 0$, it means that the function $a_i(Z, \overline{y})$ vanishes at z.

1. If this function has finitely many roots, the (finite) number of solutions of the system is no more than $(s+1)!$ times the (finite) number of solutions of the system
$$f(t_0, z, \overline{y}) = \cdots = f(t_s, z, \overline{y}) = D \cdot \begin{pmatrix} g(t_0, \overline{y}) \\ \vdots \\ g(t_s, \overline{y}) \end{pmatrix} = 0$$
where D is the ith line of the matrix
$$\begin{pmatrix} 1 & \cdots & t_0^s \\ \vdots & & \vdots \\ 1 & \cdots & t_s^s \end{pmatrix}^{-1}.$$

The number of roots of this system is computable by inductive hypothesis and theorem 4.2.3.

2. If $a_i(z, \overline{y}) = 0$ for all z, one simply removes the equation defining a_i and fix $a_i = 0$ in the others. The number of solution of the new system has to be finite and we can bound this number by induction.

As a bound for the number of solutions when $a_i = 0$, we take the maximum of the bounds obtained in each case.

Then, we take the sum of the bounds obtained in each case. It gives us a bound for the number of solutions of the above system in $(\mathcal{O}_p)^{2s+3} \times (\mathbb{C}_p)^{(s^2+s)/2}$.

We proceed similarly for the definitions of the Weierstrass coefficients in the cases where the t_i's have multiplicities greater than 1. A bound for $d(h)$ is given by the sum of the bounds obtained in all possible cases.

Let h' be a derivative of h. We can compute $d(h')$ in a similar way using the definitions given in the claims 3 and 4 in proposition 3.4.1.

□

The cases where h is equal to a function Q like in (e) or one of its derivative is obtained similarly using systems given in proposition 3.4.1. With the same argument, we can compute $d(H)$ for a general function in $W^{(m+1)}_{\widetilde{F},n}$. Indeed, H is just a polynomial combination of functions of type (a)-(e) and so is also determined by a system of equations whose functions (and their derivatives) have an effective Weierstrass bound (see proposition 3.4.1).

□

4.4 Special case: the p-adic exponential ring

In this section, we will discuss the results of chapter 3 and of section 4.3 of this chapter in the special case $F = \{E_p\}$. In this case, $\mathcal{L}_F$ is the language $\mathcal{L}_{exp}$ of p-adic exponential rings.

First, let us remark that the set of $\mathcal{L}_F$-terms is closed under derivation. So, the theorem 3.4.2 can be applied: the theory of $\mathbb{Z}_{p,\widetilde{F}}$ in the language of p-adic exponential rings expanded by decomposition functions is strongly model-complete.

However, note that we dont need to add all decomposition functions in the language. Indeed, let $K_n = \mathbb{Q}_p(\beta_n)$ as defined in chapter 3. As $E_p(\sum x_j\beta_n^j) = \prod E_p(x_j\beta_n^j)$, it is sufficient to add the decomposition functions of $E_p(x_j\beta_n^j)$ for each j, n. Say,

$$E_p(x\beta_n^j) = \widetilde{c}_{0,j,n}(x) + \widetilde{c}_{1,j,n}(x)\beta_n + \cdots + \widetilde{c}_{N_n-1,j,n}(x)\beta_n^{N_n-1}.$$

Once again, the functions $\widetilde{c}_{i,j,n}$ can be obtained as linear combinations of the $E(x_j\beta_n^j)$ determined by the relation:

$$\Big(\widetilde{c}_{i,j,n}(x)\Big)_{i<N_n} = V^{-1}\Big(E_p((\beta_n^j)^\sigma x)\Big)_{\sigma\in Gal(K_n/\mathbb{Q}_p)},$$

where V is the Vandermonde matrix of the roots of P_{β_n}, the minimal polynomial of β_n over $\mathbb{Z}_p$. These are the p-adic versions of the identities $\cos x = \frac{e^{\sqrt{-1}x}+e^{-\sqrt{-1}x}}{2}$ and $\sin x = \frac{e^{\sqrt{-1}x}-e^{-\sqrt{-1}x}}{2\sqrt{-1}}$ in the complex field.
Note that it may happen that $v(\det V) > 0$ in the above relation, which is a slight issue in some of our proofs. For this reason, we will work with the functions $c_{i,j,n} := \widetilde{c}_{i,j,n} \cdot N(\det V)$, where $N = N_{K_n|\mathbb{Q}_p}$ is the norm from K_n over $\mathbb{Q}_p$. The functions $c_{i,j,n}$ are called *trigonometric functions.*
We will consider the theory of $\mathbb{Z}_p$ in the language of rings expanded by the predicates P_k ($k \in \mathbb{N}$), the functions E_p and $c_{i,j,n}$, $n \in \mathbb{N}$, $0 \leq i, j < N_n$. This language will be denoted by $\mathcal{L}_{pEC}$. Let $\mathbb{Z}_{pEC}$ denote the structure with underlying set $\mathbb{Z}_p$ and natural interpretations for the symbols in this language. Like in chapter 3, $\mathbb{Z}_{pEC}$ is strongly model-complete. This case was first proved by A. Macintyre ([8], unpublished).
It turns out that this model-completeness result is effective. For this, by theorem 4.3.1, it is sufficient to show that the set of $\mathcal{L}_{pEC}$-terms satisfies hypothesis (W). We will give a proof of this fact. This proof is due to A. Macintyre in [8].

First, we prove the following technical lemma:

Lemma 4.4.1. *There exist computable functions $B(f), C(f) : \mathbb{Z}_p[x,\overline{y}]^{E_p} \to \mathbb{Q}_{\geq 0}$ such that $C(f) \neq 0$ and for all $f \in \mathbb{Z}[x,\overline{y}]^{E_p}$, for all $\lambda \in \mathbb{Z}_p^*$, for all $\overline{\beta} \subset \mathbb{Z}_p$, if for all k,*

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k f}{\partial x^k}(0,\overline{\beta})\right) \geq 0,$$

then, for all $\alpha \in \mathbb{Z}_p$, for all $k \geq B(f)$,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k f}{\partial x^k}(\alpha,\overline{\beta})\right) \geq k \cdot C(f).$$

Remark. In this lemma, we will denote the function E_p by E. Note that we only prove the case $p \neq 2$ but it should be obvious how one can compute the functions B and C in the case $p = 2$.

Proof. We proceed by induction on $d_x(f)$ the degree of f in x (see chapter 2 section 2.2.2).

If $d_x(f) = 0$, we set $B(f) = C(f) = 1$.

Suppose now $d_x(f) > 0$. Then, by lemma 2.2.6, we can effectively construct g such that $d_x(g) < d_x(f)$ and $d_x\left(\frac{\partial E(-g)f}{\partial x}\right) < d_x(f)$. By inductive hypothesis, we can compute $B(g), C(g), B\left(\frac{\partial E(-g)f}{\partial x}\right)$ and $C\left(\frac{\partial E(-g)f}{\partial x}\right)$.

(a) We find $B(E(-g)f), C(E(-g)f)$ as follows:

Take $\lambda \neq 0$ and assume for all k,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k E(-g)f}{\partial x^k}(0,\overline{\beta})\right) \geq 0.$$

Then, in particular, for all k,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k}{\partial x^k}\left(\frac{\partial E(-g)f}{\partial x}\right)(0,\overline{\beta})\right) \geq v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^{k+1}E(-g)f}{\partial x^{k+1}}(0,\overline{\beta})\right) - v(k+1) \geq 0.$$

So, by inductive hypothesis,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k}{\partial x^k}\left(\frac{\partial E(-g)f}{\partial x}\right)(\alpha,\overline{\beta})\right) \geq k \cdot C\left(\frac{\partial E(-g)f}{\partial x}\right),$$

for all $k \geq B\left(\frac{\partial E(-g)f}{\partial x}\right)$.

It means that

$$\begin{aligned} v\left(\frac{1}{\lambda}\frac{1}{(k+1)!}\frac{\partial^{k+1}E(-g)f}{\partial x^{k+1}}(\alpha,\overline{\beta})\right) &\geq k.C\left(\frac{\partial E(-g)f}{\partial x}\right) - v(k+1) \\ &= (k+1)\left[\frac{k}{k+1}C\left(\frac{\partial E(-g)f}{\partial x}\right) - \frac{v(k+1)}{k+1}\right]. \end{aligned}$$

But, as $v(k+1) \leq \log_p(k+1)$, $\frac{v(k+1)}{k+1} \to 0$ as $k \to \infty$ and $\frac{k}{k+1} \geq \frac{1}{2}$ for all k. So, we define

$$C(E(-g)f) = \frac{1}{2}C\left(\frac{\partial E(-g)f}{\partial x}\right) - \frac{\log_p \mu}{\mu},$$

where μ is the least integer such that $\frac{\log_p \mu}{\mu} < \frac{1}{2}C\left(\frac{\partial E(-g)f}{\partial x}\right)$. We set

$$B(E(-g)f) = B\left(\frac{\partial E(-g)f}{\partial x}\right) + \mu.$$

(b) We find $B(E(g)), C(E(g))$ as follows:

First, note that $v(E(g(0,\overline{y}))) = 0$ for all $\overline{y}$. Therefore, if for all k,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k E(g(0,\overline{y}))}{\partial x^k}\right) \geq 0,$$

then $v(\lambda) \leq 0$. So, without loss of generality, we may assume $\lambda = 1$.

Let $h := E(g)$. Then,

$$\frac{\partial h}{\partial x} = p\frac{\partial g}{\partial x}h.$$

And, by induction, we can show that for all k,

$$\frac{1}{k!}\frac{\partial^{k+1}h}{\partial x^{k+1}} = p\sum_{i+j=k}\frac{1}{i!}\frac{\partial^{i+1}g}{\partial x^{i+1}}\frac{1}{j!}\frac{\partial^j h}{\partial x^j}.$$

So, for all k,

$$v\left(\frac{1}{k!}\frac{\partial^{k+1}h}{\partial x^{k+1}}\right) \geq 1.$$

Also, let us remark that if $k+1 \geq B(g)$ and $(k+1)C(g) \geq 1$,then

$$v\left(\frac{1}{k!}\frac{\partial^{k+1}g}{\partial x^{k+1}}\right) \geq 1.$$

So, for all $k+1 \geq \max\{B(g), C(g)^{-1}\}$,

$$v\left(\frac{1}{k!}\frac{\partial^{k+1}h}{\partial x^{k+1}}\right) \geq 2.$$

Let $D(g) := \max\{B(g), C(g)^{-1}\}$ and $k_{n+1} := (n-1)D(g)$. By induction, we show that

Claim 6. *For all $k+1 \geq k_n$,*

$$v\left(\frac{1}{k!}\frac{\partial^{k+1}h}{\partial x^{k+1}}\right) \geq n.$$

We have already proved the claim for $n = 1, 2$. So, we assume that the property is true for all $l \leq n$ and prove the claim for $n+1$.

Let $i + j = k$. It is sufficient to show that

$$v\left(\frac{1}{i!}\frac{\partial^{i+1}g}{\partial x^{i+1}}\frac{1}{j!}\frac{\partial^j h}{\partial x^j}\right) \geq n.$$

First, let us remark that if $j \geq k_n$, the above inequality holds by inductive hypothesis.

In general, if $k_s \leq j < k_{s+1}$ for some $0 \leq s < n$, then

$$v\left(\frac{1}{j!}\frac{\partial^j h}{\partial x^j}\right) \geq s.$$

In this case, we have that $k - k_{s+1} < i \leq k - k_s$. So, if $k + 1 \geq k_{n+1}$, $i + 1 \geq (k_{n+1} - k_{s+1}) = (n - s)D(g)$. Therefore, $i + 1 \geq B(g)$ and $(i + 1)C(g) \geq n - s$. So,

$$v\left(\frac{1}{i!}\frac{\partial^{i+1}g}{\partial x^{i+1}}\right) \geq n - s.$$

This proves the claim.

By the claim, for all $k + 1 \geq nD(g)$,

$$v\left(\frac{1}{k!}\frac{\partial^{k+1}h}{\partial x^{k+1}}\right) \geq n.$$

So,

$$v\left(\frac{1}{k!}\frac{\partial^{k+1}h}{\partial x^{k+1}}\right) \geq (k+1)c,$$

if we find n, c such that $n \geq (k + 1)c$ and $(k + 1) \geq nD(g)$.

Let $c = \frac{1}{2}D(g)^{-1}$. Then, for all $k + 1 \geq 4D(g)$, let $n = \lceil (k + 1)c \rceil$.

We have that $(k + 1)c \leq n \leq (k + 1)c + 1$. So,

$$\frac{n}{k+1} \leq c + \frac{1}{k+1} \leq \frac{1}{2}D(g)^{-1} + \frac{1}{4}D(g)^{-1} \leq D(g)^{-1}.$$

It means that we have found n such that $n \geq (k + 1)c$ and $(k + 1) \geq nD(g)$.

So, for all $k + 1 \geq 4D(g)$,

$$v\left(\frac{1}{k!}\frac{\partial^{k+1}h}{\partial x^{k+1}}\right) \geq (k+1)c,$$

which implies

$$\begin{aligned} v\left(\frac{1}{(k+1)!}\frac{\partial^{k+1}h}{\partial x^{k+1}}\right) &= v\left(\frac{1}{k!}\frac{\partial^{k+1}h}{\partial x^{k+1}}\right) - v(k+1) \\ &\geq (k+1)c - v(k+1) = (k+1)\Big(c - \frac{v(k+1)}{k+1}\Big) \\ &\geq (k+1)\Big(c - \frac{\log_p(k+1)}{k+1}\Big). \end{aligned}$$

Let N be the least integer such that $\frac{\log_p(N+1)}{N+1} < c/2$. The following functions satisfy the properties of the lemma:

$$\begin{aligned} &C(E(g)) := c/2 = \tfrac{1}{4}D(g)^{-1}, \\ &B(E(g)) = N + 4D(g). \end{aligned}$$

(c) Finally, we find $B(f), C(f)$ as follows:

Let us remark that $f = E(g)\cdot(E(-g)f)$. By (a) and (b), we know the functions B and C relative to $E(g)$ and $E(-g)f$. This will allow us to compute $B(f)$ and $C(f)$. By Leibniz's rule,

$$\frac{1}{k!}\frac{\partial^k E(-g)f}{\partial x^k} = \sum_{i+j=k}\left[\frac{1}{i!}\frac{\partial^i E(-g)}{\partial x^i}\frac{1}{j!}\frac{\partial^j f}{\partial x^j}\right].$$

So, assume that for all k,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k f}{\partial x^k}(0,\overline{\beta})\right) \geq 0.$$

Then, for all k,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k E(-g)f}{\partial x^k}(0,\overline{\beta})\right) \geq 0.$$

We take:

$$C(f) = \frac{1}{2}\min\{C(E(g)), C(E(-g)f)\},$$
$$B(f) = 2\max\{B(E(g)), B(E(-g)f)\}.$$

Assume $k \geq B(f)$. By Leibniz's rule again,

$$\frac{1}{k!}\frac{\partial^k}{\partial x^k}\left(\frac{1}{\lambda}f\right) = \sum_{i+j=k}\left[\frac{1}{i!}\frac{\partial^i E(g)}{\partial x^i}\frac{1}{j!}\frac{\partial^j}{\partial x^j}\left(\frac{1}{\lambda}E(-g)f\right)\right].$$

Fix i, j such that $i+j=k$. Then, either $i \geq k/2 \geq B(f)/2$ or $j \geq k/2 \geq B(f)/2$. In the first case, $i \geq B(E(g))$. So,

$$\begin{aligned} v\left(\frac{1}{i!}\frac{\partial^i E(g)}{\partial x^i}\frac{1}{j!}\frac{\partial^j}{\partial x^j}\left(\frac{1}{\lambda}E(-g)f\right)\right) &\geq v\left(\frac{1}{i!}\frac{\partial^i E(g)}{\partial x^i}\right)\\ &\geq iC(E(g)) \geq 2iC(f)\\ &\geq kC(f). \end{aligned}$$

In the second case, $j \geq B(E(-g)f)$. So,

$$\begin{aligned} v\left(\frac{1}{i!}\frac{\partial^i E(g)}{\partial x^i}\frac{1}{j!}\frac{\partial^j}{\partial x^j}\left(\frac{1}{\lambda}E(-g)f\right)\right) &\geq v\left(\frac{1}{j!}\frac{\partial^j}{\partial x^j}\left(\frac{1}{\lambda}E(-g)f\right)\right)\\ &\geq jC(E(-g)f) \geq 2jC(f)\\ &\geq kC(f). \end{aligned}$$

This completes the proof of the lemma.

□

Now, we can prove the existence of an effective Weierstrass bound for E-polynomials:

Proposition 4.4.2. *There exists a computable function $D(f) : \mathbb{Z}[x,\overline{y}]^{E_p} \longrightarrow \mathbb{N}$ such that for all E_p-polynomials $f(x,\overline{y}) \in \mathbb{Z}[x,\overline{y}]^{E_p}$, if $f(x,\overline{y}) = \sum_i a_i(\overline{y})x^i$ (where $a_i(\overline{y}) \in \mathbb{Z}_p\{\overline{y}\}$) and*

$$k(\overline{y}) = \max\{i \mid \ v(a_i(\overline{y})) = \min_j\{v(a_j(\overline{y}))\}\},$$

then, for all $\overline{\beta}$, either $k(\overline{\beta}) = \infty$ (i.e. $f(x,\overline{\beta})$ is identically zero) or $k(\overline{\beta}) \leq D(f)$.

Proof. Clearly, $a_i(\overline{y}) = \frac{1}{i!}\frac{\partial^i f}{\partial x^i}(0,\overline{y})$. Fix $\overline{\beta} \in \mathbb{Z}_p^m$ and assume $k(\overline{\beta})$ finite. Let $\lambda = a_t(\overline{\beta})$ where t is chosen as the maximal index such that the valuation of $a_i(\overline{\beta})$ is minimal. Then, for all i,

$$v\left(\frac{1}{\lambda}\frac{1}{i!}\frac{\partial^i f}{\partial x^i}(0,\overline{\beta})\right) \geq 0.$$

So, by lemma 4.4.1, for all $k \geq B(f)$,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k f}{\partial x^k}(0,\overline{\beta})\right) \geq kC(f) > 1 \text{ for } k > C(f)^{-1}.$$

It means that $v(a_k(\overline{\beta})) > \lambda$ for all $k > C(f)^{-1}$, $k \geq B(f)$. So, by choice of λ, $k(\overline{\beta}) \leq \max\{C(f)^{-1}, B(f)\}$. Take $D(f) = \max\{\lceil C(f)^{-1}\rceil, B(f)\}$. □

Extending this result to general $\mathcal{L}_{pEC}$-terms with one variable X should be obvious once we have extended lemma 4.4.1. Let us remark that, for all such terms f, there is a maximal integer such that one of the $c_{i,j,n}$ occurs in the terms. Let $\theta(f)$ be this integer. Then, for all $m \geq \theta(f)$, f defines a function from V_m to V_m.

Lemma 4.4.3. *There exist computable functions B and C from the set of $\mathcal{L}_{pEC}$-terms to $\mathbb{Q}_{\geq 0}$ such that $C(f) \neq 0$ and for all $f(X,\overline{Y})$, for all $m \geq \theta(f)$, for all $\lambda \in V_m^*$ and for all $\alpha, \overline{\beta} \subset V_m$, if for all k,*

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k f}{\partial x^k}(0,\overline{\beta})\right) \geq 0,$$

then, for all $\alpha \in V_m$, for all $k \geq B(f)$,

$$v\left(\frac{1}{\lambda}\frac{1}{k!}\frac{\partial^k f}{\partial x^k}(\alpha,\overline{\beta})\right) \geq k \cdot C(f).$$

Proof. We reduce this lemma to lemma 4.4.1. Consider a subterm $c_{i,k,n}(g)$ occuring in f, we want to replace this term by a linear combination of E_p-polynomials. We know that there exist $\gamma_0, \cdots, \gamma_{\theta(f)-1}$ and $\delta_{11}, \cdots, \delta_{(\theta(f)-1)(\theta(f)-1)}$ in $V_{\theta(f)}$ such that:

$$c_{i,k,n}(x) = \sum \delta_{ij}E(\gamma_j x).$$

We replace the γ_i and δ_{ij} by new free variables t_i and u_{ij}. We substitute the subterm $c_{i,k,n}(g)$ by the term $\sum u_{ij}E(t_jg)$. We carefully replace any occurence of a $c_{i,k,n}$ and construct an exponential polynomial $f^+(x,\overline{y},\overline{t},\overline{u})$. Let us remark that for all $\alpha,\overline{\beta} \subset V_{\theta(f)}$, we have:

$$f(\alpha,\overline{\beta}) = f^+(\alpha,\overline{\beta},\overline{\gamma},\overline{\delta}).$$

And similarly for all the derivatives (with respect to X). Inspecting the proof of lemma 4.4.1, one can see that it works uniformly over V_m. The functions B and C are therefore computable using this latter. □

And we can easily extend proposition 4.4.2:

Proposition 4.4.4 (A. Macintyre [8]). *There exists a computable function $D(f)$ from the set of $\mathcal{L}_{pEC}$-terms to $\mathbb{N}$ such that for all $\mathcal{L}_{pEC}$-terms $f(x,\overline{y})$ (say, $f(x,\overline{y}) = \sum_i a_i(\overline{y})x^i$ where $a_i(\overline{y}) \in \mathbb{Z}_p\{\overline{y}\}$) and*

$$k(\overline{y}) := \max\{i \mid \ v(a_i(\overline{y})) = \min_j\{v(a_j(\overline{y}))\}\},$$

then, for all $\overline{\beta}$, either $k(\overline{\beta}) = \infty$ (i.e. $f(x,\overline{\beta})$ is identically zero) or $k(\overline{\beta}) \leq D(f)$.

The above proposition tells us exactly that the set of $\mathcal{L}_{pEC}$-terms satisfies the hypothesis (W). From this and theorem 4.3.1, it follows

Theorem 4.4.5. *The theory of $\mathbb{Z}_{pEC}$ in the language $\mathcal{L}_{pEC}$ is effectively strongly model-complete.*

Chapter 5

Decidability

We are now interested by the decidability of the full theory of $\mathbb{Z}_{p,exp}$. In chapter 4, we have proved that the theory of the corresponding $\mathcal{L}_{pEC}$-structure is effectively model-complete. It implies that the problem of the decidability can be reduced to the following question: is there an algorithm $\mathcal{A}$ which takes for entry an existential $\mathcal{L}_{pEC}$-sentence and which returns true if this sentence is true in $\mathbb{Z}_p$? Let us remark that we do not require that this algorithm returns false (or stops) if the formula is false. Indeed, let Ψ be an existential $\mathcal{L}_{pEC}$-sentence. Then, by effective model-completeness, we can compute an existential $\mathcal{L}_{pEC}$-formula φ equivalent to $\neg\Psi$. We can run in parallel the algorithm $\mathcal{A}$ for the sentences Ψ and φ. One of the two procedure eventually stops and returns true. This determines the truth value of our formula Ψ in $\mathbb{Z}_p$.

We are now given an existential sentence Ψ in $\mathcal{L}_{pEC}$. It is not hard to see that such a formula is effectively equivalent to a disjunction of formulas of the type:

$$\exists x_1 \cdots \exists x_n \; f(\overline{x}) = 0 \wedge g(\overline{x}) \neq 0,$$

where f and g are $\mathcal{L}_{pEC}$-terms. Indeed, it is easy to reduce Ψ to a disjunction of conjunctions of equalities and inequalities. And, because

$$\text{for all } x, y \in \mathbb{Z}_p, \; (x, y) = (0, 0) \text{ iff } x^2 + py^2 = 0,$$

a system of equalities is equivalent to a single equation. First, we will discuss the case where f, g are $\mathcal{L}_{exp}$-terms. We will see later how we can extend our results to the general case.

Our strategy is very similar to the strategy used for the same problem in the real case

(see [11]). In particular, the use of Newton algorithm is here substituted by Hensel's lemma:
Let $f_1, \cdots, f_n$ be $\mathcal{L}_{exp}$-terms with n variables. We can determine if the system $(f_1, \cdots, f_n)$ has non-singular roots in $\mathbb{Z}_p^n$ using the analytic Hensel's lemma 2.1.7. Indeed, assume that there exists $\bar{b} \in \mathbb{Z}_p^n$ such that

$$f_1(\bar{b}) = \cdots = f_n(\bar{b}) = 0 \neq det\ J_f(\bar{b}),$$

where J_f denotes the Jacobian of the system $f = (f_1, \cdots, f_n)$. Then, because $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, there exists $\overline{a} \in \mathbb{Z}^n$ such that

$$det\ J_f(\overline{a}) \neq 0 \text{ and } v(f(\overline{a})) > 2 \cdot v(det\ J_f(\overline{a})).$$

Conversely if such a $\overline{a} \in \mathbb{Z}^n$ exists, by the analytic Hensel's lemma, our system has a non-singular solution in $\mathbb{Z}_p$. So, the following algorithm stops and returns true if the formula

$$\exists x_1 \cdots \exists x_n\ det\ J_f(\overline{x}) \neq 0 \bigwedge_i f_i(\overline{x}) = 0$$

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

Algorithm 1. *Let $\overline{a_1}, \overline{a_2}, \cdots$ be an enumeration of $\mathbb{Z}^n$.*
For all i, if

$$det\ J_f(\overline{a_i}) \neq 0 \textit{ and } v(f(\overline{a_i})) > 2 \cdot v(det\ J_f(\overline{a_i})),$$

return true. Otherwise, go to the next step in the enumeration.

Let us note that this procedure runs forever if the system $f_1, \cdots, f_n$ doesn't have a non-singular solution in $\mathbb{Z}_p^n$.
In the first section of this chapter, we will prove that for any $\mathcal{L}_{exp}$-term g with n variables, there exists a system $f = (f_1, \cdots, f_n)$ of $\mathcal{L}_{exp}$-terms such that g has a solution which is also a non-singular solution of f. As we have seen, the existence of this latter solution can be checked effectively. We will see in section 5.2 that, assuming a conjecture in transcendence degree theory, it implies the decidability of $\mathbb{Z}_{p,exp}$. We will discuss a bit more the role of this conjecture in sections 5.2.3 and 5.3: in section 5.3, we will give a weaker conjecture that also implies (and in fact, is equivalent to) the decidability of our theory. In section 5.2.3, we will see that we can determine the truth of some sentences with one existential quantifier unconditionnally.

5.1 Desingularization of exponential systems

Let F be a subset of $\mathbb{Z}_p\{\overline{X}\}$. We assume that the set of $\mathcal{L}_F$-terms is closed under derivation. The example that we have in mind is the case where F is the set of trigonometric functions and E_p.

In this section, we consider a system of equations $f = (f_1, \cdots, f_n)$ where the $f_i's$ are $\mathcal{L}_F$-terms with m variables. Assuming that the above system has a solution in $\mathbb{Z}_p$, we want to show that there exists a system of $\mathcal{L}_F$-terms $g = (g_1, \cdots, g_m)$ such that there is a non-singular zero of the system g which is also a zero of the system f. We will actually prove the result for all finite algebraic extensions of $\mathbb{Q}_p$. This result is the p-adic version of theorem 5.1 in [17]. We will work with Noetherian differential rings like in [17]. The outline of the proof is actually the same that in the real case.

Within this section, K will denote a finite algebraic extension of $\mathbb{Q}_p$. The implicit function theorem will play an important role in our proof. We state now this result in the p-adic context.

In chapter 2, we have defined the differential $Df(\overline{a})$ of an analytic map. Given a linear map A between K^{n+m} and K^n, we can define two linear maps $A_x : K^n \longrightarrow K^n : \overline{h} \longmapsto A(\overline{h}, 0)$ and $A_y : K^m \longrightarrow K^n : \overline{k} \longmapsto A(0, \overline{k})$. Then, $A(\overline{h}, \overline{k}) = A_x\overline{h} + A_y\overline{k}$. In the case where $A = Df(\overline{a})$ as above, the matrix associated to A_x is the matrix composed of the partial derivatives with respect to the nth first variables. Similarly, A_y is the matrix composed of the partial derivatives with respect to the mth last variables.

Using these notations, we state the p-adic analytic implicit function theorem (see [2] for instance):

Theorem 5.1.1 (Implicit function theorem). *Let $f : U \times V \to K^m$ be an analytic map (where $U \times V$ is an open subset of $K^n \times K^m$) such that $f(\overline{a}, \overline{b}) = 0$ for some $(\overline{a}, \overline{b}) \in U \times V$. Let $A = Df(\overline{a}, \overline{b})$. Assume A_y invertible. Then, there exist $U_1 \subset U$ and $U_2 \subset V$, both open and containing $\overline{a}$ and $\overline{b}$ respectively, such that for all $\overline{x} \in U_1$ there is a unique $\overline{y} \in U_2$ with $f(\overline{x}, \overline{y}) = 0$.*

Furthermore, the map g defined by $g(\overline{x}) = \overline{y}$ from U_1 to U_2 is analytic and satisfies $g(\overline{a}) = \overline{b}$, $f(\overline{x}, g(\overline{x})) = 0$ for all $\overline{x} \in U_1$ and $Dg(\overline{x}) = -A_y^{-1}A_x$.

Let us remark that if the function f and the open sets U, V are definable, then so is the function g. Indeed, we can assume that the U_i's are open balls and the function g is determined by the relations $(\overline{x}, g(\overline{x})) \in U_1 \times U_2$ and $f(\overline{x}, g(\overline{x})) = 0$. Also, the derivatives of g are definable via the relation $Dg(\overline{x}) = -A_y^{-1} A_x$.

We are now given a system $f_1, \cdots, f_n$ of $\mathcal{L}_F$-terms. We first observe that such a system can be reduced to a single equation in K : indeed, as $v(\mathcal{O}_K) = \frac{1}{e}\mathbb{Z}$ for some $e \in \mathbb{N}$:

$$\text{for all } x, y \in K,\ (x, y) = (0, 0) \text{ iff } x^2 + \pi y^2 = 0,$$

where π is an element of minimal positive valuation.
So, we can consider systems with a single $\mathcal{L}_F$-term. We view K as a $\mathcal{L}_F$-structure (where $f \in F$ is interpreted by the map restricted to the valuation ring, i.e. the interpretation of f takes value $f(x)$ for $x \in \mathcal{O}_K$ and value 0 for $x \notin \mathcal{O}_K$). We also add to the language $\mathcal{L}_F$ symbols for the language of rings and constant symbols for a basis of K over $\mathbb{Q}_p$ (such that this basis is also a basis of $\mathcal{O}_K$ over $\mathbb{Z}_p$). We are interested by the local behaviour of the definable analytic maps (especially, in what happens in the valuation ring). We consider the ring of such maps where we identify two maps which coincide on a open set i.e. the ring of germs:

Definition 5.1.2. *Given a* neighbourhood system $\mathcal{N}$ *in* K^n *(i.e. a non-empty collection of non-empty open* $\mathcal{L}_F$*-definable subsets of* K^n *closed under finite intersection),* $\mathfrak{G}^{(n)}(\mathcal{N})^-$ *is the set of all* $\langle f, U\rangle$ *where* $U \in \mathcal{N}$ *and* $f : U \longrightarrow K$ *is a* $\mathcal{L}_F$*-definable function such that* f *is analytic on* U*.*
We define an equivalence relation on $\mathfrak{G}^{(n)}(\mathcal{N})^-$ *by:*
$\langle f_1, U_1\rangle \sim \langle f_2, U_2\rangle$ *iff* f_1 *and* f_2 *coincide on a neighbourhood i.e. there is* $U \in \mathcal{N}$ *such that* $U \subseteq U_1 \cap U_2$ *and for all* $x \in U$, $f_1(x) = f_2(x)$*. We denote by* $[f, U]$ *the class of* $\langle f, U\rangle$*.*
The ring of germs *is the set* $\mathfrak{G}^{(n)}(\mathcal{N}) = \mathfrak{G}^{(n)}(\mathcal{N})^-/\!\sim$ *equipped with the natural operations of addition and multiplication.*

Let us remark that $\mathfrak{G}^{(n)}(\mathcal{N})$ is a unital differential ring.

As a special case of neighbourhood system, we have the collection of all definable open neighbourhoods of a point P. We denote the ring of germs in this case by $\mathfrak{G}^{(n)}(P)$. Let $P \in K^l$ and $Q \in K^m$ and let $f_1, \cdots, f_m$ be analytic maps in $\mathfrak{G}^{(l+m)}(P, Q)$. Let $f = (f_1, \cdots, f_m)$. Assume that $f(P, Q) = 0$ and $\det J_f(P, Q) \neq 0$ i.e. $f_i(P, Q) = 0$ for all i and

$$\det \begin{pmatrix} \frac{\partial f_1}{\partial x_{l+1}}(P, Q) & \cdots & \frac{\partial f_1}{\partial x_{l+m}}(P, Q) \\ \vdots & & \vdots \\ \frac{\partial f_m}{\partial x_{l+1}}(P, Q) & \cdots & \frac{\partial f_m}{\partial x_{l+m}}(P, Q) \end{pmatrix} \neq 0,$$

i.e. $f_i(P, Q) = 0$ for all i and the vectors

$$\left(\frac{\partial f_1}{\partial x_{l+1}}(P, Q), \cdots, \frac{\partial f_1}{\partial x_{l+m}}(P, Q)\right), \cdots, \left(\frac{\partial f_m}{\partial x_{l+1}}(P, Q), \cdots, \frac{\partial f_m}{\partial x_{l+m}}(P, Q)\right)$$

are K-linearly independent. We denote these vectors by $d_{P,Q} f_i$. By the analytic implicit function theorem, there are $U_P \times U_Q \subset U$ and $\Phi' = (\Phi_{l+1}, \cdots, \Phi_{l+m})$ analytic from U_P to U_Q such that $f_i(\overline{x}, \Phi_{l+1}(\overline{x}), \cdots, \Phi_{l+m}(\overline{x})) = 0$ for all $\overline{x} \in U_P$.
As the f_i's and U are definable, this guarantees that the map Φ' is definable analytic. Therefore, Φ' determines a germ in $\mathfrak{G}^{(l)}(P)$.
Let $\Phi(\overline{x}) = (\Phi_1(\overline{x}), \cdots, \Phi_{l+m}(\overline{x}))$ where $\Phi_i(\overline{x}) = x_i$ for $i \leq l$ and Φ_{l+i} as above. We denote the morphism of rings

$$\begin{array}{rcl} \mathfrak{G}^{(l+m)}(P, Q) & \longrightarrow & \mathfrak{G}^{(l)}(P) \\ [f, U] & \longmapsto & [f(\Phi), U] \end{array}$$

by $\widehat{\quad}$. The kernel of this map is the set of germs which vanish (locally) on the set of zeros of the system $(f_1, \cdots, f_m)$ around (P, Q). In particular, $\hat{f}_i \equiv 0$ (and therefore, $\frac{\partial \hat{f}_i}{\partial x_j} \equiv 0$) in $\mathfrak{G}^{(l)}(P)$.

Lemma 5.1.3. *Let $f_1, \cdots, f_m$, (P, Q) as above. For all $g \in \mathfrak{G}^{(l+m)}(P, Q)$, $d_{P,Q} f_1, \cdots d_{P,Q} f_m, d_{P,Q} g$ are linearly independent over K iff $d_P \hat{g} \neq 0$.*

The proof is word to word the same that lemma 4.7 in [17].

Proof. Let $f_{m+1} = g$. Assume that $\sum a_i d_{P,Q} f_i = 0$ with at least one non-zero a_i. Then, as $d_{P,Q} f_1, \cdots, d_{P,Q} f_m$ are K-linearly independent, $a_{m+1} \neq 0$. Also, using the chain rule, we can deduce the relations:

$$\frac{\partial \hat{f}_i}{\partial x_j}(P) = \sum_l \frac{\partial f_i}{\partial x_l}(P, Q) \frac{\partial \Phi_l}{\partial x_j}(P) \ (*).$$

But, by definition of the map $\widehat{\quad}$, for $i \leq m$, $\frac{\partial \hat{f}_i}{\partial x_j}$ vanishes on a neighbourhood of P and therefore using the two above equalities, we find:

$$\frac{\partial \hat{f}_{m+1}}{\partial x_j}(P) = a_{m+1}^{-1} \sum_{i \leq m+1} a_i \frac{\partial \hat{f}_i}{\partial x_j}(P) = \sum_l \frac{\partial \Phi_l}{\partial x_j}(P) \left(\sum_i a_i \frac{\partial f_i}{\partial x_l}(P, Q) \right) = 0,$$

or equivalently $d_p \hat{g} = 0$.

Conversely, if $d_{P,Q} f_1, \cdots, d_{P,Q} f_{m+1}$ are linearly independent. We denote by A the $n \times (m+1)$ matrix with columns $d_{P,Q} f_i$. Then, by linear independence of the above vectors, $\ker A$ has dimension $n - (m+1) = l - 1$. Using, the equality $(*)$, we deduce that:

$$\left(\frac{\partial \Phi_1}{\partial x_j}(P), \cdots, \frac{\partial \Phi_n}{\partial x_j}(P) \right) \cdot A = \left(0, \cdots, 0, \frac{\partial \hat{f}_{m+1}}{\partial x_j}(P) \right).$$

Therefore, as by definition $\frac{\partial \Phi_i}{\partial x_j}(P) = \delta_{ij}$ (the Kronecker symbol) for all $1 \leq i, j \leq l$, the vectors $\left(\frac{\partial \Phi_1}{\partial x_j}(P), \cdots, \frac{\partial \Phi_n}{\partial x_j}(P) \right)$ for $1 \leq j \leq l$ are linearly independent. So, at least one of these vectors does not lie in $\ker A$ which means that $\frac{\partial \hat{f}_{m+1}}{\partial x_j}(P) \neq 0$ for some $j \leq l$, i.e. $d_P \hat{g} = 0$. □

We fix now some notations: let $f_1, \cdots, f_m : U \longrightarrow K$ be analytic functions (where $U \subset K^n$ open). Then,

$$V(f_1, \cdots, f_m) = \{ P \in U \mid f_1(P) = \cdots = f_m(P) = 0 \},$$
$$V^{ns}(f_1, \cdots, f_m) = \{ P \in V(f_1, \cdots, f_m) \mid d_P f_1, \cdots, d_P f_m \text{ are } K\text{-linearly independent} \}.$$

Proposition 5.1.4. *Let $P \in K^n$ and let M be a Noetherian subring of $\mathfrak{G}^{(n)}(P)$ closed under differentiation. Let $m \in \mathbb{N}$ and $[f_1, U_1], \cdots, [f_m, U_m] \in M$. Assume $P \in V^{ns}(f_1, \cdots, f_m)$. Then, exactly one of the following is true:*

(a) n=m; or,

(b) m<n and for all $[h, W] \in M$ with $h(P) = 0$, h vanishes on $U \cap V^{ns}(f_1, \cdots, f_m)$ for some U open neighbourhood of P; or,

(c) m<n and for some $[h, W] \in M$, $P \in V^{ns}(f_1, \cdots, f_m, h)$.

Again the proof is similar to the real case [17]. Note that for this proposition, we need to consider analytic functions in our case (instead of infinitely differentiable functions in [17]).

Proof. If $m < n$, say $n = l + m$, then the vectors $d_P f_1, \cdots, d_P f_m$ are linearly independent. Without loss of generality, we will assume that the matrix $A(P) = \left(\frac{\partial f_i}{\partial x_j}(P)\right)_{1\leq i\leq m, l+1\leq j\leq n}$ is invertible. Let λ be the map $\overline{x} \longmapsto \det A(\overline{x})$. On a neighbourhood U of P, this map is invertible. Let $\Lambda = [\lambda, U]$. We define $M^* := M[\Lambda^{-1}]$. Assume $P = (P_1, P_2) \in K^{l\times m}$. We define the $\widehat{\quad}$-map as before. Then, $\widehat{M^*}$, the image of M^* by this map, is Noetherian. And, by the implicit function theorem, we have

$$\begin{pmatrix} \frac{\partial \Phi_{l+1}}{\partial x_r} \\ \vdots \\ \frac{\partial \Phi_n}{\partial x_r} \end{pmatrix} = -\Lambda^{-1} \begin{pmatrix} \frac{\partial f_1}{\partial x_r} \\ \vdots \\ \frac{\partial f_m}{\partial x_r} \end{pmatrix},$$

which means that $\frac{\partial \Phi_i}{\partial x_j} \in M^*$. Therefore using the chain rule, we find that $\widehat{M^*}$ is closed under differentiation.

Let $I = \{g \in \widehat{M^*} \mid \ g(P_1) = 0\}$.

1. If $I = \{0\}$. Suppose $g = [h, W] \in M$ and $h(P) = 0$. Then, $\hat{g}(P_1) = 0$ and therefore $\hat{g} \in I$ i.e. $\hat{g} = 0$. By definition of the map $\widehat{\quad}$, it exactly means that h is vanishing on a neighbourhood of P in $V^{ns}(f_1, \cdots, f_m)$.

2. If $I \neq \{0\}$, I is not closed under differentiation. Otherwise for all $g \in I$, the partial derivatives of g vanish at P_1. This implies that all the coefficients of the power series defining g around P are zero and therefore $g = 0$ in $\widehat{M^*}$. So, there is $g \in M^*$ such that $\hat{g} \in I$ and $\frac{\partial \hat{g}}{\partial x_i} \notin I$. It means that $\hat{g}(P_1) = 0$ (i.e. $g(P) = 0$) and $\frac{\partial \hat{g}}{\partial x_i}(P_1) \neq 0$. But, for some integer s, $\Lambda^s g \in M$. Let $f = \Lambda^s g$. Then, $f(P) = 0$ and
$$\frac{\partial \hat{f}}{\partial x_i}(P_1) = \left(s\hat{\Lambda}^{s-1}(P_1)\frac{\partial \hat{\Lambda}}{\partial x_i}\hat{g}(P_1)\right) + \left(\hat{\lambda}^s(P_1)\frac{\partial \hat{g}}{\partial x_i}(P_1)\right) \neq 0.$$
So, $d_P\hat{f} \neq 0$ and therefore by lemma 5.1.3, $P \in V^{ns}(f_1, \cdots, f_m, f)$.

□

We are now able to state the desingularization theorem:

Let U be an open definable neighbourhood of the origin contained in $\mathcal{O}_K^n$. Then, $\{U\}$ forms a neighbourhood system. We denote the correspondent ring of germs by $\mathfrak{G}^{(n)}(U)$.

Let us recall that $K = \mathbb{Q}_p(\alpha_1, \cdots, \alpha_s)$ and that for this choice of $\alpha_1, \cdots, \alpha_s$, $\mathbb{Z}(\alpha_1, \cdots, \alpha_s)$ is dense in the valuation ring of K.

Theorem 5.1.5. *Let M be a Noetherian subring of $\mathfrak{G}^{(n)}(U)$ which contains $\mathbb{Z}(\overline{\alpha})[x_1, \cdots, x_n]$, is closed under differentiation and such that for all $g \in M$, the germ of g is equivalent to a definable analytic function given by a power series with coefficients in the valuation ring.*
Let $f \in M$. Assume that S is a non-empty definable subset of $V(f)$, open in $V(f)$. Then, there exist $f_1, \cdots, f_n \in M$ such that $S \cap V^{ns}(f_1, \cdots, f_n) \neq \varnothing$.

Our desingularization result is an immediate corollary of this theorem:
Let f be a $\mathcal{L}_F$-term. Then, we apply the above theorem with $U = \mathcal{O}_K$, M the ring generated over $\mathbb{Z}(\overline{\alpha})$ by the subterms of f and $S = V(f)$. The theorem exactly says that if $V(f) \neq \varnothing$, then there are $\mathcal{L}_F$-terms $f_1, \cdots, f_n$ and $\overline{a} \in \mathcal{O}_K^n$ such that

$$f(\overline{a}) = f_1(\overline{a}) = \cdots = f_n(\overline{a}) = 0 \neq det\ J_{(f_1, \cdots, f_n)}(\overline{a}).$$

Proof. First, for all $Q \in S$, we set $I_Q = \{g \in M \mid g(Q) = 0\}$. As M is Noetherian, there is some R in S such that I_R is maximal within the collection of all I_Q. Let $g_1, \cdots, g_N$ be generators of I_R and $g = \sum_i \pi^{2(i-1)} g_i^2$ (where π is a prime element of K which can be assumed to be one of the α_i). So, $g(x) = 0$ iff $g_i(x) = 0$ for all i. Then, $R \in V(g) \cap S$ and for all $Q \in V(g) \cap S$, $I_R = I_Q$.
Choose m maximal such that for some $f_1, \cdots, f_m \in M$, $R \in V^{ns}(f_1, \cdots, f_m)$.
By contradiction, assume that $m < n$; say $n = m + l$.
Note that up to a $\mathbb{Z}(\overline{\alpha})$-linear change of variables, we may assume R as close to the origin as we will need (more precisely, we need that the neighbourhood W_R below contains the origin). First, we will now prove that $V(g) \cap S$ and $V^{ns}(f_1, \cdots, f_m)$ locally coincide.

(a) $V(g) \cap S \subseteq V^{ns}(f_1, \cdots, f_m)$:
Indeed, $R \in V^{ns}(f_1, \cdots, f_m)$. So, $f_i \in I_R$ for all i and det $E \notin I_R$ (where E denotes the matrix $\left(\frac{\partial f_i}{\partial x_j}\right)$ with K-linearly independent vectors). As, for all $Q \in V(g) \cap S$, $I_Q = I_R$, it means that $f_i \in I_Q$ and det $E \notin I_Q$. So, $Q \in V^{ns}(f_1, \cdots, f_m)$.

(b) Let $Q \in V(g) \cap S$, $h \in M$ then $Q \notin V^{ns}(f_1, \cdots, f_m, h)$:
If we assume $Q \in V^{ns}(f_1, \cdots, f_m, h)$, arguing like in (a), we would find $R \in V^{ns}(f_1, \cdots, f_m, h)$ which contradicts the maximality of m.

(c) For all $Q \in V(g) \cap S$, there is W_Q an open neighbourhood of Q such that $W_Q \cap V(g) \cap S = W_Q \cap V^{ns}(f_1, \cdots, f_m)$:

By the point (b) and the proposition 5.1.4, the only possibility is that there is W' open neighbourhood of Q such that g vanishes on $W' \cap V^{ns}(f_1, \cdots, f_m)$. As $f \in I_R$, it means that $V(f) \supseteq V(g)$ and therefore that f vanishes on $W' \cap V^{ns}(f_1, \cdots, f_m)$. So, $W' \cap V^{ns}(f_1, \cdots, f_m) \subseteq W' \cap V(g) \cap V(f)$. We have that S is open in $V(f)$. So, for some W'' open neighbourhood of Q, $W'' \cap S = W'' \cap V(f)$. Take $W_Q = W' \cap W''$ and we are done.

We are given $f_1, \cdots, f_m$. Without loss of generality, we may assume that the matrix $\Delta = \left(\frac{\partial f_i}{\partial x_j}\right)_{1 \leq i \leq m; l+1 \leq j \leq n}$ has non-vanishing determinant at $R = (P, Q)$. Let $\Phi_{l+1}(\overline{x}), \cdots, \Phi_n(\overline{x})$ given by the implicit function theorem and let $\Phi_i(\overline{x}) = x_i$ for $i \leq l$. First, let us remark that up to a change of variables, we can assume that $\Phi_i(P)$ and $\frac{\partial \Phi_i}{\partial x_j}(P)$ (where $i > l \geq j$) lies in the maximal ideal $\mathfrak{M}_K$.
Indeed, by a change of variables of the type $(X_1, \cdots, X_n) \longmapsto (X_1 - N_1, \cdots, X_n - N_n)$ (where $N_i \in \mathbb{N}(\overline{\alpha})$ is a suitable approximation of P_i, Q_i), we can assume that the implicit functions are defined on a neighbourhood of 0. This means that we can assume $v(P) > t$ and $v(\Phi_i(P)) = v(Q) > t$ (where t could be any nonnegative integer). Also, we know that for all $r \leq l$

$$\begin{pmatrix} \frac{\partial \Phi_{l+1}}{\partial x_r} \\ \vdots \\ \frac{\partial \Phi_n}{\partial x_r} \end{pmatrix} (\overline{X}) = -\Delta^{-1} \begin{pmatrix} \frac{\partial f_1}{\partial x_r} \\ \vdots \\ \frac{\partial f_m}{\partial x_r} \end{pmatrix} (\overline{X}, \Phi_{l+1}(\overline{X}), \cdots, \Phi_n(\overline{X})). \tag{5.1}$$

We consider the change of variables

$$(X_1, \cdots, X_l, X_{l+1}, \cdots, X_n) \longmapsto (X_1, \cdots, X_l, X_{l+1}/\pi^t, \cdots, X_n/\pi^t).$$

Denote by $\tilde{f}$ the function obtained after this change of variables. Then, for all $i \leq m$,

$$\frac{\partial \tilde{f}_i}{\partial x_j}(\widetilde{P}, \widetilde{Q}) = \begin{cases} \frac{\partial f_i}{\partial x_j}(P, Q) & \text{for } j \leq l \\ \pi^{-t} \frac{\partial f_i}{\partial x_j}(P, Q) & \text{for } l+1 \leq j \leq n, \end{cases}$$

where $(\widetilde{P}, \widetilde{Q}) = (P, \pi^t Q)$. So, $\tilde{\Delta}(\widetilde{P}, \widetilde{Q}) = \frac{1}{\pi^t} \Delta(P, Q)$. For t large enough, $\tilde{\Delta}(\widetilde{P}, \widetilde{Q})$ has negative valuation. Therefore, by the relation (5.1),

$$v\left(\frac{\partial \widetilde{\Phi}_i}{\partial x_j}(\widetilde{P}, \widetilde{Q})\right) > 0.$$

Without loss of generality, we will assume that such a changement has be done and will denote $(\widetilde{P}, \widetilde{Q})$ by (P, Q) and similarly for the functions.

Let $h_N(\overline{X}) := \sum (X_i - N_i)^2$ for all $N = (N_1, \cdots, N_n) \in \mathbb{Z}[\alpha_1, \cdots, \alpha_s]^n$. We want to apply Hensel's lemma to the functions $\left(\frac{\partial \hat{h}_N}{\partial X_1}, \cdots, \frac{\partial \hat{h}_N}{\partial X_l}\right)$.
Our goal is to prove that for a point (P', Q'), close enough from (P, Q), the vectors $d_{(P',Q')}f_1, \cdots, d_{(P',Q')}f_m, d_{(P',Q')}h_N$ are linearly dependent. For this, by lemma 5.1.3, it is sufficient to check that the above partial derivatives vanish at P'.
We want to prove that if we choose N carefully, for all i, $\frac{\partial \hat{h}_N}{\partial X_i}(P)$ has valuation at least $2v(\text{ det } J(P)) + \varepsilon + 1$ where J is the Jacobian of the system, ε is the radius of the open set W_R given in (c). Then, the analytic Hensel's lemma gives us a root P', ε-close from P.

Claim 7. *det $J(P) \neq 0$.*

Proof. We compute the following derivatives using the chain rule :

$$g_i := \frac{\partial \hat{h}_N}{\partial X_i}(P) = \sum_{1 \le k \le n} 2 \cdot \Big(\Phi_k(P) - N_k\Big) \frac{\partial \Phi_k}{\partial X_i}(P).$$

$$\frac{\partial g_i}{\partial X_j}(P) = \frac{\partial^2 \hat{h}_N}{\partial X_j \partial X_i}(P) = \sum_k 2 \cdot \Big(\frac{\partial \Phi_k}{\partial X_i}(P) \cdot \frac{\partial \Phi_k}{\partial X_j}(P)\Big) + 2 \cdot \Big(\Phi_k(P) - N_k\Big) \frac{\partial^2 \Phi_k}{\partial X_j \partial X_i}(P).$$

We want to prove that the Jacobian of $g = (g_1, \cdots g_n)$ is non vanishing at P. In the above sum, let us denote $\sum_k 2 \cdot \frac{\partial \Phi_k}{\partial X_i}(P) \cdot \frac{\partial \Phi_k}{\partial X_j}(P)$ by B_{ij} and the other terms $\sum_k 2 \cdot \Big(\Phi_k(P) - N_k\Big) \frac{\partial^2 \Phi_k}{\partial X_j \partial X_i}(P)$ by C_{ij}. Then, let S_l be the permutation group of $\{1, \cdots, l\}$ and $sgn(\sigma)$ be the signature of an element $\sigma \in S_l$. We have:

$$\begin{aligned} \text{det } J_g(P) &= \sum_{\sigma \in S_l} sgn(\sigma) \prod J_{i\sigma(i)} \\ &= \sum sgn(\sigma) \prod (B_{i\sigma(i)} + C_{i\sigma(i)}) \\ &= \text{det } B + (\cdots), \end{aligned}$$

where in the sum $(\cdots)$, each element contains at least one factor of the form $\Big(\Phi_k(P) - N_k\Big)$.
If det $B \neq 0$, then, for N_k a suitable approximation of $\Phi_k(P)$, the valuation of det $J_g(P)$ is given by the valuation of det B (let us remark that in this case this valuation

does not depend on N). And therefore, det $J_g(P) \neq 0$.
We remark that for all $k \leq l$, $\frac{\partial \Phi_k}{\partial X_i} \cdot \frac{\partial \Phi_k}{\partial X_j} = \delta_{ijk}$ (δ is the Kronecker delta). So, if we denote by D_{ij} the sum over $k > l$ in $B_{ij}/2$, we have: $\frac{1}{2}B = Id + D$ and

$$\begin{aligned}\frac{1}{2}\text{det } B &= \sum_{\sigma \in S_r} sgn(\sigma). \prod \left(\delta_{i\sigma(i)} + D_{i\sigma(i)}\right) \\ &= \left(\text{det } D - \prod D_{ii}\right) + \prod \left(1 + D_{ii}\right).\end{aligned}$$

Now, assume by contradiction that det $B = 0$. Let us recall that for all $i > l$, for all k,

$$v\left(\frac{\partial \Phi_i}{\partial X_k}(P)\right) > 0 \ (*).$$

Therefore, $v(D_{ii}) > 0$ and as det $B = 0$,

$$v\left(\text{det } D - \prod D_{ii}\right) = v\left(\prod (1 + D_{ii})\right) = 0.$$

We deduce from these relations that $v($ det $D) = 0$. This is a contradiction with $(*)$. This completes the proof of the claim. □

Now, for $N_k \in \mathbb{Z}[\alpha_1, \cdots, \alpha_s]$ a suitable approximation of $\Phi_k(P)$, $g_i(P)$ has valuation at least $2v($ det $J(P)) + \varepsilon + 1$ (as we have seen the valuation of $J(P)$ does not depend on N in this case). So, by Hensel's lemma, there exists P' (ε-close from P) such that for all i, $g_i(P') = 0$ i.e $d_{P'}\hat{h}_N = 0$.
Let $Q' = (\Phi_{l+1}(P'), \cdots, \Phi_n(P'))$. Then, $(P', Q') \in V^{ns}(f_1, \cdots, f_m)$ and by lemma 5.1.3, $d_{(P',Q')}f_1, \cdots, d_{(P',Q')}f_m, d_{(P',Q')}h_N$ are linearly dependent over K.
But, as (P', Q') is in W_R (if we pick ε small enough), we have that $(P', Q') \in V^{ns}(f_1, \cdots, f_m) \cap W_R \subseteq V(g) \cap S$. Then, by an argument similar to the proof of (a), $d_{(P,Q)}f_1, \cdots, d_{(P,Q)}f_m, d_{(P,Q)}h_N$ are also linearly dependent for all N suitable approximation of $\Phi(P)$. As $d_{(P,Q)}f_1, \cdots, d_{(P,Q)}f_m$ are linearly independent, it implies that $d_{(P,Q)}h_N$ lies in the linear span of the other vectors.
Let $N' = (N_1, \cdots, N_{i-1}, N_i + p^{t_i}, N_{i+1}, \cdots, N_n)$, then N' is also a suitable approximation of $\Phi(P)$ (for all t_i large enough) and therefore $d_{(P,Q)}h_{N'}$ lies in the same vector space. But then, $(0, \cdots, p^{t_i}, 0, \cdots, 0) = (d_{(P,Q)}h_{N'} - d_{(P,Q)}h_N)/2$ lies in the linear span of $d_{(P,Q)}f_1, \cdots, d_{(P,Q)}f_m$ for all i, which contradicts that $m < n$. □

5.2 Decidability of the existential theory of $\mathbb{Z}_{p,exp}$

In this section, we will give a (conditional) proof of the decidability of the theory of $\mathbb{Z}_{p,exp}$. We decompose our proof in two steps. First, we will consider the case of positive existential $\mathcal{L}_{exp}$-sentences. The algorithm follows the strategy of the real case with Hensel's lemma playing the role of Newton's algorithm. In this part, our proof is conditionnal : as for the real case, Schanuel's conjecture is involved and we can guarantee that our algorithm stops only if the p-adic version of this conjecture is true. In this part, we will also give an algorithm which takes for entry a general existential $\mathcal{L}_{exp}$-sentence and which returns true if this sentence is true in $\mathbb{Z}_p$. However, this algorithm does not stop if the sentence is false.
We obtain the decidability of the full theory via the result of effective model-completeness 4.4.5 of chapter 4. We will see that the algorithm for the decidability of existential $\mathcal{L}_{exp}$-formulas can be extended naturally to formulas in the language $\mathcal{L}_{pEC}$. The main theorem will therefore follow. In the last part, we will discuss the one variable case. In this situation, p-adic Schanuel's conjecture is proved. We will see how our above arguments can be adapted to determine whether or not a system of exponential equations and inequations with one variable has a solution in $\mathbb{Z}_p$.

5.2.1 Decidability of positive existential sentences

First, it is easy to see that any existential $\mathcal{L}_{exp}$-sentence is (effectively) equivalent to a disjunction of sentences of the type:

$$\exists x_1 \cdots \exists x_n \bigwedge_j F_j(\overline{x}) = 0 \wedge \bigwedge_j G_j(\overline{x}) \neq 0,$$

where F_i and G_j are in $\mathbb{Z}[x_1, \cdots, x_n, e^{px_1}, \cdots, e^{px_n}]$.
Let us remark that to any such exponential polynomial F corresponds a polynomial in $\mathbb{Z}[x_1, \cdots, x_{2n}]$. And conversely, to a polynomial $P \in \mathbb{Z}[x_1, \cdots, x_{2n}]$ corresponds a unique element of $\mathbb{Z}[x_1, \cdots, x_n, e^{px_1}, \cdots, e^{px_n}]$. We will denote by F_P this exponential polynomial.
We start with the case where only equalities are involved. Once again, as for all $x, y \in \mathbb{Z}_p$ $(x, y) = (0, 0)$ iff $x^2 + py^2 = 0$, we are reduced to the case of a single exponential polynomial, say $F_P(x_1, \cdots, x_n)$. Then, using the desingularization theorem, we can

almost already determine if F_P has a root in $\mathbb{Z}_p$:

The idea of the algorithm is the following: if F_P admits a root $\overline{a}$ in $\mathbb{Z}_p^n$, then we know by the theorem 5.1.5 that there are $F_{P_1}, \cdots, F_{P_n}$ and $\overline{b}$ such that $F_P(\overline{b}) = 0$ and $\overline{b}$ is a non-singular zero of the system $G = (F_{P_1}, \cdots, F_{P_n})$. Let $s = v(\det J_G(\overline{b}))$. Now, using Hensel's lemma, non-singular zeros of the system G are determined by zeros in $\mathbb{Z}/p^{2s}\mathbb{Z}$. Therefore, we have that the following procedure stops if the system G has a zero:

For all tuple of integer $\overline{t}$ check if the conditions of Hensel's lemma are satisfied i.e. if $J_G(\overline{t}) \neq 0$ and $v(G(\overline{t})) > 2v(detJ_G(\overline{t}))$. If yes, the system admits a non-singular zero around $\overline{t}$.

Conversely, if the system admits a non-singular root, such a tuple exists by density of $\mathbb{Z}$ in $\mathbb{Z}_p$. This procedure is almost what we need. It just remains to deduce that $F_P(\overline{b}) = 0$ from the knowledge that $G(\overline{b}) = 0$. This is the case whenever P is in the ideal generated by $P_1, \cdots, P_n$. Indeed, $\overline{b}$ determines a zero of each P_i:

$$P_i(b_1, \cdots, b_n, e^{pb_1}, \cdots, e^{pb_n}) = 0 \text{ iff } F_{P_i}(b_1, \cdots, b_n) = 0.$$

The next lemma will give us exactly what we need : up to multiplication by a polynomial Q (such that Q does not vanish at $(b_1, \cdots, b_n, e^{pb_1}, \cdots, e^{pb_n})$), P is in the ideal generated by some $Q_1, \cdots, Q_n$ like above.

The key point of this lemma is that we can determine the transcendence degree of $\mathbb{Q}(b_1, \cdots, b_n, e^{pb_1}, \cdots, e^{pb_n})$ over $\mathbb{Q}$. This is where Schanuel's conjecture turns out to be helpful.

The first thing to observe is that as $\overline{b}$ is a non-singular zero of the system G, we certainly have that

$$\operatorname{trdeg}_{\mathbb{Q}}\mathbb{Q}(b_1, \cdots, b_n, e^{pb_1}, \cdots, e^{pb_n}) \leq n.$$

We actually need equality which can be obtained using a p-adic version of Schanuel's conjecture:

Conjecture (p-adic Schanuel's Conjecture). *Let $n \geq 1$ and $t_1, \cdots, t_n$ in $\mathbb{C}_p$ (with valuation at least $1/(p-1)$) linearly independent over $\mathbb{Q}$.*
Then, the field $\mathbb{Q}(t_1, \cdots, t_n, e^{t_1}, \cdots, e^{t_n})$ has transcendence degree at least n over $\mathbb{Q}$.

Using the p-adic version of Schanuel's conjecture, like in [11], we can prove:

Lemma 5.2.1. *Let $n \geq 1$, $P \in \mathbb{Z}[x_1, \cdots, x_{2n}]$.*
Assume that $F_P = P(x_1, \cdots, x_n, e^{px_1}, \cdots, e^{px_n})$ has a zero and that for all zeros $\overline{a}$ of F_P, its components $a_1, \cdots, a_n$ are $\mathbb{Q}$-linearly independent.
Then, there exist $b_1, \cdots, b_n \in \mathbb{Z}_p$ and $Q, Q_1, \cdots, Q_n, S_1, \cdots S_n \in \mathbb{Z}[x_1, \cdots, x_{2n}]$ such that $\overline{b}$ is a zero of F_P and a non-singular zero of $G = (F_{Q_1}, \cdots, F_{Q_n})$, that $F_Q(\overline{b}) \neq 0$ and that $QP = \sum_i Q_i S_i$.

This lemma guarantees the existence of a system such that the non-singular zeros of this system are roots of F_P.

Proof. Let $P_1, \cdots, P_n$ given by theorem 5.1.5 and $\overline{b} \in V(F_P) \cap V^{ns}(F_{P_1}, \cdots, F_{P_n})$.
By the above discussion, the transcendence degree of $\mathbb{Q}(b_1, \cdots, b_n, e^{pb_1}, \cdots, e^{pb_n})$ over $\mathbb{Q}$ is exactly n. We apply the following claim with $m = 2n$, $r = n$ and
$I = \{h \in \mathbb{Z}[x_1, \cdots, x_{2n}] \mid h(b_1, \cdots, b_n,^{pb_1}, \cdots, e^{pb_n}) = 0\}$:

Claim 8. *Let $m, r \geq 1$, I prime ideal of $\mathbb{Z}[x_1, \cdots, x_m]$ with $I \cap \mathbb{Z} = \{0\}$ and $trdeg_{\mathbb{Q}}$ Frac $(\mathbb{Z}[x_1, \cdots, x_m]/I) = r$.*
Then, there is $Q \in \mathbb{Z}[\overline{x}]$ with $Q \notin I$ such that QI is generated by $m - r$ elements.

As trdeg $\mathrm{Frac}(\mathbb{Z}[\overline{x}]/I) = \mathrm{trdeg}_{\mathbb{Q}}\mathbb{Q}(b_1, \cdots, b_n E_p(b_1), \cdots, E_p(b_n)) = n$ by Schanuel's conjecture, we can apply the claim.
Let $Q_1, \cdots, Q_n$ be generators of QI. Then, the properties of the lemma are satisfied except that $\overline{b}$ may be a singular zero of our system. But, as $P_i \in I$, $QP_i = \sum S_{ij} Q_j$ for some $S_{ij} \in \mathbb{Z}[\overline{x}]$. Using the chain rule on this relation, we find that

$$F_Q(\overline{b}) \cdot \frac{\partial F_{P_i}}{\partial x_j}(\overline{b}) = \sum_k F_{S_{ik}}(\overline{b}) \frac{\partial F_{Q_k}}{\partial x_j}(\overline{b}).$$

As $F_Q(\overline{b}) \neq 0$, we deduce that $\overline{b}$ is a non-singular zero of G. □

We will now discuss the effectivity of some basic computations that will occur in our algorithm.
The first issue is to compute the valuation of an exponential polynomial evaluated at a given integer.
Let $f \in \mathbb{Z}[x_1, \cdots x_n, e^{px_1}, \cdots, e^{px_n}]$ and a tuple of integer $\overline{t}$. Then, we are able to determine if $f(\overline{t}) = 0$ and compute the valuation of $f(\overline{t})$:
Let us remark that we can assume that $f(\overline{t})$ is a finite sum of the form

$$f(\overline{t}) = s \sum a_i e^{pi}$$

where the a_i's are integer and $s \in \mathbb{Z}_p^*$. As, e^p is transcendental over $\mathbb{Q}$, $f(\bar{t}) = 0$ iff $a_i = 0$ for all i. If this is not the case, using the Taylor expansion, we can determine the remainder of $f(\bar{t})$ modulo p^n for all n. The valuation is determined by the smallest n such that $f(\bar{t}) \not\equiv 0 \mod p^n$.

The last issue to solve is the condition that the non-singular zero $\bar{b}$ should not be a zero of the function F_Q given in the lemma 5.2.1. In fact, as F_Q has no root in a neighbourhood of $\bar{b}$, it is sufficient to be able to check that F_Q has no root in a given open set. This recursive procedure will also be useful when we will consider general existential sentences.

Lemma 5.2.2. *Let $U = \bar{a} + p^t\mathbb{Z}_p^n$ be an open set (where $\bar{a} \in \mathbb{Z}^n$, $t \in \mathbb{N}$) and let $g = (g_1, \cdots, g_k)$ be k exponential functions. Then, there is a recursive procedure which returns yes if there is no zero of g inside U.*

Proof. We just have to check that the valuation of g is bounded on U.

Let us remark that if there is $\bar{y} \in U$ such that $g(\bar{y}) = 0$, then for all $s \geq t$, there are $b_{0i}, \cdots, b_{si} \in \{0, \cdots, p-1\}$, $i \leq n$ such that

$$a_i \equiv \sum_j b_{ji}p^j \mod p^t \text{ and } g\left(\sum b_{j1}p^j, \cdots, \sum b_{jk}p^j\right) \equiv 0 \mod p^{s+1}.$$

Actually, the b_{ji}'s are the digits of b_i a suitable approximation of y_i.

So, the converse states that: if there is $s \geq t$ such that for all $b_{0i}, \cdots, b_{si} \in \{0, \cdots, p-1\}$ such that for all $i \leq n$

$$a_i \equiv \sum_j b_{ji}p^j \mod p^t,$$

we have

$$g\left(\sum_j b_{j1}p^j, \cdots, \sum_j b_{jk}p^j\right) \not\equiv 0 \mod p^{s+1},$$

then, there is no $\bar{y} \in U$ such that $g(\bar{y}) = 0$.

But these last conditions are recursively enumerable. The following algorithm does the job:

Algorithm 2. *Given $U = \bar{a} + p^t\mathbb{Z}_p^n, g = (g_1, \cdots, g_k)$.*

Proceed to an enumeration of all $s \in \mathbb{N}$, $s \geq t$. Check if for all $b_1, \cdots, b_n \in \mathbb{Z}/p^s\mathbb{Z}$ with $v(\bar{a} - \bar{b}) \geq t$, $g_i(\bar{b}) \not\equiv 0 \mod p^{s+1}$ for all i. If yes, return true. Otherwise go to the next step.

This completes the proof of the lemma. □

Let us remark that this algorithm never stops if the system has a root in U. In our situation, it does not matter. Indeed, we are guaranteed that F_Q has no such a root for a suitable U.

Proposition 5.2.3. *If Schanuel's conjecture is true, the positive existential theory of the structure $(\mathbb{Z}_p, +, \cdot, 0, 1, E_p)$ is decidable.*

Proof. Let φ be a positive existential sentence of our theory. Without loss of generality, we can assume that

$$\varphi \equiv \exists x_1 \cdots x_n F_p(\overline{x}) = 0$$

for some $P \in \mathbb{Z}[X_1, \cdots, X_{2n}]$.

First, we give an algorithm that returns true if the sentence is satisfied (and never stop otherwise). We are given F_P and we want to know if this function admits a solution in $\mathbb{Z}_p^n$. Assume that this is the case. Then, lemma 5.2.1 gives us the existence of exponential polynomial functions $G = (F_{Q_1}, \cdots, F_{Q_n})$ such that any non-singular zero of G is a zero of F_P. So, proceed to an enumeration over all possible system G and polynomials Q, S_{ij} like in the lemma. Using Hensel's lemma, we can determine if G has a non-singular root in an open U. If our sentence is satisfied, there exists such an open set U which contains a solution of G and does not contain a root of F_Q. So, we proceed to an enumeration of all open set of the type $U = \overline{a} + p^t\mathbb{Z}_p^n$ for all $\overline{a} \in \mathbb{N}^n, t \in \mathbb{N}$ and on each such a set we check if the conditions of Hensel's lemma are satisfied for some tuple in U and if F_Q has no root in U (via lemma 5.2.2).

We give now the algorithm. If Schanuel's conjecture is true, this algorithm returns true whenever F_P has at least one root in $\mathbb{Z}_p^n$ and the components of any of its roots are linearly independent. If these conditions are not satisfied, this algorithm may run forever.

Algorithm 3. *Given $n \geq 1, P \in \mathbb{Z}[x_1, \cdots, x_{2n}]$.*

Proceed to an enumeration of $Q, Q_1, \cdots, Q_n, S_1, \cdots, S_n \in \mathbb{Z}[x_1, \cdots, x_{2n}]$

and all $a_1, \cdots, a_n, t, s \in \mathbb{N}, s \geq t$

Given such a $3n+3$-uple, first check if $QP = \sum Q_i S_i$. If not go to the next step (of the enumeration).

Otherwise, check if

$$det\left(\frac{\partial F_{Q_i}}{\partial x_j}\right)(\overline{a}) \neq 0,$$

and if

$$v(F_{Q_i})(\overline{a}) > v\Big(det\left(\frac{\partial F_{Q_i}}{\partial x_j}\right)(\overline{a})\Big) + t.$$

If not, go to the next step.
If this is the case (there is a root of the system G in $U := \overline{a} + p^t\mathbb{Z}_p^n$), for all $b_{ij} \in \{0, \cdots, p-1\}$, where $0 \leq j \leq s$, $1 \leq i \leq n$, let $b_i = \sum b_{ij}p^j$ check if whenever $v(\overline{b} - \overline{a}) \geq t$, we have

$$F_Q(\overline{b}) \not\equiv 0 \mod p^{s+1}.$$

If yes (F_Q does not admit root in U), return true. Otherwise, go to the next step.

Finally, let us recall that in the above algorithm, we need to assume that the components of any root of F_P are linearly independent. But, without loss of generality, we can assume that this is the case:
Indeed, let F_P be an exponential polynomial. We proceed to an enumeration over all possible relations of $\mathbb{Z}$-linear dependence between the variables and we run in parallel the following procedure:
For each relation, we remove one of the variable according to this relation. Let $\widetilde{F_P}$ be the exponential polynomial obtained after this transformation. We remark that $\widetilde{F_P}$ has a root iff F_P has a root that satisfies the $\mathbb{Z}$-linear relation used to construct $\widetilde{F_P}$. We apply the algorithm 3 with entry $\widetilde{F_P}$. If the components of any root of $\widetilde{F_P}$ are linearly independent, then algorithm 3 returns true (in the case where $\widetilde{F_P}$ has a root) and the truth of our formula is determined. If $\widetilde{F_P}$ has a root with components linearly dependent, we restart the procedure with $F_P := \widetilde{F_P}$.
This procedure stops and returns true in the case where F_P has a root in $\mathbb{Z}_p$.

Now, we can determine the truth of a positive existential sentence : we run in parallel the algorithm 2 and algorithm 3 with entries P. If F_P has no root in $\mathbb{Z}_p^n$, the algorithm 2 stops and we return false. If not, then F_P has a root and algorithm 3 stops, in which case, we return true. □

Remark. It is not hard to see that the algorithms 2 and 3 can be adapted to determine the truth of positive existential sentences in $(\mathcal{O}_{K_N}, +, \cdot, 0, 1, E_p)$ where (K_N) is the family of algebraic extensions defined in chapter 3 section 3.3.

Let us also remark that the algorithm 3 can be easily modified to take as entries general existential sentences. Indeed, such a sentence has the form

$$\exists x_1 \cdots \exists x_n F_P(\overline{x}) = 0 \wedge \bigwedge_j F_{R_j}(\overline{x}) \neq 0.$$

Therefore, we just have to check that F_{R_j} has no root in U (exactly like we did for F_Q). However, it is not clear that we can find a procedure that stops if such a sentence is false. This can be reduced to the following question: is there a procedure that stops if $V(F_P) \subseteq V(F_{R_1}, \cdots, F_{R_s})$? If $n = 1$, we can actually solve this problem. This will be developped in the last part of this section. It is not obvious that the one variable strategy can be adapted for n greater than one. In order to avoid this issue, we extend proposition 5.2.3 to the language $\mathcal{L}_{pEC}$ and use the effective model-completeness of the theory. The decidability of the full theory is then clear: apply the above procedure in parallel for the sentence and (the existential sentence equivalent to) its negation. One of the two procedure has to stop and therefore determines the truth of the sentence in $\mathbb{Z}_p$.

5.2.2 Decidability of the $\mathcal{L}_{pEC}$-sentences

First, we recall the notations of chapter 4 section 4.4: let $K_n = \mathbb{Q}_p(\beta_n)$ as defined in this part. Let d_n be the degree of the extension. As we know, the trigonometric functions $c_{i,j,n}$ can be obtained as a polynomial combination of the functions $e^{px(\beta_n^i)^\sigma}$ (where $\sigma \in Gal(K_n/\mathbb{Q}_p)$) via the relations:

$$\begin{pmatrix} c_{0,i,n}(x) \\ \vdots \\ c_{d_n-1,i,n}(x) \end{pmatrix} = N_{K_n|\mathbb{Q}_p}(\det V) \cdot V^{-1}\Big(e^{px(\beta_n^i)^\sigma}\Big)_{\sigma \in \mathrm{Gal}(K_n/\mathbb{Q}_p)},$$

where V is the Vandermonde matrix of the roots of P_{β_n}, the minimal polynomial of β_n over $\mathbb{Z}_p$.

Let φ be an existential $\mathcal{L}_{pEC}$-sentence with n quantifiers. Then, there is N such that any term of the formula has the form

$$f(\overline{x}) = P(\overline{x}, e^{p\overline{x}}, c_{0,1,N}(\overline{x}), \cdots, c_{d_N-1,d_N-1,N}(\overline{x})) =: F_P(\overline{x})$$

for some $P(\overline{x}, \overline{y}_0, \cdots, \overline{y}_{L_N}) \in \mathbb{Z}[\overline{x}, \overline{y}_0, \cdots, \overline{y}_{L_N}]$ (where $L_N = d_N^2 - d_N$). Let us remark that the ring generated by the exponential and trigonometric functions is closed under derivation. Therefore, we can apply theorem 5.1.5:

Let f be a $\mathcal{L}_{pEC}$-term. Assume that $V(f) \neq \varnothing$. Then, there exist $Q_1, \cdots, Q_n \in \mathbb{Z}[\overline{x}, \overline{y}_0, \cdots, \overline{y}_{L_N}]$ such that $V^{ns}(F_{Q_1}, \cdots F_{Q_n}) \cap V(f) \neq \varnothing$. This implies that there is a root $\overline{a}$ of f such that:

$$\begin{aligned}&\operatorname{trdeg}_{\mathbb{Q}}\mathbb{Q}(a_1, \cdots, a_n, e^{pa_1}, \cdots, e^{pa_n}, c_{0,1,d_N}(a_1), \cdots, c_{d_N-1,d_N-1,N}(a_n))\\ &= \operatorname{trdeg}_{\mathbb{Q}}\mathbb{Q}(a_1, \cdots, a_n, e^{pa_1}, \cdots, e^{pa_n}, e^{pa_1\beta_N} \cdots, e^{pa_n\beta_N^{d_N-1}}) \leq d_N \cdot n.\end{aligned}$$

Let us remark that $1, \beta_N, \cdots, \beta_N^{d_N-1}$ are $\mathbb{Q}_p$-linearly independent. Using Schanuel's conjecture (in $\mathbb{C}_p$), we find that the above relation is actually an equality (if $a_1, \cdots, a_n$ are $\mathbb{Q}$-linearly independent). With this, we prove as before:

Lemma 5.2.4. *Let $n \geq 1$, $P \in \mathbb{Z}[\overline{X}, \overline{Y}_0, \cdots, \overline{Y}_{L_N}]$.*
Assume that $F_P = P(x_1, \cdots, x_n, e^{px_1}, \cdots, e^{px_n}, c_{0,1,N}(x_1), \cdots, c_{N,d_N-1,d_N-1}(x_n))$ has a zero in $\mathbb{Z}_p$ and that the components of any zero of F_P are $\mathbb{Q}$-linearly independent. Then, there exist $a_1, \cdots, a_n \in \mathbb{Z}_p$ and $R, R_1, \cdots, R_{T_N}, S_1, \cdots S_{T_N} \in \mathbb{Z}[\overline{X}, \overline{Y}_0, \cdots, \overline{Y}_{L_N}]$ (where $T_N = (L_N - d_N + 2) \cdot n$) such that $\overline{a}$ is a zero of F_P and a non-singular zero of a subsystem of $G = (F_{R_1}, \cdots, F_{R_{T_N}})$, that $F_R(\overline{a}) \neq 0$ and that $RP = \sum_i R_i S_i$.

Proof. We apply claim 8 with

$$I = \{h \in \mathbb{Z}[\overline{X}, \overline{Y}_0, \cdots, \overline{Y}_{L_N}] \mid \ h(\overline{a}, E_p(\overline{a}), c_{0,1,N}(\overline{a}), \cdots, c_{d_N-1,d_N-1,N}(\overline{a})) = 0\},$$

$m = (L_N^2 + 2) \cdot n$ and $r = d_N \cdot n$. Then, by the claim, there exist $R \notin I$, $R_1, \cdots, R_{T_N}$ generators of RI (where $T_N = m - r$) and $S_1, \cdots, S_{T_N}$ such that $RP = \sum R_i S_i$. Also, as $Q_i \in I$ for all i, like in lemma 5.2.1, it implies that $\overline{a} \in V^{ns}(F_{\widetilde{R_1}}, \cdots, F_{\widetilde{R_n}})$ for some $\widetilde{R_1} \cdots, \widetilde{R_n} \in \{R_1, \cdots, R_{T_N}\}$. □

If we are given φ an existential $\mathcal{L}_{pEC}$-sentence of the form:

$$\exists x_1, \cdots, x_n F_P(\overline{x}) = 0 \wedge \bigwedge_i F_{A_i}(\overline{x}) \neq 0,$$

it is quite easy to adapt the algorithm 3 to construct an algorithm that returns yes if the sentence is true in $\mathbb{Z}_p$ (and never stops otherwise):

1. Enumerate all $R, R_1, \cdots, R_{T_N}, S_1, \cdots S_{T_N}$ and $B = \overline{a} + p^k\mathbb{Z}_p^n$.

2. If $RP = \sum R_i S_i$, check if a subsystem $\widetilde{R_1} \cdots , \widetilde{R_n}$ has a unique non-singular root in B using Hensel's lemma.

3. If this is the case, use the algorithm 3 to determine if the following formula is true in V_N:

$$\exists \overline{x}\ \overline{x} \in B \wedge \overline{x} \in V^{ns}(\widetilde{R_1} \cdots , \widetilde{R_n}) \wedge \overline{x} \in V(R_1, \cdots , R_{T_N}).$$

   We use the version of algorithm 3 for formulas in K_N and in the above formula, we replace the trigonometric functions by their polynomial expression in exponential terms. Note that this procedure never stops if the above formula is false but it doesn't matter.

4. If the above formula is true, then the system $R_1, \cdots , R_{T_N}$ has a root in $\mathbb{Z}_p^n \cap B$. So, F_P has a root in $\mathbb{Z}_p^n \cap B$. It remains to check that F_{A_i} and F_R have no root in B. If this is the case, φ is true.

Now, we use effectivity of the theorem 4.4.5 to obtain a sentence ψ equivalent to the negation of the sentence φ. Surely, our algorithm stops either for φ or ψ. We can therefore determine the truth value of φ in $\mathbb{Z}_p$ by running in parallel the algorithm for φ and ψ.

The main theorem follows:

Theorem 5.2.5. *Assume that the p-adic version of Schanuel's conjecture holds. Then, the theory of $\mathbb{Z}_{pEC}$ in the language $\mathcal{L}_{pEC}$ is decidable.*

Also, by the remark after proposition 5.2.3, it is not hard to extend the above theorem to finite algebraic extensions.

5.2.3 One variable case

In this section, we prove that we can effectively determine the truth of formulas of the type: $\exists x P(x, e^{px}) = 0 \wedge Q(x, e^{px}) \neq 0$, where P, Q are polynomials with coefficients in $\mathbb{Z}$, without assuming Schanuel's conjecture.

Proposition 5.2.6. *Given $f_1, \cdots , f_t, g_1, \cdots , g_s \in \mathbb{Z}[x, e^{px}]$, the truth of the formula $\exists x \wedge_i f_i(x) = 0 \wedge_k g_k(x, e^{px}) \neq 0$ is decidable in $\mathbb{Z}_p$.*

As usual, we reduce the above proposition to the case $s = t = 1$.
Let us remark that for a formula of the type $\exists x P(x, e^{px}) = 0$, the algorithms 2 and 3 determine the truth of this formula. Here is the complete algorithm for the one-variable case. More precisely, the next algorithm determines the truth of the formula $\exists x \in U\ P(x, e^{px}) = 0$ in $\mathbb{Z}_p$ where U is an open ball.

Algorithm 4. *Given $P \in \mathbb{Z}[x, y], U = a + p^n\mathbb{Z}_p$.*
Proceed to an enumeration of $R, Q, S \in \mathbb{Z}[x, y]$ and $t, m \in \mathbb{N}, m \geq n$ with $v(a - t) \geq n$ Given such a tuple, check if for all $b_j \in \{0, \cdots, p-1\}$, $0 \leq j \leq m$, such that $v(a - \sum b_j p^j) \geq n$, we have

$$F_P\left(\sum b_i p^i\right) \not\equiv 0 \mod p^{m+1}.$$

If yes (F_P does not a admit root in U), return false.
If not, check if $RP = \sum QS$. If not go to the next step.
Otherwise, check if:

$$F'_Q(t) \neq 0$$

and if

$$v(F_Q(t)) > 2 \cdot v(F'_Q(t)) + n.$$

If this is not the case, go to the next step.
If yes (there is a root of F_Q in U), check if for all $b_j \in \{0, \cdots, p-1\}$, $0 \leq j \leq m$, with $v(t - \sum b_j p^j) \geq v(F'_Q(t)) + n$ we have

$$F_R\left(\sum b_i p^i\right) \not\equiv 0 \mod p^{m+1}.$$

If yes (the root of F_Q found using Hensel's lemma is not a root of F_R), return true. Otherwise, go to the next step.

Let us remark that in the one variable case, (the complex) Schanuel's conjecture is a theorem of C. Hermite. A p-adic version of this theorem has been proven by K. Malher in [12]. So, the above algorithm will stop if F_P has a solution in U. For the general situation, we have to consider inequalities. However, we don't want to use the theorem 4.4.5. Indeed, the existential sentence equivalent to the negation of our sentence may have more than one quantifier and therefore it would require Schanuel's conjecture to determine if this negation is true in $\mathbb{Z}_p$. As we have stated before, it is

sufficient to determine effectively if $V(F_P) \subseteq V(F_Q)$.
We know that any non-zero analytic function h (from $\mathbb{Z}_p$ to itself) has only finitely many roots in $\mathbb{Z}_p$. Also, if h has a non-singular root a, then by Hensel's lemma, there is $t \in \mathbb{Z}$ such that $v(h(t)) > 2v(h'(t))$ and furthermore, a is the unique root such that $v(a-t) > v(h'(t))$. The idea is now to prove that for all roots a in a open set U, we can recursively determine an open subset V of U such that a is the unique root of h in V. In fact, we will construct recursively a partition $\{U_i\}$ of U such that on each element U_i of the partition either our function has a unique root in U_i or the function has no root in U_i. Before writing down the algorithm, we recall that if we are given f, g two E-polynomials then they have a common root in U iff $f^2 + pg^2$ has a root in U. So, we can determine if a system of equations with one variable has a common root using algorithm 4. Our algorithm asks as entries F_P, U as before and $\{U_1, \cdots, U_s\}$ a collection of disjoint open sets contained in U such that F_P has at most one root in U_i. We allow $s = 0$. The algorithm returns a partition $\{U_1, \cdots, U_N\}$ of U with the above properties.

Algorithm 5. *We are given $P \in \mathbb{Z}[x,y]$, $U = a + p^n\mathbb{Z}_p$ and $\{U_1, \cdots, U_s\}$ disjoint open sets satisfying our condition.*
If $U = \bigcup_i U_i$, return $\{U_1, \cdots, U_s\}$. Otherwise, let $U' = U \setminus (\bigcup_i U_i)$.
Proceed to an enumeration of all $t \in U' \cap \mathbb{Z}$ and all $n, l \in \mathbb{N}$.
Let $\varepsilon = \max_{k \leq l+1}\{v(F_P^{(k)}(t)), n\}$.
If $\varepsilon = +\infty$, go to the next step of the enumeration.
Let U_{s+1} be the open ball of centre t and radius $p^{-\varepsilon}$.
Check if one of the following conditions is true running algorithm 4 in parallel with the enumeration of the t, n, l's:

(a) F_P has no root in U_{s+1}; or,

(b) The system $(F_P, F_P', \cdots, F_P^{(l)})$ admits a root in U_{s+1}, the system $(F_P, F_P', \cdots, F_P^{(l+1)})$ has no root in U_{s+1} (i.e. F_P has a root of order l in U_{s+1}) and $v(F_P^{(l)}(t)) > 2v(F_P^{(l+1)}(t))$ (the root is unique).

If for U_{s+1} either (a) or (b) is satisfied, apply algorithm 5 with entries F_P, U and $\{U_1, \cdots, U_{s+1}\}$. Otherwise go to the next step.

As F_P has only finitely many roots and by compactness of $\mathbb{Z}_p$, the algorithm stops. Indeed, for U_{s+1} sufficiently small, if condition (a) does not hold, this open set contains a unique root of F_P:

Claim 9. *If condition (b) is satisfied, then F_P has a unique root in U_{s+1}.*

Proof. Surely, by (b), F_P admits a root of order l. And, if F_P admits another root in U_{s+1}, the root has order strictly less than l. Indeed, the system $(F_P, F'_P, \cdots, F_P^{(l+1)})$ does not have a root in U_{s+1} by (b). And, by Hensel's lemma, $F_P^{(l)}$ admits a unique root a in U_{s+1}. Let b be another root of F_P of order $k < l$ (assume k maximal for this property). Then, by Hensel's lemma, $F_P^{(k)}$ admits a unique root in the ball of centre b and radius $v(F_P^{(k+1)}(b))$ (by maximality of k, this radius is finite). Now, for t like in the above algorithm, we have $v(t-b) > \varepsilon$. And so, by definition of ε (and because F_P is analytic),

$$v(F_P^{(k)}(b) - F_P^{(k)}(t)) > \varepsilon \geq v(F_P^{(k)}(t)).$$

Which means that $v(F_P^{(k)}(b)) = v(F_P^{(k)}(t))$. But, then,

$$v(a-b) \geq \min\{v(a-t), v(b-t)\} > \varepsilon \geq v(F_P^{(k)}(t)) = v(F_P^{(k)}(b)).$$

As $F_P^{(k)}(a) = 0$, by uniqueness of b, $a = b$. □

Finally, we give the algorithm that determines the truth value of the formula $\varphi \equiv \exists x F_P(x) = 0 \wedge F_Q(x) \neq 0$. The idea is to split , using algorithm 5, $\mathbb{Z}_p$ into open sets such that on each such an open set U either

- $F_P(x)$ has no root in U; or,
- F_P admits a root in U and F_Q has no root in U; or,
- F_P and F_Q have both a unique root in U.

In the two first cases, the local truth of the formula φ is obvious. In the last case, our formula is true if the system (F_P, F_Q) has no root in U (by uniqueness of the roots). This problem is solved by algorithm 4. Also, it is clear how we can extract the truth of the formula if we can determine its local truth.

Algorithm 6. *Let $U_1, \cdots, U_N$ be the open sets returned by the algorithm 5 applied with $P, \mathbb{Z}_p$ and $s = 0$.*

Let $V_{1i}, \cdots, V_{M_i,i}$ be the open sets returned by the algorithm 5 applied with Q, U_i and $s = 0$.

Let $\mathcal{V} = \{V_1, \cdots, V_M\}$ be the partition of $\mathbb{Z}_p$ by the V_{ij}'s.

For all $1 \leq i \leq M$, remove from $\mathcal{V}$ the set V_i if F_P has no root in V_i.

If $\mathcal{V}$ is now empty, return false.

Otherwise, if there is $V_i \in \mathcal{V}$ such that F_Q has no root in V_i, return true.

Otherwise, for all i:

Check using algorithm 4 if the system (F_P, F_Q) has a no solution in V_i.

If this is the case (the unique solution of F_P in V_i is different from the unique solution of F_Q in V_i), return true. Otherwise, remove V_i from $\mathcal{V}$.

If $\mathcal{V}$ is now empty, return false.

This completes the proof of the proposition.

5.3 Weak Schanuel's conjecture

As we have seen, the decidability of the p-adic exponential ring is settled if Schanuel's conjecture is true. In this section, we introduce a weaker conjecture that also implies (and actually is equivalent to) the decidability.

In this section, we will denote by $\mathcal{P}_n$ the set of $\mathcal{L}_{pEC}$-terms with n variables.

Conjecture 5.3.1. *There is $F : \mathcal{P}_n^{2n} \longrightarrow \mathbb{Q}_{>0}$ computable such that for all $f_1, \cdots, f_n$, $g_1, \cdots, g_n \in \mathcal{P}_n$, for all $\alpha \in V^{ns}(f_1, \cdots, f_n)$ and for all $\beta \in V^{ns}(g_1, \cdots, g_n)$, either $\alpha = \beta$ or $|\alpha - \beta|_p \geq F(f_1, \cdots, f_n, g_1, \cdots, g_n)$.*

Note that if the theory of the p-adic exponential rings (with the trigonometric functions) is decidable then the conjecture is true. In particular, the p-adic Schanuel's conjecture implies conjecture 5.3.1. Indeed, as both $V^{ns}(f_1, \cdots, f_n)$ and $V^{ns}(g_1, \cdots, g_n)$ are finite, there exists $k \in \mathbb{N}$ such that either $\alpha = \beta$ or $v(\alpha - \beta) \leq k$. Enumerate all $k \in \mathbb{N}$ and test the truth value of the formula Ψ_k in $\mathbb{Z}_p$ where

$$\Psi_k \equiv \forall \overline{x}, \overline{y}\Big(\overline{x} \in V^{ns}(f_1, \cdots, f_n) \wedge \overline{y} \in V^{ns}(g_1, \cdots, g_n) \wedge \overline{x} \neq \overline{y}\Big) \longrightarrow v(\overline{x} - \overline{y}) \leq k.$$

Define $F(f_1, \cdots, f_n, g_1, \cdots, g_n)$ as p^{-N} where N is the smallest integer such that Ψ_N is true. On the other hand,

Proposition 5.3.2. *If conjecture 5.3.1 is true, then $\mathbb{Z}_{pEC}$ is decidable.*

Proof. Let Ψ be a formula of the type $\exists \overline{x} g(\overline{x}) = 0 \wedge h(\overline{x}) \neq 0$. As $\mathbb{Z}_{pEC}$ is effectively model-complete, it is sufficient to find an algorithm that stops if the formula is true (and may run forever otherwise). We proceed to an enumeration of all open sets $B = \overline{a} + p^k\mathbb{Z}_p^n$ where $\overline{a} \in \mathbb{N}^n$ and $k \in \mathbb{N}$. For any such an open set B, we have a procedure that stops if for all $\overline{x} \in B$, $h(\overline{x}) \neq 0$. Let $B = \overline{a} + p^R\mathbb{Z}_p^n$ be an open set with this property. It is sufficient to find an algorithm that returns true if there is $\beta \in B$ such that $g(\beta) = 0$.

Assume that such a β exists. Then, by theorem 5.1.5, there exists $g_1, \cdots, g_n \in \mathcal{P}_n$ such that $V(g) \cap V^{ns}(g_1, \cdots, g_n) \cap B \neq \varnothing$. We proceed to an enumeration of all $f_1, \cdots, f_n \in \mathcal{P}_n$. Assume that at some step of the enumeration, we have found $f_1, \cdots, f_n$ such that there exists $\alpha \in V(g) \cap V^{ns}(f_1, \cdots, f_n) \cap B$ (eventually, we will find such a system). We give now a recursive condition that will implies the existence of α. Let us remark that

(a$_1$) either $\partial g(\alpha) := \left(\frac{\partial g}{\partial x_1}, \cdots, \frac{\partial g}{\partial x_n}\right)(\alpha) \neq 0$;

(b$_1$) or, $\partial g(\alpha) := \left(\frac{\partial g}{\partial x_1}, \cdots, \frac{\partial g}{\partial x_n}\right)(\alpha) = 0$

If (a$_1$) holds, there are $\lambda_1(\alpha), \cdots, \lambda_n(\alpha) \in \mathbb{Q}_p$ not all zeros such that

$$\partial g(\alpha) = \sum_i \lambda_i(\alpha) \partial f_i(\alpha).$$

Without loss of generality, we can assume that $\lambda_1(\alpha) \neq 0$. Then,

$$\begin{vmatrix} \frac{\partial g}{\partial x_1}(\alpha) & \cdots & \frac{\partial g}{\partial x_n}(\alpha) \\ \frac{\partial f_2}{\partial x_1}(\alpha) & \cdots & \frac{\partial f_2}{\partial x_n}(\alpha) \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial x_1}(\alpha) & \cdots & \frac{\partial f_n}{\partial x_n}(\alpha) \end{vmatrix} = \lambda_1(\alpha) \begin{vmatrix} \frac{\partial f_1}{\partial x_1}(\alpha) & \cdots & \frac{\partial f_1}{\partial x_n}(\alpha) \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial x_1}(\alpha) & \cdots & \frac{\partial f_n}{\partial x_n}(\alpha) \end{vmatrix} \neq 0$$

Therefore, $\alpha \in V^{ns}(g, f_2, \cdots, f_n) \cap B$. Using algorithm 1, we can check the existence of a non-singular solution of the system $(g, f_2, \cdots, f_n)$ in B. Surely, if this the case, then our formula is satisfied in $\mathbb{Z}_p$. And if our formula is satisfied, then this system has a non-singular solution in B whenever (a$_1$) is true.

Now, assume that (b$_1$) holds. For all i, let $g_i(\alpha) := \frac{\partial g}{\partial x_i}(\alpha) = 0$. Again, we have two possibilities for each i:

(a$_2$) either $\partial g_i(\alpha) = \left(\frac{\partial g_i}{\partial x_1}, \cdots, \frac{\partial g_i}{\partial x_n}\right)(\alpha) \neq 0$;

(b$_2$) or, $\partial g_i(\alpha) = \left(\frac{\partial g_i}{\partial x_1}, \cdots, \frac{\partial g_i}{\partial x_n}\right)(\alpha) = 0$

If (a$_2$) is satisfied for some i, as before $\alpha \in V^{ns}(f_1, \cdots, f_{j-1}, g_i, \cdots, f_n)$ for some j. Also, note that $(g + g_i)(\alpha) = 0 \neq \frac{\partial(g+g_i)}{\partial x_k}(\alpha) = \frac{\partial g_i}{\partial x_k}(\alpha)$ for some k. Then, as above, $\alpha \in V^{ns}(f_1, \cdots, f_{j'-1}, g + g_i, \cdots, f_n)$ for some j'.
Let $h^{(1)} = (h_1, \cdots, h_n) := (f_1, \cdots, f_{j-1}, g_i, \cdots, f_n)$ and
$h^{(2)} = (\widetilde{h_1}, \cdots, \widetilde{h_n}) := (f_1, \cdots, f_{j'-1}, g + g_i, \cdots, f_n)$.
Let us recall that for all ε, for all $\gamma_1 \in V^{ns}(h_1, \cdots, h_n) \cap B$ and
for all $\gamma_2 \in V^{ns}(\widetilde{h_1}, \cdots, \widetilde{h_n}) \cap B$, there exist $t_1, t_2 \in \mathbb{Z}^n$ such that

$$v(t_i - \gamma_i) > \varepsilon + v(\det\ J_{h^{(i)}}(t_i)) + R$$

and that by Hensel's lemma the existence of such a t_i with

$$v(h^{(i)}(t_i)) > 2v(\det\ J_{h^{(i)}}(t_i)) + \varepsilon + R$$

implies the existence of the root γ_i in B. Also, if we enumerate all tuple in $\mathbb{Z}^n \cap B$, we can find effectively such tuples t_1, t_2.
So, we can find t_1, t_2 like above for $\varepsilon := F(h_1, \cdots, h_n, \widetilde{h_1}, \cdots, \widetilde{h_n}) + 1$ where F is the function in conjecture 5.3.1.
Now, if $v(t_1 - t_2) > \varepsilon$, then $\gamma_1 = \gamma_2$. So, we can check effectively the existence of a tuple

$$\gamma \in V^{ns}(f_1, \cdots, f_{j-1}, g_i, \cdots, f_n) \cap V^{ns}(f_1, \cdots, f_{j'-1}, g + g_i, \cdots, f_n) \cap B.$$

Let us remark that if γ is any point in this intersection, then $g(\gamma) = g(\gamma) + g_i(\gamma) = 0$ and therefore our formula is true in $\mathbb{Z}_p$. As we have seen, such a point exists if Ψ is true in B and under the conditions (b$_1$) and (a$_2$).

If (b$_2$) is satisfied for all i, we keep going this procedure inductively.
Assume that (b$_2$), $\cdots$, (b$_k$) are satisfied for all indexes at each step. Then, for each $I = (i_1, \cdots, i_k)$, $g_I := \frac{\partial^I g}{\partial x_I}(\alpha) = 0$.
We have two possibilities for all I:

(a$_{k+1}$) either $\partial g_I(\alpha) = \left(\frac{\partial g_I}{\partial x_1}, \cdots, \frac{\partial g_I}{\partial x_n}\right)(\alpha) \neq 0$;

(b$_{k+1}$) or, $\partial g_I(\alpha) = \left(\frac{\partial g_I}{\partial x_1}, \cdots, \frac{\partial g_I}{\partial x_n}\right)(\alpha) = 0$

If (a$_{n+1}$) is satisfied for some index I, we can check that our formula is true in $\mathbb{Z}_p$ like for the case (a$_2$).
If (b$_{n+1}$) is satisfied for all I, we go to the next step of the induction.

Finally, let us recall that we can find recursively an integer d such that if for all $|I| < d$, $\frac{\partial^I g}{\partial x_I}(\alpha) = 0$, then $g \equiv 0$ (see proposition 4.4.4). So, for $|I|$ large enough, the case (b$_{|I|}$) never occurs (unless $g \equiv 0$ in which case, checking the truth of the formula is trivial) and our procedure stops (if α exists). $\square$

Chapter 6

Decidability of $\mathcal{O}_{p,exp}$

Let E_p be the exponential function as before. Then, E_p can be extended canonically to an exponential function on the valuation ring of the algebraic closure of $\mathbb{Q}_p$ and on $\mathcal{O}_p$. We have seen that the theory of the structure $\mathbb{Z}_{p,exp}$ (or any of its finite algebraic extensions) is decidable if Schanuel's conjecture is true. One may ask if the same holds for the theory of the structure with underlying set $\mathcal{O}_p$ in the language of valued exponential rings. We denote this latter structure by $\mathcal{O}_{p,exp}$. The main theorem of this chapter is:

Theorem 6.0.1. *If the p-adic Schanuel's conjecture is true, then the theory of $\mathcal{O}_{p,exp}$ is decidable.*

The strategy is the same that for $\mathbb{Z}_{p,exp}$: First, we prove a result of effective model-completeness. Then, we show (assuming Schanuel's conjecture) that the existential part of the theory is decidable.

The result of model-completeness also relies on a result of quantifier elimination in the language with full (restricted) analytic structure. The result in this case is due to L. Lipshitz [7]. It turns out to be more complicated that the case $\mathbb{Z}_{p,an}$ (the main reason being that $\mathcal{O}_p$ is not locally compact). Indeed, we need to add all functions in the *ring of separated power series.* We introduce this ring and give the result of quantifier elimination in section 6.2. In section 6.3, we will discuss the effectivity of this result: let F be any family of functions in the ring of separated power series. Assuming that the set of $\mathcal{L}_F$-terms is closed under derivation and that each $f \in F$ has an effective Weierstrass set, we will show that the Weierstrass system generated by the $\mathcal{L}_F$-terms is effective. And therefore, the theory of $\mathcal{O}_p$ is effectively model-complete in the language $\mathcal{L}_F$.

Note that we didn't mention decomposition functions. In fact, in this situation, we don't need these functions. Indeed, let us recall that the Weierstrass coefficients obtained using the Weierstrass preparation theorem with a function f can be described as a polynomial combination of the zeros of f with nonnegative valuation. As our underlying set is algebraically closed, it already contains these roots and therefore we don't need to add functions to existentially define the Weierstrass coefficients.

Finally in section 6.4, we prove the main result of this chapter. But first, let us recall some basic facts on the model theory of algebraically closed valued fields.

6.1 Algebraically closed valued fields and exponential

Let K be an algebraically closed valued field (ACVF) with value group Γ. We denote by $\mathcal{L}_v = \{+, -, \cdot, 0, 1, | \}$ the language of ACVF i.e. the language of rings expanded by $|$ a binary relation symbol interpreted by

$$x|y \text{ iff } v(x) \leq v(y).$$

We may also consider the theory of ACVF in a two sorted language

$$\mathcal{L}_\Gamma := \{+_K, -_K, \cdot_K, 0_K, 1_K, v, |, +_\Gamma, -_\Gamma, 0_\Gamma, \infty_\Gamma, <_\Gamma\}.$$

Where this language is interpreted in K by:

- The first sort is K and $+_K, -_K, \cdot_K, 0_K, 1_K$ are the natural interpretations of the language of rings;
- The second sort is the value group (with the point to infinity) and $+_\Gamma, -_\Gamma, 0_\Gamma, \infty_\Gamma$, $<_\Gamma$ are the natural interpretations of the language of ordered groups;
- v is a map $K \longrightarrow \Gamma \cup \{\infty\}$ interpreted by the valuation;
- $|$ is interpreted like above.

Then, (an extension of) a classical result due to A. Robinson tell us that

Theorem 6.1.1. *The theory of ACVF is axiomatized by (i) (K, Γ, v) is a valued field, (ii) there are $x, y \in K^*$ such that $v(x) < v(y)$, (iii) K is algebraically closed, (iv) the characteristics of K and $\overline{K}$. Furthermore, this theory admits quantifier elimination in the languages $\mathcal{L}_v$ or $\mathcal{L}_\Gamma$.*

Remark. Here, we will replace v by a function symbol $|\cdot|$ interpreted by the p-adic norm. The sort Γ will be replaced by $|K^*|$.

Let $K = \mathbb{C}_p$. Then, the function $E_p : \mathcal{O}_p \longrightarrow \mathcal{O}_p : x \longmapsto exp(px)$ defines an exponential function on $\mathcal{O}_p$. We denote by $\mathcal{L}_{exp}$ the language $\mathcal{L}_v \cup \{E_p\}$ and by $\mathcal{O}_{p,exp}$ the structure with underlying set $\mathcal{O}_p$ and natural interpretations for the symbols of $\mathcal{L}_{exp}$. The goal of this chapter is to prove the decidability of the theory of $\mathcal{O}_{p,exp}$.

6.2 The ring of separated power series and quantifier elimination

As for the case of $\mathbb{Z}_p$, the quantifier elimination in the language with restricted analytic functions relies on two main facts: Weierstrass preparation theorems and quantifier elimination in the language of valued fields (theorem 6.1.1). However, as $\mathbb{C}_p$ is not locally compact, it leads to some difficulties. Instead of $\mathcal{O}_p\{\overline{X}\}$, L. Lipshitz consider in [7] functions in the ring of separated power series i.e. 'nice' power series in $\mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]$ where the variables $\overline{\rho}$ will be evaluated in the maximal ideal $\mathfrak{M}_p$ (i.e. a power series in this ring determines a function from $\mathcal{O}_p^n \times \mathfrak{M}_p^m$ to $\mathcal{O}_p$). We give now the definition of this ring:

Definition 6.2.1. *Fix π with $0 < |\pi| < 1$. Let $R_0 \subset \mathcal{O}_p$ be the maximal discrete valuation ring contained in $\mathcal{O}_p$ with prime element π and such that $R_0/(\pi) \cong \mathbb{F}_p^{alg}$.*
For all $\{a_i\}_{i\in\omega} \subset \mathcal{O}_p$ with $|a_i| \to 0$, let $R_0\{a_i\}$ be the completion of $R_0[a_i, i \in \omega]$.
Let $R_0\{a_i\}\{\overline{X}\} = \{f = \sum b_\nu \overline{X}^\nu \in R_0\{a_i\}[[\overline{X}]] \mid |b_\nu| \to 0\}$.
Let $R_0\{a_i\}\{\overline{X}\}[[\overline{\rho}]]$ be the ring of formal power series in $\overline{\rho}$ with coefficients in $R_0\{a_i\}\{\overline{X}\}$.
Then, for all ε, for all $f \in R_0\{a_i\}\{\overline{X}\}[[\overline{\rho}]]$, there is i_ε and $g \in R_0[a_0, \cdots, a_{i_\varepsilon}, \overline{X}][[\overline{\rho}]]$ such that $\|f - g\| < \varepsilon$. Also, $R_0\{a_i\}\{\overline{X}\}[[\overline{\rho}]]$ is complete.
Let $S\{a_i\}\{\overline{X}\}[[\overline{\rho}]] = \{\pi^{-\alpha} f \mid \alpha \in \mathbb{N}, f \in R_0\{a_i\}\{\overline{X}\}[[\overline{\rho}]]\}$. We define the ring of

separated power series *by:*

$$\mathbb{C}_p\{\overline{X}\}[[\overline{\rho}]]_s := \bigcup_{\{a_i\}} S\{a_i\}\{\overline{X}\}[[\overline{\rho}]]$$

where the union is taken over all sequences $\{a_i\}$ like above. Let $\mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ be the ring of all $f \in \mathbb{C}_p\{\overline{X}\}[[\overline{\rho}]]_s$ with $\|f\| \leq 1$ i.e.

$$\mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s = \bigcup_{\{a_i\}} R_0\{a_i\}\{\overline{X}\}[[\overline{\rho}]].$$

Let $f(\overline{X}, \rho) \in \mathcal{O}_p\{x\}[[\overline{\rho}]]_s$. Then, f determines a function from $\mathcal{O}_p^n \times \mathfrak{M}_p^m$ to $\mathcal{O}_p$. Note also that

Lemma 6.2.2. *Let $f \in \mathcal{O}_p[\overline{X}, \overline{\rho}]^{E_p}$, then $f \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$.*

This follows immediately from the definitions. Actually, we have that for any $f \in \mathbb{Z}_p\{\overline{X}, \overline{Y}, \overline{Z}\}$, for any $\overline{z} \in \mathcal{O}_p^k$, $f(\overline{X}, \overline{\rho}, \overline{z}) \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$.
It turns out that the ring $\mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ is closed under (some appropriate versions of the) Weierstrass division with respect to the variables $\overline{X}$ and $\overline{\rho}$. We state now these results. We take the following notation: if $\overline{y} = (y_1, \cdots, y_n)$ is a tuple, $\overline{y}' := (y_1, \cdots, y_{n-1})$.

Definition 6.2.3. *Let $f = \sum a_i(\overline{X}', \overline{\rho})\overline{X}_M^i \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ where $a_i \in \mathcal{O}_p\{\overline{X}'\}[[\overline{\rho}]]_s$. Suppose that a_k is a unit and that for all $i > l$, $a_i = b_i + \overline{\rho}c_i$ for some $b_i, c_i \in \mathcal{O}_p\{\overline{X}'\}[[\overline{\rho}]]_s$ with $\|b_i\| < 1$. Then, we say that f is* regular in X_M of order l*. We say that f is* regular in X_M *if it is regular of order n for some n.*

Remark. If $f \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$, then f is a unit if $f = 1 - g - h$ where $g \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$, $\|g\| < 1$ and $h \in (\overline{\rho})\mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$. In this case, $f^{-1} = \sum_l (g + h)^l$.

In order words, f is regular of order l in X_M if f is congruent to a monic polynomial of degree l in X_M modulo the ideal generated by $\mathfrak{M}_p$ and $\overline{\rho}$.
The next result is due to L. Lipshitz (proposition 2.3.1 in [7]):

Proposition 6.2.4. *[Weierstrass division theorem with respect to the variables $\overline{X}$] Let $f \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ regular in X_M of order l, $g \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ with $\|g\| = 1$. Then, there are $q \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$, $r_0, \cdots, r_{l-1} \in \mathcal{O}_p\{\overline{X}'\}[[\overline{\rho}]]_s$ such that*

$$g = qf + \sum_{i<l} r_i X_M^i.$$

In particular, for $g = X_M^l$, we have $f = \left(X_M^l - \sum r_i X_M^i\right) U$ where $U \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ is a unit.

Note that in the last case, for all $\overline{x} \in \mathcal{O}_p^M$, for all $\overline{\omega} \in \mathfrak{M}_p^N$,

$$f(\overline{x}, \overline{\omega}) = 0 \text{ iff } x_M^l - \sum r_i(\overline{x}', \overline{\omega}) x_M^i = 0.$$

And for all $\overline{x}', \overline{\omega}$, $f(\overline{x}', X_M, \overline{\omega})$ has exactly l roots with in $\mathcal{O}_p$ (counting multiplicities)

We define now regularity with respect to the variables $\overline{\rho}$

Definition 6.2.5. *Let $f = \sum a_\nu(\overline{X})\overline{\rho}^\nu \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ such that $\|f\| = 1$, $a_{(0,\cdots,0,l)} = 1$ and for all $\nu = (0, \cdots, 0, i)$, $i < l$, $\|a_\nu\| < 1$. We say that f is* regular in ρ_N of order *l. We say that f is* regular in ρ_N *if it is regular of order n for some n.*

In other words, f is congruent to ρ_N^l modulo the ideal generated by $\mathfrak{M}_p$, $\rho_1, \cdots, \rho_{N-1}$ and ρ_N^{l+1}.

We have a preparation result for the variables $\overline{\rho}$ (proposition 2.4.1 in [7]):

Proposition 6.2.6. *[Weierstrass preparation theorem with respect to the variables $\overline{\rho}$] Let $f \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ regular in ρ_N of order l, $g \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ with $\|g\| = 1$. Then, there are $q \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$, $r_0, \cdots, r_{l-1} \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}']]_s$ such that*

$$g = qf + \sum_{i<l} r_i \rho_N^i.$$

In particular, for $g = \rho_N^l$, we get $f = \left(\rho_N^l - \sum r_i \rho_N^i\right) U$ where $U \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ is a unit and furthermore $r_i = r_i' + \rho' r_i''$ with $\|r_i'\| < 1$ and $\|\rho' r_i''\| \leq 1$.

Again in the last case, for all $\overline{x} \in \mathcal{O}_p^M$, for all $\overline{\omega} \in \mathfrak{M}_p^N$,

$$f(\overline{x}, \overline{\omega}) = 0 \text{ iff } \omega_N^l - \sum r_i(\overline{x}', \overline{\omega}) \omega_N^i = 0.$$

And for all $\overline{x}, \overline{\omega}'$, $f(\overline{x}, \overline{\omega}', \rho_N)$ has exactly l roots with in $\mathfrak{M}_p$ (counting multiplicities)

We consider the structure $\mathcal{O}_p$ in the 3-sorted language $\mathcal{L}_{v,M}$ with sorts:

(1) $\mathcal{O}_p$, the valuation ring. We have in the language symbols for the functions $+, \cdot, -, 0, 1$ (This sort will be called sort 1);

(2) $\mathfrak{M}_p$ its maximal ideal (called sort 2). We have symbols for the functions $+, \cdot, -, 0, 1$;

(3) $|\mathbb{C}_p|$ the valuation group (called sort 3) in the language of ordered groups.

Also, we also add a symbol for the functions $|.| : \mathcal{O}_p \longrightarrow |\mathbb{C}_p|$.
We will consider the sort $\mathfrak{M}_p$ as a subset $\mathcal{O}_p$. So, any function, variable or constant of the sort $\mathfrak{M}_p$ will also be considered as a function, variable or constant of the sort $\mathcal{O}_p$.
We denote by $\mathcal{L}_{an}$ the expansion of $\mathcal{L}_{v,M}$ where we add function symbols for each $f \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$. We define division symbols on $\mathcal{O}_p$:

$$D_0(x,y) : \mathcal{O}_p^2 \longrightarrow \mathcal{O}_p : (x,y) \longmapsto \begin{cases} x/y & \text{if } |x| \leq |y| \neq 0 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$D_1(x,y) : \mathcal{O}_p^2 \longrightarrow \mathfrak{M}_p : (x,y) \longmapsto \begin{cases} x/y & \text{if } |x| < |y| \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Then, $\mathcal{L}_{an}^D$ denotes $\mathcal{L}_{an} \cup \{D_0, D_1\}$.

Theorem 6.2.7. *[L. Lipshitz [7] theorem 3.8.1]* $(\mathcal{O}_p, \mathfrak{M}_p, |\mathbb{C}_p|)$ *admits elimination of quantifiers in* $\mathcal{L}_{an}^D$.

It is immediate from the proof that we don't need to add all the function symbols in the ring of separated power series to get quantifier elimination. It is sufficient to add symbols for a family of functions closed under Weierstrass division (with respect to the variables of sort 1 and sort 2). As in chapter 3, we define:

Definition 6.2.8. *A* separated Weierstrass system *over* $\mathcal{O}_p$ *is a family of rings* $\mathcal{O}_p[\![X_1, \cdots, X_n, \rho_1, \cdots, \rho_m]\!]_s$, $n, m \in \mathbb{N}$, *such that for all* n, m, *the following conditions hold:*

1. $\mathbb{Z}[\overline{X}, \overline{\rho}] \subseteq \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s \subseteq \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$;

2. *For all permutations* σ *of* $\{1, \cdots, n\}$ *and* τ *of* $\{1, \cdots, m\}$, *if* $f(\overline{X}, \overline{\rho}) \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s$, *then* $f(X_{\sigma(1)}, \cdots, X_{\sigma(n)}, \rho_{\tau(1)}, \cdots, \rho_{\tau(m)}) \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s$;

3. *If* $f \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s$ *and* $p^q f \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]$ *(where* $q \in \mathbb{Q}$*), then* $p^q f \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s$;

4. *If* $f \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s$ *has an inverse* g *in* $\mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]$, *then* $g \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s$;

5. *(Weierstrass division with respect to variables of sort 1) If* $f \in \mathcal{O}_p[\![\overline{X}', X_{n+1}, \overline{\rho}]\!]_s$ *and* f *is regular of order* d *in* X_{n+1}, *then, for all* $g \in \mathcal{O}_p[\![\overline{X}', X_{n+1}, \overline{\rho}]\!]_s$ *with* $\|g\| = 1$, *there are* $r_0, \cdots, r_{d-1} \in \mathcal{O}_p[\![\overline{X}', \overline{\rho}]\!]_s$ *and* $Q \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s$ *such that*

$$g(\overline{X}, \overline{\rho}) = Q(\overline{X}, \overline{\rho}) \cdot f(\overline{X}, \overline{\rho}) + \Big(X_{n+1}^{d-1} r_{d-1}(\overline{X'}, \overline{\rho}) + \cdots + r_0(\overline{X'}, \overline{\rho})\Big).$$

6. *(Weierstrass division with respect to variables of sort 2) If $f \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}', \rho_{m+1}]\!]_s$ and f is regular of order d in ρ_{m+1}, then, for all $g \in \mathcal{O}_p[\![\overline{X}', \overline{\rho}]\!]_s$ with $\|g\| = 1$, there are $r_0, \cdots, r_{d-1} \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}']\!]_s$ and $Q \in \mathcal{O}_p[\![\overline{X}, \overline{\rho}]\!]_s$ such that*

$$g(\overline{X}, \overline{\rho}) = Q(\overline{X}, \overline{\rho}) \cdot f(\overline{X}, \overline{\rho}) + \Big(\rho_{m+1}^{d-1} r_{d-1}(\overline{X}, \overline{\rho}') + \cdots + r_0(\overline{X}, \overline{\rho}')\Big).$$

Let W be a separated Weierstrass system. We denote by $\mathcal{L}_W$ the expansion of $\mathcal{L}_{v,M}$ by function symbols for elements in W. $\mathcal{L}_W^D$ denotes the expansion of $\mathcal{L}_W$ by D_0, D_1. Then, it is immediate from the proof of theorem 6.2.7 that

Theorem 6.2.9. *$(\mathcal{O}_p, \mathfrak{M}_p, |\mathbb{C}_p|)$ admits elimination of quantifiers in $\mathcal{L}_W^D$.*

Let F be a family of separated power series. As in chapter 3, we can define the separated Weierstrass system generated by the $\mathcal{L}_F$-terms. We denote this system by W_F.

Let us remark that if the set of $\mathcal{L}_F$-terms is closed under derivation, then any function $f \in W_F$ is existentially definable. Indeed, let f be a separated power series regular of order d (with respect to a variable of sort 1 or 2) and g with $\|g\| = 1$. Then, the functions defined by the Weierstrass division are existentially definable in terms of the derivatives of f and g. This is an easy consequence of proposition 3.4.1. In fact, we can use the same existential definitions that those given in this proposition. Note that here we don't need to use decomposition functions: our field is already algebraically closed and therefore the roots of f with nonnegative (resp. positive) valuation live in our structure. From this, we can show by induction on the complexity of the function $f \in W_F$ that f is existentially definable in terms of a finite number of functions in F (and their derivatives). Therefore,

Theorem 6.2.10. *Let F be a family of separated power series. Assume that the set of $\mathcal{L}_F$-terms is closed under derivation. Then, $(\mathcal{O}_p, \mathfrak{M}_p, |\mathbb{C}_p|)$ is model-complete in $\mathcal{L}_F$.*

Now, note that any $\mathcal{L}_{exp}$-formula is equivalent to a $\mathcal{L}_{\{E_p\}}$-formula in $\mathbb{C}_p$. And, it is obvious that the set of $\mathcal{L}_{\{E_p\}}$-terms is closed under derivation. So,

Theorem 6.2.11. *The theory of the structure $\mathcal{O}_{p,exp}$ is model-complete.*

6.3 Effective model-completeness

In this section, we want to prove the effectivity of theorem 6.2.11. As for the case of $\mathbb{Z}_{p,exp}$, we are reduced to compute an effective 'Weierstrass bound'. Indeed, if we inspect to proof of theorem 6.2.7 in [7], we see that every step is effective except for the use of proposition 2.7.1. In fact, this proposition use the fact that the ring $\mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$ is Noetherian and therefore may not be effective. We recall this proposition:

Proposition 6.3.1. *[L. Lipshitz [7] proposition 2.7.1] Let $f = \sum a_{\mu\nu}(\overline{X},\overline{\lambda})\overline{Y}^{\mu}\overline{\rho}^{\nu} \in \mathcal{O}_p\{\overline{X},\overline{Y}\}[[\overline{\lambda},\overline{\rho}]]_s$. Then, there is a finite set $\Gamma_f = \Gamma_{f_1}\times\Gamma_{f_2} \subseteq \mathbb{N}^M \times \mathbb{N}^N$ such that for all $(\alpha,\beta) \in \mathbb{N}^{M+N}$ and for all $(\mu,\nu)\in\Gamma_f$, there are $g_{\mu\nu\alpha\beta}(\overline{X},\overline{\lambda}) \in \mathcal{O}_p\{\overline{X}\}[[\overline{\lambda}]]_s$ such that:*

(i) $a_{\alpha\beta}(\overline{X},\overline{\lambda}) = \sum_{(\mu,\nu)\in\Gamma_f} g_{\mu\nu\alpha\beta}(\overline{X},\overline{\lambda})a_{\mu\nu}(\overline{X},\overline{\lambda})$; and,

(ii) if $\beta \notin \Gamma_{f_2}$ and there is $\nu_0 \in \Gamma_{f_2}$ with $\beta < \nu_0$, then for all $(\mu,\nu)\in\Gamma_f$ with $\nu > \beta$ and all $\alpha \in \mathbb{N}^M$, $g_{\alpha\beta\mu\nu} \in (\mathfrak{M}_p,\overline{\lambda})\mathcal{O}_p\{\overline{X}\}[[\lambda]]_s$; and,

(iii) for all $\nu_0 \in \Gamma_{f_2}$, for all $\alpha \notin \Gamma_{f_1}$, $g_{\mu\nu\alpha\nu_0} \in (\mathfrak{M}_p,\overline{\lambda})\mathcal{O}_p\{\overline{X}\}[[\lambda]]_s$.

Let $f = \sum a_\nu(\overline{X})\overline{\rho}^\nu \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$. Suppose that $a_{\nu_0} = 1$ and $\|a_\nu\| < 1$ for all $\nu < \nu_0$. In this case, we say that f is *preregular of order* ν_0. Then, we can make a change of variables of the type

$$\begin{cases} \rho_i \to \rho_i + \rho_n^{e_i} \text{ for } i < N \\ \rho_n \to \rho_N \end{cases}$$

for suitable choice of e_i such that f is regular in ρ_n. Similarly, let $f = \sum a_\mu(\overline{X},\overline{\rho})\overline{Y}^\mu$ with $a_{\mu_0} = 1$ and for all $\mu > \mu_0$, $a_\mu = b_\mu + \rho c_\mu$ where $\|b_\mu\| < 1$ and $\|\rho c_\mu\| \leq 1$. In this case, we say that f is *preregular of order* μ_0. Then after a change of variables of the type

$$\begin{cases} y_i \to y_i + y_M^{e_i} \text{ for } i < M \\ y_M \to y_M \end{cases}$$

for suitable choice of e_i, f is regular in y_M.

It means that if f is preregular of order μ_0 or ν_0 then after a change of variables it becomes regular. Note that these change of variables can be done effectively.

Let $f(\overline{X},\overline{Y},\overline{\lambda},\overline{\rho}) = \sum_{\mu,\nu} a_{\mu\nu}(\overline{X},\overline{\lambda})\overline{Y}^\mu\overline{\rho}^\nu$. Then, we say that f is preregular of order

(μ_0, ν_0) if $a_{\mu_0\nu_0} = 1$ and for all $\nu < \nu_0$ and all μ or for $\nu = \nu_0$ and all $\mu > \mu_0$, $a_{\mu\nu} \in (\mathfrak{M}_p, \overline{\lambda})\mathcal{O}_p\{\overline{X}\}[[\overline{\lambda}]]_s$. In this case, $\sum_\mu a_{\mu\nu_0}(\overline{X}, \overline{\lambda})\overline{Y}^\mu$ is preregular of order μ_0. Then, the set Γ_f of in proposition 6.3.1 determines a bound on the order of preregularity:

Let $f = \sum a_{\mu\nu}(\overline{X}, \overline{\lambda})\overline{Y}^\mu \overline{\rho}^\nu \in \mathcal{O}_p\{\overline{X}, \overline{Y}\}[[\overline{\lambda}, \overline{\rho}]]_s$. Fix $\overline{x} \in \mathcal{O}_p^N, \omega \in \mathfrak{M}_p^M$. Then(if f is not identically zero), there is $\widetilde{f}(\widetilde{x}, \overline{Y}, \widetilde{\omega}, \overline{\rho}) \in \mathcal{O}_p\{\overline{Y}\}[[\overline{\rho}]]_s$ preregular of order (μ_0, ν_0) for some $(\mu_0, \nu_0) \in \Gamma_f$ and such that

$$f(\overline{x}, \overline{Y}, \overline{\omega}, \overline{\lambda}) = a_{\mu_0,\nu_0}(\overline{x}, \overline{\omega})\widetilde{f}(\widetilde{x}, \overline{Y}, \widetilde{\omega}, \overline{\rho}).$$

Let $\Gamma := \Gamma_f$ and fix J a finite subset of Γ and $(\mu_0, \nu_0) \in J$. We define the first-order formula

$$\begin{aligned} M_{J,(\mu_0,\nu_0)}(\overline{X}, \overline{\lambda}) \equiv & \bigwedge_{(\mu,\nu)\in J\setminus\{(\mu_0,\nu_0)\}} |a_{\mu\nu}(\overline{X}, \overline{\lambda})| = |a_{\mu_0\nu_0}(\overline{X}, \overline{\lambda})| \\ & \wedge a_{\mu_0\nu_0}(\overline{X}, \overline{\lambda}) \neq 0 \wedge \\ & \bigwedge_{(\mu,\nu)\in\Gamma\setminus J} |a_{\mu\nu}(\overline{X}, \overline{\lambda})| < |a_{\mu_0\nu_0}(\overline{X}, \overline{\lambda})|. \end{aligned}$$

If none of the formula $M_{J,(\mu_0,\nu_0)}(\overline{x}, \overline{\omega})$ is satisfied in $\mathcal{O}_p$ then

$$f(\overline{x}, \overline{Y}, \overline{\omega}, \overline{\lambda}) \equiv 0.$$

Otherwise, there is a non-empty $J \subset \Gamma$ such that $\mathcal{O}_p \models M_{J,(\mu_0,\nu_0)}(\overline{x}, \overline{\omega})$ for some $(\mu_0, \nu_0) \in J$ (ν_0 is the smallest ν such that $(\mu, \nu) \in J$ for some μ and μ_0 is the largest μ such that $(\mu, \nu_0) \in J$). In that case,

$$a_{\mu\nu} = a_{\mu_0\nu_0} D_0(a_{\mu\nu}, a_{\mu_0\nu_0}) \qquad \forall(\mu, \nu) \in J \setminus \{(\mu_0, \nu_0)\},$$

and

$$a_{\mu\nu} = a_{\mu_0\nu_0} D_1(a_{\mu\nu}, a_{\mu_0\nu_0}) \qquad \forall(\mu, \nu) \in \Gamma \setminus J.$$

Furthermore, for all $(\alpha, \beta) \notin \Gamma$,

$$\begin{aligned} a_{\alpha\beta} &= \sum_{(\mu,\nu)\in\Gamma} g_{\mu\nu\alpha\beta} a_{\mu\nu} \\ &= \sum_{\substack{(\mu,\nu)\in J \\ (\mu,\nu)\neq(\mu_0,\nu_0)}} g_{\mu\nu\alpha\beta} a_{\mu_0\nu_0} D_0(a_{\mu\nu}, a_{\mu_0\nu_0}) + g_{\mu_0\nu_0\alpha\beta} a_{\mu_0\nu_0} \\ &\quad + \sum_{(\mu,\nu)\in\Gamma\setminus J} g_{\mu\nu\alpha\beta} a_{\mu_0\nu_0} D_1(a_{\mu\nu}, a_{\mu_0\nu_0}), \end{aligned}$$

where $g_{\mu\nu\alpha\beta}$ are like in proposition 6.3.1. So,

$$\begin{aligned} f = a_{\mu_0\nu_0}\Big\{ & \sum_{\substack{(\mu,\nu)\in J\\(\mu,\nu)\neq(\mu_0,\nu_0)}} D_0(a_{\mu\nu}, a_{\mu_0\nu_0})\overline{Y}^{\mu}\overline{\rho}^{\nu} + \overline{Y}^{\mu_0}\overline{\rho}^{\nu_0} \\ & + \sum_{(\mu,\nu)\in\Gamma\setminus J} D_1(a_{\mu\nu}, a_{\mu_0\nu_0})\overline{Y}^{\mu}\overline{\rho}^{\nu} \\ & + \sum_{(\alpha,\beta)\notin\Gamma}\Big[\sum_{\substack{(\mu,\nu)\in J\\(\mu,\nu)\neq(\mu_0,\nu_0)}} g_{\mu\nu\alpha\beta}D_0(a_{\mu\nu}, a_{\mu_0\nu_0}) \\ & + g_{\mu_0\nu_0\alpha\beta} + \sum_{(\mu,\nu)\in\Gamma\setminus J} g_{\mu\nu\alpha\beta}D_1(a_{\mu\nu}, a_{\mu_0\nu_0})\Big]\overline{Y}^{\alpha}\overline{\rho}^{\beta}\Big\} \\ =: {} & a_{\mu_0\nu_0}f'. \end{aligned}$$

Let $\widetilde{f}$ be the power series where we replace the $D_0(a_{\mu\nu}, a_{\mu_0\nu_0})'s$ by new variables $X_{\mu\nu}$ of sort 1 and the $D_1(a_{\mu\nu}, a_{\mu_0\nu_0})$'s by new variables $\lambda_{\mu\nu}$ of sort 2. By the properties of $g_{\mu\nu\alpha\beta}$, $\widetilde{f}$ is preregular of order $(\mu_0, \nu_0) \in \Gamma$.

Definition 6.3.2. *Let f be a separated power series. We say that f has* an effective Weierstrass set *if one can compute a set Γ_f like in proposition 6.3.1. We say that a separated Weierstrass system W is* effective *if there is a recursive procedure which takes for entry a function f in W and return a set Γ_f like in proposition 6.3.1.*

Lemma 6.3.3. *Let $f \in \mathbb{Z}[\overline{X}, \overline{Y}, \overline{\rho}, \overline{\lambda}]^{E_p}$. Then, f has an effective Weierstrass set.*

Proof. Fix $\overline{x} \in \mathcal{O}_p^N$ and $\overline{\omega} \in \mathfrak{M}_p^M$ such that $\mathcal{O}_p \models M_{J,(\mu_0,\nu_0)}(\overline{x}, \overline{\omega})$ for some non-empty $J \subset \Gamma_f$. Let $\mu_0 = (\mu_1, \cdots, \mu_I)$ and $\nu_0 = (\nu_1, \cdots, \nu_J)$.

Fix j an index such that $\nu_j \neq 0$. If such an index exists, we can assume $j = J$. Then, up to a change of variables (which will be denoted by T_J), the function $\widetilde{f}$ (as defined before) is regular in $T_J(\lambda_J)$ of order $S(J)$. So, the function $T_J(\widetilde{f}(\overline{x}, \overline{y}, \overline{\omega}, \overline{\tau}', \lambda_J))$ has exactly $S(J)$ roots in $\mathfrak{M}_p$ respectively.

If there is no index j such that $\nu_j \neq 0$, let i be an index such that $\mu_i \neq 0$. Without loss of generality, we may assume $i = I$. Then, up to a change of variables (which will be denoted by T_I), the function $\widetilde{f}$ (as defined before) is regular in $T_I(Y_I)$ of order $S(I)$. So, the functions $T_I(\widetilde{f}(\overline{x}, \overline{y}', Y_I, \overline{\omega}, \overline{\tau}))$ has exactly $S(I)$ roots in $\mathcal{O}_p$.

Note that in both case these roots are in one-to-one correspondence with the roots of $f(\overline{x}, \overline{y}', Y_I, \overline{\omega}, \overline{\tau})$ and $f(\overline{x}, \overline{y}, \overline{\omega}, \overline{\tau}', \lambda_J))$ respectively.
As f has an effective Weierstrass bound (in the sense chapter 4), one can compute a bound on $S(I)$ and $S(J)$. Let S be a upper bound of all possible $S(k)$'s computed as above. Then, we conclude that Γ_f is contained in the (computable) set

$$\{(\mu, \nu) \mid \ \mu_i, \nu_j \leq S \text{ for all } i \leq I, j \leq J\}.$$

□

Note that if $f \in \mathbb{Z}_p\{\overline{X}, \overline{Y}\}$ has an effective Weierstrass bound, then the separated power series $f(\overline{X}, \overline{\rho})$ has an effective Weierstrass set. This follows from the proof of the above lemma. Let us also remark that as in chapter 4, if we want to compute the effective Weierstrass set of a function $f \in \mathcal{O}_p\{\overline{X}\}[[\overline{\rho}]]_s$, it is sufficient to bound effectively the number of roots (counting multiplicities) of the function in $\mathcal{O}_p$ (resp. in $\mathfrak{M}_p$) uniformly over the parameters $(x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_N, \overline{\rho}) \in \mathcal{O}_p^{N-1} \times \mathfrak{M}_p^M$ (resp. the parameters $(\overline{x}, \rho_1, \cdots, \rho_{i-1}, \rho_{i+1}, \cdots, \rho_M) \in \mathcal{O}_p^N \times \mathfrak{M}_p^{M-1})$ for all i whenever for this choice of parameters this number is finite.

Let F be an effective family of separated power series such that each $f \in F$ has an effective Weierstrass set. Let W_F be the separated Weierstrass system generated by the $\mathcal{L}_F$-terms. We want to prove that W_F is an effective separated Weierstrass system. Fix $f \in W_F$. We have to prove that f has an effective Weierstrass set. We use the same strategy that in chapter 4: we proceed by induction on the complexity of f and prove that one can compute the Weierstrass set in terms of the Weierstrass sets of $f_1, \cdots, f_n$ (and their derivatives) where f_i's are the functions involved in the existential definition of f.
For this, we use the same results of tropical analytic geometry to compute a bound on the number of roots of f uniformly over the choice of parameters. Note that in the case where we want to bound the number of roots in $\mathfrak{M}_p$, we use the results to estimate the number of roots with valuation in $[1/n, \infty)$ and prove that the bound does not depend on the choice of n (for all n large enough).
To do this, as we have seen in chapter 4, it is sufficient to prove the following:

Lemma 6.3.4. *Let $f \in \mathcal{O}_p\{\overline{X}, \overline{Y}\}[[\overline{\rho}, \overline{\lambda}]]_s$ such that f and all its derivatives have an effective Weierstrass set. Then, we can effectively find an integer $E(f)$ such that for all $\overline{x} \in \mathcal{O}_p^R$, for all $\overline{\omega} \in \mathfrak{M}_p^S$, either $f(\overline{x}, \overline{Y}, \overline{\omega}, \overline{\lambda})$ is identically zero or $New(f(\overline{x}, \overline{Y}, \overline{\omega}, \overline{\lambda})) \subseteq B_{\max}(E(f))$.*

Proof. Let $f(\overline{X}, \overline{Y}, \overline{\rho}, \overline{\lambda}) = \sum_{(\mu,\nu)} a_{\mu\nu}(\overline{X}, \overline{\rho})\overline{Y}^{\mu}\overline{\lambda}^{\nu}$. Note that if f is identically zero the lemma is trivially satisfied. Fix $\overline{x}, \overline{\omega}$ such that $f(\overline{x}, \overline{Y}, \overline{\omega}, \overline{\lambda})$ is not identically zero. To keep the notation simpler, we will not indicate the parameters $\overline{x}, \overline{\omega}$ anymore. So, $f(\overline{x}, \overline{Y}, \overline{\omega}, \overline{\lambda})$ will be denoted by $f(\overline{Y}, \overline{\lambda})$ (similarly for the coefficients $a_{\mu\nu}$).

Let us recall that $New(f) := New(f(\overline{Y}, \overline{\lambda}))$ is the collection of cells which are the convex closure of

$$\pi\big(vert_{(\overline{v},\overline{w})}(f)\big) = \big\{(\mu_0, \nu_0) \mid \ v(a_{\mu_0\nu_0}) + \langle \mu_0\nu_0, \overline{vw}\rangle = min_{(\mu,\nu)}\{v(a_{\mu\nu}) + \langle \mu\nu, \overline{vw}\rangle\}\big\},$$

where $\overline{v} \in [0,\infty)^N, \overline{w} \in [1/n, \infty)^M$ (for some fixed n), and $\langle \cdot,\cdot\rangle$ denotes the usual scalar product.

We will prove that there exists a (computable) finite set $\widetilde{\Gamma}$ such that for all $(\mu,\nu) \notin \widetilde{\Gamma}$, for all $\overline{v} \in [0,\infty)^N, \overline{w} \in (0,\infty)^M$,

$$(\mu,\nu) \notin \pi\big(vert_{(\overline{v},\overline{w})}(f)\big).$$

In particular, we will show that for all $(\mu,\nu) \notin \widetilde{\Gamma}$, there is $(\mu_0,\nu_0) \in \widetilde{\Gamma}$ such that

$$v(a_{\mu\nu}) + \langle \mu, \overline{v}\rangle + \langle \nu, \overline{w}\rangle > v(a_{\mu_0\nu_0}) + \langle \mu_0, \overline{v}\rangle + \langle \mu_0, \overline{w}\rangle.$$

In that case, $New(f) \subseteq \widetilde{\Gamma}$ (independently of the choice of n).

Let $\Gamma_f = \Gamma_1 \times \Gamma_2$ like in proposition 6.3.1. Then, for all (α,β)

$$a_{\alpha\beta} = \sum_{(\mu,\nu)\in\Gamma_f} g_{\mu\nu\alpha\beta}a_{\mu\nu}.$$

We define

$$T = \max_{(\mu,\nu)\in\Gamma_f} \max_{\substack{1\le i\le N\\ 1\le j\le M}} \{\mu_i, \nu_j\},$$

and

$$\Gamma_B := \{(\mu,\nu) \mid \mu_i \le T, \nu_j \le T \text{ for all } i,j\} = \Gamma_{B1} \times \Gamma_{B2},$$

where $\mu = (\mu_1, \cdots, \mu_N),\ \nu = (\nu_1, \cdots, \nu_M)$.

We show the existence of $\widetilde{\Gamma}$ by induction on (N, M).

First, we prove the basic steps:

- If $N=1, M=0$. Let $\alpha \notin \Gamma_{B1}$. Then,

$$\begin{aligned} v(a_\alpha)+\langle\alpha,v\rangle &\geq \min_{\mu\in\Gamma_1}\{v(a_\mu)+v(g_{\mu\alpha})\}+\langle\alpha,v\rangle \\ &= v(a_{\mu_0})+v(g_{\mu_0\alpha})+\langle\alpha,v\rangle \text{ for some } \mu_0\in\Gamma_1 \\ &> v(a_{\mu_0})+\langle\mu_0,v\rangle, \end{aligned}$$

  as $v(g_{\mu_0\alpha})>0$ and $\alpha>\mu_0$. We take $\widetilde{\Gamma}=\Gamma_B$.

- If $N=0, M=1$. Let $\beta\notin\Gamma_{B2}$. Then,

$$\begin{aligned} v(a_\beta)+\langle\beta,w\rangle &\geq \min_{\nu\in\Gamma_2}\{v(a_\nu)+v(g_{\nu\beta})\}+\langle\beta,w\rangle \\ &= v(a_{\nu_0})+v(g_{\nu_0\beta})+\langle\beta,v\rangle \text{ for some } \nu_0\in\Gamma_2 \\ &> v(a_{\nu_0})+\langle\nu_0,w\rangle, \end{aligned}$$

  as $v(g_{\nu_0\beta})\geq 0$, $\beta>\nu_0$ and $w>0$. We take $\widetilde{\Gamma}=\Gamma_B$.

We take the following notations: $\overline{Z}:=(\overline{Y},\overline{\lambda})$, $\overline{u}:=(\overline{v},\overline{w})$ and if $\overline{x}=(x_1,\cdots,x_n)$ then $\check{x}_i:=(x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n)$.

We give now the construction of $\widetilde{\Gamma}$ in the general case:

- First, let us remark that that if $\gamma=(\alpha,\beta)$ is such that $\gamma_i>T$ for all i, then

$$\begin{aligned} v(a_{\alpha\beta})+\langle\gamma,\overline{u}\rangle &\geq \min_{(\mu,\nu)\in\Gamma_f}\{v(a_{\mu\nu})+v(g_{\mu\nu\alpha\beta})\}+\langle\gamma,\overline{u}\rangle \\ &= v(a_{\mu_0\nu_0})+v(g_{\mu_0\nu_0\alpha\beta})+\langle\gamma,\overline{u}\rangle \text{ for some } \gamma_0=(\mu_0,\nu_0)\in\Gamma_f \\ &> v(a_{\mu_0\nu_0})+\langle\gamma_0,\overline{u}\rangle, \end{aligned}$$

  as $v(g_{\mu_0\nu_0\alpha\beta})>0$ if $\nu_0=(0,\cdots,0)$ and for all i,j,k $\alpha_i>\mu_{0i}$, $\beta_j>\nu_{0j}$ and $w_k>0$.

- Let $1\leq k\leq M+N$ and $1\leq s\leq T$. Fix $\gamma\notin\Gamma_B$ such that $\gamma_k=s$. We define

$$f_{s,k}=\frac{1}{s!}\frac{\partial^s f}{\partial Z_k^s}(Z_1,\cdots,Z_{k-1},0,Z_{k+1},\cdots,Z_{M+N})=:\sum b_{\check{\gamma}_k}\check{Z}_k^{\check{\gamma}_k}.$$

  Then, $a_\gamma\overline{Z}^\gamma=b_{\check{\gamma}_k}\overline{Z}^\gamma$. So,

$$v(a_\gamma)+\langle\gamma,\overline{u}\rangle=v(b_{\check{\gamma}_k})+\langle\gamma,\overline{u}\rangle.$$

Furthermore, $\Gamma_{f_{s,k}} = \Gamma_{\frac{\partial^s f}{\partial Z_k^s}}$ (and is computable by hypothesis). Also, by inductive hypothesis, there is a computable $\widetilde{\Gamma}(f_{s,k})$ such that for all $\check{\gamma}_k \notin \widetilde{\Gamma}(f_{s,k})$,

$$v(b_{\check{\gamma}_k}) + \langle \check{\gamma}_k, \check{u}_k \rangle > v(b_{\check{\gamma}_{k0}}) + \langle \check{\gamma}_{k0}, \check{u}_k \rangle$$

for some $\check{\gamma}_{k0} = (\gamma_{01}, \cdots, \gamma_{0M+N-1}) \in \widetilde{\Gamma}(f_{s,k})$.

So, we have that for all γ such that $\gamma_k = s$ there is γ_0 such that $\gamma_{0k} = s$, $\check{\gamma}_{0k} \in \widetilde{\Gamma}(f_{s,k})$ and

$$v(a_\gamma) + \langle \gamma, \overline{u} \rangle > v(a_{\gamma_0}) + \langle \gamma_0, \overline{u} \rangle$$

We set

$$\check{\Gamma}(f_{s,k}) := \{\gamma \mid \gamma_k = s,\ \check{\gamma}_k \in \widetilde{\Gamma}(f_{s,k})\}.$$

Let $\Gamma' := \Gamma_B \bigcup_{1 \le k \le M+N} \bigcup_{1 \le s \le T} \check{\Gamma}(f_{s,k})$. Let $E(f) = \max_{(\mu,\nu)\in\Gamma'} \max_{i,j}\{\mu_i, \nu_j\}$ and $\widetilde{\Gamma}(f) = \{(\mu,\nu) \mid\ \mu_i \le E(f), \nu_j \le E(f) \text{ for all } i \le M, j \le N\}$.

Then, by definitions, $\widetilde{\Gamma}$ has the required properties and $E(f)$ satisfies the conditions of the lemma.

This concludes the proof of the lemma.

□

From this lemma and arguing like in chapter 4, we can prove:

Theorem 6.3.5. *Let F be an effective family of separated power series. Assume that the set of $\mathcal{L}_F$-terms is closed under derivation and that each $\mathcal{L}_F$-term has an effective Weierstrass set. Then, the theory of $(\mathcal{O}_p, \mathfrak{M}_p, |\mathbb{C}_p|)$ is effectively model-complete in the language $\mathcal{L}_F$.*

As a particular case, we have:

Theorem 6.3.6. *The theory of $\mathcal{O}_{p,exp}$ is effectively model-complete.*

6.4 Decidability

We will now prove the decidability of $\mathcal{O}_{p,exp}$ assuming Schanuel's conjecture. By the last theorem, we are reduced to determine the truth of existential $\mathcal{L}_{exp}$-sentences.

Actually, we just need an algorithm that stops if the formula is true. It is quite easy to see that any existential formula is equivalent to a disjunction of formulas of the form:

$$\exists \overline{x} \wedge_i f_i(\overline{x}) = 0 \wedge_j |g_j(\overline{x})|\Box_j|h_j(\overline{x})|,$$

where $f_i, g_j, h_j \in \mathbb{Z}[X_1, \cdots, X_n, E_p(X_1), \cdots, E_p(X_n)]$ and $\Box$ holds for $<, \leq$ or $=$.
Let $\mathbb{Z}_p^{alg}$ denote the valuation ring of $\mathbb{Q}_p^{alg}$.
It turns out that is sufficient to find a realisation of the formula in $\mathbb{Z}_p^{alg}$:

Proposition 6.4.1. *Any existential $\mathcal{L}_{exp}$-sentence with parameters in $\mathbb{Z}_p^{alg}$ realised in $\mathcal{O}_p$ is realised in $\mathbb{Z}_p^{alg}$.*

Remark. Actually, the same result holds for any $\mathcal{L}_F$-formula where F is any set of restricted power series with coefficients in the valuation ring of some finite algebraic extension of $\mathbb{Q}_p$ such that the set of $\mathcal{L}_F$-terms is closed under derivation.

Proof. In this proof, $f_i, g_j, ...$ will be elements of $\mathbb{Z}[X_1, \cdots, X_n, E_p(X_1), \cdots, E_p(X_n)]$, $\overline{m}$ will be a parameter in $\mathbb{Z}_p^{alg}$. We will prove the proposition by induction on the complexity of the formula. We proceed also by induction on n the number of variables and we prove that for all realisations $\overline{x}$ of the formula in $\mathcal{O}_p$, we can find a realisation of the formula in $\mathbb{Z}_p^{alg}$ ε-close from $\overline{x}$ (for all ε small enough).

(1) Let $\Psi \equiv \exists \overline{X} f(\overline{X}, \overline{m}) = 0$.

Assume that there is $\overline{x} \in \mathcal{O}_p$ such that $f(\overline{x}, \overline{m}) = 0$. Assume that $f(x_1, \overline{x'}, \overline{m}) = \sum_i a_i(\overline{x'}, \overline{m})x_1^i$ where $\overline{x'} = (x_2, \cdots, x_n)$.

Let $d(f)$ be the smallest integer like in lemma 4.0.1. Then,

- If $a_i(\overline{x'}, \overline{m}) = 0$ for all i such that $i < d(f)$, we find by induction on the number of variables that there is $\overline{b'} \in (\mathbb{Z}_p^{alg})^{n-1}$ ε-close from $\overline{x'}$ such that $a_i(\overline{b'}, \overline{m}) = 0$ for all $i < d(f)$. In this case, the formula Ψ is realised by any tuple $(b_1, \overline{b'})$. In particular, if $|b_1 - x_1| < \varepsilon$, $(b_1, \overline{b'})$ is ε-close from $\overline{x}$.
- If $a_k(\overline{x'}, \overline{m}) \neq 0$ and $a_i(\overline{x'}, \overline{m}) = 0$ for all $i \neq k$, $i < d(f)$. Then, $\overline{x} = (0, x_2, \cdots, x_n)$ (note that in this case, $\overline{x}$ is the unique solution of the equation $f(X, \overline{x'}, \overline{m}) = 0$). As before, let $\overline{t'}$ be a realisation ε-close from $\overline{x'}$ of the formula

$$\exists \overline{X'} \bigwedge_{\substack{i<d(f)\\ i\neq k}} a_i(\overline{X'}, \overline{m}) = 0.$$

If ε is small enough, $a_k(\overline{t'}, \overline{m}) \neq 0$ and therefore, $(0, t_2, \cdots, t_n) \in \mathbb{Z}_p^{alg}$ is a realisation of Ψ.

- If $a_i(\overline{x'}, \overline{m}) \neq 0$ for at least two $i < d(f)$. Let I be the set of indexes such that $a_i(\overline{x'}, \overline{m}) \neq 0$. Then, there exists ε such that for all $\overline{y'} \in \mathcal{O}_p^{n-1}$ with $|\overline{y'} - \overline{x'}| < \varepsilon$

$$\begin{aligned} |a_i(\overline{x'}, \overline{m})| &= |a_i(\overline{y'}, \overline{m})| && \text{for all } i \in I \\ |a_i(\overline{y'}, \overline{m})| &< \delta && \text{otherwise,} \end{aligned}$$

where

$$\delta = \min_{i \in I}\{|a_i(\overline{x'}, \overline{m})|\}.$$

Let $\overline{t} \in (\mathbb{Z}_p^{alg})^{n-1}$ such that $|\overline{t} - \overline{x'}| < \varepsilon$. Then, as the (restriction until the index $d(f)$ of the) Newton polygons of $f(X, \overline{x'}, \overline{m})$ and $f(X, \overline{t'}, \overline{m})$ are equals, we find that the formula $\exists X f(X, \overline{t'}, \overline{m})$ is realised in $\mathcal{O}_p$ and all its realisations lie in $\mathbb{Z}_p^{alg}$. In particular, there exists a realisation ε-close from x_1.

(2) Let $\Psi \equiv \exists \overline{X} f_1(\overline{X}, Y, \overline{m}) = \cdots = f_k(\overline{X}, Y, \overline{m}) = 0$.

Let $(\overline{\alpha}, \beta)$ be a realisation of the formula in $\mathcal{O}_p$. We define

$$\begin{aligned} F(\overline{X}, Y, Z, \overline{m}) &:= \sum_i f_i(\overline{X}, Y, \overline{m}) Z^{2(i-1)} \\ &= \sum_{(i,j) \in \mathbb{N}^2} a_{ij}(\overline{X}, \overline{m}) Y^i Z^j. \end{aligned}$$

So, for all $z \in \mathcal{O}_p$, $F(\overline{\alpha}, \beta, z, \overline{m}) = 0$.

By inductive hypothesis, there exists $\overline{c}$ in $\mathbb{Z}_p^{alg}$ such that for all $|i| < d(F)$ for all $j < d\left(\frac{\partial^i F}{\partial Y^i}(0, Z)\right)$

$$|a_{ij}(\overline{\alpha}, \overline{m})| = |a_{ij}(\overline{c}, \overline{m})| \text{ and } |\overline{\alpha} - \overline{c}| < \varepsilon.$$

Let $K_0 := \mathbb{Q}_p(\overline{m}, \overline{c}) \subseteq K_1 \subseteq \cdots$ be a sequence of algebraic extensions of $\mathbb{Q}_p$ such that any finite algebraic extension of K_0 of degree n is contained in K_n. Let π_n denote a prime element of K_n. Let us remark that for all $d \in \mathcal{O}_{K_n}$,

$$F(\overline{c}, d, \pi_n, \overline{m}) = 0 \text{ iff } f_i(\overline{c}, d, \overline{m}) = 0 \text{ for all } i.$$

But, for all n large enough, there is $d_n \in \mathcal{O}_p$ such that $F(\overline{c}, d_n, \pi_n, \overline{m}) = 0$. Indeed, the Newton polygons of the functions $F(\overline{\alpha}, Y, \pi_n, \overline{m})$ and $F(\overline{c}, Y, \pi_n, \overline{m})$ are equals (until the coefficients $i \geq d(F)$ but these latter are irrevelant by choice of $d(F)$)

and so the existence of β implies the existence of such a d_n.

By the Weierstrass preparation theorem, for some $|(i,j)| < d(F)$ and after a suitable change of variables, we can factorize

$$F(\overline{c}, T, Z, \overline{m}) = a_I(\overline{c}, \overline{m}) \cdot U(\overline{c}, T, Z, \overline{m}) \cdot \Big[T^s + \sum_{l<s} A_l(\overline{c}, Z, \overline{m}) T^l\Big].$$

So, in fact, $d_s \in K_s$. Therefore,

$$f_1(\overline{c}, d_s) = \cdots = f_k(\overline{c}, d_s) = 0 \text{ and } |(\overline{c}, d_s) - (\overline{\alpha}, \beta)| < \varepsilon$$

which proves our claim for the formula Ψ.

(3) General case: $\Psi \equiv \bigwedge_i f_i(\overline{X}, \overline{m}) = 0 \bigwedge_j |g_j(\overline{X}, \overline{m})| \Box_j |h_j(\overline{X}, \overline{m})|$.

Let $\overline{x}$ be a realisation of the formula in $\mathcal{O}_p$.

If $g_j(\overline{x}, \overline{m}) = 0$ or $h_j(\overline{x}, \overline{m}) = 0$ for some j, we remove the condition $g_j(\overline{x}, \overline{m}) \Box_j h_j(\overline{x}, \overline{m})$ in Ψ and replace it by $g_j(\overline{x}, \overline{m}) = 0 \wedge 0 \Box_j h_j(\overline{x}, \overline{m})$ (or respectively by $h_j(\overline{x}, \overline{m}) = g_j(\overline{x}, \overline{m}) = 0$). So, without loss of generality, we may assume that the formula has the form

$$\Psi \equiv \bigwedge_i f_i(\overline{X}, \overline{m}) = 0 \bigwedge_j 0 < |g_j(\overline{X}, \overline{m})| \Box |h_j(\overline{X}, \overline{m})|.$$

By the case (2), we know that for all ε, there is $\overline{x}_\varepsilon \in \mathbb{Z}_p^{alg}$ ε-close from $\overline{x}$ which realises the formula $\exists \overline{X} \wedge_i f_i(\overline{X}, \overline{m}) = 0$. But, for all ε small enough, $|g_j(\overline{x}_\varepsilon, \overline{m})| = |g_j(\overline{x}, \overline{m})|$ and $|h_k(\overline{x}_\varepsilon, \overline{m})| = |h_k(\overline{x}, \overline{m})|$ for all j, k. It means that, for all ε small enough, $\overline{x}_\varepsilon$ is a realisation of Ψ in $\mathbb{Z}_p^{alg}$ ε-close from $\overline{x}$.

□

We can now prove the main theorem of this section:

Theorem 6.4.2. *Assume that the p-adic Schanuel's conjecture is true. Then, the theory of $\mathcal{O}_{p,exp}$ in the language of exponential ring is decidable.*

Proof. Let Ψ be an existential sentence. Then, by proposition 6.4.1, $\mathcal{O}_p \models \Psi$ iff $\mathbb{Z}_p^{alg} \models \Psi$. So, the formula is true iff it is true in some algebraic extension of $\mathbb{Q}_p$. Let K be a finite algebraic extension of $\mathbb{Q}_p$. If Schanuel's conjecture is true, we have an algorithm that determines the truth of Ψ in $\mathcal{O}_K$. We just have to run an enumeration of all finite algebraic extensions K of $\mathbb{Q}_p$ and return true if Ψ is true in $\mathcal{O}_K$. □

Let us remark that we don't need that Schanuel's conjecture is true in $\mathbb{C}_p$ but only in $\mathbb{Q}_p^{alg}$.

Furthermore, let K_n be the family of extensions defined in chapter 3. If $K_{n,exp}$ denotes the structure with underlying set $\mathcal{O}_{K_n}$ in the language of exponential ring. Then,

Corollary 6.4.3. *If the theory of $K_{n,exp}$ is decidable for all n, then the theory of $\mathcal{O}_{p,exp}$ in the language of exponential ring is decidable.*

In particular, if a version of conjecture 5.3.1 for finite algebraic extensions is true, then the theory of $\mathcal{O}_{p,exp}$ in the language of exponential ring is decidable.

Appendix A

Tropical analytic geometry

Within this chapter K will denote a field complete with respect to val a valuation with $val(K^*) \subseteq \mathbb{R}$. We will denote by $|\cdot| = exp^{-val(\cdot)}$ the absolute value attached to the valuation. Also, we set $\Gamma := val((K^{alg})^*)$.

The goal of this section is to generalise theorem 2.1.11 on Newton polygons to systems of n restricted analytic functions with n variables. These results are due to J. Rabinoff. The reader can find the proofs and further references in [14].

In the first part, we introduce some definitions of convex geometry. Then, in the second section, we define the generalisation of the Newton polygon: the Newton polyhedron and the tropicalization of an analytic function. We state the generalisations of theorem 2.1.11 in sections A.3 and A.4.

Note that our definitions may be slightly different from [14]. Actually, we just use particular cases of the result (i.e. when the functions involved are power series well-defined on a neigbourhoud of the origin) and define the notions according to this these special cases.

A.1 Convex geometry

In this section, we introduce the basic definitions of convex geometry and we define the compactification of a polyhedron. We will need this notion to state theorem A.4.4.

First, we fix some notations for the rest of this section:

$N_{\mathbf{R}}$ will denote the n dimensional real vector space $\mathbb{R}$ and $M_{\mathbf{R}}$ its dual. $\langle \cdot, \cdot \rangle : M_{\mathbf{R}} \times N_{\mathbf{R}} \to \mathbb{R}$ denotes the canonical map. We also fix $N \cong \mathbb{Z}^n$ and $M \cong Hom_{\mathbb{Z}}(N, \mathbb{Z})$. We denote by N_Γ the tensor $N \otimes_{\mathbb{Z}} \Gamma$.

Definition A.1.1. *An* (affine) half-space *in $N_{\mathbf{R}}$ is a subset of the form*

$$H = \{v \in N_{\mathbf{R}} \mid \ \langle u, v\rangle \le a\},$$

for some $u \in M_{\mathbf{R}} \setminus \{0\}, a \in \mathbb{R}$. The space is called linear *if we can take $a = 0$. We say that H is Γ-affine if $a \in N_\Gamma$ and $u \in M$.*

An affine space *in $N_{\mathbf{R}}$ is the translated of a linear subspace. Any such a space can be obtained as a finite intersection between the (topological) boundaries of some half-spaces.*

A polyhedron *in $N_{\mathbf{R}}$ is a non-empty intersection of finitely many half-spaces. We say that a polyhedron is* Γ-affine *if all the half-spaces of the intersection can be assumed Γ-affine.*

Let P be a polyhedron and $u \in M_{\mathbf{R}}$. We define

$$face_u(P) = \{v \in P \mid \ \langle u, v\rangle \ge \langle u, v'\rangle \text{ for all } v' \in P\}.$$

A face *of P is a non-empty set of the form $F = face_u(P)$. We write $F \prec P$.*

We define the dimension of P as

$$\begin{aligned} Span(P) \ &= \text{ the smallest affine subspace containing } P, \\ dim(P) \ &= dim\ Span(P). \end{aligned}$$

Let $S \subset N_{\mathbf{R}}$. We define the convex closure *of S by*

$$conv(S) = \bigcap H,$$

where the intersection is taken over all half-spaces H such that $H \supseteq S$.

The compactification of a polyhedron is essentially the polyhedron itself together with points to infinity. We start with the definition of the compactification of $N_{\mathbf{R}}$ with respect to a special case of polyhedron: the cones.

Definition A.1.2. *A* cone *in $N_{\mathbf{R}}$ is a (non-empty) finite intersection of linear half-spaces in $N_{\mathbf{R}}$.*

We say that a cone is pointed *if $\{0\}$ is a face of the cone.*

Lemma A.1.3. *Let $v_1, \cdots, v_r \in N_{\mathbf{R}}$. Then, $\sigma = \sum v_i \mathbb{R}_{\ge 0}$ is a cone. Furthermore, any cone in $N_{\mathbf{R}}$ can be written in this form.*

Let $\sigma = \sum v_i \mathbb{R}_{\geq 0}$ be a cone. The *dual cone* is the cone

$$\sigma^\vee = \bigcap_i \{u \in M_{\mathbf{R}} \mid \ \langle u, v_i \rangle \leq 0\}.$$

Let us remark that $\sigma^{\vee\vee} = \sigma$.
The *annihilator* of a cone σ is the annihilator of the vector space $Span(\sigma)$:

$$\sigma^\perp = \{u \in M_{\mathbf{R}} \mid \ \langle u, v \rangle = 0 \text{ for all } v \in \sigma\}.$$

Let $\overline{\mathbb{R}}$ be the additive monoid $\mathbb{R} \cup \{-\infty\}$ equipped with the topology generated by the usual topology on $\mathbb{R}$ and intervals of the type $[-\infty, a)$ for $a \in \mathbb{R}$.

Definition A.1.4. *Let σ be a cone. The* partial compactification of $N_{\mathbf{R}}$ with respect to σ *is the space $N_{\mathbf{R}}(\sigma) = Hom_{\mathbb{R}_{\geq 0}}(\sigma^\vee, \overline{\mathbb{R}})$ of monoid homomorphisms respecting multiplication by elements in $\mathbb{R}_{\geq 0}$, equipped with the topology of pointwise convergence. We use the notation $\langle \cdot, \cdot \rangle_\sigma$ to denote the canonical map $\sigma^\vee \times N_{\mathbf{R}}(\sigma) \to \overline{\mathbb{R}}$.*

Roughly, it means that we add points to infinity in the direction of σ. This is made precise by

Proposition A.1.5. *[Proposition 3.4 in [14]] Let $\sigma \subset N_{\mathbf{R}}$ be a cone.*

(i) Let $\tau \prec \sigma$ and let $v \in N_{\mathbf{R}}/Span(\tau)$. We define $\iota(v)$ by:

$$\langle u, \iota(v) \rangle_\sigma := \begin{cases} \langle u, v \rangle & \text{if } u \in \tau^\perp \cap \sigma^\vee \\ -\infty & \text{otherwise,} \end{cases}$$

for $u \in \sigma^\vee$. Then, $\iota(v)$ is a well-defined element of $N_{\mathbf{R}}(\sigma)$ and

$$\iota : \coprod_{\tau \prec \sigma} N_{\mathbf{R}}/\tau \to N_{\mathbf{R}}(\sigma)$$

is a bijection. Furthermore, for all $\tau \prec \sigma$, the map ι restricted to $N_{\mathbf{R}}/\tau$ is a topological embedding.

(ii) If $\sigma^\vee = \sum_{i \leq r} u_i \mathbb{R}_{\geq 0}$, then the map

$$v \longmapsto (\langle u_1, v \rangle_\sigma, \cdots, \langle u_r, v \rangle_\sigma) : N_{\mathbf{R}}(\sigma) \hookrightarrow \overline{\mathbb{R}}^r$$

is a topological embedding with closed image.

(iii) For $\tau \prec \sigma$, the inclusion $\sigma^\vee \prec \tau^\perp$ induces a topological embedding $N_{\mathbf{R}}(\tau) \hookrightarrow N_{\mathbf{R}}(\sigma)$ with open image.

Example A.1.1. Let $\sigma = \mathbb{R}_{\geq 0}(0,1) + \mathbb{R}_{\geq 0}(1,0)$. Then, σ is a cone in $N_{\mathbf{R}}$. The faces of σ are: $\tau_1 = \mathbb{R}_{\geq 0}(0,1)$, $\tau_2 = \mathbb{R}_{\geq 0}(1,0)$, $\{(0,0)\}$ and σ. The partial compactification of $N_{\mathbf{R}}$ with respect to σ is (isomorphic to):

$$\begin{aligned} N_{\mathbf{R}}(\sigma) &= N_{\mathbf{R}} \coprod N_{\mathbf{R}}/Span(\tau_1) \coprod N_{\mathbf{R}}/Span(\tau_2) \coprod N_{\mathbf{R}}/Span(\sigma) \\ &= \mathbb{R}^2 \coprod \Big(\{+\infty\} \times \mathbb{R}\Big) \coprod \Big(\mathbb{R} \times \{+\infty\}\Big) \coprod \{(+\infty, +\infty)\}. \end{aligned}$$

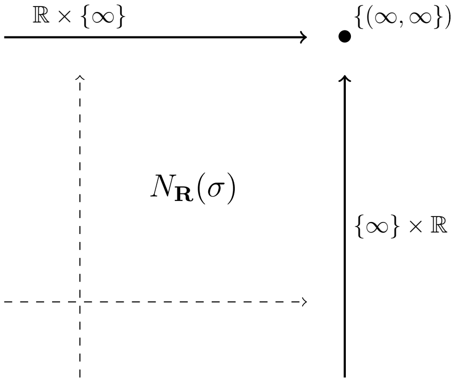

$\mathbb{R} \times \{\infty\}$
$\{(\infty,\infty\})$
$N_{\mathbf{R}}(\sigma)$
$\{\infty\} \times \mathbb{R}$

Figure A.1: The partial compactification of $\mathbb{R}^2$ with respect to σ.

Definition A.1.6. *Let $P \subset N_{\mathbf{R}}$ be a polyhedron. The* cone of unbounded direction of *P is the cone $\mathcal{U}(P)$ dual of*

$$\mathcal{U}(P)^\vee := \{u \in M_{\mathbf{R}} \mid \ face_u(P) \neq \varnothing\}.$$

We say that P is pointed *if σ is pointed.*

Definition A.1.7. *Let $P \subset N_{\mathbf{R}}$ be a polyhedron and $\sigma = \mathcal{U}(P)$. The* compactification *$\overline{P}$* of *P is the closure of P in $N_{\mathbf{R}}(\sigma)$.*

Proposition A.1.8 (Proposition 3.19 in [14])**.** *Let $P = \bigcap_{i=1}^r \{v \in N_{\mathbf{R}} \mid \ \langle u_i, v\rangle \leq a_i\}$ be a pointed polyhedron, $\sigma = \mathcal{U}(P)$ and $\overline{P}$ be the closure of P in $N_{\mathbf{R}}(\sigma)$. Then, $\overline{P} = \coprod_{\tau \prec \sigma} \pi_\tau(P)$, where we identify $N_{\mathbf{R}}(\sigma) \cong \coprod_{\tau \prec \sigma} N_{\mathbf{R}}/Span(\tau)$ and $\pi_\tau : N_{\mathbf{R}} \to N_{\mathbf{R}}/Span(\tau)$ is the canonical projection.*

Furthermore, for all $\tau \prec \sigma$,

$$\begin{aligned} \pi_\tau(P) &= \{v \in N_{\mathbf{R}}/Span(\tau) \mid \ \langle u, v\rangle_\sigma \leq \max_{v' \in P} \langle u, v'\rangle \text{ for all } u \in \sigma^\vee\} \\ &= \{v \in N_{\mathbf{R}}/Span(\tau) \mid \langle u_i, v\rangle \leq a_i \text{ for all } u_i \in \tau^\perp\}. \end{aligned}$$

and,

$$\overline{P} = \{u : \sigma^\vee \to \overline{\mathbb{R}} \mid \ \langle u, v\rangle_\sigma \leq \max_{v' \in P} \langle u, v'\rangle \textit{ for all } u \in \sigma^\vee\}.$$

Example A.1.2. Let $P = \{(x, y) \in \mathbb{R}^2 \mid \ x \geq 1, \ y, \geq 1, x + y \geq 2\}$. Then, $\mathcal{U}(P)$ is the cone σ of example A.1.1. The compactification of P is the closure of P in $N_{\mathbf{R}}(\sigma)$. With the notations of the above proposition, $\overline{P} = \coprod_{\tau \prec \sigma} \pi_\tau(P)$. As we have seen, the faces of σ are $\tau_1 = \mathbb{R}_{\geq 0}(0, 1)$, $\tau_2 = \mathbb{R}_{\geq 0}(1, 0)$, $\{(0, 0)\}$ and σ. So,

$$\begin{aligned}
\pi_{\tau_1}(P) \ &= \{(x, y) \in N_{\mathbf{R}}/Span(\tau_1) \mid \ x \geq 1, \ y \geq 1, x + y \geq 2\} \\
&= \{+\infty\} \times [1, +\infty) \\
\pi_{\tau_2}(P) \ &= [1, +\infty) \times \{+\infty\} \\
\pi_{\{(0,0)\}}(P) \ &= P \\
\pi_\sigma(P) \ &= \{(+\infty, +\infty)\}
\end{aligned}$$

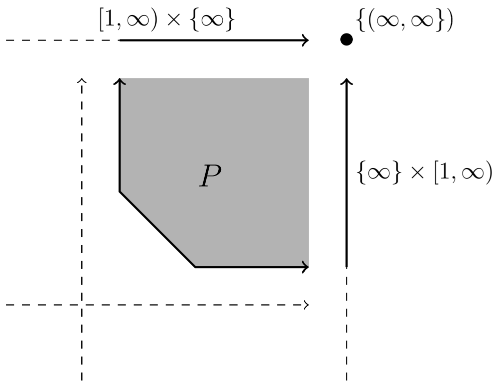

$[1, \infty) \times \{\infty\}$
$\{(\infty, \infty\})$
P
$\{\infty\} \times [1, \infty)$

Figure A.2: The compactification of P.

A.2 Tropicalization and Newton polyhedron

For the rest of this section P will denote a polyhedron in $\mathbb{R}^n$ of the form $\prod_{1 \leq i \leq n}[r_i, \infty)$, $r_i \in \Gamma$. We will denote by $\overline{P} = \prod_i [r_i, \infty]$ its compactification. We define

$$K\langle P\rangle = \left\{ \sum_{u \in \mathbb{N}^n} a_u x^u \mid \ a_u \in K \text{ and } val(a_u) + \langle u, v\rangle \to \infty \ \forall v \in P \right\},$$

where the convergence is taken on the complement of the finite subsets of $\mathbb{N}^n$. Let us note that elements $f \in K\langle P\rangle$ correspond to functions which are analytic on the ball of radius $\exp(-r_i)$ in K^n. For instance, if $P = \prod[0, \infty)$, $K\langle P\rangle = K\{x_1 \cdots, x_n\}$.

Let $\overline{x} \in K^n$. The tropicalization of $\overline{x}$, denoted by $trop(\overline{x})$, is the tuple formed by the valuations of the x_i's:

$$trop(\overline{x}) = (val(x_1), \cdots, val(x_n)).$$

Let $f \in K\langle P\rangle$. We define the tropicalization of f as the closure of the set

$$\{v \in \overline{P} \mid \text{ there exists } \overline{x} \in (K^{alg})^n \text{ such that } f(\overline{x}) = 0 \text{ and } trop(\overline{x}) = v\},$$

where the closure is taken in $\overline{P}$. We will denote this set by $Trop(f)$.

This set is actually completely determined by the coefficients of f:

Let $\sigma = \mathcal{U}(P)$, $\tau \prec \sigma$ and $f = \sum a_u \overline{x}^u \in K\langle P\rangle$. The *height graph of f with respect to τ* is

$$H(f,\tau) = \{(u, val(a_u)) \mid -u \in \sigma^\vee \cap \tau^\perp \cap M, a_u \neq 0\} \subset (\sigma^\vee \cap \tau^\perp \cap M) \times \mathbb{R}.$$

Fix $v \in N_{\mathbf{R}}/Span(\tau)$. Let

$$vert_v(f) = \{(u, val(a_u)) \in H(f,\tau) \mid val(a_u) + \langle u, v\rangle \leq val(a_{u'}) + \langle u', v\rangle \text{ for all monomials } a_{u'}\overline{x}^{u'} \text{ of } f\}.$$

This is the set of points such that the linear functional $(v, 1)$ reaches its minimun. As $f \in K\langle P\rangle$, $val(a_u) + \langle u, v\rangle \to \infty$. So, $vert_v(f)$ is actually a finite set. Furthermore,

Lemma A.2.1 (lemma 8.2 in [14]). *Let $f \in K\langle P\rangle$ nonzero. Then,*

(i) $vert_P(f) = \bigcup_{v\in P} vert_v(P)$ is finite.

(ii) There exists $\varepsilon > 0$ such that for all $f' = \sum a'_u \overline{x}^u \in K\langle P\rangle$ with

$$|f - f'| = \sup_{u\in\mathbb{N}^n, v\in P} \{|a_u - a'_u| \cdot exp(\langle u, v\rangle)\} < \varepsilon$$

and $a'_u = 0$ for all u such that $a_u = 0$, we have $vert_v(f) = vert_v(f')$ for all $v \in P$.

We define the *initial form of f with respect to v* to be

$$in_v(f) = \sum_{(u, val(a_u)) \in vert_v(f)} a_u \overline{x}^u \in K[x].$$

Let us remark that

$$vert_v(f) = \{(u, val(a_u)) \mid a_u \overline{x}^u \text{ is a monomial of } in_v(f)\}.$$

Example A.2.1. Let $f = p^2 + p^2X + X^2 + X^3 + \sum_{n\geq 1} p^n X^{n+3} \in K\langle[0,\infty)\rangle$. Then,

$$\begin{aligned}
&vert_0(f) = \{(2,0),(3,0)\}\\
&vert_v(f) = \{(2,0)\} \text{ for all } v \in (0,1)\\
&vert_1(f) = \{(0,2),(2,0)\}\\
&vert_v(f) = \{(2,0)\} \text{ for all } v \in (1,\infty)
\end{aligned}$$

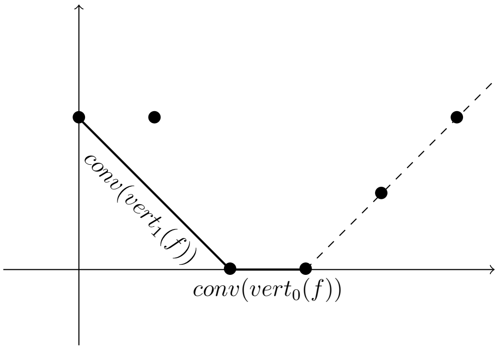


Figure A.3: $vert_P(f)$

Let us remark that $\bigcup_{v\in P} conv(vert_v(f))$ is exactly the Newton polygon of f (in the sense of section 2.1.2) restricted to its segments with negative slope. This part of the Newton polygon describes the multiplicity of the roots of f with valuation in P.

Let $f \in K\langle P\rangle$. Fix $\bar{t} \in (K^{alg})^n$ such that $f(\bar{t}) = 0$. By the ultrametric inequality, we have that for some $u, u' \in \mathbb{N}^n$ distinct, $val(a_u\bar{t}^u) = val(a_{u'}\bar{t}^{u'}) = \min_w\{val(a_w\bar{t}^w)\}$. So, if $v = val(\bar{t}) \in Trop(f)$, $inv_v(f)$ is not a monomial. A crucial result in [14] is that the converse is true:

Lemma A.2.2 (lemma 8.4 in [14])**.** *Let $f \in K\langle P\rangle$ nonzero. Then,*

$$Trop(f) = \{v \in \overline{P} \mid\ inv_v(f) \textit{ is not a monomial}\}.$$

$Trop(f) \cap N_{\mathbf{R}}$ is actually a very simple subset of $N_{\mathbf{R}}$: a polyhedral complex.

Definition A.2.3. *A* polyhedral complex *is a finite collection Π of polyhedra in $N_{\mathbf{R}}$ (called* faces *or* cells *of Π) such that*

- *if $P, P' \in \Pi$, $P \cap P' \neq \varnothing$, then $P \cap P'$ is a face of P and a face of P';*
- *for all $P \in \Pi, F \prec P$, $F \in \Pi$.*

The support *of* Π*, denoted* $|\Pi|$ *is the set* $\bigcup_{P\in\Pi} P$*. The dimension of* Π *is the dimension of the highest dimensional cell of* Π*.*

For $v \in Trop(f) \cap N_{\mathbf{R}}$, we define

$$\gamma_v = \{v' \in Trop(f) \cap N_{\mathbf{R}} \mid \; vert_{v'}(f) \supseteq vert_v(f)\}.$$

Actually, if $Trop(f)$ is non-empty, the collection $\{\gamma_v, v \in Trop(f)\cap N_{\mathbf{R}}\}$ is a polyhedral complex in $N_{\mathbf{R}}$ of codimension at least 1 (i.e. all maximal cells have dimension at most $n-1$). The support of this complex is exactly $Trop(f) \cap N_{\mathbf{R}}$. We will denote by $Trop(f) \cap N_{\mathbf{R}}$ the complex as well as its support.
Let $\pi : \mathbb{N} \times \mathbb{R} \longrightarrow \mathbb{N}$ denote the projection on the first factor. We define

$$\check{\gamma_v} = \pi(conv(vert_v(f))).$$

This a bounded polyhedron. The *Newton complex of* f is the collection of polyhedra $\{\check{\gamma_v} \mid \; v \in P\}$. We denote by $New(f)$ this set. Note that in general this set is not a polyhedral complex: some face of a polyhedron in $New(f)$ may not belong to $New(f)$. Indeed, a face of a polyhedron $\check{\gamma_v}$ may correspond to the projection of a set $conv(vert_v(f))$ where $v \notin P$. Let us remark that it is a polyhedral complex in the case where f is polynomial and we consider the set of all $\check{\gamma_v}$ for $v \in N_{\mathbf{R}}$. The support of $New(f)$ is $|New(f)| = conv\{u \in \mathbb{N} \mid (u, val(a_u)) \in vert_v(f)$ for some $v \in Trop(f) \cap N_{\mathbf{R}}\}$.
The complexes $New(f)$ and $Trop(f) \cap N_{\mathbf{R}}$ are dual to each other in the following sense:

Proposition A.2.4. *1. For all* $v, v' \in Trop(f) \cap N_{\mathbf{R}}$*,* $\gamma_v \prec \gamma_{v'}$ *iff* $\check{\gamma_v} \succ \check{\gamma_{v'}}$*.*

2. For all $v \in Trop(f) \cap N_{\mathbf{R}}$*,* γ_v *and* $\check{\gamma_v}$ *are orthogonal in the sense that the linear subspace of* $N_{\mathbf{R}}$ *associated to the affine span of* γ_v *is orthogonal to the linear subspace of* $M_{\mathbf{R}}$ *associated to the affine span of* $\check{\gamma_v}$*. Furthermore,* $dim(\gamma_v) + dim(\check{\gamma_v}) = dim(N_{\mathbf{R}})$*.*

The above proposition implies that we have one-to-one correspondence between cells of $Trop(f) \cap N_{\mathbf{R}}$ and positive dimensional polyhedra in $New(f)$.

Example A.2.2. (a) Let $f = p^2 + p^2X + X^2 + X^3 + \sum_{n\geq 1} p^n X^{n+3} \in K\langle[0,\infty)\rangle$ as in example A.2.1.

Then,

$$\begin{aligned}
\gamma_0 &= \{0\} \\
\gamma_v &= [0,1] \text{ for all } v \in (0,1) \\
\gamma_1 &= \{1\} \\
\gamma_v &= [1,\infty) \text{ for all } v \in (1,\infty)
\end{aligned}$$

and

$$\begin{aligned}
\check{\gamma}_0 &= [2,3] \\
\check{\gamma}_v &= \{2\} \text{ for all } v \in (0,1) \\
\check{\gamma}_1 &= [0,2] \\
\check{\gamma}_v &= \{0\} \text{ for all } v \in (1,\infty).
\end{aligned}$$

By theorem 2.1.11, we already know that f has exactly one zero of valuation 0 and two zeros of valuation 1 in $\mathbb{Q}_p^{alg}$. Let us remark that this coincides with the volumes of $\check{\gamma}_0$ and $\check{\gamma}_1$. The main theorem of the section A.3 is a generalisation of this observation.

(b) Let $f(x,y) = px + x^p + y^p$. We have four possibilities for $in_v(f)$:

(1) $in_v(f) = px + x^p$ when

$$v \in \{\nu = (\nu_1,\nu_2) \mid 1 + \nu_1 = p\nu_1 < p\nu_2\} = \left(\frac{1}{p-1}, \frac{1}{p-1}\right) + (0,1)\mathbb{R}^{>0} =: \gamma_1.$$

(2) $in_v(f) = px + y^p$ when

$$v \in \{\nu = (\nu_1,\nu_2) \mid 1+\nu_1 = p\nu_2 < p\nu_1\} = \left(\frac{1}{p-1}, \frac{1}{p-1}\right) + \left(1, \frac{1}{p}\right)\mathbb{R}^{>0} =: \gamma_2.$$

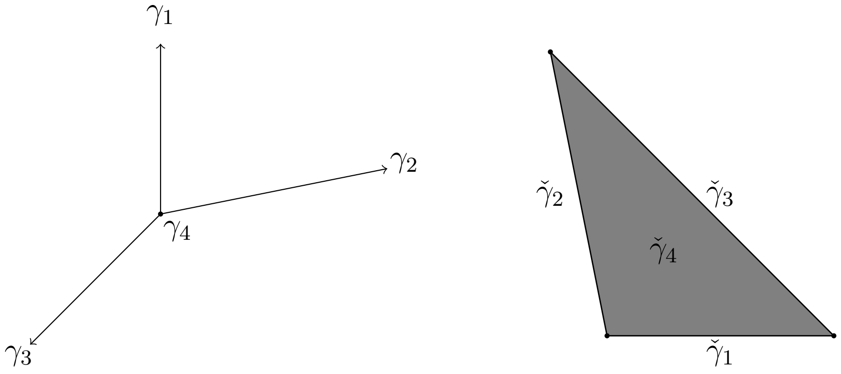
(3) $in_v(f) = x^p + y^p$ when

$$v \in \{v = (\nu_1,\nu_2) \mid p\nu_1 = p\nu_2 < 1+\nu_1\} = \left(\frac{1}{p-1}, \frac{1}{p-1}\right) + (-1,-1)\mathbb{R}^{>0} =: \gamma_3.$$

(4) $in_v(f) = px + x^p + y^p$ when

$$v \in \{\nu = (\nu_1,\nu_2) \mid 1 + \nu_1 = p\nu_1 = p\nu_2\} = \left(\frac{1}{p-1}, \frac{1}{p-1}\right) =: \gamma_4.$$

Let $v \in \gamma_1$. The corresponding cell in the Newton complex is $\check{\gamma}_1 = \pi(conv(vert_v(f))) = conv\{(1,0),(p,0)\}$.



(a) $Trop(f) \cap N_{\mathbf{R}}$ (b) $New(f)$

Where in the above figure, we take $P = (-\infty, +\infty)^2$ (with the obvious extensions of the definitions). If $P = [r, \infty) \times [s, \infty)$, then $Trop(f) \cap N_{\mathbf{R}}$ is the intersection between the set described in the above figure and P. $New(f)$ is the collection of all $\check{\gamma}_i$ such that $\gamma_i \cap P$ has the same dimension that γ_i.

A.3 Multiplicity formula

Definition A.3.1. *Let $P_1, \cdots, P_n$ be bounded polyhedra in $N_{\mathbf{R}}$. The* Minkowsky sum *of $P_1, \cdots, P_n$ is*

$$P_1 + \cdots + P_n = \{v_1 + \cdots + v_n \mid \ v_i \in P_i\}.$$

For $\lambda \in \mathbb{R}_{\geq 0}$, we set $\lambda P_i = \{\lambda v \mid \ v \in P_i\}$. We define the function

$$\begin{array}{rcl} V_{P_1 \cdots P_n} : \mathbb{R}^n_{\geq 0} & \longrightarrow & \mathbb{R} \\ (\lambda_1, \cdots, \lambda_n) & \longmapsto & vol(\lambda_1 P_1 + \cdots + \lambda_n P_n) \end{array}$$

where vol is an Euclidean volume form in $N_{\mathbf{R}}$ normalized such that the volume of a fundamental domain for the lattice N is one. The function $V_{P_1 \cdots P_n}$ is actually a homogeneous polynomial in $\lambda_1 \cdots \lambda_n$ of degree n. The mixed volume *$MV(P_1 \cdots P_n)$ is defined to be the coefficient of the $\lambda_1 \cdots \lambda_n$-term of $V_{P_1 \cdots P_n}$.*

Example A.3.1.

- If $P = [a, b] \subset \mathbb{R}$, then $MV(P) = b - a$.

- If $P = [0,1]^2$, $Q = [1,2]^2 \subset \mathbb{R}^2$, $\lambda_1 P + \lambda_2 Q = [\lambda_2, \lambda_1 + 2\lambda_2]$.

  So,

  $$vol(\lambda_1 P + \lambda_2 Q) = (\lambda_1 + \lambda_2)^2 = \lambda_1^2 + 2\lambda_1\lambda_2 + \lambda_2^2,$$

  and $MV(P,Q) = 2$.

- Let $P = [0,1]^2$, $Q = [0,1] \times \{0\}$ and $R = \{0\} \times [0,1]$ in $\mathbb{R}^2$. Then,

  $\lambda_1 P + \lambda_2 Q = [0, \lambda_1 + \lambda_2] \times [0, \lambda_1]$ and $vol(\lambda_1 P + \lambda_2 Q) = (\lambda_1 + \lambda_2)\lambda_1 = \lambda_1^2 + \lambda_1\lambda_2$.

  So, $MV(P,Q) = 1$. And,

  $$\lambda_1 Q + \lambda_2 R = [0, \lambda_1] \times [0, \lambda_2] \text{ and } vol(\lambda_1 Q + \lambda_2 R) = \lambda_1\lambda_2.$$

  So, $MV(Q,R) = 1$.

Definition A.3.2. *Let $P = \prod [r_i, \infty)$ be a polyhedron (where $r_i \in val(K^*)$). Let $f_1, \cdots, f_n \in K\langle P \rangle$. We define*

$$V(f_i) = \{\overline{x} \in (K^{alg})^n \mid f_i(\overline{x}) = 0 \text{ and } trop(\overline{x}) \in \overline{P}\}.$$

Let $Y = \bigcap_i V(f_i)$. Fix $v \in N_\Gamma \cap P$. The intersection multiplicity of $f_1, \cdots, f_n$ over v *is the dimension of the space $Y \cap trop^{-1}(\{v\})$:*

$$i_K(v, f_1 \cdots, f_n) = dim_K \Gamma(Y \cap trop^{-1}(\{v\}), \mathcal{O}_{Y \cap trop^{-1}(\{v\})}).$$

Note that $i_K(v, f_1, \cdots, f_n)$ is finite if $Y \cap trop^{-1}(\{v\})$ is a finite set, in which case

$$i_K(v, f_1 \cdots, f_n) = \sum_{trop(\xi)=v} dim_K \mathcal{O}_{Y,\xi}.$$

We refer to [14] for a formal definition of the dimensions of the space $Y \cap trop^{-1}(\{v\})$ and $dim_K \mathcal{O}_{Y,\xi}$. Note that the dimension $dim_K \mathcal{O}_{Y,\xi}$ is a generalisation of the intersection multiplicity of an algebraic variety at a point ξ. For our purpose, the intuitive meaning of 'intersection multiplicity' is sufficient. In our applications, we just need to know that the above dimension bounds the cardinality of the space defined by Y (whenever this space is finite).

It turns out that the intersection multiplicity of a system over an isolated point in $\bigcap Trop(f_i)$ is equal to the mixed volume of cells in $New(f_i)$:

Theorem A.3.3. *[Theorem 11.7 in [14]] Let P be a polyhedron as before, let $f_1, \cdots, f_n \in K\langle P\rangle$ and let $v \in \bigcap_i Trop(f_i)$ be an isolated point such that v is in the interior of P or $v \in P$ and $i_K(v, f_1, \cdots, f_n)$ is finite. Let $\check{\gamma}_i = \pi(conv(vert_v(f_i))) \in New(f_i)$ be the polyhedron corresponding to $v \in Trop(f_i)$. Then,*

$$i_K(v, f_1, \cdots, f_n) = MV(\check{\gamma}_1, \cdots, \check{\gamma}_n).$$

In particular, assume that the system $(f_1, \cdots, f_n)$ has finitely many solutions in K^{alg}. Let N be the number of solutions with valuation v (where v is an isolated point of $\bigcap Trop(f_i)$). Then, $N \leq MV(\check{\gamma}_1, \cdots, \check{\gamma}_n)$.

Example A.3.2.

- Let $f(X) = \sum a_i X^i$.

  Let $v \in Trop(f) \cap \mathbb{R}$. Let i be the minimal index such that $(i, v(a_i)) \in vert_v(f)$ and j be the maximal index such that $(j, v(a_j)) \in vert_v(f)$.

  Then, $\check{\gamma}_v = \pi(conv(vert_v(f))) = [i, j]$. So, by the above theorem, the number of zeros of f with valuation v is $MV(\check{\gamma}_v) = j - i$ (counting multiplicities).

  On the other hand, as $(i, v(a_i)), (j, v(a_j)) \in vert_v(f)$,

  $$v(a_i) + v \cdot i = v(a_j) + v \cdot j.$$

  So, the slope of the segment $conv(vert_v(f)) = conv((i, v(a_i)), (j, v(a_j)))$ is

  $$\frac{v(a_j) - v(a_i)}{j - i} = -v.$$

  It shows that theorem A.3.3 is a generalisation of theorem 2.1.11.

- We consider the sytem

  $$\begin{cases} f_1(X,Y) & = X^2 - 2X - Y^2 + 1 \\ f_2(X,Y) & = X^2 - p^2Y^2. \end{cases}$$

  Then,

  $$\begin{aligned} Trop(f_1) &= \mathbb{R}_{\geq 0}(0,1) \cup \mathbb{R}_{\geq 0}(1,0) \cup \mathbb{R}_{\geq 0}(-1,-1) \\ Trop(f_2) &= (1,0) + (1,1)\mathbb{R}. \end{aligned}$$

  So, $Trop(f_1) \cap Trop(f_2) = \{(1,0)\}$. Let $v = (1,0)$. Then,

  $$vert_v(f_1) = \Big\{ \Big((0,0), 0\Big), \Big((0,2), 0\Big) \Big\}$$

  $$P_1 := \check{\gamma}_v(f_1) = conv\Big\{(0,0), (0,2)\Big\}.$$

And,

$$vert_v(f_2) = \Big\{\Big((2,0),0\Big), \Big((0,2),2\Big)\Big\}$$
$$P_2 := \check{\gamma}_v(f_2) = conv\Big\{(2,0),(0,2)\Big\}.$$

Therefore,

$$\lambda_1 P_1 + \lambda_2 P_2 = conv\Big\{(2\lambda_2, 0), (2\lambda_1 + 2\lambda_2, 0), (0, 2\lambda_2), (2\lambda_2, 2\lambda_2)\Big\},$$

$$vol(\lambda_1 P_1 + \lambda_2 P_2) = 2\lambda_2 \cdot (2\lambda_1 + 2\lambda_2 - 2\lambda_2) = 4\lambda_1\lambda_2$$

$$MV(P_1, P_2) = 4.$$

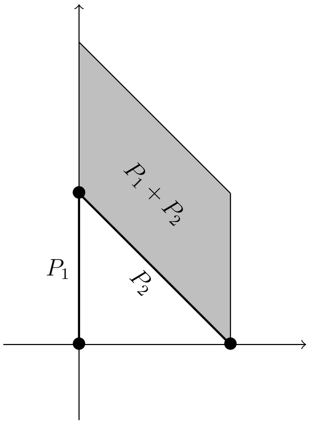


Figure A.4: $P_1 + P_2$

So, by the theorem, the number of solutions of the system $(f_1(x,y), f_2(x,y)) = (0,0)$ is 4 (counting multiplicities). And indeed, one can compute that the solutions of this system are

$$S = \left\{\left(\frac{p}{p-1}, \frac{1}{p-1}\right), \left(\frac{p}{p+1}, \frac{1}{p+1}\right), \left(\frac{p}{p-1}, \frac{-1}{p-1}\right), \left(\frac{p}{p+1}, \frac{-1}{p+1}\right)\right\}.$$

A.4 Non-proper intersection multiplicity

In the last theorem, we have seen that we can compute $\sum_{trop(\xi)=v} dim \mathcal{O}_{Y,\xi}$ using the Newton complex of the functions f_i whenever v is an isolated point of $\bigcap Trop(f_i)$. In this section, we will see how to compute a more general case (i.e. where the sum is taken over $trop(\xi) \in C$ for more general $C \subset \bigcap Trop(f_i)$). The idea is that we can apply a small perturbation to the system so that, after perturbation, the set C

corresponds to a finite set of points $\widetilde{C}$. Then, we apply theorem A.3.3 to compute the intersection multiplicity at each point of $\widetilde{C}$. It turns out that the sum of these intersection multiplicities over $\widetilde{C}$ is in relation with the sum of the multiplicities of the roots of the original system with valuation in C. However, this gives us an equality only with $\sum_{trop(\xi)\in\overline{C}} dim\mathcal{O}_{Y,\xi}$, where $\overline{C}$ is the compactification of C.

Definition A.4.1. *Let $P = \bigcap_i \{v \in N_{\mathbf{R}} \mid \langle u_i, v\rangle \leq a_i\}$ be a polyhedron in $N_{\mathbf{R}}$. A* thickening *of P is a polyhedron of the form*

$$P' = \bigcap_i \{v \in N_{\mathbf{R}} \mid \langle u_i, v\rangle \leq a_i + \varepsilon\}.$$

More generally, if Π is a polyhedral complex, a thickening *$\mathcal{P}$ of Π is a collection of polyhedra of the form $\mathcal{P} = \{P' \mid P \in \Pi\}$, where P' is a thickening of P. We set*

$$|\mathcal{P}| = \bigcup P' \qquad \textit{and} \qquad int(\mathcal{P}) = \bigcup int(P'),$$

where $int(P')$ denotes the interior of P'.

For the rest of this section, we fix $P_1, \cdots, P_n$ Γ-affine polyhedra of the type $\prod_j [r_{ij}, \infty)$ and $f_1, \cdots, f_n \in K\langle P\rangle$ nonzero. Let C be a connected component of $\bigcap Trop(f_i)$. Then, the intersection between a thickening of C and a suitable small perturbation of the $Trop(f_i)$'s is finite:

Lemma A.4.2. *Let C be a connected component of $\bigcap Trop(f_i)$ and let $\mathcal{P}$ be a thickening of C such that $|\mathcal{P}| \cap \bigcap_i Trop(f_i) = C$. Then, there exist $v_1, \cdots, v_n \in N$ and $\varepsilon \in \mathbb{R}_{\geq 0} \cap \Gamma$ such that for all $t \in (0, \varepsilon]$, the intersection*

$$|\mathcal{P}| \cap \bigcap_i \Big(Trop(f_i) + tv_i\Big)$$

is a finite set of points contained in $int(\mathcal{P})$.

Let $P = \prod_i [r_i, \infty)$ be a polyhedron in $N_{\mathbf{R}}$. We fix $t \in \Gamma$ and ξ in some algebraic extension of K such that $v(\xi) = t$.
We denote by $\widetilde{f}$ the image of the map:

$$\begin{array}{ccc} K\langle P\rangle & \longrightarrow & K\langle \widetilde{P}\rangle \\ f(x_1, \cdots, x_n) & \longmapsto & f(x_1\xi^{-1}, \cdots, x_n\xi^{-1}) \end{array}$$

where $\widetilde{P} := \prod [r_i \cdot p^t, \infty)$. Then, $Trop(\widetilde{f}) = Trop(f) + t$. Let us remark that $Trop(\widetilde{f})$ and $New(\widetilde{f})$ are independent of the choice of ξ with $v(\xi) = t$ (indeed, these sets are determined by the valuations of the coefficients of $\widetilde{f}$). It means that after a change of variables like above, the intersection between the tropicalization and a thickening of C is finite. It leads to the definition of the stable tropical intersection multiplicity along C:

Definition A.4.3. *Let $f_1, \cdots, f_n \in K\langle P\rangle$ be nonzero and let $v \in \bigcap Trop(f_i)$ an isolated point. The* stable tropical intersection multiplicity of $Trop(f_1), \cdots, Trop(f_n)$ at v *is defined to be*

$$i(v, Trop(f_1), \cdots, Trop(f_n)) = MV(\check{\gamma}_1, \cdots, \check{\gamma}_n)$$

where $\check{\gamma}_i = \pi(conv(vert_v(f_i))) \in New(f_i)$. Let $C \subset \bigcap Trop(f_i)$ be a connected component and let $\mathcal{P}, v_1, \cdots v_n, \varepsilon$ like in lemma A.4.2. The stable tropical intersection multiplicity of $Trop(f_1), \cdots, Trop(f_n)$ along C *is defined to be*

$$i(C, Trop(f_1), \cdots, Trop(f_n)) = \sum i(v, Trop(f_1) + \varepsilon v_1, \cdots, Trop(f_n) + \varepsilon v_n),$$

where the (finite) sum is taken over all v in $|\mathcal{P}| \cap \bigcap_i \Big(Trop(f_i) + \varepsilon v_i \Big)$.

The main result of this section is that (under extra assumptions) the stable tropical intersection multiplicity is equal to the sum of the multiplicities of the points of $\bigcap V(f_i)$ with valuation in $\overline{C}$ (when this sum is finite). This implies that the above definition is well-defined in that case and independent of all choices.
It follows from theorem 12.11 in [14] that:

Theorem A.4.4. *Let $f_1, \cdots, f_n \in K\langle P\rangle$. Let $S(f_i) = conv\{u : f_{iu} \neq 0\}$ (where f_{iu} denotes the coefficients of f_i). Assume that $dim(\cap_i S(f_i)) = n$. Let $C \subset \bigcap Trop(f_i)$ be a Γ-affine polyhedron and $\overline{C}$ its compactification. Let $Y := \bigcap V(f_i)$. Assume that the number of $\xi \in Y$ with valuation in $\overline{C}$ is finite. Then,*

$$i(C, Trop(f_1), \cdots, Trop(f_n)) = \sum_{trop(\xi) \in \overline{C}} dim_K \mathcal{O}_{Y,\xi}.$$

In particular, assume that the system $f = (f_1, \cdots, f_n)$ has finitely many solutions in K^{alg} and satisfies the hypothesis of the theorem. The typical example of C we have in mind is $C = \gamma_v$ (when this set is non-empty). Then, by the above theorem, the number of solutions of f with valuation v is bounded by $i(\gamma_v, Trop(f_1), \cdots, Trop(f_n))$.

Example A.4.1. Let $p \neq 2$. And, let

$$\begin{cases} f_1(X,Y) & = 2X - Y - 1 \\ f_2(X,Y) & = X + Y - 2. \end{cases}$$

Let $P = [0,\infty)^2$. We compute the number of solution of the system $f_1(X,Y) = f_2(X,Y) = 0$ using the above theorem:
First, let us remark that

$$\mathbb{R}^2 \cap Trop(f_1) = \mathbb{R}^2 \cap Trop(f_2) = (0,1)\mathbb{R}_{\geq 0} \coprod (1,0)\mathbb{R}_{\geq 0} \coprod (-1,-1)\mathbb{R}_{\geq 0}.$$

Let $C = P \cap Trop(f_1)$. Let $t_1, t_2 \in \mathcal{O}_p$. We apply the following perturbation to our system:

$$\begin{cases} \widetilde{f_1}(X,Y) & = 2t_1X - t_2Y - 1 \\ \widetilde{f_2}(X,Y) & = X + Y - 2. \end{cases}$$

Then, $\mathbb{R}^2 \cap Trop(\widetilde{f_2}) = \mathbb{R}^2 \cap Trop(f_2)$ and

$$\begin{aligned} \mathbb{R}^2 \cap Trop(\widetilde{f_1}) =& (-v_1,-v_2) + (0,1)\mathbb{R}_{\geq 0} \coprod (-v_1,-v_2) + (0,1)\mathbb{R}_{\geq 0} \\ & \coprod (-v_1,-v_2) + (-v_2,-v_1)\mathbb{R}_{\geq 0} \end{aligned}$$

where $v_i := v_p(t_i)$. Assume $v_1 > v_2 > 0$.
Then, $\mathbb{R}^2 \cap Trop(\widetilde{f_2}) \cap Trop(\widetilde{f_1}) = \{(-v_2,-v_2); (-v_1 - v_2, -v_1 - v_2)\}$. So, by the theorem, independently of any choice,

$$\begin{aligned} i(C, Trop(f_1), \cdots, Trop(f_n)) = & \ i((-v_2,-v_2), Trop(\widetilde{f_1}), Trop(\widetilde{f_2})) \\ & + i((-v_1 - v_2, -v_1 - v_2), Trop(\widetilde{f_1}), Trop(\widetilde{f_2})). \end{aligned}$$

Now, we compute the two mixed volumes:

1. Let $\nu_1 = (-v_2,-v_2)$. Then, $vert_{\nu_1}(Trop(\widetilde{f_1})) = \Big\{\Big((0,1),0\Big), \Big((0,0),0\Big)\Big\}$ and $vert_{\nu_1}(Trop(\widetilde{f_2})) = \Big\{\Big((0,1),0\Big), \Big((1,0),0\Big)\Big\}$. So,
$$MV(\check{\gamma}_{\nu_1}(\widetilde{f_1})), \check{\gamma}_{\nu_1}(\widetilde{f_2})) = 1.$$

2. Let $\nu_2 = (-v_1-v_2, -v_1-v_2)$. Then, $vert_{\nu_2}(Trop(\widetilde{f_1})) = \Big\{\Big((0,1),0\Big), \Big((1,0),0\Big)\Big\}$ and $vert_{\nu_1}(Trop(\widetilde{f_2})) = \Big\{\Big((0,1),0\Big), \Big((1,0),0\Big)\Big\}$. So,
$$MV(\check{\gamma}_{\nu_1}(\widetilde{f_1})), \check{\gamma}_{\nu_1}(\widetilde{f_2})) = 0.$$

This show that $i(C, Trop(f_1), \cdots, Trop(f_n)) = 1$. And indeed, the unique solution of the system is $(1,1)$.

Bibliography

[1] J. Ax and S. Kochen. Diophantine problems over Local Fields II. A complete set of axioms for p-adic number theory. *American journal of Mathematics, Vol 87, No. 3*, pages 631–648, 1965.

[2] N. Bourbaki. *Variétés différentielles et analytiques: fascicule de résultats.* Springer Berlin Heidelberg: Berlin, Heidelberg, 2007.

[3] J. Denef. The rationality of the Poincaré series associated to the p-adic points on a variety. *Inventiones Mathematicae, Vol. 77, No.1*, pages 1–24, 1984.

[4] 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.

[5] D. Haskell and D. Macpherson. A version of o-minimality for the p-adics. *The Journal of Symbolic Logic, Vol. 62, No. 4*, pages 1075–1092, 1997.

[6] D. Haskell, D. Macpherson, and L. van den Dries. One-dimensional p-adic subanalytic sets. *J. London Math. Soc., Vol. 59, No. 1*, pages 1–20, 1999.

[7] L. Lipshitz. Rigid subanalytic sets. *American Journal of Mathematics, Vol. 115, No. 1*, pages 77–108, 1993.

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

[9] A. Macintyre. On definable subsets of p-adic Fields. *The Journal of Symbolic Logic, Vol 41, No. 3*, pages 605–610, 1976.

[10] A. Macintyre. Decision problems for exponential rings: the p-adic case. *Lecture Notes in Comput. Sci., Vol. 158*, pages 285–289, 1983.

[11] A. Macintyre and A. Wilkie. On the decidability of the real exponential field. *Kreiseliana, 441–467, A K Peters, Wellesley*, pages 441–467, 1996.

[12] K. Malher. Ein beweis der transzendenz der p-adischen exponentialfunktion. *J. Reine Angew. Math., Issue 169*, pages 61–66, 1933.

[13] A. Prestel and P. Roquette. *Formally p-adic Fields.* Springer-Verlag, 1984.

[14] J. Rabinoff. Tropical analytic geometry, Newton polygons, and tropical intersections. *Advances in Mathematics, Vol. 229, no. 6*, pages 3192–3255, 2012.

[15] L. van den Dries. Exponential rings, exponential polynomials and exponential functions. *Pacific Journal of Mathematics, Vol. 113*, pages 51–66, 1984.

[16] L. van den Dries. On the elementary theory of restricted elementary functions. *The Journal of Symbolic Logic, Vol. 53, no.3*, pages 796–808, 1988.

[17] A. Wilkie. Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. *J. Amer. Math. Soc. 9, No. 4*, pages 1051–1094, 1996.