Model Theory, Algebra, and Geometry
MSRI Publications
Volume **39**, 2000

Classical Model Theory of Fields

LOU VAN DEN DRIES

Abstract. We begin with some thoughts on how model theory relates to other parts of mathematics, and on the indirect role of Gödel's incompleteness theorem in this connection. With this in mind we consider in Section 2 the fields of real and p-adic numbers and show how these algebraic objects are understood model-theoretically: theorems of Tarski, Kochen, and Macintyre. This leads naturally to a discussion of the famous work by Ax, Kochen and Ershov in the mid sixties on henselian fields and its number-theoretic implications.

In Section 3 we add analytic structure to the real and p-adic fields, and indicate how results such as the Weierstrass preparation theorem can be used to extend much of Section 2 to this setting. Here we make contact with the theory of subanalytic sets developed by analytic geometers in the real case.

In Section 4 we focus on o-minimal expansions of the real field that are not subanalytic, such as the real exponential field (Wilkie's theorem). We indicate in a diagram the main known o-minimal expansions of the real field. We also provide a translation into the coordinate-free language of manifolds via "analytic-geometric categories". (This has been found useful by geometers.)

Contents

1. Introduction

In model theory we associate to a structure $\mathcal{M}$ invariants of a logical nature like $\mathrm{Th}(\mathcal{M})$, the set of first-order sentences which are true in $\mathcal{M}$. Other invariants of this kind are the category of definable sets and maps over $\mathcal{M}$ or over $\mathcal{M}^{\mathrm{eq}}$ and the category of definable groups and definable homomorphisms over $\mathcal{M}$ or over $\mathcal{M}^{\mathrm{eq}}$. If we are lucky we can find a well-behaved notion of dimension for the objects in these categories, which make these objects behave more or less like algebraic varieties and algebraic groups.

We consider a little more closely the simplest of the above invariants, namely $\mathrm{Th}(\mathcal{M})$. To use it for gaining a better understanding of $\mathcal{M}$, it is desirable that $\mathrm{Th}(\mathcal{M})$ can be *effectively* described. In practice we want $\mathrm{Th}(\mathcal{M})$ to be axiomatizable by *finitely* many axiom *schemes*.

Example. $\mathrm{Th}(\mathbb{C}, +, \cdot, 0, 1)$ is axiomatized by:

- field axioms (finite in number)
- $\forall x_1 \ldots \forall x_n \, \exists y \, (y^n + x_1 y^{n-1} + \cdots + x_n = 0)$, for $n = 1, 2, 3, \ldots$
- $\underbrace{1 + \cdots + 1}_{n \text{ times}} \neq 0$, for $n = 1, 2, 3, \ldots$

Example (Gödel). $\mathrm{Th}(\mathbb{Z}, +, \cdot)$ cannot be effectively described in any reasonable way, so in contrast to the field of complex numbers, the ring of integers is "wild". (But $\mathbb{Z}$ as ordered additive group is tame again!)

We use here "tame" and "wild" very *informally*, to suggest the distinction between good and bad model-theoretic behaviour.

The requirement of effective axiomatizability of $\mathrm{Th}(\mathcal{M})$ has been known since Gödel to be a serious constraint on $\mathcal{M}$. It implies some highly intrinsic model-theoretic properties in the *tame* direction, such as non-interpretability of the ring of integers. Though these properties are far weaker than stability, simplicity, o-minimality, etcetera, this axiomatizability demand can serve as a useful guide in initial model-theoretic explorations of certain mathematical structures.

Ironically, Gödel's work is often characterized as saying that only for "uninteresting" $\mathcal{M}$ can $\mathrm{Th}(\mathcal{M})$ be effectively axiomatizable. This attitude overlooks the fact that even in ostensibly *nontame* subjects like number theory, the solution of problems frequently involves ingenious moves into tame territory! Thus the relevance of the slogan (proposed by Hrushovski):

model theory = geography of tame mathematics

Example. The field $\mathbb{Q}$ of rational numbers is not tame, but its completions $\mathbb{R}$, $\mathbb{Q}_2$, $\mathbb{Q}_3$, $\mathbb{Q}_5$, … are all tame (J. Robinson, Tarski, Ax, Kochen, Ershov). It is not known if the field $\mathbb{F}_p((t))$ is tame.

2. Elimination Theory and Henselian Fields

How does one prove that a given structure $\mathcal{M}$ is *tame*? First, choose a set T of axioms such that $\mathcal{M} \models T$, and then try to show that

1. T admits QE (quantifier elimination), or
2. T is model complete, or

$\vdots$

If this works, one typically obtains a complete description of $\mathrm{Th}(\mathcal{M})$, and in the bargain a lot of positive information about (the category of) definable sets and maps as well, for example a notion of dimension for definable sets. It should be mentioned that, especially for QE, the right choice of primitives (language) is important.

This general scheme is perhaps best illustrated by the field of real numbers.

2.1. The field of real numbers. For $\mathcal{M} := (\mathbb{R}, <, 0, 1, +, -, \cdot)$ we choose $T :=$ RCF (the axioms for Real Closed ordered Fields):

- axioms for ordered fields
- $\forall x\, \exists y\, (x > 0 \to x = y^2)$
- $\forall x_1 \ldots \forall x_{2n+1}\, \exists y\, (y^{2n+1} + x_1 y^{2n} + \cdots + x_{2n+1} = 0)$, for $n = 1, 2, 3, \ldots$

How do we show that T admits QE? There are several model-theoretic criteria that can be helpful. (We usually associate the names of A. Robinson, J. Shoenfield and L. Blum with these tests.) Here is one that we shall apply to $T =$ RCF.

Proposition (QE-test). *An $\mathcal{L}$-theory T admits QE*

$$\Longleftrightarrow$$

for any models $\mathcal{M}$ and $\mathcal{N}$ of T, each $\mathcal{L}$-embedding $\mathcal{A} \longrightarrow \mathcal{N}$ where $\mathcal{A} \subseteq \mathcal{M}$ and $\mathcal{A} \neq \mathcal{M}$ can be extended to an $\mathcal{L}$-embedding $\mathcal{A}' \longrightarrow \mathcal{N}'$ from some strictly larger *$\mathcal{L}$-substructure $\mathcal{A}'$ of $\mathcal{M}$ into some* elementary *extension $\mathcal{N}'$ of $\mathcal{N}$.*

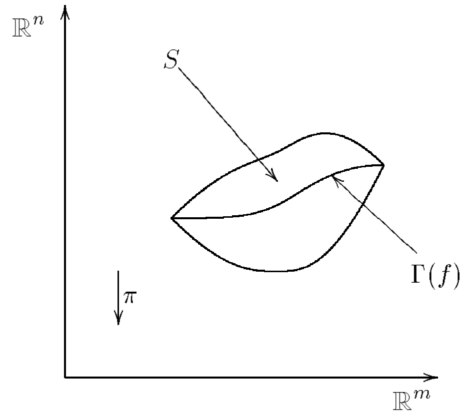
To apply this test to RCF we only need to know the following about ordered domains [Artin and Schreier 1926]:

1. Each ordered domain A has a real closure A^{rc}, that is, A^{rc} is a real closed ordered field extending A and algebraic over the fraction field of A.
2. Each embedding $A \longrightarrow L$ of an ordered domain A into a real closed ordered field L extends to an embedding $A^{\mathrm{rc}} \longrightarrow L$.
3. If A is a real closed field and $A(b)$, $A(c)$ are two ordered field extensions with $b, c \notin A$ such that b and c determine the same cut in A, then there is an A-isomorphism of ordered fields from $A(b)$ onto $A(c)$ sending b to c.

These facts easily imply that RCF admits QE: Let K and L be real closed ordered fields, $A \subseteq K$ an ordered subring and $i : A \longrightarrow L$ an embedding (of ordered rings). Assuming $A \neq K$, we want to show that i can be extended as required in the QE-test. By fact 2. above we can reduce to the case that A itself is a real closed ordered field. Take any $b \in K \setminus A$. Then b determines a cut in A: $U < b < V$, where $U := \{x \in A : x < b\}$ and $V := \{x \in A : b < x\}$. Thus $i(U) < i(V)$ in L. Replacing L by a suitable elementary extension we can take an element $c \in L$ such that $i(U) < c < i(V)$. Then by fact 3 above we can extend i to an ordered field embedding from $A(b)$ into L. $\square$

That RCF admits QE was first proved by Tarski [1951] by other means. Some routine but noteworthy consequences are:

1. $\mathrm{Th}(\mathbb{R}, <, 0, 1, +, -, \cdot) = \{$logical consequences of RCF$\}$, and thus the theory $\mathrm{Th}(\mathbb{R}, <, 0, 1, +, -, \cdot)$ is decidable.
2. The field $\mathbb{Q}^{\mathrm{rc}}$ of real *algebraic* numbers is an elementary substructure of the field of real numbers.
3. Definable = Semialgebraic (for any real closed field).
4. If $S \subseteq \mathbb{R}^{m+n}$ is semialgebraic, there is a semialgebraic map $f : \pi S \longrightarrow \mathbb{R}^n$ such that $\Gamma(f) \subseteq S$:



This last result can be read off directly from the axioms of RCF, since the existentially quantified variables in these axioms can be witnessed *definably*, by choosing for each positive element its *positive* square root, and for each odd degree polynomial its *least* zero. This trick can also be used to show that each definable function is piecewise built up from the field operations and the Skolem functions we just indicated. This way of arguing is generally available for other structures whose elementary theory we manage to axiomatize.

2.2. The field of p-adic numbers. Let p be a prime number, and equip $\mathbb{Q}$ with the (nonarchimedean) absolute value defined by

$$|a|_p := p^{-e} \quad \text{for } a = p^e \tfrac{b}{c} \text{ with } e, b, c \in \mathbb{Z},\ p \nmid bc.$$

The completion of $(\mathbb{Q}, |\ \ |_p)$ is called the field of p-adic numbers and is denoted by $(\mathbb{Q}_p, |\ \ |_p)$. Its elements can be represented uniquely as absolutely convergent series $\sum_{k\in\mathbb{Z}} a_k p^k$ with all $a_k \in \{0, 1, \dots, p-1\}$, and $a_k = 0$ for all $k < k_0$ for some $k_0 \in \mathbb{Z}$. The ring $\mathbb{Z}_p$ of p-adic *integers* is given by

$$\mathbb{Z}_p := \text{closure of } \mathbb{Z} \text{ in } \mathbb{Q}_p = \{x \in \mathbb{Q}_p : |x|_p \le 1\}.$$

It is a compact subring of the locally compact field $\mathbb{Q}_p$.

The pair $(\mathbb{Q}_p, \mathbb{Z}_p)$ is an example of a valued field: A *valued field* is a pair (K, V) with K a field and V a *valuation ring* of K (a subring of K such that $x \in K^\times \Longrightarrow x \in V$ or $x^{-1} \in V$). We remark that a valuation ring V has only one maximal ideal $\mathfrak{m}(V) = V \setminus U$, where U is the multiplicative group of units of V.

To a valued field (K, V) we associate:

- its residue field $k := V/\mathfrak{m}(V)$, and
- its value group $\Gamma := K^\times/U$, viewed as an ordered abelian group with

$$aU \le bU \iff \frac{b}{a} \in V.$$

(By convention the group operation of Γ is written additively.)

Definition. A valuation ring V is said to be **henselian** if each polynomial $X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in V[X]$ with $a_{n-1} \notin \mathfrak{m}(V)$ and $a_n \in \mathfrak{m}(V)$ has a (necessarily unique) zero in $\mathfrak{m}(V)$.

Example. $\mathbb{Z}_p$ is henselian; $k[\![t]\!]$ is henselian for any field k.

Definition. A **p-adically closed field** is a valued field (K, V) such that $\operatorname{char}(K) = 0$, V is henselian with $\mathfrak{m}(V) = pV$, $k \simeq \mathbb{F}_p$, and $[\Gamma : n\Gamma] = n$ for $n = 1, 2, 3, \dots$.

So $(\mathbb{Q}_p, \mathbb{Z}_p)$ is a p-adically closed field. Note that the definition of *p-adically closed field* basically describes a set of axioms in the language of valued fields whose models are exactly the p-adically closed fields.

Theorem [Ax and Kochen 1965; 1966; Kochen 1969]. *The theory of p-adically closed fields is complete and model complete.*

Kochen used this to characterize the p-adic rational functions in any number of variables that take only values in $\mathbb{Z}_p$ for arguments in $\mathbb{Q}_p$. A one-variable example, which in some sense generates them all, is

$$\frac{1}{p(X^p - X) - p(X^p - X)^{-1}}$$

(this is "the p-adic version of Hilbert's seventeen problem").

For elimination of quantifiers we need to add the right (definable) predicates, just as in the case of the real field where we have to single out the set of squares:

THEOREM [Macintyre 1976]. *The theory of p-adically closed fields admits QE when we extend the language of valued fields with unary relation symbols P_n (for $n = 2, 3, 4, \dots$) and add their "defining axioms":*

$$\forall x\ (P_n(x) \leftrightarrow \exists y\ (x = y^n)).$$

For a nice treatment of the theorems of Kochen and Macintyre, as well as their generalizations, see [Prestel and Roquette 1984]. Macintyre's theorem has the same kind of consequences for $\mathbb{Q}_p$ as Tarski's theorem for $\mathbb{R}$: it leads to a theory of semialgebraic sets over $\mathbb{Q}_p$ (with dimension theory for such sets, curve selection, ...); see also [Macintyre 1986] for more on this.

Denef discovered new ways to exploit this, namely for the study of various kinds of Poincaré series and local zeta functions associated to p-adic (semi-) algebraic sets. We refer to Denef's paper in this volume for more details.

We did not follow here the chronological order: the above p-adic developments came after the material to be discussed next.

2.3. Henselian valued fields of equicharacteristic 0. Consider a *henselian* valued field (K, V) of equicharacteristic 0, i.e., $\mathrm{char}(k) = 0$ (hence $\mathrm{char}(K) = 0$). Then Ax and Kochen [1965; 1966] and Ershov [1965] proved:

THEOREM. *$\mathrm{Th}(K, V)$ is determined by $\mathrm{Th}(k)$ and $\mathrm{Th}(\Gamma)$, where k is the residue field and Γ is the ordered value group.*

This extends in some sense work by Mac Lane and Kaplansky [Kaplansky 1942], who showed that under mild assumptions on Γ we can embed (K, V) into the generalized formal power series field $k((t^\Gamma))$ consisting of all formal power series $\sum_{\gamma\in\Gamma} a_\gamma t^\gamma$ with coefficients $a_\gamma \in k$, and with well ordered support

$$\{\gamma \in \Gamma : a_\gamma \neq 0\}.$$

(The valuation ring of $k((t^\Gamma))$ consists of the series with support in $\Gamma^{\geq 0}$.)

By suitably adapting Kaplansky's embedding technique, Ax and Kochen, and independently Ershov, showed that if (K_1, V_1) and (K_2, V_2) are sufficiently saturated henselian valued fields of equicharacteristic 0 with $\mathrm{Th}(k_1) = \mathrm{Th}(k_2)$ and $\mathrm{Th}(\Gamma_1) = \mathrm{Th}(\Gamma_2)$, then (K_1, V_1) and (K_2, V_2) are "back-and-forth" equivalent, and thus $\mathrm{Th}(K_1, V_1) = \mathrm{Th}(K_2, V_2)$.

The following is a routine consequence of the preceding theorem, although it is not mentioned explicitly in [Ax and Kochen 1965; 1966] or [Ershov 1965].

COROLLARY. Given an elementary statement σ about valued fields, there are elementary statements $\sigma_1, \dots, \sigma_k$ about fields and elementary statements $\tau_1, \dots, \tau_k$ about ordered groups such that for *all* henselian valued fields (K, V) of equicharacteristic 0 we have

$$(K, V) \models \sigma \iff \text{there exists } i \in \{1, \dots, k\} \text{ such that } k \models \sigma_i \text{ and } \Gamma \models \tau_i.$$

The valued field $(\mathbb{Q}_p, \mathbb{Z}_p)$ is of mixed characteristic, and the valued field

$$\big(\mathbb{F}_p((t)), \mathbb{F}_p[\![t]\!]\big)$$

is of equicharacteristic p. While neither of these valued fields is of equicharacteristic 0, the *uniformity* in the equivalence above implies a surprising connection between them:

Corollary. Let σ be an elementary statement about valued fields. Then

$$(\mathbb{Q}_p, \mathbb{Z}_p) \models \sigma \iff \big(\mathbb{F}_p((t)), \mathbb{F}_p[\![t]\!]\big) \models \sigma$$

for all but finitely many primes p.

Proof. Take σ_i and τ_i $(i = 1, \dots, k)$ as in the previous corollary. Then by Gödel's completeness theorem there must be a formal proof of

$$\sigma \longleftrightarrow (\sigma_1 \wedge \tau_1) \vee \cdots \vee (\sigma_k \wedge \tau_k)$$

from the axioms for henselian valued fields of equicharacteristic 0. But in such a proof we use only finitely many of the axioms saying that the residue field has characteristic 0. Thus this equivalence also holds in $(\mathbb{Q}_p, \mathbb{Z}_p)$ and in $\big(\mathbb{F}_p((t)), \mathbb{F}_p[\![t]\!]\big)$, for all but finitely many p. Now use the fact that $(\mathbb{Q}_p, \mathbb{Z}_p)$ and $\big(\mathbb{F}_p((t)), \mathbb{F}_p[\![t]\!]\big)$ have the same residue field $\mathbb{F}_p$ and the same value group $\mathbb{Z}$. □

Application. S. Lang showed in the early 1950s that each homogeneous polynomial of degree $d \geq 1$ in more than d^2 variables over $\mathbb{F}_p((t))$ has a non-trivial zero in that field. Hence by the last corollary, *given any* $d \geq 1$, this statement remains true when we replace $\mathbb{F}_p((t))$ by $\mathbb{Q}_p$, for all but finitely many p. This establishes an asymptotic form of a conjecture by E. Artin. Exceptions indeed occur [Terjanian 1966], and the finite set of exceptional primes depends on d.

What about QE for henselian valued fields? There are several results, by P. J. Cohen, V. Weispfenning, F. Delon, J. Denef, J. Pas, and others, that take the following general form:

Henselian valued fields of equicharacteristic 0 *have* (*uniformly*) *relative QE*: *field quantifiers can be eliminated at the cost of introducing quantifiers over the residue field*, *and over the value group*.

The exact language used here can make a difference for the applications. The next example is due to Pas, and is useful in motivic integration; see Denef's paper in this volume.

Example. For the valued field $\mathbb{C}((t))$ we have (full) QE in the language with three sorts of variables: variables ranging over the field itself, variables ranging over the residue field $\mathbb{C}$, and variables ranging over the value group $\mathbb{Z}$ (viewed as ordered abelian group with unary predicates for the sets $n\mathbb{Z}$, with $n = 2, 3, \dots$). Moreover, these sorts are related in the usual way, except that instead of the residue class map $\mathbb{C}[\![t]\!] \longrightarrow \mathbb{C}$ we consider the *leading coefficient map* $\mathbb{C}(\!(t)\!) \longrightarrow \mathbb{C}$ associating to each series its leading coefficient.

3. Expanding by Restricted Analytic Functions

Here things are easier in the p-adics than in the reals! Write $|a| := |a|_p$ for $a \in \mathbb{Q}_p$. Let $X = (X_1, \ldots, X_m)$ and put

$$\mathbb{Z}_p\langle X\rangle := \Big\{ f = \sum_{\alpha \in \mathbb{N}^m} c_\alpha X^\alpha \in \mathbb{Z}_p[\![X]\!] : |c_\alpha| \to 0 \text{ as } |\alpha| \to \infty \Big\},$$

where $|\alpha| := \alpha_1 + \cdots + \alpha_m$. Each $f \in \mathbb{Z}_p\langle X\rangle$ defines a function

$$x \mapsto f(x) = \sum_{\alpha \in \mathbb{N}^m} c_\alpha x^\alpha : \mathbb{Z}_p^m \longrightarrow \mathbb{Z}_p.$$

We extend the p-adic absolute value on $\mathbb{Z}_p$ to a norm on the ring $\mathbb{Z}_p\langle X\rangle$ by putting $|f| := \max_{\alpha \in \mathbb{N}^m} |c_\alpha|$.

We construe $\mathbb{Z}_p$ as an $\mathcal{L}_{\mathrm{an}}^D$-structure where the language $\mathcal{L}_{\mathrm{an}}^D$ has the following symbols:

- $0, 1, +, -, \cdot$ (ring operation symbols)
- P_n, for $n = 2, 3, 4, \ldots$ (to denote the set of n-th powers in $\mathbb{Z}_p$)
- an m-ary function symbol f for each $f \in \mathbb{Z}_p\langle X\rangle$
- a binary function symbol D to be interpreted as restricted division:

$$D(x, y) = \begin{cases} \dfrac{x}{y} & \text{if } |x| \le |y| \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Removal of D gives the language $\mathcal{L}_{an}$. The next result is in [Denef and van den Dries 1988], where it is applied to prove rationality of Poincaré series of p-adic analytic varieties.

THEOREM. *The $\mathcal{L}_{\mathrm{an}}^D$-structure $\mathbb{Z}_p$ admits QE.*

This amounts to a theory of p-adic subanalytic sets. (A subset of $\mathbb{Z}_p^m$ is *subanalytic* if it is the projection of a subset of $\mathbb{Z}_p^{m+n}$ defined by a quantifier free formula in $\mathcal{L}_{an}$. By the theorem this is the same as a subset of $\mathbb{Z}_p^m$ defined by a quantifier free formula in $\mathcal{L}_{an}^D$.)

IDEA OF PROOF. Consider for example a formula $\exists y\ f(x, y) = 0$, where $f \in \mathbb{Z}_p\langle X, Y\rangle$, $X = (X_1, \ldots, X_m)$, $Y = (Y_1, \ldots, Y_n)$ with $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_n)$ ranging over $\mathbb{Z}_p^m$ (the parameter space) and $\mathbb{Z}_p^n$ respectively. We have to find the (quantifier free) conditions on the parameter x for solvability in y of the equation $f(x, y) = 0$. The case $n = 0$ being trivial, assume $n > 0$. Below we use the lexicographic ordering of $\mathbb{N}^n$.

STEP 1: Write $f(X,Y) = \sum_{i\in\mathbb{N}^n} a_i Y^i$ with $a_i = a_i(X) \in \mathbb{Z}_p\langle X\rangle$. Using the noetherianity of $\mathbb{Z}_p\langle X\rangle$, we can take $d \in \mathbb{N}$ such that each a_i is of the form

$$a_i = \sum_{|j|<d} c_{ij} a_j$$

with $c_{ij} \in \mathbb{Z}_p\langle X\rangle$, such that for each j with $|j| < d$ we have $|c_{ij}| \to 0$ as $|i| \to \infty$.

STEP 2: Partition the x-space $\mathbb{Z}_p^m$ into the subsets Z and S_j for $|j| < d$, each quantifier free definable in the language $\mathcal{L}_{\mathrm{an}}$, such that

- if $x \in Z$, then $f(x,Y) = 0$ (so $f(x,y) = 0$ for all $y \in \mathbb{Z}_p^n$);
- if $x \in S_j$, then $f(x,Y) \neq 0$, $|a_j(x)| = \max_{i\in\mathbb{N}^n} |a_i(x)|$, and j is lexicographically maximal with this property.

(Note that Z is just the set defined by the formula $\bigwedge_{|j|<d} a_j(x) = 0$.)

STEP 3: Fix $j \in \mathbb{N}^n$ with $|j| < d$, and let x range over S_j. Put

$$v_{ij}(x) := \begin{cases} \dfrac{a_i(x)}{a_j(x)} & \text{if } i < j,\ |i| < d, \\[2ex] \dfrac{a_i(x)}{pa_j(x)} & \text{if } i > j,\ |i| < d. \end{cases}$$

Then $v_{ij}(x) \in \mathbb{Z}_p$. Put $v_j(x) := (v_{ij}(x))_{|i|<d, i\neq j}$. We now carry out a standard change of variables, by substituting

$$T_d(Y) := (Y_1 + Y_n^{d^{n-1}}, \ldots, Y_{n-1} + Y_n^d, Y_n)$$

for Y. We also factor out the "last" dominating coefficient $a_j(x)$. The combined result is an identity (for $x \in S_j$):

$$f(x, T_d(Y)) = a_j(x) F_j(x, v_j(x), Y)$$

where $F_j(X, V_j, Y) \in \mathbb{Z}_p\langle X, V_j, Y\rangle$, $V_j = (V_{ij})_{|i|<d, i\neq j}$, and

$$F_j \bmod p \in \mathbb{F}_p[X, V_j, Y]$$

is monic in Y_n of degree $j_1 d^{n-1} + \cdots + j_n$.

STEP 4: By p-adic Weierstrass Preparation we have

$$F_j = U \cdot (Y_n^e + c_1 Y_n^{e-1} + \cdots + c_e),$$

where U is a unit of $\mathbb{Z}_p\langle X, V_j, Y\rangle$, $c_1, \ldots, c_e \in \mathbb{Z}_p\langle X, V_j, Y'\rangle$, $Y' = (Y_1, \ldots, Y_{n-1})$, and $e = j_1 d^{n-1} + \cdots + j_n$. Thus for $x \in S_j$ and $y \in \mathbb{Z}_p^n$ we have

$$f(x, T_d(y)) = a_j(x) U(x, v_j(x), y) g(x, y', y_n),$$

where $y' := (y_1, \ldots, y_{n-1})$ and

$$g(x, y', y_n) := y_n^e + c_1(x, v_j(x), y') y_n^{e-1} + \cdots + c_e(x, v_j(x), y').$$

STEP 5: Note the equivalences

$$\begin{aligned} x \in S_j \ \wedge \ \exists y\, f(x,y) = 0 &\iff x \in S_j \ \wedge \ \exists y\, f(x, T_d(y)) = 0 \\ &\iff x \in S_j \ \wedge \ \exists y\, g(x,y) = 0 \\ &\iff x \in S_j \ \wedge \ \exists y'\, \phi(x, v_j(x), y'), \end{aligned}$$

where ϕ is quantifier free in $\mathcal{L}_{\mathrm{an}}$. For the last equivalence we used that y_n occurs only polynomially in g, so that Macintyre's theorem can be applied. We eliminated $\exists y_n$ at the cost of introducing fractions $v_{ij}(x)$, but these fractions only involve x and not any of the y-variables.

While we were dealing here with a rather special kind of formula, the above reduction of $\exists y$ to $\exists y'$ does contain the main ideas for a general quantifier elimination. □

REMARKS. 1. The appeal to noetherianity of $\mathbb{Z}_p\langle X\rangle$ may seem to make this proof non-constructive. But this appeal is made only for convenience. At the cost of complicating the exposition we could replace it by finitely many applications of p-adic Weierstrass division. This should not be too surprising, since one way to prove the noetherianity of $\mathbb{Z}_p\langle X\rangle$ goes via the p-adic Weierstrass division theorem.

2. One can indicate a few simple schemes of universal axioms in $\mathcal{L}^D_{\mathrm{an}}$ and true in $\mathbb{Z}_p$, that together with the axioms for p-adically closed valuation rings formally imply the QE above. It follows that the definable functions are piecewise superpositions of semialgebraic functions, functions given by the power series in $\mathbb{Z}_p\langle X\rangle$, and D.

Does this method also work for $\mathbb{R}$? Yes, *except* that in Weierstrass preparing a convergent power series over $\mathbb{R}$ (or $\mathbb{C}$) the domain of convergence may decrease drastically. Thus we have to work more locally, and exploit the compactness of $[-1,1]^m$ (whereas we didn't need the compactness of $\mathbb{Z}_p^m$ in the arguments above).

Details: The language $\mathcal{L}^D_{\mathrm{an}}$ (real version) has the following symbols:

- $0, 1, +, -, \cdot, <$
- for each power series $f \in \mathbb{R}[\![X_1, \ldots, X_m]\!]$ converging in a neighborhood of $[-1,1]^m$ a corresponding function symbol, also denoted f, to be interpreted as the "restricted analytic" function on $\mathbb{R}^m$ given by

$$x \mapsto \begin{cases} f(x) & \text{if } x \in [-1,1]^m, \\ 0 & \text{otherwise;} \end{cases}$$

- a binary function symbol D for restricted division:

$$D(x,y) = \begin{cases} \dfrac{x}{y} & \text{if } |x| \le |y| \le 1,\ y \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

The proof in [Denef and van den Dries 1988] that $\mathbb{R}$ admits QE in this language $\mathcal{L}_{\text{an}}^{D}$ gives an alternative approach to the theory of subanalytic sets. This subject was originally developed using other tools by Gabrielov, Hironaka and other analytic geometers. Indeed, a subset of $\mathbb{R}^n$ is definable using the language $\mathcal{L}_{\text{an}}^{D}$ if and only if it is subanalytic in its projective completion $\mathbb{P}^n(\mathbb{R})$.

An explicit axiomatization of the theory of $\mathbb{R}$ in the language $\mathcal{L}_{\text{an}}^{D}$ by finitely many schemes appears in [van den Dries et al. 1994]. This axiomatization is used to show that each field of power series over $\mathbb{R}$ with exponents in a divisible ordered abelian group carries a natural extra structure making it an elementary extension of $\mathbb{R}$ in the language $\mathcal{L}_{\text{an}}^{D}$. These power series fields with their extra analytic structure turn out to be important in the model theoretic study of the real field with restricted analytic functions and the unrestricted exponential function.

4. o-Minimal Expansions of the Real Field

For general background on o-minimality, see Macpherson's article in this volume, or the book [van den Dries 1998]. One direction in o-minimal studies that is close to classical model theory of fields involves constructing new o-minimal expansions of the field of reals. This activity received a big boost from Wilkie's theorem [1996a] that the real exponential field is model-complete. (Its o-minimality then follows from earlier work by Khovanskii.)

In this section we focus on some recent (post 1994) examples and constructions of o-minimal expansions of the real field. The main such expansions known at present are then indicated in an inclusion diagram, following Macintyre's lead.

Geometers often need the setting of manifolds rather than being tied to the particular coordinate systems of cartesian spaces $\mathbb{R}^n$. In Section 4.3 below we indicate how to accomplish this by means of the *analytic-geometric categories* of [van den Dries and Miller 1996]. This was used in [Schmid and Vilonen 1996].

4.1. Special constructions (see [van den Dries and Speissegger 1998a; 1998b]).

1. The expansion $\mathbb{R}_{\mathbf{an}^*}$, the field of reals with functions given by generalized convergent power series. In this structure one has among the basic functions those of the form $x \mapsto \sum_{n=0}^{\infty} a_n x^{r_n} : [0,1] \to \mathbb{R}$ with real coefficients a_n and real exponents r_n such that $r_n \uparrow +\infty$ and $\sum |a_n|(1+\varepsilon)^{r_n} < \infty$ for some $\varepsilon > 0$. In particular, $\mathbb{R}_{\mathbf{an}^*}$ defines the function

$$\zeta(-\log x) = \sum_{n=1}^{\infty} x^{\log n}$$

on $[0, e^{-1})$. The structure $\mathbb{R}_{\mathbf{an}^*}$ is model complete in its "natural" language, o-minimal, and polynomially bounded.

2. The expansion $\mathbb{R}_{\mathcal{G}}$, the field of reals with functions given by multisummable real power series. Among the basic operations of $\mathbb{R}_{\mathcal{G}}$ are the C^∞ functions

$f : [0,1] \longrightarrow \mathbb{R}$ whose restriction to $(0,1]$ extends to a holomorphic function on a sector

$$S(R,\phi) := \{z \in \mathbb{C} : |z| < R, |\arg z| < \phi\}$$

for some $R > 1$ and $\phi > \frac{\pi}{2}$, such that there exist positive constants A, B with $|f^{(n)}(z)| \le AB^n(n!)^2$ for all $z \in S(R,\phi)$, and $\lim_{z\to 0, z\in S(R,\phi)} f^{(n)}(z) = f^{(n)}(0)$.

Two examples of such functions:

- $$f(x) = \int_0^\infty \frac{e^{-t}}{1+xt}\,dt, \quad \text{for } 0 \le x \le 1.$$

  Its Taylor expansion at 0 is the *divergent* series $\sum_{n=0}^\infty (-1)^n n!\, x^n$.
- The continuous function ψ on $[0,1]$ given by Stirling's expansion

$$\log\Gamma(x) = (x - \tfrac{1}{2})\log x - x + \tfrac{1}{2}\log \pi + \psi\Big(\frac{1}{x}\Big), \quad \text{for } x \ge 1.$$

The structure $\mathbb{R}_{\mathcal{G}}$ is model complete in its natural language and polynomially bounded. Note that the Gamma function on $(0,+\infty)$ is definable in $\mathbb{R}_{\mathcal{G},\exp}$.

4.2. General constructions

I. If $\tilde{\mathbb{R}}$ is a polynomially bounded o-minimal expansion of the real field in which $\exp|_{[0,1]}$ is definable, then $(\tilde{\mathbb{R}}, \exp)$ is an exponentially bounded o-minimal expansion of the real field, and $\mathrm{Th}(\tilde{\mathbb{R}}, \exp, \log)$ admits QE relative to $\mathrm{Th}(\tilde{\mathbb{R}})$, see [van den Dries and Speissegger 1998b].

II. Suppose $\tilde{\mathbb{R}}$ is an o-minimal expansion of the real field by (total) C^∞ functions. Then Wilkie [1996b] proved that $\tilde{\mathbb{R}}$ remains o-minimal when expanded by the $\tilde{\mathbb{R}}$-Pfaffian functions. Here a C^∞ function $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ is $\tilde{\mathbb{R}}$-Pfaffian if there are C^∞ functions $f_1, \ldots, f_k : \mathbb{R}^n \longrightarrow \mathbb{R}$ (not necessarily definable in $\tilde{\mathbb{R}}$) such that $f = f_k$, and there are C^∞ functions $F_{ij} : \mathbb{R}^{n+i} \longrightarrow \mathbb{R}$, definable in $\tilde{\mathbb{R}}$, such that

$$\frac{\partial f_i}{\partial x_j}(x) = F_{ij}(x, f_1(x), \ldots, f_i(x))$$

for $i = 1, \ldots, k,\ j = 1, \ldots, n,\ x \in \mathbb{R}^n$.

This inspired further work along this line by Lion and Rolin [1998]. This in turn led Speissegger [1999] to prove that any o-minimal expansion $\tilde{\mathbb{R}}$ of the real field remains o-minimal when further expanded by the so-called *Rolle leaves* of 1-forms of class C^1 definable in $\tilde{\mathbb{R}}$. This expansion operation can then be iterated infinitely often to produce an o-minimal "Pfaffian closure" of $\tilde{\mathbb{R}}$.

The diagram on the next page lists the main o-minimal expansions of the real field that can be obtained by the methods above. An arrow $\mathbb{R}_{\mathcal{A}} \longrightarrow \mathbb{R}_{\mathcal{B}}$ means that the definable sets of $\mathbb{R}_{\mathcal{A}}$ are also definable in $\mathbb{R}_{\mathcal{B}}$. The bottom-left corner $\mathbb{R}_{\mathbf{alg}}$ is just the ordered field of real numbers with no further structure, and $\mathbb{R}_{\mathbf{an}}$ is the ordered real field expanded by the restricted analytic functions. The bottom arrows connect the polynomially bounded expansions, the upward pointing ones go to the expansions that can be built on top of the polynomially bounded ones by adding exp, and taking the "Pfaffian" closure.

$$\begin{tikzcd}
 & & & \mathbb{R}_{\mathrm{Pf}(\mathcal{G})} \\
\mathbb{R}_{\mathrm{Pf}(\mathbf{alg})} \arrow[r] & \mathbb{R}_{\mathrm{Pf}(\mathbf{an})} \arrow[r] \arrow[urr] & \mathbb{R}_{\mathrm{Pf}(\mathbf{an}^*)} & \\
 & & & \mathbb{R}_{\mathcal{G},\exp} \arrow[uu] \\
\mathbb{R}_{\mathbf{alg},\exp} \arrow[r] \arrow[uu] & \mathbb{R}_{\mathbf{an},\exp} \arrow[r] \arrow[uu] \arrow[urr] & \mathbb{R}_{\mathbf{an}^*,\exp} \arrow[uu] & \\
 & & & \mathbb{R}_{\mathcal{G}} \arrow[uu] \\
\mathbb{R}_{\mathbf{alg}} \arrow[r] \arrow[uu] & \mathbb{R}_{\mathbf{an}} \arrow[r] \arrow[uu] \arrow[urr] & \mathbb{R}_{\mathbf{an}^*} \arrow[uu] &
\end{tikzcd}$$

The known o-minimal expansions of the real field.

4.3. Analytic-geometric categories. In this subsection "manifold" means "real analytic manifold whose topology is Hausdorff with a countable basis". An **analytic-geometric category** $\mathcal{C}$ is given if each manifold M is equipped with a collection $\mathcal{C}(M)$ of distinguished subsets, called the **$\mathcal{C}$-subsets** of M, such that for all manifolds M and N the following holds:

1. $M \in \mathcal{C}(M)$ and $\mathcal{C}(M)$ is a boolean algebra.
2. If $A \in \mathcal{C}(M)$ then $A \times \mathbb{R} \in \mathcal{C}(M \times \mathbb{R})$.
3. If $f : M \longrightarrow N$ is a proper analytic map and $A \in \mathcal{C}(M)$, then $f(A) \in \mathcal{C}(N)$.
4. If $A \subseteq M$ and $\{U_i\}_{i \in I}$ is an open covering of M, then $A \in \mathcal{C}(M)$ iff $A \cap U_i \in \mathcal{C}(U_i)$ for all $i \in I$.
5. The boundary of every bounded $\mathcal{C}$-subset of $\mathbb{R}$ is finite.

We make a category $\mathcal{C}$ out of this by letting the objects of $\mathcal{C}$ be the pairs (A, M) with M a manifold and $A \in \mathcal{C}(M)$. The morphisms $(A, M) \longrightarrow (B, N)$ of objects (A, M) and (B, N) are continuous maps $f : A \longrightarrow B$ such that

$$\Gamma(f) := \{(a, f(a)) : a \in A\} \subseteq A \times B$$

belongs to $\mathcal{C}(M \times N)$. The composition of morphisms is given by composition of maps.

An object (A, M) of $\mathcal{C}$ is called **$\mathcal{C}$-set** A in M (or just the $\mathcal{C}$-set A). Call a morphism $f : (A, M) \longrightarrow (B, N)$ a **$\mathcal{C}$-map** $f : A \longrightarrow B$ if M and N are clear from the context.

The subanalytic subsets of a manifold M are necessarily $\mathcal{C}$-sets in M. Conversely we define an analytic-geometric category by taking just the subanalytic subsets of each manifold as its $\mathcal{C}$-sets.

By "o-minimal structure on $\mathbb{R}_{\mathbf{an}}$" we mean the system of definable sets of an o-minimal expansion of $\mathbb{R}_{\mathbf{an}}$. There is a one-to-one correspondence between o-minimal structures on $\mathbb{R}_{\mathbf{an}}$ in this sense, and analytic-geometric categories, as we now explain.

Given an analytic-geometric category $\mathcal{C}$ we get an o-minimal structure $\mathcal{S} = \mathcal{S}(\mathcal{C})$ on $\mathbb{R}_{\mathbf{an}}$ by putting

$$\mathcal{S}_n = \mathcal{S}(\mathcal{C})_n := \{X \subseteq \mathbb{R}^n : X \in \mathcal{C}(\mathbb{P}^n(\mathbb{R}))\} \quad .$$

Here we identify $\mathbb{R}^n$ with an open subset of $\mathbb{P}^n(\mathbb{R})$ via

$$(y_1, \ldots, y_n) \mapsto (1 : y_1 : \cdots : y_n) : \mathbb{R}^n \longrightarrow \mathbb{P}^n(\mathbb{R}).$$

Equivalently, for $A \subseteq \mathbb{R}^n$:

$$A \in \mathcal{S}(\mathcal{C})_n \iff \left\{ \Big(\frac{x_1}{\sqrt{1+x_1^2}}, \ldots, \frac{x_n}{\sqrt{1+x_n^2}} \Big) : x \in A \right\} \in \mathcal{C}(\mathbb{R}^n).$$

From an o-minimal structure $\mathcal{S} = (\mathcal{S}_n)$ on $\mathbb{R}_{\mathbf{an}}$ we get an analytic-geometric category $\mathcal{C} = \mathcal{C}(\mathcal{S})$ by defining the $\mathcal{C}$-subsets of an m-dimensional manifold M to be those $A \subseteq M$ such that for each $x \in M$ there is an open neighborhood U of x, an open $V \subseteq \mathbb{R}^m$ and an analytic isomorphism $h : U \longrightarrow V$ with $h(U \cap A) \in \mathcal{S}_m$.

For each analytic-geometric category $\mathcal{C}$ and each o-minimal structure $\mathcal{S}$ on $\mathbb{R}_{\mathbf{an}}$ we have $\mathcal{C}(\mathcal{S}(\mathcal{C})) = \mathcal{C}$ and $\mathcal{S}(\mathcal{C}(\mathcal{S})) = \mathcal{S}$.

Let $\mathcal{C}$ be an analytic-geometric category, M, N manifolds of dimension m, n respectively and $A \in \mathcal{C}(M)$. We can now state a number of basic facts directly in terms of this category. They follow easily from corresponding o-minimal results, using charts and partitions of unity.

1. Every analytic map $f : M \longrightarrow N$ is a $\mathcal{C}$-map.
2. $\mathrm{cl}(A), \mathrm{int}(A) \in \mathcal{C}(M)$.
3. $\mathrm{Reg}_k^p(A) \in \mathcal{C}(M)$ for each $k \in \mathbb{N}$ and positive $p \in \mathbb{N}$.
4. If A is also a C^1 submanifold of M, then its tangent, cotangent, and conormal bundles are $\mathcal{C}$-sets in their corresponding ambient manifolds: $TA \in \mathcal{C}(TM)$, $T^*A \in \mathcal{C}(T^*M)$, and $T_A^*M \in \mathcal{C}(T^*M)$.
5. A is locally connected, and has locally a finite number of components. If C is a component of A, then $C \in \mathcal{C}(M)$.
6. Every connected $\mathcal{C}$-set is path connected. The set of components of A is a locally finite subcollection of $\mathcal{C}(M)$.
7. If $\mathcal{F} \subseteq \mathcal{C}(M)$ is locally finite, then $\bigcap \mathcal{F} \in \mathcal{C}(M)$ and $\bigcup \mathcal{F} \in \mathcal{C}(M)$.
8. If $\varnothing \neq \mathcal{A} \subseteq \mathcal{C}(M)$ is locally finite, then
$$\dim\big(\bigcup \mathcal{A}\big) = \max\{\dim(A) : A \in \mathcal{A}\}.$$
9. If $f : A \longrightarrow N$ is a proper $\mathcal{C}$-map, then $\dim(C) \geq \dim(f(C))$ for all $\mathcal{C}$-sets $C \subseteq A$.
10. If $A \neq \varnothing$, then $\dim(\mathrm{closure}(A) \setminus A) < \dim(A)$.

The following results require more effort. The first one is due to Bierstone, Milman and Pawłucki in the subanalytic case.

1. If A is closed and $p \in \mathbb{N}$, there is a $\mathcal{C}$-map $f : M \longrightarrow \mathbb{R}$ of class C^p with $A = f^{-1}(0)$.
2. (Whitney stratification) Let $S \in \mathcal{C}(M)$ be closed and p be a positive integer. For every locally finite $\mathcal{A} \subseteq \mathcal{C}(M)$ there is a C^p Whitney stratification $\mathcal{P} \subseteq \mathcal{C}(M)$ of S, compatible with $\mathcal{A}$, with each stratum connected and relatively compact.

   Let $f : S \longrightarrow N$ be a proper $\mathcal{C}$-map and $\mathcal{F} \subseteq \mathcal{C}(M)$, $\mathcal{G} \subseteq \mathcal{C}(N)$ be locally finite. Then there is a C^p Whitney stratification $(\mathcal{S}, \mathcal{T})$ of f with connected strata such that $\mathcal{S} \subseteq \mathcal{C}(M)$ is compatible with $\mathcal{F}$ and $\mathcal{T} \subseteq \mathcal{C}(N)$ is compatible with $\mathcal{G}$.

References

[Artin and Schreier 1926] E. Artin and O. Schreier, "Algebraische Konstruktion reeller Körper", *Hamb. Abh.* **5** (1926), 85–99.

[Ax and Kochen 1965] J. Ax and S. Kochen, "Diophantine problems over local fields, I, II", *Amer. J. Math.* **87** (1965), 605–630, 631–648.

[Ax and Kochen 1966] J. Ax and S. Kochen, "Diophantine problems over local fields, III", *Ann. of Math.* (2) **83** (1966), 437–456.

[Denef and van den Dries 1988] J. Denef and L. van den Dries, "p-adic and real subanalytic sets", *Ann. of Math.* (2) **128**:1 (1988), 79–138.

[van den Dries 1998] L. van den Dries, *Tame topology and o-minimal structures*, London Math. Soc. Lecture Note Series **248**, Cambridge Univ. Press, Cambridge, 1998.

[van den Dries and Miller 1996] L. van den Dries and C. Miller, "Geometric categories and o-minimal structures", *Duke Math. J.* **84**:2 (1996), 497–540.

[van den Dries and Speissegger 1998a] L. van den Dries and P. Speissegger, "The real field with convergent generalized power series", *Trans. Amer. Math. Soc.* **350**:11 (1998), 4377–4421.

[van den Dries and Speissegger 1998b] L. van den Dries and P. Speissegger, "The field of reals with multisummable series and the exponential function", preprint, 1998. Available at http://www.math.utoronto.ca/~speisseg/preprints.html. To appear in *Proc. London Math. Soc.*

[van den Dries et al. 1994] L. van den Dries, A. Macintyre, and D. Marker, "The elementary theory of restricted analytic fields with exponentiation", *Ann. of Math.* (2) **140**:1 (1994), 183–205.

[Ershov 1965] Y. L. Ershov, "On elementary theories of local fields", *Algebra i Logika* (*Seminar*) **4**:2 (1965), 5–30.

[Kaplansky 1942] I. Kaplansky, "Maximal fields with valuations", *Duke Math. J.* **9** (1942), 303–321.

[Kochen 1969] S. Kochen, "Integer valued rational functions over the p-adic numbers: A p-adic analogue of the theory of real fields", pp. 57–73 in *Number Theory* (Houston, 1967), edited by W. J. Leveque and E. G. Straus, Proc. Sympos. Pure Math. **12**, Amer. Math. Soc., Providence, 1969.

[Lion and Rolin 1998] J.-M. Lion and J.-P. Rolin, "Volumes, feuilles de Rolle de feuilletages analytiques et théorème de Wilkie", *Ann. Fac. Sci. Toulouse Math.* (6) **7**:1 (1998), 93–112.

[Macintyre 1976] A. Macintyre, "On definable subsets of p-adic fields", *J. Symbolic Logic* **41**:3 (1976), 605–610.

[Macintyre 1986] A. Macintyre, "Twenty years of p-adic model theory", pp. 121–153 in *Logic colloquium* '84 (Manchester, 1984), edited by J. B. Paris et al., Stud. Logic Found. Math. **120**, North-Holland, Amsterdam, 1986.

[Prestel and Roquette 1984] A. Prestel and P. Roquette, *Formally p-adic fields*, Lecture Notes in Math. **1050**, Springer, Berlin, 1984.

[Schmid and Vilonen 1996] W. Schmid and K. Vilonen, "Characteristic cycles of constructible sheaves", *Invent. Math.* **124**:1-3 (1996), 451–502.

[Speissegger 1999] P. Speissegger, "The Pfaffian closure of an o-minimal structure", *J. Reine Angew. Math.* **508** (1999), 189–211.

[Tarski 1951] A. Tarski, *A decision method for elementary algebra and geometry*, 2nd ed., Univ. of California Press, Berkeley and Los Angeles, 1951.

[Terjanian 1966] G. Terjanian, "Un contre-exemple à une conjecture d'Artin", *C. R. Acad. Sci. Paris Sér. A-B* **262** (1966), A612.

[Wilkie 1996a] A. J. 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** (1996), 1051–1094.

[Wilkie 1996b] A. J. Wilkie, "A general theorem of the complement and some new o-minimal structures", preprint, 1996. To appear in *Selecta Math.*

Lou van den Dries
University of Illinois
Department of Mathematics
1409 W Green St.
Urbana, IL 61801-2917
United States
vddries@math.uiuc.edu