MODEL THEORY ≈ TAME MATHEMATICS

LOU VAN DEN DRIES

David Pierce transcribed (and slightly edited) these notes from slides written by Lou van den Dries and used in his talk at MSRI, Berkeley, California, USA, in 1998. Images of the slides are posted at
`http://www.msri.org/ln/msri/1998/mtf/vddries/`

1. Introduction

In model theory, we associate to a structure $\mathfrak{M}$ invariants like $\mathrm{Th}(\mathfrak{M})$, the **theory of** $\mathfrak{M}$; these invariants have a logical-combinatorial nature:

- $\mathfrak{M} \mapsto \mathrm{Th}(\mathfrak{M})$
- $\mathfrak{M} \mapsto$ category of definable sets and maps over $\mathfrak{M}$ (or over $\mathfrak{M}^{\mathrm{eq}}$)
- $\mathfrak{M} \mapsto$ category of definable groups and definable group homomorphisms over $\mathfrak{M}$ (or over $\mathfrak{M}^{\mathrm{eq}}$)

To use $\mathrm{Th}(\mathfrak{M})$, say, for the study of $\mathfrak{M}$ it is desirable that $\mathrm{Th}(\mathfrak{M})$ can be *effectively* described in practice: $\mathrm{Th}(\mathfrak{M})$ should be axiomatizable by *finitely* many axiom *schemes.*

1.1**. Example.** $\mathrm{Th}(\mathbb{C}$ as ring) is axiomatized by:

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

1.2**. Non-example** (Gödel)**.** $\mathrm{Th}(\mathbb{Z}$ as ring) cannot be effectively described in any reasonable way. (But $\mathbb{Z}$ as ordered additive group is tame!)

Since Gödel we know that the requirement of effective axiomatizability of $\mathrm{Th}(\mathfrak{M})$ is a serious constraint on $\mathfrak{M}$, and this has given rise to the impression (via popular literature) that there is a very limited scope left for "positive" contributions of logic to mathematics.

But: despite Gödel, mathematical problems, even in apparently "non-tame" subjects like number theory, do get solved, often by ingenious moves into tame territory! Thus the relevance of $\boxed{\text{model theory} \approx \text{tame mathematics}}$

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

Date: 1998; transcribed into $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-LaTeX 2002.

2. How to show tameness of an infinite structure $\mathfrak{M}$:

Find a set T of "axioms" such that $\mathfrak{M} \models T$ and show:

(1) T admits QE [quantifier-elimination] (and...) or:
(2) T is model-complete (and...) or:
(3) T is κ-categorical for some infinite cardinal κ or:
(4) ....

If any of these methods works, one usually obtains, not only a complete description of $\mathrm{Th}(\mathfrak{M})$, but also a lot of positive information about (the category of) definable sets and maps, such as a dimension theory for definable sets.

2.1. **Example.** For $\mathfrak{M} := (\mathbb{R}, <, 0, 1, +, -, \cdot)$ we take $T := \mathrm{RCF}$ (the axioms for real-closed ordered fields):

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

How do we show that RCF admits QE?

3. QE test:

An $\mathcal{L}$-theory T admits QE $\iff$
for any models $\mathfrak{M}$ and $\mathfrak{N}$ of T, each $\mathcal{L}$-embedding $\mathfrak{R} \rightarrow \mathfrak{N}$, where $\mathfrak{R} \subseteq \mathfrak{M}$ and $\mathfrak{R} \neq \mathfrak{M}$, can be extended to an $\mathcal{L}$-embedding

$$\mathfrak{R}' \rightarrow \mathfrak{N}'$$

from some *strictly larger* $\mathcal{L}$-substructure $\mathfrak{R}'$ of $\mathfrak{M}$ into some *elementary* extension $\mathfrak{N}'$ of $\mathfrak{N}$.

To apply this test to RCF, we need to know the following about ordered domains (Artin & Schreier, 1926):

Let A be an ordered (integral) domain. Then:

(1) A has a real closure A^{rc}, *i.e.* A^{rc} is a real closed ordered field extending A and algebraic over (the fraction field of) A.
(2) Every embedding $A \rightarrow L$ of A into a real closed ordered field L extends (uniquely) to an embedding $A^{\mathrm{rc}} \rightarrow L$.

Proof that RCF *admits QE.* Let K and L be real closed ordered fields, A an ordered sub-ring of K and $i : A \rightarrow L$ an embedding (of ordered rings). Assume $A \neq K$. We want to show that i can be extended as required in the QE-test. By (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, that is, $U < b < V$ where $U := \{x \in A : x < b\}$ and $V := \{x \in A : b < x\}$. Then $i(U) < i(V)$ in L. By passing to a suitable elementary extension L' of L we can take an element b' of L' such that $i(U) < b' < i(V)$. Then i extends to an embedding $i' : A[b] \rightarrow L'$ with $i'(b) = b'$. $\square$

Routine consequences:

(1) $\mathrm{Th}(\mathbb{R}, <, 0, 1, +, -, \cdot) = \{$logical consequences of RCF$\}$, and thus $\mathrm{Th}(\mathbb{R}, <, 0, 1, +, -, \cdot)$ is decidable.
(2) $\mathbb{Q}^{\mathrm{rc}}$ (the ordered field of real *algebraic* numbers) is an elementary substructure of $(\mathbb{R}, <, 0, 1, +, -, \cdot)$.
(3) Definable = semi-algebraic (for any real closed ordered field).

(4) If S is a semi-algebraic subset of $\mathbb{R}^{m+n}$, then there is a semi-algebraic map $f : \pi S \to \mathbb{R}^n$ such that $\Gamma(f) \subseteq S$: [picture]. (This can be read off directly from the axioms of RCF.)

4. The field of p-adic numbers (p prime):

Equip $\mathbb{Q}$ with the (non-Archimedean) absolute value given by $|a|_p = p^{-e}$, where $a = p^e m/n$ with $e, m, n \in \mathbb{Z}$ and $p \nmid mn$. The completion of $(\mathbb{Q}, |\cdot|_p)$ is called the field of p-adic numbers and is denoted by $(\mathbb{Q}_p, |\cdot|_p)$. Its elements are infinite sums $\sum_{k\in\mathbb{Z}} a_k p^k$ with all a_k in $\{0, 1, \dots, p-1\}$, and $a_k = 0$ for all k less than some k_0 in $\mathbb{Z}$.

$\mathbb{Z}_p =$ closure of $\mathbb{Z}$ in $\mathbb{Q}_p = \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}$, a compact sub-ring of 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 (*i.e.* a sub-ring of K such that $x \in K \implies x \in V \vee x^{-1} \in V$).

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

- its residue field $k := V/\,\mathrm{m}(V)$
- its value group $\Gamma := K^\times/V^\times$, viewed as an ordered abelian group with $aV^\times \leqslant bV^\times \iff b/a \in V$.

4.1. **Definition.** We call a valuation-ring V *Henselian* if each polynomial $X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n$ in $V[X]$ such that $a_{n-1} \notin \mathrm{m}(V)$ and $a_n \in \mathrm{m}(V)$ has a zero in $\mathrm{m}(V)$.

4.2. **Examples.** $\mathbb{Z}_p$ is Henselian, $k[[t]]$ is Henselian (for any field k).

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

So $(\mathbb{Q}_p, \mathbb{Z}_p)$ is a p-adically closed field.

4.4. **Theorem** (Kochen, late 1960s). *The theory of p-adically closed fields is complete and model-complete.*

Kochen used this to characterize rational functions in $\mathbb{Q}_p(X_1, \dots, X_n)$ that take only values in Z_p for arguments in Z_p (such as $(X^p - X)/p$). (“p-adic Hilbert’s 17th problem”)

5. Henselian valued fields of equi-characteristic 0

Consider *Henselian* valued fields (K, V) of equi-characteristic 0, *i.e.* $\mathrm{char}\, K = \mathrm{char}\, k = 0$.

5.1. **Theorem** (Ax & Kochen, Eršov, mid 1960s). *$\mathrm{Th}(K, V)$ is completely determined by the pair $(\mathrm{Th}(k), \mathrm{Th}(\Gamma))$ ($\Gamma =$ value-group).*

Proof. A classical result of Kaplansky’s (1940s) is that a valued field (K, V) of equi-characteristic 0 can be embedded as a valued field into the generalized formal power-series field $k((t^\Gamma))$ consisting of all formal series $\sum_{\gamma\in\Gamma} \alpha_\gamma t^\gamma$ with coefficients α_γ in k, and with well-ordered support $\{\gamma \in \Gamma : \alpha_\gamma \neq 0\}$ (the valuation-ring of $k((t^\Gamma))$ consisting of the series with support included in $\Gamma^{\geqslant 0}$).

By adapting suitably the embedding technique of Kaplansky, A & K and Eršov showed that if (K_1, V_1) and (K_2, V_2) are Henselian valued fields of equi-characteristic

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) have isomorphic elementary extensions. Therefore $\mathrm{Th}(K_1, V_1) = \mathrm{Th}(K_2, V_2)$. □

5.2. **Corollary.** *Given an elementary statement σ about valued fields, there are elementary statements $\sigma_1, \ldots, \sigma_k$ about fields and elementary statements $\tau_1, \ldots, \tau_k$ about ordered groups such that for* all *Henselian valued fields (K, V) of equi-characteristic* 0,

$$(K, V) \models \sigma \iff k \models \sigma_i \wedge \Gamma \models \tau_i \text{ for some } i \text{ in } \{1, \ldots, k\}.$$

Note the *uniformity*: the equivalence holds for all (K, V). This has a remarkable consequence:

6. Consequence for $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$

Let σ be an elementary statement about valued fields. Then

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

for all but finitely many primes p.

Proof. By Gödel's Completeness Theorem, there must be a formal proof of

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

from the axioms for Henselian valued fields of equi-characteristic 0. But only finitely many of the axioms saying that the fields and the residue-field have characteristic 0 can be used in such a proof. Thus the equivalence above also holds in $(\mathbb{Q}_p, Z_p)$ and in $(\mathbb{F}_p((t)), \mathbb{F}_p[[t]])$ for all but finitely many p. Now note that these two valued fields have the same residue-field and the same value-group. □

7. Application

Serge Lang showed in his thesis (early 1950s) that each homogeneous polynomial of degree d at least 1 in more than d^2 variables over $\mathbb{F}_p((t))$ has a non-trivial zero in that field. Thus, for a *given* d at least 1, this statement remains true when we replace $\mathbb{F}_p((t))$ by $\mathbb{Q}_p$, for all but finitely many p.

(Exceptions indeed occur, [Terjanian,] and may depend on d.)

What about QE for Henselian valued fields? There are several results of the following general nature (P.J. Cohen, V. Weispfenning, F. Delon, J. Denef, Pas).

Henselian valued fields of equi-characteristic 0 have (uniformly) relative QE: field-quantifiers can be *eliminated* at the cost of introducing quantified variables ranging over the residue-field, and over the value-group. (The exact language used here can make a difference for the applications.)

7.1. **Example** (Pas). For the valued field $(\mathbb{C}((t)), \mathbb{C}[[t]])$ we have (full) QE in the language with 3 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 an ordered abelian group with unary predicates for the sets $n\mathbb{Z}$, where $n = 2, 3, \ldots$); moreover, these sorts are related in the usual way, except that instead of the residue-class map $\mathbb{C}[[t]] \to \mathbb{C}$ we consider the *leading-coefficient map* $\mathbb{C}((t)) \to \mathbb{C}$ associating to each series its leading coefficient.