Quantifier Elimination For Valued Fields

Yimu Yin
Department of Philosophy
Carnegie Mellon University

September 19, 2006

Real Closed (Ordered) Fields (RCF)

The language of ordered rings: $0, 1, +, -, \times, <$

The axioms:

1. The axioms for fields.

2. (a) $x > 0 \wedge y > 0 \rightarrow x + y > 0$;

   (b) $x = 0 \vee x > 0 \vee -x > 0$;

   (c) $\neg(x > 0 \wedge -x > 0)$;

   (d) $x > 0 \wedge y > 0 \rightarrow xy > 0$.

3. (a) $\exists y\ (x = y^2 \vee -x = y^2)$;

   (b) $\exists y\ x_n y^n + \ldots + x_1 y + y_0 = 0$ for $n \geq 1$ odd.

QE stands for quantifier elimination.

Theorem. 1 (Tarski)**.** *RCF admits QE in the language of ordered rings.*

Tarski's original proof is syntactical, hence yields a recursive procedure for QE (but not practical).

There are several model-theoretic QE tests that can be used to give a model-theoretic proof of Tarski's theorem. For example,

Definition. **2.** *A theory T has the* **van den Dries property** *if and only if*

1. *For any model N, if there exists a model $M \models T$ such that $N \subseteq M$, then there is a T-closure N^* of N, that is, a model $N^* \models T$ such that $N \subseteq N^*$ and N^* can be embedded over N into any T-extension of N;*

2. *If $N, M \models T$ and $N \subsetneq M$, then there is an $a \in |M| \setminus |N|$ such that $N + a$ can be embedded into an elementary extension of N over N, where $N + a$ is the smallest submodel of M that contains $|N| \cup \{a\}$.*

Every ordered field K admits a maximal algebraic order-preserving field extension (in its algebraic closure). This is called the *real closure* of K.

For a model-theoretic proof of Tarski's theorem, the following is the key:

Theorem. 3. *Any two real closures of an ordered field K are isomorphic over K.*

We shall develop an analogue of this theorem for the p-adically closed fields (to be defined).

Theorem. 4 (Macintyre, McKenna, and van den Dries)**.** *Let K be an ordered field. If* $\mathrm{Th}(K)$ *in the language of ordered rings admits QE, then K is real closed.*

The idea of the proof: If a polynomial of degree n (odd) fails to have a root in K, then certain subset of K^n can be defined such that it is dense and codense in the Zariski topology.

Valued Fields

Let K be a field and Γ an ordered abelian group with a top element ∞. A valuation of K is a map

$$v : K \longrightarrow \Gamma$$

such that

1. $v(x) = \infty$ iff $x = 0$,

2. $v(xy) = v(x) + v(y)$,

3. $v(x + y) \geq \min(v(x), v(y))$.

Accordingly we get a ring (the valuation ring of v)

$$O = \{x \in K : v(x) \geq 0\},$$

and a maximal ideal of the ring

$$M = \{x \in K : v(x) > 0\},$$

and a residue field

$$\bar{K} = O/M.$$

Example: The p-adic number field $\mathbb{Q}_p$.

Fix a prime number p. Any nonzero rational number x can be written as

$$p^a \frac{m}{n}$$

where $a, m, n \in \mathbb{Z}$ and m, n prime to p. Define

$$\mathrm{ord}_p(x) = a.$$

Then

$$\mathrm{ord}_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

is a valuation.

This valuation induces a (non-Archimedean) norm $|\ |_p$ on $\mathbb{Q}$:

$$|x|_p = \begin{cases} \frac{1}{p^{\mathrm{ord}_p(x)}} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

The completion of $\mathbb{Q}$ with respect to the metric associated with this norm is our p-adic number field $\mathbb{Q}_p$.

Let $\mathbb{Z}_p \subseteq \mathbb{Q}_p$ be the valuation ring. This is also called the ring of p-adic integers.

Some basic facts about $\mathbb{Q}_p$:

1. $\text{ord}_p(p)$ is the minimal positive element in the value group, namely 1.

2. The residue field is $\mathbb{Z}/p\mathbb{Z}$, which is finite and has characteristic p.

3. Each element $b \in \mathbb{Q}_p$ has a unique expansion of the form
$$\frac{b_{-m}}{p^m} + \frac{b_{-m+1}}{p^{m-1}} + \ldots + b_0 + b_1 p + b_2 p^2 + \ldots$$
where $b_i \in \mathbb{Z}/p\mathbb{Z}$ for all $i \geq -m$ and
$$\text{ord}_p(a) = -m.$$

4. If K is a finite (or just algebraic) field extension of $\mathbb{Q}_p$, then there is a unique valuation on K that extends ord_p.

5. In 4, if we let $O_K, M_K \subseteq K$ be the valuation ring and its unique maximal ideal respectively, then O_K is the integral closure of $\mathbb{Z}_p$ in K.

   Let Γ_K be the value group of K. The **ramification index of K** is

$$e(K/\mathbb{Q}_p) = [\Gamma : \mathbb{Z}].$$

   The **residue degree of K** is

$$f(K/\mathbb{Q}_p) = [O_K/M_K : \mathbb{Z}/p\mathbb{Z}].$$

   If $[K : \mathbb{Q}_p] = n$ then we have

$$ef = n.$$

   If $e = 1$ then K is **unramified**. if $e = n$ then K is **totally ramified**.

p-**Valued Fields of** p-**Rank** d

p is a fixed prime number and d is a fixed natural number. (K, v) is a p-valued fields of p-rank d if

1. char$(\bar{K}) = p$ and char$(K) = 0$;

2. $O/(p)$ as a natural $\mathbb{Z}/p\mathbb{Z}$-module satisfies

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(O/(p)) = d.$$

Let $\pi \in M$ and i a natural number be such that $v(\pi)$ is the positive minimal element in Γ and

$$iv(\pi) = v(p).$$

Let

$$f = [\bar{K} : \mathbb{Z}/p\mathbb{Z}].$$

Then

$$d = if.$$

Henselianness

1. The valuation of (K, v) has a unique extension to any algebraic extension of K.

2. (Hensel's Lemma) Let $f(X) \in O[X]$. Suppose for some $a \in O$

$$\bar{f}(\bar{a}) = 0 \text{ and } \bar{f}'(\bar{a}) \neq 0.$$

Then there is an $a^* \in O$ such that

$$f(a^*) = 0 \text{ and } v(a^* - a) > 0.$$

3. (Newton's Lemma) Let $f(X) \in O[X]$. Suppose for some $a \in O$ and some $\alpha \in \Gamma$

$$vf(a) > 2\alpha \text{ and } vf'(a) \leq \alpha.$$

Then there is an $a^* \in O$ such that

$$f(a^*) = 0 \text{ and } v(a^* - a) > vf'(a).$$

Henselization

Any valued field (K, v) admits a unique minimal smallest Henselian field extension K^h, which is called the Henselization of K. we have :

1. $vK = vK^h$;

2. $\bar{K} = \overline{K^h}$.

In particular if K is a p-valued field of p-rank d then K^h is also a p-valued field of p-rank d.

The Fundamental Equality of Valuation Theory

Let L be a finite extension of (K, v). Let $v_1, \ldots, v_r$ be all the prolongations of v to L. Let $e_1, \ldots, e_r$ and $f_1, \ldots, f_r$ be the corresponding ramification indices and residue degrees. Then

$$[L : K] = \sum_{i=1}^{r} e_i f_i d_i,$$

where d_i is a power of p if $\mathrm{char}(\bar{K}) = p$, otherwise $d_i = 1$.

If $vK = \mathbb{Z}$ and L is a separable extension, then $d_i = 1$.

A Characterization of Finite Extensions of the Same p-Ranks

Let L/K be a finite extension. Suppose that (K, v) is a Henselian p-valued field of p-rank d. Then

$$\begin{aligned}\frac{d_L}{d_K} =& \frac{i_L[\bar{L} : \mathbb{Z}/p\mathbb{Z}]}{i_K[\bar{K} : \mathbb{Z}/p\mathbb{Z}]} \\ =& [\mathbb{Z}_L : \mathbb{Z}_K][\bar{L} : \bar{K}].\end{aligned}$$

By the fundamental equality we have

$$[L : K] = [vL/\mathbb{Z}_L : vK/\mathbb{Z}_K][L^o : K^o],$$

where L^o, K^o are the core fields of $(L, v), (K, v)$ respectively. Apply the fundamental equality to $[L^o : K^o]$ we get

$$[L : K] = [vL/\mathbb{Z}_L : vK/\mathbb{Z}_K][\mathbb{Z}_L : \mathbb{Z}_K][\bar{L} : \bar{K}].$$

Hence if $d_L = d_K$ then

$$[L : K] = [vL/\mathbb{Z}_L : vK/\mathbb{Z}_K] =^* [vL : vK].$$

p-Adically Closed Fields

p, d are fixed.

Definition. 5. *K is called a p-***adically closed field** *iff K does not have any proper p-valued algebraic extension of the same rank.*

Theorem. 6. *K is a p-adically closed field iff K is Henselian and $vK/\mathbb{Z}_K$ is divisible (i.e. vK is elementarily equivalent to $\mathbb{Z}$ as an ordered group, i.e. vK is a model of ordered Presburger arithemetic).*

K admits a unique p-adic closure iff $vK/\mathbb{Z}_K$ is divisible.

Let $f_K = [\bar{K} : \mathbb{Z}/p\mathbb{Z}]$ and $q = p^{f_K}$. The so called **Teichmüller representatives** are the roots of the polynomial

$$X^q - X.$$

Let $i_K = v(p)$. Choose an element $\pi \in O$ such that $v(\pi)$ is minimal positive. For each natural number $m = j + ki_K$ set

$$\omega_m = \pi^j p^k.$$

Then each element $a \in O$ admits an unique expansion of the form

$$t_0 + t_1\omega_1 + t_2\omega_2 + \ldots + t_m\omega_m + A_m$$

for each m, where each t_i is a Teichmüller representative.

How such expansions are used:

Lemma. 7. *Let $L|K$ be a p-valued extension. Suppose that K is algebraically closed in L. If $\bar{L} = \bar{K}$ then $\mathbb{Z}_L = \mathbb{Z}_K$.*

Proof. Look at the expansion of π^{i_L}/p. Construct a suitable Eisenstein polynomial

$$f(X) = X^{i_L} - pg(X) \in K[X]$$

such that $g(\pi) + A_m = \pi^{i_L}/p$ for sufficiently large m and hence

$$vf(\pi) > 2vf'(\pi).$$

$\square$

Algebraically Closed Subfield is p-Adically Closed

Theorem. 8. *Let L be a p-adically closed field. Suppose that K is a sub-value-field. If K is algebraically closed in L then K is also p-adically closed and is of the same rank as L.*

This follows from the following:

1. $\bar{K} = \bar{L}$;

2. K contains an element of L of the minimal positive value, i.e. $\mathbb{Z}_K = \mathbb{Z}_L$;

3. the factor group vL/vK is torsion free.

The Special Embedding Theorem

Let $L|K$ be any field extension. Define the radical group (a subgroup of $L^{\times}$)

$$J_{L|K} = \{t \in L : t^n \in K \text{ for some } n\}\,.$$

Theorem. 9 (Radical Structure Theorem)**.** *Let $L|K$ be an algebraic extension of the same rank. Suppose that K is Henselian. Then*

$$L = K(J_{L|K}).$$

In fact the valuation map $v : J_{L|K} \longrightarrow vL$ induces an isomorphism:

$$J_{L|K}/K^{\times} \cong vL/vK.$$

Hence if $L|K$ is a finite extension then

$$[J_{L|K} : K^{\times}] = [L : K]$$

and

$$L = K[X_1, \ldots, X_r]/I = K(t_1, \ldots, t_r)$$

where the ideal I is generated by

$$X_i^{n_i} - c_i, \quad 1 \leq i \leq r.$$

Theorem. 10 (Special Embedding Theorem). *Let $L|K$ be a Henselian algebraic extension of the same rank. Let $L'|K$ be an arbitrary Henselian valued field extension. TFAE*

1. *L can be embedded into L' over K.*

2. *$K \cap L^n \subseteq K \cap L'^n$ for all n.*

Corollary. 11. *If $L'|K$ is also a Henselian algebraic extension of the same rank, then L, L' are isomorphic over K iff $K \cap L^n = K \cap L'^n$ for all n.*

The General Embedding Theorem

Theorem. 12 (General Embedding Theorem)**.** *Let $L|K$ be a Henselian extension of the same rank. Let $L'|K$ be a p-adically closed extension. Suppose that L' is sufficiently saturated. TFAE*

1. *L can be embedded into L' over K.*

2. *$K \cap L^n \subseteq K \cap L'^n$ for all n.*

For $2 \Rightarrow 1$ we have the following reductions:

First reduction: We may replace 2 by "K is algebraically closed in L". This is equivalent to: K is Henselian and vL/vK is torsion free.

Second reduction: We may assume that $L|K$ is of transcendence degree 1.

Third reduction: We may assume that $L|K$ is finitely generated.

Fourth reduction: We may assume that $L|K$ is $K(X)$, i.e. a rational function field in one variable.

The last reduction has two cases:

Case A: $vK(X) = vK$.

Case B: $vK(X)/vK$ is infinitely cyclic with generator $v(X) + vK = \xi + vK$, i.e.

$$vK(X) = vK \oplus \xi\mathbb{Z}.$$

Quantifier Elimination for p-Adically Closed Fields of p-Rank d (VCF(p,d))

The two-sorted language:

1. The field sort (K):

(a) $0, 1, +, -, \times, /$;
(b) new constants $u_1, \ldots, u_d$;
(c) a unary nth power predicate P_n for each n.

2. The value group sort (Γ):

(a) $0, +, -, <, \infty$;
(b) a unary divisibility predicate D_n for each n.

3. A valuation function $v : K \longrightarrow \Gamma$.

The axioms:

1. All the standard axioms that guarantee the following: K is a field; Γ is an abelian group with a discrete ordering; v is a valuation.

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

3. $\forall x\ (D_n(x) \leftrightarrow \exists y\ (x = ny))$ and $\forall x\ (D_n(x) \vee D_n(x+1) \vee \ldots \vee D_n(x+n-1))$ for each n.

4. K is Henselian.

5. $u_1, \ldots, u_d$ form a basis for the $\mathbb{Z}/p\mathbb{Z}$-module $O/(p)$.

Now using a suitable modified model-theoretic QE test (e.g. van den Dries property) for many-sorted languages and the General Embedding Theorem we obtain:

Theorem. 13 (Quantifier Elimination). *For each p and each d, VCF(p, d) admits QE.*

Question. 14. *For any valued field K, suppose that K satisfies all the axioms of VCF(p, d) except Henselianness and* $\mathrm{Th}(K)$ *has QE in the language of VCF(p, d), does this imply that K is Henselian?*