Model Theory of Enriched Valued Fields

Thomas Scanlon
`http://math.berkeley.edu/~scanlon`
`scanlon@math.berkeley.edu`

Logic Colloquium 2002
(ASL European Summer meeting)
Münster
4 August 2002

Valued Fields

Definition: A valued field is a field K given together with a homomorphism $v : K^\times \to \Gamma$ from the multiplicative group of K to an ordered abelian group Γ for which the inequality $v(x+y) \geq \min\{v(x), v(y)\}$ whenever $x + y \neq 0$.

We extend v to 0 by defining $v(0) = \infty > \Gamma$ (and $\infty + \gamma = \gamma + \infty = \infty$ for $\gamma \in \Gamma \cup \{\infty\}$) so that the inequality $v(x+y) \geq \min\{v(x), v(y)\}$ holds globally.

We refer to Γ as the *value group* and usually insist that v be surjective.

Relation to Normed Fields

Recall that a *normed field* is a field K given together with a function $|\cdot| : K \to \mathbb{R}$ for which the following hold universally

- $|x| \geq 0$
- $|x| = 0 \leftrightarrow x = 0$
- $|xy| = |x| \cdot |y|$
- $|x + y| \leq |x| + |y|$

Observation: If (K, Γ, v) is a valued field and $\psi : \Gamma \to \mathbb{R}_+$ is an order-*reversing* homomorphism of groups, then K is a normed field with $|\cdot| = \psi \circ v$.

Examples of Valued Fields

- Any field K with the trivial valuation defined by $v(x) = 0$ for all $x \in K^\times$
- The field $\mathcal{M}$ of meromorphic functions on the plane with $v(f) :=$ the order of vanishing of f at zero
- Fix a prime number p. Then the p-adic valuation on $\mathbb{Q}$ is defined by $v_p(x) = r \Leftrightarrow x = p^r \frac{a}{b}$ where $\gcd(p, ab) = 1$.
- A Cauchy completion of any valued field
- The field of p-adic numbers, $\mathbb{Q}_p$, is the completion of $\mathbb{Q}$ with respect to the p-adic valuation.
- For any field k the field of Laurent series over k, $k((t))$, is a valued field via $v(f) = N \Leftrightarrow f = \sum\limits_{n \geq N} a_n t^n$ with $a_N \neq 0$.

Algebraically Closed Valued Fields

Theorem (A. Robinson): Formulate the theory of valued fields in the language $\mathcal{L}(+, -, \times, |, 0, 1)$ where we interpret $x|y \Leftrightarrow v(x) \leq v(y)$. The theory of nontrivially valued algebraically closed fields is the model completion of the theory of valued fields.

Rings of Integers

If (K, Γ, v) is a valued field, the set $\mathcal{O}_{K,v} := \{x \in K : v(x) \geq 0\}$ is a subring of K called the ring of (v)-integers. The set $\mathfrak{m}_{K,v} := \{x \in K : v(x) > 0\}$ is *the* maximal ideal of $\mathcal{O}_{K,v}$.

The quotient ring $k(v) := \mathcal{O}_{K,v}/\mathfrak{m}_{K,v}$ is called the *residue field* and the quotient map $\pi : \mathcal{O}_{K,v} \to k(v)$ is the *residue map*.

Completions of the Theory of Algebraically Closed Valued Fields

Theorem (A. Robinson): The completions of the theory of nontrivially valued algebraically closed fields are given by specifying the characteristic of the valued field and the characteristic of the residue field.

Hensel's Lemma

Lemma: Let K be a complete valued field with an archimedian value group. Let $P(X) \in \mathcal{O}_K[X]$ be is a polynomial with integral coefficients. Suppose that $a \in \mathcal{O}_K$ is a point for which $v(P(a)) > 0 = v(P'(a))$. Then there is some $b \in K$ with $v(a - b) = v(P(a))$ and $P(b) = 0$.

Proof Sketch: Use Newton's method:

$$P(a + \epsilon) \quad \equiv \quad P(a) + P'(a)\epsilon + (\epsilon^2)$$

From a produce a better approximation with $\tilde{a} := a - \frac{P(a)}{P'(a)}$.

Ax-Kochen-Eršov Theorems

We say that a valued field K is *henselian* if the conclusion of Hensel's Lemma holds in K.

Theorem (Ax & Kochen, Eršov): If K and L are two henselian fields of characteristic zero with residue fields k_K and k_L, respectively, and value groups Γ_K and Γ_L; then $K \equiv L$ if and only if $k_K \equiv k_L$ and $\Gamma_K \equiv \Gamma_K$.

Some Consequences of AKE

- If K is a henselian field of characteristic zero whose residue field and value group have decidable theories, then so does K as a valued field.
- $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ have the same limit theories as $p \to \infty$.

Elimination of Quantifiers for Henselian Fields

Henselian fields of characteristic zero eliminate quantifiers relative to their value groups and the residue field when that field has characteristic zero and the residue rings $\mathcal{O}_K/p^n\mathfrak{m}_K$ when the residue characteristic is p in natural expansions of the language of valued fields.

Analytic Functions

If K is a complete valued field with archimedean value group, then the ring $\mathcal{O}_K\langle X_1,\ldots,X_n\rangle$ of restricted analytic functions in n variables is the subring of $\mathcal{O}_K[[X_1,\ldots,X_n]]$ consisting of those power series $\sum a_\alpha X_1^{\alpha_1}\cdots X_n^{\alpha_n}$ with $v(a_\alpha)\to\infty$ as $|\alpha|\to\infty$.

Fixing a ring R of coefficients, the analytic language $\mathcal{L}_{\text{an}}$ is the expansion of the language of rings by function symbols for each restricted analytic function in any number of variables. Each such symbol is interpretted as a function with integral arguments.

Quantifier Elimination in an Expansion of $\mathcal{L}_{\text{an}}$

Theorem (Denef & van den Dries): The theory of $\mathbb{Q}_p$ in the expansion of $\mathcal{L}_{\text{an}}$ by the Macintyre power predicates and the function $D(x, y)$ defined by $D(x, y) := \frac{x}{y}$ if $v(x) \geq v(y) \neq \infty$ and $:= 0$ otherwise eliminates quantifiers.

Extensions of this theorem due to van den Dries, Gardner, Lipshitz, Z. Robinson, Schoutens, *et al* have been proved.

Valued Difference Fields

Definition: A valued difference field is a valued (K, v, Γ) given together with an endormorphism $\sigma : K \to K$ for which $v(x) = v(\sigma(x))$ for all $x \in K$.

Derivatives of Difference Polynomials

If $P(X) := \widetilde{P}(X, \sigma(X), \ldots, \sigma^n(X))$ where $\widetilde{P}(X_0, \ldots, X_n) \in \mathcal{O}_K[X_0, \ldots, X_n]$, then we define $P'(X)$ to be the linear difference operator

$$P'(X) := \sum_{i=0}^{n} \frac{\partial \widetilde{P}}{\partial X_i}(X, \sigma(X), \ldots, \sigma^n(X))\sigma^i$$

Then for any $a \in \mathcal{O}_K$ and $\epsilon \in \mathfrak{m}_K$, we have $P(a + \epsilon) \equiv P(a) + P'(a)\epsilon + \epsilon^2 \mathcal{O}_K$.

Difference Henselian Fields

Lemma: If K is a maximally complete valued difference field with a residue field in which every nontrivial linear difference operator is surjective, $P(X_0, \ldots, X_n) \in \mathcal{O}_K[X_0, \ldots, X_n]$ is a polynomial with integral coefficients and $a \in \mathcal{O}_K$ is a point with $v(P(a, \sigma(a), \ldots, \sigma^n(a))) > 0 = v(\frac{\partial P}{\partial X_i}(a, \sigma(a), \ldots, \sigma^n(a)))$ for some i, then there is some b with $P(b) = 0$ and $v(a - b) = v(P(a))$.

Definition: A valued difference field satisfying the conclusion of the above lemma and for which every value is represented by an element fixed by σ is called *difference henselian*.

Quantifier Elimination for Difference Henselian Fields

Theorem (Bélair, Macintyre, Scanlon): Working in the expansion of the the language of valued difference fields by a family of angular component functions, the theory of difference henselian fields of characteristic zero eliminates quantifiers and is complete relative to the theories of the residue rings and value group and the isomorphism type of the prime substructure.

Relative Frobenii

If k is a field of characteristic p and q is any positive integral power of p, then the function $\tau_q : k \to k$ given by $x \mapsto x^q$ is an endomorphism of k.

If R is a complete discrete valuation ring with $k \cong R/pR$, then there is a unique continuous endomorphism $\sigma : R \to R$ with $\sigma(x) \equiv x^q \pmod{p}$.

p-Derivations

Definition: A p-derivation on a ring R is a function $\delta : R \to R$ satisfying

- $(\forall x, y)\ \delta(x + y) = \delta(x) + \delta(y) + \Phi_p(x, y)$ where $\Phi_p(X, Y) = \sum_{i=1}^{p-1} \frac{-1}{p}\binom{p}{i} X^i Y^{p-i} \in \mathbb{Z}[X, Y]$
- $(\forall x, y)\ \delta(x, y) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y)$

p-Derivations and Valued D-fields

If (K, v, σ) is a valued difference field for which the relation $\sigma(x) \equiv x^p + p\mathcal{O}_K$ holds universally on the ring of integers, then the function $\delta_p(x) := \frac{\sigma(x)-x^p}{p}$ is a p-derivation on $\mathcal{O}_K$.

p-Jet Functions

Definition: Let R be a complete discrete valuation ring with a p-derivation $\delta : R \to R$. A p-jet function on R^n is a function $f : R^n \to R$ of the form $(x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n; \delta(x_1), \ldots, \delta(x_n); \ldots; \delta^m(x_1), \ldots, \delta^m(x_n))$.

Buium has developed an extensive theory of p-jet functions having produced, for instance, p-jet analogues of modular forms and of Manin homomorphisms.

Analytic Difference Rings

Let R be a complete discrete valuation ring with R/pR an alebraically closed field.

The signature of analytic difference rings (over R) is the signature of valued difference fields augented by $\mathcal{L}_{\text{an}}$ (over R). Here we include the Denef-van den Dries quotient function and a family of angular component functions modulo powers of p (a compatible family of homomorphisms $\alpha_n : K^\times \to (\mathcal{O}_K/p^n\mathcal{O}_K)^\times$ extending the reduction maps).

Theorem: The theory of R eliminates quantifiers relative to the value group.

Keys to the Proof

- A uniform version of the Weierstrass preparation theorem due to van den Dries, Haskell, and Macpherson allows us to finitize many problems.
- Differentiability of a certain class of germs of terms (where we allow division only by constants) permits Kaplansky-style approximations.

Pro-Definable Structure

If R is a complete discrete valuation ring with residue field $k = R/\mathfrak{m}$, then for each $n \in \mathbb{Z}_+$ the ring $R/\mathfrak{m}^n$ may be interpretted as k^n with ring operations given by polynomial functions.

More generally, if R has the structure of an analytic D-ring and $X \subseteq R^n$ is defined by the vanishing of a sequence of analytic functions composed with powers of D, then the same equations define a set $X_m \subseteq (R/\mathfrak{m}^m)^n$ which we may interpret in k and $X = \varprojlim X_m$.

Stable Embeddedness

Corollary: Let R be a complete discrete valuation ring with $k = R/pR$ an algebraically closed field. Let ${}^*R \succeq R$ be an elementary extension as an analytic difference ring with ${}^*k := {}^*R/p{}^*R$. If $X \subseteq ({}^*k)^n$ is a ${}^*R$-definable subset of some power of its residue field, then X is ${}^*k$-definable in the language of rings.

Uniformity

Corollary: The Nash lifting theorem holds for analytic difference equation.

Corollary: For any definable family of definable sets in k^n there is a uniform upper bound on the size of the finite sets in the family.

A Number Theoretic Consequence

Theorem: Let R be a discrete valuation ring with $R/pR = k$ algebraically closed. If $\{G_b\}_{b \in B}$ is a family of commutative algebraic groups over R and $\{X_b \subseteq G_b\}_{b \in B}$ is a family of subvarieties, then there are a natural number m and a finite set of families of algebraic subgroups of the G_b's such that for any $b \in B$ the intersection of $X_b(R)$ with the torsion group of $G_b(R)$ is a union of at most m translates of the distinguished subgroups of G_b.

Questions

- Do these results extend to the richer rigid analytic languages of Gardner, Lipshitz, Z. Robinson, and Schoutens?
- How do these theories vary with p? Restricting to power series with $\mathbb{Z}_p$-coefficients permits a good AKE theorem.
- In the strict sense, one cannot ask about the decidability of this theory. In a loose sense, it is decidable relative to a fragment of the theory of the analytic functions. Are the fragments we actually use decidable?