Cell decomposition in valued fields

Yimu Yin
Department of Philosophy
Carnegie Mellon University

October 31, 2006

The topics of this talk are contained in the following three papers:

1. *The rationality of the Poincaré series associated to the p-adic points on a variety*, Jan Denef, Invent. Math., 77, pp. 1-23, 1984.

2. *Uniform p-adic cell decomposition and local zeta functions*, Johan Pas, J. reine angew. Math., 399, pp. 137-172, 1989.

3. *Rationality of p-adic Poincaré series: uniformity in p*, Angus MacIntyre, Annals of Pure and Applied Logic, 49, pp. 31-74, 1990.

Recall Macintyre's Theorem (generalized to finite extensions of $\mathbb{Q}_p$ by Prestel and Roquette):

Theorem. 1. *The theory of p-adically closed fields of p-rank d admits quantifier elimination in Macintyre's language (with d many new constants).*

In 1984 Weispfenning gave a primitive recursive QE procedure for this theory, though it was done in a considerably expanded language.

The problem of uniformity: Develop a "natural" formalism in which the QE procedure is uniform for all

$$\mathbb{Q}_2, \mathbb{Q}_3, \mathbb{Q}_5, \mathbb{Q}_7, \ldots, \mathbb{Q}_{57}, \ldots, \mathbb{Q}_{2^{232582657}-1}, \cdots$$

that is, independent of the choice of p.

Macintyre published a paper in 1990 that offered a solution to this problem. But the formalism there is very complicated. (Verdict: unnatural.)

Paul J. Cohen's Quantifier Elimination Procedure:

1. A primitive recursive decision procedure for $\mathbb{Q}_p$.

2. Elimination takes place inside a fixed henselian field, using only Hensel's Lemma.

3. He gives a procedure for "isolating" the roots of polynomials, and simultaneously reducing conditions on the nth root of a polynomial F to "simple" conditions on the coefficients of F.

Inspired by Cohen's work, Jan Denef subsequently developed the technique of p-adic cell decomposition. He used it to prove the following theorem:

Theorem. 2. *$P(T)$ is a rational function of T.*

Let $f_1(\bar{x}), \ldots, f_r(\bar{x})$ be polynomials in m variables $\bar{x} = (x_1, \ldots, x_m)$ with coefficients in $\mathbb{Z}_p$. For $n \in \mathbb{N}$ let $N^*(n)$ be the number of elements in the set

$$\{\bar{x} \mod p^n : \bar{x} \in \mathbb{Z}_p^m \text{ and } \bigwedge_i (f_i(\bar{x}) = 0 \mod p^n)\},$$

and let $N(n)$ be the number of elements in the set

$$\{\bar{x} \mod p^n : \bar{x} \in \mathbb{Z}_p^m \text{ and } \bigwedge_i (f_i(\bar{x}) = 0)\}.$$

Define the Poincaré series

$$P^*(T) = \sum_{n=0}^{\infty} N^*(n)T^n,$$

$$P(T) = \sum_{n=0}^{\infty} N(n)T^n.$$

Igusa proved that $P^*(T)$ is a rational function if $r = 1$. Meuser proved this for every r. Serre asked whether $P(T)$ is a rational function of T.

Let $|d\bar{x}|_p = |dx_1|_p \dots |dx_m|_p$ be the Harr measure on $\mathbb{Q}_p^m$ with $\left|\mathbb{Z}_p^m\right|_p = 1$. Let

$$D = \{(\bar{x}, w) \in \mathbb{Z}_p^m \times \mathbb{Z}_p : \\ \exists \bar{y} \in \mathbb{Z}_p^m \; (x = y \mod w \wedge \bigwedge_i f_i(\bar{y}) = 0)\}.$$

For any positive real number s let

$$Z(s,p) = \int_D |w|_p^s \, |d\bar{x}|_p \, |dw|_p \, .$$

$$
\begin{aligned}
Z(s,p) &= \sum_{n=0}^{\infty} \int\limits_{\substack{D \\ \mathrm{ord}_p(w)=n}} p^{-ns}\, |d\bar{x}|_p\, |dw|_p \\
&= \sum_{n=0}^{\infty} p^{-ns} \int\limits_{\substack{(x,p^n)\in D \\ \mathrm{ord}_p(w)=n}} |d\bar{x}|_p\, |dw|_p \\
&= \sum_{n=0}^{\infty} p^{-ns} \int\limits_{(x,p^n)\in D} |d\bar{x}|_p \int\limits_{\mathrm{ord}_p(w)=n} |dw|_p \\
&= \sum_{n=0}^{\infty} p^{-ns} \frac{N(n)}{p^{nm}} \left(\frac{1}{p^n} - \frac{1}{p^{n+1}}\right) \\
&= \frac{p-1}{p} \sum_{n=0}^{\infty} N(n)(p^{-s}p^{-m-1})^n.
\end{aligned}
$$

So to prove the rationality of $P(T)$, it is enough to prove that integrals of the form

$$Z(s,p) = \int_D |h(\bar{x})|_p^s \, |d\bar{x}|_p$$

is a rational function of p^{-s}, where h is a function and D a subset of $\mathbb{Q}_p^n$ for some n, both of which are definable in a suitable language for $\mathbb{Q}_p$. (If h has no zero on $\mathbb{Q}_p^m$ then s could be any real, otherwise we have to require $s > 0$.)

A suitable language (a.k.a. the Denef-Pas language)

We have 3 sorts: a field K, a residue field $\overline{K}$, and a valuation group $\Gamma \cup \{\infty\}$.

- a valuation $v : K \longrightarrow \Gamma \cup \{\infty\}$.

- an angular component $\overline{\mathrm{ac}} : K \longrightarrow \overline{K}$.

Later we shall add more symbols to the language. For example, we want the Γ-sort to have the Presburger language at certain point.

What is an angular component?

1. $\overline{\text{ac}}(x) = 0$ iff $x = 0$;

2. $\overline{\text{ac}} : K^\times \longrightarrow \overline{K}^\times$ is a group homomorphism;

3. $\overline{\text{ac}}\, u = u + M$ for $u \in O \setminus M$.

Lemma. 3. *For $a \neq b \in K$ with $v(a) = v(b)$, $\overline{\text{ac}}\, a = \overline{\text{ac}}\, b$ iff $v(a - b) > v(a) = v(b)$.*

Axioms

1. $\operatorname{char} K = 0$;

2. $\operatorname{char} \overline{K} = 0$;

3. K is henselian;

4. v is a valuation, $\overline{\mathrm{ac}}$ is an angular component, and all other symbols are axiomatized in the standard way.

Call this theory $VF_{\overline{\mathrm{ac}}}$, valued fields with angular component.

Definition. 4. *A formula φ is simple if φ does not contain any K-quantifiers. A subset D of K^m or $K^m \times \overline{K}^n$ is simple if it is defined by a simple formula.*

Definition. 5. *A function $h : K^m \times \overline{K}^n \longrightarrow K$ is strongly definable if, for each simple formula $\varphi(t)$, there is a simple formula $\psi(x, \xi)$ such that*

$$\varphi(h(x, \xi)) \leftrightarrow \psi(x, \xi).$$

What's a cell?

Let $(x,\xi)\in K^m\times\overline{K}^n$. Let C be a simple subset of $K^m\times\overline{K}^n$, which we shall call a parameter set. Let $b_1,b_2,c: C\longrightarrow K$ be strongly definable functions. Let $\lambda\in\mathbb{N}$. Let $\square_1,\square_2$ be $<,\leq$ or no condition.

Definition. 6. *For each $\xi\in\overline{K}^n$, the set*

$$\begin{aligned}A(\xi)=\{(x,t)\in K^m\times K:(x,\xi)\in C,\\ v\,b_1(x,\xi)\ \square_1\ \lambda\, v(t-c(x,\xi))\ \square_2\ v\,b_2(x,\xi),\\ \overline{\mathrm{ac}}(t-c(x,\xi))=\xi_1\}\end{aligned}$$

is called a fiber.

Definition. 7. *Suppose that if* $\xi \neq \xi'$ *then* $A(\xi) \cap A(\xi') = \emptyset$.

$$A = \bigcup_{\xi \in \overline{K}^n} A(\xi)$$

is called a cell in $K^m \times K$ *with center* $c(x, \xi)$.

Cell decomposition

Let $f(x, t)$ be a polynomial of the form

$$g_d(x, \Delta)t^d + \ldots + g_0(x, \Delta),$$

where $g_0(x, \Delta), \ldots, g_d(x, \Delta)$ are strongly definable functions (Δ are extra parameters which will be omitted in the sequel).

Theorem. 8. *There is a finite partition of $K^m \times K$ into cells A such that:*

Write

$$f(x,t) = \sum_{i=0}^{d} a_i(x,\xi)(t - c(x,\xi))^i.$$

Let $A(\xi)$ be a fiber of A. Then for each $(x,\xi) \in A(\xi)$ we have

$$\begin{aligned} v\, f(x,t) &= v\, a_{i_0}(x,\xi)(t - c(x,\xi))^{i_0} \\ &= \min_{0 \le i \le d} v\, a_i(x,\xi)(t - c(x,\xi))^i \end{aligned}$$

and

$$\overline{\mathrm{ac}}\, f(x,t) = \xi_{j_0},$$

where i_0, j_0 are fixed (i.e. do not depend on (x,ξ,t)).

For polynomials $f_1, \ldots, f_r$:

Theorem. 9. *There is a finite partition of $K^m \times K$ into cells A such that:*

Let $A(\xi)$ be a fiber of A. Then for each $(x,t) \in A(\xi)$ and each $1 \le i \le r$ we have

$$v\, f_i(x,t) = v\, h_i(x,\xi)(t - c(x,\xi))^{\nu_i}$$

and

$$\overline{\mathsf{ac}}\, f_i(x,t) = \xi_{\mu(i)},$$

where the h_i's are strongly definable functions and $\nu_i \in \mathbb{N}$ and $1 \le \mu(i) \le n$ are fixed (i.e. do not depend on (x,ξ,t)).

Quantifier elimination

Theorem. 10. *The theory $VF_{\overline{\mathrm{ac}}}$ admits elimination of K-quantifiers.*

Sketch of the proof. Need to consider formulas of the forms

$$\bigwedge_{i=1}^{r} \overline{\mathrm{ac}}\, f_i(x,t) = \rho_i \wedge \bigwedge_{j=1}^{s} v\, g_j(x,t) = l_j.$$

After cell decomposition this is reduced to

$$(x,t) \in A(\xi) \wedge \bigwedge_{i=1}^{r} \xi_{\mu(i)} = \rho_i$$
$$\wedge \bigwedge_{j=1}^{s} \Big(v\, h_j(x,\xi) + \nu_j\, v\,(t - c(x,\xi)) = l_j \Big).$$

Introducing a new variable l for $v\,(t - c(x,\xi))$ we then add two conjuncts to the above

$$v\,(t - c(x,\xi)) = l \wedge \overline{\mathrm{ac}}(t - c(x,\xi)) = \xi_1,$$

hence reduce the whole thing to

$$\exists t\ (v\,(t - c(x,\xi)) = l \wedge \overline{\mathsf{ac}}(t - c(x,\xi)) = \xi_1),$$

which is true. $\square$

Compute zeta functions

We now work with $\mathbb{Q}_p$. We expand the language so that the Γ-sort becomes a model of Presburger arithmetic.

Theorem. 11. *Let $D \subseteq \mathbb{Q}_p^m \times \mathbb{Q}_p$ be a simple subset defined by $\varphi(x,t)$. Consider*

$$Z(0,p) = \int_D |dx|_p \, |dt|_p \, .$$

Then there are simple formulas φ_i($1 \leq i \leq s$) such that for almost all p

$$Z(0,p) = \frac{1}{p} \sum_{i=1}^{s} \sum_{\xi_i \in \overline{\mathbb{Q}}_p^{n_i}} \sum_{l \in \mathbb{Z}} p^{-l} \int_{E_i(\xi_i,l)} |dx|_p \, ,$$

where $E_i(\xi_i,l) \subseteq \mathbb{Q}_p^m$ is the set defined by $\varphi_i(x,\xi_i,l)$.

Lemma. 12. *Let $E \subseteq \mathbb{Z}^{m+1}$ be defined by a formula $\psi(l_1, \ldots, l_m, n)$ that contains only Γ-variables. Suppose*

$$J(s) = \sum_E p^{-ns-l_1-\ldots-l_m}$$

is convergent for $s \in S$, with S an open subset of $\mathbb{R}$. Then there are polynomials $Q, R \in \mathbb{Z}[X, Y]$ such that for almost all P and all $s \in S$

$$J(s) = \frac{Q(p, p^{-s})}{R(p, p^{-s})}.$$

Lemma. 13 (Meuser's Lemma). *Let* $L \subseteq \mathbb{Z}^m$ *be defined by a finite system of linear inequalities in* $(k_1, \ldots, k_m)$ *with coefficients from* $\mathbb{Z}$. *Let* $A_1(X), \ldots, A_m(X) \in \mathbb{Z}[X]$ *be linear. Suppose that*

$$J(s) = \sum_L p^{-\sum_{i=1}^m k_i A_i(s)}$$

is convergent for $s \in S$, *with* S *an open subset of* $\mathbb{R}$. *Then* $J(s)$ *is a rational function of* p^{-s} *on* S.

Theorem. 14. *Let* $h(x)$ *be a definable function and* $D \subseteq \mathbb{Q}_p^m \times \mathbb{Q}_p$ *a definable subset. Then there is a rational function* $Q(T)/R(T)$ *such that for almost all* p

$$Z(s,p) = \int\limits_D |h(\bar{x})|_p^s \, |d\bar{x}|_p = \frac{Q(p^{-s})}{R(p^{-s})}.$$

By Denef's theorem which deals with each p separately, we conclude that $Z(s,p)$ is a rational function for all p and the degrees of numerators and denominators of these rational functions are bounded.