JOHAN PAS

Some applications of uniform p-adic cell decomposition

Astérisque, tome 198-199-200 (1991), p. 265-271
<http://www.numdam.org/item?id=AST_1991__198-199-200__265_0>

SOME APPLICATIONS
OF UNIFORM p-ADIC CELL DECOMPOSITION

JOHAN PAS[1]
K.U. Leuven

In this paper we summarize some applications of uniform p-adic cell decomposition. The technique of p-adic cell decomposition was developed by Denef [**3,4**], using ideas of Cohen [**2**]. Denef gave two applications of his theorem. A first one was an elementary proof of Macintyre's quantifier elimination for p-adic fields; a second one was a proof of the rationality of the Igusa local zeta function without using Hironaka's resolution of singularities.

Denef's cell decomposition theorem holds for every p-adic field but the decomposition procedure depends on the particular field. In [**13**] and [**14**] we obtain cell decomposition theorems which are uniform in a certain class of p-adic fields. In [**13**] we prove a cell decomposition for a class of henselian valued fields of equicharacteristic zero. By the use of an ultraproduct construction, this provides a decomposition which is uniform, for almost all p, in the class $\{\mathbf{Q}_p\}_{p \text{ prime}}$ of all fields of p-adic numbers. The cell decomposition proved in [**14**] is uniform in the class of all finite unramified extensions of the field $\mathbf{Q}_p$ (with p a fixed prime number). Macintyre [**10**] obtained independently a different cell decomposition which is also uniform in these classes of fields.

The basic idea of cell decomposition is that, given a p-adic field K and a polynomial $f(x)$ with $x = (x_1, \ldots, x_m)$, one can partition K^m into

[1] Research Assistant of the National Fund of Scientific Research (Belgium)

so-called cells, such that on each of these cells the function $f(x)$ takes, in a certain sense, a simpler form. The precise meaning of 'simpler' here is determined by the formalism (defined by a first order language for p-adic fields) in which one proves the cell decomposition theorem. The use of uniform cell decomposition allows one to simplify, uniformly, formulas in the first order language and to obtain a quantifier elimination in this language which is uniform in the class of fields. This is formulated more precisely in section 1. A second application of cell decomposition is the computation of certain p-adic integrals on definable sets. Cell decomposition enables one to partition definable sets in simpler parts for which the integral can be computed. The results here are stated in section 2.

Section 1
Quantifier elimination

We define the first order language $\mathcal{L}$, in which we prove the cell decomposition for valued fields of equicharacteristic zero, and in which we obtain quantifier elimination. The language $\mathcal{L}$ is a language with three sorts of variables, namely variables for the elements of the valued field, variables for elements of the residue field and variables for elements of the value group. The language contains symbols for the standard field operations in the valued field and in the residue field, and symbols for the usual operations in the value group. One also has a function symbol for the valuation map from the field to the value group, and another function symbol for an angular component map modulo P from the field to the residue field. Such an angular component map modulo P is a multiplicative morphism from the group of units of the valued field to the group of units of the residue field, such that the restriction of this morphism to the set of elements of valuation zero is the canonical projection onto the residue field.

Cell Decomposition Theorem 3.2 of **[13]** implies

THEOREM. (**[13]** Theorem 4.1) *Let K be a henselian valued field of equicharacteristic zero which has an angular component map modulo P. Then K has elimination of field quantifiers in the language $\mathcal{L}$.*

Applying this to ultraproducts $\prod \mathbf{Q}_p/\mathcal{D}$ where $\mathcal{D}$ is a non-principal ultrafilter on the index set of prime numbers we obtain a uniform quantifier elimination for the fields of p-adic numbers.

COROLLARY. (**[13]** Corollary 4.3) *Let φ be a formula in $\mathcal{L}$. Then there exists an $\mathcal{L}$-formula ψ (which is independent of p) without field quantifiers, such that, for almost all primes p, we have*

$$\varphi \longleftrightarrow \psi \qquad \text{on } \mathbf{Q}_p.$$

Section 2
Poincaré series and Igusa local zeta functions

Let $h(x)$ be a polynomial in m variables $x = (x_1, \ldots, x_m)$ over $\mathbf{Z}$, and let K be a finite field extension of $\mathbf{Q}_p$ for some prime number p, such that K is unramified over $\mathbf{Q}_p$, that is, p is a generator for the maximal ideal of the valuation ring R of K. Suppose that the residue field of K has cardinality q. The valuation on K is denoted by $|.|$ and normalized by $|p| = 1/q$.

For every $n \in \mathbf{N}$ we consider the number of solutions of the congruence $h(x) \equiv 0 \bmod p^n$ in R,

$$N(n, K) = \mathrm{Card}\{\, x \bmod p^n \mid x \in R^m, h(x) \equiv 0 \bmod p^n \,\}.$$

The generating function of this sequence

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

is called a *Poincaré series* associated to the polynomial h. Borevich and Shafarevich [1] conjectured that this series is a rational function of T. This conjecture was first proved by Igusa [8,7] using Hironaka's resolution of singularities.

Another type of Poincaré series for h is the series associated to the p-adic points on the variety $h = 0$. Put for $n \in \mathbf{N}$,

$$\widetilde{N}(n, K) = \mathrm{Card}\{\, x \bmod p^n \mid x \in R^m,\ h(x) = 0\,\},$$

and

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

This series was studied by Oesterlé [12] and Serre [16]. Denef [3] proved that $\widetilde{P}(T, K)$ is a rational function of T.

A first step in the rationality proofs for these Poincaré series, is to relate the series to a certain p-adic integral. For the first series $P(T, K)$ this integral is the so-called *Igusa local zeta function* of h, which is defined as

$$Z(s, K) = \int_{R^m} |h(x)|^s\, |dx| \qquad \text{for } s \in \mathbf{R},\ s > 0, \tag{1}$$

where $|dx|$ is the Haar measure on K^m normalized on R^m. The relation of this integral with the Poincaré series $P(T, K)$ is given by

$$Z(s, K) = \frac{1 + (T-1)\, P(q^{-m}\, T)}{T} \qquad \text{for } T = q^{-s}. \tag{2}$$

For $\widetilde{P}(T, K)$ the corresponding integral is

$$I(s, K) = \int_{D} |w|^s\, |dx|\, |dw| \qquad \text{for } s \in \mathbf{R},\ s > 0,$$

where

$$D = \{\, (x, w) \in R^m \times R \mid \exists\, y \in R^m \,:\, x \equiv y \bmod w \text{ and } h(y) = 0\,\}.$$

Here we have

$$(3) \qquad I(s,K) = \frac{q-1}{q}\widetilde{P}(q^{-(m+1)}T, K) \qquad \text{for } T = q^{-s}.$$

We now want to study the behaviour of these Poincaré series if the field K varies in the class of all fields of p-adic numbers $\{\mathbf{Q}_p\}_{p \text{ prime}}$. By relations (2) and (3) it suffices to study the behaviour of p-adic integrals of the form

$$J(s,K) = \int_W |h(x)|^s \, |dx|,$$

where W is the subset of K^m defined by a formula ψ in the language $\mathcal{L}$.

For this kind of integrals we proved, using the uniform cell decomposition theorem, that if K varies in the class $\{\mathbf{Q}_p\}_{p \text{ prime}}$, the denominator of $J(s,K)$ as a rational function in p^{-s} does not depend on p and the degree of the numerator is bounded independently of p.

THEOREM. ([**13**] Theorem 5.1) *Let $h(x) \in \mathbf{Z}[x]$ with $x = (x_1, \ldots, x_m)$. Let ψ be an $\mathcal{L}$-formula with free field variables $x_1, \ldots, x_m$. Suppose that $W_p = \{ x \in \mathbf{Q}_p^m \mid \psi(x) \text{ holds} \}$ is bounded for all p. Consider*

$$J(s,\mathbf{Q}_p) = \int_{W_p} |h(x)|^s \, |dx|.$$

Then

$$J(s,\mathbf{Q}_p) = \frac{R_p(T)}{Q(p,T)} \qquad \text{with } T = p^{-s},$$

where (i) *the denominator $Q(p,T)$ is a rational function in p and T, which is a product of factors of the form T, p, or $1 - p^a T^b$ $(a, b \in \mathbf{Z})$;*

(ii) *for every p, $R_p(T)$ is a polynomial in T such that $\deg R_p(T)$ is bounded independently of p.*

The same result holds for the Poincaré series $P(T,\mathbf{Q}_p)$ and $\widetilde{P}(T,\mathbf{Q}_p)$ by (2) and (3).

We were not able to obtain more information on how the numerators $R_p(T)$ depend on the prime p. This problem is probably much more difficult since the coefficients of $R_p(T)$ are related to the number of points on a variety over the finite field $\mathbf{F}_p$ (which is the residue field of $\mathbf{Q}_p$).

We now consider the class of all unramified extension of $\mathbf{Q}_p$ with p a fixed prime number. Since for every $d \in \mathbf{N}$, $d > 0$, there is a unique unramified extension K_d of $\mathbf{Q}_p$ of degree d, we can denote this class by $\{K_d\}_{d \in \mathbf{N}, d>0}$. The first order language $\mathcal{L}'$ used in this case is similar to the language $\mathcal{L}$, but here we have to include additional sorts for the residue rings modulo p^n, due to the non-zero characteristic of the residue fields. From Cell Decomposition Theorem 3.2 of **[14]**, which is uniform in the class $\{K_d\}_{d \in \mathbf{N}, d>0}$, we obtain a result for $J(s, K_d)$ ($d \in \mathbf{N}$, $d > 0$) which is similar to the previous theorem for $J(s, \mathbf{Q}_p)$ (p prime). However the residue field of K_d is the field with p^d elements $\mathbf{F}_{p^d}$. Since the variation with d of the number of points on a variety over $\mathbf{F}_{p^d}$ is known by Dwork's theorem **[6]**, we are able to determine more precisely how the numerator of $J(s, K_d)$ depends on d.

THEOREM. (**[15]** Theorem 2.3) *Let $h(x) \in \mathbf{Z}[x]$ with $x = (x_1, \ldots, x_m)$. Let ψ be an $\mathcal{L}'$-formula with free field variables $x_1, \ldots, x_m$. Suppose that $W_d = \{\, x \in K_d^m \mid \psi(x) \text{ holds } \}$ is bounded for all d. Consider*

$$J(s, K_d) = \int\limits_{W_d} |h(x)|^s \, |dx|.$$

Then there exist a positive integer d_0, complex numbers $\lambda_1, \ldots, \lambda_t$ and polynomials G, $H \in \mathbf{Z}[T, X_1, \ldots, X_t]$ such that, for $d \geq d_0$,

$$J(s, K_d) = \frac{G(T, p^{d\lambda_1}, \ldots, p^{d\lambda_t})}{H(T, p^{d\lambda_1}, \ldots, p^{d\lambda_t})}, \qquad \text{with } T = p^{-ds}.$$

Meuser **[11]** calls such a function an *invariant function* of the sequence $\{K_d\}_{d \in \mathbf{N}, d>0}$. She proved the above theorem for the Igusa local zeta function (see display (1)). In this case $d_0 = 1$.

References

1. S.E. Borevich, I.R. Shafarevich, "Zahlentheorie," Birkhäuser, Basel–Stuttgart, 1966.
2. P.J. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. **22** (1969), 131–151.
3. J. Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety*, Invent. Math. **77** (1984), 1–23.
4. ———, *p-adic semi-algebraic sets and cell decomposition*, J. Reine Angew. Math. **369** (1986), 154–166.
5. ———, *On the degree of Igusa's local zeta function*, Amer. J. Math. **109** (1987), 991-1008.
6. B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.
7. J.-I. Igusa, *Complex powers and asymptotic expansions I*, J. Reine Angew. Math. **268/269** (1974), 110–130; *II*, ibid. **278/279** (1975), 307–321.
8. ———, *Some observations on higher degree characters*, Amer. J. Math. **99** (1977), 393–417.
9. A. Macintyre, *On definable subsets of p-adic fields*, J. Symbolic Logic **41** (1976), 605–610.
10. ———, *Rationality of p-adic Poincaré series : uniformity in p*, Ann. Pure Appl. Logic (to appear).
11. D. Meuser, *The meromorphic continuation of a zeta function of Weil and Igusa type*, Invent. Math. **85** (1986), 493–514.
12. J. Oesterlé, *Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbf{Z}_p^N$*, Invent. Math. **66** (1982), 325–341.
13. J. Pas, *Uniform p-adic cell decomposition and local zeta functions*, J. Reine Angew. Math. **399** (1989), 137–172.
14. ———, *Cell decomposition and local zeta functions in a tower of unramified extensions of a p-adic field*, Proc. London Math. Soc. **60** (1990).
15. ———, *Igusa local zeta functions and Meuser's invariant functions*, preprint.
16. J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES **54** (1981), 123–202.

1980 *Mathematics subject classifications*: 03C10, 11S40, 11U09

Wiskundig Instituut
Katholieke Universiteit Leuven
Celestijnenlaan 200-B
3030 Heverlee
BELGIUM

e-mail : fgaba03 at blekul11.bitnet