Counting points using uniform p-adic integration

Immi Halupczok

University of Leeds

20th March 2016

Goal/motivation

- ▷ Fix a variety V given by polynomials $f_1, \dots, f_\ell \in \mathbb{Z}[\underline{x}]$ $\quad (\underline{x} := (x_1, \dots, x_n))$
- ▷ For p prime and $r \in \mathbb{N}$:
  $N_{p^r} := \#V(\mathbb{Z}/p^r\mathbb{Z}) = \#\{\underline{x} \in (\mathbb{Z}/p^r\mathbb{Z})^n \mid f_1(\underline{x}) = \cdots = f_\ell(\underline{x}) = 0\}$
- ▷ The **Poincaré series** is: $\quad P_{V,p}(Z) := \sum_{r=0}^{\infty} N_{p^r} Z^r \quad \in \mathbb{Z}[[Z]]$

Theorem (Denef, Igusa, Meuser; 80s)

$P_{V,p}(Z) \in \mathbb{Q}(Z)$

Theorem (Denef, Loeser, Macintyre, Pas; later)

"Uniformity in p": For $P_{V,p}(Z) = \frac{g_p(Z)}{h_p(Z)}$:
- ▷ *degree of $g_p(Z)$, $h_p(Z)$ bounded*
- ▷ *description of how the coefficients of g_p and h_p can depend on p*

This talk: a proof of this using uniform p-adic integration ($\approx$ motivic integration)

Expressing things using the p-adic measure

- (Recall: variety V fixed)
- $N_{p^r} = \#V(\mathbb{Z}/p^r\mathbb{Z}) = \#V(\mathbb{Z}_p/p^r\mathbb{Z}_p)$
- $X_r := \{\underline{x} \in \mathbb{Z}_p^n \mid v(\underline{f}(\underline{x})) \geq r\}$ is a union of translates of $B_r := (p^r\mathbb{Z}_p)^n$
- N_{p^r} = number of translates of B_r covering X_r
  $= \mu(X_r)/\underbrace{\mu(B_r)}_{=p^{-n\cdot r}}$ (μ: induced by Haar measure on $\mathbb{Q}_p$ with $\mu(\mathbb{Z}_p) = 1$)
- Thus: Goal: understand $r \mapsto \mu(X_r)$
- A variant:
  - $\tilde{N}_{p^r}$ = number of points of $V(\mathbb{Z}_p/p^r\mathbb{Z}_p)$ that lift to $V(\mathbb{Z}_p)$
    = number translates of B_r needed to cover $V(\mathbb{Z}_p)$
    $= \mu(\tilde{X}_r)/\mu(B_r)$ where $\tilde{X}_r = \{\underline{x} + \underline{x}' \mid \underline{x} \in V(\mathbb{Z}_p), \underline{x}' \in B_r\}$
- The following includes both versions and much more:

Theorem

Suppose X_r is a definable family of subsets of $\mathbb{Q}_p^n$, parametrized by $r \in \mathbb{N}$.

Then $\sum_{r=0}^{\infty} \mu(X_r) Z^r \in \mathbb{Q}(Z)$.

Need to define "definable family"...

The Denef–Pas language

A **definable set** is a set given by a Denef–Pas formula.

A **definable family of sets** is a family of sets given by a Denef–Pas formula.

Example: $\tilde{X}_r = \{\underline{x} + \underline{x}' \mid \underline{x} \in V(\mathbb{Z}_p), \underline{x}' \in B_r\}$

$\quad = \{\underline{\tilde{x}} \in \mathbb{Q}_p^n \mid \phi(\underline{\tilde{x}}, r) \text{ holds}\}$, where

$$\phi(\underline{\tilde{x}}, r) = \underbrace{\exists \underline{x}\colon \big(f_1(\underline{x})=0 \wedge \cdots \wedge f_\ell(\underline{x})=0 \wedge v(x_1-\tilde{x}_1)\geq r \wedge \cdots \wedge v(x_n-\tilde{x}_n)\geq r\big)}_{\text{Denef–Pas formula}}$$

A **Denef–Pas formula** is a mathematical expression built as follows:

- ▷ three sorts of variables: valued field vars, residue field vars, value group vars
- ▷ build terms:
  - ▷ in the valued field and the residue field: use $+$, $-$, $\cdot$ and constants from $\mathbb{Z}$
  - ▷ in the value group: use $+$, $-$, 0
  - ▷ v: valued field $\to$ value group,
    ac: valued field $\to$ residue field (ac = angular component map)
- ▷ build equations $(t_1 = t_2)$ and, in the value group, inequations $(t_1 > t_2)$
- ▷ apply boolean combinations and quantifiers $\forall$, $\exists$

Note: Formulas work uniformly in p

A **definable function** is a function whose graph is a definable set.

Uniform p-adic integration

- Introduce "motivic functions": expressions for functions $X \to \mathbb{R}$, where X is a definable set.
- **Uniform p-adic integration** = symbolic integration of such expressions
- Example: $X = \{(x, r) \in \mathbb{Q}_p \times \mathbb{Z} \mid \underbrace{0 \le v(x) < r}_{\text{Denef–Pas formula}}\}$, $f(x, r) = \underbrace{p^{v(x)}}_{\text{motivic function}}$

  $$\Rightarrow \quad g(r) := \int_{X_r} f(x, r)\, dx = \underbrace{\tfrac{p-1}{p} \cdot r}_{\text{motivic function}}$$

- A **motivic functions** is a linear combination of products of:
  - $\underline{x} \mapsto \mathbf{1}_Z(\underline{x})$ for a definable set Z
  - $\underline{x} \mapsto p^{f(\underline{x})}$ for f a definable function into the value group
  - $\underline{x} \mapsto f(\underline{x})$ for f a definable function into the value group
  - A few others...
- Note: p is also a symbol, so this integration indeed treats all $\mathbb{Q}_p$ uniformly...
  ...but – in some versions – only for p sufficiently big
- A key ingredient to make such symbolic integration possible:
  "Cell decomposition": a precise description of definable subsets of $\mathbb{Q}_p$
- Note: The same symbolic integration applied in other valued fields yields motivic integration

Application to our goal

- Recall:
  Given a definable family of sets $X_r \subseteq \mathbb{Q}_p^n$, parametrized by $r \in \mathbb{N}$, understand $r \mapsto \mu(X_r)$.
- $\mu(X_r) = \int_{X_r} 1 d\underline{x}$, so $\mu(X_r) = f(r)$ for some motivic function f.
- We now need to prove: For motivic $f : \mathbb{N} \to \mathbb{R}$, we have $\sum_r f(r) Z^r \in \mathbb{Q}(Z)$
- This is rather easy, using:
  - motivic functions on $\mathbb{Z}$ are given in terms of definable functions $\mathbb{Z} \to \mathbb{Z}$
  - definable functions $\mathbb{Z} \to \mathbb{Z}$ are well understood (cf. Presburger arithmetic)

Thanks for your attention.