Definable Sets, Euler Products of p-adic Integrals, and Zeta Functions

Jamshid Derakhshan
St. Hilda's College, University of Oxford

Model Theory, Bedlewo, 07/07/2017

1. Introduction

Let $\phi(\bar{x})$ be a ring formula and $f(\bar{x})$ a definable function (over $\mathbb{Q}$). Given a p-adic field $\mathbb{Q}_p$, we consider integrals of the form

$$Z(s,p) := \int_{\phi(\mathbb{Q}_p)} |f(\bar{x})|^s dx$$

where $\phi(\mathbb{Q}_p)$ denotes the set of realizations of $\phi(\bar{x})$ in $\mathbb{Q}_p^n$, and dx an normalized additive Haar measure on $\mathbb{Q}_p^n$.

In this talk, for simplicity, we shall refer to these as "definable integrals".

In 1984, Denef proved that such definable integrals are rational functions in p^{-s}, thereby establishing a conjecture of J-P Serre on rationality of p-adic Poincare series counting p-adic points on a variety. The question was as follows.

Let $f_1(x).....f_r(x)$ be polynomials in m variables $x = (x_1, \dots, x_m)$ over $\mathbb{Z}_p$. For $n \in \mathbb{N}$, let M_n be the number of elements in the set

$$\{x \ mod \ p^n : x \in \mathbb{Z}_p^m, f(x) = 0 \ mod \ p^n, i = 1.....r\}$$

and let N_n be the number of elements in the set

$$\{x \ mod \ p^n : x \in \mathbb{Z}_p^m, f(x) = 0, i = 1.....r\}.$$

To these data one can associate the following Poincare series

$$\sum_n M_n T^n$$

and

$$P(T) := \sum_n N_n T^n$$

Borevich and Shafarevich conjectured the first series is a rational function of T. This was proved by Igusa. Serre conjectured the second series is rational, which was proved by Denef.

Denef's proof proceeds via proving that $(p-1)/pP(p^{-m-s-1})$ can be written as a definable integral for certain formulas.

Subsequently Denef, Macintyre and Pas proved that there are uniformities in the shape of these rational functions. Denef and Loeser and later Cluckers-Loeser extened such uniformities to a theory of motivic integration. Hrushovski and Kazhdan gave another approach to motivic integration with new applications.

These uniformities or motivic behaviour hinted at existence of some global well behaved versions of the local definable integrals. Global means that it should be related to properties over a global field or count objects in the global field. I will be concerned with number fields and not function fields although I believe there are appropriate versions of my results for functions fields. One thus hoped that there are number-theoretic objects for which these integrals are local components. Such a number theoretic object must satisfy appropriate global arithmetical conditions.

The global object turns out to be precisely Euler products over primes p of the above definable integrals. These have the form

$$Z(s) := \prod_p Z(s,p).$$

It turns out that these Euler products are particularly well-behaved and have good analytic properties. Among the most important analytic properties of such Euler products are convergence and meromorphic continuation to a domain larger than its domain of convergence beyond the first pole. If one can prove these properties, then by remarkable works of Tauber, Hardy-Littelwood, Ikehara and Weiner (results under the name of Tauberian theorems), one deduces arithmetical information on coefficients of the Dirichlet series $\sum_n a_n n^{-s}$ representing these Euler products. We shall prove such properties for Euler products of definable integrals.

Let $D(s) := \sum_{n\geq 1} a_n n^{-s}$ be a Dirichlet series. Assume that $D(s)$ converges for some s. Then the smallest real number σ_0 such that $D(s)$ converges in the half plane $Re(s) > \sigma_0$ is called the abscissa of convergence of $D(s)$. The series converges to the right of σ_0 and not at any point to the left of it.

Theorem 1.1. *Let $\varphi(\bar{x})$ be a formula of the language of rings and let $f(\bar{x})$ be a definable function in the language of rings. Let $Z(s,p) := \int_{\varphi(\mathbb{Q}_p)} |f(\bar{x})|^s dx$ and let*

$$Z(s) := \prod_p Z(s,p).$$

Then the Euler product $Z(s)$ has rational abscissa of convergence $\alpha \in \mathbb{Q}$ and $Z(s)$ admits meromorphic continuation to the half-pane $\{s : Re(s) > \alpha - \delta\}$ for some $\delta > 0$. The extended function has no pole on the line $\{s : Re(s) = \alpha\}$ except for a pole at α.

Using Tauberian theorems we deduce

Corollary 1.2. *Let $\sum_n a_n n^{-s} = Z(s)$. Then for any N we have*

$$a_1 + \cdots + a_N \sim cN^{\alpha}(logN)^{w-1}$$

where $c \in \mathbb{R}$ is a constant and w is the order of the pole of $Z(s)$ at α.

Some applications

The *Riemann zeta function* $\sum_{n\geq 1} n^{-s}$ has an Euler product factorization as $\prod_p (1-p^{-s})^{-1}$ (proved by Euler in somewhat more general form).

Let G be a finitely generated nilpotent group. A non-commutative generalizations of the Riemann zeta function defined by Grunewald-Segal-Smith is $\sum_n a_n(G)n^{-s}$, where $a_n(G)$ denotes the number of index n subgroups of G. This is called the subgroup growth zeta function of G.

It was proved by Grunewald-Segal-Smith that this series admits an Euler product factorization as

$$\prod_p (\sum_{n\geq 0} a_{p^n}(G)p^{-ns}).$$

du Sautoy and Grunewald proved that the subgroup growth zeta function has meromorphic continuation beyond its rational abscissa of convergence. Grunewald-Segal-Smith also defined the pro-isomorphic zeta function as $\sum_n a_n n^{-s}$ where a_n denotes the number of index n subgroups H of G whose profinite completion is isomorphic to the profinite completion of G.

Corollary 1.3. *The pro-isomorphic zeta function has meromorphic continuation beyond its rational abscissa of convergence.*

Let G be an algebraic group defined over $\mathbb{Q}$. The conjugacy class zeta function of an algebraic group G over $\mathbb{Q}$ is defined by Uri Onn as $\sum_{n\geq 1} a_n n^{-s}$ where a_n denotes the number of conjugacy classes of the finite group $G(\mathbb{Z}/n\mathbb{Z})$. The following settles a question of Onn.

Corollary 1.4. *The global conjugacy class zeta function of an algebraic group G with strong approximation has meromorphic continuation beyond its rational abscissa of convergence.*

Proof. (for the case of SL_2) By Chinese remainder theorem and using that SL_2 is generated by elementary matrices we have $SL_2(\mathbb{Z}/m\mathbb{Z}) \cong SL_2(\mathbb{Z}/p_1^{k_1}) \times \cdots \times SL_2(\mathbb{Z}/p^{k_r}\mathbb{Z})$ where $m = p_1^{k_1} \dots p_r^{k_r}$. So the class numbers are multiplicative and we have $\sum_n a_n n^{-s} = \prod_p (1-a_p p^{-s})^{-1}$ and $(1-a_p p^{-s})^{-1} = 1 + a_p p^s + a_{p^2} p^{-2s} + \dots$ This is a local conjugacy class zeta function

$$\sum_n c_n p^{-ns} = \int_{X(\mathbb{Q}_p)} |f(\bar{x})|^s dx$$

by work of Berman-Derakhshan-Onn-Paajanen (JLMS 2013), where $c_n = card(G(\mathbb{Z}_p/p^n\mathbb{Z}_p)$ and X and f are definable. □

Given an group G that is representation rigid, let a_n be the number of complex irreducible representations of Γ of dimension n. Arithmetic groups with congruence subgroup property are representation rigid. If G is a f.g. nilpotent group one has only finitely many iso-twist classes of representations of each degree and one lets a_n denote that number. In any case one has representation growth zeta functions $\sum_n a_n n^{-s}$. Avni studies these in the arithmetic case and proves Euler product factorizations. In the nilpotent case, these were studies by Lubotzky-Martin and Hrushovski-Martin-Rideau who proved Euler product factorizations into definable integrals.

Corollary 1.5. *The iso-twist representation zeta function of a f.g. nilpotent group has meromorphic continuation beyond its rational abscissa of convergence.*

This has been proved by Voll-Dong using algebra and combinatorics of the Weyl groups.

In each case, we can deduce an asymptotic formula of the form

$$a_1 + \cdots + a_N \sim cN^{\alpha}(logN)^{w-1}$$

for each of the zeta functions.

Given an elliptic curve E over $\mathbb{Q}$, the L-function is defined as the Euler product

$$L(E,s) = \prod_p \frac{1}{1 - a_p p^{-s} + \chi(p)p^{1-2s}}$$

where $a_p = p + 1 - |E(\mathbb{F}_p)|$ and $\chi(p) = 1$ if p is a prime of good reduction and $\chi(p) = 0$ otherwise.

Faltings proved that given two elliptic curves E_1 and E_2 over $\mathbb{Q}$, $L(E_1, s) = L(E_2, s)$ iff E_1 and E_2 are isogenous. By Hasse's bounds for a_p, $L(E.s)$ converges for $Re(s) > 3/2$. Wiles's modularity theorem states that $L(E, s)$ has analytic continuation to the whole complex plane into a holomorphic function (with a functional equation). The Birch-Swinnerton Dyer conjecture states that the order of vanishing of $L(E, s)$ equals the rank of the Mordell-Weil group $E(\mathbb{Q})$. It is interesting that if we define the Dirichlet series

$$D(E,s) = \sum_{n \geq 1} c_n n^{-s}$$

where $c_n = |E(\mathbb{Z}/n\mathbb{Z})|$, then $D(s)$ has some Euler product factorization and its meromorphic continuation seems to be related to the zeros of $L(E, s)$.

We remark that unlike the Riemann zeta function or the L-function of an algebraic variety, the growth zeta functions do not always have meromorphic continuation to the entire complex plane (by work of du Sautoy).

A major theme in arithmetic geometry is to understand the rational points on an algebraic variety V defined over a number field. Geometry governs arithmetic. Faltings.

Manin conjectured that for a Fano variety (anti-canonical class is ample), after passing to a finite field extension the number $N(V, L, T)$ of rational points of height at most T satisfies

$$N(V(K), L, T) \sim cT^a(logT)^b$$

where height function is defined on $\mathbb{P}^n(\mathbb{Q})$ by

$$H(x_0 : \cdots : x_n) = max\{|y_0|, \ldots, |y_n|\}$$

where $(y_0, \ldots, y_n)$ is a primitive integral vector representing the $(x_0 : \cdots : x_n)$. We have $H(x) = \prod_v max\{|x_0|_v, \ldots, |x_n|_v\}$ which is finite and also it is well defined by the product formula. Now a height function on V is pull back of a height function of $\mathbb{P}^n$ using a projective embedding or an ample line bundle L (by Weil's height machine).

There has been many results on this conjecture by Chambert-Loir, Tschinkel, Gorodnik, Oh, Sarnak, Rudnick ...

Integration of height zeta function over a definable set and the above Theorem yield new results on Manin conjecture together with equidistribution of rational points. For this one works on the ring of adeles $\mathbb{A}_K$. Integrals over adeles decompose as Euler products of p-adic integrals.

2. Some of the main ingredients in the proof:

. Suitable uniform elimination of quantifiers for almost all $\mathbb{Q}_p$. For example in Denef-Pas language with 3 sorts for the valued field, the value group, and residue field equipped with language of rings, ordered abelian groups and rings resp; and with valuation and ac-map mod p: $(ac(x) = res(xx^{-v(x)})$ if x is non-zero and zero otherwise) connecting the sorts. This together with Hironaka's embedded resolution of singularities (in char 0) implies that each local integral has the form of a finite sum of the form

$$Z(s,p) = \sum_i p^{-m} card(\psi_i(\mathbb{F}_p)) \prod_j p^{-d(A_j s + B_j)}/(1 - p^{-h(A_j s + B_j)})$$

where $h, d \in \mathbb{Z}$ and $A_j, B_j \in \mathbb{N}$, and ψ_i is a ring formula.

.Work of Chatzidakis-van den Dries-Macintyre stating the following:

1. Let $\phi(x_1, \ldots, x_n)$ be a formula of the ring language. Then there is a constant c and a finite set of pairs (d, μ), with $d \in \{0, \ldots, n\}$ and μ a positive rational number such that for each finite field $k := \mathbb{F}_q$ such that $\phi(\mathbb{F}_q)$ is non-empty, we have the inequality

$$|card(\phi(k^n)) - \mu q^d| \leq c q^{d-1/2}$$

2. Given (d, μ) there is sentence of the ring language $\phi_{(d,\mu)}$ such that for evey finite field k, $k \models \phi_{(d,\mu)}$ iff the above inequality holds with k.

3. Given a pseudo-finite field F, and a definable subset $S \subseteq F^n$, S is a finite union of sets of the form $\pi(V(F)$ where V is an F-algebraic subset of $(F^{alg})^{n+m}$ and π is projection onto the first n-coordinates. (note that $V(F)$ denotes $F^{m+n} \cap V$.)

We then expand each rational function $Z(s,p)$ into a power series in p^{-s} and let $a_{p,0}$ denote the constant coefficient of this power series. Using 1) above we can prove

Proposition 2.1. *There is a constant C such that for almost all p we have $1 \leq a_{p,0}^{-1} \leq Cp^{-1/2}$.*

This means that we can divide by $a_{p,0}$ in the Euler product. The Euler product of $a_{p,0}^{-1}Z(s,p)$ over a cofinite set of primes has the form

$$\prod_{p\notin Q}(1+\sum_i card(\psi_i(\mathbb{F}_p)\prod_j p^{-d(A_js+B_j)}/(1-p^{-h(A_js+B_j)}))$$

Here Q is a finite set of primes p such that $a_{p,0}=0$ and an embedded resolution of a certain hypersurface constructed from the conditions in the uniform quantifier elimination has bad reduction modulo p. The primes in Q give finitely many rational functions.

We restrict attention to the Euler product over primes outside Q. This later needs that the numerical data of resolution of the base change from $\mathbb{Q}$ to $\mathbb{Q}_p$ remains the same.

Now we need to analyse the numbers of points of ψ_i in $\mathbb{F}_p$.

We have F-algebraic sets V projecting to the definable sets. Sizes of fibres are bounded (algebraic boundedness of pseudo-finite fields). We consider these as smooth quasi-projective varieties over $\mathbb{Q}$.

Consider each irreducible component, say V of dim d. Decompose it into its absolutely irreducible components $V_1,\dots,V_n$. The Galois group $Gal(\mathbb{Q}^{alg}/\mathbb{Q})$ acts transitively on these.

Since the action is transitive all the V_i also have dimension d. Let $U\subseteq G$ be the kernel of this action and put $L=(\mathbb{Q}^{alg})^U$. Then L is a finite Galois extension of $\mathbb{Q}$ with Galois group $\mathcal{G}=Gal/U$ and every V_i (i = 1,... , n) is defined over L.

We take a cofinite set of of primes where the reduction V mod p is smooth and p is unramified in L (so we have a Frobenius conjugacy class $Frob_p$ in $Gal(L/Q)$).

For a smooth quasi-projective irreducible V over $\mathbb{Q}$ we define

$l_p(V)$ to be the number of irreducible components defined over $\mathbb{F}_p$ of $\bar{V}$, the reduction mod p of V, which are absolutely irreducible. Define

$$f(s)=\prod_p(1-l_p(V)p^{-s})$$

It follows that the abscissa of convergence of $f(s)$ is 1 and there is a $\delta>0$ such that $f(s)$ has a meromorphic continuation to $Re(s)>1-\delta$. This uses that

$$\prod_p det(1-\rho(Frob_p)p^{-s})$$

is (up to finitely many factors) the Artin L-function of the Galois representation coming from the permutation representation of $\mathcal{G}$.

(which has abscissa of convergence 1 and also has a meromorphic continuation to all of $\mathbb{C}$) and that

$$det(1-\rho(Frob_p)p^{-s})=1-l_p(V)+...$$

For each of the varieties V we have by Lang-Weil

$$|card(\bar{V}(\mathbb{F}_p))-l_p(V)p^d|<cp^{d-l/2}$$

and $l_p(X)>0$ for a dense set of primes p.

This gives by algebraic boundedness of pseudo-finite fields

$$|card(\psi_i(\mathbb{F}_p)) - \mu l_p(V_i)p^d| < cp^{d-l/2}$$

where we decompose the Euler product into finitely many sets of positive density of Chebotarev type corresponding to each pair (d, μ).

This way the meromorphic continuation of $f(s)$ beyond 1 implies the meromorphic continuation of our Euler product beyond its abscissa of convergence.