ELECTRONIC RESEARCH ANNOUNCEMENTS
OF THE AMERICAN MATHEMATICAL SOCIETY
Volume 5, Pages 112–122 (August 30, 1999)
S 1079-6762(99)00069-4

ZETA FUNCTIONS AND COUNTING FINITE p-GROUPS

MARCUS DU SAUTOY

(Communicated by Efim Zelmanov)

ABSTRACT. We announce proofs of a number of theorems concerning finite p-groups and nilpotent groups. These include: (1) the number of p-groups of class c on d generators of order p^n satisfies a linear recurrence relation in n; (2) for fixed n the number of p-groups of order p^n as one varies p is given by counting points on certain varieties mod p; (3) an asymptotic formula for the number of finite nilpotent groups of order n; (4) the periodicity of trees associated to finite p-groups of a fixed coclass (Conjecture P of Newman and O'Brien). The second result offers a new approach to Higman's PORC conjecture. The results are established using zeta functions associated to infinite groups and the concept of definable p-adic integrals.

1. INTRODUCTION

The classification of finite simple groups, the group theorist's Periodic table, provides us with the building blocks from which all finite groups are made. However, even if we take the simplest of the simple groups C_p, a cyclic group of order a prime p, we are very far from a classification of the groups that can be constructed from this single building block. Indeed the groups of order a power of p were generally considered too wild a category of groups to hope for any complete classification.

However, there have been two approaches to getting a hold on this wild class of groups. This paper contributes to the taming of this class of finite p-groups by announcing smooth behaviours that can be established in both these approaches.

The first approach is to ask whether, if we cannot list the p-groups of order a prime power, we can at least count how many groups of order p^n there are.

Define

$$f(n,p) = \text{the number of groups of order } p^n$$

and for $c, d \in \mathbb{N}$ define a more refined counting function $f(n,p,c,d)$ to be the number of groups of order p^n, of class at most c, generated by at most d generators.

Higman and Sims (see [12] and [17]) gave an asymptotic formula for the behaviour of $f(n,p)$ as n grows:

$$f(n,p) = p^{(2/27+o(1))n^3} \text{ as } n \to \infty.$$

Higman also conjectured in [13] that if you fix n and vary p, then $f(n,p)$ is given by a polynomial in p which depends only on the residue class of p modulo some

Received by the editors April 19, 1999.
1991 *Mathematics Subject Classification.* Primary 20D15, 11M41; Secondary 03C10, 14E15, 11M45.

fixed integer N. For example, $f(6,p)$ is described by a quadratic polynomial whose coefficients depend on the residue of p modulo 60. Higman's PORC conjecture, as this has become known, has withstood any attack since Higman's contribution in [13] nearly 40 years ago.

The theme of this paper is to show how zeta functions of groups can be used to count p-groups and in particular offer some new ideas to approach Higman's PORC conjecture.

Define

$$\zeta_{c,d,p}(s) = \sum_{n=0}^{\infty} f(n,p,c,d)p^{-ns}. \tag{1}$$

We announce the proof of the following smooth behaviour of the counting function $f(n,p,c,d)$:

Theorem 1.1. *The function $\zeta_{c,d,p}(s)$ is a rational function in p^{-s}. Hence the function $f(n,p,c,d)$ satisfies a linear recurrence relation with constant coefficients when we fix p, c and d and vary n.*

This is actually a generalization of the following very classical formula counting finite abelian p-groups of rank d:

$$\zeta_{1,d,p}(s) = \zeta_p(s)\zeta_p(2s)\cdots\zeta_p(ds), \tag{2}$$

where $\zeta_p(s) = (1-p^{-s})^{-1}$, the local Riemann zeta function. The idea of the proof of Theorem 1.1, which uses Denef's work on definable integrals, will be explained in section 2. We shall explain in section 3 an Euler product that can be formed, which allows one to count nilpotent groups. We can then apply some recent results with Fritz Grunewald [8] on asymptotics of zeta functions formed as Euler products of definable integrals to prove the following asymptotic behaviour of the function counting finite nilpotent groups:

Theorem 1.2. *For integers n, c, d define $g(n,c,d)$ to be the number of nilpotent groups of order n, of class at most c, generated by at most d elements. Then there exist a rational number $\alpha \in \mathbb{Q}$, an integer $\beta \geq 0$ and $\gamma \in \mathbb{R}$ such that*

$$g(1,c,d) + \cdots + g(n,c,d) \sim \gamma \cdot n^{\alpha} (\log n)^{\beta}.$$

The analysis of [8] also implies the following behaviour for the original function $f(n,p)$:

Theorem 1.3. *For each n there exist finitely many subvarieties E_i $(i \in T)$ of a variety Y defined over $\mathbb{Q}$ and for each $I \subset T$ a polynomial $H_I(X)$ such that for almost all primes p,*

$$f(n,p) = \sum_{I \subset T} c_{p,I} H_I(p),$$

where

$$c_{p,I} = \mathrm{card}\{a \in \overline{Y}(\mathbb{F}_p) : a \in \overline{E_i}(\mathbb{F}_p) \text{ if and only if } i \in I\}.$$

Here $\overline{Y}$ means reduction of the variety $\bmod p$ *which is defined for almost all p.*

So counting p-groups is given by counting points on varieties $\bmod p$. This reduces Higman's PORC conjecture to showing that the number of points $\bmod p$ on Boolean combinations of the varieties E_i varies smoothly with p. The varieties E_i

are canonically associated to the free nilpotent group $F_{n-1,n}$ of class $n-1$ on n generators and arise from the resolution of singularities of a polynomial defined from the structure constants of the associated free nilpotent Lie algebra and its associated automorphism group.

The second approach to understanding p-groups is more structural and involves defining an invariant called the coclass of a p-group. A group of order p^n of class c is said to have *coclass* $r = n - c$. The concept of coclass was first introduced by Leedham-Green and Newman in the 80's when they made some very insightful conjectures (Conjectures A–E) on the structure of p-groups of a fixed coclass. These conjectures have now been confirmed and we shall explain the strongest of these in section 5.

Since then a new set of conjectures (Conjectures P–S) has been proposed by Newman and O'Brien [15] concerning the structure of a directed graph $\mathcal{G}_{r,p}$ that can be associated to p-groups of coclass r. Each such group defines a node in the graph, and directed edges join two groups $P_1 \to P_2$ if there exists an exact sequence

$$1 \to C_p \to P_1 \to P_2 \to 1.$$

The graph $\mathcal{G}_{r,p}$ consists of finitely many trees $\mathcal{F}_{r,p,1}, \ldots, \mathcal{F}_{r,p,k}$ such that the complement of the union of these trees is finite. Each tree has a single infinite chain. For each $N \in \mathbb{N}$ let $\mathcal{F}_{r,p,i}(N)$ denote the tree consisting of the infinite chain and paths of length at most N from the infinite chain. So, in horticultural terms, $\mathcal{F}_{r,p,i}(N)$ is the tree $\mathcal{F}_{r,p,i}$ 'pruned' so that twigs have length at most N. We wish to announce a proof of the qualitative part of Conjecture P which concerns the periodicity of these trees:

Theorem 1.4. *The trees $\mathcal{F}_{r,p,i}(N)$ are ultimately periodic.*

For $p = 2$, note that there exists some N such that $\mathcal{F}_{r,2,i}(N) = \mathcal{F}_{r,2,i}$, i.e. the twig lengths are bounded.

Essential use is made, as we shall explain, of zeta functions which count the number of vertices in these trees. We use the flexibility of the concept of definable p-adic integrals as developed by Denef to prove the rationality of these zeta functions.

The proofs of results in sections 2–4 can be found in [7]. The proofs of results in section 5 can be found in [6].

2. Counting p-groups

The key to understanding the zeta function (1) defined in the introduction is another zeta function first introduced in [11] to understand another unclassifiable class of groups: finitely generated nilpotent groups. Let G be any finitely generated group and define

$$\begin{aligned} \zeta_G^{\triangleleft}(s) &= \sum_{N \triangleleft G} |G : N|^{-s} \\ &= \sum_{n=1}^{\infty} a_n^{\triangleleft}(G) n^{-s}. \end{aligned} \tag{3}$$

This may be regarded as a noncommutative version of the Dedekind zeta function of a number field. The coefficients $a_n^{\triangleleft}(G)$ denote the number of normal subgroups of index n in G and are finite whenever G is finitely generated either as an abstract group or topologically. One can also define the zeta function counting all subgroups of finite index, but it is this normal zeta function which will be relevant to counting p-groups.

When G is a nilpotent group, this zeta function has a natural Euler product decomposition into a product of local factors (see [11]):

$$(4) \qquad \begin{aligned} \zeta^{\triangleleft}_{G}(s) &= \prod_{p \text{ prime}} \zeta^{\triangleleft}_{G,p}(s), \quad \text{where} \\ \zeta^{\triangleleft}_{G,p}(s) &= \sum_{n=0}^{\infty} a^{\triangleleft}_{p^n}(G) p^{-ns}. \end{aligned}$$

Note that $\zeta^{\triangleleft}_{G,p}(s) = \zeta^{\triangleleft}_{\widehat{G}_p}(s)$ where $\widehat{G}_p$ denotes the pro-p completion of G. The first chapter in the theory of zeta functions of groups concerned the rationality of these local factors. In [11] this rationality is established for torsion-free nilpotent groups and generalized in [5] to pro-p groups which are p-adic analytic. For example, when $G = \mathbb{Z}_p^d$, the free abelian pro-p group of rank d, the zeta function has the following form:

$$\zeta^{\triangleleft}_{G}(s) = \zeta_p(s)\zeta_p(s-1)\cdots\zeta_p(s-d+1).$$

It is instructive to compare this with the formula (2) for the zeta function counting finite abelian p-groups of rank d. There is of course some relation between these two zeta functions. Each finite abelian p-group of rank d is a finite image of the free abelian pro-p group $\mathbb{Z}_p^d$, and vice-versa. The crucial point though is that $\zeta^{\triangleleft}_{\mathbb{Z}_p^d}(s)$ overcounts the finite abelian p-groups since each finite abelian p-group occurs in many ways as a quotient of $\mathbb{Z}_p^d$ by a normal subgroup. We shall show how we can refine the zeta function (3) to take account of this overcounting.

There is nothing special of course about being abelian in this connection between finite abelian p-groups and finite images of a free abelian pro-p group. Let $F_{c,d}$ be the free nilpotent group of class c on d generators. Then the finite p-groups of class at most c generated by d elements are precisely the finite images of the pro-p completion $\widehat{(F_{c,d})}_p$ of $F_{c,d}$.

The way to overcome the overcounting is to use the automorphism group $\mathfrak{G}_p = \mathrm{Aut}\widehat{(F_{c,d})}_p$. A pro-$p$ group G which is free in some variety has the property that an isomorphism of two finite quotients $G/N_1 \xrightarrow{\cong} G/N_2$ lifts to an automorphism of G. Applying this to the free nilpotent pro-p group $\widehat{(F_{c,d})}_p$ yields a one to one correspondence between isomorphism types of finite quotients of order p^n and normal subgroups of index p^n equivalent up to the action of the automorphism group $\mathfrak{G}_p$. We therefore have the following identity of zeta functions:

Proposition 2.1.

$$\zeta_{c,d,p}(s) = \sum_{N \triangleleft \widehat{(F_{c,d})}_p} |\widehat{(F_{c,d})}_p : N|^{-s} |\mathfrak{G}_p : \mathrm{Stab}_{\mathfrak{G}_p}(N)|^{-1}.$$

$|\mathfrak{G}_p : \mathrm{Stab}_{\mathfrak{G}_p}(N)|$ is the size of the orbit containing N under the action of $\mathfrak{G}_p$.

Theorem 2.2. *The function $\zeta_{c,d,p}(s)$ is a rational function in p^{-s}.*

Idea of proof. We show how to represent $\zeta_{c,d,p}(s)$ by a definable p-adic integral as considered by Denef in [1]. The group $F_{c,d}$ has an associated $\mathbb{Z}$-Lie algebra L with the property that for almost all primes p, there is a one to one index preserving correspondence between normal subgroups in $\widehat{(F_{c,d})}_p$ and ideals in $L \otimes \mathbb{Z}_p$. The automorphism group $\mathfrak{G}$ of L has the structure of a $\mathbb{Q}$-algebraic group with the property that $\mathfrak{G}(\mathbb{Z}_p) = \mathrm{Aut}(L \otimes \mathbb{Z}_p) \leq \mathrm{GL}_n(\mathbb{Z}_p)$, where the underlying $\mathbb{Z}$-structure of $\mathfrak{G}$ comes from a choice of basis $e_1, \ldots, e_n$ for L. For almost all primes, $\mathfrak{G}(\mathbb{Z}_p)$ is isomorphic to $\mathfrak{G}_p = \mathrm{Aut}\widehat{(F_{c,d})}_p$, and normal subgroups equivalent under the action of $\mathfrak{G}_p$ correspond to ideals equivalent under the action of $\mathfrak{G}(\mathbb{Z}_p)$. Hence for almost all p:

$$
\begin{aligned}
&\sum_{N \lhd \widehat{(F_{c,d})}_p} |\widehat{(F_{c,d})}_p : N|^{-s} |\mathfrak{G}_p : \mathrm{Stab}_{\mathfrak{G}_p}(N)|^{-1} \\
&\quad = \sum_{N \lhd L \otimes \mathbb{Z}_p} |L \otimes \mathbb{Z}_p : N|^{-s} |\mathfrak{G}(\mathbb{Z}_p) : \mathrm{Stab}_{\mathfrak{G}(\mathbb{Z}_p)}(N)|^{-1}.
\end{aligned}
\tag{5}
$$

This has linearized the problem for almost all primes p.

We now use the concept of p-adic integration to express the right hand side of (5).

Let $\mathrm{Tr}_n(\mathbb{Z}_p)$ denote the set of lower triangular matrices. For each ideal $N \lhd L \otimes \mathbb{Z}_p$, define $M(N) \subset \mathrm{Tr}_n(\mathbb{Z}_p)$ to be the subset consisting of all matrices M whose rows $\mathbf{m}_1, \ldots, \mathbf{m}_n$ form a basis for N. We get a nice description of $\mathrm{Stab}_{\mathfrak{G}(\mathbb{Z}_p)}(N)$ in terms of $M \in M(N)$, namely:

$$\mathrm{Stab}_{\mathfrak{G}(\mathbb{Z}_p)}(N) = \mathfrak{G}(\mathbb{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbb{Z}_p)M.$$

Let μ denote the additive normalized Haar measure on $\mathrm{Tr}_n(\mathbb{Z}_p)$ and let ν be the normalized Haar measure on $\mathfrak{G}(\mathbb{Z}_p)$. The value of $|\mathfrak{G}(\mathbb{Z}_p) : \mathrm{Stab}_{\mathfrak{G}(\mathbb{Z}_p)}(N)|^{-1}$ is then just the measure of the set $\mathfrak{G}(\mathbb{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbb{Z}_p)M$. Define the subset $\mathcal{M} \subset \mathrm{Tr}_n(\mathbb{Z}_p) \times \mathfrak{G}(\mathbb{Z}_p)$ by

$$\mathcal{M} = \left\{ (M, K) : M \in \bigcup_{N \lhd L \otimes \mathbb{Z}_p} M(N), K \in \mathfrak{G}(\mathbb{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbb{Z}_p)M \right\}.$$

Then the right hand side of (5), and hence $\zeta_{c,d,p}(s)$ for almost all primes, equals

$$(1 - p^{-1})^{-n} \int_{\mathcal{M}} |m_{11}|^{s-n} \cdots |m_{nn}|^{s-1} d\mu \, d\nu. \tag{6}$$

The task finally is to extend ideas in [11] and [5] to prove that this is a definable integral in the language of valued fields and apply Denef's rationality result for such definable integrals in [1] to prove Theorem 2.2. The finitely many exceptional primes can also be dealt with in a less uniform manner as compared to the above analysis.

3. Counting finite nilpotent groups

Define the following Dirichlet series counting nilpotent groups of class at most c, generated by d elements:

$$\zeta_{c,d}(s) = \sum_{n=1}^{\infty} g(n, c, d) n^{-s},$$

where $g(n, c, d)$ is defined in Theorem 1.2. Analogous to the Euler product for counting normal subgroups of finite index (4), we have the following:

Proposition 3.1.

$$\zeta_{c,d}(s) = \prod_{p \text{ prime}} \zeta_{c,d,p}(s).$$

This is just an analytic way of saying that a finite nilpotent group is a direct product of its Sylow p-subgroups.

To prove Theorem 1.2 we apply some recent work with Grunewald on Euler products of special sorts of p-adic integrals called cone integrals:

Definition 3.1. Let $|dx|$ be the normalized additive Haar measure on $\mathbb{Z}_p^m$. We call an integral

$$Z_{\mathcal{D}}(s,p) = \int_{V_p} |f_0(\mathbf{x})|^s \, |g_0(\mathbf{x})| \, |dx|$$

a cone integral defined over $\mathbb{Q}$ if $f_0(\mathbf{x})$ and $g_0(\mathbf{x})$ are polynomials in the variables $\mathbf{x} = x_1, \ldots, x_m$ with coefficients in $\mathbb{Q}$ and there exist polynomials $f_i(\mathbf{x})$, $g_i(\mathbf{x})$ $(i = 1, \ldots, l)$ over $\mathbb{Q}$ such that

$$V_p = \left\{ \mathbf{x} \in \mathbb{Z}_p^m : v(f_i(\mathbf{x})) \leq v(g_i(\mathbf{x})) \text{ for } i = 1, \ldots, l \right\}.$$

The set $\mathcal{D} = \{f_0, g_0, f_1, g_1, \ldots, f_l, g_l\}$ is called the *cone integral data.*

In [8] we prove the following about the Euler product of cone integrals over $\mathbb{Q}$:

Theorem 3.2. *Let $\mathcal{D}$ be a set of cone integral data and put*

$$Z_{\mathcal{D}}(s) = \prod_{p \text{ prime}} \left(a_{p,0}^{-1} \cdot Z_{\mathcal{D}}(s,p) \right),$$

where $a_{p,0} = Z_{\mathcal{D}}(\infty, p)$ is the constant coefficient of $Z_{\mathcal{D}}(s,p)$, i.e. we normalize the local factors to have constant coefficient 1. Then the abscissa of convergence α of $Z_{\mathcal{D}}(s)$ is a rational number and $Z_{\mathcal{D}}(s)$ has a meromorphic continuation to $\Re(s) > \alpha - \delta$ for some $\delta > 0$.

To prove Theorem 1.2 we show that for almost all primes p, the integrals (6) representing $\zeta_{c,d,p}(s)$ can be expressed in terms of cone integrals over $\mathbb{Q}$. We can then apply Theorem 3.2, Proposition 3.1 and a suitable Tauberian theorem to deduce the asymptotic behaviour of the coefficients $g(n, c, d)$ of the zeta function $\zeta_{c,d}(s)$ detailed in Theorem 1.2. The finite number of exceptional primes are no worry since we have established that all the local factors are rational functions in p^{-s}.

4. PORC AND COUNTING POINTS ON VARIETIES mod p

The proof of Theorem 3.2 relies on proving an explicit formula for cone integrals in terms of a resolution of singularities $h : Y \to \mathbb{A}^m$ of the polynomial $F = \prod_{i=0}^{l} f_i g_i$, where $\mathcal{D} = \{f_0, g_0, f_1, g_1, \ldots, f_l, g_l\}$ is the associated cone integral data. Let $E_i, i \in T$, be the irreducible components defined over $\mathbb{Q}$ of the reduced scheme $\left(h^{-1}(D)\right)_{\text{red}}$, where $D = \mathrm{Spec}\left(\frac{\mathbb{Q}[\mathbf{x}]}{(F)}\right)$. Then there exist rational functions $P_I(x,y) \in \mathbb{Q}(x,y)$ for each $I \subset T$ with the property that for almost all primes p,

$$Z_{\mathcal{D}}(s,p) = \sum_{I \subset T} c_{p,I} P_I(p, p^{-s}), \tag{7}$$

where

$$c_{p,I} = \mathrm{card}\{a \in \overline{Y}(\mathbb{F}_p) : a \in \overline{E_i}(\mathbb{F}_p) \text{ if and only if } i \in I\}$$

and $\overline{Y}$ means the reduction mod p of the scheme Y. Since $\zeta_{c,d,p}(s)$ are given by cone integrals for almost all primes p, we get a corresponding uniform description for $\zeta_{c,d,p}(s)$ as in (7).

Let $Y(n)$ and $E_i(n)$ $(i \in T(n))$ be the varieties arising from a resolution of singularities of the polynomial $F_n = \prod_{i=0}^{l} f_i g_i$ associated to the cone integrals representing $\zeta_{n-1,n,p}(s)$. Since $f(n,p,n-1,n) = f(n,p)$, the explicit formulas in [8] imply the following uniformity for $f(n,p)$:

Theorem 4.1. *For each $I \subset T(n)$ there exists a polynomial $H_I(X) \in \mathbb{Q}[X]$ such that*

$$f(n,p) = \sum_{I \subset T(n)} c_{p,I} H_I(p),$$

where

$$c_{p,I} = \mathrm{card}\{a \in \overline{Y(n)}(\mathbb{F}_p) : a \in \overline{E_i(n)}(\mathbb{F}_p) \textit{ if and only if } i \in I\} .$$

In [7], the polynomial F_n associated to $\zeta_{n-1,n,p}(s)$ is defined explicitly in terms of the structure constants of the free nilpotent Lie algebra of class $n-1$ on n generators and its associated automorphism group.

By using the recent language of motivic integration as developed by Denef and Loeser [3] and [4], it can be shown that the varieties $E_i(n)$ sitting inside a suitable completion of the Grothendieck ring of varieties, are in fact not accidental but are canonically associated to the cone integrals expressing $\zeta_{n-1,n,p}(s)$. One approach to Higman's PORC conjecture therefore is to understand the varieties $E_i(n)$ $(i \in T(n))$ arising from the resolution of F_n.

We conjecture a stronger uniformity for the behaviour of the rational functions $\zeta_{c,d,p}(s)$ as we vary p than provided by (7):

Conjecture 4.2. *Fix integers c and d. There exist finitely many rational functions $W_i(X,Y) \in \mathbb{Q}(X,Y)$ $(i = 1, \ldots, N)$ such that if $p \equiv i \bmod N$, then*

$$\zeta_{c,d,p}(s) = W_i(p, p^{-s}).$$

The rational functions $W_i(X,Y)$ have the form

$$W_i(X,Y) = \frac{P_i(X,Y)}{(1 - X^{a_{i1}} Y^{b_{i1}}) \cdots (1 - X^{a_{id_i}} Y^{b_{id_i}})}.$$

Note in particular that this conjecture implies the following:

Corollary 4.3. *Suppose Conjecture 4.2 is true. Then for $n \in \mathbb{N}$ and $i = 1, \ldots, N$ there exist polynomials $r_{n,i}(X) \in \mathbb{Q}[X]$ such that if $p \equiv i \bmod N$, then*

$$f(n,p,c,d) = r_{n,i}(p),$$

i.e. the function $f(n,p,c,d)$ is PORC in p.

Since $f(n,p,n-1,n) = f(n,p)$, this includes Higman's PORC conjecture as a special case. We can actually deduce a stronger corollary from Conjecture 4.2, which gives some relationship between the polynomials $r_{n,i}(X)$ as we vary n.

Since $\zeta_{c,d,p}(s)$ can be expressed as a cone integral for almost all p, the explicit expression in (7), valid for almost all primes, implies that the degrees of the numerators and denominators of the rational functions $\zeta_{c,d,p}(s)$ can be bounded independently of p. This bound on the degrees combined with the conjectured PORC behaviour of $f(n,p,c,d)$ would in fact imply Conjecture 4.2.

To prove Conjecture 4.2 is likely to depend on understanding the two pieces of the integral (6):

(1) one coming from the algebraic group $\mathfrak{G}$ and the behaviour of the measure $\mathfrak{G}(\mathbb{Z}_p) \cap M^{-1}\mathrm{GL}_n(\mathbb{Z}_p)M$; and

(2) the other coming from understanding the uniformity of the zeta function counting normal subgroups in the free nilpotent groups.

The uniformity of these normal zeta functions in (2) was first raised in [11], where one rational function $W(X,Y)$ is conjectured to describe $\zeta^{\triangleleft}_{F_{c,d},p}(s)$ for almost all p. However, the relationship with Higman's PORC conjecture implies that the conjecture made there is much more significant than was first realized.

In [11] the uniformity of $\zeta^{\triangleleft}_{F_{c,d},p}(s)$ is proved for $c=2$ and d arbitrary by use of Hall polynomials. Recently in joint work with Fritz Grunewald [10], we have also proved the uniformity for $d=2$ and arbitrary class c.

It remains to analyze the integral coming from the algebraic group in these cases. Note that the true PORC behaviour (i.e. dependence on residue classes) of $f(n,p)$ should be a result of the analysis of the algebraic group, since the conjectured uniformity of $\zeta^{\triangleleft}_{F_{c,d},p}(s)$ in [11] does not depend on residue classes of p.

It should be pointed out that the uniformity of $\zeta^{\triangleleft}_{F_{c,d},p}(s)$ is something special about free nilpotent groups. It was asked in [11] whether such uniformity might hold for a general nilpotent group. However, I have produced an example of class 2, Hirsch length 9 nilpotent group G whose local factors $\zeta^{\triangleleft}_{G,p}(s)$ depend on the behaviour of the number of points $\bmod p$ on the elliptic curve $y^2 = x^3 - x$, a behaviour which is far from the uniformity previously expected. This example is explained in [9].

5. Coclass and conjecture P

Definition 5.1. A p-group of order p^n and class c is said to have *coclass* $r = n - c$.

We begin with explaining the idea of the proof of the following:

Theorem 5.1. *Let $c(r,n,p)$ denote the number of p-groups of order p^n and coclass r and define the Poincaré series of p-groups of coclass r to be*

$$Z_{r,p}(X) = \sum_{n=0}^{\infty} c(r,n,p)X^n.$$

For each p and r, $Z_{r,p}(X)$ is a rational function.

We use the same idea as explained in section 2 to count finite groups by counting normal subgroups in some suitable infinite group. However, unlike counting p-groups of class c on d generators where there is a suitable free object whose finite images are precisely the groups we want to count, coclass is not a good variety of groups and no such free object exists. However, all is not lost. We can find a group whose finite images include all p-groups of coclass r which is not so big as the free group itself. This depends on the remarkable fact (conjectured by Leedham-Green and Newman and confirmed by Leedham-Green [14] and Shalev [16]) that p-groups of coclass r are almost of class two in the following sense:

Theorem 5.2 (Conjecture A). *There exists a positive integer $h = h(p, r)$ such that every p-group of coclass r has a normal subgroup of class at most 2 (1 if $p = 2$) and index dividing p^h.*

A p-group of coclass r is generated by at most $r + 1$ elements.

Definition 5.2. Define the group $\mathcal{G}_r$ by

$$\mathcal{G}_r = F/\gamma_3\left(\gamma_h(F) \cdot F^{p^h}\right),$$

where F is the free $(r + 1)$-generator pro-p group.

The following is then a Corollary of Theorem 5.2:

Corollary 5.3. *Every finite p-group of coclass r is an image of $\mathcal{G}_r$.*

Since $\mathcal{G}_r$ is free in some variety, it has the property that isomorphisms between finite quotients lift to automorphisms of $\mathcal{G}_r$. The group $\mathcal{G}_r$ and its automorphism group are compact p-adic analytic groups. We can use the ideas in section 2 and [5] to express the zeta function counting normal subgroups of $\mathcal{G}_r$ up to equivalence under the action of the automorphism of $\mathcal{G}_r$ as a definable integral, now in the analytic language for the p-adic integers as developed in [2]. However, although every finite p-group of coclass r occurs as an image of $\mathcal{G}_r$, it also has other quotients that we do not want to count. So we need to add a sentence in the definition of our definable integral to make sure we only count normal subgroups corresponding to quotients of coclass r.

But at first sight, coclass looks a very undefinable condition. As the index of the normal subgroup increases, for the quotient to have coclass r, we need to check that the class is also increasing. How can we capture this statement in a definable sentence, which necessarily bounds the length of commutators that we could check?

Here a corollary to the proof of Conjecture A comes to the rescue. Each nontrivial layer of the lower central series $\gamma_n(G)/\gamma_{n+1}(G)$ contributes

$$\log_p |\gamma_n(G)/\gamma_{n+1}(G)| - 1$$

to the coclass. The following corollary of the proof of Conjecture A says that coclass is realized in a bounded image of the group.

Theorem 5.4 (Proposition 4.5 of [16]). *There exists an integer $g = g(p, r)$ such that for every p-group of coclass r, if $n > g$, then*

$$|\gamma_n(G)/\gamma_{n+1}(G)| \leq p.$$

Therefore, to check whether a quotient has coclass r can be done by analyzing only the size of the first g layers of the lower central series. It is therefore possible to express $Z_{r,p}(p^{-s})$ as a p-adic integral definable in the analytic language of the p-adic numbers, and therefore get a proof of Theorem 5.1 by appealing to the proof of the rationality of such integrals established in [2].

Theorem 5.1 is not strong enough, however, to establish the periodicity of the associated trees $\mathcal{F}_{r,p,i}(N)$ defined in the introduction. Certainly the periodicity of these trees implies a recurrence relation for the number of vertices at each layer. But such a recurrence relation says nothing about the shape of the tree being periodic.

We have to squeeze the flexibility of the concept of definable to its limits to prove this periodicity. It can be proved that there is a bound on the valency of the tree $\mathcal{F} = \mathcal{F}_{r,p,i}$ which we shall call v. Let P_n $(n \in \mathbb{N})$ denote the p-groups which are the vertices of the infinite chain in $\mathcal{F}$. From each group P_n define the twig $\mathfrak{t}_n(N)$ to be the directed graph with unique root P_n together with all nonmainline groups of length at most N from P_n. Let $\mathfrak{T}(N, v)$ be the set of finite (directed) graphs of length bounded by N with a unique root and the valency of each node bounded by v. Then for each $\mathfrak{t} \in \mathfrak{T}(N, v)$ define a zeta function

$$\begin{aligned} \zeta_{\mathcal{F}(N),\mathfrak{t}}(s) &= \sum_{\mathfrak{t}_n(N)=\mathfrak{t}} |P_n|^{-s} \\ &= |P_1|^{-s} \sum_{\mathfrak{t}_n(N)=\mathfrak{t}} p^{-(n-1)s}. \end{aligned}$$

Theorem 5.5. *$\mathcal{F}(N)$ is ultimately periodic if and only if for all $\mathfrak{t} \in \mathfrak{T}(N, v)$, $\zeta_{\mathcal{F}(N),\mathfrak{t}}(s)$ is a rational function in p^{-s}.*

The coefficients of $\zeta_{\mathcal{F}(N),\mathfrak{t}}(s)$ are just 1 or 0 according to whether the twig of P_n of length N is isomorphic to $\mathfrak{t}$ or not. Therefore, rationality implies periodicity for occurrence of 1's in the series.

Therefore, Theorem 1.4 is a corollary of the following:

Theorem 5.6. *$\zeta_{\mathcal{F}(N),\mathfrak{t}}(s)$ is a rational function in p^{-s}.*

The strategy for the proof of Theorem 5.6 is to take the definable integral describing the number of all p-groups of coclass r and to add more definable conditions so that we are only counting p-groups which are on the infinite chain of the tree $\mathcal{F}$ with twigs of a certain shape $\mathfrak{t}$.

The details with examples of some of the rational functions for small r and p are contained in [6].

References

[1] J. Denef, The rationality of the Poincaré series associated to the p-adic points on a variety, Invent. Math. **77** (1984), 1–23. MR **86c:**11043

[2] J. Denef and L. van den Dries, p-adic and real subanalytic sets, Ann. of Math. **128** (1988), 79–138. MR **89k:**03034

[3] J. Denef and F. Loeser, Germs of arcs on singular algebraic varieties and motivic integration, Invent. Math. **135** (1999), no.1, 201–232. CMP 99:06

[4] J. Denef and F. Loeser, Motivic Igusa zeta functions, J. of Algebraic Geom. **7** (1998), no. 3, 505–537. MR **99j:**14021

[5] M.P.F. du Sautoy, Finitely generated groups, p-adic analytic groups and Poincaré series, Annals of Math. **137** (1993), 639–670. MR **94j:**20029

[6] M.P.F. du Sautoy, p-groups, coclass, model theory: a proof of conjecture P, preprint (Cambridge).

[7] M.P.F. du Sautoy, Counting finite p-groups and nilpotent groups, preprint (Cambridge).

[8] M.P.F. du Sautoy and F.J. Grunewald, Analytic properties of zeta functions and subgroup growth, preprint (M.P.I. Bonn).

[9] M.P.F. du Sautoy and F.J. Grunewald, Counting subgroups of finite index in nilpotent groups of class 2. In preparation.

[10] M.P.F. du Sautoy and F.J. Grunewald, Uniformity for 2 generator free nilpotent groups. In preparation.

[11] F.J. Grunewald, D. Segal and G.C. Smith, Subgroups of finite index in nilpotent groups, Invent. Math. **93** (1988), 185–223. MR **89m:**11084

[12] G. Higman, Enumerating p-groups, I, Proc. Lond. Math. Soc. **10** (1960), 24–30. MR **22:**4779

[13] G. Higman, Enumerating p-groups, II, Proc. Lond. Math. Soc. **10** (1960), 566–582. MR **23:**A930

[14] C.R. Leedham-Green, The structure of finite p-groups, J. London Math. Soc. **50** (1994), 49–67. MR **95j:**20022a

[15] M.F. Newman and E.A. O'Brien, Classifying 2-groups by coclass, Trans. Amer. Math Soc. **351** (1999), no. 1, 131–169. MR **99c:**20020

[16] A. Shalev, The structure of finite p-groups: effective proof of the coclass conjectures, Invent. Math. **115** (1994), 315–345. MR **95j:**20022b

[17] C.C. Sims, Enumerating p-groups, Proc. Lond. Math. Soc. **15** (1965), 151–166. MR **30:**164

DPMMS, 16 Mill Lane, Cambridge CB2 1SB, UK
E-mail address: `dusautoy@dpmms.cam.ac.uk`