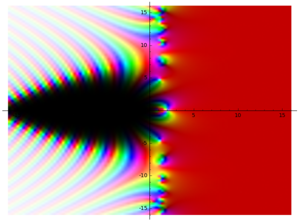
Growth in Nilpotent Groups

Tobias Rossmann

University of Auckland*

January 2018



*Supported by the Alexander von Humboldt Foundation

Some group-theoretic counting problems

Given a group G, enumerate . . .

- elements of G of given length w.r.t. some generating set
- (normal) subgroups of G according to their indices
- representations (e.g. irreducible, complex) of G according to their dimensions
- submodules of a $\mathbf{Z}G$-module according to their indices
- conjugacy classes of G/N for suitable $N \triangleleft G$
- . . .

Some group-theoretic counting problems

Given a group G, enumerate . . .

- elements of G of given length w.r.t. some generating set
- (normal) subgroups of G according to their indices
- representations (e.g. irreducible, complex) of G according to their dimensions
- submodules of a $\mathbf{Z}G$-module according to their indices
- conjugacy classes of G/N for suitable $N \triangleleft G$
- . . .

Definition

Let G be a finitely generated group. Define

$$a_n(G) = \Big(\text{number of subgroups } H \leqslant G \text{ with } |G : H| = n < \infty\Big).$$

Theorem (M. Hall '49)

Let F_r = free group of rank $r \geqslant 1$. Then $a_1(F_r) = 1$ and

$$a_n(F_r) = n(n!)^{r-1} - \sum_{i=1}^{n-1} (n-i)!^{r-1} a_i(F_r).$$

Example

$a_n(\mathbf{Z}) = 1$ for all $n \geqslant 1$.

Hence, $a_1(\mathbf{Z}) + \cdots + a_n(\mathbf{Z}) = n$.

Example

$$a_n(\mathbf{Z}^2) = \sigma(n) = \sum_{d|n} d.$$

Proof.

$a_n(\mathbf{Z}^2) =$ number of $\begin{bmatrix} c & a \\ 0 & d \end{bmatrix}$ for $cd = n$ and $a = 0, \ldots, d-1$. □

Hence, $a_1(\mathbf{Z}^2) + \cdots + a_n(\mathbf{Z}^2) \sim \frac{\pi^2}{12} n^2$ as $n \to \infty$.

Definition

A group G has **polynomial subgroup growth** (PSG) if

$$a_1(G) + \cdots + a_n(G) = \mathcal{O}(n^\alpha)$$

for some $\alpha > 0$.

PSG Theorem (Lubotzky, Mann, Segal ’93)

A finitely generated residually finite group has PSG iff it is virtually soluble of finite rank.

Other types of groups

- Profinite PSG Theorem: Segal, Shalev ’97
- A pro-p gp has PSG iff it is p-adic analytic (Lubotzky, Mann ’91).

Reminder: nilpotent groups

- Finite p-groups are nilpotent.
- Finite direct products of nilpotent groups are nilpotent.
- A finite G is nilpotent iff $G = \prod_{p} G_p$, where each G_p is a p-group.
- The elements of finite order in a nilpotent group form a subgroup.
- A f.g. torsion-free group is nilpotent iff it embeds into some

$$\mathrm{U}_d(\mathbf{Z}) = \begin{bmatrix} 1 & \mathbf{Z} & \cdots & \mathbf{Z} \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \mathbf{Z} \\ 0 & \cdots & 0 & 1 \end{bmatrix} \leqslant \mathrm{GL}_d(\mathbf{Z}).$$

Definition (Grunewald, Segal, Smith '88)

The **subgroup zeta function** of G is

$$\zeta_G(s) = \sum_{n=1}^{\infty} a_n(G) n^{-s}.$$

Remark

$\zeta_G(s)$ converges for $\mathrm{Re}(s) > \alpha$ iff $a_1(G) + \cdots + a_n(G) = \mathcal{O}(n^\alpha)$.

The infimum of all such α is the **abscissa of convergence** α_G of $\zeta_G(s)$.

Proposition (GSS'88)

Let G be a f.g. nilpotent group. Then:

- $\alpha_G \leqslant$ *Hirsch length of* G.
- $\zeta_G(s) = \prod_p \zeta_{\hat{G}_p}(s)$. ($\hat{G}_p =$ *pro-p completion of* G)

Example ("classical result"; see GSS'88)

$$\begin{aligned}\zeta_{\mathbf{Z}^d}(s) &= \zeta(s)\zeta(s-1)\cdots\zeta(s-d+1)\\ &= \prod_p \frac{1}{(1-p^{-s})(1-p^{1-s})\cdots(1-p^{d-1-s})},\end{aligned}$$

where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_p \frac{1}{1-p^{-s}}$ = Riemann zeta function.

Proof.

As above: $a_n(\mathbf{Z}^d) = \sum_{a_1\cdots a_d = n} a_1^0 a_2^1 \cdots a_d^{d-1}$.

Hence, $a_\bullet(\mathbf{Z}^d) = \mathrm{id}^0 * \cdots * \mathrm{id}^{d-1}$ (convolution), where $\mathrm{id}^k = n \mapsto n^k$. □

Consequence:

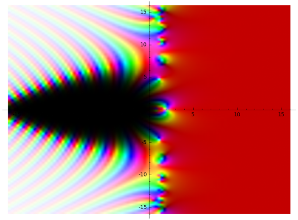
$$a_1(\mathbf{Z}^d) + \cdots + a_n(\mathbf{Z}^d) \sim \frac{\zeta(2)\cdots\zeta(d)}{d} n^d \quad \text{(Euler} \approx 1735\text{: } \zeta(2) = \pi^2/6\text{)}.$$

Example (GSS'88)

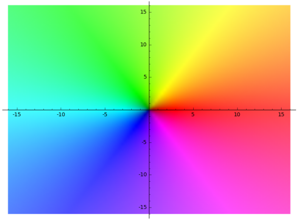
Let $H = \begin{bmatrix} 1 & \mathbf{Z} & \mathbf{Z} \\ 0 & 1 & \mathbf{Z} \\ 0 & 0 & 1 \end{bmatrix} = \mathrm{U}_3(\mathbf{Z})$ = discrete Heisenberg group. Then

$$\zeta_H(s) = \frac{\zeta(s)\zeta(s-1)\zeta(2s-2)\zeta(2s-3)}{\zeta(3s-3)}$$

and $a_1(H) + \cdots + a_n(H) \sim \frac{\zeta(2)^2}{2\zeta(3)} \cdot n^2 \log n$.



$\zeta_H(s)$



s

Let R be a "suitable" ring, e.g. $\mathbf{Z}$ or $\mathbf{Z}_p = \varprojlim_n \mathbf{Z}/p^n$ (p prime).

Definition (GSS'88)

Let L be an R-algebra. The **subalgebra zeta function** of L is

$$\zeta_L(s) = \sum_{n=1}^{\infty} a_n(L) n^{-s},$$

where $a_n(L) =$ no. of subalgebras of index n of L.

Definition (L. Solomon '77)

Let M be an R-module and let $\Omega \subset \mathrm{End}(M)$. The **submodule zeta function** of Ω acting on M is

$$\zeta_{\Omega \curvearrowright M}(s) = \sum_{n=1}^{\infty} a_n(\Omega \curvearrowright M) n^{-s},$$

where $a_n(\Omega \curvearrowright M) =$ no. of Ω-invariant submodules of index n of M.

Theorem (Malcev '49)

f.g. nilpotent groups/commensurability = f.d. nilpotent Lie $\mathbf{Q}$*-algebras/iso.*

Theorem (GSS'88)

Let G be f.g. nilpotent. There exists an additively f.g. Lie ring L s.t. for $p \gg 0$,

$$\zeta_{\hat{G}_p}(s) = \zeta_{L\otimes \mathbf{Z}_p}(s).$$

Theorem (GSS'88)

Let L be an additively f.g. free $\mathbf{Z}$*-algebra. Then* $\zeta_L(s) = \prod_p \zeta_{L\otimes\mathbf{Z}_p}(s)$ *and* $\zeta_{L\otimes\mathbf{Z}_p}(s) \in \mathbf{Q}(p^{-s})$ *for each p.*

Theorem (du Sautoy, Grunewald '00)

- *For $p \gg 0$, $\zeta_{L\otimes\mathbf{Z}_p}(s)$ depends **uniformly** on p: there are finitely many varieties $V_i/\mathbf{Q}$ and $W_i \in \mathbf{Q}(X, Y)$ s.t. for $p \gg 0$,*

$$\zeta_{L\otimes\mathbf{Z}_p}(s) = \sum_i \#\bar{V}_i(\mathbf{F}_p)\cdot W_i(p, p^{-s}).$$

- *$\alpha_L :=$ abscissa of convergence of $\zeta_L(s)$ is rational.*
- *$\zeta_L(s)$ admits meromorphic cont. to $\mathrm{Re}(s) > \alpha_L - \delta$ for some $\delta > 0$.*
- *$a_1(L) + \cdots + a_n(L) \sim c \cdot n^{\alpha_L}(\log n)^{\beta_L - 1}$.*

Relative: enumerating solutions of congruences

Definition

Igusa's local zeta function associated with $f \in \mathbf{Z}[X_1, \ldots, X_n]$ is

$$\mathsf{Z}_{f,p}(s) = \int_{\mathbf{Z}_p^n} |f(\boldsymbol{x})|_p^s \, \mathrm{d}\mu(\boldsymbol{x}).$$

Fact

$$\frac{1 - p^{-s}\mathsf{Z}_{f,p}(s)}{1 - p^{-s}} = \sum_{k=0}^{\infty} \#\Big\{\bar{\boldsymbol{x}} \in (\mathbf{Z}/p^k)^n : f(\bar{\boldsymbol{x}}) = 0\Big\} \cdot p^{-k(s+n)}.$$

- Rationality: Igusa '75, Denef '84
- Uniform formulae: Denef '87
- Toric formulae: Denef et al. '92–01, Veys, Zúñiga-Galindo '08, …

Example: $\mathfrak{sl}_2$ and $\mathfrak{gl}_2$

Recall: $\mathfrak{gl}_d = d \times d$ matrices with Lie bracket $[A, B] = AB - BA$
$\mathfrak{sl}_d =$ traceless matrices

Theorem (Ilani '99; du Sautoy '00; White '00; du Sautoy & Taylor '02)

Let $p \neq 2$. Then $\zeta_{\mathfrak{sl}_2(\mathbf{Z}_p)}(s) = W(p, p^{-s})$, where

$$W(X, Y) = \frac{1 - XY^3}{(1 - X^2Y^2)(1 - XY^2)(1 - XY)(1 - Y)}.$$

Example: $\mathfrak{sl}_2$ and $\mathfrak{gl}_2$

Recall: $\mathfrak{gl}_d = d \times d$ matrices with Lie bracket $[A, B] = AB - BA$
$\mathfrak{sl}_d =$ traceless matrices

Theorem (Ilani '99; du Sautoy '00; White '00; du Sautoy & Taylor '02)

Let $p \neq 2$. Then $\zeta_{\mathfrak{sl}_2(\mathbf{Z}_p)}(s) = W(p, p^{-s})$, where

$$W(X, Y) = \frac{1 - XY^3}{(1 - X^2Y^2)(1 - XY^2)(1 - XY)(1 - Y)}.$$

Theorem (R. '17)

Let $p \gg 0$. Then $\zeta_{\mathfrak{gl}_2(\mathbf{Z}_p)}(s) = W(p, p^{-s})$, where

$$\begin{aligned} W(X, Y) = \big(&-X^8Y^{10} - X^8Y^9 - X^7Y^9 - 2X^7Y^8 + X^7Y^7 - X^6Y^8 - X^6Y^7 \\ &+ 2X^6Y^6 - 2X^5Y^7 + 2X^5Y^5 - 3X^4Y^6 + 3X^4Y^4 - 2X^3Y^5 \\ &+ 2X^3Y^3 - 2X^2Y^4 + X^2Y^3 + X^2Y^2 - XY^3 + 2XY^2 + XY \\ &+ Y + 1\big)/\big((1 - X^7Y^6)(1 - X^3Y^3)(1 - X^2Y^2)^2(1 - Y)\big). \end{aligned}$$

Example: $\mathfrak{sl}_2$ and $\mathfrak{gl}_2$

Recall: $\mathfrak{gl}_d = d \times d$ matrices with Lie bracket $[A, B] = AB - BA$
$\mathfrak{sl}_d =$ traceless matrices

Consistent with known facts:

- $W(X^{-1}, Y^{-1}) = X^6 Y^4 \cdot W(X, Y)$ (Voll '10)
- $W(1, Y) = (1 - Y^3)/\big((1 - Y)^3 (1 - Y^2)^2\big)$ (Evseev '09)

Note: $\mathfrak{gl}_2(\mathbf{Q}) \approx \mathfrak{sl}_2(\mathbf{Q}) \oplus \mathbf{Q}$

Theorem (R. '17)

Let $p \gg 0$. Then $\zeta_{\mathfrak{gl}_2(\mathbf{Z}_p)}(s) = W(p, p^{-s})$, where

$$\begin{aligned} W(X,Y) = \big(&-X^8Y^{10} - X^8Y^9 - X^7Y^9 - 2X^7Y^8 + X^7Y^7 - X^6Y^8 - X^6Y^7 \\ &+ 2X^6Y^6 - 2X^5Y^7 + 2X^5Y^5 - 3X^4Y^6 + 3X^4Y^4 - 2X^3Y^5 \\ &+ 2X^3Y^3 - 2X^2Y^4 + X^2Y^3 + X^2Y^2 - XY^3 + 2XY^2 + XY \\ &+ Y + 1\big)/\big((1 - X^7Y^6)(1 - X^3Y^3)(1 - X^2Y^2)^2(1 - Y)\big). \end{aligned}$$

Explicit computations

Goal

Given $L \approx \mathbf{Z}^d$, compute $\zeta_{L\otimes\mathbf{Z}_p}(s) \in \mathbf{Q}(p^{-s})$ for all $p \gg 0$ simultaneously.

- For many examples of interest:
  $\exists W(X,Y)$ such that $\zeta_{L\otimes\mathbf{Z}_p}(s) = W(p, p^{-s})$ for $p \gg 0$.
  $\rightsquigarrow$ Find $W(X,Y)$.
- Previous computations (ad hoc, partially manual):
  Taylor '01, Woodward '05, ...
- Here: fully automated but restricted by genericity assumptions.

Explicit computations

- A subgroup of f.i. in $\mathbf{Z}^d$ is the row span of a $d \times d$ matrix.
- Subalgebras $\leftrightarrow$ polynomial divisibility conditions in the entries.
- Overcounting for $\zeta_{L\otimes \mathbf{Z}_p}(s)$: p-adic integration (GSS'88).
- Attempt to construct explicit V_i and W_i with

$$\zeta_{L\otimes \mathbf{Z}_p}(s) = \sum_i \#\bar{V}_i(\mathbf{F}_p) \cdot W_i(p, p^{-s}).$$

  dSG'00: impractical due to resolution of singularities
  R.: "toric resolutions" (Khovanskii et al., '70s) and "reduction"
- Attempt to compute each $\#\bar{V}_i(\mathbf{F}_p)$ as a polynomial in p for $p \gg 0$.
- Compute each W_i as a sum of rational functions.
  $\rightsquigarrow$ algorithms of Barvinok et al.
- Final summation.

The search for patterns

Theorem (R. '17)

$$\zeta_{\mathrm{U}_2(\mathbf{Z})\curvearrowright\mathbf{Z}^2}(s) = \zeta(s)\zeta(2s-1)$$

$$\zeta_{\mathrm{U}_3(\mathbf{Z})\curvearrowright\mathbf{Z}^3}(s) = \zeta(s)\zeta(2s-1)\zeta(3s-1)\zeta(4s-2)/\zeta(4s-1)$$

$$\zeta_{\mathrm{U}_4(\mathbf{Z})\curvearrowright\mathbf{Z}^4}(s) = \zeta(s)\zeta(2s-1)\zeta(3s-1)\zeta(4s-1)\zeta(4s-2)\zeta(5s-2) \times \zeta(6s-2)\zeta(7s-3)\zeta(8s-4) \times \prod_p F_4(p, p^{-s}), \textit{ where}$$

$$\begin{aligned} F_4(X,Y) = & - X^{10}Y^{30} + X^9Y^{26} + X^9Y^{25} + X^9Y^{24} - X^9Y^{23} + 2X^8Y^{23} \\ & - X^8Y^{22} + 2X^7Y^{22} - 2X^7Y^{21} - 2X^7Y^{20} + X^6Y^{21} - 2X^7Y^{19} \\ & + X^6Y^{20} - X^6Y^{18} - X^6Y^{17} - X^5Y^{18} - X^5Y^{17} + 2X^6Y^{15} \\ & - X^5Y^{16} + X^5Y^{14} - 2X^4Y^{15} + X^5Y^{13} + X^5Y^{12} + X^4Y^{13} \\ & + X^4Y^{12} - X^4Y^{10} + 2X^3Y^{11} - X^4Y^9 + 2X^3Y^{10} + 2X^3Y^9 \\ & - 2X^3Y^8 + X^2Y^8 - 2X^2Y^7 + XY^7 - XY^6 - XY^5 - XY^4 + 1 \end{aligned}$$

$$\zeta_{\mathrm{U}_5(\mathbf{Z})\curvearrowright\mathbf{Z}^5}(s) = \text{Big Formula } (\approx 2.5 \textit{ pages})$$

Observation: for $d \leqslant 5$, the abscissa of convergence of $\zeta_{\mathrm{U}_d(\mathbf{Z}) \curvearrowright \mathbf{Z}^d}(s)$ is 1.
Example:

$$\zeta_{\mathrm{U}_2(\mathbf{Z}) \curvearrowright \mathbf{Z}^2}(s) = \underset{1}{\zeta(s)}\,\underset{1}{\zeta(2s-1)}$$

$$\zeta_{\mathrm{U}_3(\mathbf{Z}) \curvearrowright \mathbf{Z}^3}(s) = \underset{1}{\zeta(s)}\,\underset{1}{\zeta(2s-1)}\,\underset{2/3}{\zeta(3s-1)}\,\underset{3/4}{\zeta(4s-2)}/\underset{1/2}{\zeta(4s-1)}$$

Remainder of talk:
prove that $\alpha_{\mathrm{U}_d(\mathbf{Z}) \curvearrowright \mathbf{Z}^d} = 1$ for $d \geqslant 1$ without computing $\zeta_{\mathrm{U}_d(\mathbf{Z}) \curvearrowright \mathbf{Z}^d}(s)$.

Submodules invariant under a matrix

- $A \in \mathrm{M}_d(\mathfrak{o})$, where $\mathfrak{o}$ = ring of integers of number field k
- $\zeta_k(s) =$ Dedekind zeta function of k = ideal zeta function of $\mathfrak{o}$
- $f_1, \dots, f_r$: monic irreducible divisors of the min. poly. of A over k
- $k_i = k[X]/f_i$

Theorem (R. '17)

There exist a finite set S of primes and $W_p(X) \in \mathbf{Q}(X)$ for $p \in S$ such that

$$\zeta_{A \curvearrowright \mathfrak{o}^d}(s) = \prod_{p \in S} W_p(p^{-s}) \cdot \prod_{i=1}^{r} \prod_{j=1}^{\ell_i} \zeta_{k_i}(a_{ij}s - j + 1),$$

where the ℓ_i and a_{ij} are determined by the rational canonical form of A over k.

Consequences:

- $\zeta_{A \curvearrowright \mathfrak{o}^d}(s)$ admits meromorphic continuation to $\mathbf{C}$
- abscissa of convergence $\in \mathbf{N}$

Theorem (R. '17)

There exist a finite set S of primes and $W_p(X) \in \mathbf{Q}(X)$ for $p \in S$ such that

$$\zeta_{A \curvearrowright \mathfrak{o}^d}(s) = \prod_{p \in S} W_p(p^{-s}) \cdot \prod_{i=1}^{r} \prod_{j=1}^{\ell_i} \zeta_{k_i}(a_{ij}s - j + 1),$$

where the ℓ_i and a_{ij} are determined by the rational canonical form of A over k.

Example

- $\zeta_{0 \curvearrowright \mathfrak{o}^d}(s) = \zeta_k(s)\zeta_k(s-1)\cdots\zeta_k(s-d+1)$ — the "classical" formula
- Let A = companion matrix of a monic irreducible $f \in \mathbf{Z}[X]$.
  Then $\zeta_{A \curvearrowright \mathbf{Z}^d}(s) = \zeta_{\mathbf{Q}[X]/f}(s) \cdot$ (exceptional factor).
- Let $N_d = \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{bmatrix}$ = companion matrix of X^d.

  Then $\zeta_{N_d \curvearrowright \mathbf{Z}^d}(s) = \zeta(s)\zeta(2s-1)\cdots\zeta(ds-d+1)$.

Submodules invariant under a matrix

Theorem (R. '17)

There exist a finite set S of primes and $W_p(X) \in \mathbf{Q}(X)$ for $p \in S$ such that

$$\zeta_{A \curvearrowright \mathfrak{o}^d}(s) = \prod_{p \in S} W_p(p^{-s}) \cdot \prod_{i=1}^{r} \prod_{j=1}^{\ell_i} \zeta_{k_i}(a_{ij}s - j + 1),$$

where the ℓ_i and a_{ij} are determined by the rational canonical form of A over k.

Sketch of proof:

- CRT: reduce to primary min. poly. f^e of A
- Jordan normal form: $A =$ scalar $+$ nilpotent over $k[X]/f$
  $\rightsquigarrow$ reduce to nilpotent A over extn of k
- Conjugate nilpotent A into a "dual normal form" (over k)
- Express Euler factors in terms of p-adic integrals (GSS'88).
  Recursively compute these.

Corollary (R. '17)

1. $\mathrm{U}_d(\mathbf{Z})$ *has linear submodule growth acting on* $\mathbf{Z}^d$ *for each* $d \geqslant 1$.
2. *Let G be a finitely generated torsion-free nilpotent group of maximal class. Then G has quadratic normal subgroup growth.*

Proof of 2.

"$\alpha_G^{\triangleleft} \geqslant 2$": G maps onto $\mathbf{Z}^2$ and $\zeta_{\mathbf{Z}^2}(s) = \zeta(s)\zeta(s-1)$ so $\alpha_{\mathbf{Z}^2} = 2$.
"$\alpha_G^{\triangleleft} \leqslant 2$": Let $\mathfrak{g}$ = Lie algebra of G.

- $\exists$ basis $(x, y_1, \ldots, y_m)$ with $[x, y_i] = y_{i+1}$, where $y_{m+1} := 0$
- normal subgps of $G \leftrightarrow$ ideals of $\mathfrak{g} \subset \mathrm{ad}(x)$-submodules
- Thm $\Longrightarrow \alpha_{\mathrm{ad}(x) \curvearrowright \mathfrak{g}} = 2$ □

Open: any example of $\zeta_G^{\triangleleft}(s)$ (or $\zeta_{\mathrm{U}_d(\mathbf{Z}) \curvearrowright \mathbf{Z}^d}(s)$) for $h(G) = d \geqslant 6$

The End