each T_k has a natural doubly-transitive permutation representation of degree l_k, on the points of the projective line over $\mathbb{F}_{p_k}$ (or equivalently, on the right cosets of a maximal subgroup of index l_k), we form the groups W_k as a sequence of iterated *permutational wreath products*. That is, $W_1 = T_0$, a permutation group of degree $l_0 = m_1$; having obtained W_i for $i \leq k$ as a permutation group of degree m_i, we take

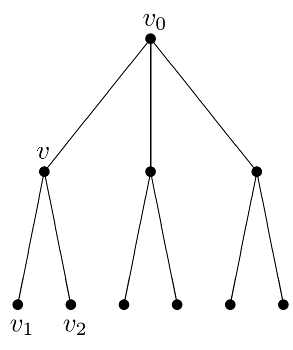
$$W_{k+1} = T_k \wr W_k$$

to be the permutational wreath product of T_k with W_k. This is the semi-direct product of $B_k = T_k^{(m_k)}$ by W_k, which acts by permuting the m_k direct factors, and W_{k+1} has a natural faithful imprimitive permutation representation of degree $l_k \cdot m_k = m_{k+1}$.

The inverse limit W of these iterated wreath products turns out to be a finitely generated profinite group; indeed, we shall see in the next section that W is the profinite completion of a finitely generated (abstract) group.

13.4 Automorphisms of rooted trees

A *rooted tree* is a tree $\mathfrak{T}$ with a distinguished vertex v_0, the root. A vertex of $\mathfrak{T}$ is said to have *level* n if n is the distance from v_0 to v, that is, the length of the unique path from v_0 to v. We consider an infinite *spherically homogeneous* rooted tree $\mathfrak{T}$, that is one where for each $n \geq 1$, all vertices of level n have the same (finite) valency $l_n + 1$. In this case we say that $\mathfrak{T}$ is of type $(l_n)_{n \geq 0}$, where l_0 is the valency of v_0. Thus if v is a vertex of level $n \geq 1$ then a unique edge e leads out of v towards v_0 (upwards, let us say), and the component of $\mathfrak{T} \setminus \{e\}$ not containing v_0 is a spherically homogeneous rooted tree of type $(l_k)_{k \geq n}$ having v as its root. This subtree is denoted $\mathfrak{T}_v$. We picture $\mathfrak{T}$ as growing downwards ('a peculiarity of the Northern hemisphere' according to M.F. Newman), and embedded in the plane; this fixes an ordering (left to right, say) on the vertices of each level.



$\mathfrak{T}[2]$

We denote by $\mathfrak{T}[n]$ the finite rooted subtree containing of all the vertices of level at most n.

Let $\Omega(n)$ denote the set of all vertices of level n; thus $\Omega(n)$ is the 'bottom layer' of $\mathfrak{T}[n]$, and each automorphism of $\mathfrak{T}[n]$ is determined by the permutation it induces on $\Omega(n)$; we use this to identify $\mathrm{Aut}(\mathfrak{T}[n])$ with a subgroup of $\mathrm{Sym}(\Omega(n))$. We may identify $\Omega(n+1)$ with the set $\{1,\ldots,l_n\}\times\Omega(n)$. Having done this, we see that $\mathrm{Aut}(\mathfrak{T}[n+1])$ is precisely the permutational wreath product

$$\mathrm{Sym}(l_n)\wr\mathrm{Aut}(\mathfrak{T}[n]).$$

Starting with $\mathrm{Aut}(\mathfrak{T}[1])=\mathrm{Sym}(l_0)$ we deduce that for each $n\geq 1$,

$$\mathrm{Aut}(\mathfrak{T}[n])=\mathrm{Sym}(l_{n-1})\wr\mathrm{Sym}(l_{n-2})\wr\ldots\wr\mathrm{Sym}(l_0).$$

(Another way to see this is to observe that $\mathrm{Aut}(\mathfrak{T}[n])$ consists of all permutations of $\Omega(n)$ that respect the sequence of equivalence relations

$$d(v,w)\leq 2r$$

for $r=1,\ldots,n-1$, where d denotes the distance between two vertices.)

Finally, since each automorphism of $\mathfrak{T}$ is determined by a sequence of compatible automorphisms of the subtrees $\mathfrak{T}[n]$, we have

$$\mathrm{Aut}(\mathfrak{T})=\varprojlim_{n\to\infty}\mathrm{Aut}(\mathfrak{T}[n])=\varprojlim_{n\to\infty}\left(\mathrm{Sym}(l_{n-1})\wr\mathrm{Sym}(l_{n-2})\wr\ldots\wr\mathrm{Sym}(l_0)\right)$$

We write $\pi_n:\mathrm{Aut}(\mathfrak{T})\to\mathrm{Aut}(\mathfrak{T}[n])\leq\mathrm{Sym}(\Omega(n))$ to denote the restriction mapping.

Suppose that for each $n\geq 0$ we have a subgroup $T_n\leq\mathrm{Sym}(l_n)$. Then

$$W_n=T_{n-1}\wr T_{n-2}\wr\ldots\wr T_0\leq\mathrm{Aut}(\mathfrak{T}[n]),\tag{13.10}$$

and the profinite group

$$W=W((\underline{T}),(\underline{l}))=\varprojlim_{n\to\infty}W_n\tag{13.11}$$

is naturally embedded in $\mathrm{Aut}(\mathfrak{T})$.

For a subgroup Γ of W, let $\mathrm{st}_\Gamma(n)$ denote the pointwise stabilizer in Γ of $\Omega(n)$; this is the kernel of the restriction map $(\pi_n)_{|\Gamma}$. We say that Γ has the *congruence subgroup property* if every subgroup of finite index in Γ contains $\mathrm{st}_\Gamma(n)$ for some n, and that Γ is *dense* in W if

$$\pi_n(\Gamma)=W_n$$

for every n, that is if Γ is dense in the natural profinite topology of W. The following is now clear, since the subgroups $\mathrm{st}_\Gamma(n)$ form a base for the neighbourhoods of 1 in Γ relative to the topology induced from the natural topology of W:

Lemma 13.4.1 *Let $\iota : \widehat{\Gamma} \to W$ be the map induced by the inclusion $\Gamma \to W$. Then ι is surjective if and only if Γ is dense in W, and ι is injective if and only if Γ has the congruence subgroup property.*

We need some notation for tree automorphisms.

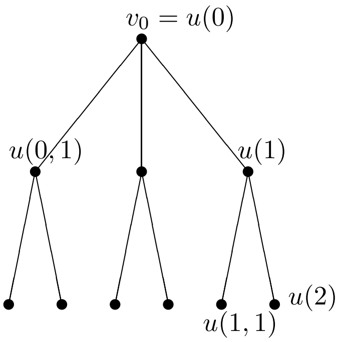
$$g = (g_1, \ldots, g_m)_n$$

indicates that $g \in \mathrm{st}_{\mathrm{Aut}(\mathfrak{T})}(n)$ and that g_i is the restriction of g to the subtree $\mathfrak{T}_{v_i}$, where v_i is the ith vertex in $\Omega(n)$ (in our chosen order, reading from left to right); here $m = |\Omega(n)|$. For any $\alpha \in \mathrm{Sym}(l_n)$ and any vertex $v \in \Omega(n)$, we write $\dot{\alpha}$ to denote the automorphism of $\mathfrak{T}_v$ that induces α on the vertices of level 1 in $\mathfrak{T}_v$ and preserves the ordering of vertices within all the subtrees $\mathfrak{T}_w$ for vertices $w \neq v$ of $\mathfrak{T}_v$; in other words, $\dot{\alpha}$ corresponds to $\alpha \in \mathrm{Sym}(l_n)$ when $\mathrm{Aut}(\mathfrak{T}_v)$ is identified with $\ldots \wr \mathrm{Sym}(l_{n+1}) \wr \mathrm{Sym}(l_n)$; we say that $\dot{\alpha}$ is *rooted at* v. For example, taking $n = 0$, we can write any automorphism g of $\mathfrak{T}$ as

$$g = (h_1, \ldots, h_{l_0})_1 \cdot \dot{\alpha}$$

where $h_i \in \mathrm{Aut}(\mathfrak{T}_{v_i})$ and $\alpha \in \mathrm{Sym}(l_0)$ is the action of g on $\Omega(1) = \{v_1, \ldots, v_{l_0}\}$.

For each $n \geq 1$, let $u(n)$ denote the rightmost vertex of level n in $\mathfrak{T}$ and $u(n,1)$ the leftmost vertex immediately below $u(n)$ (that is, the vertex $l_{n+1} - 1$ steps to the left of the rightmost vertex in $\Omega(n+1)$).



Now let us get down to specifics. Let $P = \langle x, y \rangle$ be a two-generator perfect group, and suppose that for each $n \geq 0$ we have an epimorphism

$$\phi_n : P \to T_n,$$

where T_n is a doubly-transitive subgroup of $\mathrm{Sym}(l_n)$. Write $\alpha_n = \phi_n(x)$ and $\beta_n = \phi_n(y)$. We now define four automorphisms of $\mathfrak{T}$.

$$\xi = \dot{\alpha}_0 \quad \text{rooted at } v_0$$

$$\eta = \dot{\beta}_0 \quad \text{rooted at } v_0$$

$$a \quad \text{and} \quad b$$

where a acts on each of the disjoint subtrees $\mathfrak{T}_{u(n,1)}$ for $n \geq 0$ by $\dot{\alpha}_{n+1}$ rooted at $u(n,1)$, and b acts likewise with $\dot{\beta}_{n+1}$ in place of $\dot{\alpha}_{n+1}$.

Theorem 13.4.2 *The group* $\Gamma = \langle \xi, \eta, a, b \rangle$ *is a dense subgroup of* W (*defined by* (13.11) *and* 13.10)) *and* Γ *has the congruence subgroup property.*

Before proving this, let us complete the proof of Theorem 13.1. Given a function g that satisfies condition $(*)_2$, Theorem 13.3.4 asserts that we can choose a sequence of primes (p_k) so that the profinite group $W = W((\underline{T}), (\underline{l}))$ has subgroup growth type $n^{g(n)}$, where $l_k = 1 + p_k$ and $T_k = \mathrm{PSL}_2(\mathbb{F}_{p_k})$. Now $p_k \geq 5$ for each k, so T_k is a quotient of the group $P = \mathrm{SL}_2(\mathbb{Z}[\frac{1}{6}])$. Moreover, P is generated by the two matrices

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{6} \\ 0 & 1 \end{pmatrix},$$

and P is a perfect group [Bass 1964]. Also the natural action of T_k on the l_k points of the projective line over $\mathbb{F}_{p_k}$ is doubly transitive. Now Theorem 13.4.2 provides a 4-generator subgroup Γ of W, which by Lemma 13.4.1 satisfies $\widehat{\Gamma} \cong W$. Thus $s_n(\Gamma) = s_n(W)$ for all n and Γ has growth type $n^{g(n)}$, as required. The same applies if g is a function of the type mentioned in *Variation 1* or *Variation 2* in the preceding section.

Theorem 13.4.2 depends on two key facts. One of them is a weak form of the congruence subgroup property that holds in great generality. Here, for any subgroup G of $\mathrm{Aut}(\mathfrak{T})$ we denote by $\mathrm{rst}_G(v)$ the *pointwise stabilizer* in G of $\mathfrak{T} \setminus \mathfrak{T}_v$.

Lemma 13.4.3 *Let G be a subgroup of* $\mathrm{Aut}(\mathfrak{T})$ *that acts transitively on each* $\Omega(n)$*. If N is a subgroup of finite index in G then there exists n such that* $N \geq \mathrm{rst}_G(v)'$ *for every vertex v of level n.*

Proof. We may assume that $N \lhd G$. Then G/N contains only a finite number, say k, of distinct subgroups. Let n be so large that $|\Omega(n)| > k$; since $|\Omega(j)| \geq 2\,|\Omega(j-1)|$ for each j we could take any $n > \log k$. Then there exist distinct vertices $u, w \in \Omega(n)$ such that $N\mathrm{rst}_G(u) = N\mathrm{rst}_G(w)$. Since $\mathrm{rst}_G(u)$ and $\mathrm{rst}_G(w)$ have disjoint supports in $\mathfrak{T}$, they commute elementwise. Consequently

$$\begin{aligned} \mathrm{rst}_G(w)' \leq [N\mathrm{rst}_G(w), N\mathrm{rst}_G(w)] &= [N\mathrm{rst}_G(u), N\mathrm{rst}_G(w)] \\ &\leq N[\mathrm{rst}_G(u), \mathrm{rst}_G(w)] = N. \end{aligned}$$

The result follows since $\mathrm{rst}_G(v)'$ is conjugate in G to $\mathrm{rst}_G(w)'$ for each $v \in \Omega(n)$, because G acts transitively on $\Omega(n)$. □

The second key fact is a structural property of the group Γ, expressed in the next lemma. In order to state it, we need to define a series of groups as follows. Consider a vertex v of level m. The tree $\mathfrak{T}_v$ is a spherically homogeneous rooted tree of type $(l_n)_{n \geq m}$, and we now define $\Gamma(\mathfrak{T}_v) \leq \mathrm{Aut}(\mathfrak{T}_v)$ in the same way that we defined $\Gamma \leq \mathrm{Aut}(\mathfrak{T})$ but using α_{n+m} and β_{n+m} in place of α_n and β_n, for each n.

Lemma 13.4.4 *Let $n \geq 1$. Then*

(i) $$\mathrm{st}_\Gamma(n) = \prod_{v \in \Omega(n)} \mathrm{rst}_\Gamma(v),$$

and

(ii) *for each $v \in \Omega(n)$, the group of automorphisms of $\mathfrak{T}_v$ induced by the action of $\mathrm{rst}_\Gamma(v)$ is precisely $\Gamma(\mathfrak{T}_v)$.*

Proof. Suppose we can prove this for $n = 1$. The argument can then be repeated with $\Gamma(\mathfrak{T}_v)$ in place of Γ and the result will follow for every n. So we assume that $n = 1$.

Say $\Omega(1) = \{v_1, \dots, v_l\}$ where $l = l_0$, and denote the restriction of $\mathrm{rst}_\Gamma(v_i)$ to $\mathfrak{T}_{v_i}$ by Δ_i. Write $\Gamma(i) = \Gamma(\mathfrak{T}_{v_i})$.

Now Γ contains $\langle \xi, \eta \rangle = \dot{T}_0$ which permutes $\Omega(1)$ transitively. If $\sigma \in T_0$ sends l to i then $\dot{\sigma}$ induces an isomorphism between the trees $\mathfrak{T}_{v_l}$ and $\mathfrak{T}_{v_i}$ that preserves the ordering of vertices, and hence sends $\Gamma(l)$ to $\Gamma(i)$ as well as sending Δ_l to Δ_i. Let us call this 'property $*$'.

By definition, $\Gamma(l)$ is generated by $\xi(1) = \dot{\alpha}_1$ and $\eta(1) = \dot{\beta}_1$, rooted at $v_l = u(1)$, together with $a(1)$ and $b(1)$, where $a(1)$ and $b(1)$ denote the restrictions of a and of b to the tree $\mathfrak{T}_{v_l}$.

Since a and b fix all vertices of level 1, we have

$$\mathrm{rst}_\Gamma(v_l) \leq \mathrm{st}_\Gamma(1) = \langle a, b \rangle^{\dot{T}_0} (\mathrm{st}_\Gamma(1) \cap \dot{T}_0) = \langle a, b \rangle^{\dot{T}_0},$$

because $\dot{T}_0$ acts faithfully on $\Omega(1)$. Now let $\sigma \in T_0$. If σ fixes l then $a^{\dot{\sigma}}$ acts as $a(1)$ on $\mathfrak{T}_{v_l}$. If σ sends 1 to l then $a^{\dot{\sigma}}$ acts on $\mathfrak{T}_{v_l}$ as $\xi(1)$; in every other case $a^{\dot{\sigma}}$ acts as the identity on $\mathfrak{T}_{v_l}$. Similar conclusions apply to $b^{\dot{\sigma}}$, and it follows that the group of automorphisms induced on $\mathfrak{T}_{v_l}$ by $\mathrm{st}_\Gamma(1)$ is precisely $\Gamma(l)$. In view of property $*$, this implies that $\mathrm{st}_\Gamma(1)$ induces the group $\Gamma(i)$ on $\mathfrak{T}_{v_i}$ for each i, so we have

$$\mathrm{st}_\Gamma(1) \subseteq (\Gamma(1), \dots, \Gamma(l))_1 . \tag{13.12}$$

Now let $\sigma = w(\alpha_1, \beta_1)$ and $\tau = w'(\alpha_1, \beta_1)$ be elements of T_1, where w, w' are words. Put $h = w(a, b)$ and $h' = w'(a, b)$. Then

$$h = (\dot{\sigma}, 1, \dots, 1, *)_1, \ h' = (\dot{\tau}, 1, \dots, 1, *)_1$$

where the ... represent identity automorphisms and the $*$s some automorphisms of $\mathfrak{T}_{v_l}$. Since T_0 is doubly transitive it contains an element ρ that fixes 1 and moves l. Then

$$h^{\dot{\rho}} = (\dot{\sigma}, 1, \dots, *, \dots, 1)_1$$

and then

$$[h^{\dot\rho},\, h'] = ([\dot\sigma, \dot\tau], 1, \ldots, 1)_1,$$
$$[h^{\dot\rho},\, h']^{\dot\mu} = (1, \ldots, 1, [\dot\sigma, \dot\tau])_1 = g, \text{ say}$$

where $\mu \in T_0$ sends 1 to l. Evidently $g \in \mathrm{rst}_\Gamma(v_l)$, and this shows that $[\sigma, \tau]^{\cdot} \in \Delta_l$. As T_1 is a perfect group it follows that Δ_l contains the whole of $\dot T_1$, in particular both $\xi(1)$ and $\eta(1)$.

This argument also shows that Γ contains the element $(\dot\alpha_1, 1, \ldots, 1)_1$. Therefore

$$((\dot\alpha_1, 1, \ldots, 1)_1)^{-1} \cdot a = (1, \ldots, 1, a(1))_1 \in \mathrm{rst}_\Gamma(v_l)$$

and so $a(1) \in \Delta_l$. Similarly $b(1) \in \Delta_l$, and it follows that $\Delta_l \geq \Gamma(l)$. Using property $*$ we deduce that $\Delta_i \geq \Gamma(i)$ for each i. With (13.12) this gives

$$\mathrm{rst}_\Gamma(v_i) \leq \mathrm{st}_\Gamma(1) \subseteq (\Gamma(1), \ldots, \Gamma(l))_1 \subseteq (\Delta_1, \ldots, \Delta_l)_1 .$$

This implies both (i) and (ii). □

Proof of Theorem 13.4.2. We have to show that $\Gamma \leq W$ and that $\pi_n(\Gamma) = W_n$ for each n. In fact the second claim implies the first, since W is the inverse limit of the W_n.

From the definition we see that Γ induces T_0 on $\Omega(1)$. Similarly, for a vertex v of level $n-1$, the group $\Gamma(\mathfrak{T}_v)$ induces T_{n-1} on the set of vertices of level 1 in the tree $\mathfrak{T}_v$. It follows by Lemma 13.4.4 that $\mathrm{st}_\Gamma(n)$ induces $T_{n-1} \times \cdots \times T_{n-1}$ on $\Omega(n)$, acting as the base group of W_n. Supposing inductively that $\pi_{n-1}(\Gamma) = W_{n-1}$ we may infer that

$$\pi_n(\Gamma) = T_{n-1} \wr W_{n-1} = W_n.$$

We also have to establish that Γ has congruence subgroup property. Let N be a subgroup of finite index in Γ. Since each T_j is transitive, $\pi_n(\Gamma) = W_n$ is transitive on $\Omega(n)$ for each n. We may therefore apply Lemma 13.4.3 to deduce that there exists n such that $N \geq \mathrm{rst}_\Gamma(v)'$ for every $v \in \Omega(n)$. Now we claim that each of the groups $\mathrm{rst}_\Gamma(v)$ is *perfect*; this will be proved below. Given the claim, it follows by Lemma 13.4.4(i) that

$$N \geq \prod_{v \in \Omega(n)} \mathrm{rst}_\Gamma(v) = \mathrm{st}_\Gamma(n),$$

which is what we had to prove.

It remains to show that $\mathrm{rst}_\Gamma(v)$ is perfect. Now Lemma 13.4.4(ii) shows that $\mathrm{rst}_\Gamma(v) \cong \Gamma(\mathfrak{T}_v)$. As the latter group is defined in just the same way as Γ, it will suffice to show that Γ itself is perfect. Recall that $P = \langle x, y \rangle$ is a perfect group and that $\Gamma = \langle \xi, \eta, a, b \rangle$. Here $\langle \xi, \eta \rangle = \dot T_0 \cong T_0 = \phi_0(P)$, while a and b act on each of the disjoint subtrees $\mathfrak{T}_{u(n,1)}$ as $\dot\alpha_{n+1}$ and $\dot\beta_{n+1}$ respectively, where

$\alpha_{n+1} = \phi_{n+1}(x)$ and $\beta_{n+1} = \phi_{n+1}(y)$. It follows that any relation satisfied by x and y in P is satisfied by each of the pairs $\alpha_{n+1}, \beta_{n+1}$ and hence by a and b, so

$$x \mapsto a, \ y \mapsto b$$

defines an epimorphism from P onto $\langle a, b \rangle$. Thus Γ is generated by two images of the perfect group P and hence is perfect as claimed.

This completes the proof.

Remarks

(i) Similar results may be obtained under more general hypotheses. For example, it is not necessary to assume that the permutation groups T_n are doubly transitive: it suffices to assume that each one is transitive. Using this, one can obtain a finitely generated group whose profinite completion is the iterated wreath product of any sequence of non-abelian finite simple groups. It is also not hard to show that groups like Γ are *just-infinite*, that is, every non-identity normal subgroup has finite index. For all this, see [Segal 2001] (it is assumed in that paper that the groups T_n are not only transitive but have distinct point-stabilizers: this hypothesis can be removed with a little extra argument).

(ii) In particular, the proof of Theorem 5 in [Segal 2001] shows that there is a 5-generator group Γ such that $\widehat{\Gamma} \cong W = \varprojlim W_n$ where

$$W_n = \mathrm{Alt}(n+5) \wr \ldots \wr \mathrm{Alt}(6) \wr \mathrm{Alt}(5).$$

It is easy to see that the only open normal subgroups of W are the 'level stabilizers' $\ker(W \to W_n)$, and hence that for each m,

$$s_m^{\triangleleft}(W) < \log m.$$

It follows by Theorem 11.5 that W, and hence also Γ, has *polynomial maximal subgroup growth.* Thus the sufficient condition for PMSG given in Theorem 3.5(i) is not necessary, either in profinite groups or in finitely generated abstract groups.

Notes

The construction of §§13.1 and 13.2 is due to **L. Pyber** (personal communication); it will appear in [**Pyber(b)**].

Finitely generated dense subgroups in infinite products of (pairwise non-isomorphic) alternating groups were constructed by [**Neumann 1937**], to give continuously many non-isomorphic finitely generated groups. Using a variant of Neumann's construction, [**Lubotzky, Pyber & Shalev 1996**] obtained examples of finitely generated groups with the slowest then known non-polynomial subgroup growth, of type $n^{\log n/(\log\log n)^2}$; an analogous construction using finite special linear groups instead of alternating groups provided examples with growth type $n^{\log n/\log\log n}$. In order to obtain a continuum of distinct growth types, Pyber had (a) to generalize Neumann's approach by allowing each of the alternating groups to appear several times in the product, and (b) determine the subgroup growth of what we have called 'standard subgroups' of $\mathrm{Sym}(\Omega)$; for this he had to establish an interesting new result on finite permutation groups, Theorem 13.1.2.

The construction of §§13.3 and 13.4 is from [**Segal 2001**]. Possible variations are discussed in [**Segal (a)**].

Groups generated by 'rooted' and 'directed' automorphisms of rooted trees were studied in a series of papers by R.I. Grigorchuk and others, see [**Grigorchuk 2000**]; it was the study of this article (in his role as an editor of the book [**NH**] in which it appears) that inspired the author of [**Segal 2001**]; in particular this article gives sufficient conditions for such groups to have the 'congruence subgroup property'.

The groups of Grigorchuk are mostly prosoluble. Iterated wreath products of finite simple groups were studied by [**Neumann 1986**] and [**Bhattacharjee 1994**], using permutation-group methods. The simple proof of the 'congruence subgroup property' given in §13.4 is taken from the former paper. In the latter, Bhattacharjee showed that iterated wreath products of finite simple alternating groups are (positively) finitely generated.

The spectrum of $\alpha(G)$ – the 'degree of polynomial subgroup growth' – is discussed in [**Shalev 1999**$_a$], though he concentrates mainly on the slightly different invariant

$$\deg(G) = \limsup \frac{\log a_n(G)}{\log n}.$$

Shalev proves that $\deg(G)$ never takes values in the interval $(1, 3/2)$, and states that $\alpha(G)$ never lies in the interval $(1, 2)$. It is unknown whether further 'gaps' of this kind exist.

[**du Sautoy & Grunewald 2000**] prove that $\alpha(G)$ is a rational number if G is a finitely generated nilpotent group; see Chapter 15 below.