Bounded generation and linear groups

Miklós Abért Alexander Lubotzky László Pyber

6 September, 2001.

Abstract

A group Γ is called boundedly generated (BG) if it is the set-theoretic product of finitely many cyclic subgroups. We show that a BG group has only abelian by finite images in positive characteristic representations.

We use this to reprove and generalise Rapinchuk's theorem by showing that a BG group with the FAb property has only finitely many irreducible representations in any given dimension over any field. We also give a structure theorem for the profinite completion G of such a group Γ.

On the other hand, we exhibit boundedly generated profinite FAb groups which do not satisfy this structure theorem.

1 Introduction

A group (resp. profinite group) Γ is said to have *bounded generation* (or finite cyclic width) if Γ is a product of its cyclic (resp. procyclic) subgroups $C_1, \ldots, C_k$. The smallest number k for which Γ has such a decomposition is called the *cyclic width* of Γ (which we denote by $cw(\Gamma)$).

Following the discovery [CK] that the groups $SL(n, \mathbb{Z})$ $(n \geq 3)$ have bounded generation, it has been shown that many other S-arithmetic groups over number fields have this property [Ta], and the notion received a considerable amount of attention [PR], [Lu], [Ra2], [LP] and [Mu].

Recall that Γ is said to have property FAb if for any subgroup $\Gamma_0 \subseteq \Gamma$ of finite index the commutator quotient $\Gamma_o/[\Gamma_o, \Gamma_o]$ is finite.

A major open problem in the area proposed by Bass [Ba2] is whether a residually finite FAb BG group Γ is linear. This is indeed the case if Γ is residually nilpotent [MS] (in this case we don't even have to assume property FAb).

In the current paper we make a step forward in understanding the structure of FAb BG groups and their linear representations.

We first show that unlike in characteristic 0, there are very few boundedly generated groups in characteristic p.

Theorem 1. *Let $\mathbb{F}$ be a field of positive characteristic. If Γ is a boundedly generated subgroup of $GL(n, \mathbb{F})$, then Γ has an Abelian normal subgroup of finite index.*

¿From this we can also deduce the following result, which was proved by Rapinchuk [Ra1] in characteristic 0.

Corollary 2. *Let Γ be an FAb BG group and let $\mathbb{F}$ be an arbitrary field. Then Γ has finitely many inequivalent completely reducible representations over $\mathbb{F}$ in any given dimension.*

Using the corollary, we show the following.

Theorem 3. *Let Γ be an FAb BG group and p a prime. Then Γ has finitely many upper composition factors L in Lie(p).*

Theorem 3 together with some results from [BMP] gives the following structure theorem for the profinite completions of FAb BG groups.

Theorem 4. *Let $G = \widehat{\Gamma}$ be the profinite completion of an FAb BG group Γ. Then there exist a series*

$$1 \subseteq S \subseteq H \subseteq G$$

of normal subgroups of G and a natural number r (which depends only on $cw(\Gamma)$) such that
1) G/H is finite;
2) S is prosolvable;
3) H/S is a cartesian product of finite simple groups of Lie type such that the multiplicities and the Lie ranks of these simple groups are at most r;
4) For every prime p only finitely many of these simple groups are in Lie(p).

Corollary 5. *If Γ is in addition just infinite (i.e., every non-trivial normal subgroup has finite index), then exactly one of the following holds:*
0) Γ is finite;
1) Γ is not linear and it has a finite index subgroup Γ_0 such that every finite quotient of Γ_0 is solvable;
2) Γ is a linear group embeddable as a Zariski-dense subgroup in an S-arithmetic subgroup of a semisimple algebraic group $\mathcal{G}$ defined over a number field K.

So to give a positive answer to the question of Bass for just infinite groups one should eliminate case 1) above.

It is an interesting problem to decide whether a group Γ as in Corollary 5, case 2) is in fact S-arithmetic. This question may be considered as a replacement of Platonov's conjecture, to which a counterexample has been given recently [BL].

Finally we show that Corollary 2, Theorem 3 and Theorem 4, part 4) do not hold for general FAb BG profinite groups. In Section 3 we consider examples like $\prod_p PSL(2, 2^p)$ where p runs over all primes and prove that these groups are BG and FAb. At the same time we note that $\prod_n PSL(2, 2^n)$ where n runs over all positive integers, is not BG.

Recall that in [Py] it was shown that BG groups have subgroup growth at most $n^{c \log n}$. We also construct BG profinite groups of this growth type showing that the result in [Py] is best possible. We do not know whether such a discrete group exists.

2 Boundedly generated groups

We start with a slight extension of a result of Shalev [Sh2, Proposition 5.6].

Proposition 6. *Let G be a p-adic analytic pro-p group. Assume G can be embedded in $GL(n, \mathbb{K})$ for some local field $\mathbb{K}$ of positive characteristic ℓ. Then*
1) If $\ell \neq p$ then G is finite.
2) If $\ell = p$ then G is virtually abelian.

If $\ell \neq p$, then the p-Sylow subgroups of any profinite subgroup of $GL(n, \mathbb{K})$ are finite, so G must be finite.

The case $\ell = p$ is deduced from the following result of Pink [Pi, Corollary 0.5].

Theorem 7. *Let $\mathbb{K}$ be a local field of characteristic $p > 0$ and L a compact subgroup of $GL(n, \mathbb{K})$. Then there exist normal subgroups $L_3 < L_2 < L_1 < L$ such that:*
1) L/L_1 is finite.
2) L_1/L_2 is abelian of finite exponent.
3) There exists a local field E of characteristic p, a connected adjoint semi-simple group H over E with universal covering $\pi : \tilde{H} \to H$ and an open compact subgroup $\Delta \subseteq \tilde{H}(E)$, such that L_2/L_3 is isomorphic to $\pi(\Delta)$ as a topological group.
4) L_3 is a solvable subgroup of derived length at most $\log_2 n$.

We apply Pink's theorem for $L = G$ in proving case 2 of Proposition 6. As G is a p-adic analytic pro-p group, it is finitely generated and so is L_1. Moreover L_1/L_2 is abelian of finite exponent and finitely generated, hence finite and so L_2 is also of finite index. Now, L_2/L_3 is a p-adic analytic pro-p group which is isomorphic to an open compact subgroup Δ of a semi-simple group H over a characteristic p local field E. This is impossible. Indeed, E is isomorphic to $\mathbb{F}_q((t))$ for some $q = p^\alpha$, $\alpha \in \mathbb{N}$, and Δ is commensurable to $H(\mathbb{F}_q[[t]])$. We claim that the latter has infinite rank. For $n \in \mathbb{N}$, let

$$K(n) = Ker(H(\mathbb{F}_q[[t]]) \to H(\mathbb{F}_q[[t]]/(t^n))).$$

It is easy to see that $[K(n), K(n)] \subset K(2n)$ and $K(n)^p \subset K(pn)$. Thus $K(n)/K(2n)$ is an elementary abelian p-group. When n is going to infinity, the rank of $K(n)/K(2n)$ is going to infinity as well. Thus $H(\mathbb{F}_q[[t]])$, and Δ, cannot be of finite rank and cannot be isomorphic to a p-adic analytic pro-p group [DDMS]. (One could also deduce the same conclusion from [Pi, Corollary 0.3] which shows that if two open compact subgroups of simple algebraic groups over local fields are isomorphic, then the fields are the same, and the algebraic groups are isomorphic).

We can therefore deduce that H is trivial and L_3 is of finite index in $L = G$. We have concluded that G is virtually solvable. We claim now that G is actually virtually abelian. Indeed, if G is a solvable subgroup of $GL(n, \mathbb{K})$, then over $\overline{\mathbb{K}}$, the algebraic closure of $\mathbb{K}$, a finite index subgroup of G is conjugate to the group of upper triangular matrices. So we can assume that G is upper triangular, hence unipotent by abelian. But the upper unipotent subgroup of $GL(n, \overline{\mathbb{K}})$ is torsion. As G is a p-adic analytic pro-p group it is virtually torsion-free [DDMS, 4.20]. The finite index torsion-free subgroup of G has trivial intersection with the unipotent subgroup hence it must be abelian. This finishes the proof of Proposition 6.

We deduce the following.

Proposition 8. *Let $\mathbb{F}$ be a field of positive characteristic p. Suppose that Γ is a finitely generated subgroup of $GL(n, \mathbb{F})$ such that the pro-p completion of every finite index subgroup of Γ is p-adic analytic. Then Γ is virtually abelian.*

Proof. As Γ is finitely generated it is actually in $GL(n, \mathbb{A})$ where $\mathbb{A}$ is a finitely generated subring of $\mathbb{F}$. Now $\mathbb{A}$ can be embedded into a local field. Moreover, it can be embedded into the ring of integers of some local field. So we can assume that Γ is a subgroup of $M = GL(n, \mathbb{F}_q[[x]])$ where q is a power of p and $\mathbb{F}_q$ is the field of order q. M is virtually pro-p so Γ has a finite index subgroup Γ_0 such that the closure G of Γ_0 in M is a pro-p group. By our hypothesis G must be p-adic analytic (being a quotient of a p-adic analytic pro-p group). We can now apply Proposition 6 to deduce that G, hence Γ is virtually abelian. □

This general criterion can be used in conjunction with the known characterisations of p-adic analytic pro-p groups to derive various results.

Proof of Theorem 1.

Let Γ be a boundedly generated subgroup of $GL(n, \mathbb{F})$. Then every finite index subgroup Γ_0 of Γ is boundedly generated [Ta], hence the same is true for the pro-p completion G_0 of Γ_0. By a result of Lazard (see [DDMS]) every such group G_0 is p-adic analytic.

Applying Proposition 8 we see that Γ is virtually abelian. □

Recall that a group Γ is said to have polynomial index growth (PIG), if there is a constant c such that for every finite quotient Γ/N we have $|\Gamma/N| \leq (\exp(\Gamma/N))^c$ (where $\exp(G)$ denotes the exponent of the group G). It is clear that boundedly generated groups have PIG. Using the results of Lazard (see [DDMS] and [Sh1]) together with Proposition 8 it follows that in fact the conclusion of Theorem 1 holds under the weaker assumption that Γ has PIG.

We point out another consequence of Proposition 8.

Let Γ be a finitely generated residually-finite group and let $s_n(\Gamma)$ denote the number of subgroups of Γ of index at most n. The asymptotic growth of $s_n(\Gamma)$ has been a topic of intensive research in the last decade – see [LS] and the references therein.

In [Lu] it was shown that a subgroup growth gap exists for groups Γ which are linear over fields of characteristic 0.

Theorem 9. *Let $\mathbb{F}$ be a field of characteristic 0 and Γ a finitely generated subgroup of $GL(n,\mathbb{F})$. Then one of the following holds:*
1) Γ is a virtually solvable group of finite rank (and therefore it has polynomial subgroup growth);
2) There exists a constant c such that $s_n(\Gamma) \geq n^{c \log n / \log\log n}$ for every n.

Here we prove that a larger subgroup growth gap exists for linear groups over fields of positive characteristic.

Theorem 10. *Let $\mathbb{F}$ be a field of characteristic $p > 0$ and Γ a finitely generated subgroup of $GL(n,\mathbb{F})$. The one of the following holds:*
1) Γ is a virtually abelian group of finite rank (and therefore it has polynomial subgroup growth);
2) There exists a constant c such that $s_n(\Gamma) \geq n^{c \log n}$ for infinitely many n.

Proof. Suppose that Γ is not virtually abelian. Then by Proposition 8 Γ has a subgroup Γ_0, say, of index t such that the pro-p completion G_0 of Γ_0 is not p-adic analytic. By [Sh1, Corollary 2.5] there exists infinitely many k for which $s_{p^k}(G_0) \geq p^{k^2/9}$. Hence for infinitely many numbers n we have

$$s_n(\Gamma) \geq (n/t)^{\log(n/t)/9\log p} \geq \frac{n^{\log n/9\log p}}{n^{\frac{2\log t}{9\log p}}}.$$

This implies our statement. □

By a recent result of Segal [Se2] no such gaps exist for the subgroup growth of arbitrary finitely generated groups.

We remark that for $\Gamma = SL(n,\mathbb{Z})$ $(n \geq 3)$, and many other S-arithmetic groups Γ we have $s_n(\Gamma) \leq n^{\frac{c' \log n}{\log\log n}}$ ([Lu]). By a very recent result of Nikolov [Ni], for $\Gamma = SL(n, F_p[t])$ $(n \geq 3)$ we have $s_n(\Gamma) \leq n^{c' \log n}$. Hence the above bounds are sharp.

We need the following result which is proved implicitly in [LMS].

Lemma 11. *Let Γ be a finitely generated group, n a positive integer and Ω a family of fields of characteristic p. If Γ can be embedded in the Cartesian product $\prod_{F\in\Omega} GL(n,F)$ then Γ is a subdirect product of finitely many linear groups of degree n over fields of characteristic p.*

Our next result extends Rapinchuk's theorem [Ra1].

Proof of Corollary 2.

Case 1. By Theorem 1 any representation of Γ over a field of positive characteristic has finite image. Let π be a complex linear representation of Γ. Since Γ is finitely generated, there is a finitely generated ring A with $\pi(\Gamma) \subseteq GL(n, A)$. For any transcendental $a \in A$, there is a ring homomorphism $\zeta : A \to \mathbb{K}$ where $\mathbb{K}$ is a field of positive characteristic with $\zeta(a)$ still transcendental. If for some $\gamma \in \Gamma$ we have $tr(\pi(\Gamma)) \notin \overline{\mathbb{Q}}$ then ζ defines a representation π_ζ over $\mathbb{K}$ with $tr(\pi_\zeta(\gamma))$ transcendental. Hence $\pi_\zeta(\Gamma)$ is infinite, a contradiction.

We proved that the traces of all finite dimensional complex linear representations are algebraic numbers which is equivalent to our conclusion, when the characteristic of $\mathbb{F}$ is 0 (see [Ba1, Example 5.12 (3)]).

Case 2. Suppose now that $\mathbb{F}$ has characteristic p. Denote by K the intersection of the kernels of $\mathbb{F}$-representations of degree n of the group Γ. By Lemma 11 Γ/K is a subdirect product of finitely many linear groups of degree n over fields of characteristic p. Each of these linear groups is abelian by finite by Theorem 1 hence the same is true for Γ/K. Since Γ is an FAb group this implies that Γ/K is finite. Hence the number of irreducible $\mathbb{F}$-representations of degree n of Γ is bounded by the total number of irreducible $\mathbb{F}$-representations of Γ/K which is at most $|\Gamma/K|$ [Be]. Let ρ be a completely reducible representation of degree n of Γ. By the above we have finitely many choices for the irreducible components $\rho_1, \ldots, \rho_t$ of ρ. The images $\rho_i(\Gamma)$ are finite and $\rho(\Gamma)$ is a subgroup of their direct product hence there are finitely many choices for ρ. $\square$

Remark. As the above proof shows, when the field $\mathbb{F}$ has positive characteristic, we can say a bit more; in this case all representations of a given degree factor through some finite quotient Γ/K of Γ.

Recall that an *upper section* of Γ is a group $X \cong H/K$ with H and K finite index subgroups of Γ, K normal in H. If H is subnormal in Γ and X is simple then X is an *upper composition factor* of Γ, if both H and K are normal in Γ, then X is an *upper factor* of Γ.

It is proved in [Py] that the degrees of alternating upper composition factors and the Lie ranks of Lie-type upper composition factors of a group Γ are bounded in terms of its cyclic width (if it is finite). Moreover in [BMP] it is proved that if L^r is a non-abelian upper factor of Γ, with L simple then r is bounded in terms of $cw(\Gamma)$.

To prove Theorem 3 we need these results, whose proofs rely on the classification theorem of finite simple groups (CFSG) and the following observation.

Lemma 12. *Let Γ be a finitely generated FAb group, H a normal subgroup of index m in Γ and H/K a soluble upper section of derived length d. Then there is a finite bound for $|\Gamma : K|$ which depends only on m, d and Γ.*

Proof. Denote by $I = I(m)$ be the intersection of all normal subgroups H of index m in Γ. Since Γ is finitely generated I has finite index in Γ. Let $I^{(d)}$ be the d-th term of the derived series of I. By the FAb property $I^{(d)}$ is of finite index. This index gives the desired bound. □

Proof of Theorem 3.

Let L be any non-abelian upper composition factor of Γ. Since Γ is finitely generated, there is an upper factor H/K of Γ which is isomorphic to L^r for some r. Set $C = C_\Gamma(H/K)$. Then Γ/C is the finite group of automorphisms that Γ induces on H/K. Hence Γ/C contains a subgroup B/C isomorphic to L^r such that Γ/B has an embedding into $Out(L)wrSym(r)$. As mentioned above r is bounded in terms of $cw(\Gamma)$. It is a well-known consequence of CFSG that $Out(L)$ is soluble of derived length at most 3, hence Γ/B has a normal subgroup of $cw(\Gamma)$-bounded index of derived length at most 3. By Lemma 12 we see that $|\Gamma/B|$ is bounded in terms of Γ.

If L is a simple group of rank l in $Lie(p)$ then it has a faithful representation of degree roughly l^2 over $\overline{F_p}$, the algebraic closure of F_p (see the proof of Theorem D in [MS]). By [Py] l is bounded in terms of $cw(\Gamma)$. Therefore $B/C \cong L^r$ and then also Γ/C has a faithful representation of Γ-bounded degree over $\overline{F_p}$. By Corollary **2** there are only finitely many such representations of Γ hence for given p there are only finitely many choices for L. This completes the proof. □

Proof of Theorem 4.

¿From [BMP, Theorem 2.3 and Corollary 2.4] one deduces that G has such a series of subgroups satisfying 1), 2) and 3). Now 4) follows from Theorem 3. □

Proof of Corollary 5.

As Γ is residually finite, it is embedded in $G = \widehat{\Gamma}$. Now using the notations of Theorem 4 we distinguish between several cases.

Assume first that S is of finite index in G. This implies that Γ has a finite index subgroup Γ_0 with $\widehat{\Gamma_0}$ prosolvable. If Γ_0 itself is solvable, then by the FAb property of Γ, Γ_0 and Γ are finite and we are in Case 0).

If Γ_0 is not solvable, then Γ can not be a linear group, since every non virtually-solvable linear group has infinitely many simple groups as upper composition factors. This follows easily from the Strong Approximation Theorem (see [We]). We also give a direct argument: if such a group Γ is linear, then Γ and also Γ_0 is residually finite-linear-group of the same degree. These finite linear quotients of Γ_0 are solvable of bounded derived length. Hence Γ_0 is solvable, a contradiction.

Now assume that S is of infinite index in G in which case $\Gamma \cap S = 1$. It follows that Γ is separated by bounded degree representations over finite fields, such that every characteristic occurs only finitely many times. This implies that Γ is linear over a field of characteristic 0 (see [LMS]).

As Γ is just infinite, it has a faithful specialisation into $GL(n, \overline{\mathbb{Q}})$ where $\overline{\mathbb{Q}}$ is the field of algebraic numbers (see [LM, Proposition 2.2]). As Γ is finitely generated, it is inside $GL(n, K)$ for some number field K. In fact, Γ is in $\mathcal{G}(O_S)$, where $\mathcal{G}$ is its Zariski closure, O is the ring of integers in K, S a finite set of valuations containing all the archimedean ones and $O_S = \{x \in K \mid v(x) \geq 0 \text{ for all valuations } v \notin S\}$. $\mathcal{G}$ can be made semisimple since Γ is just infinite. □

3 Profinite constructions

In contrast to Theorem 1 below we prove that the groups $SL(n, q)$ with n fixed form a family of linear groups of dimension n with n-bounded cyclic width and having no abelian normal subgroups of n-bounded index (see a forthcoming paper [AP] for a more general result saying that if G is a finite completely reducible linear group of dimension n over any field then its cyclic width is at most $1000n$). This shows that in Theorem 1, unlike in Jordan's theorem, we cannot bound the index of the abelian normal subgroup.

In fact, we obtain a more precise result which we use to construct examples of profinite groups showing that Corollary 2, Theorem 3 and Theorem 4 do not hold in the profinite category.

Lemma 13. *Let $q > 3$ be a prime power and $n \geq 2$. Then $SL(n, q)$ is the product of $10n(n-1)$ cyclic subgroups of order $q - 1$.*

Proof. We claim that the upper triangular subgroup $U \subseteq SL(2, q)$ is contained by the product of 5 cyclic subgroups of order $q-1$. We use conjugates of the diagonal subgroup D (which is a cyclic subgroup of order $q-1$). Denoting the elements of D and U by

$$d_x = \begin{bmatrix} x^{-1} & 0 \\ 0 & x \end{bmatrix} \text{ and } u_y = \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix}$$

we have $d_x^{-1} u_1 d_x = u_{x^2}$. Since $u_x u_y = u_{x+y}$ and in any finite field every nonzero element is the sum of two squares, we have

$$\left\{u_x \mid x \in F_q^*\right\} = \left\{d_{x^{-1}} u_1 d_{xy^{-1}} u_1 d_y \mid x, y \in F_q^*\right\}.$$

Choose $t \in F_q^*$ such that $t^2 \neq 1$ (here we need $q > 3$). Set $a = u_{(t^{-2}-1)^{-1}}$. A simple calculation shows that $d_t^a d_{t^{-1}} = u_1$ hence $\{I, u_1\} \subseteq D^a D$. Therefore $U = \{u_x \mid x \in F_q\} \subseteq DD^a DDD^a DD = DD^a DD^a D$. This proves our claim.

Now let $E_{ij} \subseteq SL(n,q)$ be the subgroup consisting of the matrices which differ from I only in the (i,j)-th entry $(i \neq j)$. It is well-known that E_{ij} and E_{ji} generate a subgroup isomorphic to $SL(2,q)$ and E_{ij} and E_{ji} correspond to the upper and lower triangular subgroups. By the above claim every subgroup E_{ij} is contained by the product of 5 cyclic subgroups of order $q-1$ in $SL(n,q)$.

Also let U and L denote the upper and lower triangular subgroups of $SL(n,q)$. We have $U = \prod_{i<j} E_{ij}$ and $L = \prod_{i>j} E_{ij}$ hence U and L are contained by the product of $5\frac{n(n-1)}{2}$ cyclic subgroups of order $q-1$. On the other hand $LULU = SL(n,q)$ (see [DV], the proof of Corollary 14). This implies our statement. □

Denote by p_i the i-th prime. It is easy to see that the numbers $2^{p_i}-1$ are pairwise relatively prime.

Let $G = \prod_{i=1}^{\infty} PSL(n, 2^{p_i})$ be the cartesian product of the groups $PSL(n, 2^{p_i})$ for some fixed $n \geq 2$. G is a profinite group with the usual product topology.

Theorem 14. *1) G is boundedly generated as a profinite group.*
2) G has polynomial index growth and the FAb property as an abstract group.
3) G does not contain any dense discrete boundedly generated subgroups.

Proof. Set $k = 10n(n-1)$. By Lemma 13 any group $PSL(n, 2^{p_i})$ is the product of k cyclic subgroups $C_1^i, \ldots, C_k^i$ of orders dividing $2^{p_i}-1$. For j fixed the orders of the groups C_j^i are pairwise relatively prime therefore the subgroup $C_j = \prod_{i=1}^{\infty} C_j^i$ of G is procyclic. G is the product of the procyclic subgroups C_j i.e., it is boundedly generated.

It was proved independently by Saxl and Wilson [SW] and Martinez and Zelmanov [MZ] that in a finitely generated profinite group which is a cartesian product of nonabelian finite simple groups every finite index subgroup is open. It also follows easily, that groups of this type are perfect (using the fact, first proved by Wilson [Wi], that there exists a constant r, such that every element of a nonabelian finite simple group is the product of r commutators).

In particular every finite index normal subgroup N of our G is open. It follows that G/N is a product of k cyclic subgroups hence $|G/N| \leq (\exp(G/N))^k$ for every N, i.e., G has polynomial index growth.

It is also clear that every such group N is also perfect. Hence if H is a finite index subgroup of G then H contains a perfect normal subgroup of finite index therefore G has the FAb property.

Let Γ be a finitely generated subgroup of G. For q arbitrary the group $PSL(n,q)$ can be embedded into $SL(n^2-1,q)$. Using Lemma 11 we see that Γ is a subdirect product of finitely many linear groups over fields of characteristic 2. If Γ is boundedly generated then by Theorem 1 it is a subdirect product of finitely many abelian by finite groups hence Γ itself is abelian by finite. Therefore Γ can not be dense in G. □

In view of the above example it is natural to ask whether the profinite group $H = \prod_{i=1}^{\infty} PSL(n,p^i)$ with $n \geq 2$ and p fixed is boundedly generated. We give a negative answer.

Proposition 15. *H is not boundedly generated as a profinite group.*

Proof. Suppose that H is the product of m procyclic subgroups. For an arbitrary k let $r_k = p_1 p_2 \cdots p_k$ (the product of the first k primes) and let $H_k = \prod\limits_{d|r_k} PSL(n,p^d)$. Set

$$o_k = |GL(n,p^{r_k})| = p^{r_k \frac{1}{2} n(n-1)} \prod_{i=1}^{n} (p^{r_k i} - 1).$$

If $d \mid r_k$ then $GL(n,p^d)$ can be embedded into $GL(n,p^{r_k})$, which yields $\left|PSL(n,p^d)\right| \mid o_k$. As a consequence, every element of the product H_k has order dividing o_k. Since H_k is a quotient of H it is a product of m cyclic subgroups. Thus using the obvious inequality $\left|PSL(n,p^d)\right| \geq p^d$ we obtain that

$$o_k^m \geq |H_k| \geq p^{\sum\limits_{d|r_k} d} = p^{(1+p_1)(1+p_2)\cdots(1+p_k)}.$$

Using $o_k \leq p^{r_k n^2}$ and taking logarithms we obtain

$$m \geq \frac{1}{n^2} \frac{(1+p_1)(1+p_2)\cdots(1+p_k)}{p_1 p_2 \cdots p_k} \geq \frac{1}{n^2} \sum_{i=1}^{k} \frac{1}{p_i}.$$

This is a contradiction since the right side can be made arbitrarily large. □

We remark here that our proof of Theorem 1 used a 'local method', i.e., embedding Γ into $GL(n, \mathbb{K})$ where $\mathbb{K}$ is a local field. One can give a different proof by 'global' considerations, i.e., appealing to the Strong Approximation Theorem for linear groups (see [We] and [Pi2]). From the theorem it follows that Γ has many nonabelian simple quotients and then a variant of Proposition 15 shows that Γ can not be boundedly generated. We omit the details.

Note that for every n the group of the form $\prod_p PSL(n,p)$ (p runs over all prime numbers) is a BG profinite group (see [LP] for a more general result).

Our next result has a variety of uses in constructing boundedly generated profinite groups.

Lemma 16. *Let G be a transitive permutation group on n elements and H a pointstabiliser.*
1) If G is 2-transitive then it is a product of 3 pointstabilisers.
2) Let N be the normal subgroup of G generated by all pointstabilisers. Suppose H has an orbit of length $\geq \frac{n}{r}$. Then N is a product of at most $2r$ pointstabilisers.

Proof. If G is 2-transitive, then for any $g \in G \setminus H$ we have $G = H \cup HgH$. Now H fixes exactly one point, say α, hence if H_1 is the stabiliser of $\beta \neq \alpha$ then there is a $g \in H_1 \setminus H$. Therefore $G = HH_1H$ which proves 1).

Now let G be as in 2). Our conditions imply that there is a double coset HgH of size $\geq \frac{|G|}{r}$. Hence the subset $X = g^{-1}HgH$ (which is a product of 2 pointstabilisers) also has size $\geq \frac{|G|}{r}$.

By a result of Hamidoune [Ha] if a finite group G is generated by a set of size d, then every element of G is a product of at most $2\frac{|G|}{d}$ elements of this set. Hence if M is the subgroup of N generated by X, then every element of M is a product of at most $2\frac{|M|}{|X|}$ elements of X.

If $M \neq N$ then there is a pointstabiliser $H_1 \not\subseteq M$. The set MH_1 is the union of at least 2 right cosets of M. If $MH_1 \neq N$ then there is a pointstabiliser H_2 such that MH_1 is properly contained in MH_1H_2 which then must be the union of at least 3 right cosets of M. Repeating this argument we see that N is a product of at most $2\frac{|M|}{|X|} + |N : M| - 1$ pointstabilisers. But $2\frac{|M|}{|X|} + |N : M| - 1 \leq 2\frac{|N|}{|X|} \leq 2r$ which proves 2). □

Now we define a metabelian group with some interesting properties. Let $A = \prod_{k=1}^{\infty} AGL(1, 2^{p_k})$ be the cartesian product of the finite affine groups $AGL(1, 2^{p_k})$.

Proposition 17. *1) A is an extension of an elementary abelian 2-group by a procyclic group;*
2) A is boundedly generated as a profinite group;
3) A has polynomial index growth as an abstract group;
4) A has at least $n^{\frac{1}{8}\log n - 1}$ subgroups of index n for infinitely many n;
5) A does not contain any dense discrete boundedly generated subgroups.

Proof. By definition any group $AGL(1, 2^{p_k})$ is an extension of an elementary abelian group V_k of order 2^{p_k} by a cyclic group of order $2^{p_k} - 1$. It is naturally a 2-transitive permutation group. Hence by Lemma 16 it is a product of 3 cyclic subgroups of order $2^{p_k} - 1$. 1) and 2) follow immediately (using the fact that the numbers $2^{p_k} - 1$ are relatively prime).

By a result of Segal [Se] any finite index subgroup of a finitely generated prosoluble group is open hence 2) implies 3).

For any k the linear space V_k has at least $2^{x(p_k - x)}$ subspaces of codimension x. Each such subspace defines - in an obvious way - a subgroup of index $(2^{p_k} - 1)2^x$ in A. Setting $x = \left[\frac{p_k}{3}\right]$ we obtain 4) by straightforward computation.

Finally note that $AGL(1, 2^{p_k})$ is isomorphic to a subgroup of $SL(2, 2^{p_k})$ (namely to the subgroup of all matrices with 0 above the main diagonal). As in the proof of Theorem 14 we see that any boundedly generated subgroup Γ of A is abelian by finite hence it can not be dense in A. □

There is nothing really special about the prime 2 in the above constructions. The group $AGL(1, p^t)$ has a unique subgroup $A^0(p^t)$ which is an extension of an elementary abelian p-group by a cyclic group of order $\frac{p^t - 1}{p-1}$. It is naturally a permutation group of permutation rank p (i.e., the cyclic pointstabiliser has p orbits). Using Lemma 16 one can see that $A^0(p^t)$ is a product of at most $4p$ cyclic groups of order $\frac{p^t - 1}{p-1}$. It follows that the profinite group $A^0 = \prod_{k=1}^{\infty} A^0(p^{p_k})$ is boundedly generated.

Using similar ideas one can reprove Theorem 14 and show that in fact for every fixed prime p the profinite groups of the form $\prod_{k=1}^{\infty} PSL(n, p^{p_k})$ are boundedly generated.

To obtain somewhat different examples one can use the primitive affine permutation groups of rank 3 listed in [Li]. For instance for $2^d = q^6$ the group $SL(2, q)$ acts on the nonzero elements of the group C_2^d with 2 orbits. Denote the corresponding affine groups of the form $C_2^d \bowtie SL(2, q)$ by $A^1(q)$. Using Lemma 16 one can see that $A^1(q)$ is a product of at most 40 cyclic subgroups of order $q - 1$. Therefore the profinite group $A^1 = \prod_{k=1}^{\infty} A^1(2^{p_k})$ is boundedly generated.

References

[Ba1] H. Bass, *Groups of integral representation type*, Pacific J. Math. 86 (1980), 15-51

[Ba2] H. Bass, talk given at the Conference in Algebra, Beijing, 1996

[BL] H. Bass and A. Lubotzky, *Nonarithmetic superrigid groups: counterexamples to Platonov's conjecture*, Ann. of. Math (2) 151 (2000), 1151-1173

[AP] M. Abért and L. Pyber, *Decomposing finite linear groups into products of cyclic groups*, preprint

[BMP] A. Balog, A. Mann and L. Pyber, *Polynomial index growth groups*, Int. J. Alg. Comp. 10 (2000), 773-782

[Be] S.D. Berman, *The number of irreducible representations of a finite linear group over an arbitrary field*, Dokl. Akad. Nauk. SSSR (NS) 106 (1956), 767-769 (in Russian)

[CK] D. Carter and G. Keller, *Bounded elementary generation of $SL_n(O)$*, Amer. J. Math. 105 (1983), 673-687

[DV] R.K. Dennis and L.N. Vaserstein, *On a question of M. Newman on the number of commutators*, J. Algebra 118 (1988), 150-161

[DDMS] J.D. Dixon, M.P.F. du Sautoy, A. Mann and D. Segal, *Analytic Pro-p Groups, 2nd Edition*, Cambridge Univ. Press, Cambridge, UK, 1999

[Ha] Y.O. Hamidoune, *An application of connectivity theory in graphs to factorizations of elements in groups*, European J. Comb. 2 (1981), 349-355

[Li] M.W. Liebeck, *The affine permutation groups of rank three*, Proc. London Math. Soc. (3) 54 (1987), 477-516

[LP] M.W. Liebeck, L. Pyber, *Finite linear groups and bounded generation*, Duke Math. J., to appear

[Lu] A. Lubotzky, *Subgroup growth and congruence subgroups*, Invent. Math. 119 (1995), 267-295.

[LM] A. Lubotzky and A. Mann, *On groups of polynomial subgroup growth*, Invent. Math. 104 (1991), 521-533

[LMS] A. Lubotzky, A. Mann and D. Segal, *Finitely generated groups of polynomial subgroup growth*, Israel. J. Math. 82 (1993), 363-371

[LS] A. Lubotzky and D. Segal, *Subgroup Growth*, book in preparation

[MS] A. Mann and D. Segal, *Uniform finiteness conditions in residually finite groups*, Proc. London Math. Soc. 61 (1990), 529-545

[MZ] C. Martinez and E. Zelmanov, *Products of powers in finite simple groups*, Israel J. Math. 96 (1996), 469-479

[Ni] N. Nikolov, *Subgroup growth of Chevalley groups in positive characteristic*, in preparation

[Mu] V. Kumar Murty, *Bounded and finite generation of arithmetic groups*, Canad. Math. Soc. Conf. Proceedings 15 (1995), 249-261

[Pi] R. Pink, *Compact subgroups of linear algebraic groups*, J. Algebra 206 (1998), 438-504

[Pi2] R. Pink, *Strong approximation for Zariski dense subgroups over arbitrary global fields*,

[PR] V. Platonov and A.S. Rapinchuk, *Abstract properties of S-arithmetic subgroups and the congruence subgroup problem*, Izv. R. Acad. Sci. Ser. Math. 56 (1992), 483-508.

[Py] L. Pyber, *Bounded generation and subgroup growth*, Bull. London Math. Soc., to appear

[Ra1] A.S. Rapinchuk, *Representations of groups with bounded generation*, Dokl. Acad. Nauk. SSSR 315 (1990), 536-540 (in Russian)

[Ra2] A.S. Rapinchuk, *On SS-rigid groups and A. Weil's criterion for local rigidity I.*, Manuscripta Math. 97 (1998), 529-543

[SW] J. Saxl and J.S. Wilson, *A note on powers in simple groups*, Math. Proc. Cambridge Phil. Soc. 122 (1997), 91-94

[Se] D. Segal, *Closed subgroups of profinite groups*, Proc. London Math. Soc. (3) 81 (2000), 29-54

[Se2] D. Segal, *The finite images of finitely generated groups,* Proc. London Math. Soc. (3) 82 (2001), 597-613

[Sh1] A. Shalev, *Growth functions, p-adic analytic groups and groups of finite coclass*, J. London Math. Soc. (2) 46 (1992), 111-122

[Sh2] A. Shalev, *Lie methods in the theory of pro-p groups*, in "New horizons in pro-p groups" (M. du Sautoy, D. Segal and A. Shalev eds.), Progress in Mathematics 184, Birkhäuser, Boston, 2000

[Ta] O. I. Tavgen, *Bounded generation of Chevalley groups over rings of algebraic S-integers*, Math. USSR. Izv. 36 (1991), 101-128.

[We] B. Weisfeiler, *Strong approximation for Zariski-dense subgroups of semi-simple algebraic groups*, Annals of Math. 120 (1984), 270-315

[Wi] J.S. Wilson, *On simple pseudofinite groups*, J. London Math. Soc. (2) 51 (1995), 471-490