The lower rank of some pro-p groups and the number of generators of simple Lie algebras

Yiftach Barnea*
Institute of Mathematics, The Hebrew University
Jerusalem 91904, Israel
e-mail: yiftach@math.huji.ac.il

January 27, 1998

Preprint No. 9
1997/98

Abstract

Let G be a profinite group. We define the **lower rank** of G to be

$$\liminf\{d(H) | H \leq_o G\},$$

where $H \leq_o G$ means that H is an open subgroup of G and $d(H)$ denote the minimal number of generators of H as a topological group.

Let G be an $F_p[[t]]$-standard pro-p group, e.g. $SL_d^1(F_p[[t]])$. We can associate with G a graded Lie algebra $L(G) = \mathfrak{g} \otimes tF_p[t]$, where $\mathfrak{g}$ is a Lie algebra over F_p, e.g. $L(SL_d^1(F_p[[t]])) = \mathfrak{sl}_d(F_p) \otimes tF_p[t]$.

We prove that if $\mathfrak{g}$ is a simple Lie algebra then the lower rank of G is $\leq d(\mathfrak{g}) + 1$, where $d(\mathfrak{g})$ is the minimal number of generators of $\mathfrak{g}$. We show that in many of these cases the lower rank is actually 2.

---

*Partially supported by the Edmund Landau Center for Research in Mathematical Analysis and Related Areas, sponsored by the Minerva Foundation (Germany).

1991 *Mathematics Subject Classification:* Primary 20E18, 17B50; Secondary 20F40, 17B67.

1 Introduction

In the theory of pro-p groups the class of p-adic analytic groups is rather well understood. Much less is known on other classes of pro-p groups. Lubotzky and Mann proved in [LM] that the lower rank of a p-adic analytic pro-p group coincides with the minimal number of generators of its p-adic Lie algebra. They asked if a pro-p group with finite lower rank is it necessarily p-adic analytic.

In [LSh] Lubotzky and Shalev initialized a systematic study of another class of pro-p groups, the Λ-standard ones, where Λ is a complete commutative Noetherian local ring. In particular they gave a negative answer to the question above. In this paper we will focus on the case where $\Lambda = F_p[[t]]$, the ring of formal power series over a field of p elements, and study the lower rank of such groups.

We say that G is an $F_p[[t]]$**-standard group**, if for some fixed d, G equals as a set to all the d-tuples over $tF_p[[t]]$, the maximal ideal of $F_p[[t]]$, with a group law arising from a formal group defined over $F_p[[t]]$. This means that the multiplication in the group is expressed by a fixed power series.

We recall some basic properties and definitions of $F_p[[t]]$-standard groups. For more detailed background we refer the reader to [LSh]. Let G be an $F_p[[t]]$-standard group, with d as above. The set of d-tuples over $t^nF_p[[t]]$ has a natural structure of a subgroup of G, and we denote this subgroup G_n. Recall Lemma 2.5 from [LSh]:

Lemma 1.1. *For positive integers n, m we have:*
(1) G_n is a normal subgroup of G.
(2) G_n/G_{n+1} is a finite elementary abelian p-group.
(3) $(G_n, G_m) \subseteq G_{n+m}$.
(4) $(G_n)^p \subseteq G_{pn}$.
(5) G equals to the inverse limit of G/G_n.

Corollary 1.2. *Every $F_p[[t]]$-standard group is a pro-p group.*

It is worthwhile mentioning that $F_p[[t]]$-standard groups are not p-adic analytic.

Denote $L_n = G_n/G_{n+1}$, and $L(G) = \oplus_{n\geq 1} L_n$. $L(G)$ has a natural structure of a Lie algebra over F_p, where for homogeneous elements $[xG_{n+1}, yG_{m+1}] = (x, y)G_{n+m+1}$. It can be shown that $L(G) = \mathfrak{g} \otimes tF_p[t]$, where $\mathfrak{g}$ is a finite dimensional Lie algebra over F_p.

We call G $F_p[[t]]$**-simple (perfect) group** if $\mathfrak{g}$ is a simple (perfect) Lie algebra. The basic example of $F_p[[t]]$-perfect group is the first congruence subgroup of $SL_d(F_p[[t]])$, where $d \neq 2$ or $p \neq 2$. There the nth congruence subgroup is:

$$G_n = SL_d^n(F_p[[t]]) = Ker(G \to SL_d(F_p[[t]]/t^n F_p[[t]])) \ \ (n \geq 1).$$

It is not hard to see that

$$L(G_1) \cong \mathfrak{g} \otimes_{F_p} tF_p[t] \cong \mathfrak{sl}_d(tF_p[t]), \tag{1}$$

as Lie algebras, where $\mathfrak{g} = \mathfrak{sl}_d(F_p)$. We should mention here that a definition of Λ-simple (perfect) groups can actually be made over more general rings Λ (see [LSh]).

Let G be an $F_p[[t]]$-simple group. Suppose $H \leq G$ is a closed subgroup of G. Notice that we can view

$$(H \cap G_n)G_{n+1}/G_{n+1} \subseteq G_n/G_{n+1} \cong \mathfrak{g}$$

as a subspace of $\mathfrak{g}$. We can associate with H a graded F_p-subalgebra of $L(G)$. This is done in the following way:

$$\oplus_{n\geq 1}(H \cap G_n)G_{n+1}/G_{n+1},$$

by abuse of notation we denote this subalgebra by $L(H)$. Notice that if $K \subset H$ are two closed subgroups then $L(K) \subset L(H)$ and

$$\log_p |H : K| = \dim_{F_p} L(H)/L(K).$$

In particular $|G : H| = \infty$ if and only if $L(H)$ has infinite codimension in $L(G)$.

Lubotzky and Shalev ([LSh], Theorem 4.6) gave a proof that Λ-perfect pro-p groups have finite lower rank. Their proof actually shows that in the case of $F_p[[t]]$-perfect groups the lower rank does not exceed $2\dim(\mathfrak{g})$.

Denote by $d(\mathfrak{g})$ the minimal number of generators of $\mathfrak{g}$ as a Lie algebra. We show the following:

Theorem 1.3. *Let G be an $F_p[[t]]$-simple group. If $L(G) = \mathfrak{g} \otimes tF_p[t]$, then the lower rank of G is at most $d(\mathfrak{g}) + 1$.*

We can use the same method to improve the bounds on the lower rank of Λ-simple groups in general, but the improvement is not significant as in the case of $F_p[[t]]$-simple groups, so we omit it.

Definition: Let $\mathfrak{g}$ be a simple Lie algebra over a field F. Let M be a graded Lie F-subalgebra of infinite index of $\mathfrak{g} \otimes tF[t]$. We say that M is **weakly maximal** if the only graded F-subalgebras that contain M are M itself and F-subalgebras of $\mathfrak{g} \otimes tF[t]$ of finite codimension.

Remark: Note that since $\mathfrak{g} \otimes tF[t]$ is finitely generated, every graded subalgebra of infinite codimension can be extended to a weakly maximal subalgebra.

The main tool in the proof of Theorem 1.3 is the classification of weakly maximal subalgebras of $\mathfrak{g} \otimes tF[t]$, which was obtained in a joint work with Shalev and Zelmanov (see [BShZ]).

Kuranishi proved that for a simple Lie algebra $\mathfrak{g}$ over $\mathbb{C}$, $d(\mathfrak{g}) = 2$ (see [Ku]). Classical simple Lie algebras in the modular case have the same structure theory as simple Lie algebras over $\mathbb{C}$, see Seligman [Se] Chapter 2 for more details. Using Kuranishi's idea we prove the following theorem.

Theorem 1.4. *Let $\mathfrak{g}$ be a classical simple Lie algebra over F_p, where $p > 3$. Then $d(\mathfrak{g}) \leq 4$. In the cases where $\mathfrak{g} = \mathfrak{sl}_d(F_p)$ or $p > r^2 + r(r-1)/2$, where r is the dimension of the Cartan subalgebra of $\mathfrak{g}$, $d(\mathfrak{g}) = 2$.*

We remark here that except in the case where the Dynkin diagram of $\mathfrak{g}$ is of type G_2 the theorem is also true for $p = 3$.

Corollary 1.5. *Let G be an $F_p[[t]]$-simple group such that $L(G) = \mathfrak{g} \otimes tF_p[t]$. If $\mathfrak{g}$ is a classical simple Lie algebra, and $p > 3$ then the lower rank of G is at most 5. In in the case where $p > r^2 + r(r-1)/2$, where r is the dimension of the Cartan subalgebra of $\mathfrak{g}$ the lower rank of G is at most 3.*

In fact we can improve this as follows:

Theorem 1.6. *Let G be an $F_p[[t]]$-simple group such that $L(G) = \mathfrak{g} \otimes tF_p[t]$. If $\mathfrak{g}$ is a classical simple Lie algebra, and $p > r^2 + r(r-1)/2$, where r is the dimension of the Cartan subalgebra of $\mathfrak{g}$ then the lower rank of G is 2.*

The following corollary settles Lubotzky's and Shalev's question whether the lower rank of $SL_2^1(F_p[[t]])$ is 2 or 3.

Corollary 1.7. *If $p > 2$ then the lower rank of $SL_2^1(F_p[[t]])$ is 2.*

We remark that the lower rank of another famous pro-p group, the Nottingham group, is known to be 2 when $p > 3$, see [Sh]. This can be proved using very similar arguments as ours.

2 Weakly maximal subalgebras of $\mathfrak{g} \otimes tF[t]$

Let $\mathfrak{g}$ be a finite dimensional simple Lie algebra over F. The centroid, $\mathrm{Cent}(\mathfrak{g})$, of $\mathfrak{g}$ consists of all elements $T \in \mathrm{End}_F(\mathfrak{g})$ satisfying:

$$[T(x), y] = T([x, y]) \qquad (x, y \in \mathfrak{g}).$$

It is not hard to see that $\mathrm{Cent}(\mathfrak{g})$ is a finite field extension of F. In particular in the case of F_p, $\mathrm{Cent}(\mathfrak{g}) = F_q$, where $q = p^e$.

Definition. Let k be a positive integer, and let $\mathfrak{g} = \oplus_{i=0}^{k-1} \mathfrak{g}_i$ be a $\mathbb{Z}_k$-grading of $\mathfrak{g}$ (where $\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$). Let α be the k-tuple $(\mathfrak{g}_0, \ldots, \mathfrak{g}_{k-1})$. Define

$$L(\mathfrak{g}, k, \alpha) = \oplus_{n \in \mathbb{N}} \mathfrak{g}_{n \bmod k} \otimes t^n.$$

We allow the trivial $\mathbb{Z}_k$-grading $\alpha = (\mathfrak{g}, 0, \ldots, 0)$. It is not hard to see that $L(\mathfrak{g}, k, \alpha)$ is a graded F-subalgebra of $\mathfrak{g} \otimes tF[t]$ which is of infinite codimension.

Below is the classification of weakly maximal subalgebras of $\mathfrak{g} \otimes tF[t]$ which was obtained in a joint work with Shalev and Zelmanov (see [BShZ, §4]).

Theorem 2.1. *Let F be any field and let $\mathfrak{g}$ be a simple finite-dimensional Lie algebra over F. Let M be a weakly maximal subalgebra of $\mathfrak{g} \otimes tF[t]$. Denote the centroid of $\mathfrak{g}$ by K. Then one of the following holds:*

(i) $M = \mathfrak{h} \otimes tF[t]$, where $\mathfrak{h}$ is a maximal subalgebra of $\mathfrak{g}$.

(ii) For some $\lambda \in K^*$ and a maximal subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ satisfying $K \cdot \mathfrak{h} = \mathfrak{g}$ we have $M = \oplus_{n \in \mathbb{N}} \lambda^n \mathfrak{h} \otimes t^n$.

(iii) $M = L(\mathfrak{g}, q, \alpha)$ for some prime q and a $\mathbb{Z}_q$-grading α of $\mathfrak{g}$.

Definition. Let $M = \oplus_{n \in \mathbb{N}} M_n \otimes t^n$ be a graded subalgebra of $\mathfrak{g} \otimes tF[t]$. We say that M is **periodic** if there is k such that for all n $M_n = M_{n+k}$.

Lemma 2.2. *Suppose $\mathfrak{g}$ is defined over a finite field F_p. Then every weakly maximal subalgebra $M = \oplus_{n\in\mathbb{N}} M_n \otimes t^n$ of $\mathfrak{g} \otimes tF_p[t]$ is periodic. Moreover in the case where M is of type (ii) or (iii) the minimal period k exceeds 1. If $(n-m) \neq 0 \bmod k$, then $M_n \cap M_m = 0$.*

Proof. Surely the argument holds for weakly maximal subalgebras of type (i) and (iii). Suppose the subalgebra is of type (ii). Then there is a minimal integer k such that $\lambda^k \in F_p$, which implies that the subalgebra has period k. Suppose $M_n \cap M_m \neq 0$. Then there are $x, y \in \mathfrak{g}$ such that $\lambda^n x = \lambda^m y$. Since $\mathfrak{g}$ is simple the adjoint represention is faithful. Therefore we can view $\mathfrak{g}$ as a matrix algebra, and in particular we can assume x, y are matrices. Either $x = y = 0$ or if we view x and y as matrices there are i, j such that the i, j entry of $\lambda^n x$ is not trivial and equals the i, j entry of $\lambda^m y$. But $x_{i,j}, y_{i,j} \in F_p$, which implies that $\lambda^{n-m} \in F_p$. Since k is minimal we deduce that k divides $n - m$. □

3 The lower rank of $F_p[[t]]$-simple groups

Recall that the lower rank of a profinite group G is

$$\liminf\{d(H) | H \leq_o G\},$$

where $H \leq_o G$ means that H is an open subgroup of G and $d(H)$ denote the minimal number of generators of H as a topological group.

Proof of Theorem 1.3: Set $d = d(\mathfrak{g})$. Let $x_1, \ldots, x_d \in \mathfrak{g}$ be a set of generators of $\mathfrak{g}$. Given $N > 0$, set $n_1 = \cdots = n_d = N$, $x_{d+1} = x_1$, and $n_{d+1} = N + 1$. First we show that $x_1 \otimes t^{n_1}, \ldots, x_{d+1} \otimes t^{n_{d+1}}$ generate a subalgebra of finite index. Suppose they do not. Then they lie in a graded subalgebra of infinite index. Therefore they lie in a weakly maximal subalgebra $M = \oplus M_n \otimes t^n$. We now apply Theorem 2.1. Since $x_1, \ldots, x_d$ generate $\mathfrak{g}$ M cannot be of type (i). Therefore M has period $k > 1$. Since $0 \neq x_1 \in M_N \cap M_{N+1}$ by Lemma 2.2 k divide $1 = N + 1 - N$, a contradiction.

Now for each i we can find $g_i \in G_{n_i}$ such that $g_i G_{n_i+1}/G_{n_i+1} = x_i \otimes t^{n_i}$. Let H be the closed subgroup generated by the g_i's. Since $x_1 \otimes t^{n_1}, \ldots, x_{d+1} \otimes t^{n_{d+1}} \in L(H)$, we see that $L(H)$ is of finite codimension. This implies that H is of finite index, i.e. open. Notice that $H \subset G_N$ and H is generated by k elements. Since G_n form a base to the neighborhoods of the identity the result follows.

□

Proof of Theorem 1.4: We start with case where $p > r^2 + r(r-1)/2$. Since $\mathfrak{g}$ is classical we can write $\mathfrak{g} = H \oplus (\oplus_{\alpha\in\Phi}\mathfrak{g}_\alpha)$, where H is a maximal toral subalgebra of $\mathfrak{g}$, Φ a root system, and $\mathfrak{g}_\alpha$ is one dimensional. Let $\Delta \subset \Phi$ be a base of the root system, notice $|\Delta| = r$. For each $\alpha \in \Phi$ set $0 \neq x_\alpha \in \mathfrak{g}_\alpha$.

Let α be a positive root. Then there is a sequence of roots of the form $\beta_1 = \alpha_{i_1}$, and for $1 < j \leq k$ $\beta_j = \beta_{j-1} + \alpha_{i_j}$, where $\beta_k = \alpha$, and $\alpha_{i_j} \in \Delta$ [Se, Lemma II.5,2]. If $\alpha, \beta, \alpha+\beta$ are non-zero roots then $[\mathfrak{g}_\alpha, \mathfrak{g}_\beta] = \mathfrak{g}_{\alpha+\beta}$ [Se, Lemma II.4.1]. We conclude that the elements $\{x_\alpha\}_{\alpha\in\pm\Delta}$ generate $\mathfrak{g}$.

We wish to find $h \in H$ such that if $\alpha \neq \beta \in \pm\Delta$ then $\alpha(h) \neq \beta(h)$. That is equivalent to $(\alpha+\beta)(h) \neq 0$, where $\alpha, \beta \in \Delta$, and $(\alpha-\beta)(h) \neq 0$, where $\alpha \neq \beta \in \Delta$. The first condition means that h is not in the kernel of r^2 functionals. The second means that h is not in the kernel of $r(r-1)/2$ functionals (we divide by 2 because the kernel of $\alpha - \beta$ is the same as the kernel of $\beta - \alpha$). Since $p > r^2 + r(r-1)/2$ we can find such $h \in H$.

Set $x = \sum_{\alpha\in\pm\Delta} x_\alpha$. Notice that $\mathrm{ad}_h^k(x) = \sum_{\alpha\in\pm\Delta} \alpha(h)^k x_\alpha$. Let us look at a matrix $2r$ by $2r$, where the rows are labeled by the roots in $\pm\Delta$. Suppose we let the α, k entry to be equal to $\alpha(h)^k$, we get a Vandermonde's matrix. We deduce that a subalgebra that contains x and h also contains $\{x_\alpha\}_{\alpha\in\pm\Delta}$. Therefore x and h are generators of $\mathfrak{g}$.

We point out the fact that $\mathrm{ad}_h^{p-1}(x) = x$, since $\alpha(h)^{p-1} = 1$ for all α.

Now suppose $\mathfrak{g} = \mathfrak{sl}_d(F_p)$. We view $\mathfrak{g}$ in the standard way as d by d matrices with trace zero. Set $e_{i,j}$ to be the d by d matrix such that the (i,j) entry of it is one and all other entries are zero. Set $h = e_{1,1} - e_{2,2}$ and $x = \sum_{i=1}^{d-1}(e_{i,i+1} + e_{i+1,i})$. Notice that

$$[h, e_{1,2}] = 2e_{1,2}, \quad [h, e_{2,1}] = -2e_{2,1}, \quad [h, e_{2,3}] = e_{2,3}, \quad [h, e_{3,2}] = -e_{3,2},$$

and $[h, e_{i,i+1}] = [h, e_{i+1,i}] = 0$ for $i > 2$.

Since $p > 3$ the elements $1, -1, 2, -2$ are distinct. Using again the argument with Vandermonde's matrix we deduce that $\mathfrak{h}$ the subalgebra of $\mathfrak{g}$ which is generated by x, h contains $e_{1,2}, e_{2,1}, e_{2,3}, e_{3,2}$, and $\sum_{i=3}^{d-1}(e_{i,i+1}+e_{i+1,i})$. This implies that $e_{2,2} - e_{3,3} = [e_{2,3}, e_{3,2}] \in \mathfrak{h}$. Continuing by induction with $e_{2,2} - e_{3,3}$ and $\sum_{i=3}^{d-1}(e_{i,i+1} + e_{i+1,i})$ we conclude that for all i $e_{i,i+1}, e_{i+1,i} \in \mathfrak{h}$, hence $\mathfrak{h} = \mathfrak{g}$.

Finely we deal with the general case where $\mathfrak{g}$ is classical with no restrictions. Let Φ and Δ be as above. If the Dynkin diagram of Φ is of type

G_2 the result follows since $|\Delta| = 2$. Otherwise we view the possible Dynkin diagrams. We see that in all cases there is one root $\alpha \in \Delta$ such that by removing α we get a root system isomorphic to A_n for some n. Since A_n is the root system of $\mathfrak{sl}_{n+1}(F_p)$ we see that there is a subalgebra generated by two elements that contains $\pm\Delta$ except $\pm\alpha$. Adding $\pm\alpha$ finishes the proof. □

Proof of Theorem 1.6: Suppose $p > r^2 + r(r-1)/2$. Let x, h be as in the first part of the proof of Theorem 1.4. Given $N > 0$. As in the proof of Theorem 1.3 it is enough to show that $h \otimes t^N$ and $(h+x) \otimes t^{N+1}$ are not contained in a weakly maximal subalgebra. Since h and $h+x$ are generators of $\mathfrak{g}$ we only have to deal with weakly maximal subalgebras of type type (ii) or (iii).

Suppose $h \otimes t^N, (h+x) \otimes t^{N+1} \in M$ a weakly maximal subalgebra. We see that

$$\mathrm{ad}_h(h+x) \otimes t^{2N+1} = \mathrm{ad}_h(x) \otimes t^{2N+1}$$

lies in M. By induction for all $k \geq 1$

$$\mathrm{ad}_h^k(h+x) \otimes t^{(k+1)N+1} = \mathrm{ad}_h^k(x) \otimes t^{(k+1)N+1}$$

lies in M.

Recall that $\mathrm{ad}_h^{p-1}(x) = x$. Therefore

$$\mathrm{ad}_h^{p-1}(x+h) \otimes t^{pN+1} = x \otimes t^{pN+1}$$

and

$$\mathrm{ad}_h^p(x+h) \otimes t^{(p+1)N+1} = \mathrm{ad}_h(x) \otimes t^{(p+1)N+1}$$

lie in M. Therefore

$$\mathrm{ad}_{h+x}(x) \otimes t^{pN+1+N+1} = ad_h(x) \otimes t^{(p+1)N+2}$$

lies in M. From Lemma 2.2 we conclude that the period of M must divide $((p+1)N+2) - ((p+1)N+1) = 1$. This is a contradiction because the periods of subalgebras of type (ii) and (iii) are strictly greater than 1. □

Proof of Corollary 1.7: Recall that $\mathfrak{g}$ the Lie algebra associated with $SL_2^1(F_p[[t]])$ is $\mathfrak{sl}_2(F_p)$. Notice that r the dimension of the Cartan subalgebra of $\mathfrak{sl}_2(F_p)$ is one. The assertion follows from Theorem 1.6. □

Acknowledgment. I wish to thank Aner Shalev for his helpful comments on earlier drafts of this paper.

References

[BShZ] Y. Barnea, A. Shalev and E.I. Zelmanov, Graded subalgebras of affine Kac-Moody algebras, to appear in *Israel J. Math.*

[Ku] M. Kuranishi, On everywhere dense imbedding of free groups in Lie groups, *Nagoya Math. J.* **2** (1951), 63–71.

[LM] A. Lubotzky and A. Mann, Powerful p-groups. I, II. *J. Algebra* **105** (1987), 484–515.

[LSh] A. Lubotzky and A. Shalev, On some Λ-analytic pro-p groups, *Israel J. Math.* **85** (1994), 307–337.

[Se] G.B. Seligman, *Modular Lie Algebras*, Springer, Berlin, 1967.

[Sh] A. Shalev, Some problems and results in the theory of pro-p groups, in *Groups '93 Galway/St. Andrews*, Vol 2 (London Math. Soc. Lecture note Series **212**, Cambridge University Press, Cambridge, 1995) 528–542.