

# Congruence subgroup growth of arithmetic groups in positive characteristic

Miklós Abért  
Nikolay Nikolov  
Balázs Szegedy

## Abstract

We prove a new uniform bound for subgroup growth of a Chevalley group  $G$  over the local ring  $\mathbb{F}[[t]]$  and also over local pro- $p$  rings of higher Krull dimension. This is applied to the determination of congruence subgroup growth of arithmetic groups over global fields of positive characteristic. In particular we obtain that the subgroup growth of  $SL_n(\mathbb{F}_p[[t]])$  ( $n \geq 3$ ) is of type  $n^{\log n}$ . This was one of the main problems left open by Alex Lubotzky in his article [7].

The essential tool for proving the results is the use of graded Lie algebras. We sharpen Lubotzky's bounds on subgroup growth via a result on subspaces of a Chevalley Lie algebra  $L$  over a finite field  $\mathbb{F}$ . The proof of this theorem is by algebraic geometry and can be modified to obtain a lower bound on the codimension of proper Lie subalgebras of  $L$ .

## 1 Introduction

Let  $p$  be a prime and  $K$  be a global field of characteristic  $p$ .  $K$  is a finite extension of  $F(t)$  where  $F$  is the field of  $p$  elements.  $\mathcal{V}$  is the set of equivalence classes of non-archimedean valuations of  $K$  and for a finite subset  $S$  of  $\mathcal{V}$ ,  $\mathcal{O}_S$  is the ring of  $S$ -integers  $\{x \in K \mid v(x) \geq 0, \forall v \in \mathcal{V} \setminus S\}$ .

For each Dynkin diagram  $X \in \{A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4, G_2\}$  there is a group scheme  $X(-)$  of algebraic groups of universal Chevalley type  $X$ . Throughout the paper we make the restriction that if  $p = 2$  then  $X \neq A_1, C_l$ .

Let  $\Gamma = X(\mathcal{O}_S)$ . A group  $G \leq X(K)$  is called *arithmetic* if it is commensurable with  $\Gamma$ , i.e., if  $G \cap \Gamma$  has finite index in both  $G$  and  $\Gamma$ . A subgroup  $H \leq G$  is called a *congruence subgroup* if it contains

$$\Gamma(\mathfrak{m}) = \ker(\Gamma \rightarrow X(\mathcal{O}_S/\mathfrak{m}))$$

for some ideal  $\mathfrak{m}$  of  $\mathcal{O}_S$ .

Let  $\gamma_n(G)$  be the number of congruence subgroups of  $G$  of index  $\leq n$ . We are interested in the growth of the series  $\gamma_n(G)$ . Since  $G$  and  $\Gamma$  are commensurable it is easy to see that there are two constants  $a_1, a_2$  such that

$$a_1 \log \gamma_n(G) \leq \log \gamma_n(\Gamma) \leq a_2 \log \gamma_n(G)$$

So we can restrict ourselves to investigating  $\gamma_n(\Gamma)$ .

In the pioneering article [7] (see also [5], Chapter 6) Lubotzky proved the existence of two constants  $a, b$  (depending on  $\Gamma$ ) such that

$$n^{a \log n} \leq \gamma_n(\Gamma) \leq n^{b(\log n)^2}$$

We obtain the following improvement of the upper bound.

**Theorem 1** *Assuming  $X \neq A_1, C_l$  when  $p = 2$ , there is a constant  $C = O(l)$  which depends only on the Lie rank  $l$  of  $X$ , such that*

$$\gamma_n(\Gamma) \leq n^{C \log n}$$

Our theorem complements the result of Lubotzky [7] who showed that if  $\Gamma$  is an arithmetic group in characteristic 0, then  $\gamma_n(\Gamma)$  grows like  $n^{\frac{\log n}{\log \log n}}$ .

Interest in counting congruence subgroups arose in connection with the problem of characterising groups of polynomial subgroup growth.

Whenever the Congruence Subgroup Property holds for  $\Gamma$ , as in the case of  $SL_n(F_p[t])$  ( $n \geq 3$ ), the subgroup growth is equal to the congruence subgroup growth.

The congruence subgroups of  $X(\mathcal{O}_S)$  correspond to the open subgroups of its congruence completion  $\tilde{\Gamma}$ . Denote by  $\hat{\mathcal{O}}_S$  the profinite completion of the ring  $\mathcal{O}_S$ . Then by the strong approximation theorem

$$\tilde{\Gamma} \simeq X(\hat{\mathcal{O}}_S) \simeq \prod_{v \in \mathcal{V} \setminus S} X(\mathcal{O}_v)$$

where  $\mathcal{O}_v$  is the completion of  $\mathcal{O}_S$  at  $v$ . Thus it is necessary to understand the local factors  $X(\mathcal{O}_v)$  first.

Fix valuations  $v_1, \dots, v_r$  and put  $G_i = X(\mathcal{O}_{v_i})$ . The group  $G_i(k)$  is defined as the  $k$ -th congruence subgroup of  $G_i$  with respect to the unique maximal ideal  $m_i$  of  $\mathcal{O}_{v_i}$ , i.e.  $G_i(k) = \{x \in G_i \mid x \equiv 1 \pmod{m_i^k}\}$ . We define

$$G = \prod_{i=1}^r G_i, \quad G(k) = \prod_{i=1}^r G_i(k)$$

Here  $G(1)$ , the first congruence subgroup of  $G$  is an  $F[[t]]$ -analytic pro- $p$  group, which is in fact  $F[[t]]$ -perfect (cf. [6] definition 3.1 and [3] Chap. 13).

For a pro  $p$ -group  $B$  let  $s_{p^k}(B)$  be the number of open subgroups of  $B$  of index at most  $p^k$ . If  $B$  is  $F[[t]]$ -perfect, then by a result of Lubotzky and Shalev [6] there exists a constant  $C$  depending on  $B$  such that  $s_{p^k}(B) \leq p^{Ck^2}$ .

For the  $F[[t]]$ -analytic Chevalley group  $G(1)$  considered above we obtain the following improvement.

**Theorem 2** *Let  $m$  be the dimension of  $G(1)$  as an  $F[[t]]$ -analytic group. Then*

$$s_{p^k}(G(1)) \leq p^{\frac{7}{2}k^2 + mk}$$

What is new here is that the leading term is an absolute constant. Theorem 2 can be generalised to rings of higher Krull dimension, see Section 4.

A crucial ingredient in the proof of Theorem 2 is the following result which is interesting in itself.

Let  $F_i$  be finite extensions of the ground field  $F$  for  $1 \leq i \leq k$ . Let  $L_i$  be the Chevalley Lie algebra of type  $X$  over the field  $F_i$  and let  $L = \oplus_i L_i$ . For the  $F$ -subspaces  $U, V \subseteq L$  we define the  $F$ -subspace

$$[U, V] := F\langle [u, v] \mid u \in U, v \in V \rangle$$

**Theorem 3** *For every pair of  $F$ -subspaces  $U, V \subseteq L$  we have*

$$\dim L/[U, V] \leq 2(\dim L/U + \dim L/V)$$

We use algebraic geometric tools to obtain Theorem 3. Using the proof we can easily get an estimate on the maximal dimension of proper subalgebras of classical Lie algebras.

**Theorem 4** *Let  $T$  be an arbitrary field of characteristic  $p \neq 2, 3, 5$  and let  $L$  be a Chevalley Lie algebra of rank  $l$  over  $T$ . Suppose  $M \subset L$  is a proper Lie subalgebra. Then*

$$\text{codim } M \geq l - \dim Z(L)$$

We note that in their paper [2] Barnea and Shalev state that for subalgebras of  $sl_{l+1}(T)$  the bound  $\text{codim } M \geq l$  holds, but if  $p$  divides  $l+1$ , their proof, like ours, gives only  $l-1$ . Our approach works for the other Chevalley types as well and is quite short.

We note that Theorem 4 implies that there is a gap in the Hausdorff spectrum of the group  $G = X(F[[t]])$  (see Section 5 for the details).

The structure of the rest of the paper is as follows. Section 2 derives Theorem 1 from Theorem 2, Section 3 contains the proof of Theorem 2 modulo Theorem 3, while Section 4 generalizes Theorem 2 to rings of higher Krull dimension. The final section contains the proof of Theorems 3 and 4.

## 2 The global case: $X(\mathcal{O}_S)$

Now we will prove Theorem 1. Our proof basically follows the one in [7], Section 4, pp 288-290 until the last step where we apply Theorem 2.

**Proof of Theorem 1.** Let  $d = \dim X$  be the dimension of the algebraic group scheme  $X$ . It is also the dimension of the  $F$ -Lie algebra  $L_0$  associated to  $X$ .

We use the following proposition due to Pyber and Shalev [9]:

**Proposition 5** *There is a constant  $c = O(l)$  which depends only on the lie rank  $l$ , such that for each open subgroup  $H$  of index at most  $n$  in  $\tilde{\Gamma}$  there is a subnormal subgroup  $H_1 < \tilde{\Gamma}$  such that  $H_1 \leq H \leq \tilde{\Gamma}$  and*

$$[\tilde{\Gamma} : H_1] \leq [\tilde{\Gamma} : H]^c \leq n^c$$

Further, it is shown in [7] that there is a finite set of valuations  $A = \{v_1, v_2, \dots, v_r\}$  such that

$$\prod_{v \in \mathcal{V} \setminus A} X(\mathcal{O}_v) \subseteq H_1$$

and we choose  $A$  to be minimal set with this property. Thus  $H_1$  and  $H$  can be identified with their intersections with the direct summand  $G$  of  $\tilde{\Gamma}$ , where

$$G = G_A := \prod_{i=1}^r X(\mathcal{O}_{v_i})$$

The filtration  $G \geq G(1) \geq G(2) \geq \dots$  has been defined Section 1. Recall that  $m_i$  is the maximal ideal of  $\mathcal{O}_{v_i}$ . Put  $\mathfrak{m}_i = \mathcal{O}_S \cap m_i$ . Then  $\mathcal{O}_S/\mathfrak{m}_i \simeq \mathcal{O}_{v_i}/m_i \simeq F_i$ , the finite field of  $p^{e_i}$  elements which is a finite extension of  $F$ . Let  $L$  be the Lie algebra  $\oplus_i L_i$  defined as in the introduction for these fields  $F_i$ .

Now we use Theorem 2 and deduce that the number  $s_{p^k}(G(1))$  of subgroups of index  $\leq p^k$  in  $G(1)$  is at most

$$s_{p^k}(G(1)) \leq p^{\frac{7}{2}k^2 + mk}$$

where  $m = \dim L = d(e_1 + e_2 + \dots + e_r)$ . We define

$$\tilde{G} = G/G(1) = \prod_i X(\mathcal{O}_{v_i}/m_i) = \prod_{i=1}^r X(F_i).$$

This is a quasi-semisimple group of size about  $p^m$ .

Now let  $H$  be a subgroup of  $G$  of index at most  $n$  and let  $H_1$  be as above. From the argument in [7, Lemma 4.7 and the argument after] it follows that  $H_1G(1)/G(1)$  lies in the centre of  $\tilde{G}$ . So

$$|\tilde{G}/Z(\tilde{G})| \leq [G : H_1] \leq n^c.$$

$|Z(\tilde{G})|$  is negligible compared to  $|\tilde{G}|$  so by enlarging the constant  $c$  slightly we can assume that  $|\tilde{G}| \leq n^c$ . But  $p^m$  is approximately  $|\tilde{G}|$  so by another slight enlargement of  $c$  we have  $p^m \leq n^c$  whence  $m \leq c \log_p n$ .

We want to estimate the number of subgroups  $H \leq G$  of index at most  $n$ . Put  $Q = G(1)H$  and  $P = G(1) \cap H$ . Then  $[G : Q][G(1) : P] = [G : H] \leq n$ . Now  $G/G(1)$  is a group of size at most  $n^c$ , so there are at most  $|G/G(1)|^{2 \log n} \leq n^{2c \log n}$  possibilities for the subgroup  $Q/G(1)$  of index  $[G : Q] \leq n$ . Here we use the result of Pyber [8] saying that for a finite group  $G$  we have

$$s_n(G) \leq |G|^{2 \log n}$$

Also  $[G(1) : P] \leq n$  so there are at most

$$p^{\frac{7}{2}(\log_p n)^2 + m \log_p n} = n^{\frac{7}{2} \log_p n + m}$$

possibilities for  $P$  in  $G(1)$ .

Having chosen  $P$  and  $Q$  then  $H/P \simeq Q/G(1)$  is a complement to  $N_{G(1)}(P)/P$  in  $N_Q(P)/P$  and the number of those is at most

$$|\text{Der}(Q/G(1), N_{G(1)}(P)/P)| \leq n^{c \log n}$$

since  $Q/G(1)$  can be generated by at most  $\log |Q/G(1)| \leq c \log n$  elements and  $|N_{G(1)}(P)/P| \leq [G(1) : P] \leq n$ . Hence the total number of possibilities for  $H \leq G$  of index  $n$  is at most

$$n^{2c \log n} n^{m + \frac{7}{2} \log_p n} n^{c \log n}$$

Now using  $m \leq c \log_p n$  we have

$$s_n(G) \leq n^{2c \log n} n^{c \log_p n + \frac{7}{2} \log_p n} n^{c \log n} \leq n^{(4c + \frac{7}{2}) \log n}.$$

It remains to estimate the number of subsets  $A \subset \mathcal{V}$  with  $p^m \leq n^c$ . The valuation  $v_i$  is determined by the prime ideal  $\mathfrak{m}_i$  in  $\mathcal{O}_S$  of index at most  $p^{e_i}$ . Therefore the set  $A$  is determined by the ideal  $\mathfrak{m}_1 \mathfrak{m}_2 \dots \mathfrak{m}_r$  of index  $I \leq p^{e_1 + \dots + e_k} = p^{m/d} \leq n^{c_1}$  where  $c_1$  is an absolute constant (since  $c = O(\sqrt{d})$ ). There are at most  $I$  choices for the ideal  $\mathfrak{m}_1 \mathfrak{m}_2 \dots \mathfrak{m}_r \cap F[t]$  and then there are at most  $c_2^{\log I}$  choices for  $\mathfrak{m}_1 \mathfrak{m}_2 \dots \mathfrak{m}_r \triangleleft \mathcal{O}_S$  where  $c_2 = [K : F(t)]$ . So the number of subsets  $A$  of valuations is bounded from above by  $n^{c_1} c_2^{c_1 \log n} < n^{c_3}$  for some absolute constant  $c_3$ . Thus with  $C = 4c + \frac{7}{2} = O(l)$  we have

$$s_n(\Gamma) \leq n^{c_3 + C \log n},$$

the statement we wanted to prove.  $\square$

Observe that if  $G_1$  is as above, by a result of Shalev [10]  $\gamma_n(G_1) > n^{\frac{1}{8} \log n}$  for infinitely many  $n$  and the same is therefore true for  $\gamma_n(\Gamma)$ . We conjecture that there is a uniform bound  $\gamma_n(\Gamma) < n^{C \log n}$  where  $C$  is an absolute constant for all Lie types  $X$ . The presence of  $c = O(l)$  in our proof comes from the application of Proposition 5. Further progress on this must therefore involve a more delicate reduction to  $G(1)$  than Proposition 5.

### 3 The local case: $G(1)$ and its graded Lie algebra

Recall that  $F$  is the field of  $p$  elements,  $L_0 = L_F$ ,  $L_i = L_{F_i} = L_0 \otimes_F F_i$  and  $L = \bigoplus_i L_i$ . We define  $\mathcal{L} := L \otimes_F tF[t]$ . The bracket in  $\mathcal{L}$  is given by

$$[a \otimes t^n, b \otimes t^m] = [a, b] \otimes t^{n+m}$$

Then in the notation of [3] Chapter 13,  $\mathcal{L}$  is isomorphic to the graded Lie algebra of  $G(1)$  associated to the filtration  $G(1) > G(2) > \dots$ :

$$\mathcal{L} \simeq \text{gr}(G(1)) = \bigoplus_{i=1}^{\infty} G(i)/G(i+1).$$

See [3, Example 11, pp 353].

Open subgroups of  $H \leq G(1)$  correspond to Lie subalgebras

$$L(H) = \bigoplus_{i=1}^{\infty} (HG(i+1) \cap G(i)/G(i+1))$$

of finite codimension in  $\mathcal{L}$  and such that  $\dim \mathcal{L}/L(H) = \log_p[G(1) : H]$

Suppose now  $\mathcal{K} = L(H)$  is a Lie subalgebra corresponding to an open subgroup  $H < G(1)$ . Now  $m = \dim L$  is also the dimension of  $G(1)$  as an  $F[[t]]$ -analytic group. Using Theorem 3 we can deduce

**Lemma 1** *Let  $\mathcal{K}$  be a Lie subalgebra of finite codimension in  $\mathcal{L}$ . Then*

$$\dim \mathcal{K}/\mathcal{K}' \leq m + 7 \dim \mathcal{L}/\mathcal{K}$$

where  $\mathcal{K}' = [\mathcal{K}, \mathcal{K}]$ .

**Proof** Every  $a \in \mathcal{L}$  can be written uniquely in as

$$a = \sum_{s=1}^{\infty} a_s \otimes t^s \quad \text{with } a_s \in L$$

We define the leading term  $l(a) := a_s$  where  $s$  is the least integer such that  $a_s \neq 0$  and we call this  $s$  the degree  $\deg(a)$  of  $a$ . Put

$$K_i := \langle l(a) \mid a \in \mathcal{K} \text{ with } \deg(a) = i \rangle$$

Therefore

$$\dim \mathcal{L}/\mathcal{K} = \sum_{i=1}^{\infty} \dim L/K_i$$

and from the finiteness of  $\dim \mathcal{L}/\mathcal{K}$  the sum is assumed to be finite. We have

$$[K_i \otimes t^i, K_j \otimes t^j] = [K_i, K_j] \otimes t^{i+j} \subseteq K'_{i+j} \otimes t^{i+j}$$

where

$$K'_{i+j} = \langle l(a) \mid a \in \mathcal{K}', \deg(a) = i+j \rangle$$

and therefore  $\dim L/[K_i, K_j] \geq \dim L/K'_{i+j}$ . Adding up these inequalities for  $i = j$  and  $i = j + 1$  and using Theorem 3 we have

$$\begin{aligned} \dim \mathcal{L}/\mathcal{K}' &= \sum_{i=1}^{\infty} \dim L/K'_i \leq \dim L + \sum_{1 \leq i \leq j \leq i+1} \dim L/[K_i, K_j] \leq \\ &\leq m + \sum_{1 \leq i \leq j \leq i+1} 2(\dim L/K_i + \dim L/K_j) \leq m + 8 \dim \mathcal{L}/\mathcal{K} \end{aligned}$$

and therefore

$$\dim \mathcal{K}/\mathcal{K}' \leq m + 7 \dim \mathcal{L}/\mathcal{K},$$

the result we wanted to prove.  $\square$

From the definition of  $L(H)$  it is immediate that  $L(H)' = \mathcal{K}' \subseteq L(H')$  where  $H = [H, H]$ . Thus  $\log_p[H : H'] \leq \dim \mathcal{K}/\mathcal{K}'$  and we can state the following

**Corollary 1** *If  $H$  is an open subgroup of  $G(1)$  then  $\log_p[H : H'] \leq m + 7 \log_p[G(1) : H]$*

So  $d(H)$  (the number of topological generators of  $H$ ) is bounded linearly by  $\log_p[G(1) : H]$ :

$$d(H) = \log_p[H : \Phi(H)] \leq \log_p[H : H'] \leq m + 7 \log_p[G(1) : H] \quad (1)$$

(  $\Phi(H) = H^p H'$  denotes the Frattini subgroup of  $H$ .)

**Proof of Theorem 2** This follows word-for-word from the proof of Lemma 4.1 in [6]. For the sake of completeness we reproduce it here:

Suppose  $[G(1) : H] \leq p^k$ . Find a sequence  $H = H_k \leq H_{k-1} \leq \dots \leq H_0 = G(1)$  with  $[H_s : H_{s+1}] = 1$  or  $p$ . We have  $d(H_s) \leq m + 7s$  by (1). On the other hand  $\Phi(H_s) \leq H_{s+1} \leq H_s$  and  $H_s/\Phi(H_s) = F^{d(H_s)}$ , so  $H_{s+1}/\Phi(H_s)$  is a subspace of codimension at most 1 in  $H_s/\Phi(H_s)$ . Hence the number of choices for  $H_{s+1}$  given  $H_s$  is

$$1 + \frac{p^{d(H_s)} - 1}{p - 1} \leq p^{d(H_s)} \leq p^{m+7s}$$

so the number of possibilities for  $H = H_k$  is no more than

$$p^m p^{m+7} \dots p^{m+7(k-1)} < p^{\frac{7}{2}k^2 + mk},$$

the result we needed.  $\square$

## 4 Rings of higher Krull dimension

The argument we have given above about subgroup growth of  $F[[t]]$ -analytic groups of Chevalley type can be generalized to 'pro- $p$ ' rings of higher Krull dimension. More specifically, let  $R$  be a Noetherian commutative complete local ring with a unique maximal ideal  $I$  such that  $R/I \simeq \mathbb{F}$ , the finite field of  $q$  elements. We also assume that  $pR = 0$ .

**Example** Consider  $R = \mathbb{F}[[t_1, t_2, \dots, t_k]]$ , the ring of power series in the commuting variables  $t_1, t_2, \dots, t_k$  with  $I = (t_1, t_2, \dots, t_k)$ .

Let  $r = \dim_{\mathbb{F}} I/I^2$  and let  $r'$  be the Krull dimension of  $R$ . Then  $r' \leq r$  with equality if  $R$  is regular. Define

$$gr(R) := \bigoplus_{i=0}^{\infty} I^i/I^{i+1}, \quad I^0 = R.$$

and more generally

$$gr(I^k) := \bigoplus_{i=k}^{\infty} I^i/I^{i+1}$$

Let  $a_n = \dim_{\mathbb{F}} R/I^n$ ,  $b_n = a_{n+1} - a_n = \dim_{\mathbb{F}} I^n/I^{n+1}$ . The Hilbert-Serre theorem gives that  $a_n/n^{r'}$  tends to a constant as  $n \rightarrow \infty$ .

As before, let  $X$  be an algebraic group scheme of Chevalley groups and let  $G = X(R)$ . (For example  $G = SL_d(\mathbb{F}[[t]])$ ). We are interested in the subgroup growth of  $G_1$ , the first congruence subgroup of  $G$ . Then under our restrictions on  $p$  and  $X$   $G_1$  is an  $R$ -standard analytic group with filtration  $G_1 > G_2 > \dots$  where  $G_i = \ker X(R) \rightarrow X(R/I^i)$  (cf [6] definition 3.1). The graded Lie algebra of  $G_1$  is isomorphic to

$$\mathcal{L} = L \otimes_{\mathbb{F}} gr(I),$$

where  $L = L_{\mathbb{F}}$  is the Lie algebra of type  $X$  over  $\mathbb{F}$ . Let  $m = \dim_{\mathbb{F}} L$ . Since  $L$  is perfect the filtration  $\{G_i\}$  satisfies  $[G_i, G_j] = G_{i+j}$  and

$$L(G_k) = L \otimes_{\mathbb{F}} gr(I^k)$$

Hence  $[G_k : G_{k+1}] = p^{mb_n}$  and  $\log_p[G_1 : G_k] = m(a_k - a_1)$  and  $d(G_k) = \log_p[G_k : G_{2k}] = m(a_{2k} - a_k)$ . We have  $\frac{a_{2k}}{a_k} \rightarrow 2^{r'}$  so

$$\frac{d(G_k)}{\log_p[G_1 : G_k]} = \frac{a_{2k} - a_k}{a_k - 1} \rightarrow 2^{r'} - 1$$

as  $n \rightarrow \infty$ .

Now  $G_k/G_{2k}$  is an elementary  $p$ -group of order  $p^{m(a_{2k}-a_k)}$  and has about  $p^{m(a_{2k}-2a_k) \cdot ma_k}$  subgroups of index  $p^{ma_k}$ . Put  $n = m(2a_k - a_1)$ . We have just shown that

$$s_{p^n}(G_1) \geq p^{n^2 c'} \text{ where } c' = \frac{a_k(a_{2k} - 2a_k)}{(2a_k - a_1)^2}$$

So  $c' \rightarrow (2^{r'} - 2)/4$  as  $n \rightarrow \infty$ .

Therefore in trying to establish a bound of the type  $s_{p^n}(G_1) \leq p^{n^2 c}$  for all  $n$  we see that  $c \geq 2^{r'-2} - 1$  and so must grow exponentially with  $r'$  (and  $r$ ). We can prove the following:

**Proposition 6** *Let  $\mathcal{K}$  be an  $F$ -subalgebra of  $\mathcal{L}$  of finite codimension. Then*

$$\dim \mathcal{K}/\mathcal{K}' \leq (2^r - 1)m + (2^{r+2} - 1) \dim \mathcal{L}/\mathcal{K}.$$

**Proof** The argument runs very closely to the one in [6] but we obtain a sharper bound independent of the type  $X$  of  $G$ . Let  $t_1, t_2, \dots, t_r$  be a basis for  $I/I^2$  over  $\mathbb{F}$ . Then the  $t_i$  together with 1 generate  $R$  topologically. In fact the set of monomials of total degree  $k$  in the  $t_i$  span  $I^k/I^{k+1}$  over  $\mathbb{F}$ . There is a collection  $C$  of monomials such that:

1. If  $C_k$  is the set of  $y \in C$  of total degree  $k \geq 0$  then  $C_k$  is a basis for  $I^k/I^{k+1}$  over  $\mathbb{F}$ .
2.  $C$  is an *order ideal* of monomials. In other words if  $y \in C$  and  $z$  divides  $y$  then  $z \in C$ .

The construction of  $C$  is similar to the construction of a Schreier set of coset representatives for a subgroup of a free group. We take  $C_1 = \{t_1, t_2, \dots, t_r\}$  and then at each step we pick a 'minimal' monomial not in the  $\mathbb{F}$ -span of the rest. The details can be found in [11] Theorem 2.1. Now take a total ordering  $<$  of

$C$  respecting degree, for example the reverse lexicographic ordering in each  $C_k$  ( so  $t_1 < t_2 < \dots < t_r$ ). Every  $a \in \mathcal{L}$  is written uniquely as

$$a = \sum_{x \in C} a_x \otimes x \text{ with } a_x \in L.$$

Let  $x \in C$  be the least monomial such that  $a_x \neq 0$ . Define the *leading term* of  $a$ :  $l(a) = a_x$  and the *degree* of  $a$ :  $\deg(a) = x$ . For every  $x \in C$  define

$$K_x = F\langle l(a) \mid a \in \mathcal{K}, \deg(a) = x \rangle$$

$$K'_x = F\langle l(a) \mid a \in \mathcal{K}', \deg(a) = x \rangle$$

Then  $\dim \mathcal{L}/\mathcal{K} = \sum_{x \in C} \dim L/K_x$  and the sum is finite. Notice that

$$[K_x, K_y] \subseteq K'_{xy} \text{ for all } xy \in C$$

For a monomial  $x = t_1^{s_1} t_2^{s_2} \dots t_r^{s_r}$  we define

$$x_- = t_1^{\lfloor s_1/2 \rfloor} t_2^{\lfloor s_2/2 \rfloor} \dots t_r^{\lfloor s_r/2 \rfloor}, \quad x_+ = t_1^{\lceil s_1/2 \rceil} t_2^{\lceil s_2/2 \rceil} \dots t_r^{\lceil s_r/2 \rceil}$$

so  $x = x_- x_+$ .

For each  $x \in C$  of degree  $> 1$  in at least one variable  $t_i$ , we have that  $x_-, x_+ \in C$  and by Lemma 1

$$\dim L/[K_{x_-}, K_{x_+}] \leq 2(\dim L/K_{x_-} + \dim L/K_{x_+})$$

We add up these inequalities as  $x$  ranges over  $C' = C \setminus \{t_1^{s_1} t_2^{s_2} \dots t_r^{s_r} \mid s_i = 0, 1\}$ .

Let's estimate how many  $x \in C'$  give the same  $x_-$ . If  $x_- = t_1^{l_1} t_2^{l_2} \dots t_r^{l_r}$  then  $x = t_1^{l_1} t_2^{l_2} \dots t_r^{l_r}$  where  $l_i = 2s_i$  or  $2s_i + 1$ . But of course not all such  $x$  will have to lie in  $C$ . In any case at most  $2^r$  of the  $x \in C$  give the same  $x_-$ .

The same estimate holds for  $x_+$  as well. Therefore

$$\sum_{x \in C'} \dim L/[K_{x_-}, K_{x_+}] \leq 2^{r+2} \sum_{x \in C} \dim L/K_x$$

by using Lemma 1 again. Hence

$$\begin{aligned} \dim \frac{\mathcal{L}}{\mathcal{K}'} &= \sum_{x \in C} \dim L/K'_x \leq |C \setminus C'|m + \sum_{x \in C'} \dim L/[K_{x_-}, K_{x_+}] \leq \\ &\leq (2^r - 1)m + 2^{r+2} \sum_{x \in C} \dim L/K_x = (2^r - 1)m + 2^{r+2} \dim \mathcal{L}/\mathcal{K} \end{aligned}$$

as we wanted to prove.  $\square$  Now, in the same way as we deduced Corollary 1 and Theorem 2 from Lemma 1 we have

**Corollary 2** *If  $H$  is an open subgroup of  $G_1$  then*

$$d(H) \leq (2^r - 1)m + (2^{r+2} - 1) \log_p[G_1 : H]$$

and also

$$s_{p^k}(G_1) \leq p^{(2^r - 1)m k + (2^{r+2} - 1)k(k-1)/2}$$

## 5 Subspaces of Chevalley Lie algebras

In this section we use some basic algebraic geometry.

Let  $L$  be an irreducible algebraic variety. A subset  $M$  is called *algebraic* if it can be obtained from subvarieties of  $L$  using Boolean operators.  $M$  is *almost*  $L$  if the complement of  $M$  has dimension smaller than the dimension of  $L$ . It is easy to see that the set of almost  $L$  algebraic subsets is closed under finite intersection. It also follows that if  $L$  is a finite union of algebraic subsets then at least one of them is almost  $L$ .

Let  $\Phi$  be the root system of  $X$  and  $\Pi$  be the set of fundamental roots of  $\Phi$ . If  $\text{char } F = 2$  we have the standing assumption that  $X \neq A_1, C_l$ . Let  $L$  be the Chevalley Lie algebra of type  $X$  over  $F$ . So  $L$  is perfect with center  $Z(L)$  of dimension at most 2 and such that  $L/Z(L)$  is simple. Moreover  $\dim Z(L) = 2$  only if  $p = 2$  and  $X = D_l$  with  $l \geq 4$  and even. See [4], Chapter 0.13 and references therein.

Consider the Cartan decomposition

$$L = H \oplus \left( \bigoplus_{\alpha \in \Phi} L_\alpha \right)$$

into root spaces  $L_\alpha$ .  $H$  is a Cartan subalgebra of  $L$  of dimension  $l = |\Pi|$ . The roots  $\Phi$  are elements of the dual vector space  $H^*$  of  $H$ .

**Proof of Theorem 3.** First we prove the theorem in the special case when  $\mathbb{F} = F$  and  $L = L_F$ .

Let  $K$  be the algebraic closure of  $F$ . By extending the scalars to  $K$  and taking the dimensions with respect to  $K$  instead of  $F$ , we see that it is sufficient to prove the theorem with  $K$  in place of  $F$ . In this case  $L = L_K$  is the Lie algebra of the simply connected simple algebraic group  $\tilde{G} = X(K)$ . The adjoint map  $Ad : \tilde{G} \rightarrow Aut(L)$  gives an action of  $\tilde{G}$  on  $L$  whose image is the group of inner automorphisms  $\text{Inn}(L)$ .

An element  $x \in L$  is called *semisimple* if  $ad(x)$  is diagonalizable, and *regular* if  $\dim_K C_L(x) = l$ . It is a fact that for an arbitrary  $x \in L$  we have  $\dim_K C_L(x) \geq l$  with equality iff  $x$  is regular. Moreover the set of semisimple elements is the union of the conjugates  $H^g$  of  $H$  under  $\tilde{G}$ .

We denote by  $S$  the set of the regular semisimple elements of  $L$ , i.e.

$$S = \{x \in L \mid ad(x) \text{ is diagonalizable with non-zero eigenvalues}\}$$

So

$$S \cap H = \{h \in H \mid \alpha(h) \neq 0, \text{ for all } \alpha \in \Phi\}.$$

**Proposition 7** *If  $U$  is a subspace of  $L$  then there is  $x \in U$  with  $\dim C_L(x) \leq l + \dim L/U$ .*

**Proof.** Consider the adjoint action of  $\tilde{G}$  on  $L$  and let  $\tilde{G} \backslash L$  be the collection of orbits.

The results about orbits of semisimple elements of  $L$  under  $Ad(\tilde{G})$  which we use below can be found in Humphrey's book [4], chapter 4. and also in [12].

The set of semisimple orbits (i.e those consisting of semisimple elements) is in 1-1 correspondence with  $\mathcal{W}\backslash H$ , (the orbits of  $H$  under the Weyl group  $\mathcal{W}$ ) and thus can be given a structure of  $l$ -dimensional affine variety  $\mathbf{A}$ . There is a map of algebraic varieties  $\nu : L \rightarrow \mathbf{A}$  which is the analogue of the Steinberg map for  $\bar{G}$ :  $\nu$  is constant on each orbit of  $\bar{G}$  and in fact  $\nu(x) = (f_1(x), \dots, f_l(x)) \in \mathbf{A}$  where the  $f_i$  are  $\bar{G}$ -invariant homogeneous polynomials, whose restrictions to  $H$  form a basis for the algebra  $K[H]^{\mathcal{W}}$  of  $\mathcal{W}$ -invariant polynomial functions.

It is known that each fiber of  $\nu$  contains only finitely many orbits, among which there is a unique semisimple one. For example when  $L = sl_{l+1}(K)$ , we have  $\nu(x) = \nu(x_s) = (\chi_2(x), \dots, \chi_{l+1}(x))$  where  $x_s$  is the semisimple part of the matrix  $x$  and  $\chi_i(x)$  is the  $i$ -th coefficient of the characteristic polynomial of the matrix  $x$ .

Consider the variety  $Y = \{(x, y) | [x, y] = 0\}$  of pairs of commuting elements of  $L$ . We claim that the dimension of  $Y$  as algebraic set is equal to  $\dim L + l$ . Consider the map  $f : Y \rightarrow \mathbf{A}$  given by  $f(x, y) = \nu(x)$ . The fibers of this map have dimension  $\dim L$ : Given  $x \in \mathbf{A}$  there are only finitely many representatives, say  $x_1, \dots, x_r$  for the orbits of  $\bar{G}$  on  $\nu^{-1}(x)$ . One of these orbits, say  $x_1^{\bar{G}}$  consists of semisimple elements. If  $C_i = C_L(x_i)$  then  $C_1$  has minimal dimension among  $C_1, \dots, C_r$  and the orbit  $x_1^{\bar{G}}$  has the largest algebraic dimension among  $x_1^{\bar{G}}, \dots, x_r^{\bar{G}}$ . Thus

$$f^{-1}(x) = \cup_{i=1}^r \{(x_i^g, C_i^g) | g \in \bar{G}\}$$

and so it has algebraic dimension

$$\dim x_1^{\bar{G}} + \dim C_1 = \dim L - \dim \bar{G}_{x_1} + \dim C_L(x_1) = \dim L$$

So the fibers of  $f$  have dimension  $\dim L$  and thus the dimension of  $Y$  is  $\dim L + l$  proving the claim.

Let  $U_i := \{x \in U | \dim C_L(x) = i\}$ .  $U_i$  is an algebraic subset of  $U$  and  $U = \cup_i U_i$ . So there is some  $j \leq \dim L$  such that  $U_j$  has algebraic dimension  $\dim U$ . Then  $\{(x, y) | x \in U_j, [x, y] = 0\}$  has dimension  $\dim U + j$  which must be at most  $\dim L + l$  giving that  $j \leq \dim L/U + l$ .  $\square$

Now we return to the proof of Theorem 3.

For such an  $x \in U$  given by the proposition above we have

$$\dim[x, V] \geq \dim V - l - \dim L/U$$

So  $\dim L/[U, V] \leq l + \dim L/U + \dim L/V$ .

**Case 1.** If  $\dim L/U + \dim L/V \geq l$  then

$$\dim L/[U, V] \leq l + \dim L/U + \dim L/V \leq 2(\dim L/U + \dim L/V)$$

and we are done.

**Case 2.** Suppose  $\dim L/U + \dim L/V < l$ . Then the codimension of either  $U$  and  $V$  is less than  $l - \dim Z(L)$ . Without loss of generality suppose that  $\dim L/U < l - \dim Z(L)$ .

We claim that  $S \cap U \neq \{0\}$ . For suppose this is not the case. Then  $S \cap U^g = \{0\}$  for all  $g \in \bar{G}$ . For any  $\alpha \in \Phi$  define

$$\bar{G}_\alpha = \{g \in \bar{G} \mid U^g \cap H \subseteq \ker \alpha\}.$$

It is an algebraic subset of  $\bar{G}$ . We have  $U^g \cap H \subseteq \cup_\alpha \ker \alpha$  and as  $U^g \cap H$  is a subspace it must be in one of the hyperplanes  $\ker \alpha$  for some  $\alpha$  depending on  $g$ . Now, varying over all  $g \in \bar{G}$  and  $\alpha \in \Phi$  we get that  $\cup_\alpha \bar{G}_\alpha = \bar{G}$ . So  $\bar{G}_{\alpha_0}$  is almost  $\bar{G}$  for some  $\alpha_0 \in \Phi$ .

The Weyl group  $\mathcal{W} = N_G(H)/C_G(H)$  normalizes  $H$  and acts transitively on the roots of equal length in  $\Phi$ . This implies that  $\bar{G}_\alpha$  is almost  $\bar{G}$  for all  $\alpha \in \Phi$  with  $|\alpha| = |\alpha_0|$ . So the intersection of those  $\bar{G}_\alpha$  is almost  $\bar{G}$ . Choosing an element  $g$  of the intersection we have

$$U^g \cap H \subseteq \bigcap_{|\alpha|=|\alpha_0|} \ker \alpha$$

We find by examining all the root systems that with the noted exception the set of roots  $\alpha$  with  $|\alpha| = |\alpha_0|$  spans the vector space  $K\langle\Phi\rangle \subseteq H^*$  over  $K$ . Therefore  $U^g \cap H \subseteq \Phi^0$  where

$$\Phi^0 = \bigcap_{\alpha \in \Phi} \ker \alpha = Z(L)$$

Since  $\dim L/U^g = \dim L/U < \dim H/Z(L)$  we have a contradiction. This proves our claim.

Take a nonzero  $x \in S \cap U$ . Without loss of generalities we can assume  $x \in H$ . Then  $[x, L_\alpha] = L_\alpha$  for all  $\alpha \in \Phi$ . So

$$\bigoplus_{\alpha \in \Phi} L_\alpha \subseteq [x, L].$$

We claim that we can find a  $y \in L$  such that

$$[x, L] + [y, L] = L.$$

It is sufficient to know that  $[y, L]$  projects onto  $H$ . Let  $y = h + \sum_\alpha a_\alpha \cdot x_\alpha$ , where  $a_\alpha \in K$  and  $x_\alpha$  is a fixed basis for the one dimensional root space  $L_\alpha$ . Let  $h_\alpha = [x_\alpha, x_{-\alpha}] \in H$  be the co-root of  $\alpha$ . Then  $[y, x_{-\alpha}]$  has  $H$ -component  $a_\alpha \cdot h_\alpha$  and therefore  $a_\alpha \cdot h_\alpha \in [y, L] + [x, L]$ .

If now  $\theta \subset \Phi$  is a subset of the roots such that the co-roots  $\{h_\alpha \mid \alpha \in \theta\}$  span  $H$  then the condition  $\prod_{\alpha \in \theta} a_\alpha \neq 0$  on  $y$  ensures that  $h_\alpha \in [y, L] + [x, L]$  for all  $\alpha \in \theta$  and so  $[y, L] + [x, L] = L$ .

By examining the root systems we can find at least  $l$  such pairwise disjoint spanning subsets  $\theta_1, \dots, \theta_l$  of roots. Let  $\mathbb{V}$  be the subvariety of  $L$  defined by the  $l$  equations  $\prod_{\alpha \in \theta_i} a_\alpha = 0$ ,  $i = 1, 2, \dots, l$ . Then  $\mathbb{V}$  has dimension  $\dim L - l$  as algebraic variety. As  $\dim L/U < l$  it is impossible that  $U \subseteq \mathbb{V}$  so we can find  $y \in U \setminus \mathbb{V}$  and then  $[x, L] + [y, L] = L$  as claimed. Therefore

$$\dim([x, V] + [y, V]) \geq \dim L - 2 \dim L/V$$

whence  $\dim L/[U, V] \leq 2 \dim L/V$  in this case. We see that in both cases we have

$$\dim L/[U, V] \leq 2(\dim L/U + \dim L/V)$$

thus proving Theorem 3 in this case.

Notice that in fact we have proved something more.

**Proposition 8** *If  $L = L_K$  is Chevalley simple over an algebraically closed field  $K$  and  $U$  is a subspace of  $L$  then for almost all pairs  $(a, b) \in U \times U$  we have*

$$\dim([a, L] + [b, L]) \geq \dim L - 2 \dim L/U.$$

Now suppose that  $L$  semisimple so it is a direct sum  $L = L_1 \oplus \cdots \oplus L_n$  of simple classical algebras over  $K$ . Suppose  $U$  is a  $K$ -subspace of  $L$ . Let  $\phi_i : L \rightarrow L_i$  be the projection onto  $L_i$  and put  $U_i = \phi_i(U) \subseteq L_i$ . By considering the images of elements  $a, b \in U$  under  $\phi_i$  and applying the proposition above we have that:

For any chosen  $i = 1, 2, \dots, n$  and for almost all  $a, b \in U$  we have that

$$\dim_K([a, L_i] + [b, L_i]) \geq \dim L_i - 2 \dim L_i/U_i$$

Since an algebraic set is not a finite union of algebraic subsets of strictly smaller dimension we deduce that there exist  $a, b \in U$  for which the above inequalities hold for all  $i = 1, 2, \dots, n$ . Observe that  $\sum_{i=1}^n \dim L_i/U_i \leq \dim L/U$  and therefore

$$\dim_K([a, L] + [b, L]) \geq \dim L - 2 \sum_{i=1}^n \dim L_i/U_i \geq \dim L - 2 \dim L/U,$$

giving that  $\dim([a, V] + [b, V]) \geq \dim L - 2(\dim L/U + \dim L/V)$ .

Now we can finish the proof of Theorem 3 by extending the base field  $F$  to  $K$  and restricting the scalars. In this way  $L_F \otimes_F K$  is identified with  $L_K \oplus \cdots \oplus L_K$  via

$$a \in L_F \mapsto (\psi_1(a), \dots, \psi_s(a))$$

where  $\psi_1, \dots, \psi_s$  are the embeddings of  $L_F$  in  $L_K$  coming from all the embeddings of  $\mathbb{F}$  in  $K$ . So the theorem is reduced to the case of semisimple Lie algebra over  $K$  which we have already proved.  $\square$

**Proof of Theorem 4.** As before we can assume that the field  $T$  is algebraically closed. Suppose  $\dim_T L/M < l - \dim Z(L)$ . We claim that  $M$  contains a regular semisimple element with *distinct* eigenvalues in its adjoint action on  $L$ .

Suppose not. Then for any  $g \in \tilde{G}$  there are a pair of distinct roots  $\alpha, \beta \in \Phi \cup \{0\}$  such that  $M^g \cap H \subseteq \ker(\alpha - \beta)$  and the restriction on  $\mathfrak{p}$  implies that  $\ker(\alpha - \beta)$  is a proper subspace of  $H$ . Just as before, the algebraic irreducibility of  $\tilde{G}$  implies that there is  $g \in \tilde{G}$  such that

$$M^g \cap H \subseteq \bigcap_{w \in \mathcal{W}} (\ker(\alpha - \beta))^w$$

The subspace of  $H$  on the right is  $\mathcal{W}$ -invariant proper subspace. By the indecomposability of  $X$  we know that any such invariant subspace is contained in the centre  $Z(L)$ . So  $\dim M^g \cap H \leq \dim Z(L)$  and this contradicts  $\dim L/M < l - \dim Z(L)$ , proving the claim.

So w.l.o.g,  $M$  contains a regular element  $h$  with  $\alpha(h)$  all distinct (and non zero) for all  $\alpha \in \Phi$ .  $M$  is  $ad(h)$  invariant so it is a direct sum of eigenspaces of  $ad(h)$ :

$$M = M_1 \oplus \left( \bigoplus_{\alpha \in \Phi'} L_\alpha \right),$$

where  $M_1 \subseteq H$  and  $\Phi' \subseteq \Phi$ . For roots  $\alpha, \beta$  we have  $[L_\alpha, L_\beta] = L_{\alpha+\beta}$  provided  $\alpha + \beta \in \Phi$ .  $M$  is a Lie subalgebra, so  $\Phi'$  is a subset of the roots  $\Phi$  closed under addition, i.e.,  $\alpha, \beta \in \Phi'$  and  $\alpha + \beta \in \Phi$  implies  $\alpha + \beta \in \Phi'$ . In these circumstances it is well known that any proper subset  $\Phi'$  leaves at least  $l$  elements of  $\Phi$ .  $\square$

The Hausdorff dimension of a closed subgroup  $H$  of  $G = X(F[[t]])$  (with respect to the congruence subgroups filtration  $G(n)$ ) is defined to be

$$\dim_{\text{H}}(H) := \liminf_{n \rightarrow \infty} \frac{\log |HG(n)/G(n)|}{\log |G/G(n)|} \in [0, 1].$$

If we now substitute Theorem 4 for Theorem 1.7 in Barnea and Shalev's paper, we deduce

**Proposition 9** *Let  $l' = l - \dim Z(L)$ . If  $H$  is a closed subgroup of infinite index in  $G = X(F[[t]])$  then its Hausdorff dimension is at most  $1 - \frac{l'}{\dim L}$ . So in the Hausdorff spectrum of  $G$  there is a gap between  $1 - \frac{l'}{\dim L}$  and 1.*

The first and third authors would like to express their gratitude to the second author who initiated them into this nice part of group theory.

## References

- [1] M.F. Atiyah, I.G. MacDonald, Introduction to Commutative Algebra. Addison-Wesley, Reading Mass., 1969.
- [2] Y. Barnea, A. Shalev, Hausdorff dimension, pro- $p$  groups, and Kac-Moody algebras, Trans. Amer. Math. Soc. 349 (1997) no. 12, 5073-5091.
- [3] J. Dixon, M. du Sautoy, A. Mann and D. Segal, Analytic pro- $p$  Groups, 2nd edition, CUP, 1999.
- [4] J.E. Humphreys, Conjugacy classes in semi-simple algebraic groups. Mathematical Surveys and Monographs, v. 43, 1995.
- [5] A. Lubotzky and D. Segal, Subgroup growth. Progr. Math. Birkhauser, 2003.

- [6] A. Lubotzky and A. Shalev, On some  $\Lambda$ -analytic pro- $p$  groups, *Israel J. Math.* 85 (1994), 307-337.
- [7] A. Lubotzky, Subgroup growth and congruence subgroups. *Invent. Math.* 119 (1995), 267-295.
- [8] L. Pyber, Asymptotic results for simple groups and some applications, in *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, Vol 28 (1997), 309-327.
- [9] L. Pyber, A. Shalev, Normal and subnormal subgroups in residually finite groups, *in preparation*.
- [10] A. Shalev, Growth functions,  $p$ -adic analytic groups, and groups of finite coclass, *J. London Math. Soc.*, 46 (1992), 111-122.
- [11] R.P. Stanley (1978), Hilbert functions of graded algebras, *Adv. in Math.* 28 (1978), 57-83.
- [12] T. Springer, R. Steinberg, Conjugacy Classes, in *Seminar on algebraic groups and related finite groups*, *Lecture Notes in Mathematics* 131, Springer-Verlag, 1970.