New Uniform Diameter Bounds in Pro-p Groups

Henry Bradford

Abstract

We give new upper bounds for the diameters of finite groups which do not depend on a choice of generating set. Our method exploits the commutator structure of certain profinite groups, in a fashion analogous to the Solovay-Kitaev procedure from quantum computation. We obtain polylogarithmic upper bounds for the diameters of finite quotients of: groups with an analytic structure over a pro-p domain (with exponent depending on the dimension); Chevalley groups over a pro-p domain (with exponent independent of the dimension) and the Nottingham group of a finite field. We also discuss some consequences of our results for random walks on groups.

1 Introduction

The interplay between growth, spectral gap and diameter for finite groups has been a highly active area of study within group theory in recent years. Given a finite group G and a generating set $S \subseteq G$, recall that the *diameter* of the pair (G, S) is given by:

$$\mathrm{diam}(G, S) = \min\{n \in \mathbb{N} : B_S(n) = G\}$$

where $B_S(n)$ is the (closed) *word-ball* of radius n, given by:

$$B_S(n) = \{s_1 \cdots s_n : s_1, \ldots, s_n \in S \cup S^{-1} \cup \{1\}\}.$$

In this paper we investigate techniques for establishing upper bounds for $\mathrm{diam}(G, S)$ (such bounds will usually be expressed as a function of $|G|$).

Meanwhile the *spectral gap* of the pair (G, S) is a measure of the *mixing time* of the simple random walk on (G, S): that is, if (G, S) has large spectral gap then only a small number of steps must be taken in such a walk before the associated probability distribution on G is close to uniform (we make these notions and their relationship to diameter precise later).

Our interest shall be in upper bounds for the diameter which do not depend on the generators. With this in mind, we define for a finite group G:

$$\mathrm{diam}(G) = \max\{\mathrm{diam}(G, S) : S \subseteq G, \langle S \rangle = G\}.$$

This quantity is referred to by many authors as the *worst-case diameter* for G.

1.1 Statement of Results

Fix p prime. Let R be a commutative unital Noetherian ring. Recall that R is called a *local ring* if R has a unique non-zero maximal ideal $\mathcal{M}$ (we shall refer to *the local ring* $(R, \mathcal{M})$). The quotient $R/\mathcal{M}$ is called the *residue field* of R. There is a topology on R, called the $\mathcal{M}$*-adic topology*, induced by declaring the filtration $(\mathcal{M}^n)_n$ to be a basis for the neighbourhoods of 0.

Definition 1.1. *The local ring* $(R, \mathcal{M})$ *is called a* pro-p ring *if:*

(i) The residue field of R *is finite of characteristic* p

(ii) R *is complete with respect to the* $\mathcal{M}$*-adic topology.*

A pro-p *ring* $(R, \mathcal{M})$ *where* $\mathcal{M}$ *is principal is called a* discrete valuation pro-p ring *and a pro-*p *ring which is an integral domain will be called a* pro-p domain*.*

Let $\mathbb{K}$ be the field of fractions of R. Fix $c \in (0, 1)$ and define a norm $\|\cdot\|$ on R (compatible with the $\mathcal{M}$-adic topology) by:

$$\|a\| = c^n \text{ for } a \in \mathcal{M}^n \setminus \mathcal{M}^{n+1};\ \|0\| = 0.$$

In particular if $(R, \mathcal{M})$ is a discrete valuation ring, with $\mathcal{P} \in \mathcal{M}$ such that $\mathcal{M} = (\mathcal{P})$, then $\|\mathcal{P}\| = c$. In this case, we extend $\|\cdot\|$ to $\mathbb{K}$ via:

$$\|a\| = \|a\mathcal{P}^n\|c^{-n} \text{ for } n \text{ sufficiently large that } a\mathcal{P}^n \in R.$$

In what follows we take $(R, \mathcal{M})$ to be a pro-p domain and a discrete valuation ring. By work of Cohen [9] every such R arises as a finitely generated free module over a subring of the form $\mathbb{Z}_p$ or $\mathbb{F}_p[[t]]$.

Our first result concerns compact groups with a compatible structure as an R-analytic manifold. Every such group has an open subgroup with an especially simple R-analytic structure, called an R*-standard group*. Precise definitions are given in Section 4. In a d-dimensional R-analytic group G, an R-standard subgroup may be identified (as a space) with the product space $\mathcal{M}^{(d)}$; the balls $(\mathcal{M}^n)^{(d)}$ around 0 form a filtration by open normal subgroups. The commutator structure in $\mathcal{M}^{(d)}$ is controlled by the Lie algebra $\mathcal{L}_G$. Recall that a Lie algebra $\mathcal{L}$ is called *perfect* if $\mathcal{L}$ is equal to its derived subalgebra $(\mathcal{L}, \mathcal{L})$.

Theorem 1.2. *Let G be a d-dimensional R-standard group, $K_n = (\mathcal{M}^n)^{(d)} \lhd_o G$. Suppose $\mathcal{L}_G$ is perfect. Then there exist $C_1(G)$, $C_2(d) > 0$ such that:*

$$\mathrm{diam}(G/K_n) \leq C_1(\log|G/K_n|)^{C_2}.$$

In the case $R = \mathbb{Z}_p$, we can say more, exploiting the concept of a *uniform* subgroup and associated additional features of the Lie theory (explained in detail in Section 4.1). Every $\mathbb{Z}_p$-standard group is uniform and every compact p-adic analytic group has an open characteristic uniform subgroup. In a $\mathbb{Z}_p$-standard group G, the balls K_n described in Theorem 1.2 coincide with the terms of the lower central p-series for G.

Definition 1.3. *Let G be a profinite group. G is* FAb *if every open subgroup has finite abelianisation.*

Theorem 1.4. *Let $p \geq 3$. Let G be a d-dimensional compact p-adic analytic group. Let $K_1 \leq G$ be an open characteristic uniform subgroup; $(K_n)_n$ its lower central p-series. If G is FAb then there exist $C_1(G), C_2(d) > 0$ such that:*

$$\mathrm{diam}(G/K_n) \leq C_1(\log|G/K_n|)^{C_2}. \tag{1}$$

For $G = K_1$ then conversely: if G satisfies (1) then G is FAb.

One familiar family of R-analytic groups is the class of Chevalley linear algebraic groups over R. Here we have a stronger conclusion than that available in the general setting of Theorem 1.2: the degree C_2 in the diameter bound may be taken to be *independent of the dimension.*

Theorem 1.5. *Let $(R, \mathcal{M})$ be a commutative unital discrete valuation pro-p domain, with $\mathcal{M}$ generated by $\mathcal{P}$. Let $G \leq \mathrm{GL}_d(R)$ be the adjoint Chevalley group of type $X_l \in \{A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4, G_2\}$ over R. Suppose $(X_l, p) \notin \{(A_1, 2), (B_l, 2), (C_l, 2), (D_l, 2)\}$. Let $K_n = G \cap (I_d + \mathcal{P}^n \mathbb{M}_d(R))$. Then there exist $C_1(G) > 0$ and an absolute constant $C_2 > 0$ such that:*

$$\mathrm{diam}(G/K_n) \leq C_1(\log|G/K_n|)^{C_2}.$$

Moreover, the same bound holds for $G = \mathrm{SL}_d(R), \mathrm{SO}_d(R)$ or $\mathrm{Sp}_d(R)$ provided $p \geq 3$, and for $G = \mathrm{SL}_d(R)$ with $p = 2$ provided $d \geq 3$.

Recall the correspondence between the classical root system of type X_l and the associated adjoint Chevalley group G: if $X_l = A_l$ then $G = \mathrm{PSL}_d(R)$, and in particular if $X_l = A_1$ then $G = \mathrm{PSL}_2(R)$; if $X_l = B_l$ or D_l then $G = \mathrm{PSO}_d(R)$ (with the dichotomy between B_l and D_l corresponding to the parity of d); if $X_l = C_l$ then $G = \mathrm{PSp}_d(R)$.

In the case $R = \mathbb{Z}_p$, this result was proved by Dinai [13], under the additional hypothesis $p > \max\{\frac{l+2}{2}, 19\}$.

Finally we consider a class of non-linear examples. Recall that, for R a commutative unital ring, the *Nottingham group* $\mathcal{N}(R)$ of R is the set of formal power series over R with constant coefficient 0 and 1st order coefficient 1, with the operation of formal composition of power series. That is, an element $f \in \mathcal{N}(R)$ has the form:

$$f(t) = t + \sum_{k=2}^{\infty} \lambda_k t^k$$

for some $\lambda_k \in R$, and for $g \in \mathcal{N}$,

$$f \cdot g = g\Big(t + \sum_{k=2}^{\infty} \lambda_k t^k\Big).$$

We take $R = \mathbb{F}_q$ a finite field (for q a power of the prime p) and write $\mathcal{N}_q$ for $\mathcal{N}(\mathbb{F}_q)$. $\mathcal{N}_q$ is often used as a test case for more general techniques or conjectures in pro-p group theory. The reason for this is twofold: first, computations in $\mathcal{N}_q$ can be made reasonably explicitly and simply. Second, $\mathcal{N}_q$ has extreme properties among pro-p groups: as was proved first by Camina [6] and then by Fesenko [15], every countably based pro-p group embeds as a closed subgroup of $\mathcal{N}_q$. We shall be concerned with the filtration by open normal subgroups:

$$K_n = \Big\{t + \sum_{k=n+1}^{\infty} \lambda_k t^k \in \mathcal{N}_q\Big\}$$

(so that in particular $K_1 = \mathcal{N}_q$).

Theorem 1.6. *Suppose $p \geq 3$. Then there exist $C_1(q) > 0$ and an absolute constant $C_2 > 0$ such that:*

$$\mathrm{diam}(\mathcal{N}_q/K_n) \leq C_1(\log|G/K_n|)^{C_2}.$$

As an application of these results, we make some elementary observations about mixing times of random walks in the finite groups we study. The direct relationship between diameter and spectral gap was recently exploited by Varjú, who in [21] used a representation-theoretic argument to produce uniform weak spectral gap estimates for $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$, and deduced polylogarithmic diameter bounds. Here we reverse the direction of the argument, and deduce weak spectral gap estimates from uniform diameter bounds. As an aside, the diameter estimates for $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ obtained

by Varjú are uniform in p but not in d, whereas those obtained via the Solovay-Kitaev procedure are uniform in d but not in p. It may be instructive to apply Varjú's method to other of the finite groups we treat in this paper to obtain diameter or spectral gap estimates which are similarly complementary to those given here.

Let $S \subseteq \Gamma$ be a finite symmetric set, with $1 \in S$. Let $X_1, X_2, \ldots$ be a sequence of independent random variables, each with law:

$$\tfrac{1}{|S|}\chi_S \in \ell^2(\Gamma).$$

For $l \in \mathbb{N}$, the *simple random walk on* (Γ, S) *at time* l is the random variable $Y_l = X_1 \cdots X_l$.

For $(R, \mathcal{M})$ a discrete valuation pro-p domain; G a d-dimensional R-standard group; $x_1, \ldots, x_d$ an R-basis for $\mathcal{M}^{(d)}$ (a set of so-called "co-ordinates of the first kind") and $(1 \in)S \subseteq G$ a finite symmetric subset, we may express the simple random walk on (G, S) by:

$$Y_l = L_1^{(l)} x_1 + \cdots + L_d^{(l)} x_d$$

for some random variables $L_1^{(l)}, \ldots, L_d^{(l)}$ supported on R.

Corollary 1.7. *Suppose $\mathcal{L}_G$ is perfect and $S \subseteq G$ generates a dense subgroup. Then there exists $C(d) > 0$, such that for any $C' > 0$ there exists $C''(G, |S|, C') > 0$ and $C'''(d, |R/\mathcal{M}|, C') > 0$ such that, for any $(\lambda_1, \ldots, \lambda_d) \in R^{(d)}$, and for any $N \in \mathbb{N}$, we have:*

$$\left| \mathbb{P}\left[\|L_1^{(l)} - \lambda_1\|, \ldots, \|L_d^{(l)} - \lambda_d\| \leq c^{N+1} \right] - \tfrac{1}{|R/\mathcal{M}|^{dN}} \right| \leq e^{-C''' N^{C'}}$$

whenever $l \geq C'' N^{C+C'}$.

In other words, for such l the probability that Y_l is close to any element of $\mathcal{M}^{(d)}$ is nearly constant, with error at most $e^{-C''' N^{C'}}$.

For a d-dimensional uniform pro-p group G, an alternative representation for elements is available: for any $g \in G$ and any minimal (ordered) generating set $a_1, \ldots, a_d$ for G, there exist $\mu_1, \ldots, \mu_d \in \mathbb{Z}_p$ such that $g = a_1^{\mu_1} \cdots a_d^{\mu_d}$ (so-called "co-ordinates of the second kind"). We therefore have:

$$Y_l = a_1^{M_1^{(l)}} \cdots a_d^{M_d^{(l)}}$$

for some random variables $M_1^{(l)}, \ldots, M_d^{(l)}$ supported on $\mathbb{Z}_p$.

Corollary 1.8. *Let $p \geq 3$. Suppose G is uniform and FAb and $S \subseteq G$ generates a dense subgroup. Then there exists $C(d) > 0$, such that for any $C' > 0$ there exists $C''(G, |S|, C') > 0$ and $C'''(d, p, C') > 0$ such that, for any $\mu_1, \ldots, \mu_d \in \mathbb{Z}_p$, and for any $N \in \mathbb{N}$, we have:*

$$\left| \mathbb{P}\left[\|M_1^{(l)} - \mu_1\|, \ldots, \|M_d^{(l)} - \mu_d\| \leq p^{-N-1} \right] - \tfrac{1}{p^{dN}} \right| \leq e^{-C''' N^{C'}}$$

whenever $l \geq C'' N^{C+C'}$.

In the Nottingham group $\mathcal{N}_q$, the question of mixing times for the groups $\mathcal{N}_q / K_n$ was raised by Diaconis [11]. We may express:

$$Y_l = t + \sum_{i=2}^{\infty} A_i^{(l)} t^i$$

for some random variables $A_i^{(l)}$ supported on $\mathbb{F}_q$.

Corollary 1.9. *Let $p \geq 3$. Suppose $S \subseteq \mathcal{N}_q$ generates a dense subgroup. Then there exists an absolute constant $C > 0$, such that for any $C' > 0$ there exists $C''(q, |S|, C') > 0$ and $C'''(q, C') > 0$ such that, for any sequence $(\alpha_i)_i$ in $\mathbb{F}_q$, and for any $N \in \mathbb{N}$, we have:*

$$\left| \mathbb{P}[A_2^{(l)} = \alpha_2, \ldots, A_N^{(l)} = \alpha_N] - \tfrac{1}{q^{N-1}} \right| \leq e^{-C''' N^{C'}}$$

whenever $l \geq C'' N^{C+C'}$.

1.2 Background

The work of estimating the diameter and spectral gap for finite groups with respect to various generating sets has been going on for many years: see for instance [11] for an overview of some of the work on *card-shuffling* problems, that is, questions of mixing and diameter in the symmetric group $\mathrm{Sym}(n)$.

In the past decade however, there has been a flood of results which provide diameter or spectral gap estimates for finite simple groups of Lie type, and which systematically treat all (or at least most) generating sets simultaneously. In many ways this programme was begun by Helfgott [17] who established polylogarithmic diameter bounds for $G = \mathrm{PSL}_2(p)$, independent of S. These bounds were deduced from lower bounds on the growth of an arbitrary generating set under multiplication with itself. A series of papers by many authors quickly followed, many expressed in the language

of *approximate groups*, which generalised Helfgott's work to arbitrary finite simple groups of Lie type (see [4], [20] for the most general statements).

A key motivation for the development of this field was the discovery, first made by Bourgain and Gamburd in [1], that such growth results could be harnessed to construct new examples of *expanders*. These are sequences of pairs $(G_n, S_n)_n$ for which the spectral gap is bounded below, independent of n. In particular, for such sequences $\mathrm{diam}(G_n, S_n)$ is logarithmic in $|G_n|$. Bourgain and Gamburd deduced from Helfgott's result that $(\mathrm{PSL}_2(p))_p$ is an expander with respect to *random* generators. With the proliferation of growth results and the popularization of the Bourgain-Gamburd philosophy came a corresponding set of papers producing new examples of expanders, culminating in the recent work of Breuillard, Green, Guralnick and Tao [5], who showed that *any* sequence of finite simple groups of Lie type of bounded rank is an expander with respect to random generators.

For finite groups G which arise as images of linear groups over pro-p rings, the situation is very different from in the simple case: a group such as $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ has many large normal subgroups, arising as the kernels of congruence maps $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{SL}_d(\mathbb{Z}/p^m\mathbb{Z})$ for $m \leq n$. The presence of such subgroups is both a blessing and a curse. On the one hand, a clean statement about the growth of arbitrary subsets à la Helfgott becomes less accessible (there are in some sense too many subgroups in which a generating set may become partially trapped). On the other, the filtration by the congruence kernels opens the way to arguments by induction on the level of the filtration. One such is the *Solovay-Kitaev Procedure*, originally applied to $\mathrm{SU}(d)$ in the study of compilers in quantum computation [10], but equally valid in the profinite world. This procedure works by exploiting the commutator structure of the groups concerned: approximating elements at lower levels in the filtration by commutators of elements at higher levels.

Several papers have already exploited this idea: Gamburd and Shahshahani [16] used it to establish upper bounds on $\mathrm{diam}(\mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z}))$. Their analysis was extended by Dinai [13] to arbitrary Chevalley groups over $\mathbb{Z}/p^n\mathbb{Z}$, with bounds independent of the rank of the Chevalley group scheme. Finally Bourgain and Gamburd ([2] and [3]) combined a Solovay-Kitaev-type argument with results on random matrix products and the sum-product phenomenon in the ring $\mathbb{Z}/p^n\mathbb{Z}$ to produce many new examples of expander Cayley graphs of $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ (though without uniformity in d). In fact, the ideas explored in [16] and [13] are relevant to a much broader class of groups. It is the goal of this paper to present the Solovay-Kitaev procedure for profinite groups in an appropriate level of generality and to exploit it for uniform diameter bounds in families of finite groups which

have not been considered previously.

The paper is structured as follows. In Section 2 we discuss analogues of the Solovay-Kitaev Procedure for profinite groups upon which all our results will be based. In Section 3 we prove Theorem 1.5 in the case of classical groups. This is achieved via a very concrete analysis of the Lie algebras of these groups, in their standard matrix representation, and does not require any understanding of the associated root systems. In Section 4 we study the Lie algebras of R-analytic groups, prove Theorem 1.2 and deduce both Theorem 1.4 and the exceptional case of Theorem 1.5. In Section 5 we prove Theorem 1.6. Consequences of these results for mixing times of random walks are explained in Section 6.

I am deeply grateful to my supervisor, Marc Lackenby, for suggesting that I investigate diameters of p-groups; for his many suggestions concerning this project and for his continued support and enthusiasm for my research. I am also grateful to EPSRC for providing financial support during the undertaking of this work. Several results from this paper were first presented at the Postgraduate Conference in Group Theory, held at the University of Birmingham in June 2014. I would like to thank the organizers of that conference for their hard work and for providing me with a warm welcome.

2 The Profinite Solovay-Kitaev Procedure

In this section we prove general results about the diameters of finite quotients of a finitely generated profinite group G under some hypotheses on the behaviour of commutators in G. The proofs of Theorems 1.2, 1.5 and 1.6 will thereby be reduced to a verification that commutators in the groups concerned satisfy these hypotheses. Our first result in this direction, which will also serve as a warm-up for the more general technical result required for some applications, is:

Proposition 2.1. *Let G be a profinite group, $(K_n)_{n\geq 1}$ a descending sequence of open normal subgroups of G. Suppose:*

(i) For all $m, n \geq 1$, $[K_m, K_n] \subseteq K_{m+n}$;

(ii) There exists $n_0 \geq 1$ such that for all $m, n \geq n_0$ satisfying $n \leq m \leq 2n$, and all $g \in K_{n+m}$, there exist:

$$g_1, \dots, g_A \in K_n \ , \ h_1, \dots, h_A \in K_m$$

such that $[g_1, h_1] \cdots [g_A, h_A] g^{-1} \in K_{2n+m}$.

Then $G/\bigcap_{n=1}^{\infty} K_n$ is finitely generated and there exists $C > 0$ (depending only on A, $|G/K_{2n_0}|$) such that for all $n \geq 1$,

$$\mathrm{diam}(G/K_n) \leq C n^{\frac{\log(8A^2+6A)}{\log(2)}}.$$

Remark 2.2. *In all the examples we consider below, we will have in addition that the sequence $(|K_i/K_{i+1}|)_i$ is constant, so that a bound for $\mathrm{diam}(G/K_n)$, which is polynomial in n, is polylogarithmic in $|G/K_n|$.*

If we imagine the subgroups K_n to be balls in G around the identity of radius c^n, for some $c \in (0,1)$, then hypothesis (i) of Proposition 2.1 says roughly that a commutator of two elements is of size quadratic in the sizes of those two elements, whereas hypothesis (ii) says that every element may be approximated by a product of (a bounded number of) commutators of larger elements. Indeed, in a real Lie group such as SU_d, replacing the K_n with Euclidean balls around Id and interpreting "size"as "Euclidean distance", we recover the properties on which the proof of the original Solovay-Kitaev Theorem is based. In this sense then, it is legitimate to describe Proposition 2.1 as a "profinite Solovay-Kitaev Theorem".

In fact, rather than hypothesis (i) itself the proof uses a reformulation (i'), as explained in the following Lemma. Under the interpretation just outlined, hypothesis (i') says that, given a pair of elements g, h and a pair of "approximations"g', h' up to some error, $[g', h']$ approximates $[g, h]$ up to an error which is quadratic in the sizes of g and h, and the errors in the original approximations g' and h'.

Lemma 2.3. *Let G be a profinite group, $(K_n)_{n\geq 1}$ a descending sequence of open normal subgroups. The following conditions are equivalent:*

(i) For all $m, n \geq 1$, $[K_m, K_n] \subseteq K_{m+n}$.

(i') For all $m, m', n, n' \geq 1$, with $m \leq m'$, $n \leq n'$, and for all $g, g' \in K_n$; $h, h' \in K_m$ with $g^{-1}g' \in K_{n'}$; $h^{-1}h' \in K_{m'}$,

$$[g, h]^{-1}[g', h'] \in K_{\min(m+n', m'+n)}.$$

Proof. Assuming (i), write $\tilde{g} = g^{-1}g', \tilde{h} = h^{-1}h'$. Then:

$$[g', h'] = [g, \tilde{h}][g, h][[g, h], \tilde{h}][[g, h\tilde{h}], \tilde{g}][\tilde{g}, h\tilde{h}]$$

by standard commutator identities. Now:

$$[g, \tilde{h}] \in K_{n+m'}$$
$$[[g, h], \tilde{h}] \in K_{n+m+m'}$$
$$[[g, h\tilde{h}], \tilde{g}] \in K_{n+n'+m}$$
$$[\tilde{g}, h\tilde{h}] \in K_{n'+m}$$

by (i), so that $[g, h] \equiv [g', h'] \bmod K_{\min(m+n', m'+n)}$.

Conversely, assuming (i'), let $g \in K_n$, $h \in K_m$. We may assume $n \leq m$. Then $g^{-1}h \in K_n$. Taking $n' = n$, $m' > m$ in (i'), we have $\min(m + n', m' + n) = n + m$, so we may set $g' = h' = h$ to obtain:

$$e = [h, h] \equiv [g, h] \bmod K_{n+m}.$$

In other words, $[g, h] \in K_{n+m}$, as required. □

The diameter bound will come from the following Lemma, the conditions of which we shall verify in the setting of Proposition 2.1.

Lemma 2.4. *Let G be a profinite group, $(K_n)_{n\geq 1}$ a descending sequence of open normal subgroups. Suppose there exist $n_0, B, D \in \mathbb{N}$, with $D \geq 2$, such that, for every $n \geq n_0$ and every symmetric $X \subseteq G$ with $1 \in X$,*

$$K_n/K_{Dn} \subseteq K_{Dn}X/K_{Dn} \Rightarrow K_{Dn}/K_{D^2n} \subseteq K_{D^2n}X^B/K_{D^2n}. \qquad (2)$$

Then $G/\bigcap_{n=1}^{\infty} K_n$ is finitely generated and there exists $C > 0$ (depending only on $B, |G/K_{Dn_0}|$) such that for any $n \in \mathbb{N}$,

$$\operatorname{diam}(G/K_n) \leq Cn^{\frac{\log(B)}{\log(D)}}.$$

Proof. Let $S \subseteq G$, and suppose the restriction of the natural epimorphism $\pi_{Dn_0} : G \twoheadrightarrow G/K_{Dn_0}$ to $\langle S \rangle$ is surjective. Then for some $l_0 \in \mathbb{N}$ (independent of S),

$$K_{Dn_0}B_S(l_0)/K_{Dn_0} = G/K_{Dn_0}$$

(we may always take $l_0 \leq |G/K_{Dn_0}|$). In particular we have $K_{n_0}/K_{Dn_0} \subseteq K_{Dn_0}B_S(l_0)/K_{Dn_0}$. By an easy induction involving (2), we have for any $i \in \mathbb{N}$,

$$K_{D^in_0}/K_{D^{i+1}n_0} \subseteq K_{D^{i+1}n_0}B_S(B^il_0)/K_{D^{i+1}n_0}.$$

It follows that, for any $n \leq D^in_0$,

$$\operatorname{diam}(G/K_n, S) \ll_{B,l_0} B^i.$$

Hence for arbitrary n, choosing i such that $D^{i-1}n_0 \leq n \leq D^i n_0$,

$$\mathrm{diam}(G/K_n, S) \ll_{B,l_0} B^{\frac{\log(n)}{\log(D)}} = n^{\frac{\log(B)}{\log(D)}}.$$

Now let $\overline{S} \subseteq G/K_n$ and suppose $\langle \overline{S} \rangle = G/K_n$. If $n \leq Dn_0$, then $\mathrm{diam}(G/K_n, \overline{S}) \leq l_0$. Otherwise, the image of $\overline{S}$ in G/K_{Dn_0} is a generating set, and the preceding argument applies.

In particular, let $\tilde{S} \subseteq G$ be finite with image in G/K_{Dn_0} a generating set. Then for every n, $\tilde{S}$ generates G modulo K_n, so $\tilde{S}$ maps to a topological generating set in $G/\bigcap_{n=1}^{\infty} K_n$. □

Proof of Proposition 2.1. Let $n \geq n_0$. Let $X \subseteq G$ be symmetric, with $1 \in X$, and suppose:

$$K_n/K_{2n} \subseteq K_{2n}X/K_{2n}. \tag{3}$$

Let $g \in K_{2n}$. By hypothesis (ii) there exist $g_1, \ldots, g_A, h_1, \ldots, h_A \in K_n$ such that:

$$g \equiv [g_1, h_1] \cdots [g_A, h_A] \bmod K_{3n}.$$

By (3) there exist $g_1', \ldots, g_A', h_1', \ldots, h_A' \in X$ with $g_i \equiv g_i', h_i \equiv h_i' \bmod K_{2n}$ for $i = 1, \ldots, A$. By hypothesis (i') from Lemma 2.3, $[g_i, h_i] \equiv [g_i', h_i'] \bmod K_{3n}$. Hence $g \equiv [g_1', h_1'] \cdots [g_A', h_A'] \bmod K_{3n}$, so that:

$$K_{2n}/K_{3n} \subseteq K_{3n}X^{4A}/K_{3n}. \tag{4}$$

Likewise, let $g \in K_{3n}$. There exist $g_1, \ldots, g_A \in K_n$, $h_1, \ldots, h_A \in K_{2n}$ such that:

$$g \equiv [g_1, h_1] \cdots [g_A, h_A] \bmod K_{4n}.$$

By (3) and (4) there exist $g_1', \ldots, g_A' \in X$ and $h_1', \ldots, h_A' \in X^{4A}$ such that $g_i \equiv g_i' \bmod K_{2n}$ and $h_i \equiv h_i' \bmod K_{3n}$, so that $[g_i, h_i] \equiv [g_i', h_i'] \bmod K_{4n}$ for $i = 1, \ldots, A$ and:

$$g \equiv [g_1', h_1'] \cdots [g_A', h_A'] \bmod K_{4n}.$$

Hence:

$$K_{3n}/K_{4n} \subseteq K_{4n}X^{8A^2+2A}/K_{4n}. \tag{5}$$

Combining (3), (4) and (5), we obtain $K_{2n}/K_{4n} \subseteq K_{4n}X^{8A^2+6A}/K_{4n}$. The required result now follows from Lemma 2.4, applied with $B = 8A^2 + 6A$, $D = 2$. □

Proposition 2.1 will suffice to prove Theorem 1.5 in the case of classical groups over pro-p rings. For general analytic pro-p groups and for the Nottingham group, however, generating elements as products of commutators is more difficult. For example, $[K_n, K_m]$ may not be the whole of K_{n+m} (as will always be the case in the setting of Proposition 2.1) but some deeper subgroup K_{n+m+k} (with $k \geq 1$ bounded independent of m, n). To circumvent these and other complexities of the general case, we prove a stronger version of Proposition 2.1, in which hypothesis (ii) has been weakened:

Proposition 2.5. *Let G be a profinite group, $(K_n)_{n\geq 1}$ a descending sequence of open normal subgroups of G. Suppose:*

(i) For all $m, n \geq 1$, $[K_m, K_n] \subseteq K_{m+n}$;

(ii) There exists $\epsilon \in (0,1)$; $A, M_1, M_2 \in \mathbb{N}$ such that for all $n \geq M_1$, there exist $n_i, m_i \in \mathbb{N}$ (for $i = 1, 2, 3$) with:

$$\tfrac{n}{3}(2+i+\epsilon) \leq n_i \leq m_i \leq \tfrac{2n}{3}(2+i);\ n_i + m_i = (2+i)n - M_2$$

and for all $g \in K_{(2+i)n}$, there exist:

$$g_1, \ldots, g_A \in K_{n_i}\ ,\ h_1, \ldots, h_A \in K_{m_i}$$

such that $[g_1, h_1] \cdots [g_A, h_A] g^{-1} \in K_{(2+i)n+n_i-M_2} = K_{2n_i+m_i}$.

Then $G/\bigcap_{n=1}^{\infty} K_n$ is finitely generated and there exists $C > 0$ (depending on A, $|G/K_{3n_0}|$, where $n_0 = \max\{2M_1, \lceil \frac{3M_2}{\epsilon} \rceil\}$) such that:

$$\operatorname{diam}(G/K_n) \leq C n^{\frac{6\log(4A+1)}{\log(3)}}.$$

Proof. First claim that for any $n \geq \max\{2M_1, \frac{3M_2}{\epsilon}\}$ and any symmetric $X \subseteq G$ with $1 \in X$,

$$K_n/K_{3n} \subseteq K_{3n}X/K_{3n} \Rightarrow K_n/K_{6n} \subseteq K_{6n}X^{(4A+1)^3}/K_{6n}. \tag{6}$$

Let $g \in K_{3n}$. By (ii), there exist $g_1, \ldots, g_A \in K_{n_1}$, $h_1, \ldots, h_A \in K_{m_1}$ with:

$$g \equiv [g_1, h_1] \cdots [g_A, h_A] \bmod K_{3n+n_1-M_2}.$$

By assumption, there exist $g_1', \ldots, g_A', h_1', \ldots, h_A' \in X$ such that $g_i \equiv g_i'$, $h_i \equiv h_i' \bmod K_{3n}$, so that $g_i' \in K_{n_1}$, $h_i' \in K_{m_1}$. By Lemma 2.3,

$$[g_i, h_i] \equiv [g_i', h_i'] \bmod K_{3n+n_1}.$$

Hence $g \equiv [g_1', h_1'] \cdots [g_A', h_A'] \bmod K_{3n+n_1-M_2}$.

Therefore:

$$K_{3n}/K_{3n+n_1-M_2} \subseteq K_{3n+n_1-M_2}X^{4A}/K_{3n+n_1-M_2}$$

and, combining with the hypothesis $K_n/K_{3n} \subseteq K_{3n}X/K_{3n}$,

$$K_n/K_{3n+n_1-M_2} \subseteq K_{3n+n_1-M_2}X^{4A+1}/K_{3n+n_1-M_2}.$$

In particular, since $n_1 \geq n + \frac{\epsilon n}{3} \geq n + M_2$, $K_n/K_{4n} \subseteq K_{4n}X^{4A+1}/K_{4n}$.

We now simply repeat the same procedure: let $n_2, m_2 \in \mathbb{N}$ be as above. We deduce:

$$K_{4n}/K_{4n+n_2-M_2} \subseteq K_{4n+n_2-M_2}X^{4A(4A+1)}/K_{4n+n_2-M_2}.$$

Combining this estimate with $K_n/K_{4n} \subseteq K_{4n}X^{4A+1}/K_{4n}$, and since $4n + n_2 - M_2 \geq 5n$, we have:

$$K_n/K_{5n} \subseteq K_{5n}X^{(4A+1)^2}/K_{5n}.$$

Finally let $n_3, m_3 \in \mathbb{N}$ be as above. We have:

$$K_{5n}/K_{5n+n_3-M_2} \subseteq K_{5n+n_3-M_2}X^{4A(4A+1)^2}/K_{5n+n_3-M_2}.$$

Combining with $K_n/K_{5n} \subseteq K_{5n}X^{(4A+1)^2}/K_{5n}$, since $5n + n_3 \geq 6n$, the claim follows.

In particular, (6) implies that for $n \geq \max\{2M_1, \frac{3M_2}{\epsilon}\}$,

$$K_n/K_{3n} \subseteq K_{3n}X/K_{3n} \implies K_{2n}/K_{6n} \subseteq K_{6n}X^{(4A+1)^3}/K_{6n}.$$

Applying (6) again, with n replaced by $2n$ and X replaced by $X^{(4A+1)^3}$,

$$K_{2n}/K_{12n} \subseteq K_{12n}X^{(4A+1)^6}/K_{12n}$$

so that in particular, $K_{3n}/K_{9n} \subseteq K_{9n}X^{(4A+1)^6}/K_{9n}$. The result now follows from Lemma 2.4, applied with $B = (4A+1)^6$, $D = 3$. □

The proof of Proposition 2.5 is sufficiently robust that qualitatively similar (though quantitatively worse) diameter bounds should be available under even weaker hypotheses. We shall not pursue such results here, as the level of generality already achieved is sufficient for all the examples we shall consider. We conclude this section by noting some cases in which hypothesis (i) of Propositions 2.1 and 2.5 is always satisfied.

Example 2.6. *(i) Let G be* any *pro-p group; K_n be the nth term of the lower central p-series for G.*

(ii) Let R be a unital profinite ring; $G \leq R^*$; $I \lhd R$ a proper two-sided open ideal. Define $K_n = G \cap (1 + I^n) \lhd G$. Let $n, m \in \mathbb{N}$ with $n \leq m$ and let $g \in K_n$, $h \in K_m$. Let $a, \tilde{a} \in I^m$, $b, \tilde{b} \in I^n$ be such that:

$$g = 1 + a,\ g^{-1} = 1 + \tilde{a},\ h = 1 + b,\ h^{-1} = 1 + \tilde{b}.$$

Then $a + \tilde{a} + \tilde{a}a = b + \tilde{b} + \tilde{b}b = 0$, so:

$$\begin{aligned}[g, h] &\equiv 1 + ab + \tilde{a}b + \tilde{a}\tilde{b} + \tilde{b}a \\ &\equiv 1 + ab - ba \mod I^{2n+m}.\end{aligned}$$

In particular, $[g, h] \in K_{n+m}$.

(iii) As a particular case of (ii), letting $R = \mathbb{F}_p G$ and $I \lhd R$ be the augmentation ideal, K_n is the nth mod-p dimension subgroup of G.

3 Classical Groups over R

In this section we prove Theorem 1.5 in the case for which X_l is classical, so that the associated adjoint Chevalley group over R is one of $\mathrm{PSL}_d(R)$, $\mathrm{PSO}_d(R)$, or $\mathrm{PSp}_d(R)$ (with d even in the latter case). To be more precise, we prove the diameter bound for $G = \mathrm{SL}_d(R), \mathrm{SO}_d(R)$ or $\mathrm{Sp}_d(R)$; $K_n = G \cap (I_d + \mathcal{P}^n \mathbb{M}_d(R))$. It shall be useful at this point to make a general observation, to the effect that diam behaves well with respect to extensions.

Lemma 3.1. *Let G be a finite group, $K \lhd G$. Then:*

(i) $\mathrm{diam}(G/K) \leq \mathrm{diam}(G)$.

(ii) $\mathrm{diam}(G) \leq (2 \cdot \mathrm{diam}(G/K) + 1) \cdot (\mathrm{diam}(K) + \frac{1}{2}) - \frac{1}{2}$.

Proof. (i) is straightforward.

(ii) Let $S \subseteq G$ be a generating set. Then $B_S(\mathrm{diam}(G/K))$ contains a transversal T to K in G, with $1 \in T$. By the Reidemeister-Schreier process, $B_S(2 \cdot \mathrm{diam}(G/K) + 1)$ contains a generating set for K. Hence:

$$\mathrm{diam}(G, S) \leq \mathrm{diam}(G/K) + \mathrm{diam}(K) \cdot (2 \cdot \mathrm{diam}(G/K) + 1).$$

□

The required result for the adjoint form then follows straightforwardly: letting $\rho : G \to GL_D(R)$ be the adjoint representation of G on the associated Lie algebra (of dimension D), for any $g \in G$, if $g \equiv I_d \bmod \mathcal{P}^n$ then $\rho(g) \equiv I_D \bmod \mathcal{P}^n$. Thus letting $K_n = G \cap (I_d + \mathcal{P}^n \mathbb{M}_d(R))$, $L_n = \rho(G) \cap (I_D + \mathcal{P}^n \mathbb{M}_D(R))$, ρ descends to an epimorphism $G/K_n \twoheadrightarrow \rho(G)/L_n$. By Lemma 3.1 (i),

$$\mathrm{diam}(\rho(G)/L_n) \leq \mathrm{diam}(G/K_n) \leq C_1(\log|G/K_n|)^{C_2}.$$

The polylogarithmic diameter bound in $|G/K_n|$ then translates to a polylogarithmic bound in $|\rho(G)/L_n|$ (with possibly larger constant C_1). For $|G/K_n| \ll |R/\mathcal{M}|^{d^2 n}$ and $|\rho(G)/L_n| \gg |R/\mathcal{M}|^n$.

We verify the hypotheses of Proposition 2.1 for $G = \mathrm{SL}_d(R)$, $\mathrm{SO}_d(R)$, or $\mathrm{Sp}_d(R)$. Recall that we permit ourselves the assumption that $p \geq 3$ unless $G = \mathrm{SL}_d(R)$ and $d \geq 3$. Hypothesis (i) follows immediately from Example 2.6 (ii). Moreover, for $g \in K_n$, $h \in K_m$, with $n \leq m \leq 2n$, writing:

$$g = I_d + \mathcal{P}^n X;\ h = I_d + \mathcal{P}^m Y$$

for some $X, Y \in \mathbb{M}_d(R)$, we have:

$$[g, h] \equiv I_d + \mathcal{P}^{m+n}(X, Y) \bmod \mathcal{P}^{m+2n}$$

where $(X, Y) = XY - YX$ is the Lie bracket. Hence for $g_1, \ldots, g_A \in K_n$, $h_1, \ldots, h_A \in K_m$, writing $g_i = I_d + \mathcal{P}^n X_i$, $h_i = I_d + \mathcal{P}^m Y_i$, we have:

$$[g_1, h_1] \cdots [g_A, h_A] \equiv I_d + \mathcal{P}^{m+n}((X_1, Y_1) + \ldots + (X_A, Y_A)) \bmod \mathcal{P}^{m+2n}.$$

To verify hypothesis (ii) of Proposition 2.1, it therefore suffices to find $A \in \mathbb{N}$ (independent of G) such that, for any $g \in K_{m+n}$, we can find $X_1, \ldots X_A$, $Y_1, \ldots, Y_A \in \mathbb{M}_d(R)$ such that:

(a) $g - I_d \equiv \mathcal{P}^{m+n}((X_1, Y_1) + \ldots + (X_A, Y_A)) \bmod \mathcal{P}^{m+2n}$;

(b) There exist $g_1, \ldots, g_A \in K_n$, $h_1, \ldots, h_A \in K_m$ such that

$$g_i - I_d \equiv \mathcal{P}^n X_i \bmod \mathcal{P}^{2n},\ h_i - I_d \equiv \mathcal{P}^m Y_i \bmod \mathcal{P}^{2m}$$

for $1 \leq i \leq A$.

As in the statement of Proposition 2.1, finding A independent of G yields an exponent C_2 in Theorem 1.5 independent of X_l. For $G = \mathrm{SL}_d(R)$, $\mathrm{SO}_d(R)$ or $\mathrm{Sp}_d(R)$, let $\mathfrak{g} = \mathfrak{sl}_d(R)$, $\mathfrak{so}_d(R)$ or $\mathfrak{sp}_d(R)$ be the associated Lie ring over R. Conditions (a), (b) above will follow straightforwardly from the following assertions, which we then verify for each group scheme in turn.

(a') For every $n \in \mathbb{N}$ and every $g \in K_n$, there exists $X \in \mathfrak{g}$ such that such that $g - I_d \equiv \mathcal{P}^n X \bmod \mathcal{P}^{2n}$.

(b') There exists $A \in \mathbb{N}$ (independent of $\mathfrak{g}$) such that every element of $\mathfrak{g}$ is the sum of at most A brackets in $\mathfrak{g}$ (as we shall see, it suffices to take $A = 3$).

(c') There exists $\mathcal{B} \subseteq \mathfrak{g}$, generating $\mathfrak{g}$ as a $\mathbb{Z}$-module, such that for every $n \in \mathbb{N}$ and every $X \in \mathcal{B}$, there exists $g \in K_n$ such that $g - I_d \equiv \mathcal{P}^n X \bmod \mathcal{P}^{2n}$.

For, given $g \in K_{n+m}$, we immediately produce X_i, Y_i as in (a) by applying (a'), (b') to g. Now writing an arbitrary element $Z \in \mathfrak{g}$ as $\sum_{i=1}^r Z_i$, for $Z_i \in \mathcal{B}$, and letting $k_1, \ldots, k_r \in K_l$ be such that $k_i - I_d \equiv \mathcal{P}^l Z_i \bmod \mathcal{P}^{2l}$ as in (c'), we have:

$$I_d + \mathcal{P}^l Z \equiv k_1 \cdots k_r \in K_l \bmod \mathcal{P}^{2l}.$$

Applying this observation to X_i, Y_i with $l = n, m$ respectively, we obtain g_i, h_i as in (b).

3.1 SL_d

Let $\mathfrak{sl}_d(R)$ denote the space of traceless $d \times d$ matrices over R; it is spanned over R by the matrices $E_{i,j}$, $D_{a,b}$, for $i \neq j$, $a < b$, where:

$$(E_{i,j})_{r,s} = \delta_{i,r}\delta_{j,s},\ (D_{a,b})_{r,s} = \delta_{a,r}\delta_{a,s} - \delta_{b,r}\delta_{b,s}.$$

(a') Let $g \in K_n$. Write $g = I_d + \mathcal{P}^n X$, for some $X \in \mathbb{M}_d(R)$. Then:

$$1 = \det(g) \equiv 1 + \mathcal{P}^n \operatorname{tr}(X) \bmod \mathcal{P}^{2n}$$

so $\operatorname{tr}(X) \equiv 0 \bmod \mathcal{P}^n$. Hence there exists $X' \in \mathfrak{sl}_d(R)$ such that $X \equiv X' \bmod \mathcal{P}^n$.

(b') First suppose $d \geq 3$. Define the R-module endomorphisms $T_1, T_2 : \mathfrak{sl}_d(R) \to \mathfrak{sl}_d(R)$ by:

$$T_1(X) = \Big(X, \sum_{i=1}^{d-1} E_{i+1,i}\Big), T_2(X) = \Big(X, \sum_{i=1}^{d-1} E_{i,i+1}\Big).$$

Then:

$$\begin{aligned} D_{j,j+1} &= T_1(E_{j,j+1}) \text{ for } j = 1, \ldots, d-1, \\ E_{i,j-1} - E_{i+1,j} &= T_1(E_{i,j}) \text{ for } 1 \leq i \leq d-1,\ i+2 \leq j \leq d, \\ E_{1,i+1} &= T_1(-E_{i,1}) \text{ for } 2 \leq i \leq d-1, \\ E_{3,2} - 2E_{2,1} &= T_1(D_{1,2}). \end{aligned}$$

Transposing, the following also lie in $\mathrm{im}(T_2)$:

$$\begin{aligned} E_{i-1,j} - E_{i,j+1}, \text{ for } 1 \le j \le d-1,\ j+2 \le i \le d, \\ E_{j+1,1}, \text{ for } 2 \le j \le d-1, \\ E_{2,3} - 2E_{1,2} \end{aligned}$$

It may therefore be seen that $\mathrm{im}(T_1) \cup \mathrm{im}(T_2)$ contains an R-basis for $\mathfrak{sl}_d(R)$, so $\mathfrak{sl}_d(R) = \mathrm{im}(T_1) + \mathrm{im}(T_2)$. Now suppose $d = 2$ and $p > 2$. Then for any $a, b, c, \in R$,

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} = (\begin{pmatrix} 0 & -b \\ c & 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} \end{pmatrix}) + (\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}).$$

(c') Let $\mathcal{B} = \{xE_{i,j} : x \in R, i \neq j\} \cup \{x(D_{a,b} + E_{a,b} - E_{b,a}) : x \in R, a < b\}$. Then $\mathcal{B}$ clearly spans $\mathfrak{sl}_d(R)$ and, for any $n \in \mathbb{N}$, $X \in \mathcal{B}$, $\det(I_d + \mathcal{P}^n X) = 1$.

Remark 3.2. *The preceding argument breaks down for $d = 2$, $p = 2$. Let $X, Y \in \mathbb{M}_2(R)$ with $\mathrm{tr}(X) = \mathrm{tr}(Y) = 0$. Then:*

$$(X, Y) \equiv (X_{12}Y_{21} - X_{21}Y_{12}) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mod \mathcal{P}.$$

Hence we cannot express an arbitrary traceless matrix as a sum of brackets, as we do above in higher characteristic.

3.2 SO_d

Denote by $\mathfrak{so}_d(R)$ the space of skew-symmetric $d \times d$ matrices over R; it is spanned over R by the matrices $X_{i,j} = E_{i,j} - E_{j,i}$, for $1 \le i < j \le d$.

(a') Let $g \in K_n$. Write $g = I_d + \mathcal{P}^n X$, for some $X \in \mathbb{M}_d(R)$. Then:

$$I_d = (I_d + \mathcal{P}^n X)(I_d + \mathcal{P}^n X^T) \equiv I_d + \mathcal{P}^n (X + X^T) \mod \mathcal{P}^{2n}$$

so $X^T \equiv -X \mod \mathcal{P}^n$. Hence there exists $X' \in \mathfrak{so}_d$ such that $X \equiv X' \mod \mathcal{P}^n$.

(b') Define the R-module endomorphisms $T_1, T_2, T_3 : \mathfrak{so}_d(R) \to \mathfrak{so}_d(R)$ by:

$$\begin{aligned} T_1(X) &= \big(X, \sum_{i=1}^{d-1} X_{i,i+1}\big), \\ T_2(X) &= (X, X_{1,d-1} + X_{1,d} + X_{2,d}), \\ T_3(X) &= (X, X_{1,2}). \end{aligned}$$

Then for $1 < i < d-1$,

$$X_{i,i+2} - X_{i-1,i+1} = T_1(X_{i,i+1});\ X_{i+1,d} - X_{i-1,d} - X_{i,d-1} = T_1(X_{i,d}).$$

For $1 < j < d-1$,

$$X_{2,j} + X_{1,j+1} - X_{1,j-1} = T_1(X_{1,j}).$$

For $1 < i, j < d$, with $i + 1 < j$,

$$X_{i+1,j} + X_{i,j+1} - X_{i-1,j} - X_{i,j-1} = T_1(X_{i,j}).$$

For $3 \leq j \leq d-2$,

$$X_{1,j} = T_2(X_{j,d-1});\ X_{j,d} = T_2(-X_{2,j})$$

and:

$$X_{1,2} = T_2(-X_{2,d});\ X_{d-1,d} = T_2(X_{1,d-1});\ X_{1,d-1} = T_3(-X_{2,d-1});$$
$$X_{1,d} = T_3(-X_{2,d});\ X_{2,d} = T_3(-X_{1,d}).$$

Therefore $\mathrm{im}(T_1) \cup \mathrm{im}(T_2) \cup \mathrm{im}(T_3)$ contains an R-basis for $\mathfrak{so}_d(R)$, so $\mathfrak{so}_d(R) = \mathrm{im}(T_1) + \mathrm{im}(T_2) + \mathrm{im}(T_3)$.

(c') For $\alpha \in R$, $l \in \mathbb{N}$, consider the polynomial $f(X) = X^2 - (1 - \alpha^2\mathcal{P}^{2l})$. Then $f(1) = \alpha^2\mathcal{P}^{2l} \equiv 0 \bmod \mathcal{P}^{2l}$ but $f'(1) = 2 \not\equiv 0 \bmod \mathcal{P}$. By Hensel's Lemma, there exists $\beta \in R$ such that $f(\beta) = 0$ and $\beta \equiv 1 \bmod \mathcal{P}^{2l}$. Hence for any $i \neq j$,

$$g_{i,j}^{(l)}(\alpha) := I_d + \alpha\mathcal{P}^l(E_{i,j} - E_{j,i}) + (\beta - 1)(E_{i,i} + E_{j,j}) \in K_l$$

and $g_{i,j}^{(l)}(\alpha) \equiv I_d + \alpha\mathcal{P}^l(E_{i,j} - E_{j,i}) \bmod \mathcal{P}^{2l}$.

Remark 3.3. In contrast to the cases of $\mathrm{SL}_d(R)$ and $\mathrm{Sp}_d(R)$, $\mathrm{SO}_d(R)$ is not in general the universal form of the Chevalley group of its type; the universal form is rather a proper central extension of $\mathrm{SO}_d(R)$ by a finite group. Increasing the constant C_1 in Theorem 1.5, the diameter bounds obtained above for SO_d extend to the universal form by Lemma 3.1 (ii).

3.3 Sp_d

Let $d = 2g$ and let $\Omega = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}$, so that $\mathfrak{sp}_d(R)$ is the set of $d \times d$ matrices X over R satisfying the relation $X^T\Omega + \Omega X = 0$. Suppose $p > 2$.

For $1 \leq i, j \leq g$, define the following elements of $\mathfrak{sp}_d(R)$:

$$A_{i,j} = \begin{pmatrix} E_{i,j} & 0 \\ 0 & -E_{j,i} \end{pmatrix}, B_{i,j} = \begin{pmatrix} 0 & E_{i,j} + E_{j,i} \\ 0 & 0 \end{pmatrix},$$
$$C_{i,j} = \begin{pmatrix} 0 & 0 \\ E_{i,j} + E_{j,i} & 0 \end{pmatrix}.$$

We have:

$$\begin{aligned}
(A_{i,j}, A_{k,l}) &= \delta_{j,k}A_{i,l} - \delta_{i,l}A_{k,j}, \\
(A_{i,j}, B_{k,l}) &= \delta_{j,k}B_{i,l} + \delta_{j,l}B_{i,k}, \\
(A_{i,j}, C_{k,l}) &= \delta_{i,l}C_{j,k} - \delta_{i,k}C_{j,l}, \\
(B_{i,j}, C_{k,l}) &= \delta_{j,k}A_{i,l} + \delta_{j,l}A_{i,k} + \delta_{i,k}A_{j,l} + \delta_{i,l}A_{j,k}.
\end{aligned}$$

Hence:

$$\begin{aligned}
A_{i,j} &= (A_{i,j}, A_{j,j}), \text{ for } i \neq j, \\
A_{i,i} &= (\frac{1}{2}B_{i,i}, \frac{1}{2}C_{i,i}), \\
B_{i,j} &= (A_{i,k}, B_{k,j}), \text{ for } i \neq k \neq j, \\
C_{i,j} &= (A_{k,i}, C_{j,k}), \text{ for } i \neq k \neq j.
\end{aligned}$$

(a') Let $g \in K_n$. Write $g = I_d + \mathcal{P}^n X$, for some $X \in \mathbb{M}_d(R)$. Then:

$$\begin{aligned}
\Omega &= g^T\Omega g \\
&= \Omega + \mathcal{P}^n(\Omega X + X^T\Omega) + \mathcal{P}^{2n}X^T\Omega X \\
&\equiv \Omega + \mathcal{P}^n(\Omega X + X^T\Omega) \mod \mathcal{P}^{2n}
\end{aligned}$$

so $\Omega X + X^T\Omega \equiv 0 \mod \mathcal{P}^n$. Hence there exists $X' \in \mathfrak{sp}_d(R)$ such that $X \equiv X' \mod \mathcal{P}^n$.

(b') Define the R-module endomorphisms $U_1, U_2 : \mathfrak{sp}_d(R) \to \mathfrak{sp}_d(R)$ by:

$$U_1(X) = \big(X, \sum_{i=1}^{g} A_{i,i}\big)$$
$$U_2(X) = \big(X, \sum_{i=1}^{g} (B_{i,i} + C_{i,i})\big).$$

Then for any $1 \leq i, j \leq g$, $B_{i,j}, C_{i,j} \in \mathrm{im}(U_1)$, $A_{i,j} + A_{j,i} \in \mathrm{im}(U_2)$. Define the R-Lie subring $V \leq \mathfrak{sp}_d(R)$:

$$V = \{ \begin{pmatrix} X & 0 \\ 0 & -X^T \end{pmatrix} : X \in \mathfrak{gl}_g(R) \}.$$

We show that, for any $X \in \mathfrak{so}_g(R)$, there exist $v_1, v_2 \in V$ and symmetric $Z \in \mathfrak{gl}_g(R)$ such that:

$$\begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} = (v_1, v_2) + \begin{pmatrix} Z & 0 \\ 0 & -Z \end{pmatrix}.$$

Now for an arbitrary element $v \in \mathfrak{sp}_d(R)$ there exist $X \in \mathfrak{so}_g(R)$ and symmetric $B, C, Y \in \mathfrak{gl}_g(R)$ such that:

$$\begin{aligned} v &= \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} + \begin{pmatrix} Y & 0 \\ 0 & -Y \end{pmatrix} + \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix} \\ &= (v_1, v_2) + \begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix} + \begin{pmatrix} Y+Z & 0 \\ 0 & -(Y+Z) \end{pmatrix} \end{aligned}$$

and $\begin{pmatrix} 0 & B \\ C & 0 \end{pmatrix} \in \mathrm{im}(U_1)$, $\begin{pmatrix} Y+Z & 0 \\ 0 & -(Y+Z) \end{pmatrix} \in \mathrm{im}(U_2)$, so that every element of $\mathfrak{sp}_d(R)$ is expressible as a sum of three brackets.

It will suffice to check that any element of $\mathfrak{so}_g(R)$ is expressible as the sum of a bracket in $\mathfrak{gl}_g(R)$ and a symmetric matrix. Define the R-module endomorphisms $S_1, S_2 : \mathfrak{gl}_g(R) \to \mathfrak{gl}_g(R)$ by:

$$\begin{aligned} S_1(X) &= (X, E_{1,1}) \\ S_2(X) &= \big(X, \sum_{i=1}^{d-1} (E_{i,i+1} - E_{i+1,i})\big) \end{aligned}$$

and for $X \in \mathfrak{gl}_g(R)$, write $X = X_1 + X_2$, with X_1 symmetric, X_2 skew-symmetric. Then:

$$\big(X, E_{1,1} + \sum_{i=1}^{d-1} (E_{i,i+1} - E_{i+1,i})\big) - S_1(X_1) - S_2(X_2)$$

is symmetric. We already described the image of $S_2 \mid_{\mathfrak{so}_g(R)}$ (in the guise of T_1 in our analysis of SO_d). For $2 \leq i \leq g$,

$$S_1(E_{1,i} + E_{i,1}) = E_{i,1} - E_{1,i}.$$

These elements, together with $\mathrm{im}(S_2 \mid_{\mathfrak{so}_g(R)})$, span $\mathfrak{so}_g(R)$ over R, and the result follows.

(c') For any $\alpha \in R$ and any $l \in \mathbb{N}$ we have:

$$I_d + \alpha\mathcal{P}^l B_{i,j}, I_d + \alpha\mathcal{P}^l C_{i,j} \in K_l \text{ for any } 1 \leq i, j, \leq d.$$
$$I_d + \alpha\mathcal{P}^l A_{i,j} \in K_l \text{ provided } i \neq j.$$

Finally, $(1+\alpha\mathcal{P}^l)^{-1} \equiv 1 - \alpha\mathcal{P}^l \mod \mathcal{P}^{2l}$, so:

$$g := I + \begin{pmatrix} \alpha\mathcal{P}^l E_{i,i} & 0 \\ 0 & ((1+\alpha\mathcal{P}^l)^{-1} - 1)E_{i,i} \end{pmatrix} \in K_l$$

and $g \equiv I + \alpha t^{\mathcal{P}} A_{i,i} \mod \mathcal{P}^{2l}$.

Remark 3.4. For $R = \mathbb{Z}_p$, the value $A = 3$ was achieved in [13], under the additional assumption that $p \geq \frac{l+2}{2}$, where l is the rank of the associated Chevalley group scheme. This assumption was necessary in the specific manipulations the root systems which were applied in Dinai's argument. Hence even in the p-adic case, the results of this Section are new in large rank for small p.

4 Analytic Pro-p Groups

In this section we prove Theorem 1.2. We start by recalling some preliminaries about groups with an R-analytic structure. Recall that $(R, \mathcal{M})$ is a discrete valuation pro-p domain, with $\mathcal{M}$ generated by $\mathcal{P} \in \mathcal{M}$. For proofs of results quoted, refer to Chapter 13 of [14].

Definition 4.1. *Denote by $R[[\underline{X}, \underline{Y}]]$ the ring of formal non-commuting power series in the $2d$ variables $X_1, \ldots, X_d, Y_1, \ldots, Y_d$. For $i = 1, \ldots, d$, let $F_i(\underline{X}, \underline{Y}) \in R[[\underline{X}, \underline{Y}]]$. Then $\underline{F} = (F_1, \ldots, F_d)$ is a* formal group law*, of dimension d over R, if:*

(i) $\underline{F}(\underline{X}, \underline{0}) = \underline{X}$ *and* $\underline{F}(\underline{0}, \underline{Y}) = \underline{Y}$,

(ii) $\underline{F}(\underline{X}, \underline{F}(\underline{Y}, \underline{Z})) = \underline{F}(\underline{F}(\underline{X}, \underline{Y}), \underline{Z})$.

Proposition 4.2 (13.16 in [14])**.** *Let $\underline{F}$ be a formal group law. There exist power series $\underline{B}(\underline{X}, \underline{Y})$, $\underline{I}(\underline{X})$, $\underline{O}(\underline{X}, \underline{Y})$, $\underline{P}(\underline{X})$, $\underline{Q}(\underline{X}, \underline{Y})$, with $\underline{B}$ bilinear in $\underline{X}$ and $\underline{Y}$; every term of $\underline{O}, \underline{P}, \underline{Q}$ having total degree at least 3 and every term of $\underline{O}, \underline{Q}$ having degree at least 1 in each of $\underline{X}, \underline{Y}$, such that:*

(i) $\underline{F}(\underline{X},\underline{Y}) = \underline{X} + \underline{Y} + \underline{B}(\underline{X},\underline{Y}) + \underline{O}(\underline{X},\underline{Y})$,

(ii) $\underline{I}(\underline{X}) = -\underline{X} + \underline{B}(\underline{X},\underline{X}) + \underline{P}(\underline{X})$ *and* $\underline{F}(\underline{X},\underline{I}(\underline{X})) = \underline{0} = \underline{F}(\underline{I}(\underline{X}),\underline{X})$,

(iii) $\underline{F}((\underline{I}\circ\underline{F})(\underline{Y},\underline{X}),\underline{F}(\underline{X},\underline{Y})) = \underline{B}(\underline{X},\underline{Y}) - \underline{B}(\underline{Y},\underline{X}) + \underline{Q}(\underline{X},\underline{Y})$.

Definition 4.3. *An* R-standard group *of dimension* d *is a topological group* $(G,\cdot)$ *with underlying space* $G = \mathcal{M}^{(d)}$ *such that there exists a formal group law* $\underline{F}$ *of dimension* d *such that, for all* $g,h \in G$,

$$g \cdot h = \underline{F}(g,h).$$

Note that, for $\underline{B},\underline{I},\underline{Q}$ *as in Proposition 4.2, we have:*

$$g^{-1} = \underline{I}(g),\ [g,h] = \underline{B}(g,h) - \underline{B}(h,g) + \underline{Q}(g,h).$$

Example 4.4. *(i)* $(\mathcal{M}^{(d)},+)$ *is an* R*-standard group of dimension* d.

(ii) Let $\mathrm{GL}_d^1(R) = I_d + \mathcal{PM}_d(R)$. *Then* $\mathrm{GL}_d^1(R) \leq \mathrm{GL}_d(R)$ *and, identifying* $\mathrm{GL}_d^1(R)$ *with* $\mathcal{M}^{(d^2)}$ *in the obvious way, multiplication in* $\mathrm{GL}_d^1(R)$ *is given by a formal group law of dimension* d^2.

(iii) Let $\mathrm{SL}_d^1(R) = \mathrm{SL}_d(R) \cap \mathrm{GL}_d^1(R)$ *be the kernel of the congruence map* $\mathrm{SL}_d(R) \twoheadrightarrow \mathrm{SL}_d(R/\mathcal{M})$. *Then we may identify* $\mathrm{SL}_d^1(R)$ *with* $\mathcal{M}^{(d^2-1)}$ *via* $A \mapsto ((A-I_d)_{i,j})_{(i,j)\neq(d,d)}$ *(since these* d^2-1 *co-ordinates together with the determinant condition uniquely determine* $A_{d,d}$*). Under this identification, multiplication in* $\mathrm{SL}_d^1(R)$ *is given by a formal group law of dimension* d^2-1.

Proposition 4.5 (13.22 in [14])**.** *For* $n,m \in \mathbb{N}$, *let* $K_n = (\mathcal{M}^n)^{(d)} \subseteq G$. *Then:*

(i) $K_n \lhd_o K_1 = G$,

(ii) $[K_n,K_m] \subseteq K_{n+m}$,

(iii) If $m \leq n$, K_n/K_{n+m} *is isomorphic to the additive group* $(\mathcal{M}^n/\mathcal{M}^{n+m})^{(d)}$

(iv) $G \cong \varprojlim G/K_n$ *is a pro-p group.*

Theorem 4.6 (13.20 in [14])**.** *Let* G *be an* R*-analytic group. Then* G *has an open* R*-standard subgroup.*

Proposition 4.7 (13.24 in [14])**.** *For* $v,w \in \mathcal{M}^{(d)}$, *define:*

$$(v,w) = \underline{B}(v,w) - \underline{B}(w,v).$$

Then $L(G) = (\mathcal{M}^{(d)}, +, (\cdot,\cdot))$ is a R-Lie ring. That is, $(\cdot,\cdot)$ satisfies the Jacobi identity (and is obviously R-bilinear antisymmetric).

Remark 4.8. *For each n, $\mathcal{P}^n L(G)$ is a Lie subring of $L(G)$. As a set it is equal to K_{n+1}. Moreover by Proposition 4.2, the additive cosets of $\mathcal{P}^n L(G)$ in $L(G)$ are the same as the multiplicative cosets of K_{n+1} in G.*

Definition 4.9. *The* Lie algebra *of G is $\mathcal{L}_G = L(G) \bigotimes_R \mathbb{K}$, where $\mathbb{K}$ is the field of fractions of R.*

Example 4.10. *(i) For $G = (\mathcal{M}^{(d)}, +)$, $\mathcal{L}_G$ is the d-dimensional abelian $\mathbb{K}$-Lie algebra.*

(ii) $\mathcal{L}_{\mathrm{GL}_d^1(R)} = \mathfrak{gl}_d(\mathbb{K})$.

(iii) $\mathcal{L}_{\mathrm{SL}_d^1(R)} = \mathfrak{sl}_d(\mathbb{K})$.

Proposition 4.11. *Suppose $\mathcal{L}_G$ is perfect. There exists $k \in \mathbb{N}$ such that every element of $(\mathcal{M}^k)^{(d)}$ is expressible as a sum of at most d brackets in L_G.*

Proof. Let $\{x_1, \ldots, x_d\}$ be a R-basis for $L(G)$. Then there exist $r_i, s_i \in \{1, \ldots, d\}$ such that $\{(x_{r_1}, x_{s_1}), \ldots, (x_{r_d}, x_{s_d})\}$ is a $\mathbb{K}$-basis for $\mathcal{L}_G$. Let $\lambda_{i,j} \in \mathbb{K}$ be such that:

$$x_i = \sum_{j=1}^{d} \lambda_{i,j}(x_{r_j}, x_{s_j}).$$

Let $k \in \mathbb{N}$ be defined by:

$$\|\mathcal{P}\|^{-k} = \max(\{1\} \cup \{\|\lambda_{i,j}\| : 1 \leq i, j \leq d\}).$$

Then for any $1 \leq i, j \leq d$, $\mathcal{P}^k \lambda_{i,j} \in R$. Hence for any $x \in L(G)$, there exist $\mu_1, \ldots, \mu_d \in R$ such that:

$$\begin{aligned} \mathcal{P}^k x = \mathcal{P}^k \sum_{i=1}^{d} \mu_i x_i &= \mathcal{P}^k \sum_{i=1}^{d} \mu_i \sum_{j=1}^{d} \lambda_{i,j}(x_{r_j}, x_{s_j}) \\ &= \sum_{j=1}^{d} (\sum_{i=1}^{d} \mu_i \mathcal{P}^k \lambda_{i,j} x_{r_j}, x_{s_j}) \end{aligned}$$

as required. □

Proof of Theorem 1.2. We verify the hypotheses of Proposition 2.5. Hypothesis (i) is Proposition 4.5 (ii). For hypothesis (ii), we take ϵ arbitrary; $A = d$; $M_1 \geq \max\{\frac{k}{3} + 1, 2\}$; $M_2 = k$, where k is as in Proposition 4.11. For $i = 1, 2, 3$ choose $\frac{n}{3}(2 + i + \epsilon) \leq n_i \leq m_i \leq \frac{2n}{3}(2 + i)$ such that $n_i + m_i = (2 + i)n - M_2$ (this is possible by our choice of M_1, M_2).

Let $g \in K_{(2+i)n}$. Let $h \in K_{M_2}$ be such that $g = \mathcal{P}^{n_i+m_i}h$. Selecting $g_1, \ldots, g_d, h_1, \ldots, h_d \in G$ such that:

$$h = \sum_{i=1}^{d} (g_i, h_i),$$

$$\begin{aligned} g &= \sum_{i=1}^{d} (\mathcal{P}^{n_i} g_i, \mathcal{P}^{m_i} h_i) \\ &\equiv \sum_{i=1}^{d} [\mathcal{P}^{n_i} g_i, \mathcal{P}^{m_i} h_i] \bmod \mathcal{P}^{2n_i+m_i} \text{ (by Proposition 4.2 (iii))} \\ &\equiv [\mathcal{P}^{n_i} g_1, \mathcal{P}^{m_i} h_1] \cdots [\mathcal{P}^{n_i} g_d, \mathcal{P}^{m_i} h_d] \bmod \mathcal{P}^{2n_i+2m_i} \text{ (by Proposition 4.2 (i)).} \end{aligned}$$

Since $2n_i + m_i = (2 + i)n + n_i - M_2$, we are done. □

4.1 FAb p-adic Analytic Groups

In the case of a group G with an analytic structure over $\mathbb{Z}_p$, there is an alternative approach to constructing the Lie algebra of G, based on the concept of a *uniform* subgroup, rather than a $\mathbb{Z}_p$*-standard* subgroup. We will utilise this approach to complete the proof of Theorem 1.4. Let $p \geq 3$ be prime. Let G be a finitely generated pro-p group. Let $(G_n)_n$ be the lower central p-series of G.

Definition 4.12. *G is* powerful *if $G/\overline{G^p}$ is abelian. G is* uniform *if it is powerful and torsion-free. The* dimension *of a uniform group G is the minimal size of a topological generating set.*

Example 4.13. Recall ([19]) that every compact p-adic analytic group has an open characteristic uniform subgroup. Indeed, every $\mathbb{Z}_p$-standard group of dimension d is a uniform pro-p group of dimension d (8.31 of [14]). Conversely, if G is a d-dimensional uniform pro-p group, then G_2 is a d-dimensional $\mathbb{Z}_p$-standard group (8.23 (iii) of [14]). In particular, every compact p-adic analytic group has an open characteristic $\mathbb{Z}_p$-standard subgroup. We describe the formal group law on G_2 below.

We recall some properties of uniform groups. Unless otherwise specified, let G be a d-dimensional uniform group.

Theorem 4.14 (3.6, 4.9 in [14]). *Let $\{a_1, \ldots, a_d\}$ be a topological generating set for G; $n, m \in \mathbb{N}$.*

(i) $(\lambda_1, \ldots, \lambda_d) \mapsto a_1^{\lambda_1} \cdots a_d^{\lambda_d}$ *defines a homeomorphism* $\mathbb{Z}_p^d \to G$.

(ii) G_{n+1} *is uniform of dimension* d.

(iii) $(G_{n+1})_{m+1} = G_{m+n+1}$.

(iv) $G_{n+1} = \{x^{p^n} : x \in G\}$.

(v) $\{a_1^{p^n}, \ldots, a_d^{p^n}\}$ *is a topological generating set for* G_{n+1}

There is a complete normed $\mathbb{Q}_p$-algebra $\hat{A}$, an embedding $G \hookrightarrow \hat{A}^*$ satisfying:

$$\forall g \in G, g - 1 \in \hat{A}_0, \text{ where } \hat{A}_0 = \{x \in \hat{A} : \|x\| \leq p^{-1}\}$$

and mutually inverse analytic functions:

$$\log : 1 + \hat{A}_0 \to \hat{A}_0,$$
$$\exp : \hat{A}_0 \to 1 + \hat{A}_0.$$

$\hat{A}$ is naturally a $\mathbb{Q}_p$-Lie algebra with Lie bracket:

$$(x, y) = xy - yx.$$

$\log(G)$ is a free d-dimensional $\mathbb{Z}_p$-module and a $\mathbb{Z}_p$-Lie subalgebra of $\hat{A}$.

Lemma 4.15 (6.25 and 7.12 from [14]). *Let $x \in \hat{A}_0$, $n \in \mathbb{Z}$.*

(i) $\exp(nx) = \exp(x)^n$.

(ii) $\log((1 + x)^n) = n \log(1 + x)$.

(iii) $(\log(G), \log(G)) \subseteq p \log(G)$.

Moreover, for $g \in G$, $\lambda \in \mathbb{Z}_p$, $\lambda \log(g) = \log(g^\lambda)$.

Combining this Lemma with Theorem 4.14 (iv), we have:

Corollary 4.16. *For all $n \in \mathbb{N}$, $p^n \log(G) = \log(G_{n+1})$.*

Proposition 4.17 (6.27 and 6.28 in [14]). *There are formal non-commutative power series $\Phi(X,Y)$, $\Psi(X,Y)$ satisfying:*

$$\Phi(X,Y) = X + Y + \frac{1}{2}(XY - YX) + h.o.(X,Y)$$
$$\Psi(X,Y) = (XY - YX) + h.o.(X,Y)$$

(with $h.o.(X,Y)$ denoting terms composed of brackets of length at least three) such that, for $x, y \in \hat{A}_0$,

(i) $\Phi(x,y)$ *converges to* $\log(\exp(x)\exp(y))$,

(ii) $\Psi(x,y)$ *converges to* $\log(\exp(-x)\exp(-y)\exp(x)\exp(y))$.

Remark 4.18. *Let $x_1, \ldots, x_d \in \log(G)$ be a $\mathbb{Z}_p$-basis for $\log(G)$. Identify $\mathbb{Z}_p^{(d)}$ with $\log(G)$ via:*

$$\theta : (\alpha_i)_{i=1}^d \mapsto \sum_{i=1}^d \alpha_i x_i.$$

Then, identifying $\mathbb{Z}_p^{(d)}$ with G via $\exp \circ \theta$, multiplication in G corresponds to the formal group law:

$$(\underline{a}, \underline{b}) \mapsto \theta^{-1}(\Phi(\theta(\underline{a}), \theta(\underline{b})))$$

on $\mathbb{Z}_p^{(d)}$. Moreover, under this identification the subgroup G_{n+1} corresponds to $p^n \log(G) = \theta((p^n\mathbb{Z}_p)^{(d)})$, by Corollary 4.16. In particular, $G_2 \cong (p\mathbb{Z}_p)^{(d)}$ is a $\mathbb{Z}_p$-standard subgroup.

Proposition 4.19 (4.8 and 4.31 in [14]). *Let H be a uniform closed subgroup of G; $N \lhd G$ be closed such that G/N is uniform.*

(i) $\log(H)$ *is a $\mathbb{Z}_p$-subalgebra of* $\log(G)$.

(ii) N *is uniform, with* $\dim(N) = \dim(G) - \dim(G/N)$.

(iii) $\log(N)$ *is an ideal in* $\log(G)$, *and* $\log(G/N) \cong \log(G)/\log(N)$.

Proposition 4.20 (7.15 in [14]). *Let S be a $\mathbb{Z}_p$-Lie subalgebra of $\log(G)$ such that the $\mathbb{Z}_p$-module $\log(G)/S$ is torsion-free.*

(i) $\exp(S)$ *is a closed uniform subgroup of G.*

(ii) If S is an ideal of $\log(G)$, then $\exp(S) \lhd G$ and $G/\exp(S)$ is uniform.

Define $\mathcal{L}_G = \mathrm{span}_{\mathbb{Q}_p}(\log(G))$, a d-dimensional $\mathbb{Q}_p$-Lie algebra. By Remark 4.18, this is isomorphic to the Lie algebra described in Definition 4.9.

Proposition 4.21. *The following are equivalent:*

(i) G has finite abelianisation.

(ii) G is FAb.

(iii) $\mathcal{L}_G$ is perfect.

Proof. $(ii) \Rightarrow (i)$ is clear.

For $(iii) \Rightarrow (ii)$, suppose $H \leq_o G$ is such that $\exists \phi : H \twoheadrightarrow \mathbb{Z}_p$. We may suppose that $H = G^{p^n}$ for some $n \in \mathbb{N}$. For if $h \in H$ is such that $\mathbb{Z}_p = \overline{\langle \phi(h) \rangle}$, and $n \in \mathbb{N}$ is such that $G^{p^n} \leq H$, then $h^{p^n} \in G^{p^n}$, and $p^n \mathbb{Z}_p = \overline{\langle \phi(h^{p^n}) \rangle} \leq \phi(G^{p^n}) \leq \mathbb{Z}_p$, so $\phi(G^{p^n}) \leq_o \mathbb{Z}_p$, and $\phi(G^{p^n}) \cong \mathbb{Z}_p$.

Now let $N = \ker(\phi)$, so that by Proposition 4.19 (ii), $N \lhd_c H$ is uniform of dimension $d-1$; $\log(H) = p^n \log(G)$ and $\log(H)/\log(N) \cong \mathbb{Z}_p$.

Hence $\mathcal{L}_H = \mathcal{L}_G$ so $\mathcal{L}_G / \mathcal{L}_N \cong \mathbb{Q}_p$, and $\mathcal{L}_G$ is not perfect.

For $(i) \Rightarrow (iii)$, suppose $\mathcal{I} \lhd \mathcal{L}_G$, with $\dim(\mathcal{I}) = d-1$. Let $I = \log(G) \cap \mathcal{I} \lhd \log(G)$ (so that $\mathcal{I} = \mathrm{span}_{\mathbb{Q}_p}(I)$). Let $v \in \log(G)$, and suppose $\exists \lambda \in \mathbb{Z}_p \setminus \{0\}$ such that $\lambda v \in I$. Then $v = \lambda^{-1}(\lambda v) \in \mathcal{I}$, so $v \in \mathcal{I} \cap \log(G) = I$. Thus $\log(G)/I$ is torsion-free, so by Proposition 4.20, $\exp(I) \lhd G$ is uniform and $G/\exp(I)$ is uniform, with:

$$\begin{aligned} \dim(G/\exp(I)) &= \dim(G) - \dim(\exp(I)) \\ &= \mathrm{rk}(\log(G)) - \mathrm{rk}(I) \\ &= \dim(\mathcal{L}_G) - \dim(\mathcal{I}) = 1. \end{aligned}$$

and a 1-dimensional uniform group is by definition infinite procyclic, so $G/\exp(I) \cong \mathbb{Z}_p$. □

Proof of Theorem 1.4. First suppose that G is a FAb compact p-adic analytic group. As noted in Example 4.13, G has an open characteristic uniform subgroup H. By Remark 4.18, H_2 is $\mathbb{Z}_p$-standard. Let $K_n \lhd_o H_2$ be as in Theorem 1.2. Then by Remark 4.18 and Theorem 4.14 (iii),

$$K_n = (H_2)_n = H_{n+1}$$

and H_{n+1} is a characteristic subgroup of H. In particular, $K_n \lhd_o G$. As in the proof of Theorem 1.2, $(K_n)_n$ satisfies the hypotheses of Proposition 2.5 and the result follows.

Now suppose that G is uniform and not FAb. By Proposition 4.21, $\exists \phi : G \twoheadrightarrow \mathbb{Z}_p$. By Proposition 4.19, $N = \ker(\phi)$ is uniform of dimension $d-1$. We may therefore choose a generating set $S = \{a_1, \ldots, a_d\}$ for G such that $\{a_1, \ldots, a_{d-1}\}$ is a generating set for N and $\overline{\langle \phi(a_d) \rangle} = \mathbb{Z}_p$.

Let $\pi_n : \mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$ be the natural projection. Then $G_{n+1} \subseteq \ker(\pi_n \circ \phi)$, so:

$$\operatorname{diam}(G/G_{n+1}, S) \geq \operatorname{diam}(\mathbb{Z}/p^n\mathbb{Z}, \{(\pi_n \circ \phi)(a_d)\}) \geq Cp^n = C|G/G_{n+1}|^{\frac{1}{d}}.$$

In particular $\operatorname{diam}(G/G_{n+1}, S)$ is not polylogarithmic in $|G/G_{n+1}|$. $\square$

4.2 Exceptional Groups over R

With Theorem 1.2 in hand we may complete the proof of Theorem 1.5. We start by marshalling some facts about Chevalley groups. Unless otherwise stated, proofs of assertions left unproven in this section may be found in [8].

Let Φ be a root system of type $X_l \in \{A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4, G_2\}$, $\Pi \subseteq \Phi$ be a fundamental system of roots, and S be a commutative unital ring. We define the *universal Chevalley group of type X_l over S* to be the group $\mathcal{G}_S(X_l)$ abstractly generated by the symbols $\{x_\alpha(t)\}_{\alpha \in \Phi; t \in S}$, subject to the *Steinberg relations*. These are described in detail in [8]; the only fact we require about them is:

(a) If S' is a subring of S, then the inclusion of $\{x_\alpha(t)\}_{\alpha \in \Phi; t \in S'}$ into $\{x_\alpha(t)\}_{\alpha \in \Phi; t \in S}$ induces a homomorphism $\psi : \mathcal{G}_{S'}(X_l) \to \mathcal{G}_S(X_l)$ (in other words, for each Φ, every Steinberg relation over S' is also a Steinberg relation over S).

We define, for each $\alpha \in \Phi, s \in S^*$, the element:

$$c_\alpha(s) = x_\alpha(s)x_{-\alpha}(-s^{-1})x_\alpha(s)(x_\alpha(1)x_{-\alpha}(-1)x_\alpha(1))^{-1}.$$

Trivially,

(b) $c_\alpha(1) = e$.

Theorem 4.22 (Exercise 13.11 in [14])**.** *Let $(R, \mathcal{M})$ be a pro-p domain. For each $n \geq 1$, let $G_n \leq \mathcal{G}_R(X_l)$ be the subgroup generated by the set:*

$$\{x_\alpha(t)\}_{\alpha \in \Phi; t \in \mathcal{M}^n} \cup \{c_\alpha(1+s)\}_{\alpha \in \Phi; s \in \mathcal{M}^n}.$$

Then:

(i) $G_n \lhd_f \mathcal{G}_R(X_l)$, *for all* $n \geq 1$.

(ii) The map $\theta_n : (\mathcal{M}^n)^{(|\Phi|+|\Pi|)} \to G_n$, *given by:*

$$\theta(\underline{t}) = \big(\prod_{\alpha\in\Phi^+} x_\alpha(t_\alpha)\big)\big(\prod_{\alpha\in\Pi} c_\alpha(1+t_\alpha)\big)\big(\prod_{\alpha\in\Phi^-} x_\alpha(t_\alpha)\big)$$

(with the products ordered by the height function induced on Φ *by* Π*) is a bijection, for every* $n \geq 1$. *Identifying* G_1 *with* $\mathcal{M}^{(|\Phi|+|\Pi|)}$ *via* θ_1, G_1 *is an* R*-standard group of dimension* $|\Phi| + |\Pi|$.

(iii) $\mathcal{L}_{G_1}$ *is perfect, unless* $p = 2$ *and* $X_l = A_1$ *or* C_l. *Indeed* $\mathcal{L}_{G_1}$ *is the* $\mathbb{K}$*-Lie algebra of type* X_l.

For K a field, $\mathcal{G}_K(X_l)$ acts on the K-Lie algebra $\mathcal{L}_K(X_l)$ of type X_l by linear automorphisms. For $\{E_\alpha\}_{\alpha\in\Phi} \cup \{H_\beta\}_{\beta\in\Pi}$ a Chevalley basis for $\mathcal{L}_K(X_l)$, the action may be defined by:

(i) $x_\alpha(t)(E_\alpha) = E_\alpha$

(ii) $x_\alpha(t)(E_{-\alpha}) = E_{-\alpha} + tH_\alpha - t^2E_\alpha$

(iii) $x_{\alpha(t)}(H_\alpha) = H_\alpha - 2tE_\alpha$

(iv) $x_{\alpha(t)}(H_\beta) = H_\beta - A_{\beta,\alpha}tE_\alpha$

(v) $x_{\alpha(t)}(E_\beta) = E_\beta + \sum_{i=1}^{q} M_{\alpha,\beta,i}t^iE_{i\alpha+\beta}$

for any $\alpha, \beta \in \Phi$ linearly independent and $t \in K$. Here $A_{\beta,\alpha} = \frac{2(\beta,\alpha)}{(\alpha,\alpha)}$ is the *Cartan integer*; $M_{\alpha,\beta,i}$ are integers and $q \in \mathbb{N}$ is maximal such that $q\alpha + \beta \in \Phi$.

Now take $K = \mathbb{K}$, the field of fractions of R. Let $\rho : \mathcal{G}_{\mathbb{K}}(X_l) \to \mathrm{GL}_d(\mathbb{K})$ be the above-described action (where d $= |\Phi| + |\Pi|$ is the dimension of $\mathcal{L}_K(X_l)$). Let $\psi : \mathcal{G}_R(X_l) \to \mathcal{G}_K(X_l)$ be as described in observation (a). The *adjoint Chevalley group of type* X_l *over* R is defined to be the group $G_{\mathrm{ad}} = \rho(\psi(\mathcal{G}_R(X_l)))$. It is clear from (i)-(v) above that:

(c) $G_{\mathrm{ad}} \leq \mathrm{GL}_d(R)$.

(d) For any $\alpha \in \Phi; s, t \in R$ and $n \geq 1$, if $s \equiv t \bmod \mathcal{M}^n$ then $\rho(x_\alpha(s)) \equiv \rho(x_\alpha(t)) \bmod \mathcal{M}^n$.

(e) In particular, for $t \in \mathcal{M}^n$, $\rho(x_\alpha(t)) \equiv I_d \bmod \mathcal{M}^n$.

From observations (b) and (d), it follows that for any $\beta \in \Phi, s \in \mathcal{M}^n$, $\rho(c_\beta(1+s)) \equiv I_d \bmod \mathcal{M}^n$. Combining with observation (e), we have:

$$\rho(\psi(G_n)) \leq K_n := G_{\mathrm{ad}} \cap (I_d + \mathbb{M}_d(\mathcal{M}^n)). \tag{7}$$

Proof of Theorem 1.5. If $X_l \in \{A_l, B_l, C_l, D_l\}$, G_{ad} is one of $\mathrm{PSL}_d(R)$, $\mathrm{PSO}_d(R)$ or $\mathrm{PSp}_d(R)$. The result then follows as in Section 3. If not, then letting G_1 be as in Theorem 4.22, G_1 satisfies the hypothesis of Theorem 1.2, so that for some $\tilde{C}_1, C_2 > 0$,

$$\mathrm{diam}(\mathcal{G}_R(X_l)/G_n) \leq \tilde{C}_1(\log|\mathcal{G}_R(X_l)/G_n|)^{C_2}.$$

The map $\rho \circ \psi : \mathcal{G}_R(X_l) \twoheadrightarrow G_{\mathrm{ad}}$ descends, by (7), to an epimorphism $\mathcal{G}_R(X_l)/G_n \twoheadrightarrow G_{\mathrm{ad}}/K_n$. By Lemma 3.1 (i),

$$\mathrm{diam}(G_{\mathrm{ad}}/K_n) \leq \mathrm{diam}(\mathcal{G}_R(X_l)/G_n).$$

Finally, $|\mathcal{G}_R(X_l)/G_n| \ll_{R,X_l} |R/\mathcal{M}|^{dn}$ and $|G_{\mathrm{ad}}/K_n| \geq |R/\mathcal{M}|^n$, so $(\log|\mathcal{G}_R(X_l)/G_n|)^{C_2} \ll (\log|G_{\mathrm{ad}}/K_n|)^{C_2}$ and the result follows (replacing $\tilde{C}_1$ by some larger constant C_1).

The bound we thus obtain for C_2 is independent of X_l, since we need only apply Theorem 1.2 for finitely many types X_l. □

Remark 4.23. (i) The method of this section is also applicable to the classical Chevalley groups, though does not yield uniformity in the exponent C_2. In particular we obtain a diameter bound in the case $(X_l, p) = (B_l, 2)$ or $(D_l, 2)$, which does not fall under the purview of Theorem 1.5. The case $(X_l, p) = (A_1, 2)$ or $(C_l, 2)$ is beyond the scope of our methods, however, because the associated Lie algebras are not perfect.

(ii) The best degree C_2 in Theorem 1.5 which we can obtain by the above method is based on taking $A = 248$ in Proposition 2.5, because 248 is the dimension of $\mathcal{G}_R(X_l)$ as an R-analytic group in the case $X_l = E_8$. It is likely that this is far from optimal, and that a much lower degree could be obtained via a more direct analysis of the Lie algebras of the exceptional groups, akin to that employed for the classical groups in Section 3. In the case $R = \mathbb{Z}_p$, this has already largely been achieved by Dinai in [13]: he showed that for $p > 19$, every element of the $\mathbb{Z}_p$-Lie ring associated to an exceptional group can be expressed as the sum of three brackets.

5 The Nottingham Group

We first collect some facts about generation and commutators in $\mathcal{N}_q$ with which to deduce Theorem 1.6 from Proposition 2.5. Details can be found in [7]; [18]; [22]. For $n \geq 2$ and $\lambda \in \mathbb{F}_q$, define:

$$e_{n,\lambda}(t) = t + \lambda t^{n+1} \in K_n.$$

The elements $e_{n,\lambda}$ form an infinite topological generating set for $\mathcal{N}_q$, as follows:

Lemma 5.1. *(i) For any $n \geq 1$ $\lambda, \mu \in \mathbb{F}_q$,*

$$e_{n,\lambda} \cdot e_{n,\mu} \equiv e_{n,\lambda+\mu} \mod K_{2n}$$

(so in particular $e_{n,\lambda}^k \equiv e_{n,k\lambda} \mod K_{2n}$ for all $k \in \mathbb{N}$).

(ii) $\mathcal{N}_q = \{e_{1,\lambda_1} \cdot e_{2,\lambda_2} \cdots : (\lambda_k)_k \in \mathbb{F}_q^{\mathbb{N}}\}$.

The commutator structure of $\mathcal{N}_q$ is well-behaved; in particular we verify hypothesis (i) of Proposition 2.5:

Lemma 5.2. *Let $m, n \in \mathbb{N}$.*

(i) Let $g = t + \sum_{k=n+1}^{\infty} \lambda_k t^k \in K_n \setminus K_{n+1}$, $h = t + \sum_{k=m+1}^{\infty} \mu_k t^k \in K_m \setminus K_{m+1}$, so that $\lambda_{n+1}, \mu_{m+1} \neq 0$. Then:

$$[g, h] \equiv t + \lambda_n \mu_m (n - m) t^{m+n+1} \mod K_{m+n+1}.$$

(ii) For any $\lambda, \mu \in \mathbb{F}_q$,

$$[e_{n,\lambda}, e_{m,\mu}] \equiv e_{m+n,\lambda\mu}^{n-m} \mod K_{\min(m+2n,2m+n)}.$$

(iii) For $p \geq 3$, if $p \nmid (n - m)$ (respectively $p \mid (n - m)$), then $[K_n, K_m] = K_{m+n}$ (respectively $[K_n, K_m] = K_{m+n+1}$).

We shall show that, provided $p \geq 3$, for $n \leq m \leq 2n$ satisfying $p \nmid (m - n)$ every element of K_{m+n} may be expressed, modulo K_{m+2n}, as $[g_1, h_1][g_2, h_2]$ for some $g_i \in K_m$, $h_i \in K_n$. Now, for any $\epsilon \in (0, 1)$, $n \geq 5$ and $i = 1, 2, 3$, there exist $n_i, m_i \in \mathbb{N}$ such that $n_i + m_i = (2 + i)n$; $\frac{n}{3}(2 + i + \epsilon) \leq n_i \leq m_i \leq \frac{2n}{3}(2 + i)$ and $m_i - n_i \in \{1, 2\}$. We therefore satisfy hypothesis (ii) of Proposition 2.5 with ϵ arbitrary; $A = 2$; $M_1 = 5$; $M_2 = 0$.

For any $\lambda_i, \nu \in \mathbb{F}_q$; $K, M, N \in \mathbb{N}$ with $N \leq M$; applying Lemma 5.2 (iii) and an easy induction, we have:

$$[g, e_{M,\nu}] \equiv [e_{N,\lambda_1}, e_{M,\nu}] \cdots [e_{N+K-1,\lambda_K}, e_{M,\nu}] \bmod K_{2N+M+1}$$

where $g = e_{N,\lambda_1} \cdots e_{N+K-1,\lambda_K}$. Moreover, by Lemma 5.1 (i) and Lemma 5.2 (ii),

$$\begin{aligned}[e_{N+i,\lambda_{i+1}}, e_{M,\nu}] &\equiv (e_{M+N+i,\lambda_{i+1}\nu})^{(N-M)+i} \bmod K_{2N+M+2i} K_{N+2M+i} \\ &\equiv e_{M+N+i,\lambda_{i+1}\nu((N-M)+i)} \bmod K_{2M+2N+2i}.\end{aligned}$$

Hence for any $\lambda_i, \mu_i \in \mathbb{F}_q$, setting:

$$\begin{aligned}g_1 &= e_{n,\lambda_1} \cdots e_{2n-1,\lambda_n} \\ g_2 &= e_{n,\mu_1} \cdots e_{2n-2,\mu_{n-1}}\end{aligned}$$

we have:

$$\begin{aligned}[g_1, e_{m,1}][g_2, e_{m+1,1}] &\equiv \Big(\prod_{i=0}^{n-1} e_{n+m+i,\lambda_{i+1}(n+i-m)}\Big)\Big(\prod_{i=1}^{n-1} e_{n+m+i,\mu_i(n-m-2+i)}\Big) \\ &\equiv e_{n+m,\lambda_1(n-m)}\Big(\prod_{i=1}^{n-1} e_{n+m+1,\lambda_{i+1}(n-m+i)+\mu_i(n-m-2+i)}\Big) \bmod K_{2n+m}\end{aligned}$$

since K_{n+m}/K_{2n+m} is abelian. $p \nmid (n-m)$, and since $p \geq 3$, for each $1 \leq i \leq n-1$, p divides at most one of $n-m+i, n-m-2+i$. Hence by varying the λ_i and μ_i, using the form described in Lemma 5.1 (ii), we can express any element of K_{n+m} modulo K_{2n+m}.

6 Limit Theorems for Random Walks

The purpose of this section is to prove Corollaries 1.7, 1.8 and 1.9. Let Γ be a countable group. For $\phi, \psi \in \ell^2(\Gamma)$, with ϕ of finite support, we define the convolution $\phi * \psi \in \ell^2(\Gamma)$ by:

$$(\phi * \psi)(g) = \sum_{h \in \Gamma} \phi(h)\psi(h^{-1}g).$$

For $l \in \mathbb{N}$, we define the *convolution power* ϕ^{*l} of ϕ recursively by:

$$\phi^{*0} = \chi_e;\ \phi^{*(l+1)} = \phi^{*l} * \phi.$$

Let $S \subseteq \Gamma$ be a finite symmetric set. Let $X_1, X_2, \ldots$ be a sequence of independent random variables, each with law:

$$\tfrac{1}{|S|}\chi_S \in \ell^2(\Gamma).$$

For $l \in \mathbb{N}$, the simple random walk $Y_l = X_1 \cdots X_l$ on (Γ, S) at time l has law $\frac{1}{|S|^l}\chi_S^{*l}$. We relate the asymptotics of the distributions of the Y_l to diameters of finite groups via the following method:

For G a finite group, $S \subseteq G$ a symmetric generating set, define a linear operator $A_S : \ell^2(G) \to \ell^2(G)$ (called the *adjacency operator*) by:

$$A_S(f) = (\tfrac{1}{|S|}\chi_S) * f.$$

Let $\ell_0^2(G) \leq \ell^2(G)$ be the space of functions of mean zero on G (that is, the orthogonal complement of the constant functions), and note that $\ell_0^2(G)$ is preserved by A_S. Let ρ be the norm of $A_S \mid_{\ell_0^2(G)}$ in the Banach space $B(\ell_0^2(G))$ of bounded linear operators on $\ell_0^2(G)$. We define the *spectral gap* of the pair (G, S) to be the quantity $1 - \rho$. As we intimated in the introduction, a large spectral gap implies rapid mixing of the random walk on (G, S). Specifically:

Lemma 6.1. *For any $l \in \mathbb{N}$; $g, h \in G$,*

$$|\langle A_S^l \chi_g, \chi_h \rangle - \tfrac{1}{|G|}| \leq \rho^l.$$

Proof. Noting that $\chi_g - \frac{1}{|G|}\chi_G \in \ell_0^2(G)$,

$$\begin{aligned} |\langle A_S^l \chi_g, \chi_h \rangle - \frac{1}{|G|}| &= |\langle A_S^l(\chi_g - \frac{1}{|G|}\chi_G), \chi_h \rangle| \\ &\leq \|A_S^l(\chi_g - \frac{1}{|G|}\chi_G)\|_2 \end{aligned}$$

by the Cauchy-Schwarz inequality. The result follows, since:

$$\|\chi_g - \tfrac{1}{|G|}\chi_G\|_2 \leq 1.$$

□

Finally, ρ is related to $\operatorname{diam}(G, S)$ via the following inequality (see [12] for a proof):

Proposition 6.2. *Suppose $1 \in S$. Then:*

$$\tfrac{\operatorname{diam}(G,S)-1}{\log|G|} \leq \tfrac{1}{1-\rho} \leq |S| \operatorname{diam}(G, S)^2.$$

In particular, for $\mathrm{diam}(G,S) \leq C_1 \log^{C_2}|G|$,

$$1-\rho \geq \tfrac{1}{|S|C_1^2 \log^{2C_2}|G|}$$

so, setting $C_3 = |S|C_1^2$, and applying Lemma 6.1, we have:

$$|\langle A_S^l \chi_g, \chi_h\rangle - \tfrac{1}{|G|}| \leq (1 - \tfrac{1}{C_3 \log^{2C_2}|G|})^l.$$

Recall that $(1-\frac{1}{x})^x$ is an increasing function for $x > 1$, converging to e^{-1} as $x \to \infty$. Hence, setting $l = C_3 \log^{2C_2+C_4}|G|$, for some $C_4 > 0$, we deduce:

$$|\langle A_S^l \chi_g, \chi_h\rangle - \tfrac{1}{|G|}| \leq e^{-\log^{C_4}|G|}.$$

Moreover, the quantity $|\langle A_S^l \chi_g, \chi_h\rangle - \frac{1}{|G|}|$ is non-increasing, so this last inequality holds for any $l \geq C_3 \log^{2C_2+C_4}|G|$.

Proof of Corollary 1.7. We may identify:

$$G/K_{N+1} \cong \{\lambda_1 x_1 + \cdots + \lambda_d x_d : \lambda_1, \ldots, \lambda_d \in R/\mathcal{M}^N\} \cong (R/\mathcal{M}^N)^d,$$

as a set, so $|G/K_{N+1}| = |R/\mathcal{M}|^{dN}$ and:

$$\left|\mathbb{P}\big[\|L_1^{(l)} - \lambda_1\|, \ldots, \|L_d^{(l)} - \lambda_d\| \leq c^{N+1}\big] - \tfrac{1}{|R/\mathcal{M}|^{dN}}\right| = |\langle A_S^l \chi_e, \chi_g\rangle - \tfrac{1}{|G/K_{N+1}|}|$$

where $g = \lambda_1 x_1 + \cdots + \lambda_d x_d \in G/K_{N+1}$. The result is now a consequence of Theorem 1.2 and the discussion following Proposition 6.2, taking:

$$C = 2C_2, C' = C_4, C'' = C_3(d \cdot \log|R/\mathcal{M}|)^{2C_2+C_4}, C''' = (d \cdot \log|R/\mathcal{M}|)^{C_4}.$$

□

Proof of Corollary 1.8. By Theorem 4.14,

$$G/K_{N+1} \cong \langle K_{N+1}a_1\rangle \times \ldots \times \langle K_{N+1}a_d\rangle \cong (\mathbb{Z}/p^N\mathbb{Z})^d,$$

as a set, so $|G/K_{N+1}| = p^{dN}$ and:

$$\left|\mathbb{P}\big[\|M_1^{(l)} - \mu_1\|, \ldots, \|M_d^{(l)} - \mu_d\| \leq p^{-N-1}\big] - \tfrac{1}{p^{dN}}\right| = |\langle A_S^l \chi_e, \chi_g\rangle - \tfrac{1}{|G/K_{N+1}|}|$$

where $g = K_{N+1}a_1^{\mu_1} \cdots a_d^{\mu_d} \in G/K_{N+1}$. The result now follows from Theorem 1.4 and the discussion following Proposition 6.2, taking:

$$C = 2C_2, C' = C_4, C'' = C_3(d \cdot \log(p))^{2C_2+C_4}, C''' = (d \cdot \log(p))^{C_4}.$$

□

Proof of Corollary 1.9. Letting $G_N = \mathcal{N}_q/K_N$, $|G_N| = q^{N-1}$, so:

$$\left|\mathbb{P}\big[A_2^{(l)} = \alpha_2, \ldots, A_N^{(l)} = \alpha_N\big] - \tfrac{1}{q^{N-1}}\right| = |\langle A_S^l \chi_e, \chi_g\rangle - \tfrac{1}{|G_N|}|,$$

where $g = t + \sum_{i=2}^{N} \alpha_i t^i$. The result follows from Theorem 1.6 and the discussion following Proposition 6.2, taking:

$$C = 2C_2, C' = C_4, C'' = C_3(\log(q))^{2C_2+C_4}, C''' = \log(q)^{C_4}.$$

□

References

[1] J. Bourgain and A. Gamburd, Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$. *Annals of Mathematics* **167** (2008), 625-642.

[2] J. Bourgain and A. Gamburd, Expansion and random walks in $SL_d(\mathbb{Z}/p^n\mathbb{Z})$: I. *J. Eur. Math. Soc.* **10**, (2008), Issue 4, 987-1011.

[3] J. Bourgain and A. Gamburd, Expansion and random walks in $SL_d(\mathbb{Z}/p^n\mathbb{Z})$: II. *J. Eur. Math. Soc.* **11** (2009), Issue 5, 1057-1103.

[4] E. Breuillard, B. Green and T. Tao, Approximate subgroups of linear groups. *Geom. Funct. Anal.* **21** (2011), 774-819.

[5] E. Breuillard, B. Green, R. Guralnick and T. Tao, Expansion in finite simple groups of Lie type. *J. Eur. Math. Soc* **17** (2015), 1367-1434.

[6] R. Camina, Subgroups of the Nottingham group. *J. Algebra* **196** (1997), 101-113.

[7] R. Camina, The Nottingham group. In *New horizons in pro-p groups*, Progr. Math. 184, Birkhauser, Boston 2000, 205-221.

[8] R.W. Carter, *Simple groups of Lie type*, Pure and applied mathematics 28, Wiley-Interscience, London 1972.

[9] I.S. Cohen, On the structure and ideal theory of complete local rings. *Trans. Amer. Math. Soc.* **59** (1946), 54-106.

[10] C.M. Dawson and M.A. Nielsen, The Solovay-Kitaev algorithm. *Quant. Info. Comp.* **6** (2006), 81-95.

[11] P. Diaconis, Random walks on groups: characters and geometry. In *Groups St Andrews 2001 in Oxford*, vol. 2, London Math. Soc. Lecture Note Ser. 304-305, Cambridge University Press, Cambridge 2003, 120-142.

[12] P. Diaconis and L. Saloff-Coste, Comparison techniques for random walk on finite groups. *Ann. Probab.* **21** (1993), Issue 4, 2131-2156.

[13] O. Dinai, Diameters of Chevalley groups over local rings. *Archiv der Mathematik* **99** (2012), Issue 5, 417-424.

[14] J.D. Dixon, M.P.F. Du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, 2nd Edition, Cambridge studies in advanced mathematics 61, Cambridge University Press, Cambridge 1999.

[15] I. Fesenko, On just infinite pro-p groups and arithmetically profinite extensions of local fields. *J. Reine Angew. Mathematik* **517** (1999), 61-80.

[16] A. Gamburd and M. Shahshahani, Uniform diameter bounds for some families of Cayley graphs. *Int. Math. Res. Notices* **71** (2004), 3813-3824.

[17] H. A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$. *Annals of Mathematics* **167** (2008), 601-623.

[18] B. Klopsch, Normal subgroups in substitution groups of the formal power series. *J. Algebra* **228** (2000), Issue 1, 91-106.

[19] M. Lazard, Groupes analytiques p-adiques. *Inst. Hautes Etudes Scientifiques, Publ. Math.* **26** (1965), 389-603.

[20] L. Pyber and E. Szabo, Growth in finite simple groups of Lie type. *J. Amer. Math Soc.* **29** (2016), 95-146.

[21] P. P. Varjú, Random walks in compact groups. *Documenta Mathematica* **18** (2013), 1137-1175.

[22] I. York, The group of formal power series under substitution. Ph.D. thesis, Nottingham University, Nottingham 1990.