Arch. Math. 99 (2012), 417–424

0003-889X/12/050417-8
published online November 17, 2012
DOI 10.1007/s00013-012-0451-6

Archiv der Mathematik

Diameters of Chevalley groups over local rings

Oren Dinai

Abstract. Let G be a Chevalley group scheme of rank l. Let $G_n := G(\mathbb{Z}/p^n\mathbb{Z})$ be the family of finite groups for $n \in \mathbb{N}$ and some fixed prime number $p > p_0$. We prove a uniform poly-logarithmic diameter bound of the Cayley graphs of G_n with respect to arbitrary sets of generators. In other words, for any subset S which generates G_n, any element of G_n is a product of Cn^d elements from $S \cup S^{-1}$. Our proof is elementary and effective, in the sense that the constant d and the functions $p_0(l)$ and $C(l,p)$ are calculated explicitly. Moreover, we give an efficient algorithm for computing a short path between any two vertices in any Cayley graph of the groups G_n.

1. Introduction. We start by recalling a few essential definitions and background results. Let G be any group, and let $S \subset G \setminus \{1\}$ be a non-empty subset. Define $Cay(G,S)$, the (left) Cayley graph of G with respect to S, to be the undirected graph with vertex set $V := G$ and edges $E := \{\{g, sg\} : g \in G, s \in S\}$.

Now, given any finite graph $\Gamma = (V,E)$, one defines $\mathrm{diam}(\Gamma)$, the diameter of Γ, to be the minimal $l \geq 0$ such that any two vertices are connected by a path involving at most l edges (with $\mathrm{diam}(\Gamma) = \infty$ if the graph is not connected). Now define the diameter of a group G with respect to $S \subseteq G$ to be $\mathrm{diam}(G,S) := \mathrm{diam}(Cay(G,S))$.

One is naturally interested in minimizing the diameter of a group with respect to an *arbitrary* set of generators. For this we define

$$\mathrm{diam}(G) := \max\{\mathrm{diam}(G,S) : S \subseteq G \text{ and } S \text{ generates } G\}.$$

The diameter of groups, aside from being a fascinating field of research, has a huge amount of applications to other important fields. In addition to Group theory and Combinatorics, the diameter of groups is widely known for its role in Theoretical Computer Science areas such as Communication Networks, Algorithms and Complexity (for a detailed review about these aspects, see [4]). The wide spectrum of applications involved makes this an interdisciplinary field.

It turns out that quite a lot is known about the "best" generators, i.e. that a small number of well-chosen generators can produce a relatively small diameter (see [4]). But very little was known until recently about the worst case. A well known conjecture of Babai (cf. [2,3]) asserts:

Conjecture 1 (*Babai*). There exist two constants $d, C > 0$ such that for any finite non-abelian simple group G we have

$$\mathrm{diam}(G) \leq C \cdot \log^d(|G|).$$

This bound may even be true for $d = 2$, but not for smaller d, as the groups $Alt(n)$ demonstrate.

For these type of groups, there has been enormous progress recently, due in particular to Pyber–Szabó [18] and Breuillard et al. [6], when many families of Cayley graphs of finite groups of Lie type have been shown to be expander families (see also [5,10,13] for previous results). Recently there was also some progress concerning the Alternating groups by Helfgott–Seress [14].

However, although most of the known results are effective, in the sense that the constants can be computed in principle, they are usually not explicit: no specific values are given, the exception being [15] which contains an explicit version of Helfgott's solution of Babai's conjecture for $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. But even this does not give an efficient algorithm for computing a short path between any two vertices in the Cayley graph, whose existence is guaranteed by the diameter bounds.

In Sect. 2 we introduce the required definitions to be used in the next sections. In Sect. 3 we prove Theorem 1.1 which is the main result of this manuscript and gives explicit bounds for the constant d and the functions $p_0 = p_0(l)$ and $C = C(l, p)$ as stated in the abstract. In Sect. 4 we explain the variant of the "Solovay–Kitaev" algorithm that provides fast computations of representations of a given element as a short word, with respect to an arbitrary set of generators.

Theorem 1.1. *Let G be a Chevalley group scheme of rank l and dimension k. Fix a prime number $p > \max\left\{\frac{l+2}{2}, 19\right\}$. Denote $G_n := G(\mathbb{Z}/p^n\mathbb{Z})$ for $n \in \mathbb{N}$. For any $i \geq 2$ set $C_i(p,k) := \mathrm{diam}(G_i)$ and $d_i = d_i(3)$ where $d_i(r) := \frac{\log(4r)}{\log(2i)-\log(i+1)}$. Then for any $n \geq 1$ and $i \geq 2$, we have*

$$\mathrm{diam}(G_n) \leq C_i n^{1+d_i}.$$

Note that $C_i \leq |G_i| \leq p^{ik}$, and d_i is monotone decreasing to $2 + \log_2(3)$.

The following corollary is a special case of Theorem 1.1.

Corollary 1.2. *Let G be a Chevalley group of rank l and dimension k, and let p and G_n be chosen as above. Then for any $n \geq 1$ we have*

$$\mathrm{diam}(G_n) \leq Cp^{2k}n^{10},$$

for some constant C which depends on G but not on p.

This result extends [9] which proves a similar bound for the groups SL_l. The results in [9] improve the work of Gamburd and Shahshahani [12], who prove similar bounds for restricted sets of generators which are projections of subsets in $\mathrm{SL}_2(\mathbb{Z})$ with certain density properties (cf. [12, Theorem 2.1]). Their work was influenced by the Solovay–Kitaev Lemma (cf. [8,16,17]). A recent preprint of Varju [19] uses different methods to get similar polylog diameter bounds in some contexts. For a comparison of the advantages and disadvantages between our results and those of Varju see [19].

Note that, for a fixed family of generating sets, one can often prove that the relevant Cayley graphs form an expander family, which provides asymptotically better bounds, however these bounds are not usually explicit. There is also some interest in poly-logarithmic bounds for the diameter of groups: in [11], there are applications of such bounds to questions in arithmetic geometry, and there is a possibility that explicit bounds as we have obtained could be useful to obtain more quantitative versions of certain of those results.

2. Preliminaries.

First, we begin with a few preliminary definitions.

Definition 2.1. Let A, B be subsets of a group G and $r \in \mathbb{N}$. Denote:

- $A \cdot B = \{ab : a \in A, b \in B\}$.
- $A^{(r)}$ the subset of products of r elements of A with $A^{(0)} = \{1\}$.
- $A^{[r]}$ the subset of products of r elements of $A \cup A^{-1} \cup \{1\}$.

Denote the commutator word $\{a, b\} := (ba)^{-1}ab$, and denote

- $\{A, B\}_1 := \{\{a, b\} : a \in A, b \in B\}$,
- $\{A, B\}_r$ the subset of products of r elements of $\{A, B\}_1$.

The group G will be called r-*strongly perfect* if $G = \{G, G\}_r$. Similarly, if L is a Lie algebra with Lie bracket $[a, b]$, then we replace the previous notations by $[A, B]_r$ and the product by summation, and L will be called r-strongly perfect if $L = [L, L]_r$.

Definition 2.2. Let G be a Chevalley group scheme associated with a connected complex semi-simple Lie group G_c, and let L be its Lie algebra (cf. [1]). Let p be a prime number and $\mathbb{Z}_p$ be the p-adic integers. Set $\Gamma_0 := G(\mathbb{Z}_p)$, $L_0 := L(\mathbb{Z}_p)$, and denote for $n \geq 1$:

- $G_n := G(\mathbb{Z}_p/p^n\mathbb{Z}_p) \cong G(\mathbb{Z}/p^n\mathbb{Z})$.
- π_n the natural projection from Γ_0 onto G_n.
- $\Gamma_n := \Gamma(p^n) = \mathrm{Ker}(\pi_n)$.
- Given $g, h \in \Gamma_0$ denote $g \underset{n}{\equiv} h$ if $\pi_n(g) = \pi_n(h)$.
- $\Delta_n := \Gamma_n/\Gamma_{n+1}$.

Both Γ_0 and L_0 have an operator ultra-metric which is induced by the l_∞-norm and the absolute value on $\mathbb{Z}_p$ (which is defined, say, by $|p| = \frac{1}{2}$ and then extended uniquely to $\mathbb{Z}_p$).

We will use the following proposition due to Weigel [20, Prop. 4.9]. The proof for the classical groups is easy, so we give here an elementary proof of it.

Proposition 2.3 (Weigel). *Let G be a Chevalley group over $\mathbb{Z}_p$ and L_0 and Γ_n be as in Definition 2.2. Then*

$$\Gamma_n = \exp(p^n L_0).$$

Proof. The case $\exp(p^n L_0) \subseteq \Gamma_n$ is trivial, so we will prove the opposite inclusion. We will prove only $\Gamma_1 \subseteq \exp(pL_0)$ since the case $n > 1$ follows by the same argument. Let $g \in \Gamma_1$ be $g = I + pA$ for some p-adic matrix A. Since $\ln(g) = pA - \frac{1}{2}(pA)^2 + \frac{1}{3}(pA)^3 - \dots$ converges, we are left to show that $\overline{\ln}(g) \in L_0$ where $\overline{\ln}(g) := A - \frac{1}{2}pA^2 + \frac{1}{3}p^2A^3 - \dots$ is the "normalized" logarithm.

We can assume that L is a simple Lie algebra since the statement holds for semi-simple Lie algebras if it holds for simple Lie algebras. We will prove this claim when G is a classical Chevalley group, i.e., of type A_l, B_l, C_l, or D_l. In all these cases we will use the classical faithful matrix representations of G and L (over $\overline{\mathbb{Q}}_p$). If G is of type A_l, then $g \in G(\mathbb{Z}_p) \Leftrightarrow \det(g) = 1$ and $A \in L(\mathbb{Z}_p) \Leftrightarrow \mathrm{Tr}(g) = 0$. Since $p\,\mathrm{Tr}(\overline{\ln}(g)) = \mathrm{Tr}(\ln(g)) = \ln(\det(g)) = 0$ we are done[1] in this case.

Now suppose G is a Chevalley group of type B_l, C_l, or D_l. Then we have a vector space V of finite dimension (over $\mathbb{Q}_p$) with some non-singular bilinear form β on V. For $A \in \mathrm{End}(V)$ denote by A^* the β-adjoint[2] of A. Then $g \in G(\mathbb{Z}_p) \Leftrightarrow gg^* = I$ and $A \in L(\mathbb{Z}_p) \Leftrightarrow A + A^* = 0$. Since $\ln(g)$ and $\ln(g^*) = \ln(g)^*$ converge and g, g^* commute, we get that

$$\ln(gg^*) = \ln(g) + \ln(g)^* = p(\overline{\ln}(g) + (\overline{\ln}(g))^*) = \ln(I) = 0,$$

so we are done in these cases as well. $\square$

Definition 2.4. Let $N \leq H \leq G$ be a chain of groups (not necessarily normal) and $S \subseteq G$. Denote:

- $\mathrm{diam}(H/N; S) = \min\{l : H \subseteq S^{[l]}N\}$.
- $\mathrm{diam}_G(H/N) := \max\{\mathrm{diam}(H/N; S) : \langle S \rangle = G\}$.
- $\mathrm{diam}(H/N) := \mathrm{diam}_H(H/N)$.

Note that $\mathrm{diam}(H/N)$ is the worst diameter of the Schreier graphs of H/N, and if $N = 1$, then this is the worst diameter of the Cayley graphs of H.

Simple Fact 2.5. Let $N \leq H \leq G$ be a chain of groups and $S \subseteq G$. Then,

- $\mathrm{diam}(G/N; S) \leq \mathrm{diam}(G/H; S) + \mathrm{diam}(H/N; S)$,
- $\mathrm{diam}(G/N) \leq \mathrm{diam}_G(G/H) + \mathrm{diam}_G(H/N)$.

3. Main results.

Theorem 3.1. *Suppose $L(\mathbb{Z}_p)$ is r-strongly perfect. Then for any $i, j \in \mathbb{N}$,*

$$\Delta_{i+j} = \{\Delta_i, \Delta_j\}_r.$$

Proof. The direction $[\supseteq]$: This is clear since $\{\Gamma_i, \Gamma_j\}_r \subseteq \Gamma_{i+j}$. Moreover, if $g, g' \in \Gamma_0$ and $g \underset{i+1}{\equiv} I + p^i A, g' \underset{j+1}{\equiv} I + p^j A'$ for some matrices A, A', then $\{g, g'\} \underset{i+j+1}{\equiv} I + p^{i+j}[A, A']$.

[1]We used the identity $\det(e^A) = e^{\mathrm{Tr}(A)}$ which is valid over any valuation ring (using the Jordan decomposition of A over an algebraic closed field extending the ring).

[2]So that $A \mapsto A^*$ is an anti-automorphism of $\mathrm{End}(V)$ of order 2 with $\beta(Av, w) \equiv \beta(v, A^*w)$.

The direction [$\subseteq$]: Let $g \in \Gamma_n/\Gamma_{n+1}$ with $n = i + j$. By Lemma 2.3, $g \underset{n+1}{\equiv} \exp(p^n A)$ for some $A \in L_0$. Therefore $g \underset{n+1}{\equiv} I + p^n A$. By the assumption, $A = \sum_{k=1}^{r} [A_k, A'_k]$ for some $A_1, A'_1, \ldots, A_r, A'_r \in L_0$. Denote $g_k := \exp(p^i A_k) \in \Gamma_i$ and $g'_k := \exp(p^j A'_k) \in \Gamma_j$. Therefore $g_k \underset{i+1}{\equiv} I + p^i A_k$ and $g'_k \underset{j+1}{\equiv} I + p^j A_k$ and

$$g \underset{n+1}{\equiv} I + p^n A \underset{n+1}{\equiv} \{g_1, g'_1\} \cdot \ldots \{g_r, g'_r\}.$$

$\square$

Lemma 3.2. *Let G be a Chevalley group of rank l, L its Lie algebra, and let $p \geq \frac{l+2}{2}$ be an odd prime number. If G is a group of exceptional Lie type, then suppose that $p > 19$. Then $L(\mathbb{Z}_p)$ is 3-strongly perfect.*

Proof. Let $B = \{e_s, h_r : s \in \Phi, r \in \Pi\}$ be a Chevalley basis of L, where Φ is the root system associated to L and Π are the simple roots of Φ^+ (for some fixed order). Without loss of generality,[3] we can assume that Φ is irreducible.

For any $r \in \Phi$ denote $L_r := \mathbb{Z}_p e_r$ and $H_r := \mathbb{Z}_p h_r$ where $h_r = [e_r, e_{-r}]$ is the co-root of r. We have $L(\mathbb{Z}_p) = L_\Phi \oplus H$ where $H := \bigoplus_{r \in \Pi} H_r$ and $L_\Phi := \bigoplus_{r \in \Phi} L_r$. We will use the following facts about the Lie bracket of the root system. For any $h \in H$ and $s \in \Phi$ we have $[h, e_s] = (h, s) e_s$ where $(\cdot, \cdot)$ is the inner product in H. For any linearly independent pair of roots (i.e., $r \neq \pm s$) we have $[e_r, e_s] \in L_\Phi$, and if their sum $r + s \notin \Phi$, then $[e_r, e_s] = 0$.

For any $X \subseteq \Phi$ denote $L_X := \bigoplus_{r \in X} L_r$. We will say that X is *covered* if there exists $h \in H$ with $(h, X) \subseteq (\mathbb{Z}_p)^\times$. We will say that Φ is *k-covered* if $\Phi = X_1 \cup \ldots \cup X_k$ and each X_i is covered. Note that if X is covered by some h, then $L_X \subseteq [L(\mathbb{Z}_p), L(\mathbb{Z}_p)]_1$, i.e., every element of L_X is a bracket; indeed if $y = \sum a_r e_r \in L_X$, then $[h, y'] = y$ where $y' = \sum \frac{a_r}{(r,h)} e_r \in L_X$.

Note also that $H \subseteq [L(\mathbb{Z}_p), L(\mathbb{Z}_p)]_1$; indeed for any $x = \sum a_r h_r \in H$ we have $x = [x', x'']$ where $x' = \sum_{r \in \Pi} a_r e_r$ and $x'' = \sum_{r \in \Pi} e_{-r}$. Therefore we see that $L(\mathbb{Z}_p)$ is $(k+1)$-strongly perfect provided Φ is *k-covered*. In order to complete the proof, we will show that Φ is 2-covered.

We will use the following notations. Suppose that Φ can be embedded into an Euclidean space $E \cong H$ of dimension l such that $\{\alpha_i\}$ is an orthonormal basis of E. Set $h_1 := \sum \alpha_i \in H$ and $h_2 := \sum \lambda_i \alpha_i \in H$ where $\lambda_1, \ldots, \lambda_l \in \mathbb{Z} \cap (-p, p)$, and for any $i \neq j$ we have $\lambda_i - \lambda_j \in \mathbb{Z} \backslash p\mathbb{Z}$; e.g., we can take the λ_i's to be a subset of $\left\{0, \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}\right\}$. Later we will put more restrictions on the choice of the λ_i's.

First suppose that Φ is one of the classical root systems. If $\Phi = A_l$, then by [9] it is 2-strongly perfect since Φ is covered (cf. [12]). Now suppose Φ is of type B_l, C_l, or D_l. Set $\Phi = X_1 \cup X_2$ where $X_1 \subseteq \{\pm(\alpha_i - \alpha_j) : i \neq j\}$ and $X_2 \subseteq \{\pm(\alpha_i + \alpha_j), \pm\alpha_i, \pm 2\alpha_i : i \neq j\}$. If $p > 2$, then $(h_1, X_1) \subseteq \{\pm 1, \pm 2\} \subseteq (\mathbb{Z}_p)^\times$. If in addition $2(p-1) \geq l$, then we can find $\lambda_1, \ldots, \lambda_l$ as above such that $\sum \lambda_i = 0$; therefore $(h_2, X_2) \subseteq (\mathbb{Z}_p)^\times$. We got that the classical root systems are 2-covered, and so they are 3-strongly perfect.

[3]Since the statement holds for semi-simple Lie algebras if it holds for simple Lie algebras.

Now we shall see that essentially the same argument works if Φ is an exceptional root system (cf. [7, §8] for a complete list of roots of each type). If Φ is of type G_2 with $l = 2$, then $(h_1, X_1) \subseteq \{\pm 1, \dots, \pm 5\}$; therefore $(h_1, X_1) \subseteq (\mathbb{Z}_p)^\times$ provided $p > 5$; so Φ is 1-covered provided $p \geq 5$.

Now suppose Φ is of type F_4 and $\Phi = \left\{\pm\alpha_i, \pm\alpha_i \pm \alpha_j, \sum_{k=1}^4 \pm\alpha_k : i \neq j\right\}$. Split the set $\Phi = X_1 \cup X_2$ where X_1 is the "unbalanced" subset of sums where the number of $+$'s is not equal to the number of $-$'s and X_2 is the "balanced" subset; i.e., $X_2 := \{\alpha_i - \alpha_j, \alpha_{i_1} + \alpha_{i_2} - \alpha_{i_3} - \alpha_{i_4}\}$. Set $\{\lambda_i\} = \{0, 1, \pm 2\}$. Then $(h_1, X_1) \subseteq \{\pm 1, \pm 2, \pm 4\}$ and $(h_2, X_2) \subseteq \{\pm 1, \pm 2, \pm 4\}$. Therefore Φ is 2-covered provided $p \geq 5$.

Now let us show that E_8 is 3-covered (and therefore also E_6, E_7). Now $l = 8$, and again we split Φ into an unbalanced set X_1 and a balanced set X_2. Set $\{\lambda_i\} = \{0, 1, \pm 2, \pm 3, \pm 4\}$. Then $(h_1, X_1) \subseteq \pm\{2, 4, 8\}$ and $(h_2, X_2) \subseteq \pm\{1, \dots, 19\}$. Therefore we get that Φ is 2-covered provided $p > 19$; so we are done. □

Now we are in position to prove Theorem 1.1.

Proof of Theorem 1.1. Denote $L_n(j) = \mathrm{diam}_{G_n}(\Delta_j)$ for $0 \leq j < n$. Then by Fact 2.5,

$$\mathrm{diam}(G_n) \leq L_n(0) + L_n(1) + \cdots + L_n(n-1).$$

By induction on j, we will prove that for any $i \geq 2$ and $0 \leq j < n$,

$$L_n(j) \leq C_i j^{d_i},$$

and therefore,

$$\mathrm{diam}(G_n) \leq \sum_{j=0}^{n-1} C_i j^{d_i} \leq C_i n^{1+d_i},$$

as we claimed.

Fix some $i \geq 2$. The induction base is for $j < i$, and then trivially $L_n(j) \leq \mathrm{diam}(G_i) = C_i$. Now suppose $j \geq i$. Then by Theorem 3.1, by Lemma 3.2 with $r = 4$, and by the induction assumption, we get

$$L_n(j) \leq 4rL_n\left(\left\lfloor \frac{j+1}{2} \right\rfloor\right) \leq 4rC_i\left(\frac{j+1}{2}\right)^{d_i} = 4r\left(\frac{j+1}{2j}\right)^{d_i} C_i j^{d_i} \leq C_i j^{d_i},$$

since by the definition of d_i, $4r(\frac{j+1}{2j})^{d_i} \leq 1$ for any $j \geq i$. □

Remark 3.3. The combination of Theorem 3.1, Lemma 3.2, and Theorem 1.1 gives a generalization of what is known as the "Solovay–Kitaev method".

Geometrically we divide the group Γ_0 into neighborhoods of the identity Γ_n and their "layers" Δ_n. First, we use the global properties of the Lie brackets in order to get local properties of the commutators in these layers. Then Theorem 1.1 allows us to "glue" the local properties valid in these layers into a global property.

Note that this method can prove, at best, a bound of order of magnitude $\log^d(|G|)$, with d arbitrary close to 2, but not a better bound. This follows because the best possible situation is that L is 1-strongly perfect.

4. The Solovay–Kitaev algorithm. Now we give an explicit description and analysis of the Solovay–Kitaev algorithm (cf. [8, §3] and also [17]). First we describe a procedure based on Theorem 3.1 and Lemma 3.2 from the previous section. This procedure is an effective version of these statements about finding an explicit decomposition of an element as a product of (at most four) commutators.

4.1. Commutator decomposition. The main algorithm (in the next section) will use the subalgorithm $SK'(g,n)$, which gets an input $g \in \Gamma_n$ with $n \geq 2$; then it returns a pair of quadruples $((g_i),(g_i'))$ such that $\{g_1,g_1'\}\cdots\{g_4,g_4'\} \underset{n+1}{\equiv} g$ where $g_i, g_i' \in \Gamma_m$ with $m \geq \frac{n-1}{2}$. Note that this is a direct consequence of Theorem 3.1 and Lemma 3.2; if $g \underset{n+1}{\equiv} \exp(p^n A) \underset{n+1}{\equiv} I + p^n A$ for some $A \in L_0$ and $A = \sum_{k=1}^r [A_k, A_k']$ (with $r = 4$), then by Theorem 3.1 we get the required solution $g \underset{n+1}{\equiv} \{g_1,g_1'\}\cdot\ldots\{g_r,g_r'\}$; in order to solve $A = \sum_{k=1}^r [A_k, A_k']$, we first find the decomposition of A as a linear combination in the Chevalley basis and then use Lemma 3.2 in order to decompose it as a sum of (at most) four Lie brackets.

4.2. The Solovay–Kitaev algorithm. Denote by $SK(g,\overline{s},n)$ the Solovay–Kitaev algorithm; the algorithm gets an element $g \in \Gamma_0, n \in \mathbb{N}$, and a m-tuple $\overline{s}$ with entries in Γ_0 that generates $G_n = \Gamma_0/\Gamma_n$; then it returns a word $w \in F_m$ (in m letters) such that $g \underset{n}{\equiv} w(\overline{s})$. If $n \leq 2$, then SK returns such a word simply by checking all the possible words of length $l(w) \leq |G_2| = |G(\mathbb{Z}/p^2\mathbb{Z})|$. If $n > 2$, set $w_0 = SK(g,\overline{s},n-1)$ and $z = w_0(\overline{s})^{-1}g \in \Gamma_{n-1}$ and let $(\overline{x},\overline{y}) = SK'(z,n-1)$. Set for $k = 1,\ldots 4, w_k := SK(x_k,\overline{s},n-1)$ and $w_k' := SK(y_k,\overline{s},n-1)$ and return $w := w_0 \cdot \{w_1,w_1'\}\cdot\ldots\{w_4,w_4'\}$.

4.3. Analysis of the algorithm. The return length of the output word of the algorithm is $C_i n^{1+d_i}$, the same as was described in Theorem 1.1. Note that $d_2 < 9; C_i \leq p^{ik}$ where $k = \dim(L) = |\Phi| + |\Pi|$; and d_i is monotone decreasing to $2 + \log_2(3)$.

Acknowledgements. I would like to thank Alex Lubotzky for bringing to my attention Thomas Weigel's results and Emmanuel Kowalski for many helpful comments and suggestions.

References

[1] E. Abe, Chevalley groups over local rings, Tohoku Mathematical Journal **21** (1969), 474–494.

[2] L. Babai and Á. Seress, On the diameter of Cayley graphs of the symmetric group, Journal of Combinatorial Theory, Series A **49** (1988), 175–179.

[3] L. Babai and Á. Seress, On the diameter of permutation groups, European journal of combinatorics **13** (1992), 231–243.

[4] L. Babai et al., On the diameter of finite groups, Proceedings of the 31st Annual Symposium on Foundations of Computer Science (1990), 857–865.

[5] J. Bourgain and A. Gamburd, New results on expanders, Comptes Rendus Mathematique **342** (2006), 717–721.

[6] E. Breuillard, B. Green, and T. Tao, Linear approximate groups, Arxiv preprint arXiv:1001.4570 (2010).

[7] R.W. Carter, Lie algebras of finite and affine type, vol. 96, Cambridge Univ Pr, 2005.

[8] C.M. Dawson and M.A. Nielsen, The Solovay-Kitaev algorithm, arXiv preprint quant-ph/0505030 (2005).

[9] O. Dinai, Poly-log diameter bounds for some families of finite groups, Proceedings of the American Mathematical Society **134** (2006), 3137–3142.

[10] O. Dinai, Growth in SL_2 over finite fields, Journal of Group Theory **14** (2011), 273–297.

[11] J. Ellenberg, C. Hall, and E. Kowalski, Expander graphs, gonality and variation of Galois representations, Duke Math. Journal (to appear).

[12] A. Gamburd and M. Shahshahani, Uniform diameter bounds for some families of Cayley graphs, International mathematics research notices no 71 (2004).

[13] H.A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, arXiv preprint math/0509024 (2005).

[14] H.A. Helfgott and A. Seress, On the diameter of permutation groups, arXiv preprint arXiv:1109.3550 (2011).

[15] E. Kowalski, Explicit growth and expansion for SL_2, preprint (2012).

[16] M.A. Nielsen and I. Chuang, Quantum information and computation, Cambridge University Press, 2000.

[17] M.A. Nielsen, I. Chuang, and L.K. Grover, Quantum computation and quantum information, American Journal of Physics **70** (2002), pp. 558.

[18] L. Pyber and E. Szabó, Growth in finite simple groups of Lie type of bounded rank, arXiv preprint arXiv:1005.1858 (2010).

[19] P.P. Varjú, Random walks in compact groups, arXiv preprint arXiv:1209.1745 (2012).

[20] T. Weigel, On the rigidity of Lie lattices and just infinite powerful groups, Journal of the London Mathematical Society **62** (2000), 381–397

Oren Dinai
Department of Mathematics,
ETH Zurich Ramistrasse 101,
8092 Zurich,
Switzerland
e-mail: `oren.dinai@math.ethz.ch`;
`oren.dinai@gmail.com`

Received: 13 March 2012