PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 134, Number 11, November 2006, Pages 3137–3142
S 0002-9939(06)08384-5
Article electronically published on June 8, 2006

POLY-LOG DIAMETER BOUNDS FOR SOME FAMILIES OF FINITE GROUPS

OREN DINAI

(Communicated by Jonathan I. Hall)

ABSTRACT. Fix a prime p and an integer m with $p > m \geq 2$. Define the family of finite groups

$$G_n := SL_m(\mathbb{Z}/p^n\mathbb{Z})$$

for $n = 1, 2, \ldots$. We will prove that there exist two positive constants C and d such that for any n and any generating set $S \subseteq G_n$,

$$diam(G_n, S) \leq C \cdot \log^d(|G_n|)$$

when $diam(G, S)$ is the diameter of the finite group G with respect to the set of generators S. It is defined as the maximum over $g \in G$ of the length of the shortest word in $S \cup S^{-1}$ representing g.

This result shows that these families of finite groups have a poly-logarithmic bound on the diameter with respect to *any* set of generators. The proof of this result also provides an efficient algorithm for finding such a poly-logarithmic representation of any element.

1. INTRODUCTION

The diameter of a finite group G with respect to a set of generators S is defined to be the diameter of the corresponding Cayley graph, i.e., the minimal number k for which any element in G can be written as a product of at most k elements in $S \cup S^{-1}$. We denote this number $diam(G, S)$. We will be interested in minimizing the diameter of a group with respect to *any* set of generators. For this we define

$$diam_{worst}(G) := \max_{S \subset G} \{diam(G, S) : \ S \text{ generates } G\}.$$

While quite a lot is known about the "best" generators, i.e. a small number of generators which produce a relatively small diameter (see [BHKLS]), very little is known about the worst case.

A well-known conjecture of Babai (see [BS1]) asserts:

Conjecture 1.1 (Babai)**.** *There exist constants d, C such that for any finite non-abelian simple group G,*

$$diam_{worst}(G) \leq C \cdot \log^d(|G|).$$

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

Received by the editors October 26, 2004 and, in revised form, June 8, 2005.
2000 *Mathematics Subject Classification.* Primary 05C25; Secondary 05C12.

But as of now, there is no family of finite simple groups for which the Babai's conjecture holds (see [BS1, BS2] for the best known results).

The goal of this paper is to present for the first time, as far as we know, a family of finite groups with a poly-logarithmic bound for the worst-diameter, and to also give an algorithm for calculating such a poly-logarithmic representation. Our groups are not simple, though.

Theorem 1.2. *Fix a prime p such that $p > m \geq 2$ and define $G_n := SL_m(\mathbb{Z}/p^n\mathbb{Z})$. Then for every real number $d > 4$ the following holds:*

$$diam_{worst}(G_n) = O\left(\log^d(|G_n|)\right).$$

Furthermore we will show that if $m > 2$, p can be chosen equal to m and if $m = 2$, d can be arbitrarily close to 3.

Our method of proof is a slight improvement of the work of Gamburd and Shahshahani [GS]. Their work was influenced by the Solovay-Kitaev Lemma (see [NC]).

2. Preliminaries

We first restrict ourselves to the case of $m = 2$, and then consider the required modifications for proving the more general case. From now on we assume that p is an odd prime and S is a generating set for $G_n := SL_m(\mathbb{Z}/p^n\mathbb{Z})$. Both are *arbitrary* but *fixed*. From now $\log x$ stands for $\log_2 x$ and $\mathbb{Z}_p$ stands for the p-adic integers. First we begin with some definitions:

Definition 2.1. For any integer $n \geq 0$, define

$$\Gamma_n := \left\{\gamma \in SL_2(\mathbb{Z}) :\ \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\text{mod } p^n)\right\}.$$

Equivalently, $\Gamma_n = \ker(SL_2(\mathbb{Z}) \xrightarrow{\pi_n} SL_2(\mathbb{Z}/p^n\mathbb{Z}))$, where π_n is the natural projection. Note that with the above definitions we get that $\Gamma_0 = SL_2(\mathbb{Z})$ and $\Gamma_{n+1} \subset \Gamma_n$ for any n. Since π_n is *onto* we have

$$G_n \cong \Gamma_0/\Gamma_n.$$

By abuse of notation, instead of doing calculations in G_n we will do them in Γ_0 mod Γ_n, so we will treat the elements in G_n as being in Γ_0.

Definition 2.2. For two subsets $X \subset Y \subset SL_2(\mathbb{Z})$ denote $X \equiv Y \left(\text{mod } p^k\right)$ if $\pi_k(X) = \pi_k(Y)$. Also denote

$$Y \overset{l}{\rightsquigarrow} X \tag{2.1}$$

if every element in Y can be moved into X by a multiplication of at most of l elements in $S \cup S^{-1}$. Explicitly, $\forall y \in Y$, $\exists s_1, s_2, \ldots, s_k \in S \cup S^{-1}$, for some $k \leq l$, such that $y \cdot s_1 \cdot s_2 \cdot \ldots \cdot s_k \in X$.

We need to distinguish between the group commutator and the Lie bracket operations. For elements g, h in a group G we denote $\{g, h\} := g^{-1}h^{-1}gh$ for the group commutator. For elements A, B in the Lie algebra $\mathfrak{sl}_m(R)$ for some commutative ring R, we write $[A, B] := AB - BA$ for the Lie bracket, when $\mathfrak{sl}_m(R)$ is the set of matrices in $M_m(R)$ with Trace $= 0$.

3. Statement of the main results

The first lemma, Lemma 3.1, concerns some generation properties in the Lie algebras $\mathfrak{sl}_m(R)$. The next three statements, Lemma 3.2, Proposition 3.3 and Theorem 3.4, are restricted to the case $m = 2$ while Theorem 3.5 is a generalization of these statements to $m \geq 2$. Lemma 3.2 is due to Michael Larsen. We will see later that this lemma already has almost all the key ideas for proving Theorem 1.2. This lemma will give us a reduction from the groups $SL_m(\mathbb{Z}_p)$ to the algebras $\mathfrak{sl}_m(\mathbb{Z}_p)$.

The following lemma is the main ingredient for Theorem 3.5 which is a generalization of Theorem 3.4.

Lemma 3.1. *For any prime p and integer m with $p > m \geq 2$, any element in $\mathfrak{sl}_m(\mathbb{Z}_p)$ is a sum of two Lie brackets. This is also true for $p \geq m > 2$. Furthermore, in the case $p > m = 2$, any element in $\mathfrak{sl}_2(\mathbb{Z}_p)$ can be expressed as one Lie bracket.*

The following Lemma 3.2 and Proposition 3.3 are restricted to the case $m = 2$. Remember that we have defined $\Gamma_n = \{\gamma \in SL_2(\mathbb{Z}) : \ \gamma \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) (\mathrm{mod}\ p^n)\}$.

Lemma 3.2. *For any integers $i, j \geq 0$ and for any $k \leq \min\{i, j\}$ the group commutator map*

$$\begin{array}{rccc} \Gamma_i/\Gamma_{i+k} \times \Gamma_j/\Gamma_{j+k} & \xrightarrow{\{\cdot,\cdot\}} & \Gamma_{i+j}/\Gamma_{i+j+k}, \\ (\overline{\alpha}, \overline{\beta}) & \mapsto & \overline{\{\alpha, \beta\}} \end{array} \tag{3.1}$$

is surjective.

Lemma 3.2 will imply the following iteration step needed for Theorem 3.4.

Proposition 3.3. *For any $d > 2$ there exists C such that for any $n \geq 1$*

$$\Gamma_n \overset{Cn^d}{\rightsquigarrow} \Gamma_{n+1}.$$

With this proposition we will prove Theorem 3.4, which is equivalent to Theorem 1.2 for the case $m = 2$.

Theorem 3.4. *Fix $p > 2$ and set $G_n := SL_2(\mathbb{Z}/p^n\mathbb{Z})$. Then for any $d > 3$ there exists a real constant C such that for any set of generators $S \subseteq G_n$, any element in G_n can be written as a product of at most Cn^d elements in $S \cup S^{-1}$.*

The next theorem is equivalent to Theorem 1.2 for the case $m > 2$ (see Remark 4.1).

Theorem 3.5. *Fix a prime p and an integer m with $p \geq m > 2$. Define the family of finite groups $G_n := SL_m(\mathbb{Z}/p^n\mathbb{Z})$ for $n = 1, 2, \ldots$. For any real d with $d > 4$ there exists a real constant C such that for any set of generators $S \subseteq G_n$, any element in G_n can be written as a product of at most Cn^d elements in $S \cup S^{-1}$.*

4. Proofs

Proof of Lemma 3.1. Let us denote $diag(\lambda_1, \ldots, \lambda_m)$ to be the diagonal matrix with these values on its diagonal. For a matrix $A \in \mathfrak{sl}_m(\mathbb{Z}_p)$ denote by $diagA$ the diagonal matrix with the same diagonal of A. Now choose $D = diag(\lambda_1, \ldots, \lambda_m)$ such that $\sum_{i=1}^m \lambda_i = 0$ and $(\lambda_i - \lambda_j)$ is a unit in $\mathbb{Z}_p$ for any $i \neq j$. Take for example $\{\lambda_i\}$ to be $\pm 1, \ldots, \pm k$ if $m = 2k$ or $0, \pm 1, \ldots, \pm k$ if $m = 2k + 1$. Since for any

$i \neq j$, $[D, E_{i,j}] = (\lambda_i - \lambda_j)E_{i,j}$ all we need to show is that given $A \in \mathfrak{sl}_m(\mathbb{Z}_p)$ we can find two matrices B', B'' s.t. $diag[B', B''] = diagA$. For if we write $A - [B', B''] = \sum_{i \neq j} a_{i,j}E_{i,j}$ we get $A = [B', B''] + \sum_{i \neq j} a_{i,j}E_{i,j} = [B', B''] + [D, \sum_{i \neq j} \frac{a_{i,j}}{(\lambda_i - \lambda_j)}E_{i,j}]$.

Let us denote by B^g the representation of the matrix B in the basis $e_1, e_1 + e_2, e_1 + e_2 + e_3, \ldots, e_1 + \ldots + e_m$, where $\{e_1, \ldots, e_m\}$ is the standard basis. For any $i < m$ we get $diag[D^g, E^g_{i,i+1}] = diag[D, E_{i,i+1}]^g = diag(\lambda_i - \lambda_{i+1})E^g_{i,i+1} = (\lambda_i - \lambda_{i+1})(E_{i+1,i+1} - E_{i,i})$. So if we write $diagA = \sum_{i=1}^{m-1} a_i(E_{i+1,i+1} - E_{i,i})$ we get that $diagA = \sum_{i=1}^{m-1} a_i(E_{i+1,i+1} - E_{i,i}) = diag[D^g, \sum_{i=1}^{m-1} \frac{a_i}{(\lambda_i - \lambda_{i+1})}E^g_{i,i+1}]$, so we are done. Note that when $m > 2$, p is odd we can take m to be equal $p = 2k+1$ and follow the same arguments.

The following improvement to the case $\mathfrak{sl}_2(\mathbb{Z}_p)$ is due to Larsen. In $\mathfrak{sl}_2(\mathbb{Z}_p)$ we have the following identity: for every $C,\ D \in \mathfrak{sl}_2(\mathbb{Z}_p)$:

$$[[C,\, D]\,,\, C] = 2Tr\,(CD)\,C - 2Tr\left(C^2\right)D \tag{4.1}$$

(this identity can be checked by expressing the matrices C and D explicitly via their entries). From identity (4.1) we get the following identity for every $A,\ B \in \mathfrak{sl}_2(\mathbb{Z}_p)$:

$$[[[A,\, B]\,,\, A]\,,\, [A,\, B]] = -2Tr\left([A,\, B]^2\right)A \tag{4.2}$$

by setting $C = [A, B]\,,\ D = A$ and observing that the first term of the right-hand side of (4.1) vanished since $Tr\,(CD) = Tr\,([A, B]\,A) = Tr\,([A, BA]) = 0$.

First we want to use identity (4.2) to show that any element in $\mathfrak{sl}_2(\mathbb{Z}_p) \setminus p \cdot \mathfrak{sl}_2(\mathbb{Z}_p)$ is a bracket. If $A = \left(\begin{smallmatrix} u & v \\ w & -u \end{smallmatrix}\right)$ is not in $p \cdot \mathfrak{sl}_2(\mathbb{Z}_p)$ it has at least one entry which is a unit in $\mathbb{Z}_p$. By a straightforward calculation we get that for $B = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Tr([A, B]^2)$ equals $2w^2, 2v^2$ or $-8u^2$ respectively. Therefore $-2\beta Tr([A, B]^2)$ equals 1 for some $B \in \mathfrak{sl}_2(\mathbb{Z}_p)$ and some $\beta \in \mathbb{Z}_p$. Note that here we used the fact that p is odd and so 2 is unit in $\mathbb{Z}_p$. So we can find $A_1, A_2 \in \mathfrak{sl}_2(\mathbb{Z}_p)$ when $A_1 = \beta\,[[A,\, B]\,,\, A]\,,\ A_2 = [A,\, B]$ s.t. $[A_1, A_2] = [\beta\,[[A,\, B]\,,\, A]\,,\, [A,\, B]] = A$ as we wanted.

Now we show that any element A in $\mathfrak{sl}_2(\mathbb{Z}_p)$ can be expressed as one Lie bracket. For $A = 0$ the statement is clear so take $A \neq 0$ in $\mathfrak{sl}_2(\mathbb{Z}_p)$; then there exists k such that $A' = p^{-k}A$ and $A' \in \mathfrak{sl}_2(\mathbb{Z}_p) \setminus p \cdot \mathfrak{sl}_2(\mathbb{Z}_p)$. By the previous paragraph there exist B', B'' with $A' = [B', B'']$ and so $A = [p^k B', B'']$, and we are done. □

Proof of Lemma 3.2. First we observe that the commutator map (3.1) is well defined since for any $\alpha \in \Gamma_i\,,\ \beta \in \Gamma_j\,,\ \ \alpha' \in \Gamma_{i+k}\,,\ \beta' \in \Gamma_{j+k}$ there exists 4 matrices $A, B, A', B' \in SL_2(\mathbb{Z})$ s.t. $\alpha = I + p^i A\,,\ \alpha' = I + p^{i+k}A'\,,\ \beta = I + p^j B\,,\ \beta' = I + p^{j+k}B'$, and so we get

$$\{\alpha, \beta\} \equiv \{\alpha\alpha', \beta\beta'\} \equiv I + p^{i+j}\,[A, B] \left(\mathrm{mod}\ p^{i+j+k}\right).$$

Secondly we observe that we can work p-adicly, which means that we can do all the calculations over $\mathbb{Z}_p$-the ring of p-adic integers instead over $\mathbb{Z}$. Indeed if we denote $\overline{\Gamma_m} := \ker\left(SL_2(\mathbb{Z}_p) \xrightarrow{\overline{\pi_m}} SL_2(\mathbb{Z}_p/p^m\mathbb{Z}_p)\right)$, then we get for any $m, k \geq 0$

$$\Gamma_m/\Gamma_{m+k} \cong \overline{\Gamma_m}/\overline{\Gamma_{m+k}}.$$

Instead of doing the group commutator we want to reduce our problem to Lie algebras and their bracket product, which is easier to handle. We have the following

bijections for any $m \geq 1$:

$$\overline{\Gamma_m} \overset{\log(1+x)}{\longrightarrow} p^m \mathfrak{sl}_2(\mathbb{Z}_p), \tag{4.3}$$

$$I + p^m A \mapsto \log(I + p^m A) = p^m A - \frac{p^{2m}}{2} A^2 + \frac{p^{3m}}{3} A^3 - \ldots, \tag{4.4}$$

i.e. $\log(1+x) := \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}$. If we denote by $\overline{L} := \mathfrak{sl}_2(\mathbb{Z}_p)$ the Lie algebra over $\mathbb{Z}_p$, then we get the following commutative diagram:

$$\begin{array}{ccc} \left(\overline{\Gamma_i}/\overline{\Gamma_{i+k}}\right) \times \left(\overline{\Gamma_j}/\overline{\Gamma_{j+k}}\right) & \overset{\{\cdot,\cdot\}}{\longrightarrow} & \overline{\Gamma_{i+j}}/\overline{\Gamma_{i+j+k}} \\ \varphi_1 \downarrow & & \downarrow \varphi_2 \\ \left(p^i\overline{L}/p^{i+k}\overline{L}\right) \times \left(p^j\overline{L}/p^{j+k}\overline{L}\right) & \overset{[\cdot,\cdot]}{\longrightarrow} & p^{i+j}\overline{L}/p^{i+j+k}\overline{L} \end{array} \tag{4.5}$$

When φ_1, φ_2 are the bijections, $\varphi_1(x_1, x_2) := \log(1+x_1) \times \log(1+x_2)$ and $\varphi_2(x) := \log(1+x)$ as in (4.3). Note that the summation in (4.4) indeed converge since we are over $\mathbb{Z}_p$ and its general element converge to zero (for more details see [Di]).

In order to show that the commutator map $\{\cdot,\cdot\}$ in (4.5) is onto, it is enough to show that the bracket map $[\cdot,\cdot]$ in (4.5) is onto. So it suffices to show that for every $k \geq 1$, every element in the Lie algebra $\overline{L}/p^k\overline{L} = \mathfrak{sl}_2(\mathbb{Z}_p)/p^k\mathfrak{sl}_2(\mathbb{Z}_p)$ is a bracket of two elements in $\mathfrak{sl}_2(\mathbb{Z}_p)/p^k\mathfrak{sl}_2(\mathbb{Z}_p)$. By Lemma 3.1 we are done. □

Proof of Proposition 3.3. We need to prove that any element in Γ_n/Γ_{n+1} can be written as a product in at most Cn^d elements in $S \cup S^{-1}$. Let us denote the minimal length of $\gamma \in \Gamma_n/\Gamma_{n+1}$ by $l(\gamma)$. We prove that $l(\gamma) \leq Cn^d$ by induction on n. For any $d > 2$ we can choose N_0 s.t. for any $n > N_0$, $4\left(\frac{n+1}{2n}\right)^d < 1$. Choose a constant C big enough s.t. $l(\gamma) \leq Cn^d$ for any $\gamma \in \Gamma_n/\Gamma_{n+1}$ and any $n \leq N_0$. Now let $n > N_0$ and let $\gamma \in \Gamma_n/\Gamma_{n+1}$. There are always $k, m \leq \frac{n+1}{2}$ with $k+m = n$. Hence by Lemma 3.2 there exists $\gamma_1 \in \Gamma_m/\Gamma_{m+1}$ and $\gamma_2 \in \Gamma_k/\Gamma_{k+1}$ with $\gamma = \{\gamma_1, \gamma_2\}$ and so $l(\gamma) \leq 2(l(\gamma_1) + l(\gamma_2))$, and by the induction hypothesis we get

$$l(\gamma) \leq 2(Ck^d + Cm^d) \leq 4C\left(\frac{n+1}{2}\right)^d = 4\left(\frac{n+1}{2n}\right)^d Cn^d < Cn^d,$$

as claimed. □

Now it remains to combine the proceeding and get Theorem 3.4, but before that we remark on the equivalence of Theorems 1.2, 3.4 and 3.5.

Remark 4.1. For the equivalence between Theorems 1.2, 3.4 and 3.5 we note that $|G_n| = |SL_m(\mathbb{Z}/p^n\mathbb{Z})| = p^{\theta(nm^2)}$. Therefore, $\log|G_n| \sim \log(p) m^2 n$, and so the equivalence is clear.

Proof of Theorem 3.4. By applying $(n-1)$ times Proposition 3.3 and then combining those steps together, we get that for any $d > 2$ there exists C such that

$$\Gamma_1 \overset{C(1^d + 2^d + \ldots + (n-1)^d)}{\rightsquigarrow} \Gamma_n.$$

If we choose l_0 such that $\Gamma_0 \overset{l_0}{\rightsquigarrow} \Gamma_1$ and we can assume that $l_0 \leq C$, then we get $\Gamma_0 \overset{Cn^{d+1}}{\rightsquigarrow} \Gamma_n$. Therefore we achieved the result we wanted: for any $d > 3$ there exist C such that

$$diam(SL_2(\mathbb{Z}/p^n\mathbb{Z}), S) \leq Cn^d.$$

□

Proof of Theorem 3.5. Now we make the required modification to the definitions and statements of Definitions 2.1, 2.2, Lemma 3.2 and Proposition 3.3. Let us replace in these definitions all the occurrences of $SL_2(), \mathfrak{sl}_2()$ by $SL_m(), \mathfrak{sl}_m()$, respectively.

Let us modify Lemma 3.2 to the following: every element in $\Gamma_{i+j}/\Gamma_{i+j+k}$ can be expressed as a product of two commutators $\{\alpha,\beta\}\{\alpha',\beta'\}$ when $\alpha,\alpha' \in \Gamma_i/\Gamma_{i+k}$ and $\beta,\beta' \in \Gamma_j/\Gamma_{j+k}$. The proof of this follows the same lines of the proof of Lemma 3.2, but instead of representing every element in $\mathfrak{sl}_2$ by one Lie bracket, we use the previous Lemma 3.1 regarding representing each element by a sum of two Lie brackets, and so we get the required representation as a product of two commutators.

Now let us modify Proposition 3.3 to the same claim for any $d > 3$. In its proof we see that if we use the previous lemma about expressions as a product of b commutators (we proved it for $b = 2$), then we get $l(\gamma) \leq 2b\left(l(\gamma_1) + l(\gamma_2)\right)$ and so

$$l(\gamma) \leq 2b(Ck^d + Cm^d) \leq 4bC(\frac{n+1}{2})^d = 4b(\frac{n+1}{2n})^d Cn^d < Cn^d$$

when the last inequality is true if $d > \log(4b) = 2 + \log(b)$ and n is big enough. Now for $b = 2$ we get the result we wanted for any $d > 3$.

In conclusion if we combine all the previous modifications we can use them in the proof of Theorem 3.4 to get the generalization we wanted: for any $d > 4$ there exist C such that

$$diam(SL_m\left(\mathbb{Z}/p^n\mathbb{Z}\right), S) \leq Cn^d$$

for *any* generating set S of $SL_m(\mathbb{Z}/p^n\mathbb{Z})$. □

Acknowledgement

This work is part of the author's M.sc thesis. I wish to thank my advisor Professor Alex Lubotzky for sharing his ideas, and for his guidance and assistance in writing this work. I also wish to thank Professor Michael Larsen for Lemma 3.2 and to the referee for his careful report and for many of his suggestions and observations.

References

[BKL] Babai, L., Kantor, W.M., Lubotzky, A.: Small diameter Cayley graphs for finite simple groups, Europ. J. Combinatorics, 10, (1989), 507-522. MR1022771 (91a:20038)

[BHKLS] Babai, L., Hetyei, G., Kantor, W. M., Lubotzky, A., Seress, A.: On the diameter of finite groups. In 31st Annual Symposium on Foundations of Computer Science, volume II, pages 857-865, St. Louis, Missouri, 22-24 October 1990. IEEE. MR1150735

[BS1] Babai, L., Seress, A.: On the diameter of Cayley graphs of the symmetric group, J. Combinatorial Theory-A 49, (1988), 175-179. MR0957215 (89i:05141)

[BS2] Babai, L., Seress, A.: On the diameter of permutation groups, Europ. J. Comb. 13, (1992), 231-243. MR1179520 (93h:20001)

[Di] Dinai, O.: Poly-log diameter bounds for some families of finite groups, Master's thesis, Hebrew University (2004).

[GS] Gamburd, A., Shahshahani, M.: Uniform diameter bounds for some families of Cayley graphs, Internat. Math. Res. Notices, 71, (2004), 3813-3824. MR2104475

[NC] Nielsen, M.A., Chuang, I.L., Quantum computation and quantum information, Cambridge University Press, Cambridge (2000). MR1796805 (2003j:81038)

Einstein Institute of Mathematics, Edmond Safra Campus, Givat Ram, 91904 Jerusalem, Israel