ISRAEL JOURNAL OF MATHEMATICS **158** (2007), 193–203
DOI: 10.1007/s11856-007-0009-7

FINITE GROUPS OF UNIFORM LOGARITHMIC DIAMETER

BY

Miklós Abért*

Department of Mathematics, University of Chicago
5734 S University Avenue, Chicago IL 60637, USA
e-mail: abert@math.uchicago.edu

AND

László Babai

Department of Computer Science, University of Chicago
1100 E 58th St, Chicago IL 60637-1504, USA
e-mail: laci@cs.uchicago.edu

ABSTRACT

We demonstrate the existence of an infinite family of finite groups with 2 generators and logarithmic diameter with respect to any set of generators. This answers a question of A. Lubotzky. Moreover, in our groups, all minimal sets of generators have at most 3 elements.

1. Introduction

Let G be a finite group and X a set of generators. Let $\mathrm{Cay}(G,X)$ denote the undirected Cayley graph of G with respect to X, defined by having vertex set G and $g \in G$ being adjacent to $gx^{\pm 1}$ for $x \in X$.

We define $\mathrm{diam}(G,X)$ to be the diameter of $\mathrm{Cay}(G,X)$, that is, the smallest k such that every element of G can be expressed as a word of length at most k in X (inversions permitted). The diameter of a Cayley graph is related to its isoperimetric properties (cf. [1, 3, 8]). It is easy to see that

$$\mathrm{diam}(G,X) \geq \frac{\log(|G|-1)}{\log(2|X|)}. \tag{1}$$

A generating set X is **minimal** if no proper subset of X generates G.

* Research partially supported by NSF Grant DMS 0401006
Received May 20, 2005 and in revised form November 11, 2005

Definition 1: Let $\mathcal{G}$ be a family of finite groups. We say that $\mathcal{G}$ has **uniform logarithmic diameter** if there exists a constant C such that for all $G \in \mathcal{G}$ and all minimal generating sets X of G we have

$$\operatorname{diam}(G, X) \leq C \frac{\log |G|}{\log |X|}. \tag{2}$$

In other words, for such a family, the trivial bound (1) is tight within a constant factor for all minimal generating sets.

Our main result is the following.

THEOREM 2: *There exists an infinite family of finite groups of uniform logarithmic diameter.*

For a finite group G, let $\operatorname{diam}_{\max}(G)$ denote its **worst diamater**,

$$\operatorname{diam}_{\max}(G) := \max_{\langle X \rangle = G} \operatorname{diam}(G, X). \tag{3}$$

Alex Lubotzky [9] asked whether there exists an infinite family of finite groups G_n and a constant C such that the G_n have a bounded number of generators and the worst diameter is logarithmic:

$$\operatorname{diam}_{\max}(G) \leq C \log |G_n|. \tag{4}$$

Note that one cannot omit the requirement that G_n has a bounded number of generators, because otherwise C_2^n becomes a trivial family of examples. Definition 1 seems to be a more natural way of avoiding trivial examples.

Lubotzky's question has been addressed by Oren Dinai [4], who proved that the family $G_n = SL_2(\mathbb{Z}/p^n\mathbb{Z})$ (where p is a fixed prime) has worst diameter which is polylogarithmic in the size of G_n. His result relies on the work of Gamburd and Shahshahani [5], who proved the corresponding result in the case when the generating set projects onto G_1. Another very recent, deep result due to Helfgott [7] asserts that the family $SL_2(\mathbb{Z}/p\mathbb{Z})$ has polylogarithmic worst diameter (over all primes p).

Our proof of Theorem 2 constructs a family of groups with 2 generators and therefore a positive answer to Lubotzky's question follows. Theorem 2 will follow from the following result. Let r, p be distinct odd primes and let $W(r, p)$ denote the wreath product $W(r, p) = C_r \wr C_p$.

THEOREM 3: *We have*

$$\operatorname{diam}_{\max} W(r, p) \leq \frac{3}{2}(4r - 1)(p - 1) + 1. \tag{5}$$

Using our methods, one can also give a general (weaker) bound on the worst diameter of a wreath product of a cyclic group of prime order by an arbitrary finite group.

THEOREM 4: *Let H be a nontrivial finite group, let r be a prime and let $G = C_r \wr H$. Then*

$$\mathrm{diam}_{\max}(G) < (2r-1)|H|^2 < (2r-1)\log^2|G|.$$

It is natural to ask whether the $O(|H|^2)$ bound can be improved.

QUESTION 5: *Do there exist constants C and $\epsilon > 0$ depending only on r such that*

$$\mathrm{diam}_{\max} C_r \wr H < C|H|^{2-\epsilon}? \tag{6}$$

The real question is to find the right invariant of H to replace $|H|^2$ in Theorem 4.

The most intriguing question suggested by Theorem 2 is whether one can omit the minimality restriction.

QUESTION 6: *Does there exist an infinite family of finite groups G_n and $C > 0$ such that for all generating sets X of G_n we have*

$$\mathrm{diam}(G, X) < C\frac{\log|G|}{\log|X|}?$$

Helfgott [7] proves that for every generating set of $SL_2(\mathbb{Z}/p\mathbb{Z})$ of size at least p^δ ($\delta > 0$), the diameter is bounded above by a function of δ. Although even a uniform logarithmic diameter is far from being known for an infinite family of almost simple groups, this result suggests that $SL_2(\mathbb{Z}/p\mathbb{Z})$ is a possible candidate answer to Question 6.

ACKNOWLEDGEMENT: Theorem 4 was not part of our initial submission; we are grateful to the anonymous referee for pointing out that this result follows from our methods. We also thank the referee for the thorough reading of our paper which helped improve the presentation.

2. Proofs

Let us describe some basic properties of our groups. Let $F = \mathbb{F}_r$ denote the field of r elements. For a finite group G let FG denote the group algebra of G over F.

The wreath product $W = W(r,p)$ is the semidirect product of the F-vector-space $U \lhd W$ of dimension p and the cyclic group $C = C_p < W$ of order p. The structure of the C-module U is governed by the irreducible factors of the polynomial $x^p - 1$ over F. It turns out that U decomposes as

$$U = T \times M_1 \times \cdots \times M_k$$

where T is a trivial (one-dimensional) module and the M_j are nontrivial, pairwise inequivalent simple modules $(1 \le j \le k)$. This follows from the fact that $x^p - 1$ has no multiple roots over F. Since the Galois group of the corresponding extension of F is generated by the Frobenius automorphism $x \mapsto x^r$, the dimension of each simple module M_i is equal to

$$\dim_F(M_i) = o_p(r) \tag{7}$$

where $o_p(r)$ denotes the multiplicative order of r modulo p.

The center of W is T. It will be more convenient to factor out T and compute the diameter of Cayley graphs in the quotient group W/T first.

Let

$$G = G(r,p) = W/T.$$

Then G is the semidirect product of the C-invariant subspace $V \lhd W$ of dimension $p-1$ and C. Let us fix a generator c of C. We shall write elements of G in the form vc^i where $v \in V$ and $i \in \{0, \dots, p-1\}$. The C-module V decomposes as

$$V = M_1 \times \cdots \times M_k \tag{8}$$

where the M_j are as above. For an arbitrary $v_i \in V$ let

$$v_i = (v_{i,1}, \dots, v_{i,k})$$

denote the decomposition of v_i according to (8).

Lemma 7: *The automorphism group* $\mathrm{Aut}(G)$ *acts transitively on* $G \setminus V$.

Proof: Using the identity

$$v^{-1}cv = v^{-1}(0c)v = (v^{c^{-1}} - v)c = v^{c^{-1}-1}c,$$

we see that the element c is conjugate to an arbitrary element wc where $w \in V^{(c^{-1}-1)} = V$ (here we use that the M_j are simple nontrivial modules).

Now the wreath product W can be understood as the semidirect product of the group algebra FC_p by C_p. This shows that every automorphism of C_p extends to an automorphism of W. Since the center is characteristic, the same holds for G. That is, the $p-1$ conjugacy classes outside V collapse into one automorphism class. ∎

The following well-known observation appears, e.g., as [2, Lemma 5.1].

Lemma 8: *Let G be a finite group and let $N \triangleleft G$. Then*

$$\begin{aligned} &\operatorname{diam}_{\max}(G) \leq \\ &\qquad 2\operatorname{diam}_{\max}(G/N)\operatorname{diam}_{\max}(N) + \operatorname{diam}_{\max}(N) + \operatorname{diam}_{\max}(G/N). \end{aligned} \tag{9}$$

Proof: For completeness, we include the proof. Let X be a set of generators of G. Then there exists a set T of coset representatives of N in G such that every element of T can be expressed as a word of length at most $\operatorname{diam}_{\max}(G/N)$ in X. Now the set S of Schreier generators, defined as

$$S = \{txu^{-1} \mid t \in T, x \in X, u \in txN \cap T\}, \tag{10}$$

generates N, so every element of N can be expressed as a word of length

$$\leq (2\operatorname{diam}_{\max}(G/N) + 1)\operatorname{diam}_{\max}(N) \tag{11}$$

in X. Finally, $G = TN$ gives us the required estimate. ∎

We note that Lemma 8 also holds if the subgroup $N \leq G$ is not normal; in this case $\operatorname{diam}_{\max}(G/N)$ should denote the worst diameter of a Schreier graph of G with stabilizer N.

Theorem 9: $\operatorname{diam}_{\max}(G) \leq (4r-1)(p-1)/2$.

The essence of the proof will be contained in the following two lemmas which refer to a specific type of generating set.

Lemma 10: *Let $X = \{c, w_2, \ldots, w_n\}$ where $w_2, \ldots, w_n \in V$. Then the following are equivalent:*

(A) *X generates G;*
(B) *$\{w_2, \ldots, w_n\}$ generates V as a C-module;*
(C) *For all $1 \leq j \leq k$ there exists $2 \leq i \leq n$ such that $w_{i,j} \neq 0$.*

Moreover, the generating set X is minimal if and only if the following holds:

(D) *for all $2 \leq i \leq n$ there exists $1 \leq j \leq k$ such that for all $\ell \neq i$ we have $w_{\ell,j} = 0$.*

Proof: Let FC denote the group algebra of C over F. Let H be the group generated by X. Let $v \in H$ be a product of elements of X. It is easy to see that $v \in V$ if and only if the exponent sum of c is divisible by p. By a standard rewriting argument and using that c has order p, this means that v can be written as a product of conjugates of the w_i by powers of c. Changing to module notation, we obtain

$$H \cap V = w_2FC + \cdots + w_nFC. \tag{12}$$

Since c generates C, this shows that (A) is equivalent to (B).

It is trivial that (B) implies (C). Assume that (C) holds. Let

$$W = w_2FC + \cdots + w_nFC. \tag{13}$$

Then W is a submodule of V such that all projections of W to the M_i in the decomposition (8) have nonzero images ($1 \le i \le k$). Since the M_i are pairwise inequivalent simple modules, we obtain $W = M_1 + \cdots + M_k = V$. So (C) implies (B).

We have shown that (A), (B) and (C) are equivalent.

The last claim now easily follows from (C). Indeed, let $2 \le i \le n$. Then $X \backslash \{w_i\}$ satisfies (C) if and only if for all j ($1 \le j \le k$) there exists $\ell \ne i$ such that $w_{\ell,j} \ne 0$. Thus (D) is equivalent to saying that $X \backslash \{w_i\}$ is not a generating set for $2 \le i \le n$, which holds if and only if X is minimal. ∎

Lemma 11: *Let $X = \{c, w_2, \ldots, w_n\}$ where $w_2, \ldots, w_n \in V$ and assume X generates G. Then every $v \in V$ can be obtained as a word of length at most $(r+1)(p-1)/2$ in X with the w_i occurring at most a total of $(r-1)(p-1)/2$ times.*

Proof: We may assume that $c, w_2, \ldots, w_n$ is a minimal generating set; otherwise, drop some of the w_i. For $2 \le i \le n$ let

$$A_i = \{1 \le j \le k \mid w_{i,j} \ne 0\}$$

and let

$$B_i = A_i \backslash \bigcup_{l=2}^{i-1} A_l.$$

Then the B_i are pairwise disjoint, nonempty (because the generating set is minimal) and

$$\bigcup_{i=2}^{n} B_i = \{1, \ldots, k\}.$$

Also for $2 \leq i \leq n$ let

$$V_i = \prod_{j \in B_i} M_j \subseteq M_1 \times \cdots \times M_k = V.$$

Then

$$V = V_2 \times \cdots \times V_n. \tag{14}$$

Let $d_i = \dim_F V_i$ $(2 \leq i \leq n)$. The vector w_i is not necessarily an element of V_i. Let w_i' be the V_i-component of w_i $(2 \leq i \leq n)$ corresponding to the decomposition (14).

Let $F[x]_d$ denote the space of polynomials of degree at most d over F. Since V_i is a direct product of simple pairwise inequivalent $F[x]$-modules, w_i' generates V_i and

$$V_i = w_i' F[x] = w_i' F[x]_{d_i - 1} \tag{15}$$

(otherwise a polynomial of degree at most $d_i - 1$ would annihilate V_i, a contradiction). This implies that the subspace $w_i F[x]_{d_i-1}$ projects surjectively onto V_i and so

$$V = w_2' F[x]_{d_2-1} + \cdots + w_n' F[x]_{d_n-1} = w_2 F[x]_{d_2-1} + \cdots + w_n F[x]_{d_n-1}.$$

Changing to group notation, this means that for all $v \in V$ there exist polynomials $f_2, \ldots, f_n$ such that $\deg f_j \leq d_j - 1$ and

$$v = w_2^{f_2(c)} + \cdots + w_n^{f_n(c)}.$$

Now we will use the Horner scheme to obtain v as a short word in the generating set $c, w_2, \ldots, w_n$.

Let $w \in V$ and $f(x) \in F[x]$ of degree $d - 1$. We claim that $w^{f(c)}$ can be obtained as a word in c and w of length at most $(r+1)d$ and we use w at most $(r-1)d$ times. This goes by induction on d. For $d = 1$ the claim is obvious.

If $d > 1$ then $f(c) = cg(c) + \epsilon$ where

$$\epsilon \in F = \{-\frac{r-1}{2}, \ldots, \frac{r-1}{2}\}$$

and $\deg g = d - 2$. Now

$$w^{f(c)} = c^{-1} w^{g(c)} c + \epsilon w$$

which by induction has length at most

$$2 + \frac{r-1}{2}(d-1) + \frac{r-1}{2} = \frac{r-1}{2}d.$$

Also, we used w at most $(r-1)d$ times. This proves the claim.

In particular $w_j^{f_j(c)}$ can be obtained as a word in c and w_j of length at most $(r+1)d_j/2$. Adding up, v can be obtained as a word in $c, w_2, \ldots, w_n$ of length at most $(r+1)(p-1)/2$ where we used the w_j at most $(r-1)(p-1)/2$ times. ∎

Now we turn to the proof of Theorem 9.

Proof of Theorem 9: Let $v_1c_1, \ldots, v_nc_n$ be a set of generators of G. For $\alpha \in \mathrm{Aut}(G)$ the Cayley graphs

$$\mathrm{Cay}(G, \{(v_1c_1)^\alpha, \ldots, (v_nc_n)^\alpha\}) \quad \text{and} \quad \mathrm{Cay}(G, \{v_1c_1, \ldots, v_nc_n\})$$

are isomorphic. Since at least one of the c_i has to be nontrivial, using Lemma (7) we can assume that $v_1 = 0$ and $c_1 = c$.

Now $c, v_2c_2, \ldots, v_nc_n$ generate G if and only if $c, v_2, \ldots, v_n$ do. For $2 \le i \le n$ let us define

$$w_i = [c, v_ic_i] = c^{-1}c_i^{-1}v_icv_ic_i = v_i^{c_ic-c_i} = (v_i^{c_i})^{c-1}.$$

Since the M_j are nontrivial simple, $w_{i,j} = 0$ if and only if $v_{i,j} = 0$. Using Lemma 10 this shows that $c, w_2, \ldots, w_n$ also generate G.

Let us now apply Lemma 11 to this latter set of generators. Noting that $w_j = [c, v_jc_j]$ can be obtained as a word of length 4 in c and v_jc_j, we infer from Lemma 11 that any $v \in V$ can be obtained as a word in the original generating set $v_1c_1, \ldots, v_nc_n$ of length at most

$$4(r-1)(p-1)/2 + (p-1) = (2r-1)(p-1).$$

So the diameter of G with respect to $v_1c_1, \ldots, v_nc_n$ is at most

$$(2r-1)(p-1) + \frac{p-1}{2} = \frac{(4r-1)(p-1)}{2}.$$

This completes the proof of the theorem. ∎

Proof of Theorem 3: The center $T = Z(W)$ has order 2 so $\mathrm{diam}_{\max}(T) = 1$. Using Theorem 9 and Lemma 8 we get

$$\mathrm{diam}_{\max}(W) \le 3\,\mathrm{diam}_{\max}(G) + 1 \le \frac{3}{2}(4r-1)(p-1) + 1$$

as claimed. ∎

For a finite group G let $m(G)$ denote the largest size of a minimal generating set of G. This measure has been investigated by Saxl and Whiston (see [10] and references therein) for various classes of groups.

We are ready to prove our main theorem.

Proof of Theorem 2: Heath-Brown's solution [6] to Artin's conjecture tells us that, with maybe two exceptions, every prime r is a primitive root modulo p for infinitely many primes p. In particular, for one of $r = 3, 5$ or 7 there exists an infinite set $p_1, p_2, \dots$ of primes such that $o_{p_i}(r) = p_i - 1$ for all i.

Let

$$W_i = W(r, p_i).$$

We claim that the family $\{W_i\}$ has uniform logarithmic diameter. Indeed, in the decomposition (7), $V = M_1$ is itself irreducible and so $U = T \times M_1$. Using Lemma 10 it follows that

$$m(W_i) = 3 \quad (i \geq 1).$$

Now let X be a minimal generating set for G_i. Applying Theorem 3 and estimating for $r = 3, 5, 7$ we get

$$\lim_{i \to \infty} \frac{\operatorname{diam}(G_i, X) \log |X|}{\log |G_i|} \leq \frac{3(4r-1)\log 3}{2 \log r} < 22.9.$$

This implies that for infinitely many i we have

$$\operatorname{diam}(G_i, X) < 23 \frac{\log |G_i|}{\log |X|}.$$

This completes the proof of Theorem 2. ∎

Note that all the results and estimates hold for $r = 2$ with somewhat weaker constants.

Finally, we prove the weaker but more general estimate stated in Theorem 4.

Proof of Theorem 4: Let $k = |H|$. The group G is a semidirect product of $V = C_r^k$ and H. Let $X = \{v_1 h_1, \dots, v_n h_n\}$ be a generating set of G with $v_i \in V$ and $h_i \in H$ $(1 \leq i \leq n)$. Then $\{h_1, \dots, h_n\}$ trivially generates H. Since any undirected Cayley graph of H has diameter at most $k - 1$, for all $h \in H$ there exists a word w_h in $h_1, \dots, h_n$ of length less than k such that $w_h(h_1, \dots, h_n) = h$. For $h \in H$ let

$$\widetilde{h} = w_h(v_1 h_1, \dots, v_n h_n)$$

and let $T = \{\widetilde{h} \mid h \in H\}$. Then T is a transversal for V in G, so

$$Y = \{txu^{-1} \mid t, u \in T, x \in X, Vu \in Vtx\}$$

is a set of Schreier generators for V. Let Z be a minimal generating subset (basis) of Y.

Now each element of Z has length at most $2(k-1)+1 < 2k$ in X. Each element of V has length at most $(r-1)k$ in Z and so it has length at most $2(r-1)k^2$ in X. This gives us

$$\operatorname{diam}(G, X) < 2(r-1)k^2 + k < (2r-1)|H|^2 \leq (2r-1)\log^2|G|,$$

completing the proof of Theorem 4. ∎

Remark: As we have seen, generation in $W(r,p)$ is governed by the structure of the underlying module and the maximum size of a minimal generating set of $W(r,p)$ is

$$m(W(r,p)) = 2 + (p-1)/o_p(r). \tag{16}$$

From Heath-Brown's result, $m(W(r,p)) = 3$ occurs infinitely often even if we restrict r to be one of $3, 5$ or 7. It is interesting to observe that the other extreme, namely, when $o_p(r)$ takes on its minimal possible value $\log_r(p-1)$, occurs exactly when $r = 2$ and p is a Mersenne prime.

References

[1] D. Aldous, *On the Markov chain simulation method for uniform combinatorial distributions and simulated annealing*, Probability in Engineering and Informational Sciences **1** (1987), 33–46.

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

[3] L. Babai and M. Szegedy, *Local expansion of symmetrical graphs*, Combinatorics, Probability, and Computing **1** (1992), 1–11.

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

[5] A. Gamburd and M. Shahshahani, *Uniform diameter bounds for some families of Cayley graphs*, International Mathematics Research Notices **71** (2004), 3813–3824.

[6] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, The Quarterly Journal of Mathematics. Oxford **37** (1986), 27–38.

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

[8] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Progress in Mathematics 125, Birkhäuser Verlag, Basel, 1994.

[9] A. Lubotzky, *Collected Problems at the Conference on Automorphic Forms*, Group Theory and Graph Expansion, Institute for Pure and Applied Mathematics, Los Angeles, 2004.

[10] J. Saxl and J. Whiston, *On the maximal size of independent generating sets of* $\mathrm{PSL}_2(q)$, Journal of Algebra **258** (2002), 651–657.