Finite groups of uniform logarithmic diameter

Miklós Abért* and László Babai†

May 20, 2005

Abstract

We give an example of an infinite family of finite groups G_n such that each G_n can be generated by 2 elements and the diameter of every Cayley graph of G_n is $O(\log(|G_n|))$. This answers a question of A. Lubotzky.

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 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, 7]).

Let us define the *worst diameter* of G,

$$\mathrm{diam}_{\max}(G) = \max \{\mathrm{diam}(G, X) \mid X \subseteq G, \langle X \rangle = G\}$$

to be the maximum diameter over all sets of generators of G.

Alex Lubotzky [8] asked whether there exists a family of groups G_n such that the G_n have a bounded number of generators and the worst diameter of G_n is $O(\log |G_n|)$.

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 poly-logarithmic in the size of G_n. Her 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_2.

*Email: abert(at)math(dot)uchicago(dot)edu. Partially supported by NSF Grant DMS-0401006.

†Email: laci(at)cs(dot)uchicago(dot)edu.

We demonstrate that there exists a family of solvable groups with logarithmic worst diameter. Let p be an odd prime and let $W(p)$ denote the wreath product $W_p = C_2 \wr C_p$.

Theorem 1 $\quad \mathrm{diam}_{\max}(W_p) \leq 20(p-1).$

Since the groups W_p can be generated by 2 elements and the size of W_p is $|W_p| = p2^p$, this answers Lubotzky's question affirmatively.

Let us fix some notation. Let $F = \mathbb{F}_2$ denote the field of 2 elements. The wreath product $W = W_p$ 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 splits as

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

where T is a trivial (one-dimensional) module and the M_i are nontrivial, pairwise inequivalent simple modules. 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 $x \longmapsto x^2$, the dimension of each simple module M_i is equal to the multiplicative order of 2 modulo p.

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

Let $G = W/T$. Then G is the semidirect product of the F-vectorspace $V \lhd W$ of dimension $p-1$ and C. Let us fix a generator c of C. We shall write the elements of G in the form vc^i where $v \in V$ and $i \in \{0, \ldots, p-1\}$. The C-module V splits as

$$V = M_1 \times \cdots \times M_k$$

where the M_i are as above.

Lemma 2 *The automorphism group* $\mathrm{Aut}(G)$ *acts transitively on* $G \backslash V$*.*

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_i are simple nontrivial modules).

Now the wreath product W_p 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 3 *Let G be a finite group and let $N \lhd G$. Then*

$$\mathrm{diam}_{\max}(G) \leq 2\,\mathrm{diam}_{\max}(G/N)\,\mathrm{diam}_{\max}(N) + \mathrm{diam}_{\max}(N) + \mathrm{diam}_{\max}(G/N)$$

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 $\mathrm{diam}_{\max}(G/N)$ in X. Now the set S of Schreier generators, defined as

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

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

$$\leq (2\,\mathrm{diam}_{\max}(G/N) + 1)\,\mathrm{diam}_{\max}(N)$$

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

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

Theorem 4 $\quad \mathrm{diam}_{\max}(G_p) \leq \frac{13}{2}(p-1)$.

The essence of the proof will be contained in the following case which refers to a specific type of generating set.

Lemma 5 *Let $X = \{c, w_2, \ldots, w_n\}$ where $w_2, \ldots, w_n \in V$ and assume X generates G_p. Then every $v \in V$ can be obtained as a word of length $\leq 3(p-1)$ in X with the w_i occurring at most a total of $p-1$ times.*

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

$$A_i = \{j \mid w_{i,j} \neq 0\}$$

and

$$B_i = A_i \setminus \bigcup_{j=2}^{i-1} A_j.$$

Then the B_i are disjoint, non-empty (because of the irredundancy) and

$$\bigcup_{j=2}^{n} B_j = \{2, \ldots, n\}$$

Also let

$$V_j = \prod_{i \in B_j} M_i \subseteq M_1 \times \cdots \times M_k = V.$$

Then

$$V = V_2 \times \cdots \times V_n.$$

Let $d_j = \dim_F V_j$.

Let $F[x]_d$ denote the space of polynomials of degree at most d over F. Since V_j is a direct product of simple pairwise non-equivalent $F[x]$-modules, if $v \in V_j$ is a generator of V_j then

$$V_j = vF[x] = vF[x]_{d_j - 1}$$

(otherwise a polynomial of degree at most $d_j - 1$ would annihilate V_j, a contradiction).

This implies that

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

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 $c, w_2, \ldots, w_n$.

We claim that if $w \in V$ and $f(x) \in F[x]$ of degree $d - 1$ then $w^{f(c)}$ can be obtained as a word in c and w of length at most $3d$ and we use w at most d times. This goes by induction on d. For $d = 1$ it is obvious. If $d > 1$ then $f(c) = cg(c) + \epsilon$ where $\epsilon = 0$ or 1 and $\deg g = d - 2$. Now

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

which by induction has length at most $2 + 3(d-1) + 1 = 3d$ (and we used w at most 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 $3d_j$. Adding up, v can be obtained as a word in $c, w_2, \ldots, w_n$ of length at most $3(p-1)$ where we used the w_j at most $p-1$ times. ■

Now we turn to the proof of Theorem 4.

Proof of Theorem 4. Let $v_1c_1, \ldots, v_nc_n$ be a set of generators of G. For $\alpha \in \mathrm{Aut}(G)$ the Cayley graphs

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

are isomorphic. Since at least one of the c_i have to be nontrivial, using Lemma 2 we can assume that $v_1 = 0$ and $c_1 = c \neq 1$.

Now $c, v_2c_2, \ldots, v_nc_n$ generate G if and only if $c, v_2, \ldots, v_n$ do.

Let

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

be the decomposition of v_i according to $V = M_1 \times \cdots \times M_k$. It is easy to see that $c, v_2, \ldots, v_n$ generate G if and only if $v_2, \ldots, v_n$ generate V as a C_p-module and this happens if and only if for all j $(1 \leq j \leq k)$ there exists i such that $v_{i,j} \neq 0$.

For $2 \leq i \leq n$ 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 the observation made in the previous paragraph, this shows that $c, w_2, \ldots, w_n$ also generate G.

Let us now apply Lemma 5 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 5 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 $6(p-1)$. So the diameter of G with respect to $v_1c_1, \ldots, v_nc_n$ is at most

$$6(p-1) + \frac{p-1}{2} = \frac{13}{2}(p-1).$$

■

Proof of Theorem 1. The center $T = Z(W)$ has order 2 so $\mathrm{diam}_{\max}(T) = 1$. Using Theorem 4 and Lemma 3 we get

$$\mathrm{diam}_{\max}(W) \leq 3\,\mathrm{diam}_{\max}(G) + 1 \leq \frac{39}{2}(p-1) + 1 \leq 20(p-1)$$

what we wanted to show. ∎

Remark. A similar proof shows that the wreath product $C_q \wr C_p$, where q is a fixed prime and p runs through all primes not equal to p, has worst diameter

$$\mathrm{diam}_{\max}(C_q \wr C_p) \leq K_q p$$

where K_q depends only on q.

For a finite group G let $r(G)$ denote the largest size of irredundant generating sets. (A generating set X is irredundant if no proper subset of X generates G). This measure has been investigated by Saxl and Whiston (see [9] and references therein) for various classes of groups.

It is natural to ask the value of $r(G_p)$. As we have seen, generation in G_p is governed by the structure of the underlying module and so $r(G_p) = 1 + k$ where $k = (p-1)/o_p(2)$, where $o_p(2)$ denotes the multiplicative order of 2 modulo p.

This permits a wide range of values for $r(G_p)$ in terms of p:

$$2 \leq r(G_p) \leq 1 + \frac{p-1}{\log_2(p-1)}. \tag{1}$$

Let us look at the extremes.

The minimum possible value $r(G_p) = 2$ occurs if and only if 2 is a primitive root modulo p. Heath-Brown's solution [6] to Artin's conjecture tells us that, with maybe two exceptions, every prime q is a primitive root modulo p for infinitely many primes p. So with any luck (that is, if 2 is not one of these exceptions), we have infinitely many primes such that $r(G_p) = 2$. In case we are not lucky, one of $C_3 \wr C_p$ and $C_5 \wr C_p$ will do, according to the remark above.

Conversely, the smallest possible value for $o_p(2)$ is $\log_2(p-1)$ and this occurs if and only if p is a Mersenne prime. In this case, $r(G_p)$ takes its largest possible value, $(p-1)/\log_2(p-1)$.

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, Á. Seress: On the diameter of permutation groups. *Europ. J. Comb.* **13** (1992), 231-243.

[3] L. Babai, 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. Manuscript, 2004.

[5] A. Gamburd and M. Shahshahani: Uniform diameter bounds for some families of Cayley graphs. *Int. Math. Res. Not.* **71** (2004), 3813–3824.

[6] D. R. Heath-Brown: Artin's conjecture for primitive roots. *Quart. J. Math. Oxford* **37** (1986), 27-38.

[7] A. Lubotzky: *Discrete groups, expanding graphs and invariant measures.* Progress in Mathematics 125, Birkhäuser Verlag, Basel, 1994.

[8] A. Lubotzky: Collected Problems at the Conference on Automorphic Forms, Group Theory and Graph Expansion. IPAM 2004

[9] J. Saxl and J. Whiston: On the maximal size of independent generating sets of $\mathrm{PSL}_2(q)$. *J. Algebra* **258/2** (2002), 651–657.