Discrete Applied Mathematics 25 (1989) 99-104
North-Holland

SOME CAYLEY GRAPHS FOR SIMPLE GROUPS

W.M. KANTOR*

Mathematics Department, University of Oregon, Eugene, OR 97403, USA

Received 9 January 1989

1. Introduction

Let $\mathscr{G}$ be a finite connected regular graph of degree $k>2$ having n vertices and diameter d. Fix a vertex x. Each vertex at distance $i<d$ from x is joined to at most $k-1$ vertices at distance $i+1$ from x. Thus, $n\leq 1+k+k(k-1)+k(k-1)^2+\cdots+k(k-1)^{d-1}\leq 2k^d$, so that $d\geq(\log\frac{1}{2}n)/(\log k)$, where logarithms are to the base 2. This argument suggests that graphs $\mathscr{G}$ in which $d\leq C\log n$ have a "tree-like structure".

One way to look for such (families of) graphs is to use Cayley graphs. Let S be a subset generating a finite group G, where we assume that $1\notin S$. The corresponding Cayley graph $\mathscr{G}(G,S)$ is the undirected graph (without loops) whose vertices are the elements of G and whose edges are the pairs $\{g,sg\}$ with $g\in G$ and $s\in S$. The group G acts as a vertex-transitive automorphism group of $\mathscr{G}(G,S)$ (with $h\in G$ sending the vertex g to the vertex gh). In particular, $\mathscr{G}(G,S)$ is a regular graph, whose degree k satisfies $k\leq 2|S|$ (note that the vertices g and g' ar? adjacent if and only if $g'g^{-1}\in S\cup S^{-1}$, the latter set having size $\leq 2|S|$—with equality if and only if S contains no element of order 2). The distance $d(g,g')$ is the same as $d(1,g'g^{-1})$, which is the minimal length of the expressions of $g'g^{-1}$ as words in the alphabet $S\cup S^{-1}$. In particular, the diameter of $\mathscr{G}(G,S)$ is the smallest integer d such that every element of G can be expressed as a word of length $\leq d$ in the alphabet $S\cup S^{-1}$. We are interested in the case in which $|S|$ is bounded and $d\leq C\log|G|$.

Nonexample: It is easy to see that no such set S (of bounded size) can exist for the case of cyclic groups G of prime order.

The remainder of this note is devoted to a discussion of the following joint work with Babai and Lubotzky [1].

Theorem (Babai, Kantor and Lubotzky [1]). *There is a constant C such that every nonabelian finite simple group has a set S of at most 7 generators for which the diameter of $\mathscr{G}(G,S)$ is at most $C\log|G|$.*

* Supported in part by NSF grants DMS 87-01794 and INT 85-12644.

The constant C can be taken to be |Monster|, but this is a gross overestimate. It seems likely that the number 7 can be lowered to 2, but we have not yet been able to do this. One obstacle to such a reduction will be seen below. It should also be possible to find both a set S of at most 7 generators (in fact, just 2 generators) and an $O(\log |G|)$ step algorithm which will write an arbitrary element of G as a word in $S \cup S^{-1}$. Below we will implicitly see examples of such algorithms. However, presumably it would be unreasonably difficult to expect to be able to find the *shortest* expression for an element of G as a word in $S \cup S^{-1}$.

The proof of the theorem uses the classification of finite groups—or, more precisely, the fact that there are only finitely many sporadic simple groups, which can therefore be ignored. In other words, the theorem really concerns the alternating groups A_n and the finite groups of Lie type (i.e., the finite analogues of the simple Lie groups over $\mathbb{C}$). The proof applies to a slightly more general situation, that of "nearly simple" groups: groups G such that $S \leq G \leq \operatorname{Aut} S$ for a nonabelian simple group S. The most obvious example is S_n, in which case the theorem is almost familiar. However, the very familiar 2-element Bubble Sort [3] generating set $\{(1,2),(1,2,3,\ldots,n)\}$ produces a graph of diameter $\theta(n^2)$, which suggests that it is not straightforward to find 2 generators yielding a diameter of $O(\log n!) = O(n \log n)$.

The theorem leaves many interesting questions. Does every pair of generators of a finite simple group produce a Cayley graph of polylog diameter (i.e., diameter $O(\log^c |G|)$ for some constant c)? For example, as indicated above the Bubble Sort generators behave in this manner. On the other hand it is conceivable that "most" pairs of generators of S_n produce diameter $O(n \log n)$—more precisely, that a random pair of generators has this property with probability close to 1. However, even the weaker result, that a random pair of generators has polynomial diameter with probability close to 1, would be extremely interesting.

Steinberg [7] produced a pair of generators for each group of Lie type. What is the diameter of the corresponding Cayley graph? While it seems to be difficult to answer this, a modification of his approach produces diameter $O(\log |G|)$ in many situations.

The girth g of a graph satisfies $g \leq 2d$. Therefore, just as it is natural to bound d from above it is natural to try to bound g from below. In particular, in the situation of the theorem, is there a constant C' such that each G has a set S of generators as in the theorem for which, in addition, $g \geq C' \log |G|$? Examples for $\mathrm{PSL}(2,p)$ are given in [5].

In the remainder of this note we will sketch the arguments used in the following three situations:

- S_n (which is similar to but slightly simpler than A_n),
- $\mathrm{PSL}(2,p)$ for an odd prime p,
- $\mathrm{PSL}(2,q)$ for an odd prime power q.

Most finite groups of Lie type are built from the groups S_n and $\mathrm{PSL}(2,q)$ (this is described in [2, Ch. 8]). This is not to say that the general case is easy, rather that these are the basic cases—besides being the most interesting ones.

Recall that, if g and h are elements of a group, then $g^h = h^{-1}gh$.

2. Symmetric groups

In this section we will exhibit 3 generators of S_n, with respect to which the diameter is $O(\log n!) = O(n \log n)$. Let X be an n-element set.

Case 1: $n-1$ *odd*. Identify X with $\{\infty\} \cup \mathbb{Z}_{n-1}$, and consider the 2 permutations $b_0 : x \to 2x$ and $b_1 : x \to 2x+1$ (both fixing ∞). Any element $t \in \mathbb{Z}_{n-1}$ can be written

$$t = \sum_{i=0}^{m} a_i 2^i = (\cdots(a_m 2 + a_{m-1})2 + \cdots)2 + a_0,$$

where $m = [\log n]$ and each $a_i \in \{0,1\}$ (the second equality is "Horner's rule"). Thus, our arbitrary $t \in \mathbb{Z}_{n-1}$ can be written $t = 0^w$ for the element $w = b_{a_m} b_{a_{m-1}} \cdots b_{a_0} \in \langle b_0, b_1 \rangle$ of length $O(\log n)$.

We claim that $S := \{(\infty, 0), b_0, b_1\}$ behaves as desired. For, if t and w are as above, then (∞, t) can be written $(\infty, t) = (\infty, 0)^w$, and hence has length $\leq 2(m+1)+1$ in S. Moreover, any element of S_n is easily written as a product of $\leq 2n$ of the transpositions (∞, t), $t \neq 0$. Thus, each element of S_n has length $\leq 2n(2m+3) = O(n \log n)$ in $S \cup S^{-1}$.

Case 2: $n-1$ *even*. This time identify X with $\{\infty, \infty'\} \cup \mathbb{Z}_{n-2}$, and consider the permutations $b_0 : x \to 2x$ and $b_1 : x \to 2x+1$ (both fixing ∞ and ∞'). As before, it is easy to check that $S := \{(\infty, 0), (\infty, \infty')b_0, b_1\}$ behaves as required. (Namely, we first obtain $(\infty', 0) = (\infty, 0)^{(\infty, \infty')b_0}$ and $(\infty, \infty') = (\infty, 0)^{(\infty', 0)}$, then one of the transpositions (α, t), $\alpha \in \{\infty, \infty'\}$ for each $t \in \mathbb{Z}_{n-2}$, and finally use the fact that $(\infty, t) = (\infty', t)^{(\infty, \infty')}$.)

The same idea works for A_n as well, if sufficient care is taken to deal only with even permutations. Decreasing from 3 to 2 generators requires some uninformative arithmetical bookkeeping, and hence is omitted.

Note that there is an $O(n \log n)$ algorithm implicit in the above sketch, writing an arbitrary element of S_n as a "short" product of members of $S \cup S^{-1}$.

3. PSL(2, q)

In this section we will consider the groups $G = \mathrm{PSL}(2, q)$ with q a power of an odd prime p. These are defined as follows.

Let $\mathrm{SL}(2, q)$ denote the group of all 2×2 matrices, with entries in $\mathrm{GF}(q)$, having determinant 1. Then $\mathrm{PSL}(2, q)$ is just $\mathrm{SL}(2, q)/\langle -1 \rangle$. (Equivalently, $\mathrm{PSL}(2, q)$ is the group of all linear fractional transformations $x \to (ax+b)/(cx+d)$ with $a,b,c,d \in \mathrm{GF}(q)$ and $ad-bc=1$.)

We will write elements of PSL(2, q) as matrices, with the understanding that each matrix is to be identified with its negative. Note that $|\mathrm{PSL}(2,q)| = \frac{1}{2}q(q^2-1)$, so that $\mathrm{O}(|\mathrm{PSL}(2,q)|) = \mathrm{O}(\log q)$.

When $q=p$, a standard and natural generating set for G is

$$\left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}\right\}.$$

It is, indeed, true that the resulting Cayley graph has diameter $\mathrm{O}(\log p)$. This is proved in [1], using expanders somewhat as in [4, 5], by means of very deep number theoretic results [6, 8]. However, there is no known algorithm (in the sense of Section 1) for this generating set.

Note that each of the above generators has order p. Thus, a basic problem here is dealing with all the powers of such generators.

Another natural generating set of PSL(2, p) is

$$\left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right\}.$$

However, this suffers from the same problems as the previous one. In fact, it is easy to check that each of the new generators has length ≤ 3 in the old ones and their inverses, and vice versa.

As we will soon see, a slight modification

$$\left\{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & -2\\ \frac{1}{2} & 0\end{pmatrix}\right\}$$

behaves as required in the theorem.

First we will need some notation. Write

$$x(t) = \begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}, \quad h(b) = \begin{pmatrix}b^{-1} & 0\\ 0 & b\end{pmatrix} \quad \text{for } b \neq 0, \quad t \in \mathrm{GF}(q),$$

$$r = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

These matrices behave as follows:

$$x(t+u) = x(t)x(u), \quad x(t)^{h(b)} := h(b)^{-1}x(t)h(b) = x(tb^2)$$
$$\text{for all } b \neq 0, \ t, u \in \mathrm{GF}(q).$$

Case 1: $q=p$. We will show that

$$S = \{x(1), s\}, \text{ where } s = h(\tfrac{1}{2})r,$$

works. Note that this is precisely the generating set mentioned above. If $ad-bc=1$, then a straightforward calculation yields that, for $c \neq 0$,

$$g := \begin{pmatrix} a & b \\ c & d \end{pmatrix} = x(-c^{-1}+ac^{-1})x(-c)^r x(-c^{-1}+dc^{-1}). \qquad (*)$$

In case $c=0$ use rg instead of g. As we will see, this reduces the proof to showing that each $x(a)$, $a\in \mathrm{GF}(p)$, has length $O(\log p)$ with respect to the given set S.

Every element $t\in \mathrm{GF}(p)$ can be written in the form

$$t=\sum_{i=0}^{m} a_i 2^{2i} = (\cdots(a_m 2^2 + a_{m-1})2^2 + \cdots)2^2 + a_0$$

(the second equality is "Horner's rule" once again), where $m\leq \log p$ and $a_i\in \{0,1,2,3\}$ (base 4 representation of t).

By matrix multiplication,

$$h(2)^{-1} = h(\tfrac{1}{2}) = x(1)^{-2}(x(1)^2)^s x(1)(x(1)^{-4})^s$$

has length ≤ 13. Since $s=h(\frac{1}{2})r$, it follows that r has length ≤ 14. Moreover,

$$x(t) = (\cdots(x(a_m)^{h(2)}x(a_{m-1}))^{h(2)}\cdots)^{h(2)}x(a_0)$$

by Horner's rule. Here, each $x(a_i)=x(1)^{a_i}$ has length ≤ 3, while $h(2)$ has length ≤ 13. Thus $x(t)$ has length $\leq 2\cdot 13m+\sum a_i = O(\log p)$.

Let $X=\{x(t)\mid t\in \mathrm{GF}(p)\}\cong \mathrm{GF}(p)^+$, and set $Y=X^r$. By (*), $G=\{1,r\}XYX$. We just saw that each element of X has length $O(\log p)$. Hence, every element of G has length $3\cdot O(\log p)=O(\log|G|)$.

Case 2: $q=p^e$, $e\geq 2$. Let θ be a primitive element of $\mathrm{GF}(q)$. This time we will show that

$$S=\{x(1), h(\tfrac{1}{2})r, h(\theta)\}$$

works.

Note that $\mathrm{GF}(q)=\mathrm{GF}(p)(\theta^2)$, so that every element $t\in \mathrm{GF}(q)$ can be written in the form

$$t=\sum_{i=0}^{e-1} a_i\theta^{2i} = (\cdots(a_{e-1}\theta^2 + a_{e-2})\theta^2+\cdots)\theta^2 + a_0$$

with $a_i\in \mathrm{GF}(p)$. As above, each $x(t)$ is a word

$$x(t) = (\cdots(x(a_{e-1})^{h(\theta)}x(a_{e-2}))^{h(\theta)}\cdots)^{h(\theta)}x(a_0)$$

in e elements $x(a)$, $a\in \mathrm{GF}(p)$, and $2e$ elements $h(\theta)^{\pm 1}$. We just saw that each such $x(a)$ has length $O(\log p)$. Thus, each $x(t)$ has length $2e+e\cdot O(\log p)=O(\log q)$.

By (*), each element of G has length $O(\log q)=O(\log|G|)$.

By crudely counting lengths it is easy to check that the diameter just found for $\mathrm{PSL}(2,q)$ is $\leq 135\log|G|$.

Note that there is an algorithm (cf. Section 1) implicit in the above argument.

We have seen that $\mathrm{PSL}(2,p)$ has a 2-generator set producing a Cayley graph of diameter $O(\log p)$. However, we have not been able to obtain such a 2-generator set for $\mathrm{PSL}(2,q)$. This is a major obstacle for the reduction of the "7" in the theorem to "2". The argument we have just used would go through if the following conjecture holds:

Conjecture. There is an effectively computable constant C such that, for any finite field GF(q) of odd order and some generator θ of GF(q)*, every element $t \in$ GF(q) can be written

$$t = \sum_{i=0}^{m} a_i \theta^{2i}$$

with $m \leq C \log q$ and all $a_i \in \mathbb{Z}$ with $|a_i| \leq C$.

In fact, it seems plausible that every generator θ of GF(q) behaves in the required manner (even in the case $q = p$).

References

[1] L. Babai, W.M. Kantor and A. Lubotzky, Small diameter Cayley graphs for finite simple groups, European J. Combin., to appear.

[2] R. Carter, Simple Groups of Lie Type (Wiley, London, 1972).

[3] D.E. Knuth, The Art of Computer Programming 3: Sorting and Searching (Addison-Wesley, Reading, MA, 1973).

[4] A. Lubotzky, R Phillips and P. Sarnak, Explicit expanders and the Ramanujan conjecture, in: Proceedings 18th Symp. Theory of Computation (1986) 240-246.

[5] A. Lubotzky, R. Phillips and P. Sarnak, Ramanujan graphs, Combinatorica 8 (1988) 261-277.

[6] A. Selberg, On the estimation of Fourier coefficients of modular forms, AMS Proc. Symp. Pure Math. 8 (1965) 1-15.

[7] R. Steinberg, Generators for simple groups, Canad. J. Math. 14 (1962) 277-283.

[8] A. Weil, Sur les courbes algébriques et les variétés que s'en déduisent, Acta Sci. Ind. 1041 (1948).