Europ. J. Combinatorics (1989) **10**, 507–522

Small-diameter Cayley Graphs for Finite Simple Groups

L. Babai, W. M. Kantor and A. Lubotsky

Let S be a subset generating a finite group G. The corresponding Cayley graph $\mathscr{G}(G, S)$ has the elements of G as vertices and the pairs $\{g, sg\}$, $g \in G$, $s \in S$, as edges. 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 $\leqslant d$ using elements from $S \cup S^{-1}$. A simple count of words shows that $d \geqslant \log_{2|S|}(|G|)$. We prove that 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 $C \log |G|$.

1. Introduction

Let S be a subset generating a finite group G. The pair (G, S) determines a connected Cayley graph $\mathscr{G}(G, S)$, the vertices of which are the elements of G and the edges of which are the pairs $\{g, sg\}$ with $g \in G$ and $s \in S$. The diameter diam $\mathscr{G}(G, S)$ of $\mathscr{G}(G, S)$ is the smallest integer d such that every element of G can be expressed as a word of length $\leqslant d$ using elements from $S \cup S^{-1}$. A simple count of words shows that $d \geqslant \log_{2|S|}(|G|)$. If we require that $|S|$ be bounded—so that the valence of $\mathscr{G}(G, S)$ is bounded—then it follows that d cannot be better than $O(\log |G|)$ (here, and unless otherwise indicated, logarithms will be to the base 2). We will prove the following:

Theorem 1.1. *There is a constant C such that every nonabelian finite simple group G has a set S of at most 7 generators for which the diameter of $\mathscr{G}(G, S)$ is at most $C \log |\mathrm{G}|$.*

A crude estimate for C is 10^{10}, but we will not include the bookkeeping required to estimate C. Nevertheless, our arguments will make it clear that a bound C is tedious but not difficult to compute.

The proof of the theorem uses the classification of finite simple groups; or, more precisely, the fact that there are only finitely many sporadic simple groups, which can therefore be ignored throughout the paper. Somewhat detailed properties of groups of Lie type will be required for our arguments. These will be used to reduce to groups of rank 1, which are among the most interesting cases (see the last remarks in Sections 3 and 6).

Note that the theorem is not true in the case of cyclic groups G of prime order. Also note that the very familiar 'Bubble Sort' generating set $\{(1, 2), (1, 2, \ldots, n)\}$ of the symmetric group S_n produces a graph of diameter $\theta(n^2)$. In Section 2 we present unfamiliar, somewhat complicated 2-element generating sets for A_n and S_n producing Cayley graphs of diameter $O(n \log n)$ (as well as 3-element $O(n \log n)$ generating sets of a fairly nice sort). The generating sets in section 2 share with the Bubble Sort pair the property of having an associated algorithm: an $O(\log |G|)$ step algorithm which will write any given element of G as a word in $S \cup S^{-1}$.

A standard pair of generators for $G = SL(2, p)$, p prime, consisting of the matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

generates G with corresponding diameter $O(\log |G|) = O(\log p)$. However, the only

0195-6698/89/060507 + 16 \$02.00/0

proof we know for this depends on deep number-theoretic results of Selberg [15] and Weil [21], involving the estimation of the eigenvalues of the Laplacian operator of some arithmetic hyperbolic surfaces (see Section 8, where there is also an indication of connections between our work and eigenvalues, expanders, Ramanujan graphs, and Kazhdan's Property (T)). In Section 3 we present another pair of generators of $SL(2,p)$ for which there is an elementary proof that the diameter is $O(\log p)$. Moreover, this new set has an associated algorithm, whereas we do not know such an algorithm for the above standard pair of generators.

While our theorem concerns Cayley graphs arising from 'optimal' generating sets, one can also ask for information concerning the diameters produced by arbitrary generating sets. In [4] it was conjectured that, for a finite nonabelian simple group G, any generating set produces a graph of diameter $O((\log|G|)^c)$. For a description of results concerning this, and related questions, see Section 9.

The theorem leaves open several other interesting questions. Some of these are mentioned in Section 8 and 9. Here we will only mention two. First, in (1.1) it should be possible to use only 2 generators, but we have not been able to use our arguments (or the generators in [16]) in order to produce such a precise result. In fact, even for $PSL(2,q)$, q a prime power, we do not know such a generating set. Second, we conjecture (cf. Section 8) that every finite simple group produces Cayley graphs of bounded valence that are expanders. Even for A_n (and S_n) this is open.

This paper is organized as follows. The case of A_n is handled in Section 2. At the same time we deal with the corresponding questions concerning S_n. The case $PSL(n,q)$ is dealt with for $n=2$ and $n\geqslant 3$ in Sections 3 and 4, respectively. The arguments used in those sections are then extended to all of the remaining nonsporadic finite simple groups (i.e., the remaining groups of Lie type) in Sections 5–7. All of these arguments eventually reduce primarily to the situations S_n and $PSL(2,q)$ already considered in Sections 2 and 3. Implicit in our arguments is an associated algorithm, but we have not included this here.

2. Alternating Groups

In this section we prove (1.1) for the alternating groups as well the corresponding result for the symmetric groups. We also consider some closely related groups (the Weyl groups of type B_l and D_l).

Theorem 2.1. *S_n has a set of 2 generators with respect to which the diameter is $O(n\log n)$.*

Before giving the proof of this result, we will present some motivation together with a proof of a weaker result in which 3 generators are used. This weaker version is much simpler, but contains the essential ingredients for a proof of (2.1).

Let X be an n-element set. Let ∞ be a point of X. It suffices to construct a set S such that some transposition (∞,x) has length $O(\log n)$, and such that all points of X-$\{\infty,x\}$ can be obtained from x by using elements w of S-length $O(\log n)$ fixing ∞. For then all transpositions $(\infty,x)^w=(\infty,x^w)$ will have S-length $O(\log n)$. Since every permutation is a product of at most $2n$ transpositions of the form (∞,x), it will follow that every element of G has S-length $O(n\log n)$, as required.

Assume first that $n-1$ is odd. Identify X with $\{\infty\}\cup\mathbb{Z}_{n-1}$, and consider the 2 permutations $b\colon x\mapsto 2x$ and $c\colon x\mapsto 2x+1$ (both fixing ∞). Any element $t\in\mathbb{Z}_{n-1}$ can be written as

$$t=\sum_0^m a_i2^i=(\cdots(a_m2+a_{m-1})2+\cdots)2+a_0,$$

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

When $n-1$ is even, this argument does not work. However, in that case identify X with $\{\infty, \infty'\} \cup \mathbb{Z}_{n-2}$, and consider the permutations $b: x \mapsto 2x$ and $c: x \mapsto 2x+1$ (both fixing ∞ and ∞'). As before, it is easy to check that $S = \{(\infty, 0), (\infty, \infty')b, c\}$ behaves as required. (Namely, we can first obtain $(\infty', 0) = (\infty, 0)^{(\infty,\infty')b}$, $(\infty, \infty') = (\infty, 0)^{(\infty', 0)}$, and b as words of length at most 8 in S, and then as above obtain the transpositions (∞', t) for each $t \in \mathbb{Z}_{n-2}$.)

The same idea works for A_n as well, if sufficient care is taken to deal only with even permutations.

In order to decrease from 3 to 2 generators, we would like to proceed as follows. Assume once again that $n-1$ is odd. Note that b fixes 0, so that $((\infty, 0)b)^2 = b^2$. If $|b|$ happens to be both odd and $O(\log n)$, then $(\infty, 0)$ will be a power of $(\infty, 0)b$ of length $O(\log n)$. In this situation, we would be able to proceed exactly as before—or rather, we would use $S = \{(\infty, 0)b^{\frac{1}{2}}, c\}$, where $\frac{1}{2}$ represents $\frac{1}{2}(|b|+1)$.

Unfortunately, there is no reason to expect either that $|b|$ is odd or that it is small. Therefore, some amount of effort will be used in order to obtain a situation in which these requirements (small and odd) are both met. This will be accomplished by means of some bookkeeping. (N.B. Some of the strange constants in the following argument can be decreased. They are designed to work not only for S_n, but also below for A_n as well.)

Proof of (2.1). We may assume that $n \geqslant 2^{11}$. Let $l \geqslant 7$ be an integer such that $(6, l) = 1$ and $2^{l+10} \geqslant n \geqslant 2^{l+4}$. Partition the n-set X into 13 subsets $X_1, X_2, \ldots, X_{12}, E$ such that $|X_i| = 2^l - 1$ for each i. Note that l has been chosen so that $|E| > 0$ and $100 + |E|/100 < |X_2 \cup \cdots \cup X_{12}|$. Let ∞ denote a point of E.

Identify X_1 with $\mathbb{Z}_{2^l-1}$. In particular, $0 \in X_1 \subset X$. Start with the permutations $b_1: x \mapsto 2x$ and $c_1: x \mapsto 2x+1$ of X_1, both of which have order l—where l has been constructed so as to be *both odd and* $O(\log n)$. (Since the orbit of 1 under $\langle b_1\rangle$ has length l, it is easy to see that b_1 has order l. That c_1 also has order l follows from the fact that it is the conjugate of b_1 by the permutation $x \mapsto x-1$.)

Now define $\tilde{b}_1$ to be such that $(\tilde{b}_1)^{12} = b_1$ on X_1 and $\tilde{b}_1 = 1$ on $X - X_1$. (Recall that the order l of b_1 is relatively prime to 12.) Also, let f be the product of pairwise disjoint 101-cycles the supports of which are in $(E\text{-}\{\infty\}) \cup X_2 \cup \cdots \cup X_{12}$ and cover $E\text{-}\{\infty\}$. (Since $100 + |E|/100 < |X_2 \cup \cdots \cup X_{12}|$, such an f can be obtained as the product of $[|E|/100]$ or $[|E|/100] + 1$ cycles, all but at most one of which use 100 points of E.)

The desired permutations b and c are as follows:

$$b = (\infty, 0) f \tilde{b}_1,$$

and

c induces the 12-cycle $(X_1, X_2, \ldots, X_{12})$ on the X_i,
$c^{12} = c_1$ on X_1, and $c = 1$ on E.

Note that $\langle b^{12}, c^{12}\rangle$, restricted to X_1, is the same sort of group as the one called '$\langle b, c\rangle$' in the remarks preceding this proof. (For, $f = 1$ on X_1.)

Let $S = \{b, c\}$. *We claim that every element of* S_n *has* S*-length* $O(n \log n)$. It suffices to show that every transposition (∞, z), $z \in X\text{-}\{\infty\}$, has length $O(\log n)$.

First note that $b^{101l} = (\infty, 0)$ since $101l$ is odd, and hence $(\infty, 0)$ has length $O(\log n)$. Conjugating by elements of $\langle b^{12}, c^{12}\rangle$ we find (via Horner's rule) that each transposition (∞, x_1), $x_1 \in X_1$, has length $O(\log n)$. Conjugating by c we obtain the same for all transpositions (∞, x), $x \in X_2 \cup \cdots \cup X_{12}$. Finally, conjugation by b^i for $1 \leqslant i \leqslant 100$ produces the transpositions (∞, e), $e \in E\text{-}\{\infty\}$. □

It is not at all clear that one can deduce the A_n case from the S_n one. However, some minor modifications of the above argument produce that result:

THEOREM 2.2. *A_n has a set of 2 generators with respect to which the diameter is $O(n \log n)$.*

PROOF. Use the same l, $X_1, X_2, \ldots, X_{12}$, E, as before. Note that $|E| \geqslant 2$, and this time let ∞ and ∞' denote distinct points of E. Let $\bar{b}_1$ be as before, and let f be as before, except that this time the support of f is in $(E\text{-}\{\infty, \infty'\}) \cup X_2 \cup \cdots \cup X_{12}$ and covers $E\text{-}\{\infty, \infty'\}$.

Now define b and c as follows:

$$b = (\infty, \infty', 0) f \bar{b}_1$$

and

c induces the 12-cycle $(X_1, X_2, \ldots, X_{12})$ on the X_i, $c^{12} = c_1$ on X_1, $c = 1$ on $E\text{-}\{\infty, \infty'\}$, and c interchanges ∞ and ∞'.

We claim that $S = \{b, c\}$ behaves as required. First note that $b, c \in A_n$. (Namely, $|b|$ is odd, while the restriction of c to $X_1 \cup \cdots \cup X_{12}$ is an odd permutation.) Also, $b^{101l} = (\infty, \infty', 0)^{\pm 1}$ (since $101l \not\equiv 0 (\operatorname{mod} 3)$), so that $(\infty, \infty', 0)$ has length $O(\log n)$. It suffices to show that each 3-cycle of the form (∞, ∞', z), $z \in X\text{-}\{\infty, \infty'\}$, has length $O(\log n)$. This is proved exactly as in (2.1): first we obtain all (∞, ∞', x_1), $x_1 \in X_1$, then all (∞, ∞', x), $x \in X_2 \cup \cdots \cup X_{12}$, and finally all (∞, ∞', e), $e \in E\text{-}\{\infty, \infty'\}$. □

REMARKS. (1) Note that there are $O(n \log n)$ algorithms implicit in the above proofs, enabling one to write any given element of S_n or A_n as a product of members of $S \cup S^{-1}$.

(2) The Bubble Sort generators $t = (1, 2)$ and $s = (1, 2, \ldots, n)$ for S_n produce diameter $O(n^2)$, a fact that is needed later (e.g., in (2.4)). In fact, the diameter is $\theta(n^2)$. This can be proved by considering the permutation $x \mapsto n + 1 - x$. Namely, the cyclic order of $1, 2, \ldots, n$ induces a cyclic order on each unordered triple from $\{1, 2, \ldots, n\}$. Note that s preserves the cyclic order of each triple, while t changes the cyclic order of only $n - 2$ triples. Therefore, any representation of the permutation $x \mapsto n + 1 - x$ as a word in $s^{\pm 1}$ and t must contain at least $\binom{n}{3}/(n-2) = \theta(n^2)$ occurrences of t.

The remainder of this section is needed only for the proof of the main Theorem (1.1) in the cases of orthogonal, symplectic and unitary groups, and can therefore be omitted by readers primarily interested in the alternating or $PSL(n, q)$ cases of that theorem. First, we will need to describe the Weyl groups of types B_l and D_l, which will be denoted by $W(B_l)$ and $W(D_l)$, respectively.

Consider the l-sets $X = (1, \ldots, l\}$ and $X' = \{1', \ldots, l'\}$. Then $W(B_l)$ is the group of permutations of $X \cup X'$ preserving the partition $\bar{X} = \{\{x, x'\} \mid x \in X\}$. Each such permutation induces a permutation of $\bar{X}$, all of S_l being induced, and the kernel of the homomorphism is just $\mathbb{Z}_2^l$. Thus, $W(B_l)$ can be written $W(B_l) = \mathbb{Z}_2^l \rtimes S_l$, where S_l consists of the permutations of $X \cup X'$ obtained by extending permutations of X in the obvious manner.

There is a natural subgroup $\mathbb{Z}_2^{l-1}$ of our kernel consisting of all even permutations. With S_l as above, $W(D_l)$ is defined as $W(D_l) = \mathbb{Z}_2^{l-1} \rtimes S_l$; alternatively, $W(D_l) = W(B_l) \cap A_{2l}$. The groups $W(B_l)$ and $W(D_l)$ are groups generated by reflections in $\mathbb{R}^l$. In the present notation, these reflections are the following permutations for all distinct i, j: $(i, j)(i', j')$, $(i, j')(i', j)$, and in addition (i, i') in the case of $W(B_l)$. For a further discussion of these groups, see Section 7, Step (5).

Now write

$$
\begin{aligned}
&s=(1,\ldots,l)(1',\ldots,l'), && \text{and then let}\\
(2.3)\qquad &S=\{(1,2)(1',2'),\, s,\, (l,l')\} && \text{for } W(B_l), \text{ and}\\
&S=\{(1,2)(1',2'),\, s,\, (1,2')(1',2)\} && \text{for } W(D_l).
\end{aligned}
$$

Later we will need the following

LEMMA 2.4. *For the above* 3*-element sets S, $W(B_l)$ and $W(D_l)$ have S-diameter $O(l^2)$.*

PROOF. This is straightforward. For example, consider the case $W(D_l)$. Every element of S_l has length $O(l^2)$, by Bubble Sort. Since $W(D_l)=\mathbb{Z}_2^{l-1}S_l$ it suffices to show that each element of $\mathbb{Z}_2^{l-1}$ has S-length $O(l^2)$. Note that $(1,2)(1',2')\cdot(1,2')(1',2)=(1,1')(2,2')\in\mathbb{Z}_2^{l-1}$. By conjugating this by the powers of s we see that the $l-1$ permutations $(i,i')(i+1,(i+1)')$ with $1\leqslant i\leqslant l-1$ have length $O(l)$. These form a basis of the $\mathbb{Z}_2$-space $\mathbb{Z}_2^{l-1}$, so that every element of $\mathbb{Z}_2^{l-1}$ has length $O(l)$ in these $l-1$ generators. Thus, every element of $\mathbb{Z}_2^{l-1}$ has S-length $O(l^2)$. □

REMARK. It is not difficult to imitate the proof of (2.1) in order to obtain 2-element subsets of $G=W(B_l)$ or $W(D_l)$ with respect to which the diameter is $O(\log|G|)=O(l\log l)$. However, the above generators are the ones that will arise later: they occur naturally within the context of Weyl groups of groups of Lie type.

3. *PSL*(2, *q*)

In the next two sections we will prove (1.1) for the groups $PSL(n,q)$. The proof breaks up into two separate situations, requiring entirely different methods, according to whether $n=2$ or $n\geqslant 3$. The arguments used are essentially the same as those that will be used in the case of all of the remaining groups of Lie type (Section 5–7). We have separated them out for the case $PSL(n,q)$ since they are easier to understand and require no background beyond linear algebra.

Let $G=PSL(2,q)$ or $SL(2,q)$ with q a power of a prime p, where we will write elements of $PSL(2,q)$ as matrices mod ±I. Write

$$x(t)=\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix} \quad\text{and}\quad h(b)=\begin{pmatrix}b^{-1} & 0\\ 0 & b\end{pmatrix} \quad \text{for } b\neq 0,\ t\in\mathbb{F}_q, \text{ and } r=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}.$$

Then $x(t+u)=x(t)x(u)$ and $x(t)^{h(b)}=x(tb^2)$ for all $b\neq 0$, t, $u\in\mathbb{F}_q$. Also, $H=\{h(b)\mid b\neq 0\}$ is a cyclic group of order $q-1$ or $\frac{1}{2}(q-1)$ (the order is $q-1$ except when $G=PSL(2,q)$ with q odd).

THEOREM 3.1. Let $G=PSL(2,q)$ *or* $SL(2,q)$.

(i) *If q is an odd prime then G has diameter $O(\log|G|)$ with respect to $S=\{x(1),h(\frac{1}{2})r\}$.*

(ii) *For any q, if θ is a primitive element of $\mathbb{F}_q$ as an extension of the prime field $\mathbb{F}_p$, then G has diameter $O(\log|G|)$ with respect to the set*

$$S=\{x(1),h(\tfrac{1}{2})r,h(\theta)\}\ \text{if } q \text{ is odd},$$

and

$$S=\{x(1),r,h(\theta)\}\ \text{if } q \text{ is even}.$$

Proof. If $ad-bc=1$ then a straightforward calculation yields that, for $c \neq 0$,

$$g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=x(-c^{-1}+ac^{-1})x(-c)^r x(-c^{-1}+dc^{-1}). \tag{3.2}$$

In case $c=0$ use rg instead of g. This reduces the proof to showing that the length of each $x(a)$, $a \in \mathbb{F}_q$, is small with respect to the given set S.

Define $\theta \in \mathbb{F}_q$ as follows. If $q=p$ is an odd prime write $\theta=2$. If $q>p$ let θ be as in (ii). In either case, $\mathbb{F}_q=\mathbb{F}_p(\theta^2)$. Every element $t \in \mathbb{F}_q$ can be written in the form

$$t=\sum_0^m a_i\theta^{2i}=(\cdots(a_m\theta^2+a_{m-1})\theta^2+\cdots)\theta^2+a_0$$

(the second equality is Horner's rule once again), where either

$q=p$, $m+1 \leqslant \frac{1}{2}\log q$, and $a_i \in \{0, 1, 2, 3\}$ (base 4 representation of t), or
$q>p$, $m+1 \leqslant \log_p q$, and $a_i \in \mathbb{F}_p$.

Case $q=p$. We may assume that $p>2$ (since $SL(2, 2)$ has order 6 and is generated by $x(1)$ and r). Write $r'=h(\frac{1}{2})r \in S$. By matrix multiplication, $h(2)^{-1}=x(1)^{-2}(x(1)^2)^{r'}x(1)(x(1)^{-4})^{r'}$ has length $\leqslant 13$. 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 $x(a_i)$ has length $\leqslant 3$, while $h(2)$ has length $\leqslant 13$. Thus $x(t)$ has length $O(\log p)$.

By (3.2), each element of G has length $O(\log p)=O(\log|G|)$. This proves (i) (and, of course, the case $p=2$ of (ii)).

Case $q>p$. As above, each $x(t)$ is a word

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

in $m+1$ elements $x(a)$, $a \in \mathbb{F}_p$, and $2m$ elements $h(\theta)^{\pm 1}$. We just saw that each $x(a)$ has S-length $O(\log p)$. Thus, each $x(t)$ has length $m \cdot O(\log p)=O(\log q)$.

By (3.2), each element of G has length $O(\log q)=O(\log|G|)$. □

Remarks. (1) By crudely counting the lengths in the above arguments, it is easy to check that the diameters are $\leqslant 45\log|G|$ in (i) and $\leqslant 135\log|G|$ in (ii).
(2) There is an algorithm (cf. Section 1) implicit in the above proof.
(3) There is an alternative to the use of Horner's rule, which will be needed later in Sections 4 and 7 when polynomials will not be available. Namely, with t as above we can first write

$$x(t)=\prod_{i=0}^m x(a_i)^{h(2)^i},$$

and then observe that the cancellations of the form $h(2)^ih(2)^{-(i+1)}=h(2)^{-1}$ imply that the above product has S-length at most $O(m)+(m+1)\cdot$(sum of the lengths of the $x(a_i)$). That is, these cancellations let us avoid the occurrence of the sum of the lengths of the $h(2)^i$.
(4) We do not know any 2-element set S generating $PSL(2, q)$ with respect to which the diameter is $O(\log q)$. This is a major obstacle to decreasing the '7' in (1.1).

4. *PSL(n, q)*

We turn next to the groups $G=PSL\ (n, q)$ for $n \geqslant 3$. In this case we will introduce the standard Lie notation used later in the general case (cf. Section 5). By abuse of notation, we will regard G as consisting of $n \times n$ matrices. (In fact, we will actually be handling the case of $SL(n, q)$.)

For $1 \leqslant i < j \leqslant n$, let X_{ij} be the group of matrices with 1's on the diagonal, an arbitrary (i, j)-entry, and 0's elsewhere. Then X_{ij} is isomorphic to the additive group $\mathbb{F}_q^+$ of $\mathbb{F}_q$. Moreover,

$$U := \langle X_{ij} \mid 1 \leqslant i < j \leqslant n \rangle$$

is a Sylow p-subgroup of G, and $U = \prod_{i<j} X_{ij}$ with the $\frac{1}{2}n(n-1)$ factors written in any order.

If $e_1, \ldots, e_n$ is the standard basis of $\mathbb{F}_q^n$, for $1 \leqslant i < n$ let r_i be the matrix of the transformation sending $e_i \rightarrow e_{i+1} \rightarrow -e_i$ and fixing all other e_j. Also, for $1 \leqslant i \leqslant n-1$ let $h_i(t) = \mathrm{diag}(1, \ldots, 1, t^{-1}, t, 1, \ldots, 1)$ for $t \in \mathbb{F}_q^*$, with t^{-1} as the ith diagonal entry. If we write $H_i = \langle h_i(t) \mid t \in \mathbb{F}_q^* \rangle$ for $1 \leqslant 1 \leqslant n-1$, then

$$H := \prod_i H_i$$

is the group of all diagonal matrices. Also,

$$L_{i,i+1} := \langle X_{i,i+1}, r_i \rangle \cong SL(2, q) \qquad \text{and} \qquad L_{i,i+1} \cap H = H_i.$$

Moreover, the group B of all upper triangular matrices is $B = UH \rhd U$, while

$$N := \langle H, r_i \mid 1 \leqslant 1 < n \rangle$$

is the group of all monomial matrices and satisfies $N/H \cong S_n$ with the r_i behaving as the 'adjacent' transpositions $(i, i+1)$. We also have

$$G = BNB \qquad \text{(Bruhat decomposition)}.$$

Proposition 4.1. *$G = PSL(n, q)$ has a set of 4 generators with respect to which the diameter is $O(\log |G|)$.*

Proof. The set S will consist of the following:

an element s of N projecting onto an n-cycle of $N/H \cong S_n$,

and

the 3-element generating set for L_{12} given in (3.1ii).

Note that one of the elements $r' = h(\frac{1}{2})r_1$ or r_1 of that 3-element generating set for L_{12} projects onto $(1, 2)$. In particular, if we choose s so that it projects onto the n-cycle $(1, \ldots, n)$ then $z := sr'$ projects onto the $n-1$-cycle $(2, \ldots, n)$.

First we will show that every element of U has S-length $O(\log(|G|)$. Order the groups X_{ij}, $i < j$, in such a way that

$$U = \prod_{i=1}^{n} \prod_{k=0}^{n-i-1} X_{i,i+1+k}.$$

Then $U \subset YY^sY^{s^2} \cdots Y^{s^{n-1}}$ where $Y := X_{12}X_{12}^{z}X_{12}^{z^2} \cdots X_{12}^{z^{n-2}}$.

Note that there are cancellations occurring in the above products, since $s^k(s^{k+1})^{-1} = s^{-1}$ and $z^k(z^{k+1})^{-1} = z^{-1}$. Each element of X_{12} has length $O(\log q)$ in view of the definition of S in terms of (3.1ii). Consequently, each element of Y has length $O(n \cdot \log q)$, and each element of U has length $O(n \cdot n \log q) = O(\log |G|)$.

Next, consider the abelian group $H = \prod_i H_i$. Recall that each element of H_1 has length $O(\log q)$. By definition, $H_i = (H_1)^{s^i}$. It follows that each element of H has length $O(n \log q)$. (N.B. Again there are cancellations of the form $s^i(s^{i+1})^{-1} = s^{-1}$, but these are not needed for the proof of (4.1).)

Consequently, each element of $B = UH$ has length $O(\log |G|)$.

On the other hand, $G = BNB$ by the Bruhat decomposition. Here, $G = BNB = UHNHU = UNU$. We have available the Bubble Sort generators $Hr' = Hr_1$ and Hs of N/H. Thus, every coset Hg, $g \in N$, has a coset representative g of S-length $O(n^2)$. Consequently, each element of G has length $O(\log |G|)$. □

5. Groups of Lie Type: Notation

The remainder of this paper is concerned with finite groups of Lie type. This section summarizes many of the basic properties of such groups that we will need (cf. [7]).

Let G be a finite simple group of Lie type of characteristic p and rank l. We will use the following detailed but standard notation:

- Φ the root system of G (for unitary groups we will let Φ have type B_l)
- $\alpha_1, \ldots, \alpha_l$ the simple roots
- Φ^+ the set of positive roots
- W the Weyl group, so that W has at most 2 orbits on Φ
- X_α the root group associated with the root α, where with $(X_\alpha)^w = X_{\alpha^w}$ for $\alpha \in \Phi$, $w \in W$
- U the Sylow p-subgroup U of G such that $U = \prod_{\alpha \in \Phi^+} X_\alpha$ (with the factors in any order)
- $B = N_G(U)$ a Borel subgroup
- H a complement to U in B, so that $B = U \rtimes H$
- N the usual group of BN-pair frame, so that $N \triangleright H$, $W = N/H$ and $G = BNB$ (Bruhat decomposition)
- L_α the group $\langle X_\alpha, X_{-\alpha} \rangle$, where α is any root, so that

$$H = \prod_i H \cap L_{\alpha_i}$$

and

$$W = \langle N \cap L_{\alpha_i} \mid 1 \leqslant i \leqslant l \rangle H/H$$

- q the power of p appearing in the usual 'name' for G

If $l \geqslant 2$ then, for each α,

$$L_\alpha \cong PSL(2, q^\varepsilon),\ SL(2, q^\varepsilon),\ PSU(3, q) \text{ or } SU(3, q) \text{ for } \varepsilon = 1, 2 \text{ or } 3,$$

except that L_α can be $Sz(q)$ for one W-orbit of roots α when $G = {}^2F_4(q)$.

Remark. Not every group of Lie type is simple. However, there are very few exceptions (namely, $PSL(2, 2)$, $PSL(2, 3)$, $PSp(4, 2)$, $G_2(2)$ and ${}^2F_4(2)$ [7, p. 268]), and these can be ignored.

6. Groups of Rank 1

Let G be as in Section 5. In this section we will prove (1.1) in the case of groups of rank 1. These are precisely the groups $PSL(2, q)$, $PSU(3, q)$, $SU(3, q)$, $Sz(q)$ and ${}^2G_2(q)$ [7]. The cases $PSL(2, q)$ and $SL(2, q)$ were dealt with in Section 3.

PROPOSITION 6.1. *(i) If G is $PSU(3, q)$, $SU(3, q)$ or $Sz(q)$ then there is a set S of 3 generators, including a generator of the cyclic group H and an involution in $N - H$, with respect to which G has dimater $O(\log q)$.*

(ii) There is a set of 4 generators of $G = {}^2G_2(q)$ with respect to which G has diameter $O(\log q)$.

We begin with two lemmas.

LEMMA 6.2. *If S is a subset of G not contained in B and such that every element of U has S-length $\leq C \log q$, then every element of G has S-length $O(\log q)$.*

PROOF. Let $s \in S - B$. Since U is transitive on $U^G - \{U\}$, every p-element of G lies in U or U^{su} for some $u \in U$, and hence has S-length $O(\log q)$. Since $G = BNB = UHNHU = UNU$, we only need deal with N.

Note that, every case, $N/Z(G)$ is a dihedral group, so that each element of $H/Z(G)$ is the product of 2 involutions of $G/Z(G)$. Also, if $Z(G) \neq 1$ then any non-trivial element of $Z(G)$ is the cube of an element of G (this is relevent only when $G = SU(3, q)$, with $q \equiv -1 \pmod 3$)). Thus, it is only necessary to show that all involutions of $G/Z(G)$ have length $O(\log q)$. In particular, we may now assume that $Z(G) = 1$.

For each of the groups G, all involutions are conjugate. Some involution can be written uvu' with u, $u' \in U$ and $v \in U^s$ (by [19] or a direct calculation). Hence, each involution can be written as the product of three p-elements, and so has length $O(\log q)$. □

LEMMA 6.3. *Let $\mu \in \mathbb{F}_q$ be such that $\mathbb{F}_q = \mathbb{F}_p(\mu)$ and such that the multiplicative group $\langle \mu \rangle$ contains $\mathbb{F}_p^*$. Consider the group $A = \mathbb{F}_q^+ \rtimes M$ of 1-dimensional affine transformations $x \mapsto mx + a$, where $m \in \langle \mu \rangle$, $a \in \mathbb{F}_q$. Fix $b \in \mathbb{F}_q^*$. Let A_0 consist of those transformations with $m = 1$ and $a \in b\mathbb{F}_p$, and let h be the element $x \mapsto \mu x$ of A. Then every element $x \mapsto x + \alpha$ of A can be written as a word of length $\leq 3 \log_p q$ in $A_0 \cup \{h\}$.*

PROOF. By hypothesis, if $q = p^e$ then every element $t \in \mathbb{F}_q$ can be written in the form

$$t = \sum_0^{e-1} ba_i\mu^i = (\cdots(ba_{e-1}\mu + ba_{e-2})\mu + \cdots)\mu + ba_0 \qquad \text{(Horner's rule)}$$

with $a_i \in \mathbb{F}_p$.

By hypothesis, A_0 is the group of all additions $f: x \mapsto x + ba$ by elements $ba \in b\mathbb{F}_p$. On the other hand, h is just multiplication by μ, so that $f^h: x \mapsto x + ba\mu$. Consequently, the above expression for t implies that the element $x \mapsto x + t$ of A has length $\leq 3e$ in $A_0 \cup \{h\}$. □

PROOF OF (6.1). In view of (6.2), we will focus on elements of U. Our set S will consist of the following:

a suitable nontrivial element $u \in U$,
a suitable element $r \in N - H$, and
a generator h of H.

(In the case ${}^2G_2(q)$ a fourth element will be used, taken from U.)

We will deal with the various groups G on a case-by-case basis.

Case $G = Sz(q)$, where $q = 2^{2e+1}$. Here U consists of all ordered pairs $(a, b) \in \mathbb{F}_q^2$, with a suitable multiplication. Moreover, $Z(U) = U'$ consists of the pairs $(a, 0)$, and

$Z(U) \cong U/Z(U) \cong \mathbb{F}_q^+$. We have $H \cong \mathbb{F}_q^*$, and with this identification each $\gamma \in H$ acts on U via $(a, b) \mapsto (a\gamma, b\gamma^{\sigma+1})$, where $\sigma = 2^e$ [18, 19].

The group $Sz(2)$ has order 20, and is contained in G (with 'co-ordinates' in $Sz(2) \cap U$ taken from $\mathbb{F}_2$). The element $u = (0, 1)$ has order 4, and $u^2 \in Z(U)$. If r is any involution in $Sz(2) - \langle u \rangle$ then $\langle u, r \rangle = Sz(2)$.

Set $S = \{u, r, h\rangle$.

We may assume that $e > 0$. Then (6.3) can be applied in the two cases $A = Z(U)H$ or $(U/Z(U))H$ (with $A_0 = \langle u^2 \rangle$ and $\langle Z(U)u \rangle$, respectively) in order to see that every element of U has length $O(\log q)$ in our generators.

Cases PSU(3, *q*) *and SU*(3, *q*). This time U consists of all ordered pairs $(a, \alpha) \in \mathbb{F}_q \times \mathbb{F}_{q^2}$ with a suitable multiplication, and $Z(U) = U'$ consists of the pairs $(a, 0)$, $U' = Z(U) \cong \mathbb{F}_q^+$, where $U/Z(U) \cong \mathbb{F}_{q^2}^+$. Moreover, $H/Z(G)$ is isomorphic to a subgroup of $\mathbb{F}_{q^2}^*$ of index $(3, q+1)$, and with this identification each $\gamma \in H/Z(G)$ acts on U via $(a, \alpha) \mapsto (a\gamma^{q+1}, \alpha\gamma^q)$. (Here $|Z(G)|$ is either 1 or $(3, q+1)$.)

Let h be a generator of H.

Let u be any element of $U - Z(U)$. Set $u_1 = u^h u^{-1}$. Then u_1 is a nontrivial element of $U' = Z(U)$.

There is a subgroup $G_0 \cong SL(2, q)$ generated by 2 conjugates of $Z(U)$, normalized by H, and such that $B \cap G_0$ is a Borel subgroup of G_0. Write $H_0 = H \cap G_0$, so that $B \cap G_0 = Z(U)H_0$.

Let $G_1 \leqslant G_0$ be such that $G_1 \cong SL(2, p)$ and $B \cap G_1$ is a Borel subgroup of G_1. Let $\{u_1, r\}$ be a 2-element generating set of G_1 with respect to which the diameter is $O(\log p)$: use (3.1), identifying $u_1 \in U \cap G_1 \leqslant U \cap G_0$ with $x(1)$ and letting r have order 2 (mod $Z(G_1)$) (namely, if $p = 2$ use any element r in $G_1 - \langle u_1 \rangle$ of order 2, and if $p > 2$ use the element called $h(\frac{1}{2})r$ in (3.1i)).

Set $S = \{u, r, h\}$. We claim that S behaves as required.

First note that every element of G_0 has $\{u_1, r, h\}$-length $O(\log q)$. This is proved by repeating the argument used for the case $SL(2, q)$ already considered in (3.1). Namely, since H normalizes G_0 that argument applies essentially verbatim: $x(t)^h = x(t\gamma^{q+1})$ for all $t \in \mathbb{F}_q$ and some γ generating $\mathbb{F}_{q^2}$. (N.B. We started with $\langle u_1, r \rangle = G_1$ and h. We did not have H_0 at our disposal: a generator of this group is a 'large' power of h, and hence is inaccessible until after we have repeated the argument in (3.1).)

In particular, every element of H_0 has $\{u_1, r, h\}$-length $O(\log q)$, and hence has S-length $O(\log q)$ since $u_1 = u^h u^{-1}$ has length $\leqslant 4$.

Next note that all elements in $\{u^{h'} \mid h' \in H_0\}$ or $\{u^{h'} \mid h' \in H_0\}^h$ also have length $O(\log q)$ with respect to S. Each of the subsets $Z(U)\{u^{h'} \mid h' \in H_0\}$ and $Z(U)\{u^{h'} \mid h' \in H_0\}^h$ of $U/Z(U)$ consists of all the nonzero vectors in a 1-space when $U/Z(U)$ is viewed as a 2-dimensional vector space over $\mathbb{F}_q$ (recall that $\beta \in H$ acts on U be sending (a, α) to $(a\beta^{q+1}, \alpha\beta^q)$). Moreover, these are distinct 1-spaces, and hence span $U/Z(U)$. Thus, every element of $U/Z(U)$ either lies in $\{u^{h'} \mid h' \in H_0\}$ or $\{u^{h'} \mid h' \in H_0\}^h$, or else is a product of 2 elements, one from each of the sets. Since we already know that each element of $Z(U)$ has S-length $O(\log q)$, it follows that the same is true of each element of U, as required in (6.2).

Case ${}^2G_2(q)$, *where* $q = 3^{2e+1}$. This time U consists of all ordered triples $(a, b, c) \in \mathbb{F}_q^3$, with a suitable multiplication [19]. Moreover, $Z(U)$ consists of all of the triples $(a, 0, 0)$, U' consists of all of the triples $(a, b, 0)$, and $Z(U) \cong U'/Z(U) \cong U/U' \cong \mathbb{F}_q^+$. This time $H \cong \mathbb{F}_q^*$, and with this identification each $\gamma \in H$ acts on U via $(a, b, c) \mapsto (a\gamma, b\gamma^{\sigma+1}, c\gamma^{\sigma+2})$, where $\sigma = 3^e$ [19, 20].

There are subgroups G_0 and G_1 of G with the following properties [20];

$G_0 = {}^2G_2(3) \cong P\Gamma L(2, 8)$;
$G_1 = PSL(2, q)$;
$G_0 \cap G_1 = PSL(2, 3)$;
$B \cap G_i$ is a Borel subgroup of G_i for $i = 0, 1$;
$U \cap G_0$ consists of those triples (a, b, c) belonging to $\mathbb{F}_3^3$;
$U \cap (G_0)'$ is cyclic of order 9 and $U \cap (G_0)' \cap G_1 = 1$.

Let S consist of the following elements:

a generator u_0 of $U \cap (G_0)'$;
u and r taken from $G_0 \cap G_1$ and generating that group; and
a generator h of H.

It is easy to check that $G_0 = \langle u_0, u, r\rangle$.

Every element of $U \cap G_0$ has S-length $O(1)$, where $U \cap G_0$ has elements projecting nontrivially into each of the groups U/U', $U'/Z(U)$ and $Z(U)$. Consequently, we can apply (6.3) to the three groups $(U/U')H$, $(U'/Z(U))H$ and $Z(U)H$ (letting A_0 be the group generated by a nontrivial element of $(U \cap G_0)U'/U'$, $(U' \cap G_0)Z(U)/Z(U)$, or $Z(U) \cap G_0$, respectively). Then all elements of U have S-length $O(\log q)$, as required. □

REMARK. We do not know any 2-element set S generating the above rank 1 groups with respect to which the diameter is $O(\log q)$. As in Section 3, this is major obstacle to decreasing the '7' in (1.1).

7. HIGHER RANK

In this section we will complete the proof of (1.1) by handling the groups of Lie type of rank at least 2.

PROOF OF (1.1). Let G be as in Section 5. By Section 6 we may assume that G has rank $l \geq 2$.

In view of (4.1), we may assume that G is not $PSL(n, q)$. Our argument is, however, just an elaboration of that in Section 4.

We will proceed in several steps. Our notation is that of Section 5.

(1) Let α_1 and α_2 be distinct simple roots. They will be specified more carefully when additional notation has been introduced.

Abbreviate $X_j = X_{\alpha_j}$ and $L_j = L_{\alpha_j}$ for $j = 1, 2$.

Let E_j be a set of 2 or 3 elements generating L_j obtained as in (3.1) or (6.1).

Note that one of the elements of E_j projects mod H onto the element r_{α_j} of $N/H = W$. That element of E_j will also be called r_{α_j}.

(2) The desired set S consists of

E_j for $j = 1, 2$ (for suitably chosen α_j; see below), and
an element $s \in N$ that we will now define.

If G is not a classical group let $Hs \in N/H = W$ be the product of the l simple reflections ($Hs = r_{\alpha_1} \cdots r_{\alpha_l}$). In this case it is straightforward to check that α_1 and α_2 can be chosen so that $W = \langle r_{\alpha_1}, r_{\alpha_2}, Hs\rangle$ and $\Phi = \alpha_1^W \cup \alpha_2^W$.

If G is a classical group, then the Weyl group W of G is $W(B_l)$ or $W(D_l)$ in the notation of Section 2. (Namely, $W \cong W(B_l)$ when G is $PSp(2l, q)$, $P\Omega(2l+1, q)$, $P\Omega^-(2l+2, q)$, $PSU(2l, q)$ or $PSU(2l+1, q)$; and $W \cong W(D_l)$ when G is $P\Omega^+(2l, q)$.) Then s will taken to be any element of N projecting mod H onto the l-cycle called s in

(2.3), while α_1 and α_2 will be chosen so that r_{α_1} and r_{α_2} are the remaining two generators appearing in (2.3). Then $W = \langle r_{\alpha_1}, r_{\alpha_2}, Hs\rangle$ and $\Phi = \alpha_1^W \cup \alpha_2^W$ once again (see Step (5) below).

Note that $|E_j| = 3$ for $j = 1, 2$, so that $|S| \leqslant 3 + 3 + 1$.

By (2.4), every coset Hg $(g \in N)$ belonging to $W = \langle r_{\alpha_1}, r_{\alpha_2}, Hs\rangle$ has a coset representative g of S-length $O(l^2)$.

(3) In Steps (4)–(6) we will show that every element of U has S-length $O(\log |G|)$. Assuming this for the time being, we can complete the proof of (1.1).

Consider the abelian group $H = \prod_i (H \cap L_{\alpha_i})$. If $w \in W$ and $\beta \in \Phi$ then $(H \cap L_\beta)^w = H \cap L_{\beta^w}$. In particular, since $\Phi = \alpha_1^W \cup \alpha_2^W$ each group $H \cap L_{\alpha_i}$ is a conjugate of $H \cap L_j$ by an element of W for $j = 1$ of 2. In view of the choice of E_j, each element of $H \cap L_j$ has S-length $O(\log q)$. In particular, if G is not classical then $|W| = O(1)$ and hence each element of H has length $O(\log q)$. On the other hand, if G is classical then it is easy to check (see Step (5) below) that each α_i has the form $\alpha_1^{s^k}$ or α_2 with $0 \leqslant k \leqslant l-2$, and then each element of $H = \prod_i (H \cap L_{\alpha_i})$ again has length $O(l \log q)$.

Consequently, in view of our assumption about the lengths of the elements of U, each element of $B = UH$ has length $O(\log |G|)$.

On the other hand, $G = BNB$ by the Bruhat decomposition. By Step (3), every coset Hg $(g \in N)$ belonging to W has a coset representative g of S-length $O(l^2)$. Since $\log |G| = O(l^2 \log q)$, each element of G has length $O(\log |G|)$.

(4) It remains to deal with $U = \prod_{\alpha \in \Phi^+} X_\alpha$, where the factors can be written in any convenient order. Every root α has the form $\alpha = \alpha_j^w$ for $j = 1$ or 2 and some $w \in W$, and then $X_\alpha = (X_{\alpha_j})^w$.

In particular, if G is *not* a classical group then l and $|\Phi|$ are $O(1)$, so that each X_α consists of elements of length $O(\log q)$ and hence so does each element of U. This completes the proof when G is not classical.

(5) *From now on, G will be a classical group.* In order to imitate the argument in Section 4, we will need a description of the set Φ^+ of positive roots for each possible Φ (of type B_l, C_l or D_l). For Euclidean descriptions, see [7]. For our purposes, it suffices to describe Φ and Φ^+ in terms of the set $X \cup X'$ appearing in Section 2.

B_l, C_l:
Φ: $X \cup X'$ and all pairs $\{u, v\}$ with $u, v \in X \cup X'$ and $v \neq u$, $v \neq u'$ and $u \neq v'$
Φ^+: X and all pairs $\{x, y\}$ or $\{x, y'\}$ with $x, y \in X$ and $x < y$
$\alpha_1 = \{1, 2'\}$, $\alpha_2 = l \in X$; the remaining simple roots have the form $\{i, (i+1)'\}$; and the corresponding reflections are $(1,2)(1',2')$, (l, l'), and $(i, i+1)(i', (i+1)')$, respectively.

D_l:
Φ: all pairs $\{u, v\}$ with $u, v \in X \cup X'$ and $v \neq u$, $v \neq u'$ and $u \neq v'$
Φ^+: all pairs $\{x, y\}$ or $\{x, y'\}$ with $x, y \in X$ and $x < y$
$\alpha_1 = \{1, 2'\}$, $\alpha_2 = \{1, 2\}$; the remaining simple roots have the form $\{i, (i+1)'\}$; and the corresponding reflections are $(1,2)(1',2')$, $(1,2')(1',2)$, and $(i, i+1)(i', (i+1)')$, respectively.

(N.B. The difference between B_l and C_l concerns the lengths of roots, and these will not arise in the following arguments.) Note that the simple roots α_1 and α_2 are such that the corresponding reflections r_{α_1} and r_{α_2} behave exactly as in (2.3). Also note that the group generated by the permutation s appearing in (2.3) sends α_1 to every simple root other than α_2 (a fact that was needed in Step (3)).

(6) We will write $X_\alpha = X_x$, X_{xy} or $X_{xy'}$ when $\alpha = x$, $\{x, y\}$ or $\{x, y'\}$, respectively. Recall that the elements of $S \cap N$ induce elements of $N/H = W$ behaving as in (2.3) and (2.4).

Now we can proceed as in Section 4. Namely, write

$$U = \prod_{\alpha \in \Phi^+} X_\alpha = \prod_x \prod_{x<y} X_{xy} \prod_x \prod_{x<y} X_{xy'} \prod_x X_x \qquad \text{or} \qquad U = \prod_x \prod_{x<y} X_{xy} \prod_x \prod_{x<y} X_{xy'}$$

in the respective cases B_l (or C_l) or D_l.

Write $z := sr_{\alpha_1}$, which is just $(2, 3, \ldots, l)(2', 3', \ldots, l')$ viewed within W, $Y := X_{12} X_{12}^z X_{12}^{z^2} \cdots x_{12}^{z^{l-2}}$, and $Y' := X_{12'} X_{12'}^z X_{12'}^{z^2} \cdots X_{12'}^{z^{l-2}}$.

Case B_l (or C_l): We have

$$U \subset YY^s Y^{s^2} \cdots Y^{s^{l-1}} \cdot Y' Y'^s Y'^{s^2} \cdots Y'^{s^{l-1}} \cdot X_l X_l^s \cdots X_l^{s^{l-1}}.$$

Each element of $X_{\alpha_1} = X_{12'}$ has S-length $O(\log q)$ by the definition of E_1, and hence the same is true of each element of $X_{12} = X_{12'}^t$, where $t = r_{\alpha_2}^{s^2} = (2, 2')$. Due to cancellations of the form $z^k (z^{k+1})^{-1} = z^{-1}$ and $s^k (s^{k+1})^{-1} = s^{-1}$, it follows first that each element of Y or Y' has length $O(l \cdot \log q)$, and then that each element of U has length $O(l \cdot l \log q) = O(\log |G|)$.

Case D_l. This time $U \subset YY^s Y^{s^2} \cdots Y^{s^{l-1}} \cdot Y' Y'^s Y'^{s^2} \cdots Y'^{s^{l-1}}$, while $X_{12} = X_{\alpha_2}$. Once again, each element of U has length $l \cdot O(\log q) = O(\log |G|)$. □

Remark. Motivated by the arguments in this and the preceding section, we conjectured that every element g of G can be written as a product of two p-elements—and that, for 'most' g, the first of those elements can be chosen from the group U. This conjecture has now been proven by R. Steinberg. Unfortunately, this does not lead to a shorter—or essentially different—argument or set S.

8. Appendix: Eigenvalues and Diameter

In [2, (2.7)] it is shown that a connected k-regular graph $\mathscr{G}$ on N vertices has diameter $\leqslant 2[(k/\lambda_1)^{\frac{1}{2}} \log N]$, where $\lambda_1 = \lambda_1(\mathscr{G})$ is the smallest positive eigenvalue of the matrix $kI - A$ with A the adjacency matrix of $\mathscr{G}$. Thus, for a family of k-regular graphs, if λ_1 is bounded uniformly away from 0 then the graphs have diameter $O(\log N)$. By elaborating on the use in [12] of Kazhdan's Property (T) concerning the respresentations of Lie groups, the following is deduced in [2]. For a fixed $n \geqslant 3$, $PSL(n, p)$ has diameter $\leqslant C_n \log p$ with respect to the generating set $\{s, X_{12}(1)\}$ (compare the notation of Section 4); it is not known whether this diameter is $O(\log |PSL(n, p)|) = O(n^2 \log p)$. For the same two generators, we have the following in the case $n = 2$ (the proof is taken from a preliminary version of [10]):

Proposition 8.1. *For a prime p, $PSL(2, p)$ has diameter $O(\log p)$ with respect to*

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

Proof. The group $\Gamma = PSL(2, \mathbb{Z})$ acts on the upper half plane $\mathfrak{H} = \{x + iy \mid x, y \in \mathbb{R}, y > 0\}$, with fundamental domain $D = \{x + iy \mid -\frac{1}{2} \leqslant y \leqslant \frac{1}{2}, x^2 + y^2 \geqslant 1\}$. Note that S is the image mod p of the standard set (also called S) of generators $S = \{z \to z + 1, z \to -1/z\}$ of Γ. Let $M = \Gamma \backslash \mathfrak{H}$ be the quotient space, and let $M_p = \Gamma_p \backslash \mathfrak{H}$ be the quotient space with respect to the congruence subgroup $\Gamma_p := \operatorname{Ker}(\Gamma \to PSL(2, p))$. Then M_p is a finite-sheeted covering of M on which $PSL(2, p)$ acts with fundamental domain D_p, the image of D under the natural projection $\mathfrak{H} \to \Gamma_p \backslash \mathfrak{H}$.

The Cayley graph $\mathscr{G}(PSL(2,p),S)$ can be visualized on M_p in the following way. The vertices are the images gD_p of D_p under the elements of $g\in\Gamma$, and the domains gD_p and $g'D_p$ are joined if and only if they are adjacent (i.e., intersect in a curve).

Let Δ be the Laplacian operator of the manifold M_p, and let $\lambda_1(M_p)$ be its smallest positive eigenvalue [8]. In [5, 6] it is shown (in a more general situation) that there exists a constant $c_1>0$ such that $\lambda_1(M_p)\geqslant c_1$ for all p if, and only if, there is a constant $c_2>0$ such that $\lambda_1(\mathscr{G}(PSL(2,p),S))\geqslant c_2$ for all p. By [15], $\lambda_1(M_p)\geqslant 3/16$ (and it has been conjectured that $\lambda_1(M_p)\geqslant 1/4$). Therefore, $\lambda_1(\mathscr{G}(PSL(2,q),S))$ is bounded away from 0, and by the result from [2] mentioned at the beginning of this Appendix, diam $\mathscr{G}(PSL(2,p),S)=O(\log p)$. □

Remarks. (1) Note that the eigenvalue $\lambda_1(\mathscr{G}(PSL(2,p),S'))$ is bounded away from 0 for every set S' of generators of $PSL(2,\mathbb{Z})$ taken mod p.
(2) One can also show (again using [15]) that, for the generating set S given in (3.11), $\lambda_1(\mathscr{G}(PSL(2,p),S))$ is bounded away from 0.
(3) Using the reduction in [5] produces the crude upper bound diam $\mathscr{G}(PSL(2,p),S)\leqslant 500\log p$ for the trivalent graphs in (9.1).
(4) When $k=6$ and 5 is a square mod p, a 3-generator set S is given for $PSL(2,p)$ in [11] such that $\lambda_1(\mathscr{G}(PSL(2,p),S))\geqslant k-2\sqrt{k-1}$. Those k-regular graphs satisfying this optimal inequality are called 'Ramanujan graphs' in [10, 11]. It is also shown in [11] that diam $\mathscr{G}(PSL(2,p),S)<2\log_5 p+2$, which is better than the bound obtained using the eigenvalue bound [2]. Results essentially identical to some of those in [10, 11] have also been obtained in [13].

Finally, we remark that these eigenvalue estimates produce stronger information than the diameter concerning the graphs we have discussed in this section: they are (k,ε)-*expanders* with $\varepsilon=\frac{1}{2}\lambda_1/k$ [2, 10]. That is, they are k-regular graphs on N vertices such that, for each set A of $\leqslant\frac{1}{2}N$ vertices, at least $\varepsilon\,|A|$ vertices not in A are joined to vertices in A. From this definition it follows immediately that (for fixed k, and ε bounded from below), (k,ε)-expanders have diameter $O(\log N)$. In view of (1.1), this leads to the following:

Conjecture. There are k and $\varepsilon>0$ such that every finite nonabelian simple group G has a set S of k generators such that $\mathscr{G}(G,S)$ is a $(2k,\varepsilon)$-expander (or, equivalently, such that $\lambda_1(\mathscr{G}(G,S))$ is bounded away from 0; cf. [1]).

9. Appendix: Further Remarks on Diameters of Cayley Graphs

We have concentrated on finding a small, efficient set of generators for nonabelian finite simple groups. Other papers deal with the diameters of Cayley graphs with respect to arbitrary sets of generators of families of groups.

It is not difficult to show that any Cayley graph of an abelian group has diameter $>\frac{1}{2}(n^{\{1/|S|\}}-1)$. On the other hand, it has been conjectured [4] that all Cayley graphs of nonabelian finite simple groups are fairly good: more precisely, it was conjectured that there exists a constant C such that the diameter of any Cayley graph of any nonabelian finite simple group G is less than $(\log|G|)^C$. This conjecture is open even for the alternating groups; in fact, the upper bound $\exp(c(n\log n)^{\frac{1}{2}})$ is the best estimate known when $G=A_m$ [4]. It is even conceivable that 'most' pairs of generators of S_n or A_n produce diameter $O(n\log n)$. For the groups $PSL(2,p)$ we do not know generators for which the diameters are not $O(\log p)$.

In view of (1.1) and the preceding paragraph, it is natural to ask how the structure of G can force the diameter to be 'large' or 'small' with respect to a bounded number of generators. It is interesting to note that, without a size restriction on the number of generators, the structure of the group cannot make a significant difference. More precisely, a simple combinatorial argument is used in [3] to prove that every finite group G has a set of $s < \log |G| + \log \log |G| + 3$ generators $g_1, \ldots, g_s$ such that every member of G can be written as $g_1^{e_1} g_2^{e_2} \cdots g_s^{e_s}$, where each $e_i \in \{0, 1\}$. In particular, the resulting Cayley graph has diameter $\leqslant s$.

In conclusion, we remark that part of the motivation for constructing Cayley graphs of small diameter comes from applications to interconnection networks. Indeed, Cayley graphs have long been recognized as a source of effectively constructible networks of small diameter. Many authors have noted that the celebrated network of 'cube connected cycles' [14] is a Cayley graph of the wreathed product $Z_2 \, wr \, Z_m$. Sorting procedures have been associated with these same Cayley graphs (perfect shuffles [17]) and with Cayley graphs of the symmetric group (pancake graph [9]). Also, the expansion properties of the graphs in Section 8 have been used for network constructions [2, 10].

AKNOWLEDGEMENTS

We are grateful to N. Alon and B. Weiss, and to D. Kazhdan and M. Ben-Or, for helpful comments concerning the S_n and the $PSL(2, p)$ cases, respectively. Part of this work was done while the first and third authors were at the University of Chicago, and other parts were done while the second author visited the Hebrew University, ATT Bell Laboratories or Universität Bielefeld. The hospitality and support of these institutions are gratefully acknowledged. The research was also supported in part by NSF and BSF grants.

REFERENCES

1. N. Alon, Eigenvalues and expanders, *Combinatorica*, **6** (1986), 83–96.
2. N. Alon and V. D. Milman, λ_1, isoperimetric inequalities for graphs, and superconcentrators, *J. Comb. Theory. Ser. B*, **38** (1985), 73–88.
3. L. Babai and P. Erdös, Representation of group elements as short products, in *Theory and Practice of Combinatorics* (A. Rosa, G. Sabidussi and J. Turgeon, Eds), *Ann. Discr. Math.*, **12** (1982), 27–30.
4. L. Babai and A. Seress, On the diameter of Cayley graphs of symmetric groups, *J. Comb. Theory. Ser. A* (to appear).
5. R. Brooks, The spectral geometry of a tower of coverings, *J. Diff. Geom.*, **23** (1986), 97–107.
6. R. Brooks, Combinatorial problems in spectral geometry, in *Curvature and Topology of Riemannian Manifolds* (K. Shiohana, T. Sakai and T. Sunada, eds), pp. 14–32, Springer Lecture Notes in Mathematics 1201, 1986.
7. R. Carter, *Simple Groups of Lie Type*, John Wiley, Chichester, 1972.
8. I. Chavel, *Eigenvalues in Riemannian Geometry*, Academic Press, London, 1984.
9. W. H. Gates and C. H. Papadimitriou, Bounds for sorting by prefix reversal, *Disc. Math.*, **27** (1979), 47–57.
10. A. Lubotzky, R. Phillips and P. Sarnak, Explicit expanders and the Ramanujan conjecture, *18th Symp. Theory of Computation* 1986, 240–246.
11. A. Lubotzky, R. Phillips and P. Sarnak, Ramanujan graphs, *Combinatorica* **8** (1988) 261–277.
12. G. A. Margulis, Graphs without short cycles, *Combinatorica*, **2** (1982), 71–78.
13. G. A. Margulis, Arithmetic groups and graphs without short circuits (Russian; to appear).
14. F. Preparata and J. Vuillemin, The cube-connected cycles: a versatile network for parallel computation, *Commun. ACM*, **24** (1981), 300–309.
15. A. Selberg, On the estimation of Fourier coefficients of modular forms, *AMS Proc. Symp. Pure Math.*, **8** (1965), 1–15.

16. R. Steinberg, Generators for simple groups, *Can. J. Math.*, **14** (1962), 277–283.
17. H. S. Stone, Parallel processing with the perfect shuffle, *IEEE Trans. Comput.*, **C-20** (1971), 153–161.
18. M. Suzuki, On a class of doubly transitive groups, I. *Ann. Math.*, **75,** (1962), 105–145.
19. J. Tits, Les groupes simples de Suzuki et Ree, *Sém. Bouraki #210,* 1960.
20. H. N. Ward, On Ree's series of simple groups, *Trans. AMS,* **121** (1966), 62–89.
21. A. Weil, Sur les courbes algébriques et les variétés que s'en déduisent, *Act. Sci. Ind.*, **1041** (1948).

Received 7 August 1987 and in revised form 9 April 1989

L. Babai
Department of Algebra, Eötvös University, Budapest H-1088, Hungary

W. M. Kantor
Department of Mathematics, University of Oregon, Eugene, Oregon 97403, U.S.A.
and
A. Lubotzky
Institute of Mathematics, Hebrew University, Jerusalem, Israel