Some large trivalent graphs having small diameters
William M. Kantor*

This note concerns an improvement of a result of Babai–Kantor–Lubotzky [BKL]. In that paper it was shown that there is a constant C such that every nonabelian finite simple group G has a set S of 7 generators for which \( d(G,S) \leq C \log |G| \). Here, S was a carefully chosen generating set for G, and d(G,S) denotes the diameter of the corresponding undirected Cayley graph. This bound is best possible, since a simple count (the "Moore bound") shows that \( d(G,S)+1 \geq \log_2 |G| \).

In this note we will decrease |S| so as to have |S|=2 and \( |S \cup S^{-1}|=3 \) in case \( G=PSL(n,q) \) with \( n \geq 10 \):

**Theorem.** If \( n \geq 10 \) then there is a trivalent (undirected) Cayley graph for \( G=PSL(n,q) \) whose diameter is \( O(\log |G|) \).

Moreover, there is an algorithm which, when given \( g \in G \), finds a word in S representing g in \( O(\log |G|) \) steps (i.e., multiplications and inversions of elements of S). Actually, we will only need to assume that \( n \geq 8 \) when \( q \) is even. There are analogous results obtainable by similar arguments for all the finite simple groups of Lie type, provided that the ranks are not too small. Steinberg [Ste] obtained two generators for each finite group of Lie type; but his generators do not include an involution, and his argument does not produce the desired diameter bound.

**Proof.** Given a generating set S, the diameter \( d(G,S) \) of the corresponding Cayley graph can be interpreted group-theoretically as the maximum of the lengths of the elements of G as words in \( S \cup S^{-1} \). We will work inside of \( SL(n,q) \), where \( q \) is a power of a prime \( p \). In order to obtain a trivalent graph we will find a set \( S=\{s,g\} \) consisting of two matrices, one of which has order 2, such that the corresponding diameter is \( O(\log |G|) \).

For \( 1 \leq i,j \leq n \) with \( i \neq j \) let \( x_{ij}(\alpha) \) be the matrix with 1's on the diagonal, \((i,j)\)-entry \( \alpha \in \mathbb{F}_q \), and 0's elsewhere. Then \( X_{ij}:=(x_{ij}(\alpha) \mid \alpha \in \mathbb{F}_q) \) is isomorphic to the additive group of \( \mathbb{F}_q \). \( U:=\langle X_{ij} \mid 1 \leq i < j \leq n \rangle \) is the group of all upper triangular matrices with 1's on the diagonal, 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 \( \mathbb{F}_p^n \), for \( 1 \leq i \leq n \) let \( r_i \) and \( s \) be the matrices of the transformations behaving as follows:

- \( r_i : e_i \to e_{i+1} \to -e_i \) and \( e_j \to e_j \) for \( j \neq i, i+1 \), and
- \( s : e_i \to e_{i+1} \to \cdots \to e_n \to (-1)^{n-1}e_1 \).

Then \( r_i=s^i \) (where \( g^h:=h^{-1}gh \) in any group). If \( t \in \mathbb{F}_q^* \) write \( h_1(t):=\text{diag}\left(t,1,\ldots,1\right) \).

* This research was supported in part by NSF grant DMS 87-01794 and NSA grant MDA 904-88-H-2040.
$h_{i+1}(t) = h_i(t)^{s_i}$ and $H_i = \langle h_i(t) \mid t \in \mathbb{F}_q^* \rangle$ for $1 \leq i < n$, so that $H := \prod_i H_i$ is the group of all diagonal matrices in $SL(n,q)$. Also let $d_i := \text{diag}(1,1,\ldots,1)$ and $d_i^{s_i} := d_i^1$; note that $d_i = -1$ and $d_i^2 = 1$.

Calculating with $2 \times 2$ matrices, we find that (for any $t = 0$ and $\alpha$)

$$x_{i,i+1}(\alpha)^{h_i(t)} = x_{i,i+1}(\alpha^{2}) \cdot h_i(t)^{r_i}, \quad r_i^{d_i} = r_i^{-1} \quad \text{and} \quad r_i^4 = 1.$$

Let $\theta$ denote a generator of $t \in \mathbb{F}_q^*$. 

**Case:** $q$ is odd and $n \geq 12$. Write
g := $r_1 d_1 \cdot h_3(2) \cdot r_3 d_3 \cdot h_5(2) \cdot r_5 d_5 \cdot r_7 x_{9,10}(1) d_9 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$\begin{pmatrix} 0 & 1/2 \\ 2 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1/2 \cos \phi \\ 2 \cos \phi & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1/2 \cos \phi \\ 2 \cos \phi & 0 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1/2 \cos \phi \\ 2 \cos \phi & 0 \end{pmatrix} \quad \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$$

We will show that $S := \{ s, g \}$ behaves as required.

Clearly, $\det g = 1$ and $g^2 = 1$. In particular, $|S \cup S^{-1}| = 3$.

**Claim 1.** All elements of $x_{34}(\mathbb{F}_p)$ have length $O(\log p)$. For,

$$g^4 = h_3(16) h_5(\theta^4) x_{9,10}(4)$$

$$[g^4, g^4 s]^{-8} g = [x_{9,10}(4), x_{10,11}(4)]^{-8} g = x_{13}(16)^{-8} g = x_{13}(16) x_{13}(16)^{d_4} h_3(2) = x_{23}(8).$$

Thus, $x_{34}(8) = x_{23}(8)^n$ has length $O(1)$, while $x_{34}(8)^2 = x_{34}(8 \cdot 2^2)$. Now, as in [BKL], use Horner's Rule to express an arbitrary $t \in \mathbb{F}_p$ in the form

$$t = 8(t/8) = 8 \sum_{i=0}^m b_i 2^i = \cdots (8b_{m-2} 2^2 + 8b_{m-1}) 2^2 + \cdots 2^2 + 8b_0$$

where $m < \log p$ and the $b_i$ are integers satisfying $0 \leq b_i < 2^2$. Then

$$x_{34}(t) = x_{34}(8)^{b_m} x_{34}(8)^{b_{m-1}} x_{34}(8)^{b_{m-2}} \cdots x_{34}(8)^{b_0}$$

has length $O(\log p)$, as claimed.

**Claim 2.** All elements of $X_{S_6} = x_{56}(\mathbb{F}_q)$ and $X_{65}$ have length $O(\log q)$. For, all elements of
$x_{56}(\mathbb{F}_p) = x_{34}(\mathbb{F}_p)s^2$ have length $O(\log p)$. If $a \in \mathbb{F}_p$ then $x_{56}(a)^g = x_{56}(a\theta^2)$. By writing an arbitrary element of $\mathbb{F}_q$ in the form $t = \sum_{i=0}^{m} a_i \theta^{2i}$, where $m < \log p$ and $a_i \in \mathbb{F}_p$, we can proceed as above to see that each element of $X_{56}$ looks like

$$x_{56}(t) = (\cdots(x_{56}(a_m)^g x_{56}(a_{m-1}))^g \cdots)^g x_{56}(a_0)$$

for some $t \in \mathbb{F}_q$ and hence has length $O(\log q)$. Now conjugate by $g$ in order to obtain the claim.

From this point on the arguments in [BKL] can be used, essentially verbatim. We will merely outline them; the reader is referred to that paper for the details. First one shows that all elements of $L_{12} = \langle X_{12}, X_{21} \rangle \cong \text{SL}(2,q)$ have length $O(\log q)$, and hence in particular $r_1$ and all elements of $H_1$ do. Then so does $z := sr_1$. Note that $U \subset YY^s \cdots Y^{s^{n-1}}$ where $Y := X_{12} \ X_{12}^z \ X_{12}^{z^2} \cdots X_{12}^{z^{n-2}}$, and there are cancellations occurring in these products since $s^k(s^{k+1})^{-1} = s^{-1}$ and $z^k(z^{k+1})^{-1} = z^{-1}$. It follows that each element of $Y$ has length $O(n \log q)$, so that each element of $U$ has length $O(n \log q)$. Each element of $H = H_1 \ H_1^S \cdots H_1^{S^{n-2}}$ also has length $O(n \log q)$. Moreover, if $N := \langle H, r_i \mid 1 \leq i < n \rangle$ then $H \leq G$, and each element of $N/H \cong S_n$ has $\{r_i, H \mid 1 \leq i < n\}$-length $O(n)$ since the involution $r_i H$ (of $S$-length $O(n \log q)$) can be identified with the transposition $(i, i+1) \in S_n$. Then each element of $N$ has $S$-length $O(n^2 \log q) = O(\log |G|)$, and hence so does each element of $G = \text{UNU}$.\\

**Case:** $q$ is odd and $n = 10$ or $11$. This time write $g := h_1(\theta) r_1 d_1 \cdot h_3(2\theta) r_3 d_5 \cdot d_5 x_{78}(1) d_7$ and $S := \{s, g\}$, and calculate:

$$g' := gg^2 = h_1(\theta) r_1 d_1 \cdot h_3(2\theta) r_3^{-1} x_{78}(1) x_{9,10}(1) d_9$$

$$f := [(gg^2)^4]^{s^2} = h_1(16) x_{56}(4)$$

$$f^2 = h_1(16^2) x_{56}(8).$$

$$v = f^{s^4} = h_5(16) x_{9,10}(4)$$

$$f^{-1} f^v = x_{56}(4 \cdot 1 6^2 - 4)$$

Thus, $x_{56}(b)$ has length $O(1)$ for some $b \in \mathbb{F}_p^*$ (i.e., $b = 4 \cdot 16^2 - 4$ or $8$), and hence so does $x_{34}(b) = x_{56}(b)s^{-2}$. Since $x_{34}(b)^g = x_{34}(4b)$, as before it follows that all elements of $x_{34}(\mathbb{F}_p)$ have length $O(\log p)$. Then the same is true of $x_{i,i+1}(\mathbb{F}_p)$ for each $i$, and hence also of $[\cdots [x_{23}(\mathbb{F}_p), x_{34}(1)], x_{45}(1)], \cdots, x_{n1}(1)] = x_{21}(\mathbb{F}_p)$ (since $n$ is bounded!). Now $r_1 = x_{12}(1)x_{21}(-1)x_{12}(1)$ has length $O(\log p)$, and then so does $g' := gr_1$, where $x_{12}(a)^g = x_{12}(a\theta^2)$. Now proceed as before.

**Case:** $q$ is even. This time let $g := r_1 \cdot h_4(\theta) r_4 \cdot x_{78}(1)$ and $S := \{s, g\}$. Then

$$g' := gg^s = r_1 r_2 h_4(\theta) r_4 h_5(\theta) r_5 x_{78}(1) x_{89}(1)$$

$$(g^6)^s^{-6} g = [x_{78}(1), x_{89}(1)] x^{-6} g = x_{78}(1) x^{-6} g = x_{13}(1) g = x_{23}(1).$$
Thus, $x_{78}(1) = x_{23}(1)^3$ and $g x_{78}(1) = r_1 h_4(\theta) r_4$ have length $O(1)$, and hence so does $u = gx_{78}(1) (gx_{78}(1))^3 = r_1 h_4(\theta) r_7$. Since $x_{45}(a) = x_{45}(a\theta^2)$ for all $a$, by using Horner's Rule we find that all elements of $X_{45}$ have length $O(\log q)$, and hence so do all elements of $X_{54} = (X_{45})^8$.

Now proceed as before. □

It should be noted that a major difference between the cases of odd and even $q$ is that, in the former, in order to use the Horner's Rule argument from [BKL] we needed to have available $h_i(2)$ in addition to $h_i(\theta)$ for some $i$ and $j$. Those elements were introduced by having the additional dimensions.

A very crude estimate for the diameter obtained in the above argument is $d(G,S) < 10^7 \log |G|$.

**Remark.** The analogue of the Theorem holds for the groups $G = A_n$ and $S_n$. We will only indicate this here with an example. It is straightforward to use the methods in [BKL] to modify this in order to handle the general case.

Let $G = S_n$ with $n = 2k+1-1$ and $k$ odd. Identify the set $X = \{0,1,\ldots,2k-2\}$ with $\mathbb{Z}_{2k-1}$, and let $X' = \{x' \mid x \in X\}$ be another copy of $X$. Consider the $n$-set $\{\infty\} \cup X \cup X'$ and (letting $x$ range over $X$) the permutations

$$t: x \mapsto x', \infty \mapsto \infty,$$

$$g: = (\infty,0)(x \mapsto ax)(x' \mapsto [ax + a - 1]),$$

where $a = 2^{k+1}$ so that $a^2 \equiv 2 \pmod{2k-1}$. (Note that $x \mapsto ax$ fixes $0$.) We claim that $S = \{t, g\}$ behaves as required: $|S \cup S^{-1}| = 3$ and $d(G,S) = O(\log |G|)$. First note that

$$g^2 = (x \mapsto 2x)(x' \mapsto [2x+1])$$

and

$$(g^2)^k = (x \mapsto 2x+1)(x' \mapsto [2x'])$$

Every $x \in X$ is the image of $0$ by a word $w(x)$ in $\{g^2, (g^2)^k\}$ of length $O(k) = O(\log n)$: using Horner's Rule we can write $x = \sum_{i=0}^{k} a_i 2^i = 0^w(x)$ where $w(x) = (g^2)^{a_k} (g^2)^{a_{k-1}} \cdots (g^2)^{a_0}$ with all $a_i \in \{0,1\}$ (cf. [BKL]). Also, $g^k = (\infty,0)$ since $k$ is odd, so that $(\infty,0)$ has length $O(\log n)$. If $x \in X$ then the transposition $(\infty,x) = (\infty,0)^w(x)$ also has length $O(\log n)$. Then the same is true of every transposition $(\infty,x') = (\infty,x)^k$, $x \in X$. Since each element of $S_n$ is a word of length $O(n)$ in the transpositions just constructed, this proves the claim. This time crude estimates yield that $d(G,S) < 25 n \log n$.

**References**
