DIAMETERS OF CAYLEY GRAPHS OF CHEVALLEY GROUPS

M. KASSABOV AND T. R. RILEY

ABSTRACT. We show that for integers $k \geq 2$ and $n \geq 3$, the diameter of the Cayley graph of $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ associated to a standard two-element generating set, is at most a constant times $n^2 \ln k$. This answers a question of A. Lubotzky concerning $\mathrm{SL}_n(\mathbb{F}_p)$ and is unexpected because these Cayley graphs do not form an expander family. Our proof amounts to a quick algorithm for finding short words representing elements of $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$. We generalize our results to other Chevealley groups over $\mathbb{Z}/k\mathbb{Z}$.

1. INTRODUCTION

This paper concerns expressing elements of $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$, for integers $k \geq 2$ and $n \geq 3$, as words in the two-element generating set $\{\mathcal{A}_n, \mathcal{B}_n\}$, where

$$\mathcal{A}_n := \begin{pmatrix} 1 & 1 & & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \quad \mathcal{B}_n := \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1 \\ (-1)^{n-1} & & & & 0 \end{pmatrix}.$$

From the point of view of word length, one might suspect this to be an inefficient generating set because the conjugates of $\mathcal{A}_n$ by small powers of $\mathcal{B}_n$ generate a nilpotent group, and the diameters of nilpotent groups are large [1]. However we show in this paper:

Theorem 1.1. *For all integers $k \geq 2$ and $n \geq 3$,*

$$\mathrm{Diam}\ \mathrm{Cay}(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\}) \leq 3600\, n^2 \ln k.$$

Moreover, there is an algorithm which expresses matrices in $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ as words on $\mathcal{A}_n$ and $\mathcal{B}_n$ of length $O(\ln |\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})|)$ in time $O(\ln |\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})|)$.

The $n^2 \ln k$ term is the best possible because a logarithm of $|\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})| \sim k^{n^2-1}$ gives a lower bound on the diameter of $\mathrm{Cay}(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\})$. More precise tracking of word length in our arguments would lead to an

Date: October 14, 2005.

2000 *Mathematics Subject Classification.* primary 20F05; secondary 05C25, 05C35, 20D06.

Key words and phrases. special linear, diameter, Cayley graph, finite simple groups.

The second author gratefully acknowledges support from NSF grant 0404767.

improvement of the constant from 3600 to at least 1400, but at the expense of complicating the exposition.

Our result is better than that obtainable by known methods that use the heavy machinery of Property T, Kazhdan constants and expander families. For fixed $n \geq 3$, Property T of $\mathrm{SL}_n(\mathbb{Z})$ implies that

$$\{\mathrm{Cay}(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\}) \mid k \geq 2\}$$

is an expander family. So the diameter of $\mathrm{Cay}(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\})$ is at most $C(n) \ln k$, where the constant $C(n)$ is related to the Kazhdan constant $\mathcal{K}(\mathrm{SL}_n(\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\})$ by $C(n) < n^2/\mathcal{K}(\mathrm{SL}_n(\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\})^2$. Lower bounds for Kazhdan constants are hard to come by. Using the bounds of [8] for $\mathcal{K}(\mathrm{SL}_n(\mathbb{Z}), S)$, where S is the set of all elementary matrices $e_{i,j}$, one can show $\mathcal{K}(\mathrm{SL}_n(\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\}) > n^{-3/2}$. This implies that $C(n) = O(n^5)$.

Were

$$\{\mathrm{Cay}(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\}) \mid k \geq 2, n \geq 3\}$$

an expander family, our $O(n^2 \ln k)$ bound would immediately follow. But this is not so: on page 105 of [11] an argument of Yael Luz is given that shows the expander constant of $\mathrm{Cay}(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}_n, \mathcal{B}_n\})$ to be at most $5/n$, which is not bounded away from 0.

Analogous results for $\mathrm{SL}_2(\mathbb{Z}/k\mathbb{Z})$ and other rank one Chevalley groups cannot be proved using our methods. Indeed, there is no known fast algorithm which writes elements in $\mathrm{SL}_2(\mathbb{F}_p)$ as short words in $\mathcal{A}$ and $\mathcal{B}$. For results in this direction see [3, 4, 6, 9].

This article builds on methods in [13], where it is shown (Theorem 5.1) that for all $n \geq 3$, the diameter of $\mathrm{Cay}(\mathrm{SL}_n(\mathbb{F}_p), S)$ is at most a constant times $n^2 \ln p$, where S is the set of all elementary matrices $e_{i,j}$. By expressing the elementary matrices as words in $\mathcal{A}_n$ and $\mathcal{B}_n$ one deduces [13, Corollary 1.1] that the diameter of $\mathrm{Cay}(\mathrm{SL}_n(\mathbb{F}_p), \{\mathcal{A}_n, \mathcal{B}_n\})$ is at most a constant times $n^3 \ln p$.

Theorem 1.1 affirmatively answers a question of A. Lubotzky [10, Problem 8.1.3] and improves on, and provides a constructive proof for, a result of Lubotzky, Babai and Kantor:

Proposition 1.2 ([2, 10])**.** *There exists $K > 0$ such that for all $n \geq 3$ and primes p, there is a set Σ of three generators for $\mathrm{SL}_n(\mathbb{F}_p)$ such that*

$$\mathrm{Diam}\ \mathrm{Cay}(\mathrm{SL}_n(\mathbb{F}_p), \Sigma) \ \leq \ Kn^2 \ln p.$$

In [2], it is shown that there is a constant $K > 0$ such that every finite simple non-abelian group Γ has a seven-element generating set S such that $\mathrm{Diam}\ \mathrm{Cay}(\Gamma, S) \leq K \ln |\Gamma|$. For $\Gamma = \mathrm{PSL}_n(\mathbb{F}_q)$ and $n \geq 10$, Kantor [7] improved this by showing that S could be found with only two elements, one of which is an involution.

These methods can be generalized to show that, with respect to a generating set consisting of a Weyl element and a generator of a root subgroup, there exists $K > 0$ such that the diameter of any Chavalley group Γ over

$\mathbb{Z}/k\mathbb{Z}$, of rank at least 2, is at most $K \ln |\Gamma|$. We give a proof only in the case of rank at least 4. The rank 2 and 3 cases can be established in a similar way but the proof is significantly more technical.

Theorem 1.3. *There exits a constant K such that for every classical Chavalley group Γ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, of rank at least 2, there exists a two element generating set S consisting of a Weyl element and a generator of a root subgroup such that* $\text{Diam Cay}(\Gamma, S) \leq K \ln |\Gamma|$.

A further extension shows that for every finite simple group Γ of Lie type and of rank at least 2, there is a 3 element generating set S such that $\text{Diam Cay}(\Gamma, S) \leq K \ln |\Gamma|$. Combined with a similar result for the rank 1 groups from [2] and the corresponding result for the alternating/symmetric groups [10, Proposition 8.1.6], this yields

Theorem 1.4. *There exists $K > 0$ such that every finite simple non-abelian group Γ has a 4 element generating set S such that*

$$\text{Diam Cay}(\Gamma, S) \leq K \ln |\Gamma| .$$

Moreover, as all the proofs are suitably constructive, there is a fast algorithm which, given $g \in \Gamma$ produces a word on S representing g, provided that Γ is not a factor of a lattice in a rank 1 Lie group.

2. Generating bit-row and bit-column matrices

All the computations in this and the next section are in $\text{SL}_n(\mathbb{Z})$ where $n \geq 3$ (or in some extension of such a group). Let us fix some notation and terminology. Denote the matrix with 1's on the diagonal and in the i, j-th place, and 0's everywhere else by $e_{i,j}$. Let $\mathcal{A} = e_{1,2}$, which is a generator of a root subgroup in $\text{SL}_n(\mathbb{Z})$, and let $\mathcal{B}$ be any element such that $\mathcal{B}^{-s}\mathcal{A}\mathcal{B}^s = e_{s+1,s+2}$ for all $0 \leq s \leq n-2$, i.e., using the simple root α_1 we can obtain all other simple roots just by conjugating with powers $\mathcal{B}$. We observe that $\mathcal{A}_n$ and $\mathcal{B}_n$, defined in Section 1, have these properties. Define a *row* (*column*) *matrix* to be a square upper triangular matrix whose diagonal entries are all 1's and which differs from the identity only in one row (column). A *bit*-row (*bit*-column) matrix is a row (column) matrix whose entries are all in $\{0, \pm 1\}$. For a sequence $\mathbf{m} = \{m_i\}_{i=2}^n$ define $R_{\mathbf{m}}$ to be the row matrix whose entries all agree with those of the identity matrix except for those in row 1 which is

$$(1,\ m_2,\ m_3,\ m_4,\ \ldots,\ m_n).$$

This section is devoted to proving the following proposition and an analogue concerning column matrices.

Proposition 2.1. *Suppose $M \in \text{SL}_n(\mathbb{Z})$ is a bit-row matrix. There is a word on $\mathcal{A}$ and $\mathcal{B}$ that represents M and, if the first row of M differs from the identity, has length at most $48n$, and at most $49n$ otherwise.*

Proof. For integers $s_2, \dots, s_{n-1}$, $t_2, \dots, t_{n-2}$ define

$$N := \begin{pmatrix} 1 & 0 & 0 & & & & \\ & 1 & -s_2 & -t_2 & & & \\ & & 1 & -s_3 & -t_3 & & \\ & & & 1 & -s_4 & \ddots & \\ & & & & 1 & \ddots & -t_{n-2} \\ & & & & & \ddots & -s_{n-1} \\ & & & & & & 1 \end{pmatrix}.$$

Lemma 2.2. *The matrix $Ne_{1,2}N^{-1}$ is equal to $R_{\mathbf{m}}$, where the sequence $\{m_i\}$ is defined recursively by $m_2 = 1$, $m_3 = s_2$ and $m_i = m_{i-1}s_{i-1} + m_{i-2}t_{i-2}$ for $4 \leq i \leq n$.*

Proof. Rows 2 to n of $R_{\mathbf{m}}N$ and $Ne_{1,2}$ are the same as rows 2 to n of N. The recursion defining $\{m_i\}$ ensures that the first rows of $R_{\mathbf{m}}N$ and $Ne_{1,2}$ also agree.

Lemma 2.3. *Suppose $m_2 = 1$ and $m_3, \dots, m_n \in \{0, \pm 1, \pm 2\}$ satisfy one of the two conditions:*

(i) *$m_{2i} = 1$ for all i,*
(ii) *$m_{2i+1} = 1$ for all i.*

Then there exist $s_2, \dots, s_{n-1} \in \{0, \pm 1, \pm 2\}$ and $t_2, \dots, t_{n-2} \in \{0, 1\}$ satisfying the equations in Lemma 2.2.

Proof. There is a solution in case (i) with $s_{2i} = m_{2i+1}$, $s_{2i+1} = 0$, $t_{2i} = 1$, $t_{2i+1} = 0$ for all $i \geq 1$, and in case (ii) with $s_2 = 1$, $s_{2i+2} = 0$, $s_{2i+1} = m_{2i+2}$, $t_{2i} = 0$, $t_{2i+1} = 1$, for all $i \geq 1$.

Our next lemma is an immediate consequence of the previous two.

Lemma 2.4. *If $m_2 = 0$ and $m_3, \dots, m_n \in \{0, \pm 1\}$ then there exist two matrices N_1, N_2 of the same form as N, having all entries in $\{0, \pm 1, \pm 2\}$, and satisfying $R_{\mathbf{m}} = N_1 e_{12} {N_1}^{-1} N_2 e_{12}{}^{-1} {N_2}^{-1}$.*

Lemma 2.5. *If $s_2, \dots, s_{n-1} \in \{0, \pm 1, \pm 2\}$ and $t_2, \dots, t_{n-2} \in \{0, \pm 1\}$ then the word*

$$w \;:=\; \mathcal{B}^{-(n-2)} Q_{n-1} \mathcal{B} Q_{n-2} \mathcal{B} \dots Q_2 \mathcal{B},$$

where $Q_i := \mathcal{A}^{-s_i} [\mathcal{A}, \mathcal{B}^{-1}\mathcal{A}\mathcal{B}]^{-t_i}$ and $t_{n-1} := 0$, represents N and has length at most $12n - 24$ as a word on $\mathcal{A}$ and $\mathcal{B}$.

Proof. This result follows from the observations that w equals

$$(\mathcal{B}^{-(n-2)}Q_{n-1}\mathcal{B}^{n-2})(\mathcal{B}^{-(n-3)}Q_{n-2}\mathcal{B}^{n-3})\dots(\mathcal{B}^{-1}Q_2\mathcal{B}),$$

in $\mathrm{SL}_n(\mathbb{Z})$, and $(\mathcal{B}^{-(i-1)}Q_i\mathcal{B}^{i-1})$ equals the row matrix whose entries in the i-th row agree with those of N and whose remaining entries agree with the identity matrix.

To complete the proof of Proposition 2.1 in the row matrix case, first suppose $M = R_{\mathbf{m}}$ where $m_2 = 0$ and $m_3, \dots, m_n \in \{0, \pm 1\}$. Lemmas 2.4 and 2.5 supply a word $w_{\mathbf{m}}$ on $\mathcal{A}$ and $\mathcal{B}$ that represents M and has length at most $4(12n-24)+2$. We can change m_2 to ± 1 by right-multiplying by ${e_{1,2}}^{\pm 1} = \mathcal{A}^{\pm 1}$. This proves that $\ell(w_{\mathbf{m}}) < 48n$, as claimed.

Conjugating a matrix by a power of $\mathcal{B}$ moves its entries diagonally. So any given bit-row matrix M equals $\mathcal{B}^l R_{\mathbf{m}} \mathcal{B}^{-l}$ for some $\mathbf{m} = \{m_i\}_{i=2}^n$ with $m_i \in \{0, \pm 1\}$, and some $-n/2 \le l \le n/2$. The cost to word length of conjugating is at most n and so M can be written as a word on $\mathcal{A}$ and $\mathcal{B}$ of length at most $49n$. □

There is a natural analog of Proposition 2.1 for bit-column matrices:

Proposition 2.6. *If $M \in \mathrm{SL}_n(\mathbb{Z})$ is a bit-column matrix then there is a word on $\mathcal{A}$ and $\mathcal{B}$ that represents M and has length at most $48n$ if the final column differs from the identity, and at most $49n$ otherwise.*

Proof. As in Proposition 2.2, if we define

$$\widetilde{N} := \begin{pmatrix} 1 & -s_1 & -t_1 & & & & & \\ & 1 & -s_2 & -t_2 & & & & \\ & & \ddots & \ddots & \ddots & & & \\ & & & 1 & -s_{n-3} & -t_{n-3} & & \\ & & & & 1 & -s_{n-2} & 0 & \\ & & & & & 1 & 0 & \\ & & & & & & 1 & \end{pmatrix},$$

we find $\widetilde{N}^{-1} e_{n-1,n} \widetilde{N}$ is a column matrix $C_{\mathbf{m}'}$ whose final column is

$$(m'_1, \dots, m'_{n-1}, 1)^{tr},$$

where $m'_{n-1} = 1$, $m'_{n-2} = s_{n-2}$ and $m'_i = m'_{i+1}s_i + m'_{i+2}t_i$ for $1 \le i \le n-3$.

The analogue of Lemma 2.3, implies that if $m'_1, \dots, m'_{n-2} \in \{0, \pm 1, \pm 2\}$ satisfies $m'_{2i} = 1$ for all i, or $m'_{2i+1} = 1$ for all i, then $C_{\mathbf{m}'}$ can be written as a short word on $\mathcal{A}$ and $\mathcal{B}$. And, as in Lemma 2.4, two such column matrices can be multiplied to produce any given bit-column matrix $C_{\mathbf{m}''}$ in which $m''_{n-1} = 0$. Then m''_{n-1} can then be changed to ± 1 if required by left-multiplying by ${e_{n-1,n}}^{\pm 1}$.

In this context, the analogue of the length bound of Lemma 2.5 is $12n-26$. Therefore the cost of producing $C_{\mathbf{m}''}$ is at most $4(12n-26)+10$ because $e_{n-1,n} = \mathcal{B}^2\mathcal{A}\mathcal{B}^{-2}$ if n is odd and $e_{n-1,n} = \mathcal{B}^2\mathcal{A}^{-1}\mathcal{B}^{-2}$ if n is even, which has

word length 5 in both cases. This also shows that the cost of altering m''_{n-1} is at most 5. The total cost, then, is within the claimed bound of $48n$. As in the row matrix case, it follows that every bit-column matrix can be written as a word on $\mathcal{A}$ and $\mathcal{B}$ of length at most $49n$. □

Remark 2.7. This construction yields an algorithm with running time $O(n)$ which produces a short word on $\mathcal{A}$ and $\mathcal{B}$ representing any given bit-row or bit-column matrix in $\mathrm{SL}_n(\mathbb{Z})$.

3. Generating row and column matrices

Before we come to the main result of this section we give a lemma which is essentially [13, Lemma 2.2]. It concerns expressing matrices ${e_{i,j}}^{F_{2l}}$ and ${e_{i,j}}^{F_{2l+1}}$, where the powers are Fibonacci numbers (defined recursively by $F_0 = 0$, $F_1 = 1$, and $F_{i+2} = F_{i+1} + F_i$), as short words on $\{e_{i,j} \mid i \neq j\}$. This lemma will be superseded by Lemma 3.3, but the detailed calculation we give in the proof of this simpler case is key to understanding the proof of the more general result.

Lemma 3.1. *For non-negative integers l, the words*

$$e_{1,2}{}^2(e_{2,1}e_{1,2})^l e_{1,3}(e_{2,1}e_{1,2})^{-l} e_{1,2}{}^{-1}(e_{2,1}e_{1,2})^l e_{1,3}{}^{-1}(e_{2,1}e_{1,2})^{-l} e_{1,2}{}^{-1}, \quad \textit{and}$$
$$e_{1,2}{}^2(e_{2,1}e_{1,2})^l e_{2,3}(e_{2,1}e_{1,2})^{-l} e_{1,2}{}^{-1}(e_{2,1}e_{1,2})^l e_{2,3}{}^{-1}(e_{2,1}e_{1,2})^{-l} e_{1,2}{}^{-1}$$

equal ${e_{1,3}}^{F_{2l}}$ and ${e_{1,3}}^{F_{2l+1}}$, respectively, in $\mathrm{SL}_3(\mathbb{Z})$.

Proof. We multiply out the first of these words from left to right as follows. The calculation for the second is similar. The notation for each step shown is $S \xrightarrow{T} ST$.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{{e_{1,2}}^2} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{2,1}e_{1,2})^l} \begin{pmatrix} F_{2l+2} & F_{2l+3} & 0 \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{1,3}} \begin{pmatrix} F_{2l+2} & F_{2l+3} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{2,1}e_{1,2})^{-l}} \begin{pmatrix} 1 & 2 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{{e_{1,2}}^{-1}} \begin{pmatrix} 1 & 1 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{2,1}e_{1,2})^l} \begin{pmatrix} F_{2l+1} & F_{2l+2} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{{e_{1,3}}^{-1}} \begin{pmatrix} F_{2l+1} & F_{2l+2} & F_{2l} \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{2,1}e_{1,2})^{-l}} \begin{pmatrix} 1 & 1 & F_{2l} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{{e_{1,2}}^{-1}} \begin{pmatrix} 1 & 0 & F_{2l} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

□

Let $\mathcal{A}$ and $\mathcal{B}$ be matrices as in the beginning of Section 2 and let $\mathcal{C} = e_{2,1}$ (a generator of the opposite root subgroup). Assume $\mathcal{B}^{-s}\mathcal{C}\mathcal{B}^s = e_{s+2,s+1}$ for all $0 \leq s \leq n-2$ (as is the case for $\mathcal{B} = \mathcal{B}_n$, for example).

Proposition 3.2. *Suppose $M \in \mathrm{SL}_n(\mathbb{Z})$ is a row or column matrix with entries in $\{-K+1, \ldots, 0, \ldots, K-1\}$, where $K \geq 1$. Then there is a word on $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$, representing M, of length $1200n \ln K + 400n$, where $\mathcal{C}$ appears at most $50 \ln K + 50$ times.*

Proof. The proof in the row matrix case generalizes Lemma 3.1 – instead of using $e_{1,3}$ and $e_{2,3}$ we use general bit-row matrices; they allow the simultaneous construction of sums of Fibonacci numbers in entries $3, \ldots, n$ of the first row. These sums of Fibonacci numbers are as per Zeckendorf's Theorem [5, 15], which states that every nonzero integer m can be expressed in a unique way as

$$m = \pm(F_{l_1} + F_{l_2} + \cdots + F_{l_r}),$$

with $l_1 \geq 2$ and $l_{j+1} - l_j \geq 2$ for all $1 \leq j < r$. This result can be proved by an easy induction argument and, in fact, F_{l_r} is the largest Fibonacci number no bigger than $|m|$, and $F_{l_{r-1}}$ is the largest no bigger than $|m| - F_{l_r}$, and so on. Since $F_s = (\tau^s - (-\tau)^{-s})/\sqrt{5}$ for all $s \in \mathbb{N}$, where $\tau := (1+\sqrt{5})/2$, we get $F_s \geq (\tau^s - 1)/\sqrt{5}$. Thus, as $F_{l_r} \leq |m|$, we find

$$l_r \leq \log_\tau(1 + |m|\sqrt{5}) < 2 + 3\ln|m|,$$

from which we derive the bound on L in the following lemma.

Lemma 3.3. *Suppose $\mathbf{m} := \{m_i\}_{i=3}^n$ is a sequence of integers, such that $|m_i| < K$ for all i. As per Zeckendorf's Theorem, write*

$$m_i \;=\; \sum_{j=1}^{L} (c_{ij} F_{2j} + d_{ij} F_{2j+1})$$

where $c_{ij}, d_{ij} \in \{0, \pm 1\}$ and $L \leq (2 + 3\ln K)/2 - 1/2$. Let $u_{\mathbf{m}}$ be the word

$$(e_{2,1}e_{1,2})a_1b_1(e_{2,1}e_{1,2})a_2b_2(e_{2,1}e_{1,2})\ldots(e_{2,1}e_{1,2})a_Lb_L$$

in which a_j is the row matrix with first row $(1, 0, c_{3j}, \ldots, c_{nj})$ and b_j is the row matrix with second row $(0, 1, d_{3j}, \ldots, d_{nj})$. Let $v_{\mathbf{m}}$ be the word obtained from $u_{\mathbf{m}}$ by replacing each a_j and b_j by its inverse. Define

$$w_{\mathbf{m}} := {e_{1,2}}^2 u_{\mathbf{m}} (e_{2,1}e_{1,2})^{-L} {e_{1,2}}^{-1} v_{\mathbf{m}} (e_{2,1}e_{1,2})^{-L} {e_{1,2}}^{-1}.$$

Then in $\mathrm{SL}_n(\mathbb{Z})$ the row matrix with first row $(1, 0, m_3, \ldots, m_n)$ is represented by $w_{\mathbf{m}}$.

Proof. Lemma 3.1 gives the special cases of this lemma in which $n = 3$ and m_3 is F_{2l} or F_{2l+1}. Below we multiply out $w_{\mathbf{m}}$ from left to right, using a more general and concise version of the calculation used to prove Lemma 3.1.

We display the top two rows only; all others agree with the identity matrix throughout the calculation. All the summations range over $j = 1, \dots, L$.

$$\begin{pmatrix} 1 & 2 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}$$

$$\Big\downarrow u_{\mathbf{m}}$$

$$\begin{pmatrix} F_{2L+2} & F_{2L+3} & \sum(c_{3j}F_{2j+2} + d_{3j}F_{2j+3}) & \cdots & \sum(c_{nj}F_{2j+2} + d_{nj}F_{2j+3}) \\ F_{2L} & F_{2L+1} & \sum(c_{3j}F_{2j} + d_{3j}F_{2j+1}) & \cdots & \sum(c_{nj}F_{2j} + d_{nj}F_{2j+1}) \end{pmatrix}$$

$$\Big\downarrow (e_{2,1}e_{1,2})^{-L}$$

$$\begin{pmatrix} 1 & 2 & \sum(c_{3j}F_{2j+2} + d_{3j}F_{2j+3}) & \cdots & \sum(c_{nj}F_{2j+2} + d_{nj}F_{2j+3}) \\ 0 & 1 & \sum(c_{3j}F_{2j} + d_{3j}F_{2j+1}) & \cdots & \sum(c_{nj}F_{2j} + d_{nj}F_{2j+1}) \end{pmatrix}$$

$$\Big\downarrow {e_{1,2}}^{-1}v_{\mathbf{m}}$$

$$\begin{pmatrix} F_{2L+1} & F_{2L+2} & \sum(c_{3j}F_{2j} + d_{3j}F_{2j+1}) & \cdots & \sum(c_{nj}F_{2j} + d_{nj}F_{2j+1}) \\ F_{2L} & F_{2L+1} & 0 & \cdots & 0 \end{pmatrix}$$

$$\Big\downarrow (e_{2,1}e_{1,2})^{-L}{e_{1,2}}^{-1}$$

$$\begin{pmatrix} 1 & 0 & \sum(c_{3j}F_{2j} + d_{3j}F_{2j+1}) & \cdots & \sum(c_{nj}F_{2j} + d_{nj}F_{2j+1}) \\ 0 & 1 & 0 & \cdots & 0 \end{pmatrix}.$$

The sums in this final matrix are, by definition, equal to $m_3, \dots, m_n$ and so the lemma is proved.

Returning to the proof of Proposition 3.2, note that a conjugate of M by a power of $\mathcal{B}$ is a row matrix $\mathrm{R}_{\mathbf{m}}$ in which the first row is $(1, m_2, m_3, \dots, m_n)$. On the alphabet $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$, we find $e_{1,2} = \mathcal{A}$ and $e_{2,1} = \mathcal{C}$, and so both have length 1, and a_j, b_j are both bit-row matrices and so, by Proposition 2.1, can be expressed as words of length at most $48n$. So the word $w_{\mathbf{m}}$ of Lemma 3.3 can be re-expressed as a word on $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$. of length $200nL$, where the contributions to this estimate are

$$\begin{aligned} 4 + 4L \ &\times \ 1 \ \text{ from } \ e_{1,2} \\ 4L \ &\times \ 1 \ \text{ from } \ e_{2,1} \\ 2L \ &\times \ 48n \ \text{ from } \ a_j \\ 2L \ &\times \ 48n \ \text{ from } \ b_j. \end{aligned}$$

A revised version of Lemma 3.3 in which we build up Fibonacci numbers in columns 2 and 3 using $e_{2,3}$ and $e_{3,2}$ rather than in columns 1 and 2 using $e_{1,2}$ and $e_{2,1}$, produces a word on $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ that represents the row

matrix with first row $(1, m_2, 0, \ldots, 0)$. Mildly revising the estimates above, we check that the length of this word is at most $200nL$. Multiplying the two words together gives a word of length at most $400nL$ that represents $R_{\mathbf{m}}$. Conjugating by a power of $\mathcal{B}$ recovers M at a further expense to word length of at most n. Then, using the bound on L in Lemma 3.3, we learn that M can be represented by a word on $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ of length at most $1200n \ln K + 400n$, where $\mathcal{C}$ appears at most $50 \ln K + 50$ times

Obtain the same bound in the column matrix case by transposing and using Proposition 2.6 in place of 2.1: reverse the orders of the terms in $w_{\mathbf{m}}, u_{\mathbf{m}}$ and $v_{\mathbf{m}}$, interchange the $e_{1,2}$'s and $e_{2,1}$'s, and make the a_i and b_i bit-column matrices rather than bit-row matrices. □

Remark 3.4. It follows from the construction above that there is an algorithm with running time $O(n \ln K)$ which produces a short word in $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ that represents any given row matrix in $\mathrm{SL}_n(\mathbb{Z})$ with entries in $\{-K+1, \ldots, 0, \ldots, K-1\}$.

4. The diameter of $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$.

Proof of Theorem 1.1. All row matrices in $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ come from row matrices in $\mathrm{SL}_n(\mathbb{Z})$ with entries of absolute value less than $k/2$ and so can be represented by short words on $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ as per Proposition 3.2. Observe that $\mathcal{C} = \mathcal{B}^{-1} e_{1,n} \mathcal{B}$ and by Lemma 2 can be written as a word on $\mathcal{A}$ and $\mathcal{B}$ of length at most $48n$. So Lemma 4.3 below completes the proof of the bound in Theorem 1.1.

Our proof is constructive and amounts to an algorithm for expressing matrices in $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ as words on $\mathcal{A}_n$ and $\mathcal{B}_n$ with running time

$$O(n^2 \ln k) = O(\ln |\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})|),$$

provided that k is decomposed as a product of prime numbers. □

We start with a technical lemma which is also valid for rings satisfying the Bass stable range condition – see [14].

Lemma 4.1. *Let $a, b \in \mathbb{Z}/k\mathbb{Z}$. Then there exists $s \in \mathbb{Z}/k\mathbb{Z}$ such that the ideal generated by a and b is the same as the ideal generated by $a + sb$.*

Proof. If $k = \prod {p_i}^{m_i}$ then

$$\mathbb{Z}/k\mathbb{Z} \simeq \prod \mathbb{Z}/{p_i}^{m_i}\mathbb{Z}$$

by the Chinese Remainder Theorem. Let a_i and b_i be the components of a and b in $\mathbb{Z}/{p_i}^{m_i}\mathbb{Z}$. Define $s_i := 0$ if the ideal generated by a_i in $\mathbb{Z}/{p_i}^{m_i}\mathbb{Z}$ contains b_i and $s_i := 1$ otherwise. Let s be the element in $\mathbb{Z}/k\mathbb{Z}$ with components s_i. By construction, the components of $a + sb$ are $a_i + s_i b_i$ and in the ring $\mathbb{Z}/{p_i}^{m_i}\mathbb{Z}$ the ideal generated by $a_i + s_i b_i$ is the same as the ideal generated by a_i and b_i. □

Corollary 4.2. *Suppose $\{a_i\}_{i=1}^{l}$ are elements of $\mathbb{Z}/k\mathbb{Z}$ such that the ideal they generate is the whole ring. Then there exist $\{t_i\}_{i=2}^{l}$ such that*

$$a_1 + t_2a_2 + t_3a_3 + \cdots + t_la_l$$

is invertible in $\mathbb{Z}/k\mathbb{Z}$.

In fact, (given the decomposition of k into prime factors) we can write a fast algorithm to find these coefficients. This is because a_i and b_i of Lemma 4.1 can be found quickly, being $a \bmod {p_i}^{m_i}$ and $b \bmod {p_i}^{m_i}$, respectively. The maximal power of p_i dividing a_i and b_i determines s_i. And in the proof of Lemma 4.1 we can use $k \sum s_i/{p_i}^{m_i}$, which is easier to compute.

Lemma 4.3. *If $M \in \mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ then the matrix M can be written as a product of n row matrices, n column matrices and n elementary matrices.*

Proof. We use a version of Gauss-Jordan elimination to prove by induction on $r = 0, \ldots, n$ that M can be transformed to a matrix in which the top r rows agree with the identity matrix by left- and right-multiplying by a total of $3r$ row, column and elementary matrices.

The base step $r = 0$ holds vacuously. For the induction step assume $r < n$ and the top r rows agree with the identity matrix. If the final entry on the $(r+1)$-st row is not invertible in $\mathbb{Z}/k\mathbb{Z}$ then, using Corollary 4.2, it can be made invertible by right-multiplying by some column matrix, because the ideal generated by the $(r+1)$-st to n-th entries in row $r+1$ is the whole ring $\mathbb{Z}/k\mathbb{Z}$. Then make the $r+1, r+1$-entry 1 by right-multiplying by the appropriate power of $e_{n,r+1}$. Then clear all the off-diagonal entries in row $r+1$ by right-multiplying by the appropriate row matrix. □

Remark 4.4. The constructions in this paper can be used to express matrices $M \in \mathrm{SL}_n(\mathbb{Z})$ as short words on $\mathcal{A}_n$ and $\mathcal{B}_n$ (cf. [13, Theorem 4.1]). However, the resulting upper bounds on word length are not very good because if we express M as a product of row matrices R_i then the absolute values of the entries in the R_i may be significantly larger than the absolute values of the entries in M.

5. Diameters of Chavalley groups.

Proof of Theorem 1.3. For any given Chevalley group over $\mathbb{Z}/k\mathbb{Z}$ we could define the notion of 'row' and 'column' matrices and modify then generalise the proof of Theorem 1.1. Instead, we are going to first show that some sufficiently large copy of SL_n, with small diameter with respect to the chosen generating set, can be embedded in Chevalley group over $\mathbb{Z}/k\mathbb{Z}$. When combined with a recent result of Nikolov [12], this will prove Theorem 1.3.

If the type of the root system of Γ is C_n then the Chevalley group is $\mathrm{Sp}_n(\mathbb{Z}/k\mathbb{Z})$. Let x be a generator of the root subgroup corresponding to the

simple root α_1 and let w be the Weyl element corresponding to $s_1 s_2 \cdots s_n$. Then w acts on the roots as follows:

$$\alpha_1 \ \to \ \alpha_2 \ \to \ \cdots \ \to \ \alpha_{n-1} \to \ \alpha_1 + \cdots + \alpha_n \ \to \ -\alpha_1 \ \to \ -\alpha_2 \ \to \ \cdots$$

Thus x, w and $w^{-n} x w^n$ play the role of $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ in the copy of $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ generated by the roots corresponding to $\pm\alpha_i$ for $i = 1, \ldots, n-1$. This allows us to apply Proposition 2.6 and mimic the proof of Theorem 1.1 to see that any element in this group can be written as a word of length $3600n^2 \ln k$ on x and w. By a result of Nikolov [12] the group $\mathrm{Sp}_n(\mathbb{Z}/k\mathbb{Z})$ can be written as a product of 200 copies of $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ which are obtained by conjugation with powers of w. This implies that the diameter of the Cayley graph is less than $10^6 n^2 \ln k$.

If the root system is of type B_n or D_n then the Chevalley group is $\mathrm{SO}_{2n+1}(\mathbb{Z}/k\mathbb{Z})$ or $\mathrm{SO}_{2n}(\mathbb{Z}/k\mathbb{Z})$, arising from the quadratic form with signature $(1^{n+1}, -1^n)$ or $(1^{n+1}, -1^n)$. Let x be a generator of the root subgroup corresponding to the simple root α_n and let w be the Weyl element corresponding to $s_1 s_2 \cdots s_n$ in the case of B_n and to $s_n s_1 \cdots s_{n-1}$ in the case of D_n. It can be seen that w acts on the copy $\mathrm{SL}_{n-1}(\mathbb{Z}/k\mathbb{Z})$ generated by the roots corresponding to $\pm\alpha_i$ for $i = 1, \ldots, n-2$ as the element $\mathcal{B}$. We can also write $\mathcal{C}$ as a word of length $O(n)$ because some power of w acts as -1 on the roots. However there is not expression for $\mathcal{A}$ as a word of constant length on x and w. Nevertheless, the bit-row matrix with first row $a_2, \ldots, a_{n-1}$ can be written as word of length $O(n)$: in the case of B_n the expression is

$$[w^{n-1} x w^{-n+1}, w^{-2} x^{a_2} w^{-1} x^{a_3} w^{-1} \ldots w^{-1} x^{a_{n-1}} w^{n-1}]$$

and in the case of D_n it is similar. This allows us to modify the proofs of Proposition 2.6 and Theorem 1.1 to see that any element in this copy of $\mathrm{SL}_{n-1}(\mathbb{Z}/k\mathbb{Z})$ can be written as a word of length $4000n^2 \ln k$ on x and w. Again we can apply the result of Nikolov to see that $\mathrm{SO}_{2n+1}(\mathbb{Z}/k\mathbb{Z})$ and $\mathrm{SO}_{2n}(\mathbb{Z}/k\mathbb{Z})$ can be written as a product of 200 copies of $\mathrm{SL}_{n-1}(\mathbb{Z}/k\mathbb{Z})$, each of which is a conjugate of the copy discussed above by some power of w. This implies that the diameter of the Cayley graph is less than $10^6 n^2 \ln k$.

References

[1] F. Annexstein and M. Baumslag. On the diameter and bisector size of Cayley graphs. *Math. Systems Theory*, 26(3):271–291, 1993.

[2] L. Babai, W. M. Kantor, and A. Lubotzky. Small-diameter Cayley graphs for finite simple groups. *European J. Combin.*, 10(6):507–522, 1989.

[3] O. Dinai. Poly-log diameter bounds for some families of finite groups. Master's thesis, Hebrew University, 2004.

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

[5] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics*. Addison Wesley, 2nd edition, 1994.

[6] H. A. Helfgott. Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. `arXiv:math.GR/0509024`, 2005.

[7] W. M. Kantor. Some large trivalent graphs having small diameters. *Discrete Appl. Math.*, 37/38:353–357, 1992.
[8] M. Kassabov. Kazhdan constants for $\mathrm{SL}_n(\mathbb{Z})$. `arXiv:math.GR/0311487`, to appear in Internat. J. Algebra Comput.
[9] M. Larsen. Navigating the Cayley graph of $\mathrm{SL}_2(\mathbb{F}_p)$. *Int. Math. Res. Not.*, 27:1465–1471, 2003.
[10] A. Lubotzky. *Discrete groups, expanding graphs and invariant measures*, volume 125 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1994. With an appendix by J. D. Rogawski.
[11] A. Lubotzky and B. Weiss. Groups and expanders. In *Expanding graphs (Princeton, NJ, 1992)*, volume 10 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 95–109. Amer. Math. Soc., 1993.
[12] N. Nikolov. A product decomposition for the classical quasisimple groups. `arXiv:math.GT/0510173`, 2005.
[13] T. R. Riley. Navigating the Cayley graphs of $\mathrm{SL}_N(\mathbb{Z})$ and $\mathrm{SL}_N(\mathbb{F}_p)$. Preprint, `http://www.math.cornell.edu/~riley/`, to appear in Geometriae Dedicata.
[14] L. N. Vaserstein. Bass's first stable range condition. *J. Pure Appl. Algebra*, 34(2-3):319–330, 1984.
[15] E. Zeckendorf. Représentation des nombres naturel par une somme de nombres Fibonacci ou se nombres de Lucas. *Bulletin de la Société Royale des Liège*, 41:179–182, 1972.

Department of Mathematics, Cornell University, 310 Malott Hall, Ithaca, NY 14853, USA
E-mail address: `kassabov@aya.yale.edu`
E-mail address: `tim.riley@math.cornell.edu`
URL: `http://www.math.cornell.edu/~riley/`