Diameters of Cayley graphs of $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$

Work in collaboration with Martin Kassabov

Barcelona
June 2005

Tim Riley

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

generate $\mathrm{SL}_n(\mathbb{Z})$.

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

generate $\mathrm{SL}_n(\mathbb{Z})$.

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

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

Who cares?

Who cares?

- A. Lubotzky

Who cares?

- A. Lubotzky

Why?

Who cares?

- A. Lubotzky

Why?

- $$\{Cay(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}, \mathcal{B}\}) \mid k \geq 2, n \geq 3\}$$
  is not an expander family.

Who cares?

- A. Lubotzky

Why?

- $$\{Cay(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}, \mathcal{B}\}) \mid k \geq 2, n \geq 3\}$$
  is not an expander family.

- It is a better result than you get using Property (T) and is constructive and efficient.

Who cares?

- A. Lubotzky

Why?

- $$\{Cay(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), \{\mathcal{A}, \mathcal{B}\}) \mid k \geq 2, n \geq 3\}$$
  is not an expander family.

- It is a better result than you get using Property (T) and is constructive and efficient.

- The result is best possible because
  $$|\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})| \sim k^{n^2-1}.$$

Broader Context

Fix $n \geq 3$.

Problem. Does $\mathrm{SL}_n(\mathbb{Z})$ have uniform Property (T)?

Broader Context

Fix $n \geq 3$.

Problem. Does $\mathrm{SL}_n(\mathbb{Z})$ have uniform Property (T)?

Problem. Does there exist $K > 0$ such that for all generating sets X for $\mathrm{SL}_n(\mathbb{Z})$ and all $k \geq 2$

$$\mathrm{Diam}\, Cay(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), X) \;\leq\; K \ln k \;\; ?$$

Broader Context

Fix $n \geq 3$.

Problem. Does $\mathrm{SL}_n(\mathbb{Z})$ have uniform Property (T)?

Problem. Does there exist $K > 0$ such that for all generating sets X for $\mathrm{SL}_n(\mathbb{Z})$ and all $k \geq 2$

$$\mathrm{Diam}\, Cay(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), X) \;\leq\; K \ln k \;\; ?$$

Problem. Give an elementary proof of the result of Gromov that $\mathrm{SL}_3(\mathbb{Z})$ admits an exponential Dehn function.

Broader Context

Fix $n \geq 3$.

Problem. Does $\mathrm{SL}_n(\mathbb{Z})$ have uniform Property (T)?

Problem. Does there exist $K > 0$ such that for all generating sets X for $\mathrm{SL}_n(\mathbb{Z})$ and all $k \geq 2$

$$\mathrm{Diam}\, Cay(\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z}), X) \;\leq\; K \ln k \;\; ?$$

Problem. Give an elementary proof of the result of Gromov that $\mathrm{SL}_3(\mathbb{Z})$ admits an exponential Dehn function.

Problem. Prove Thurston's assertion that $\mathrm{SL}_n(\mathbb{Z})$ admits a quadratic isoperimetric function for all $n \geq 4$.

A *row* (*column*) *matrix* is a square matrix whose diagonal entries are all 1’s and which differs from the identity only in one row (column).

A *row* (*column*) *matrix* is a square 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 $\{0, \pm 1\}$.

A *row* (*column*) *matrix* is a square 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 $i \neq j$ define e_{ij} to be the matrix with entry ij and all diagonal entries 1 and all other entries 0.

Our proof of the theorem has three parts:

I) Using Gaussian elimination, matrices in $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ can be written as a product of n row matrices, n column matrices and n elementary matrices.

Our proof of the theorem has three parts:

I) Using Gaussian elimination, matrices in $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ can be written as a product of n row matrices, n column matrices and n elementary matrices.

IIa) Bit-row and bit-column matrices in $\mathrm{SL}_n(\mathbb{Z})$ can be represented by words on $\mathcal{A}$ and $\mathcal{B}$ of length $< 50n$.

Our proof of the theorem has three parts:

I) Using Gaussian elimination, matrices in $\mathrm{SL}_n(\mathbb{Z}/k\mathbb{Z})$ can be written as a product of n row matrices, n column matrices and n elementary matrices.

IIa) Bit-row and bit-column matrices in $\mathrm{SL}_n(\mathbb{Z})$ can be represented by words on $\mathcal{A}$ and $\mathcal{B}$ of length $< 50n$.

IIb) Row and column matrices in $\mathrm{SL}_n(\mathbb{Z})$ with entries in

$$\{-K+1, \ldots, K-2, K-1\}$$

can be represented by words on $\mathcal{A}$ and $\mathcal{B}$ of length $\leq 1200n \ln K$.

IIa) Generating bit-row and bit-column matrices

For $m_3, \ldots, m_n \in \{0, \pm 1\}$, matrices

$$\begin{pmatrix} 1 & 0 & m_3 & m_4 & m_5 & \cdots & m_n \\ & 1 & & & & & \\ & & 1 & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

can be expressed as $N_1 e_{1\,2} {N_1}^{-1} N_2 e_{1\,2}{}^{-1} {N_2}^{-1}$ where N_1 and N_2 have the form

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

for some $s_2, \ldots, s_{n-1} \in \{0, \pm 1, \pm 2\}$ and $t_2, \ldots, t_{n-2} \in \{0, 1\}$.

Such N_1 and N_2 can be expressed as

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

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

Such N_1 and N_2 can be expressed as

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

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

where

$$Q_i := \mathcal{A}^{-s_i} [\mathcal{A}, \mathcal{B}^{-1} \mathcal{A} \mathcal{B}]^{-t_i} = \begin{pmatrix} 1 & -s_i & -t_i & & \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

and w has length $\leq 12n - 24$ as a word on $\mathcal{A}$ and $\mathcal{B}$.

Then, by fixing up the second entry in row 1 and conjugating by a power of $\mathcal{B}$, we can produce any given bit-row matrix.

A similar proof works for bit-column matrices. Deduce –

Bit-row and bit-column matrices in $\mathrm{SL}_n(\mathbb{Z})$ can be represented by words on $\mathcal{A}$ and $\mathcal{B}$ of length $< 50n$.

IIb) Generating row and column matrices

Fibonacci numbers:

$$F_0=0,\quad F_1 = 1, F_{i+2}=F_{i+1} + F_i.$$

IIb) Generating row and column matrices

Fibonacci numbers:

$$F_0=0,\ \ F_1\ =\ 1, F_{i+2}=F_{i+1}+F_i.$$

Claim. For non-negative integers l,

$$e_{12}^{\,2}(e_{21}e_{12})^{l}e_{13}(e_{21}e_{12})^{-l}e_{12}^{\,-1}(e_{21}e_{12})^{l}e_{13}^{\,-1}(e_{21}e_{12})^{-l}e_{12}^{\,-1},$$

equals $e_{13}^{\,F_{2l}}$ in $\mathrm{SL}_3(\mathbb{Z})$.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{12}{}^2} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^l} \begin{pmatrix} F_{2l+2} & F_{2l+3} & 0 \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{12}{}^2} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^l} \begin{pmatrix} F_{2l+2} & F_{2l+3} & 0 \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} F_{2l+2} & F_{2l+3} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{-l}} \begin{pmatrix} 1 & 2 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{12}{}^{2}} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{l}} \begin{pmatrix} F_{2l+2} & F_{2l+3} & 0 \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} F_{2l+2} & F_{2l+3} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{-l}} \begin{pmatrix} 1 & 2 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{12}{}^{-1}} \begin{pmatrix} 1 & 1 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{l}} \begin{pmatrix} F_{2l+1} & F_{2l+2} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{12}{}^{2}} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{l}} \begin{pmatrix} F_{2l+2} & F_{2l+3} & 0 \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} F_{2l+2} & F_{2l+3} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{-l}} \begin{pmatrix} 1 & 2 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{12}{}^{-1}} \begin{pmatrix} 1 & 1 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{l}} \begin{pmatrix} F_{2l+1} & F_{2l+2} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{13}{}^{-1}} \begin{pmatrix} F_{2l+1} & F_{2l+2} & F_{2l} \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{-l}} \begin{pmatrix} 1 & 1 & F_{2l} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{e_{12}{}^{2}} \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{l}} \begin{pmatrix} F_{2l+2} & F_{2l+3} & 0 \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{13}} \begin{pmatrix} F_{2l+2} & F_{2l+3} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{-l}} \begin{pmatrix} 1 & 2 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{12}{}^{-1}} \begin{pmatrix} 1 & 1 & F_{2l+2} \\ 0 & 1 & F_{2l} \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{l}} \begin{pmatrix} F_{2l+1} & F_{2l+2} & F_{2l+2} \\ F_{2l} & F_{2l+1} & F_{2l} \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{13}{}^{-1}} \begin{pmatrix} F_{2l+1} & F_{2l+2} & F_{2l} \\ F_{2l} & F_{2l+1} & 0 \\ 0 & 0 & 1 \end{pmatrix} \xrightarrow{(e_{21}e_{12})^{-l}} \begin{pmatrix} 1 & 1 & F_{2l} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\xrightarrow{e_{12}{}^{-1}} \begin{pmatrix} 1 & 0 & F_{2l} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Produce $e_{13}{}^{F_{2l+1}}$ similarly.

Produce $e_{13}{}^{F_{2l+1}}$ similarly.

For arbitrary integers $K > 0$ we can write $e_{13}{}^{K}$ as a word of length $\leq \ln K$ on $e_{12}, e_{21}, e_{23}, e_{13}$ by using –

Zeckendorf's Theorem.
Every positive integer K can be expressed as

$$K = F_{k_1} + F_{k_2} + \cdots + F_{k_r},$$

with $k_1 \geq 2$ and $k_{j+1} - k_j \geq 2$ for all $1 \leq j < r$.

Produce $e_{13}{}^{F_{2l+1}}$ similarly.

For arbitrary integers $K > 0$ we can write $e_{13}{}^{K}$ as a word of length $\leq \ln K$ on $e_{12}, e_{21}, e_{23}, e_{13}$ by using –

Zeckendorf's Theorem.
Every positive integer K can be expressed as

$$K = F_{k_1} + F_{k_2} + \cdots + F_{k_r},$$

with $k_1 \geq 2$ and $k_{j+1} - k_j \geq 2$ for all $1 \leq j < r$.

Replacing the e_{13} and e_{23} by bit-row matrices we can build sums of Fibonacci numbers in entries $3, 4, \ldots, n$ of row 1, and hence produce arbitrary row matrices.

Produce arbitrary column matrices similarly.

These methods also yield –

- An upper bound of $O(\log k)$ on the *worst–case non–deterministic* complexity of the subtractive Euclid's algorithm for computing the gcd of $n \geq 3$ integers $(a_1, \ldots, a_n)$, where $k := \max\{|a_1|, \ldots, |a_n|\}$.

These methods also yield –

- An upper bound of $O(\log k)$ on the *worst–case non–deterministic* complexity of the subtractive Euclid's algorithm for computing the gcd of $n \geq 3$ integers $(a_1, \ldots, a_n)$, where $k := \max\{|a_1|, \ldots, |a_n|\}$.

- An elementary, constructive proof of the Mozes–Lubotzky– Raghunathan Theorem for $\mathrm{SL}_n(\mathbb{Z})$ when $n \geq 3$.

These methods also yield –

- An upper bound of $O(\log k)$ on the *worst–case non–deterministic* complexity of the subtractive Euclid's algorithm for computing the gcd of $n \geq 3$ integers $(a_1, \ldots, a_n)$, where $k := \max\{|a_1|, \ldots, |a_n|\}$.

- An elementary, constructive proof of the Mozes–Lubotzky– Raghunathan Theorem for $\mathrm{SL}_n(\mathbb{Z})$ when $n \geq 3$.

- A *normal form* of *linearly bounded length* for $\mathrm{SL}_n(\mathbb{Z})$.