Bounded generation of special linear groups

Dave Witte Morris

Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, AB T1K 3M4
Dave.Morris@uleth.ca

Abstract

We present the main ideas of a nice proof (due to D. Carter, G. Keller, and E. Paige) that every matrix in $SL(3,\mathbb{Z})$ is a product of a bounded number of elementary matrices. The two main ingredients are the Compactness Theorem of first-order logic and calculations of Mennicke symbols. (These symbols were developed in the 1960s in order to prove the Congruence Subgroup Property.) Similar methods apply to $SL(2,A)$ if $A=\mathbb{Z}[\sqrt{2}]$ (or any other ring of integers with infinitely many units).

Thm (Carter-Keller). $SL(3,\mathbb{Z})$ *is boundedly generated by elementary matrices.*

Eg. Elementary matrices:

$$\begin{bmatrix}1&25&0\\0&1&0\\0&0&1\end{bmatrix},\ \begin{bmatrix}1&0&0\\0&1&0\\-8&0&1\end{bmatrix},\ \begin{bmatrix}1&0&0\\0&1&16\\0&0&1\end{bmatrix}.$$

Recall. Every invertible matrix can be reduced to Id by elementary column operations.

Prop. $T\in SL(3,\mathbb{Z}) \Rightarrow T \rightsquigarrow \mathrm{Id}$ *by* $\mathbb{Z}$ *column operations.*

Prop. $T\in SL(3,\mathbb{Z}) \Rightarrow T \rightsquigarrow \mathrm{Id}$ *by* $\mathbb{Z}$ *column operations.*

Eg. $$\begin{bmatrix}13&5\\31&12\end{bmatrix}\rightsquigarrow\begin{bmatrix}3&5\\7&12\end{bmatrix}\rightsquigarrow\begin{bmatrix}3&2\\7&5\end{bmatrix}\rightsquigarrow\begin{bmatrix}1&2\\2&5\end{bmatrix}\rightsquigarrow\begin{bmatrix}1&0\\2&1\end{bmatrix}\rightsquigarrow\begin{bmatrix}1&0\\0&1\end{bmatrix}.$$

Cor. $T\in SL(3,\mathbb{Z}) \Rightarrow T =$ *product of elementary mats.*
I.e., $SL(3,\mathbb{Z})$ is generated by elementary matrices.

Thm (Carter-Keller). $T =$ *prod of* 48 *elem mats.*
So $SL(3,\mathbb{Z})$ is *boundedly* generated by elem mats.

Remark. No such bound exists for $SL(2,\mathbb{Z})$:
$SL(2,\mathbb{Z})$ **not** boundedly generated by elem mats.

Rem. Γ = any group.

Γ has *bounded generation* iff $\exists$ finite $S\subset\Gamma$, integer r,
s.t. $\forall\ \gamma\in\Gamma,\quad \gamma = s_1^{k_1}\, s_2^{k_2}\cdots s_r^{k_r}$.

I.e., $\Gamma = X_1\,X_2\cdots X_r$ with X_i cyclic groups.

Thm (C–K). $\Gamma = SL(3,\mathbb{Z})$ *bddly gen'd by elem mats.*

Consequences.

- Γ is *superrigid* ($<\infty$ irred reps of each dim) [Rapinchuk]
- Γ has the *Congruence Subgroup Property*: $\times_p SL(3,\mathbb{Z}_p)$ is profinite completion of $SL(3,\mathbb{Z})$. [Lubotzky, Platonov-Rapinchuk]
- $SL(3,\mathbb{Z})$ has *Kazhdan's property T* (with explicit ϵ)
  Conjecture. $SL(3,\mathbb{Z}[x])$ has property T. [Shalom]
- Γ has **no** action on $\mathbb{R}$ (nontriv, orient-pres). [Lifschitz-M]

How to prove bounded generation [C-K-P].

- Compactness Thm (1st-order logic) / *ultraproduct*
- Mennicke symbols (Algebraic K-Theory)

Prop. $SL(3,\mathbb{Z})$ *boundedly generated by elem mats*
$\Leftrightarrow SL(3,\mathbb{Z}^\infty)$ *generated by elem mats.*

Proof. ($\Leftarrow$) Contrapos: $\exists\ g_r$, not prod of r elem mats.
In $SL(3,\mathbb{Z})^\infty$, element $(g_r)_{r=1}^\infty$ not prod of elem mats.
So elem mats do not generate $SL(3,\mathbb{Z})^\infty \cong SL(3,\mathbb{Z}^\infty)$.

$\mathbb{Z}^\infty$ is a bad ring (not integral domain): use ${}^*\mathbb{Z} = \mathbb{Z}^\infty/\mathfrak{p}$,
where $\mathfrak{p}$ = prime ideal containing $\{e_1,e_2,\ldots\}$
(and $(x_k)\in\mathfrak{p} \Rightarrow$ some x_k is 0). (${}^*\mathbb{Z}$ = ultraprod)

Prop. $SL(3,\mathbb{Z})$ *boundedly generated by elem mats*
$\Leftrightarrow SL(3,{}^*\mathbb{Z}) \doteq \langle\,\text{elem mats}\,\rangle$ (up to finite index).

Thm (Carter-Keller). $SL(3,\mathbb{Z})$ *bdd gen by elems.*

Prove: $\langle\,\text{elem mats}\,\rangle$ finite index in $SL(3,{}^*\mathbb{Z})$.
Let $C = C_{{}^*\mathbb{Z}} = SL(3,{}^*\mathbb{Z})\ /\ \langle\,\text{elem mats}\,\rangle$. (finite??)

Thm. A *commutative* $\Rightarrow \langle\,\text{elem mats}\,\rangle \lhd SL(3,A)$.
So C is a group. In fact, C is abelian.

Step 1. Exponent of C divides 24 (i.e., $x^{24}=e$).

Step 2. C cyclic. (Any 2 elts are in same cyclic subgrp.)

Recall $C = \mathrm{SL}(3, {}^*\mathbb{Z})/\langle \text{elem mats} \rangle$.

Let $W = W_{^*\mathbb{Z}} = \{ (a,b) \in {}^*\mathbb{Z}^2 \mid a,b \text{ rel prime} \}$
$= \{ \text{1st rows of elements of } \mathrm{SL}(2, {}^*\mathbb{Z}) \}$.

Define $\begin{bmatrix} \ \end{bmatrix} : W \to C$ by $\begin{bmatrix} b \\ a \end{bmatrix} \equiv \begin{bmatrix} a & b & 0 \\ * & * & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

- $\begin{bmatrix} \ \end{bmatrix}$ is well def'd (easy) and onto ("stable range").
- (MS1) $\begin{bmatrix} b+ta \\ a \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = \begin{bmatrix} b \\ a+tb \end{bmatrix}$.
- (MS2a) $\begin{bmatrix} b_1 \\ a \end{bmatrix} \begin{bmatrix} b_2 \\ a \end{bmatrix} = \begin{bmatrix} b_1 b_2 \\ a \end{bmatrix}$ (need $n \geq 3$).

Step 2. Any 2 elts of C are in same cyclic subgrp.

Given $\begin{bmatrix} b_1 \\ a_1 \end{bmatrix}, \begin{bmatrix} b_2 \\ a_2 \end{bmatrix} \in C$ (nontrivial).

Dirichlet: $\exists$ large prime $p \equiv b_1 \pmod{a_1}$.
$\begin{bmatrix} b_1 \\ a_1 \end{bmatrix} = \begin{bmatrix} p \\ a_1 \end{bmatrix}$; we may assume $b_1 = p$ prime.
In fact, wma all a_i, b_i are large primes ($b_1 \neq b_2$).

CRT: $\exists\, q$, s.t. $q \equiv a_i \pmod{b_i}$; wma $a_1 = q = a_2$.

$(\mathbb{Z}/q\mathbb{Z})^\times$ cyclic $\Rightarrow \exists\, b, e_i$, s.t. $b_i \equiv b^{e_i} \pmod{q}$.
$$\begin{bmatrix} b_i \\ a_i \end{bmatrix} = \begin{bmatrix} b_i \\ q \end{bmatrix} = \begin{bmatrix} b^{e_i} \\ q \end{bmatrix} = \begin{bmatrix} b \\ q \end{bmatrix}^{e_i} \in \left\langle \begin{bmatrix} b \\ q \end{bmatrix} \right\rangle.$$

$(\mathbb{Z}/q\mathbb{Z})^\times$ cyclic $\Rightarrow \exists b, e_i$, s.t. $b_i \equiv b^{e_i} \pmod{q}$.
$$\begin{bmatrix} b_i \\ a_i \end{bmatrix} = \begin{bmatrix} b_i \\ q \end{bmatrix} = \begin{bmatrix} b^{e_i} \\ q \end{bmatrix} = \begin{bmatrix} b \\ q \end{bmatrix}^{e_i} \in \left\langle \begin{bmatrix} b \\ q \end{bmatrix} \right\rangle.$$

Note: Since $C^{24} = e$, only need $(\mathbb{Z}/q\mathbb{Z})^\times$ cyclic modulo 24th powers.

This follows from the componentwise calculation:

$(b_i - z^{24})(b_i - bz^{24})(b_i - b^2 z^{24}) \cdots (b_i - b^{23} z^{24})$
is 0 in every coordinate.
So it is 0.

Since ${}^*\mathbb{Z}$ is integral domain, then $b_i = b^{e_i} z^{24}$.

Thm (Liehl). $\mathrm{SL}(2, \mathbb{Z}[1/2])$ *bddly gen'd by elem mats.*
I.e., $T \rightsquigarrow \mathrm{Id}$ by $\mathbb{Z}[1/2]$ col ops, # steps is bdd.

Easy proof. Assume **Artin's Conjecture**.

Eg. 2 is a *primitive root* modulo 13:
$\{2^k\} = \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$.
Complete set of residues.

Conj (Artin). $\forall r \neq \pm 1$, *perfect square,*
$\exists\, \infty$ *primes* q*, s.t.* r *is prim root modulo* q*.*
Assume $\exists q$ in every arith progression $\{a + kb\}$.

Thm (Liehl). $\mathrm{SL}(2, \mathbb{Z}[1/2])$ *bddly gen'd by elem mats.*
I.e., $T \rightsquigarrow \mathrm{Id}$ by $\mathbb{Z}[1/2]$ col ops, # steps is bdd.

Proof. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $\quad q = a + kb$ prime, 2 is prim root

$\rightsquigarrow \begin{bmatrix} q & b \\ * & * \end{bmatrix}$ $\quad 2^\ell \equiv b \pmod{q}$; $2^\ell = b + k'q$

$\rightsquigarrow \begin{bmatrix} q & 2^\ell \\ * & * \end{bmatrix}$ $\quad 2^\ell$ unit $\Rightarrow$ can add *anything* to q

$\rightsquigarrow \begin{bmatrix} 1 & 2^\ell \\ * & * \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 \\ * & 1 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. $\square$

References

H. Bass, *Algebraic K-theory*, Benjamin, New York, 1968.

H. Bass, J. Milnor, and J.-P. Serre, Solution of the Congruence Subgroup Problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), *Inst. Hautes Études Sci. Publ. Math.* 33 (1967), 59–137.

D. Carter and G. Keller, Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$, *Amer. J. Math.* 105 (1983), 673–687.

D. Carter and G. Keller, Elementary expressions for unimodular matrices, *Comm. Algebra* 12 (1984), 379–389.

D. Carter, G. Keller, and E. Paige: Bounded expressions in $\mathrm{SL}(n, A)$, (unpublished).

I. V. Erovenko and A. Rapinchuk, Bounded generation of some S-arithmetic orthogonal groups, *C. R. Acad. Sci. Paris Sér. I Math.* 333 (2001), no. 5, 395–398.

I. V. Erovenko and A. Rapinchuk, Bounded generation of S-arithmetic subgroups of isotropic orthogonal groups over number fields, (preprint).

B. Liehl: Beschränkte Wortlänge in SL_2. *Math. Z.* 186 (1984), no. 4, 509–524.

L. Lifschitz and D. W. Morris: Isotropic nonarchimedean S-arithmetic groups are not left orderable, *C. R. Math. Acad. Sci. Paris* 339 (2004), no. 6, 417–420.

A. Lubotzky: Subgroup growth and congruence subgroups, *Invent. Math.* 119 (1995), no. 2, 267–295.

D. W. Morris: Bounded generation in $\mathrm{SL}(n, A)$ (after D. Carter, G. Keller, and E. Paige) (preprint).
`http://arxiv.org/abs/math/0503083`

V. P. Platonov and A. S. Rapinchuk: Abstract characterizations of arithmetic groups with the congruence property, *Soviet Math. Dokl.* 44 (1992), no. 1, 342–347.

A. S. Rapinchuk: Representations of groups of finite width, *Soviet Math. Dokl.* 42 (1991), no. 3, 816–820.

Y. Shalom: Bounded generation and Kazhdan's property (T), *Inst. Hautes Études Sci. Publ. Math.* No. 90, (1999), 145–168 (2001).

O.I. Tavgen, Bounded generation of Chevalley groups over rings of algebraic S-integers, *Math. USSR-Izv.* 36 (1991), no. 1, 101–128.

O.I. Tavgen, Finite width of arithmetic subgroups of Chevalley groups of rank ≥ 2, *Soviet Math. Dokl.* 41 (1990), no. 1, 136–140.