Efficient bounded generation

Dave Witte Morris
University of Lethbridge, Alberta, Canada
http://people.uleth.ca/~dave.morris
Dave.Morris@uleth.ca

Abstract. A subset X "boundedly generates" a group G if every element g of G is the product of a bounded number of elements of X. This is a very powerful notion in abstract group theory, but geometric group theorists may need the bounded generation to be "efficient," which means that each g can be written as a bounded number of elements of X whose sizes are bounded by a constant times the word length of g. Twenty-five years ago, Lubotzky, Mozes, and Raghunathan observed that $\mathrm{SL}(n,\mathbb{Z})$ is efficiently boundedly generated by the elements of its natural $\mathrm{SL}(2,\mathbb{Z})$ subgroups. We will explain the proof of this result, and discuss a recent generalization to other arithmetic groups. This is joint work with A. Brown, D. Fisher, and S. Hurtado.

Bounded generation

Linear algebra

Subspaces $X_1,\ldots,X_k$ ***span*** V if $V = X_1 + X_2 + \cdots + X_k$.
I.e., $\forall v \in V,\ v = x_1 + x_2 + \cdots + x_k \quad (x_i \in X_i)$.

Group theory

Subgroups $H_1,\ldots,H_k$ ***generate*** G if
$\forall g \in G,\ \exists \ell,\ g = h_1 h_2 \cdots h_\ell \quad (h_i \in H_*)$.

Modern group theory (Rapinchuk 1990)

Subgroups $H_1,\ldots,H_k$ ***boundedly generate*** G if
$\exists \ell,\ \forall g \in G,\ g = h_1 h_2 \cdots h_\ell \quad (h_i \in H_*)$.
I.e., $G = H_1 H_2 \cdots H_{k\ell}$. (subscripts modulo k)

Modern group theory (Rapinchuk 1990)

Subgroups $H_1,\ldots,H_k$ ***boundedly generate*** G if
$G = H_1 H_2 \cdots H_\ell$. (subscripts modulo k)

G is ***boundedly generated*** if it is boundedly generated by cyclic groups: $G = \langle x_1\rangle\langle x_2\rangle\cdots\langle x_\ell\rangle$.

Exer. nonabelian Free groups <u>not</u> bddly gen'd. (Burnside groups)

Exer. $\mathrm{SL}(2,\mathbb{Z})$ is **not** bddly gen'd. (finite-index free subgrp)

Theorem (Carter-Keller 1983)

$\mathrm{SL}(n,\mathbb{Z})$ is bddly gen'd if $n \ge 3$. (*by elementary matrices*)

Theorem (Carter-Keller-Paige 1990's)

$\mathrm{SL}(2,\mathbb{Z}[\sqrt{2}])$ bddly gen'd. [Morgan-Rapinchuk-Sury $\ell \le 9$]

Exer. G bddly gen'd, acts by isometries on X, each cyclic subgrp has a bdd orbit $\Rightarrow$ G has a bdd orbit.

Exer. G bddly gen'd $\Rightarrow$ no ∞-index subgrp intersects every nontrivial subgroup of G nontrivially.

Theorem (Rapinchuk 1990)

*G bddly gen'd $\Rightarrow$ G is **abstractly superrigid**:*
$< \infty$ irred representations of each finite dim'n.
(*unless finite-index subgroup has ∞ abelianization*)

Theorem (Lubotzky, Platonov-Rapinchuk 1991)

G bddly gen'd nonuniform arithmetic group,
*$\Rightarrow$ G has **congruence subgroup property***

Efficient bounded generation

Linear algebra

Subspaces $X_1,\ldots,X_r$ ***span*** V if $\forall v \in V$,
$v = x_1 + x_2 + \cdots + x_k \quad (x_i \in X_i)$.
Can choose x_i with $\|x_i\| \le C\|v\|$.

Geometric group theory

$H_1,\ldots,H_r$ ***efficiently boundedly generate*** G if
$\exists \ell,\ \forall g \in G,\ g = h_1 h_2 \cdots h_\ell \quad (h_i \in H_*)$
<u>and</u> $\boldsymbol{\ell_G(h_i) \le C\,\ell_G(g)}$.

Fix finite gen set S of G. $\ell_G(g) = \min\{\ell \mid g = s_1\cdots s_\ell,\ s_i \in S^{\pm 1}\}$.

Open problem

$\mathrm{SL}(n,\mathbb{Z})$ eff'ly bddly gen'd? (by elem mats)? $(\exists n \ge 3?)$
(Then would be true for all larger n.)

Open problem

$\mathrm{SL}(n,\mathbb{Z})$ eff'ly bddly gen'd? (by elem mats)? $(\exists n \ge 3?)$
(Then would be true for all larger n.)

Theorem (Lubotzky-Mozes-Raghunathan 1993)

$\forall \gamma \in \mathrm{SL}(n,\mathbb{Z}),\quad \ell(\gamma) \asymp \log\|\gamma\|$. $(n \ge 3)$

Prop [L–M–R]. $\exists \ell,\ \forall \gamma \in \mathrm{SL}(n,\mathbb{Z}),\ \gamma = s_1 s_2 \cdots s_\ell$
where s_i *is* 2×2 *and* $\|s_i\| \overset{\text{poly}}{<} \|\gamma\|$.

Defn. γ is $\mathbf{2\times 2}$ if $\gamma = \mathrm{I}$ except
$(i,i),(j,j),(i,j),(j,i)$.

$$\begin{array}{cc} & \begin{matrix} \; & \; & i & \; & \; & j & \; & \; \end{matrix} \\ \begin{matrix} \\ \\ i \\ \\ \\ j \\ \\ \\ \end{matrix} & \begin{bmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && * &&& * && \\ &&& 1 &&&& \\ &&&& 1 &&& \\ && * &&& * && \\ &&&&&& 1 & \\ &&&&&&& 1 \end{bmatrix} \end{array}$$

(For **fixed** i, j, $\cong \mathrm{SL}(2,\mathbb{Z})$)

Prop [L–M–R]. $\exists \ell$, $\forall \gamma \in \mathrm{SL}(n,\mathbb{Z})$, $\gamma = s_1 s_2 \cdots s_\ell$
where s_i *is* 2×2 *and* $\|s_i\| \overset{\text{poly}}{\prec} \|\gamma\|$.

Lemma

$$\forall v = \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{Z}^2, \exists \gamma \in \mathrm{SL}(2,\mathbb{Z}), \gamma v = \begin{bmatrix} + \\ 0 \end{bmatrix}$$

and $\|\gamma\| \overset{\text{poly}}{\prec} \|v\|$.

Proof.

Let $d = \gcd(x,y)$. $\exists a,b \in \mathbb{Z}$, $ax - by = d$.

Let $\gamma = \begin{bmatrix} x/d & b \\ y/d & a \end{bmatrix}^{-1} = \begin{bmatrix} a & -b \\ -y/d & x/d \end{bmatrix}$. □

Exer. Can take $|a| \le |y|$ and $|b| \le |x|$ unless $xy = 0$.

Prop [L–M–R]. $\exists r$, $\forall \gamma \in \mathrm{SL}(n,\mathbb{Z})$, $\gamma = s_1 s_2 \cdots s_\ell$
where s_i *is* 2×2 *and* $\|s_i\| \overset{\text{poly}}{\prec} \|\gamma\|$.

Lem. $\forall v \in \mathbb{Z}^2$, $\exists \gamma \in \mathrm{SL}_2(\mathbb{Z})$, $\gamma v = [\,{}^{+}_{0}\,]$ & $\|\gamma\| \overset{\text{poly}}{\prec} \|v\|$

Proof of bounded generation by 2×2 matrices.

Replace s_i with inverse: we want $s_\ell s_{\ell-1} \cdots s_1 \gamma = I$.

$$\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & * \end{bmatrix} \overset{1,2}{\rightsquigarrow} \begin{bmatrix} + & * & * \\ 0 & * & * \\ * & * & * \end{bmatrix} \overset{1,3}{\rightsquigarrow} \begin{bmatrix} + & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix}$$

$$\overset{2,3}{\rightsquigarrow} \begin{bmatrix} + & * & * \\ 0 & + & * \\ 0 & 0 & * \end{bmatrix} = \begin{bmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{bmatrix} \rightsquigarrow \cdots \rightsquigarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$ □

Theorem (Lubotzky-Mozes-Raghunathan 1993)

$\forall \gamma \in \mathrm{SL}(n,\mathbb{Z})$, $\ell(\gamma) \asymp \log \|\gamma\|$. $(n \ge 3)$

Generalization (L-M-R 2000)

$\mathbf{G}$ = simple algebraic $\mathbb{Q}$-group, $\mathrm{rank}_{\mathbb{R}} \mathbf{G} \ge 2$
$\Rightarrow \forall \gamma \in \mathbf{G}(\mathbb{Z})$, $\ell(\gamma) \asymp \log \|\gamma\|$.

Lem [LMR]. $\mathrm{SL}_n(\mathbb{Z})$ *eff'ly bddly gen'd by* *standard* $\mathrm{SL}_2(\mathbb{Z})$*'s.*

Theorem (Brown-Fisher-Hurtado 2017)

$\mathrm{SL}(n,\mathbb{Z})$ *acts by diffeos on cpct* M, $\dim M < n - 1$
$\Rightarrow$ *action is via a finite group.*

Lem[LMR]. $\mathbf{G}(\mathbb{Z})$ *eff'ly gen'd* by standard* $\mathbb{Q}$*-rank-1 subgrps.*

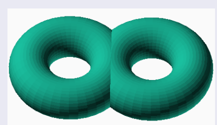
Proposition (Brown-Fisher-Hurtado-Morris 2018$^+$)

$\mathbf{G}(\mathbb{Z})$ *eff'ly bddly gen'd* by standard* $\mathbb{Q}$*-rank-1 subgrps.*

Definition

$\mathbb{Q}$-rank Γ = dim(far-away view of G/Γ)

G/Γ compact



$\mathbb{Q}$-rank Γ $= \dim(\cdot)$ $= 0$

G/Γ has cusps

$\mathbb{Q}$-rank Γ $= \dim(\succ)$ $= 1$

G/Γ worse

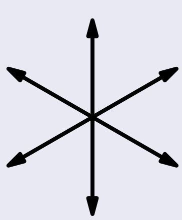
$\mathbb{Q}$-rank Γ $= \dim(\blacktriangleleft)$ > 1

Proposition (Brown-Fisher-Hurtado-Morris 2018$^+$)

$\mathbf{G}(\mathbb{Z})$ *eff'ly bddly gen'd* by standard* $\mathbb{Q}$*-rank-1 subgrps.*

$$\begin{bmatrix} * & * & * \\ * & * & * \\ * & * & * \end{bmatrix} \overset{1,2}{\rightsquigarrow} \begin{bmatrix} + & * & * \\ 0 & * & * \\ * & * & * \end{bmatrix} \overset{1,3}{\rightsquigarrow} \begin{bmatrix} + & * & * \\ 0 & * & * \\ 0 & * & * \end{bmatrix} \overset{2,3}{\rightsquigarrow} \begin{bmatrix} + & * & * \\ 0 & + & * \\ 0 & 0 & * \end{bmatrix}$$

Place to zero-out = $\mathbb{Q}$-***root*** α.
Bruhat decomp: $\gamma = u_1 u_2 \cdots u_r p$
$u_i \in \mathbf{G}_{\alpha_i}(\mathbb{Q})$, p upper triangular.



standard $\mathbb{Q}$-rank-1 subgroup
$= \langle \mathbf{G}_{\alpha,2\alpha}, \mathbf{G}_{-\alpha,-2\alpha} \rangle = \mathbf{G}_{\pm\alpha}$

Use $\mathbf{G}_{\pm\alpha}(\mathbb{Z})$ to zero-out the root α.

Use $\mathbf{G}_{\pm\alpha}(\mathbb{Z})$ to zero-out the root α.

$\gamma = u_\alpha u_\beta \cdots u_\zeta\, p$ $\quad \mathbf{G}_{\pm\alpha} = \langle \mathbf{G}_{\alpha,2\alpha}, \mathbf{G}_{\alpha,-2\alpha} \rangle$

$\mathbf{G}_{\pm\alpha}(\mathbb{Q}) = \mathbf{G}_{\pm\alpha}(\mathbb{Z})\, F\, \mathbf{P}_\alpha(\mathbb{Q})$.
F is a **finite** subset of $\mathbf{G}_\alpha(\mathbb{Q})$ (Reduction theory)

$u_\alpha = \gamma_\alpha\, f\, p_\alpha$

Multiply by γ_α^{-1} to annihilate u_α:
$\gamma_\alpha^{-1} \gamma = f \quad u_\beta{}' \cdots u_\zeta{}'\, p'$
Annihilate u_β' with element of $f\, \mathbf{G}_{\pm\beta}(\mathbb{Z})\, f^{-1}$.

Conjugate by elements of a finite set, so still have a finite collection of standard $\mathbb{Q}$-rank-1 subgroups.

Efficient [L-M-R]: $\|\gamma_\alpha\| \overset{\text{poly}}{\prec} \|u_\alpha\| + \mathrm{denom}(u_\alpha) \overset{\text{poly}}{\prec} \|\gamma\|$.

References

A. Lubotzky, S. Mozes, and M. S. Raghunathan:
Cyclic subgroups of exponential growth
and metrics on discrete groups.
C. R. Acad. Sci. Paris 317 (1993) 735–740.
MR 1244421

A. Lubotzky, S. Mozes, and M. S. Raghunathan:
The word and Riemannian metrics on lattices of semisimple groups.
Inst. Hautes Études Sci. Publ. Math. 91 (2000) 5-53.
MR 1828742

Bounded generation

A. S. Rapinchuk: Congruence subgroup problem for algebraic groups: old and new.
Astérisque 209 (1992) 73–84. MR 1211004

A. S. Rapinchuk: Representations of groups of finite width, *Soviet Math. Dokl.* 42 (1991) 816–820.
MR 1099467

A. V. Morgan, A. S. Rapinchuk, and B. Sury: Bounded generation of SL_2 over rings of S-integers with infinitely many units.
`https://arxiv.org/abs/1708.09262`

Wikipedia: “boundedly generated group"