Groups with bounded generation: properties and examples

I will give a brief survey of groups with bounded generation, referring for more details to the talk I gave in the Number Theory seminar last May – the recording is available. Then I would to show you a couple of proofs. First, we will show that $SL_n(\mathbb{Z})$, $n \geq 3$, has bounded generation by showing that every unimodular integer matrix is a bounded product of elementary matrices (Carter-Keller, 1983). One may expect this property to be true for SL_n, $n \geq 3$ over arbitrary Euclidean rings, but this is not the case (v.d. Kallen, 1982). This result is by far less known than the result of Carter-Keller, so I'll give a sketch of the argument. Time permitting, I'll speak about another technique for proving bounded generation of arithmetic subgroups of groups of classical types developed in a joint work with my former student Erovenko. In 2 weeks, Jinbo Ren will tell about a recent joint result of ours with P. Corvaja and U. Zannier

Recall the following

Definition An abstract group Γ has bounded generation if there exist elements $\gamma_1, \ldots, \gamma_d \in \Gamma$ (not necessarily distinct) such that $\Gamma = \langle\gamma_1\rangle \cdots \langle\gamma_d\rangle$, where $\langle\gamma_i\rangle$ is the cyclic subgroup generated by γ_i.

We have already seen that this property is helpful for analyzing the first-order rigidity but in fact it has many more application. But initially our interest to (BG) was stimulated by two consequences, for SS-rigidity and the congruence subgroup property.

SS-rigidity. A group Γ is said to be SS-rigid if it has only finitely many inequivalent completely reducible complex representations $\rho: \Gamma \to GL_d(\mathbb{C})$ in each dimension d.

If Γ is finitely generated, one can consider the character variety $X_d(\Gamma)$, and then Γ is SS-rigid iff dim $X_d(\Gamma) = 0$ for all d.

Examples of such groups are not easy to find, and typically the justification of SS-rigidity relies on such results as Margulis's Superrigidity. On the other hand, we have the following "abstract" result.

<u>Theorem</u> (R, 1951?) Let Γ be a group with (BG). Assume that Γ also satisfies the following condition

(F^{ab}) every subgroup of finite index $\Gamma_1 \subset \Gamma$, has <u>finite</u> abelianization $\Gamma_1^{ab} = \Gamma_1 / [\Gamma_1, \Gamma_1]$

Then Γ is SS-rigid.

(We should note that (F^{ab}) is necessary for Γ to be SS-rigid. Also, we actually use a weaker property of profinite BG for the profinite completion $\hat{\Gamma}$)

Another application has to do with the congruence subgroup problem. Let G an absolutely almost simple algebraic group over a number field K, S be a set of places of K containing all archimedean places, and $\mathcal{O}(S)$ be the ring of S-integers, $\Gamma = G(\mathcal{O}(S))$ be the corresponding S-arithmetic subgroup. We are interested in the congruence subgroup problem for Γ, which amounts to the computation of the congruence kernel $C = C^S(G)$ (simply connected)...

<u>Theorem</u> (Lubotzky, Platonov-R, 1992) If Γ has (BG), then C is finite.

At that time we felt that (BG) could be a uniform approach to the CSP, particularly since there was word from F. Grunewald that using the computer he was able to verify (BG) for some quaternionic groups - which was and still is one of the open cases in the CSP. Jinbo will tell us next time what we know about (BG) of quaternionic groups now.

Other applications ~~were~~ of (BG) ~~where~~ were found over the years. Let me just mention that Shalom - Willis used (BG) to prove some cases in the Margulis - Zimmer conjecture. (BG) was also used to estimate Kazhdan constants etc.

Of course, these nice properties of groups with (BG) raise the question of what groups actually do have (BG)? Historically, the first result on (BG) was obtained even before the formal definition was given. More precisely, it was shown by Carter and Keller that every matrix in $SL_n(\mathbb{Z})$, $n \geq 3$, is a product of a bounded number of elementaries, which immediately implies (BG). (We note that this property fails for $n=2$, but is true for $SL_n(\mathcal{O})$, $n \geq 3$, for any ring of algebraic S-integers $\mathcal{O}$, and also for $SL_2(\mathcal{O})$ if the group of units $\mathcal{O}^\times$ is infinite)

Let us now sketch the argument for bounded generation of $SL_n(\mathbb{Z})$, $n \geq 3$, by elementaries.

- An elementary argument shows that any $A \in SL_n(\mathbb{Z})$ can be reduced to $\begin{pmatrix} a & b & \\ c & d & \\ & & I_{n-2} \end{pmatrix}$ by $\leq \frac{1}{2}(3n^2 - n)$ elementary operations. So, it is enough to show that $\begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix} \Longrightarrow I_3$ by a bounded number of elementary transformations.

- the proof uses the bounded multiplicativity of Menniche symbols: for any $l>0$

$$\begin{pmatrix} a & b & \\ * & * & \\ & & 1 \end{pmatrix}^{l} \Rightarrow \begin{pmatrix} a^{l} & b & \\ * & * & \\ & & 1 \end{pmatrix}$$

by 16 ellementory operation:

- Effect of one elementory operation

$$\begin{pmatrix} a & b & \\ c & d & \\ & & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} a & b+ta & \\ c & d+tc & \\ & & 1 \end{pmatrix}$$

So, using Dirichlet's prime Number theorem, we can assume that $b = p$ is a prime. In fact, applying Dirichlet's theorem twice, we can assume that

$$A = \begin{pmatrix} u & p & \\ q & v & \\ & & 1 \end{pmatrix}$$ with p, q odd primes and g.c.d. $\left(\frac{p-1}{2}, \frac{q-1}{2}\right) = 1$

Find $m, n > 0$ such that

$$m \cdot \frac{p-1}{2} - n \cdot \frac{q-1}{2} = \pm 1$$

$$s = m \cdot \frac{p-1}{2}, \quad t = n \cdot \frac{q-1}{2}$$

~~We have~~

- We have $u^{s} \equiv \pm 1 \pmod{p}$, so

$$A^{s} \xRightarrow{16} \begin{pmatrix} u^{s} & p & \\ * & * & \\ & & 1 \end{pmatrix} \xRightarrow{1} \begin{pmatrix} \pm 1 & p & \\ * & * & \\ & & 1 \end{pmatrix},$$

which is a bounded product of elementaries. So, A^{s} is a bounded product of elementaries

- Taking the transpose of A and using the same argument, we find that

A^t is also a bounded product of elementaries. Then $A^{\pm 1} = (A^t)(A^t)^{-1}$ is a bounded product of elementaries.

While this argument does use some number-theoretic results, one may wonder if bounded generation by elementaries can be established, say, over any Euclidean ring.

Theorem (van der Kallen, 1982). There is no N such that every matrix $A \in SL_n(\mathbb{C}[x])$, where $n \geq 3$, is a product of $\leq N$ elementaries.

The proof is based on properties of ~~the~~ K_2-functor, so let us recall the necessary definitions.

Let R be a commutative ring. We then have natural embeddings $GL_n(R) \to GL_{n+1}(R)$, $A \to \left(\begin{array}{c|c} A & \begin{matrix}0\\0\end{matrix} \\ \hline 0\cdot 0 & 1\end{array}\right)$

We can consider the direct system

$$GL_2(R) \hookrightarrow GL_3(R) \hookrightarrow \dots$$

and we let $GL(R) = \varinjlim GL_n(R)$. Furthermore, for each n, we consider the subgroup $E_n(R)$ generated by all elementary matrices $e_{ij}(\lambda) = \begin{pmatrix}1 & & \alpha\\ & \ddots & \\ & & 1\end{pmatrix}$, $i \neq j$, $\lambda \in R$. Clearly, under the standard embedding $E_n(R)$ is mapped to $E_{n+1}(R)$, and we let $E(R) = \varinjlim E_n(R)$.

Whitehead's Lemma. $E(R) = [GL(R), GL(R)]$ and $E(R) = [E(R), E(R)]$.

Then one defines $K_1(R) = GL(R)/E(R)$ (abelian group). Next, since $E(R)$ is perfect, $E(R) = [E(R), E(R)]$, $E(R)$ has a universal central extension, which is called the Steinberg group $\pi: St(R) \to E(R)$. Then $\ker \pi = K_2(R)$. (In other words, $K_2(R)$ is the Schur multiplier of $E(R)$).

The group $St(R)$ has a more constructive description. Recall that elementary matrices satisfy the following relations ($[a,b] = aba^{-1}b^{-1}$)

$$[e_{ij}(\lambda), e_{kl}(\mu)] = \begin{cases} 1, & j \neq k \text{ and } i \neq l \\ e_{il}(\lambda\mu), & j = k \text{ and } i \neq l \\ e_{kj}(-\mu\lambda), & i = l \text{ and } j \neq k. \end{cases}$$

(Recall that $E(R) = \langle e_{ij}(\lambda) \mid i \neq j, \lambda \in R \rangle$).

Then $St(R)$ can be described as the group generated by $\tilde{e}_{ij}(\lambda)$ $\forall i \neq j$, $\lambda \in R$, subject to the following relations:

$$(1)\quad \tilde{e}_{ij}(\lambda)\,\tilde{e}_{ij}(\mu) = \tilde{e}_{ij}(\lambda+\mu)$$

$$(2)\quad [\tilde{e}_{ij}(\lambda), \tilde{e}_{kl}(\mu)] = \begin{cases} 1, & j \neq k \text{ and } i \neq l \\ \tilde{e}_{il}(\lambda\mu), & j \neq k \text{ and } i \neq l \\ \tilde{e}_{kj}(-\mu\lambda) \end{cases}$$

Then the homomorphism (u.c.e.) $\pi: St(R) \to E(R)$ carries $\tilde{e}_{ij}(\lambda)$ to $e_{ij}(\lambda)$. It is easy to see that the definition ~~of~~ description of $St(R)$ is functorial with respect to ring homomorphisms, implying that $K_2(R)$ is also functorial with respect to ring homomorphisms.

In K-theory, there are various stability results. Namely, $K_i(R)$ for $i=1,2$ were defined using infinite dimensional groups $GL(R) \supset E(R)$, but it turns out that in certain situations one ~~can~~ say that for n sufficiently large we have $E_n(R) \triangleleft GL_n(R)$ and $K_{1,n} = GL_n(R)/E_n(R)$ is naturally isomorphic to $K_1(R) = GL(R)/E(R)$. For example, this is the case when R is a commutative Noetherian ring having finite Krull dimension d and $n \geq d+3$ if $d>1$ and $n=3$ if $d=1$. In the context of K_2, again the stability holds if $n \geq d+3$ (van der Kallen, 1976).

If stability holds, then we will freely switch between "finite-dimensional" and "infinite-dimensional" groups. Here ~~[illegible]~~ for $n \geq 3$ we define $St_n(R)$ as the group generated by $\tilde{e}_{ij}(\lambda)$ for $i,j \in \{1,\dots,n\}$, $i \neq j$ and $\lambda \in R$, $\pi_n: St_n(R) \to E_n(R)$ sends $\tilde{e}_{ij}(\lambda)$ to $e_{ij}(\lambda)$, and $K_{2,n}(R) = \ker \pi_n$.

Next, we need to introduce special elements in $K_2(R)$ (that actually come from $K_{2,3}(R)$), called symbols. In general, to construct elements of $K_2(R)$, it is enough to take two commuting elements $a, b \in E(R)$, take arbitrary lifts $\tilde{a} \in \pi^{-1}(a)$, $\tilde{b} \in \pi^{-1}(b)$ and consider their commutator $[\tilde{a}, \tilde{b}] \in K_2(R)$, which depends only on a, b but not on the choice of lifts. Let us apply this construction tr

$$h_{12}(u) = \begin{pmatrix} u & & \\ & u^{-1} & \\ & & 1 \end{pmatrix} \quad \text{and} \quad h_{13}(v) = \begin{pmatrix} v & & \\ & 1 & \\ & & v^{-1} \end{pmatrix}$$

$u, v \in R^{\times}$.

Definition. The element

$$[\widetilde{h_{12}(u)}, \widetilde{h_{13}(v)}] = \{u, v\} \in K_2(R)$$

is called the (Steinberg) symbol.

One can think of the symbol as a map $R^{\times} \times R^{\times} \xrightarrow{\{,\}} K_2(R)$

It satisfies the following properties:

(1) it is bimultiplicative and skew-symmetric

(2) $\{u, -u\} = 1 \quad \forall u \in R^{\times}$

(3) $\{u, 1-u\}$ if $u, 1-u \in R^{\times}$.

We introduced symbols as commutators, but they can also be defined as cocycles. For this we need to describe a canonical way to lift diagonal matrices.

Namely, for any $u \in R^{\times}$, we have

$$w_{12}(u) = e_{12}(u)\, e_{21}(-u^{-1})\, e_{12}(u) = \begin{pmatrix} 0 & u \\ -u^{-1} & 0 \end{pmatrix}$$

$$h_{12}(u) = w_{12}(u)\, w_{12}(-1) = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$$

Mimicking these formulas, we define the following elements in the Steinberg group, which provide canonical lifts (for any $i \neq j$ and any $u \in R^{\times}$)

$$\tilde{w}_{ij}(u) = \tilde{e}_{ij}(u)\,\tilde{e}_{ij}(-u^{-1})\,\tilde{e}_{ij}(u)$$

$$\tilde{h}_{ij}(u) = \tilde{w}_{ij}(u)\,\tilde{w}_{ij}(-1)$$

Then one shows that

$$\tilde{h}_{ij}(uv) = \tilde{h}_{ij}(u)\cdot\tilde{h}_{ij}(v)\cdot\{u,v\}$$

Thus, if H_{ij} is the subgroup of $E(R)$ formed by $h_{ij}(u)$ with $u \in R^{\times}$, then $\{*,*\}$ is a cocycle corresponding to the central extension

$$1 \to K_2(R) \to \pi^{-1}(H_{ij}) \xrightarrow{\pi} H_{ij} \to 1$$

<u>Theorem 1.</u> (Matsumoto) Let F be a field. Then $K_2(F)$ is generated by the symbols $\{u,v\}$, $u,v \in F^{\times}$, and all relations between these symbols are consequences of the following relations

(1) bimultiplicativity;

(2) $\{x, 1-x\} = 1 \quad \forall x \in F \setminus \{0,1\}$

Thus,

$$K_2(F) = F \otimes_{\mathbb{Z}} F / \langle x \otimes (1-x) \mid x \in F \setminus \{0,1\} \rangle.$$

Required results from K-theory

<u>Proposition 1.</u> Let F be a field, $n \geq 3$. There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that if $X \in K_{2,n}(F)$ is a product of $\leq N$ generators $\tilde{e}_{ij}(\lambda)$, $i,j \in \{1,\dots,n\}$, $i \neq j$, $\lambda \in F$, then X is a product of $\leq f(N)$ Steinberg symbols.

This follows from the construction of Bruhat decomposition in $St_n(F)$ in Milnor's book. The way it works is that if we know the Bruhat decomposition of $z \in St_n(F)$, then the process shows how to construct the Bruhat decomposition of $z\tilde{e}_{ij}(\lambda)$.

Theorem 2. Let $\mathbb{F}$ be a field. Then the natural embedding $\mathbb{F} \hookrightarrow \mathbb{F}[x]$ induces an isomorphism $K_2(\mathbb{F}) \simeq K_2(\mathbb{F}[x])$.

Theorem 3. Let $\mathbb{F}$ be a field having infinite transcendence degree over its prime subfield. Then $K_2(\mathbb{F})$ does not have bounded generation with respect to the Steinberg symbols.

Proof of van der Kallen's theorem.

First, we note that for any $a \in \mathbb{F}$, one can consider the evaluation homomorphism $\mathcal{E}_a : \mathbb{F}[x] \to \mathbb{F}$, which induces a homomorphism

$$\mathcal{E}_a^* : St_n(\mathbb{F}[x]) \longrightarrow St_n(\mathbb{F})$$

such that if $A = \prod \tilde{e}_{ij}(\lambda)$ then $\mathcal{E}_a^*(A) = \prod \tilde{e}_{ij}(\mathcal{E}_a(\lambda))$.

We will also write $A(a) \in St_n(\mathbb{F})$ for $\mathcal{E}_a^*(A)$.

For $s \in \mathbb{F}^\times$, we consider the following matrix

$$A_s(x) = e_{12}(s)\, e_{21}(s^{-1}(x-1))\, e_{12}(s)\ e_{12}(-1)\, e_{21}(1-x)\, e_{12}(-1) \in SL_n(\mathbb{F}[x])$$

Let $\tilde{A}_s(x)$ be its canonical lift to $St_n(\mathbb{F}[x])$, i.e

$$\tilde{A}_s(x) = \tilde{e}_{12}(s)\, \tilde{e}_{21}(s^{-1}(x-1)) \cdots$$

Then $\tilde{A}_s(0) = \tilde{w}_{12}(s)\, \tilde{w}_{12}(-1) = \tilde{h}_{12}(s)$, and

$$\tilde{A}_s(1) = \tilde{e}_{12}(2(s-1)).$$

Next, for $s, t \in \mathbb{F}^\times$ consider

$$B_{s,t}(x) = A_{st}(x)\, A_t(x)^{-1}\, A_s(x)^{-1},$$

and its canonical lift

$$\tilde{B}_{s,t}(x) = \tilde{A}_{st}(x)\, \tilde{A}_t(x)^{-1}\, \tilde{A}_s(x)^{-1}.$$

Then $\tilde{B}_{s,t}(0) = \tilde{h}_{12}(st)\, \tilde{h}_{12}^{-1}(t)\, \tilde{h}_{12}^{-1}(s) = \{s,t\}$,

and $\tilde{B}_{s,t}(1) = \tilde{e}_{12}(2(s-1)(t-1))$

By Theorem 3, for each $m \geq 1$, we can find $2m$ elements

$$s_1, t_1, \dots, s_m, t_m \in \mathbb{F}^\times$$

such that the product $\{s_1, t_1\} \cdots \{s_m, t_m\}$ cannot be expressed as a product of $< m$ Steinberg symbols. Set

$$C_m(x) = \prod_{j=1}^{m} B_{s_j, t_j}(x)$$

<u>Proposition 2.</u> There is no N such that $C_m(x)$ can be expressed as a product of $\leq N$ elementaries for all m.

<u>Proof.</u> Let

$$\tilde{C}_m(x) = \prod_{j=1}^{m} \tilde{B}_{s_j, t_j}(x)$$

be the canonical lift of $C_m(x)$ to $\mathrm{St}_n(\mathbb{F}[x])$.

Then

$$\tilde{C}_m(0) = \prod_{j=1}^{m} \{s_j, t_j\} \quad \text{and} \quad \hat{C}_m(1) = \tilde{e}_{12}(2((s_1-1)(t_1-1)+\dots))$$

On the other hand, suppose

$$C_m = u_1(x) \cdots u_N(x)$$

where $u_1, \dots, u_N$ are elementaries. Then

$$\tilde{C}_m(x) = s(x) \cdot \tilde{u}_1(x) \cdots \tilde{u}_N(x),$$

where $s(x) \in K_2(\mathbb{F}[x])$. But by Theorem 2, $K_2(\mathbb{F}[x]) = K_2(\mathbb{F})$ (in fact, by stability $K_{2,n}(\mathbb{F}[x]) = K_{2,n}(\mathbb{F})$ for $n \geq 4$), i.e. $s(x)$ is a product of $\tilde{e}_{ij}(\lambda)$ with $\lambda \in \mathbb{F}$. This implies that $s(a)$ is independent of $a \in \mathbb{F}$. As a consequence, we obtain that

$$\tilde{C}_m(1)^{-1} \tilde{C}_m(0) = \tilde{u}_N(1)^{-1} \cdots \tilde{u}_1(1)^{-1} \tilde{u}_1(0) \cdots \tilde{u}_N(0)$$

On the other hand, $\tilde{C}_m(1)^{-1} \tilde{C}_m(0) = \tilde{e}_{12}(2((s_1-1)(t_1-1)+\dots))^{-1}$

$$\times \prod_{j=1}^{m} \{s_j, t_j\}$$

Thus, $\prod_{j=1}^{m}\{s_j, t_j\}$ is a product of $\le 2N+1$ elementaries. By Proposition 1, this means that $\prod_{j=1}^{m}\{s_j, t_j\}$ is a product of $f(2N+1)$ symbols So, we obtain a contradiction by letting $m \to \infty$.

(Erovenko, R.)

Theorem. Let K be a number field, S be a finite set of places of K containing all archimedean ones, q be a nondegenerate quadratic form of dimension $n \geq 5$. Assume that either the Witt index of q is ≥ 2 or it is 1 and S contains a nonarchimedean place. Then for $G = SO_n(q)$, the S-arithmetic group $\Gamma = G_{\mathcal{O}(S)}$ has (BG).

We will outline the idea of the proof when the Witt index of q is ≥ 2, so one can choose a basis $e_1, e_2, \dots, e_n$ in K^n in which the form looks as follows

$$q(x_1, \dots, x_n) = 2x_1x_2 + 2x_3x_4 + a_5x_5^2 + \dots + a_nx_n^2.$$

The proof goes by induction on n. If $n = 5$, then the group is split, and (BG) is a result of Tavgen. To do the induction step, we take $a = e_{n-1}$, $b = e_n$, and let $G(a)$, $G(b)$ denote the corresponding stabilizers. One basically proves that one can choose a finite set of places V and a V-adically open set U such that $G_{\mathcal{O}(S)} \cap U$ is contained in a bounded product of the groups $G(a)_{\mathcal{O}(S)}$ and $G(b)_{\mathcal{O}(S)}$ which by induction have (BG). This is sufficient for (BG) for $G_{\mathcal{O}(S)}$. "Basically" means that in the argument we need to pass to the simply connected group since the argument

Overall, the argument is rather technical, so in order to explain the idea, I will show you the corresponding statement for rational (rather than S-integral) points.

Proposition. Let $a, b \in K^n$ be two orthogonal anisotropic vectors. Assume that $n \geq 5$ and that $\langle a, b\rangle^{\perp}$ is isotropic. Then for $G = SO_n(q)$ we have

$$G_K = G(a)_K \, G(b)_K \, G(a)_K.$$

Proof. First, let us analyze the situation. Recall that given anisotropic $c, d \in K^n$, by Witt's theorem $\exists\, g \in G$ such that $g(c) = d \Leftrightarrow q(c) = q(d)$. Also by Witt's Theorem, if we want to find such $g \in G(a)$, we need one more condition:

$$(c|a) = (d|a),$$

where $(\,|\,)$ is the corresponding bilinear form.

Now, suppose g $\in G_K$ $= xyz$, with $x, z \in G(a)$, $y \in G(b)$. Then $g(a) = xy(a)$. Let $y(a) = t$. We want $x \in G(a)$ such that $g(a) = x(t)$. As we pointed out above, for this we need the condition

$$(t|a) = (g(a)|a) \quad (\text{in addition to } q(t) = q(a)$$

Next, we want $y \in G(b)$ such that $y(a) = t$. For this we need the condition

$$(t|b) = (a|b)$$

This prompts the following construction

Let $Y = \{ t \mid q(t) = q(a) \}$ be the corresponding "sphere".

Set $Z = \left\{ (g,t) \in G \times Y \;\middle|\; \begin{array}{l} (t|a) = (g(a)|a) \\ (t|b) = (a|b) \end{array} \right\}$

Then we factor the product map $\mu : G(a) \times G(b) \times G(a) \to G$ as $\mu = \psi \circ \varphi$ where

$\varphi : G(a) \times G(b) \times G(a) \to Z$ $(x, y, z) \mapsto (xyz, y(a))$

$\psi : Z \to G$, $(g, t) \mapsto g$.

The fact that $\langle a, b \rangle^{\perp}$ is isotropic immediately implies that for any $g \in G_K$, the fiber $\psi^{-1}(g)_K \neq \emptyset$. (Assuming that $t \neq \pm a$, $g(a) \neq \pm a$)

Let $(g, t) \in \psi^{-1}(g)_K$. because of the condition $(t|a) = (g(a)|a)$, by Witt's theorem we can find $x \in G(a)_K$ such that $x(t) = g(a)$. Similarly, because of condition $(t|b) = (a|b)$, we can find $y \in G(b)_K$ such that $t = y(a)$. Then $g(a) = xy(a)$, so $z := (xy)^{-1} g \in G(a)_K$ and $g = xyz$ as required.

Remark. To handle the case where the Witt index is 1, it is more convenient to consider factorizations of the form $G_K = G(a)_K \, G(b)_K \, G(a)_K \, G(b)_K$ into four factors.