MICHAEL COWLING - BRIAN DOROFAEFF
School of Mathematics, University of New South Wales

RANDOM SUBGROUPS OF LIE GROUPS

Conferenza tenuta l'8 settembre 1997

SUNTO. Si esaminano i sottogruppi di gruppi di Lie semisemplici con due generatori casuali.

In recent years, attention has been paid to the structure of random subgroups of finite groups—see, e.g., [4]. Bill Kantor, one of the protagonists of this investigation, asked what can be said about random subgroups of Lie groups. This paper presents some answers to Kantor's question. We consider subgroups $\langle x, y \rangle$ generated by two randomly chosen elements x and y of a semisimple algebraic group G, under the hypothesis that x and y are chosen with a sufficiently continuous probability distribution. We shall see that:

- the subgroup $\langle x, y \rangle$ is almost surely free
- the subgroup $\langle x, y \rangle$ is almost surely Zariski-dense
- if the probability density is highly concentrated, then $\langle x, y \rangle$ is almost surely dense (in the usual topology)
- if the probability density is highly diffuse, then $\langle x, y \rangle$ is probably discrete (in the usual topology).

We now make the working hypotheses more precise. Let G be a connected semisimple algebraic subgroup of $GL(n, \mathbb{C})$, with Lie algebra $\mathfrak{g}$. We denote by G_0 a real form of G (i.e., the fixed-point set a conjugate analytic involutive automorphism of G) and by $\mathfrak{g}_0$ its Lie algebra. Then $(\mathfrak{g}_0)_{\mathbb{C}} = \mathfrak{g}$. The connected component of the identity of G_0 is denoted G_e.

Let ν be a Borel probability measure on $G \times G$, supported in $G_e \times G_e$.* We shall assume that, if V is any algebraic subvariety of $G \times G$, other than $G \times G$ itself, then $\nu(V) = 0$. Let ω and Γ_ω denote the random variable in $G \times G$ with law ν and the subgroup $\langle x, y \rangle$, where $\omega = (x, y)$.

*We can also deal with the case where ν is supported in $G_0 \times G_0$, but the statements become more complicated. Similarly, we can also extend our arguments to deal with reductive G, but in the interest of simplicity we do not do this here in detail.

This note owes much to H. Furstenberg, G. Lehrer, W. Neumann, and R.J. Zimmer, who offered useful comments about preliminary versions of this material.

1 Freedom of random subgroups

Theorem 1.1 *With probability* 1, Γ_ω *is free.*

Proof. Let W denote the set of nontrivial finite reduced words in x, y, x^{-1} and y^{-1}. Each w in W gives rise to an algebraic subvariety V_w of $G \times G$. By Tits' theorem [5], G contains a free subgroup, so each subvariety V_w is a proper subvariety of $G \times G$. Thus $\nu(V_w) = 0$ for each w in W, so $\nu(\cup_{w \in W} V_w) = 0$, and Γ_ω is almost surely free. ▭

This sort of argument goes back at least as far as S. Balcerzyk and J. Mycielski [2]. It extends *verbatim* to the (nonabelian) reductive case.

2 Zariski-denseness of random subgroups

Theorem 2.1 *With probability* 1, Γ_ω *is Zariski-dense in* G.

Proof. We give details for the case where $G = SL(n, C)$. The general case is similar.

The key is the fact that the set

$$\{(x, y) \in G \times G : \langle x, y\rangle \text{ is not Zariski-dense in } G\}$$

is a proper closed subvariety $G \times G$. Indeed, if x is regular (i.e., the eigenspaces of $\mathrm{Ad}(x)$ associated to nonzero eigenvalues all have dimension 1, and the eigenspace associated to the eigenvalue zero is of minimal dimension), which is a probability one occurrence, and $\langle x, y\rangle$ is not Zariski-dense, then there is a parabolic subgroup of G containing both x and y, i.e., there exists k such that, in an appropriate basis,

$$x_{ij} = y_{ij} = 0 \qquad 1 \le i \le k,\ k + 1 \le j \le n.$$

In this case, the dimension of the linear span of the set L, given by

$$L = \{x, x^2, \dots, x^{n-1}\} \cup \{y, xyx^{-1}, x^2yx^{-2}, \dots, x^{n^2-n}yx^{n-n^2}\},$$

in the space of $n \times n$ matrices is less then n^2. On the other hand, if x is chosen in G such that $\mathrm{Ad}(x)$ has $n^2 - n + 1$ distinct eigenvalues (the maximal number), then "most" y in G have the property that the dimension of the linear span of the above set is exactly n^2.

For the argument in the general semisimple case, see Tits [5]. ▭

Mutatis mutandis, this extends easily to the reductive case.

3 Structure of Zariski-dense subgroups

Lemma 3.1 *Let H be a Zariski-dense subgroup of G, contained in the real form G_0. Let $\mathfrak{h}$ be the Lie algebra of the (usual) closure of H in G_0. Then $\mathfrak{h}$ is an ideal in $\mathfrak{g}_0$.*

Proof. Let $\{e_1, \ldots, e_n\}$ be a basis for $\mathfrak{g}_0$ over $\mathbb{R}$, such that $\{e_1, \ldots, e_k\}$ is a basis for $\mathfrak{h}$, and let $\{f_1, \ldots, f_n\}$ be the dual basis. We may also consider these as bases of $\mathfrak{g}$ and its complex dual.

First, $\mathrm{Ad}(H)$ maps $\mathfrak{h}$ into $\mathfrak{h}$. This can be seen by observing that conjugation by h in H maps H into H, so maps $\overline{H}$ into $\overline{H}$, and then differentiating. Next,

$$\{h \in G : f_j(\mathrm{Ad}(h)e_i) = 0 \qquad 1 \le i \le k,\ k+1 \le j \le n\}$$

is an algebraic subvariety of G containing the Zariski-dense subgroup H, and hence is all G. Thus $\mathfrak{h}_{\mathbb{C}}$ is an $\mathrm{Ad}(G)$-invariant subalgebra of $\mathfrak{g}$, and $\mathfrak{h}$ is an ideal in $\mathfrak{g}_0$. □

Corollary 3.2 *Suppose additionally that G is simple. Then with probability 1, Γ_ω is either dense or discrete.*

If G is semisimple, then the dichotomy of the corollary need not hold. For instance, suppose that G may be written as a direct product:

$$G = G_1 \times \ldots \times G_k.$$

If H_i is a Zariski-dense subgroup of G_i for each i, then $H_1 \times \ldots \times H_k$ is Zariski-dense in $G_1 \times \ldots \times G_k$. If some H_i are dense and others are discrete in G_i, then the product group is neither dense nor discrete.

4 A criterion for denseness

The arguments of Lemma 4.1 and Proposition 4.2 below are essentially a simplified version of Margulis' Lemma (see, e.g., [1, p. 101]).

We equip the space M_n of $n \times n$ matrices with the usual operator norm $\|\cdot\|$.

Lemma 4.1 *If $\|X\| \le 1$ and $\|Y\| \le 1$, then*

$$\begin{aligned} &\left\|\exp(X)\exp(Y)\exp(-X)\exp(-Y) - I - \frac{1}{2}[X,Y]\right\| \\ &\qquad \le 16e^4\,\|X\|\,\|Y\|\,(\|X\| + \|Y\|). \end{aligned}$$

Proof. For the duration of this proof, fix X and Y in M_n; we write x_t and y_t for $\exp(tX)$ and $\exp(tY)$ respectively.

Consider the function $\phi : [0,1] \to M_n(\mathbb{C})$ given by

$$\phi(t) = x_t\, y_t\, x_{-t}\, y_{-t}.$$

It is easy to check that $\phi(0) = I$, $\phi'(0) = 0$, $\phi''(0) = [X,Y]$, and that

$$\phi'''(t) = \sum_{i,j,k=1}^{4} x_t\, \phi^1_{i,j,k}(X)\, y_t\, \phi^2_{i,j,k}(Y)\, x_{-t}\, \phi^3_{i,j,k}(-X)\, y_{-t}\, \phi^4_{i,j,k}(-Y),$$

where

$$\phi^l_{i,j,k}(Z) = \begin{cases} Z^3 & \text{if all of } i,\ j, \text{ and } k \text{ are equal to } l \\ Z^2 & \text{if two of } i,\ j, \text{ and } k \text{ are equal to } l \\ Z & \text{if one of } i,\ j, \text{ and } k \text{ is equal to } l \\ 1 & \text{if none of } i,\ j, \text{ and } k \text{ is equal to } l. \end{cases}$$

By Taylor's theorem,

$$\begin{aligned} &\left\|\exp(X)\exp(Y)\exp(-X)\exp(-Y) - I - \frac{[X,Y]}{2}\right\| \\ &\qquad \le \frac{1}{2}\sup\{\|\phi'''(t)\| : t \in [0,1]\}. \end{aligned}$$

We estimate $\|\phi'''(t)\|$ by grouping the terms: if all of i, j, k are odd, we obtain the term

$$x_t X^3 y_t x_{-t} y_{-t} - 3x_t X^2 y_t X\, x_{-t} y_{-t} + 3x_t X\, y_t X^2 x_{-t} y_{-t} - x_t y_t X^3 x_{-t} y_{-t}$$

which is equal to

$$x_t\,[X^3\, y_t - y_t\, X^3]\, x_{-t}\, y_{-t} - 3x_t\, X[X\, y_t - y_t\, X]\, X\, x_{-t}\, y_{-t},$$

and the norm of this expression is at most

$$e^3 \left\|X^3 y_t - y_t X^3\right\| + 3e^3 \|X\|^2 \|X y_t - y_t X\|.$$

Since

$$\begin{aligned} \|X^p y_t - y_t X^p\| &= \|X^p(y_t - I) - (y_t - I)X^p\| \\ &\le 2\, \|X\|^p\, \|y_t - I\| \\ &\le 2e\, \|X\|^p\, \|Y\|, \end{aligned}$$

the contribution of these "all odd" terms is at most $8e^4 \|X\|^3 \|Y\|$. Similarly, the contribution of the terms with all of i, j, and k even is at most $8e^4 \|X\| \|Y\|^3$. Each term with at least one of i, j, and k even and at least one of i, j, and k odd contributes a factor which is at most $e^4\,\|X\|^2\,\|Y\|$ or $e^4\,\|X\|\,\|Y\|^2$, and the lemma is proved. □

Let U be the subset $\exp V$ of $GL(n, \mathbb{C})$, where

$$V = \{X \in M_n(\mathbb{C}) : \|X\| \le 0.02\}.$$

Proposition 4.2 *Suppose that G is simple, that $x, y \in G_e \cap U$, and that $\langle x, y\rangle$ is free and Zariski-dense. Then $\langle x, y\rangle$ is dense in G_e.*

Proof. Write $x = \exp(X)$ and $y = \exp(Y)$, where $X, Y \in V$. We define y_n inductively as follows: $y_0 = y$, and $y_n = x y_{n-1} x^{-1} y_{n-1}^{-1}$. We shall show that $y_n \in U$; it follows that $\langle x, y\rangle$ has an accumulation point inside $\overline{U}$. Thus $\langle x, y\rangle$ is not discrete, so is dense.

To see that $y_n \in U$, suppose inductively that $y_{n-1} = \exp(Y_{n-1})$, where $Y_{n-1} \in V$; then Lemma 4.1 implies that

$$||y_n - I - \frac{1}{2}[X, Y_{n-1}]|| \le 0.015,$$

so that

$$||y_n - I|| \le 0.015 + \frac{1}{2}\,\|[X, Y_{n-1}]\| \le 0.016.$$

Now

$$\log y_n = (y_n - I) - \frac{1}{2}(y_n - I)^2 + \frac{1}{3}(y_n - I)^3 - \dots,$$

so

$$||\log(y_n)|| \le 0.016 + \frac{1}{2}[0.016]^2 + \frac{1}{3}[0.016]^3 + \dots < 0.02,$$

and $\log(y_n)$ is in V, as required. □

We take now a product of such sets inside an almost direct product of simple groups, and we obtain the following.

Theorem 4.3 *There exists a neighbourhood U of e in G_e such that, if* $\operatorname{supp}\nu \subseteq U \times U$, *then Γ_ω is dense in G_e with probability* 1.

To extend this to the reductive case, we again need some control of the size of the centre Z_0 of G_0.

5 A criterion for discreteness

Suppose that x and y are transformations of a space B, and that there is a point b in B and subsets U and V of B such that $\{b\}$, U, and V are pairwise disjoint, and

$$\begin{aligned} x^m(\{b\} \cup V) &\subseteq U \qquad \forall m \in \mathbb{Z}\backslash\{0\} \\ y^m(\{b\} \cup U) &\subseteq V \qquad \forall m \in \mathbb{Z}\backslash\{0\}. \end{aligned}$$

Then, as observed by Tits [5], $\langle x, y\rangle$ is free. Indeed, if w is any nontrivial word in x, y, x^{-1} and y^{-1}, then $wb \in U \cup V$, so $wb \neq b$, and $w \neq e$. This argument also implies that $\langle x, y\rangle$ is discrete, at least if U and V are closed sets. For if w_n is any sequence of nontrivial words tending to the identity, $w_n b$ tends to b, so b lies in the closure of $U \cup V$.

Theorem 5.1 *If μ is a "reasonable" probability measure on G, and x_n and y_n are independent identically distributed random variables with law $\mu * \ldots * \mu$ (n times), then*

$$\lim_{n\to\infty} \mathbb{P}(\langle x_n, y_n\rangle \text{ is discrete}) = 1.$$

Idea of the proof. According to work of Y. Guivarc'h [G], based on ideas of Furstenberg and of V.I. Oseledets, as n increases, x_n and y_n act increasingly "contractively" on the boundary B of G. More precisely, there are small subsets U_n, V_n, P_n and Q_n of B such that, if $m \neq 0$,

$$(x_n)^m(B\backslash P_n) \subseteq U_n \qquad \text{and} \qquad (y_n)^m(B\backslash Q_n) \subseteq V_n$$

and as n increases, U_n, V_n, B_n, and P_n become smaller. Provide that

$$U_n \cap Q_n = \emptyset, \qquad V_n \cap P_n = \emptyset, \qquad \text{and} \qquad b \in B\backslash(P_n \cup Q_n \cup U_n \cup V_n),$$

which has probability 1 in the limit as n increases, the criterion for discreteness above is satisfied. □

In the reductive case, Γ_ω is almost surely discrete if, in addition, Z_0 is big enough.

References

[1] BALLMANN W., GROMOW M., and SCHROEDER V., "*Manifolds of Nonpositive Curvature*", Birkhäuser, Boston, Basel, Stuttgart, (1985)

[2] BALCERZYK S., and MYCIELSKI J., *"On faithful representations of free products of groups"*, Fund. Math. **50**,(1961), 63–71

[3] GUIVARC'H Y., *"Produits de matrices aléatoires et applications aux propriétés géométriques des sous-groupes du groupe linéaire"*, Ergodic Theory Dynamical Systems 10, (1990), 483–512

[4] KANTOR W.M., and LUBOTZKY A., *"The probability of generating a finite classical group"*, Geom. Dedic. **36**, (1990), 67–87

[5] TITS J., *"Free subgroups in linear groups"*, J. Algebra **20**,(1972), 250–270

M. Cowling
School of Mathematics
University of New South Wales
Sydney, NSW 2052 Australia

Pervenuta in Redazione il 04.08.1997