Random Nilpotent Groups of Maximal Step

Phillip Harris

Abstract. Let G be a random torsion-free nilpotent group generated by two random words of length ℓ in $U_n(\mathbb{Z})$. Letting ℓ grow as a function of n, we analyze the step of G, which is bounded by the step of $U_n(\mathbb{Z})$. We prove a conjecture of Delp, Dymarz, and Schaffer-Cohen, that the threshold function for full step is $\ell = n^2$.

A group G is nilpotent if its lower central series

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{1\}$$

defined by $G_{i+1} = [G, G_i]$, eventually terminates. The first index r for which $G_r = \{1\}$ is called the *step* of G. One may ask what a generic nilpotent group looks like, including its step. Questions about generic properties of groups can be answered with *random groups*, first introduced by Gromov [5]. Since Gromov's original *few relators* and *density* models are nilpotent with probability 0, they cannot tell us about generic properties of nilpotent groups. Thus there is a need for new random group models that are nilpotent by construction.

Delp et al [3] introduced a model for random nilpotent groups, motivated by the observation that any finitely generated torsion-free nilpotent group can be embedded in the group $U_n(\mathbb{Z})$ of $n \times n$ upper triangular integer matrices with ones on the diagonal [4]. Note that, since any finitely generated nilpotent group contains a torsion-free subgroup of finite index, we are not losing much by restricting our attention to torsion-free groups. (Another model is considered in [2]).

We construct a random subgroup of $U_n(\mathbb{Z})$ as follows. Let $E_{i,j}$ be the elementary matrix with 1's on the diagonal, a 1 at position (i, j) and 0's elsewhere. Then $S = \{E_{i,i+1}^{\pm 1} : 1 \leq i < n\}$ forms the standard generating set for $U_n(\mathbb{Z})$. We call the entries at positions $(i, i+1)$ the *superdiagonal* entries. Define a *random walk* of length ℓ to be a product

$$V = V_1 V_2 \dots V_\ell$$

where each V_i is chosen independently and uniformly from S. Let V and W be two independent random walks of length ℓ. Then $G = \langle V, W \rangle$ is a random subgroup of $U_n(\mathbb{Z})$. We have $\text{step}(G) \leq \text{step}(U_n(\mathbb{Z}))$, and it is not hard to check that $\text{step}(U_n(\mathbb{Z})) = n - 1$. If $\text{step}(G) = n - 1$ we say G has *full step*.

Now let $n \to \infty$ and $\ell = \ell(n)$ grow as a function of n. We say a proposition P holds *asymptotically almost surely* (a.a.s.) if $\mathbb{P}[P] \to 1$ as $n \to \infty$. Delp et al. gave results on the step of G, depending on the growth rate of ℓ with respect to n. Recall that $f = o(g(n))$ means $f(n)/g(n) \to 0$ as $n \to \infty$ and $f = \omega(g(n))$ means $f(n)/g(n) \to \infty$ as $n \to \infty$.

Theorem 1 (Delp-Dymarz-Schaffer-Cohen)**.** *Let $n, \ell(n) \to \infty$ and $G = \langle V, W \rangle$ where V, W are independent random walks of length ℓ. Then:*

(1) *If $\ell(n) = o(\sqrt{n})$ then a.a.s. step$(G) = 1$, i.e. G is abelian.*

(2) *If* $\ell(n) = o(n^2)$ *then a.a.s.* $step(G) < n - 1$.
(3) *If* $\ell(n) = \omega(n^3)$ *then a.a.s.* $step(G) = n - 1$, *i.e.* G *has full step.*

In this paper we close the gap between cases 2 and 3.

Theorem 2. *Let* $n, \ell(n) \to \infty$ *and* $G = \langle V, W \rangle$. *If* $\ell(n) = \omega(n^2)$ *then a.a.s.* G *has full step.*

To prove this requires a careful analysis of the nested commutators that generate G_{n-1}. In Section 1, we give a combinatorial criterion for a nested commutator of V's and W's to be nontrivial. In Section 2, we show this criterion is satisfied asymptotically almost surely when V, W are random walks.

1. Nested Commutators

Let $G = G_0 \geq G_1 \geq \dots$ be the lower central series of G. We have

$$G_i = [G, G_{i-1}] = [G, [G, \dots, [G, G] \dots]]$$

In particular, G_i includes all $i + 1$-fold nested commutators of elements of G. We restrict our attention to commutators where each factor is V or W.

Let $\{0,1\}^d$ be the d-dimensional cube, or the set of all length d binary vectors. For $x \in \{0,1\}^d, y \in \{0,1\}^e$ we define the norm $N(x) = \sum_{1 \leq i \leq d} x_i$ and the concatenation $xy \in \{0,1\}^{d+e}$. For example if $x = (1,0,0)$ and $y = (0,1)$ then $xy = (1,0,0,0,1) = 10^3 1$.

We define a family of maps $C_d : \{0,1\}^d \to G_d$ as follows.

$$C_1(1) = V$$
$$C_1(0) = W$$
$$C_d(1x) = [V, C_{d-1}(x)]$$
$$C_d(0x) = [W, C_{d-1}(x)]$$

Thus for example $C_5(10^3 1) = C_5(10001) = [V, [W, [W, [W, V]]]]$. We omit the subscript d when it is obvious. To prove G has full step it suffices to find an $x \in \{0,1\}^{n-1}$ such that $C(x)$ is nontrivial. We begin with Lemma 2.3 from [3], which gives a recursive formula for the entries of a nested commutator.

Lemma 1. *Let* $a \in \{0,1\}, x \in \{0,1\}^{d-1}$. *Then* $C(ax) \in G_d$ *and we have*

$$C(ax)_{i,i+d} = C(a)_{i,i+1} C(x)_{i+1,i+d} - C(a)_{i+d-1,i+d} C(x)_{i,i+d-1}$$

and furthermore $C(ax)_{i,j} = 0$ *for* $j < i + d$.

In particular, for $d = n - 1$ only the upper rightmost entry $C(ax)_{1,n}$ can be nonzero.

From the formula it is clear that $C(ax)_{i,i+d}$ is a degree-d polynomial in the superdiagonal entries of V and W. Let us state this more precisely and analyze the coefficients of the polynomial.

Lemma 2. *Let* $d \geq 1$. *There exists a function* $K_d : \{0,1\}^d \times \{0,1\}^d \to \mathbb{Z}$ *such that for* $1 \leq i \leq n - d$ *we have*

$$C(x)_{i,i+d} = \sum_{\substack{y \in \{0,1\}^d \\ N(y) = N(x)}} K_d(x, y) \prod_{i \leq j < i+d} V_{j,j+1}^{y_j} W_{j,j+1}^{1-y_j}$$

Furthermore, setting $K_d(x,y) = 0$ for $N(x) \neq N(y)$ we have a recursion

$$K_d(ax, byc) = K_1(a,b)K_{d-1}(x,yc) - K_1(a,c)K_{d-1}(x,by)$$

with base cases

$$K_1(0,0) = K_1(1,1) = 1$$
$$K_1(0,1) = K_1(1,0) = 0$$

Note that $K_d(x,y)$ does not depend on i. We also drop the subscript d since it can be inferred from x and y.

Proof. Abbreviate

$$U(i,d,y) := \prod_{i \leq j < i+d} V_{j,j+1}^{y_j} W_{j,j+1}^{1-y_j}$$

We first prove inductively that there exist coefficients $K_d : \{0,1\}^d \times \{0,1\}^d \to \mathbb{Z}$ such that

$$C(x)_{i,i+d} = \sum_{y \in \{0,1\}^d} K_d(x,y)U(i,d,y)$$

The case $d = 1$ is trivial. Assume it holds for $d-1$. Let $a \in \{0,1\}$ and $x \in \{0,1\}^{d-1}$, then we have

$$C(ax)_{i,i+d} = C(a)_{i,i+1}C(x)_{i+1,i+d} - C(a)_{i+d-1,i+d}C(x)_{i,i+d-1}$$

Expanding $C(a)_{i,i+1}$ and $C(x)_{i+1,i+d}$, the first term is

$$\begin{aligned}
&= [K_1(a,1)V_{i,i+1} + K_1(a,0)W_{i,i+1}] \left[\sum_{y \in \{0,1\}^{d-1}} K_{d-1}(x,y)U(i+1,d-1,y) \right] \\
&= \sum_{y \in \{0,1\}^{d-1}} K_1(a,1)K_{d-1}(x,y)U(i,d,1y) + K_1(a,0)K_{d-1}(x,y)U(i,d,0y) \\
&= \sum_{\substack{b,c \in \{0,1\} \\ y' \in \{0,1\}^{d-2}}} K_1(a,b)K_{d-1}(x,y'c)U(i,d,by'c)
\end{aligned}$$

Similarly the second term is

$$= \sum_{\substack{b,c \in \{0,1\} \\ y' \in \{0,1\}^{d-2}}} K_1(a,c)K_{d-1}(x,by')U(i,d,by'c)$$

Combining we get

$$C(ax)_{i,i+d} = \sum_{\substack{b,c \in \{0,1\} \\ y \in \{0,1\}^{d-2}}} \left[K_1(a,b)K_{d-1}(x,yc) - K_1(a,c)K_{d-1}(x,by)\right] U(i,d,byc)$$

And setting $K_d(ax,byc) = K_1(a,b)K_{d-1}(x,yc) - K_1(a,c)K_{d-1}(x,by)$ the lemma is proved for d. It is also easy to see inductively that $K_d(x,y) = 0$ for $N(x) \neq N(y)$, so we may add the condition $N(x) = N(y)$ under the sum. □

We now have a strategy for choosing $x \in \{0,1\}^{n-1}$ such that $C(x)$ is nontrivial. In the random model, it may happen that $V_{i,i+1} = 0$ for some i. Define the vector $v \in \{0,1\}^{n-1}$ by $v_i = 1$ if $V_{i,i+1} \neq 0$ and $v_i = 0$ otherwise. For now assume $0 < N(v) < n-1$. If we choose x such that $N(x) = N(v)$, then Equation **??** simplifies to

$$C_{n-1}(x)_{1,n} = K_d(x,v) \prod_{1 \leq i < n} V_{i,i+1}^{v_i} W_{i,i+1}^{1-v_i}$$

If we assume there is no i such that $V_{i,i+1} = W_{i,i+1} = 0$, the product of matrix entries is nonzero. So we just need to choose x such that $K_d(x,v) \neq 0$. We can do this with some additional assumptions on v.

Lemma 3. *Let $v \in \{0,1\}^{n-1}$ with $0 < N(v) < n-1$. Write $v = 1^{a_1}01^{a_2} \dots 1^{a_k-1}01^{a_k}$. Assume that $a_i \geq 1$ for all i, i.e., there are no adjacent 0's, and that $a_1 \neq a_k$. Then there exists $x \in \{0,1\}^{n-1}$ such that $K(x,v) \neq 0$.*

We will prove in section 2 that all assumptions used hold asymptotically almost surely.

Proof. Using the recursion from Lemma 2, the following identities are easily verified by induction:

(1) If $a, b \geq 0$, then

$$K(1^{a+b}0, 1^a01^b) = \binom{a+b}{a}(-1)^b$$

(2) If $a, b \geq 1, c \geq 0$ with $c < \min(a,b)$, then

$$K(1^c0x, 1^ay1^b) = 0$$

(3) Let $a, b \geq 0$. If $a < b$ then

$$K(1^a0x, 1^a0y1^b) = K(x, y1^b)$$

If $b < a$ then

$$K(1^b0x, 1^ay01^b) = K(x, 1^ay)(-1)^{b+1}$$

(4) If $a, b \geq 0$ then

$$K(1^{a+b}0^2x, 1^a01y101^b) = 2\binom{a+b}{a}(-1)^bK(x, 1y1)$$

Let $v = 1^{a_1}01^{a_2} \dots 01^{a_k}$. First assume $k = 2\ell$ is even. We set

$$x = 1^{a_1+a_{2\ell}}0^21^{a_2+a_{2\ell-1}}0^2 \dots 1^{a_\ell+a_{\ell+1}}0$$

Then applying identity 4 repeatedly followed by identity 1, we obtain

$$K(x,v) = 2^\ell(-1)^{a_{2\ell}+a_{2\ell-1}+\dots+a_{\ell+1}}\binom{a_1+a_{2\ell+1}}{a_1}\binom{a_2+a_{2\ell}}{a_2}\dots\binom{a_\ell+a_{\ell+1}}{a_\ell}$$

If k is odd, we apply identity 3 once and proceed as before. □

2. Asymptotics

In Section 1 we derived a combinatorial condition on the superdiagonal entries of V and W sufficient for G to have full step. Define

$$\mathcal{V} = \{i : 1 \leq i < n, V_{i,i+1} = 0\}$$
$$\mathcal{W} = \{i : 1 \leq i < n, W_{i,i+1} = 0\}$$

Then to apply Lemma 3 we need that

(1) $\mathcal{V}$ and $\mathcal{W}$ are nonempty.
(2) $\mathcal{V} \cap \mathcal{W} = \emptyset$.
(3) $\mathcal{V}$ has no adjacent elements.
(4) $\min \mathcal{V} \neq n - \max \mathcal{V}$.

If condition (1) does not hold, then Theorem 2 follows by a modification of Lemma 5.4 in [3]. We now show that in the random model, if $\ell = \omega(n^2)$, then the superdiagonal entries satisfy conditions (2)-(4) asymptotically almost surely. Recall that V and W are random walks

$$V = V_1 V_2 \dots V_\ell$$
$$W = W_1 W_2 \dots W_\ell$$

where each V_i, W_i is chosen independently and uniformly from the generating set $S = \{E_{i,i+1}^{\pm 1} : 1 \leq i < n\}$. Define

$$\sigma_j(Z) = \begin{cases} 1 & \text{if } Z = E_{j,j+1} \\ -1 & \text{if } Z = E_{j,j+1}^{-1} \\ 0 & \text{otherwise} \end{cases}$$

Then we have

$$V_{i,i+1} = \sum_{j=1}^{\ell} \sigma_i(V_j)$$

When $\ell \gg n$, the superdiagonal entries $V_{i,i+1}$ behave roughly like independent random walks on $\mathbb{Z}$. We restate Corollary 3.2 from [3].

Lemma 4. *Suppose $\ell = \omega(n)$. Then uniformly for $1 \leq k_1 < k_2 < \dots < k_d < n$ we have*

$$\mathbb{P}[k_i \in \mathcal{V} \cap \mathcal{W} \text{ for all } i] \sim \left(\frac{n}{2\pi\ell}\right)^d$$

By the union bound we have $\mathbb{P}[\mathcal{V} \cap \mathcal{W} \neq \emptyset] \ll n^2/\ell \to 0$. Thus condition (2) holds a.a.s. For conditions (3) and (4) we will need a bound on the size of $\mathcal{V}$.

Lemma 5. *Fix $\epsilon > 0$. Then $\mathbb{P}[|\mathcal{V}| > \epsilon\sqrt{n}] \to 0$ as $n \to \infty$.*

Proof. Define random variables

$$X_i = \begin{cases} 1 & V(i, i+1) = 0 \\ 0 & V(i, i+1) \neq 0 \end{cases}$$

So $|\mathcal{V}| = \sum_i X_i$. From Lemma 4 we have $\mathbb{E}[X_i] \ll \sqrt{n/\ell}$ and $\mathbb{E}[X_i X_j] \ll n/\ell$ for $1 \leq i < j < n$. Hence $\mathbb{E}[|\mathcal{V}|] \ll \sqrt{n^3/\ell}$ and $\mathrm{Var}[|\mathcal{V}|] \ll n^3/\ell$. By Chebyshev's

inequality

$$\mathbb{P}[|\mathcal{V}| \geq \epsilon\sqrt{n}] \leq \mathbb{P}\left[|\mathcal{V}| - \sqrt{n^3/\ell} \geq \sqrt{n}(\epsilon - \sqrt{n^2/\ell})\right]$$
$$\leq \frac{1}{(\epsilon - \sqrt{n^2/\ell})^2(\ell/n^2)} \to 0$$

□

Observe that the distribution of $\mathcal{V}$ is invariant under permutation. In other words, for a fixed set $\mathcal{S} \subset \{1, \ldots, n-1\}$ and a permutation π on $\{1, \ldots, n-1\}$ we have

$$\mathbb{P}[\mathcal{V} = \mathcal{S}] = \mathbb{P}[\mathcal{V} = \pi\mathcal{S}]$$

and hence

$$\mathbb{P}[\mathcal{V} = \mathcal{S}] = \frac{1}{\binom{n-1}{|\mathcal{S}|}} \mathbb{P}[|V| = |\mathcal{S}|]$$

Let $A(k)$ be the number of sets $\mathcal{S} \subset \{1, \ldots, n-1\}$ of size k with at least one pair of adjacent elements. We have

$$A(k) \leq (n-2)\binom{n-3}{k-2}$$

Let $B(k)$ be the number of sets $\mathcal{S}$ for which $\min \mathcal{S} = n - \max \mathcal{S}$. Summing over the possible values of $\min \mathcal{S}$ we have

$$B(k) \leq \sum_{1 \leq a \leq n/2} \binom{n-1-2a}{k-2}$$

One easily checks

$$\frac{A(k) + B(k)}{\binom{n-1}{k}} \leq \frac{2k^2}{n}$$

For $k \leq \epsilon\sqrt{n}$ this is $\leq 2\epsilon^2$. On the other hand $\mathbb{P}[|V| > \epsilon\sqrt{n}] \to 0$, so we are done.

Acknowledgements. We thank Tullia Dymarz for suggesting this problem and for many helpful discussions. This research was supported by NSF grants DMS-2037851 and DMS-1902173.

References

[1] Baumslag, Gilbert. Lectures on nilpotent groups. *Regional Conference Series in Mathematics American Mathematical Society, Providence, R.I.* **2** (1971).

[2] Cordes, Matthew, Duchin, Moon, Duong, Yen, and Sánchez, Andrew P. Random nilpotent groups 1. *International Mathematics Research Notices* **7** (2018) 1921-1953. https://doi.org/10.1093/imrn/rnv370

[3] Delp, Kelly ; Dymarz, Tullia; Schaffer-Cohen, Anschel. A matrix model for random nilpotent groups. *International Mathematics Research Notices.* **1** (2019) 201–230. https://doi.org/10.1093/imrn/rnx128

[4] Hall, Philip. The Edmonton notes on nilpotent groups. *Queen Mary College Mathematics Notes, Mathematics Department, Queen Mary College, London.* (1969)

[5] Ollivier, Yann. Invitation to random groups. *Ensaios Matemáticos [Mathematical Surveys], Sociedade Brasileira de Matemática, Rio de Janeiro.* **10** (2005).