d-WISE GENERATION OF SOME INFINITE GROUPS

ANDREA LUCCHINI, ATTILA MARÓTI, DARREN SEMMEN

Abstract. What is the largest possible size of a subset of $SL(n, \mathbb{Z})$ from which every pair of elements will be a generating set? We prove a general result on generation probabilities in profinite groups that suggests the cardinality of a maximal such subset equals that of the analogous subset of $SL(n, \mathbb{Z}/2\mathbb{Z})$.

Let $d$ be a positive integer greater than or equal to 2, and let $G$ be a discrete or profinite group that can be topologically generated by $d$ elements. If there is a largest integer $m$ with the property that there exists an $m$-tuple of elements of $G$ such that any $d$ entries together (topologically) generate $G$ then denote this number by $\mu_d(G)$, and otherwise set $\mu_d(G)$ equal to $\infty$. If $G$ cannot be generated by $d$ elements then set $\mu_d(G) = 0$.

A motivation for studying $\mu_d(G)$ is given by Theorem 12.

Another reason why the function $\mu_d(G)$ may be interesting is that it can be computed explicitly for certain groups $G$. For if $G$ is any of the groups $S_n$ for sufficiently large odd $n$, or $A_n$ for sufficiently large $n$ congruent to 2 modulo 4, or $GL(n,q)$, $PGL(n,q)$, $SL(n,q)$, $PSL(n,q)$ for $n$ at least 12 and not congruent to 2 modulo 4, or $M_{11}$, or $M_{23}$, then there is an explicit and exact formula for $\mu_d(G)$.

(For $d = 2$ this formula is found in [2], [3] and [4] respectively where it is also shown that $\mu_2(G) = \sigma(G)$ where $\sigma(G)$ is defined in the first paragraph of Section 2. Now apply Lemma 2 to conclude that $\mu_d(G) = (d-1)\mu_2(G)$.)

If $n$ is a positive integer greater than or equal to 2 then the group $SL(n, \mathbb{Z})$ is 2-generated. Hence, it makes sense to investigate $\mu_d(SL(n, \mathbb{Z}))$. Since $SL(n, \mathbb{Z}/2\mathbb{Z})$ is a factor group of $SL(n, \mathbb{Z})$, we certainly have $\mu_d(SL(n, \mathbb{Z})) \leq \mu_d(SL(n, \mathbb{Z}/2\mathbb{Z}))$. This, Lemma 2, Fact 8 taken from [3], and a bit of computation yields that $\nu_d(G)$ defined by

$$(b \cdot \mu_d(G))/((d-1)(\prod_{i=1}^{n-1} (2^n - 2^i) + [N(b)/2]))$$

is less than $1 + 2^{-n+1}$ for $G = SL(n, \mathbb{Z})$ and $n \geq 12$ where $b$ is the smallest prime divisor of $n$, the integer $N(b)$ is the number of subspaces of a fixed $n$-dimensional vector space over the field of 2 elements and $[x]$ denotes the largest integer less than or equal to $x$. Moreover, by Fact 8 taken from [3], if the answer to the following question is affirmative for $n \geq 12$, then we also have $\nu_d(SL(n, \mathbb{Z})) \geq 1$ for $n \geq 12$.

Question 1. Is it true that $\mu_d(SL(n, \mathbb{Z})) = \mu_d(SL(n, \mathbb{Z}/2\mathbb{Z}))$ for all integers $n$ and $d$ greater than or equal to 2?

Everything we do in this paper is intended to suggest that the answer should be “yes” rather than “no”. We prove that for $n \geq 12$ the answer is “yes” if we replace $SL(n, \mathbb{Z})$ by its profinite completion, and so $1 \leq \nu_d(SL(\widehat{\mathbb{Z}})) < 1 + 2^{-n+1}$

---

Research of the second author was partially supported by NSF Grant DMS 0140578 and by OTKA T049841.

Date: 1st of May 2008.
for \( n \geq 12 \) (with equality on the left-hand-side if (but not necessarily only if) \( n \) is not congruent to 2 modulo 4). Furthermore, when \( n \geq 3 \), the probability is positive that a random \( \mu_d(\hat{SL}(n, \mathbb{Z})) \)-tuple will have the property that any \( d \) entries will together generate \( SL(n, \mathbb{Z}) \). Since \( SL(n, \mathbb{Z}) \) is dense in its profinite completion, this suggests that the answer to our question is “yes”, though it hardly proves it.

1. Computing \( \mu_d(\hat{SL}(n, \mathbb{Z})) \)

For a group \( G \) let \( \sigma(G) \) denote the minimal cardinality of a covering of \( G \), i.e., a collection of proper subgroups whose union is \( G \). If \( G \) cannot be expressed as a union of proper subgroups, i.e., \( G \) is cyclic, then set \( \sigma(G) = \infty \).

Our first observation is what allows us to compute explicit formulae for \( \mu_d \).

Lemma 2. If the non-cyclic group \( G \) can be generated by 2 elements, then
\[
(d - 1)\mu_2(G) \leq \mu_d(G) \leq (d - 1)\sigma(G).
\]

Proof. The result is trivial if \( \mu_2(G) = \infty \). So suppose that \( \mu_2(G) \) is finite. Suppose \( g_1, \ldots, g_n \) pairwise generate \( G \). Let \( x \) be a \((dn-n)\)-tuple whose first \((d-1)\) entries equal \( g_1 \), whose second \((d-1)\) entries equal \( g_2 \), etc. Then, any \( d \) entries of \( x \) will generate \( G \). The second inequality follows from the fact that, for any \( d \) entries of a tuple \( \tau \) to generate \( G \), if \( C \) is a covering of \( G \) then at most \( d-1 \) entries of \( \tau \) can belong to any one element of \( C \). \( \square \)

The simplest case of the discrete general linear group is the only one we can handle.

Lemma 3. \( \mu_d(SL(2, \mathbb{Z})) = 4(d - 1) = \mu_d(SL(2, \mathbb{Z}/2\mathbb{Z})) \).

Proof. Because \( SL(2, \mathbb{Z}) \) is pairwise generated by the four matrices,
\[
\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},
\]
we have \( \mu_2(SL(2, \mathbb{Z}/2\mathbb{Z})) \geq \mu_2(SL(2, \mathbb{Z})) \geq 4 \). On the other hand, the group \( SL(2, \mathbb{Z}/2\mathbb{Z}) \) is isomorphic to the symmetric group on three letters and so has a minimal covering consisting of the Sylow 3-subgroup and the three Sylow 2-subgroups. Now apply Lemma 2. \( \square \)

For \( n \geq 3 \) we will move to the profinite completion \( \hat{SL}(n, \mathbb{Z}) \) of \( SL(n, \mathbb{Z}) \). Three of the easy observations can be stated for any profinite group.

Lemma 4. For any profinite group \( G \) that can be generated topologically by \( d \) elements,
\[ \mu_d(G) = \min\{\mu_d(G/N) \mid N \text{ is an open normal subgroup of } G\} \]

Proof. Clearly, \( \mu_d(G) \leq \mu_d(G/N) \) for each open normal subgroup \( N \). Suppose that the positive integer \( \ell \) is such that \( \mu_d(G/N) \geq \ell \) for each open normal subgroup \( N \). Let \( X_N \) be the subset of \( (G/N)^\ell \) whose elements are exactly those tuples from which any choice of \( d \) entries will form a set that generates \( G/N \). Let \( Y_N \) be the preimage of \( X_N \) in \( G^\ell \). Then each \( Y_N \) is closed and the intersection of any finite number of the \( Y_N \) is nonempty. Since \( G \) is compact, the intersection is non-empty and so \( \mu_d(G) \geq \ell \). \( \square \)
If $G$ is a group that is the union of finitely many proper subgroups then

$$\sigma(G) = \min\{\sigma(G/N) \mid N \text{ is a finite-index normal subgroup of } G\}.$$ 

**Lemma 6.** For any group $G$ we have both $\mu_d(G) = \mu_d(G/\Phi(G))$ and $\sigma(G) = \sigma(G/\Phi(G))$, where $\Phi(G)$ denotes the Frattini subgroup of $G$.

Note that $SL(n, \mathbb{Z})$ has the congruence subgroup property for $n \geq 3$ (cf. [1] or [7]). This is why we next consider groups of the form $SL(n, \mathbb{Z}/N\mathbb{Z})$, where $N$ is a positive integer.

Let $N$ be a positive integer with prime power decomposition $N = p_1^{i_1} \cdots p_t^{i_t}$. Then, by the Chinese Remainder Theorem, $SL(n, \mathbb{Z}/N\mathbb{Z}) = \prod_{i=1}^t SL(n, \mathbb{Z}/p_i^{i_i}\mathbb{Z})$. We also have $\Phi(SL(n, \mathbb{Z}/N\mathbb{Z})) = \prod_{i=1}^t \Phi(SL(n, \mathbb{Z}/p_i^{i_i}\mathbb{Z}))$.

**Lemma 7.** Let $n$ and $N$ be positive integers with $n \geq 5$. Let $\alpha$ denote $\mu_d$ or $\sigma$. Then, $\alpha(SL(n, \mathbb{Z}/N\mathbb{Z})) = \min_{1 \leq t \leq T} \{\alpha(PSL(n, \mathbb{Z}/p_i\mathbb{Z}))\}$, where $p_1, \ldots, p_t$ are the distinct prime divisors of $N$.

**Proof.** We have

$$\alpha(SL(n, \mathbb{Z}/N\mathbb{Z})) = \alpha(SL(n, \mathbb{Z}/N\mathbb{Z})/\Phi(SL(n, \mathbb{Z}/N\mathbb{Z})))$$

$$= \alpha\left(\prod_{i=1}^t SL(n, \mathbb{Z}/p_i^{i_i}\mathbb{Z})/\Phi(SL(n, \mathbb{Z}/p_i^{i_i}\mathbb{Z}))\right)$$

$$= \alpha\left(\prod_{i=1}^t PSL(n, \mathbb{Z}/p_i\mathbb{Z})\right)$$

$$= \min_{1 \leq t \leq T} \alpha(PSL(n, \mathbb{Z}/p_i\mathbb{Z})),$$

where the first equality follows from Lemma 6, the third equality follows from a result of Weigel [9, Theorem B], and the last equality follows from the fact that the direct summands are non-isomorphic simple groups.

**Fact 5** (Neumann, [8]). If $G$ is a group that is the union of finitely many proper subgroups then

$$\sigma(G) = \min\{\sigma(G/N) \mid N \text{ is a finite-index normal subgroup of } G\}.$$ 

**Theorem 9.** Let $n$ be a positive integer greater than or equal to 12. Then, the following three statements are true.

1. $\mu_d(SL(n, \mathbb{Z})) = \mu_d(SL(n, \mathbb{Z}/2\mathbb{Z}))$.
2. $\sigma(SL(n, \mathbb{Z})) = \sigma(SL(n, \mathbb{Z})) = \sigma(SL(n, \mathbb{Z}/2\mathbb{Z}))$.
3. If $n$ is not congruent to 2 modulo 4 then

$$\mu_d(SL(n, \mathbb{Z})) = (d - 1)\mu_d(SL(n, \mathbb{Z}/2\mathbb{Z})).$$
Proof. Remember that $SL(n, \mathbb{Z})$ has the congruence subgroup property when $n \geq 3$.

Fact 5 and Lemma 7 show that $\sigma(SL(n, \mathbb{Z}))$ and $\sigma(SL(n, \mathbb{Z}))$ both equal the minimum of $\sigma(PSL(n, \mathbb{Z}/p\mathbb{Z}))$, where $p$ ranges over all prime natural numbers. By Fact 8, this minimum occurs when $p = 2$.

By Lemmas 4 and 7, $\mu_d(SL(n, \mathbb{Z}))$ will equal the minimum of $\mu_d(PSL(n, \mathbb{Z}/p\mathbb{Z}))$, where $p$ ranges over all prime natural numbers. By Lemma 2 and Fact 8, this minimum occurs when $p = 2$.

When $n$ is not congruent to 2 modulo 4, Fact 8 states that $\sigma(SL(n, \mathbb{Z}/2\mathbb{Z}))$ equals $\mu_2(SL(n, \mathbb{Z}/2\mathbb{Z}))$ and the rest of the third statement then follows from Lemma 2. □

2. Generation probabilities in profinite groups

Next we will show that, whenever $n \geq 3$ and $d \geq 2$, the probability is positive that a randomly chosen $\mu_d(SL(n, \mathbb{Z}))$-tuple with entries from $SL(n, \mathbb{Z})$ has the property that any $d$ entries will together generate $SL(n, \mathbb{Z})$. This will follow from Theorem 12 and the fact (see page 442 of [5]) that whenever $n \geq 3$ and $d \geq 2$, the probability is positive that a randomly chosen $d$-tuple with entries from $SL(n, \mathbb{Z})$ will generate $SL(n, \mathbb{Z})$. (On the other hand, $SL(2, \mathbb{Z})$ is virtually profree and the probability is zero that a randomly chosen pair of elements will generate the group.)

Let $G$ be a profinite group that can be generated by $d$ elements. Let $\nu$ be the normalized Haar measure of $G$; abusing notation, we also denote by $\nu$ the corresponding measure on direct products of copies of $G$. For any $k \geq d$, let $\Omega(G, k, d)$ be the set of $k$-tuples of elements of $G$ with the property that every $d$ distinct entries together generate $G$. Let $P(G, k, d) = \nu(\Omega(G, k, d))$ and $P(G, d) = P(G, d, d)$.

For each open normal subgroup $N$ of $G$, define $P(G, N, d)$ as follows. Let $\pi : G^d \to (G/N)^d$ be the canonical quotient map. For any $x \in \Omega(G/N, d, d)$, let $P(G, N, d) = \nu(\pi^{-1}(x) \cap \Omega(G, d, d))/\nu(\pi^{-1}(x))$. By Lemma 10, this is independent of the choice of $x$, so $P(G, d) = P(G, N, d)P(G, N, d)$.

Lemma 10. Let $N$ be an open normal subgroup of $G$ and let $\pi : G^d \to (G/N)^d$ be the canonical quotient map. For any elements $x$ and $y$ of $\Omega(G/N, d, d)$, $\nu(\pi^{-1}(x) \cap \Omega(G, d, d)) = \nu(\pi^{-1}(y) \cap \Omega(G, d, d))$.

Proof. Once this is proven for all finite groups $G$, the result for profinite $G$ will pass through the inverse limit.

For finite $G$, we proceed by induction on the cardinality of $N$. Let $\mathcal{C}$ be the collection of proper subgroups $H$ of $G$ that satisfy $HN = G$. By induction, for each $H \in \mathcal{C}$, $|H \cap N|^d P(H, H \cap N, d)$ equals the number of elements of $\pi^{-1}(x)$ with the property that every $d$ distinct entries together generate $H$. Thus,

$$\frac{\nu(\pi^{-1}(x) \cap \Omega(G, d, d))}{\nu(\pi^{-1}(x))} = 1 - \sum_{H \in \mathcal{C}} \left( \frac{|H \cap N|^d}{N^d} \right) P(H, H \cap N, d),$$

and the latter value is independent of the choice of $x$. □

The following technical lemma will make short work of the main theorem:

Lemma 11. If $N$ is an open normal subgroup of $G$ then

$$P(G, k, d) \geq P(G/N, k, d) \left( 1 - (1 - P(G, N, d)) \binom{k}{d} \right).$$
Proof. Clearly, if \((g_1, \ldots, g_k) \in \Omega(G, k, d)\), then \((g_1N, \ldots, g_kN) \in \Omega(G/N, k, d)\). So, assume \((g_1N, \ldots, g_kN) \in \Omega(G/N, k, d)\) and let
\[
\Lambda = \{(n_1, \ldots, n_k) \in N^k \mid \langle g_1n_1, \ldots, g_kn_k \rangle \notin \Omega(G, k, d)\}.
\]
To prove the lemma it suffices to show that \(\nu(\Lambda)/\nu(N^k) \leq (1 - P(G, N, d))(\binom{k}{d})\).

For each subset \(I = \{i_1, \ldots, i_d\}\) of \(\{1, \ldots, k\}\) with cardinality \(d\), let \(\Lambda_I\) equal
\[
\{(n_1, \ldots, n_k) \in N^k \mid \langle g_{i_1}n_{i_1}, \ldots, g_{i_d}n_{i_d} \rangle \neq G\}.
\]
The lemma then follows from the fact that \(\nu(\Lambda_I)/\nu(N^k) = 1 - P(G, N, d)\) and \(\Lambda = \bigcup_I \Lambda_I\).

\begin{theorem}
For a profinite group \(G\) and a positive integer \(d\), the following two conditions are equivalent.

1. \(P(G, d) > 0\).
2. \(P(G, \mu_d(G), d) > 0\).
\end{theorem}

The condition that \(P(G, d) > 0\) for some positive integer \(d\) is equivalent to \(G\) having polynomial maximal subgroup growth. This is a theorem of Mann [5] and Mann and Shalev [6].

Proof. Projection from \(\Omega(G, \mu_d(G), d)\) to \(\Omega(G, d, d)\) yields the implication of (1) from (2). We only show that (1) implies (2).

We want to prove that if \(P(G, d) > 0\) and \(\Omega(G, k, d) = \emptyset\) then \(P(G, k, d) > 0\).

Because \(G\) can be topologically generated by a finite number of elements, it possesses a countable descending chain of open normal subgroups, \(N_i\), that has trivial intersection. Since \(\lim_{i \to \infty} P(G/N_i, d) = P(G, d) > 0\) and, for all \(i\), \(P(G, d) = P(G/N_i, d)\), we see that \(\lim_{i \to \infty} P(G, N_i, d) = 1\). Therefore there exists a natural number \(i\) such that \((1 - P(G, N_i, d))(\binom{k}{d}) < 1\). Setting \(N\) equal to \(N_i\) in Lemma 11, we conclude that \(P(G, k, d) > 0\). \(\square\)

References


Andrea Lucchini, Dipartimento di Matematica Pura ed Applicata, Via Trieste 63, 35121 Padova, Italy.
E-mail address: lucchini@math.unipd.it

Attila Marót. Current address: The Mathematical Sciences Research Institute, 17 Gauss Way, Berkeley, CA 94720-5070, USA. Previous address: Department
of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA.
E-mail addresses: attilam@msri.org and maroti@usc.edu

Darren Semmen, Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA.
E-mail address: semmen@usc.edu