

On the probability of satisfying a word in a group

Miklós Abért ^{*†}

November 12, 2005

Abstract

We show that for any finite group G and for any d there exists a word $w \in F_d$ such that a d -tuple in G satisfies w if and only if it generates a solvable subgroup. As a corollary, the probability that a word is satisfied in a fixed non-solvable group can be made arbitrarily small, answering a question of Alon Amit.

It also follows that there is no absolute bound in the Baumslag-Pride theorem for the minimal index of a subgroup of a group with at least two more generators than relators that can be mapped homomorphically onto a nonabelian free group.

1 Introduction

Let F_n denote the free group on n letters and let G be a group. For $w \in F_n$ we say that the n -tuple $(g_1, g_2, \dots, g_n) \in G^n$ satisfies w if the substitution $w(g_1, g_2, \dots, g_n) = 1$. Our first result is the following.

Theorem 1 *Let G be a finite group. Then for all n there exists a word $w \in F_n$ such that for all $g_1, g_2, \dots, g_n \in G$, the tuple (g_1, g_2, \dots, g_n) satisfies w if and only if the subgroup $\langle g_1, g_2, \dots, g_n \rangle \leq G$ is solvable.*

Note that if G itself is not solvable, then a word as in Theorem 1 has to contain at least $n - 2$ letters of F_n . Indeed, if w omits at least two letters, then any two elements of G generate a solvable subgroup, which, using a theorem of Thompson [Tho] (see also [Fla]) implies that G itself is solvable.

For $w \in F_n$ let $\langle F_n \mid w \rangle$ denote the one-relator group defined by w . As an immediate corollary of Theorem 1, we get the following.

Corollary 2 *Let G be a finite non-solvable group. Then for all n there exists a word $w \in F_n$ such that $\langle F_n \mid w \rangle$ cannot be mapped homomorphically onto G .*

^{*} *Mathematics Subject Classification* 20F05, 20F69, 20P05

[†] Research partially supported by NSF grant DMS-0401006

It is natural to ask whether this property holds exactly when G is not solvable.

Question 1. *Let G be a finite solvable group. Does there exist $N \in \mathbb{N}$ such that for all $n \geq N$ and every $w \in F_n$ the one-relator group $\langle F_n \mid w \rangle$ can be mapped homomorphically onto G ?*

We call a group Γ *large*, if there is a subgroup $\Delta \leq \Gamma$ of finite index which can be mapped homomorphically onto a non-abelian free group. A well-known theorem of Baumslag and Pride [BaP] shows that groups with two more generators than relators are large. In particular, for $n \geq 3$ every one-relator group $\Gamma = \langle F_n \mid w \rangle$ is large. In turn, Stallings [St1] has shown that for every n there exists $w \in F_n$ such that $\langle F_n \mid w \rangle$ itself does not homomorphically map onto F_2 . Theorem 1 implies the following strengthening of Stallings's result.

Corollary 3 *For all n and N there exists a word $w \in F_n$ such that if $\Delta \leq \langle F_n \mid w \rangle$ is a subgroup of index at most N , then Δ cannot be mapped homomorphically onto a non-abelian free group.*

For $w \in F_n$ let $P(G, w)$ denote the probability that for n independent uniform random elements $g_1, \dots, g_n \in G$ we have $w(g_1, \dots, g_n) = 1$. Note that $P(G, w)$ only depends on the word w and not on n so we can assume $w \in F_\infty$.

The probabilities $P(G, w)$ have been investigated in the literature mainly for a fixed word and varying G . The strongest result in this direction is of Dixon, Pyber, Seress and Shalev [DPSS] who proved that for any word $1 \neq w$ the probability $P(G, w)$ tends to 0 as $|G| \rightarrow \infty$ assuming that G is non-abelian simple. In this paper we will fix the finite group G and let w run through F_∞ .

Alon Amit [Ami] has shown that if G is nilpotent then there exists a constant $c > 0$ depending on G only such that for all $w \in F_\infty$ we have $P(G, w) > c$. Note that this answers Question 1 affirmatively for nilpotent groups. He conjectures that the same holds if G is solvable and that if G is nilpotent then in fact

$$P(G, w) \geq \frac{1}{|G|} \text{ for all } w \in F_\infty.$$

He also asked if in turn for a non-solvable finite group G the probability $P(G, w)$ can be made arbitrarily small with a suitable $w \in F_\infty$.

It is easy to see that Theorem 1 already answers Amit's question affirmatively, but the following stronger result also holds. A group G is *just non-solvable* if every proper quotient of G is solvable, but G itself is not.

Theorem 4 *Let G be a finite just non-solvable group. Then the set*

$$\{P(G, w) \mid w \in F_\infty\}$$

is dense in $[0, 1]$.

Acknowledgement. The author is grateful to Alon Amit for communicating his results and questions to him, to Laci Pyber for helpful advices on how to present the paper and to Schmuel Weinberger for asking whether Corollary 3 holds.

2 Proofs

Let us introduce some notation. Let G be a just non-solvable group and let N be a minimal normal subgroup of G . Then $N \cong S^m$ for some simple group S . By the minimality of G the quotient G/N is solvable, so S is non-abelian and $Z(N) = 1$, which implies that $G/C_G(N)$ is non-solvable so $C_G(N) = 1$. Then G embeds into the wreath product

$$\text{Aut}(N) \cong \text{Aut}(S) \text{ wr } \text{Sym}(m)$$

where $\text{Sym}(m)$ denotes the symmetric group on m letters and by the minimality of N , G has a transitive image in $\text{Sym}(m)$. Since G/N is solvable, N is a characteristic subgroup of G . Also, every nontrivial normal subgroup $K \triangleleft G$ contains N (using the minimality of N and that G is just non-solvable). Finally, if in addition $K = K'$ (the commutator subgroup of K), then $K = N$.

From now on G , N , S and m will be as above. Let $G_j \cong G$ ($1 \leq j \leq n$), let

$$P = G_1 \times \cdots \times G_n$$

and let

$$\pi_j : P \rightarrow G_j \quad (1 \leq j \leq n)$$

denote the projection to the j -th coordinate. Let

$$N \cong N_j \triangleleft G_j (1 \leq j \leq n),$$

let $N_j = S_{j,1} \times \cdots \times S_{j,m}$ where $S_{j,i} \cong S$ and let

$$M = N_1 \times \cdots \times N_n \triangleleft P.$$

The first lemma is folklore (see e.g. [Rob, Lemma 3.3.16.]).

Lemma 5 *If S_1, \dots, S_n are nonabelian finite simple groups, then every normal subgroup $K \triangleleft S_1 \times \cdots \times S_n$ is of the form*

$$K = K_1 \times \cdots \times K_n$$

where $K_i = S_i$ or 1 ($1 \leq i \leq n$).

The next lemma tells us about the normal subgroup structure of subgroups of P which project onto each G_j .

Lemma 6 Let $H \leq P$ be a subgroup containing M such that

$$\pi_j(H) = G_j \quad (1 \leq j \leq n)$$

Let K be a normal subgroup of H . Then

$$K \cap M = \bigoplus_{\pi_j(K) \neq 1} N_j$$

Proof. $K \cap M$ is normal in

$$M \cong \bigoplus_{1 \leq j \leq n, 1 \leq i \leq m} S_{j,i}$$

so by Lemma 5 it is the direct product of some of the $S_{j,i}$, that is,

$$K \cap M = K_1 \times \cdots \times K_n$$

where $K_j \triangleleft N_j$ ($1 \leq j \leq n$).

If $\pi_j(K) = 1$ then $K \cap N_j = 1$ so $K_j = 1$.

If $\pi_j(K) \neq 1$ then $\pi_j(K) \triangleleft \pi_j(H) = G_j$ so $N_j \leq \pi_j(K)$, since N_j is a minimal normal subgroup in G_j . In this case

$$K \cap M \geq [K, M] \geq [K, N_j] = [\pi_j(K), N_j] = N_j$$

so $K_j = N_j$ (here we use the direct product form and that the commutator $[N_j, N_j] = N_j$).

The lemma holds. ■

Let

$$(a_1, \dots, a_k), (b_1, \dots, b_k) \in G^k$$

be k -tuples from G . We say that (a_1, \dots, a_k) and (b_1, \dots, b_k) are *automorphism independent over G* if there exists no $\alpha \in \text{Aut}(G)$ such that $a_i^\alpha = b_i$ for all $1 \leq i \leq k$.

Our next lemma shows that subgroups of $G_1 \times \cdots \times G_n$ satisfying some natural conditions contain $N_1 \times \cdots \times N_n$.

Lemma 7 Let $a_{i,j} \in G_j$ ($1 \leq i \leq k, 1 \leq j \leq n$), such that we have

$$\langle a_{1,j}, \dots, a_{k,j} \rangle = G_j \quad (1 \leq j \leq n)$$

and that for all $1 \leq j < l \leq n$ the k -tuples $(a_{1,j}, \dots, a_{k,j})$ and $(a_{1,l}, \dots, a_{k,l})$ are *automorphism independent over G* . For $1 \leq i \leq k$ let

$$h_i = (a_{i,1}, \dots, a_{i,n}) \in G_1 \times \cdots \times G_n$$

and let

$$H = \langle h_1, \dots, h_k \rangle \leq G_1 \times \cdots \times G_n$$

Then

$$M = N_1 \times \cdots \times N_n \leq H.$$

Proof. Let

$$f : G_1 \times \cdots \times G_n \rightarrow G_1 \times \cdots \times G_{n-1}$$

denote the projection to the first $n - 1$ coordinates. Let $H_1 = f(H)$ and let

$$R = \pi_n(\text{Ker}(f)) \leq G_n.$$

By induction on n , we have $N_1 \times \cdots \times N_{n-1} \leq H_1$. Also R is normal in G_n so by the minimality of N_n in G_n either $N_n \leq R$ or $R = 1$.

We claim that $N_n \leq R$. Assume $R = 1$. Let us define the function $\varphi : H_1 \rightarrow G_n$ by

$$\varphi(g_1, \dots, g_{n-1}) = g_n \text{ if } (g_1, \dots, g_{n-1}, g_n) \in H.$$

Then φ is well-defined, since

$$(g_1, \dots, g_{n-1}, g_n), (g_1, \dots, g_{n-1}, g'_n) \in H$$

implies $g_n^{-1}g'_n \in R$. So φ is a homomorphism. Using $\langle a_{1,n}, \dots, a_{k,n} \rangle = G_n$ we also see that φ is surjective.

Let $K = \text{Ker}(\varphi)$. Then K is normal in H_1 and

$$H_1/K \cong G_n \cong G$$

which is not solvable. Since $N_1 \times \cdots \times N_{n-1} \leq H_1$, the use of Lemma 6 for H_1 and K gives us

$$K \cap M = \bigoplus_{\pi_j(K) \neq 1} N_j.$$

Now $M \leq K$ would imply that H_1/K is solvable, a contradiction. So there exists a coordinate $1 \leq l < n$ such that $\pi_l(K) = 1$, that is, $K \leq \text{Ker}(\pi_l)$. Moreover

$$H_1/\text{Ker}(\pi_l) \cong G_l \cong G$$

which implies $K = \text{Ker}(\pi_l)$. This shows that the function $\alpha : G_l \rightarrow G_n$ defined by

$$\alpha(g_l) = g_n \text{ if } (g_1, \dots, g_l, \dots, g_n) \in H$$

is an isomorphism. In particular, $\alpha(a_{i,l}) = a_{i,n}$ ($1 \leq i \leq k$), so the k -tuples $(a_{1,l}, \dots, a_{k,l})$ and $(a_{1,n}, \dots, a_{k,n})$ are not automorphism independent over G which contradicts the assumptions of the lemma. So the claim $N_n \leq R$ holds and so $1 \times \cdots \times 1 \times N_n \leq H$.

Now let $L = f^{-1}(N_1 \times \cdots \times N_{n-1}) \leq H$. Let $L^{(i)}$ denote the i -th element of the derived series of L and let r be a number such that $L^{(r)} = L^{(r+1)}$. Then $f(L^{(r)}) = N_1 \times \cdots \times N_{n-1}$ and since $1 \times \cdots \times 1 \times N_n \leq L$ also $1 \times \cdots \times 1 \times N_n \leq L^{(r)}$. Now $J = \pi_n(L^{(r)})$ is normal in G_n , $N_n \leq J$ and $J' = J$, so $J = N_n$. This implies

$$L^{(r)} = N_1 \times \cdots \times N_n \leq H$$

which is what we wanted to prove. ■

Remark. This lemma is well-known in the case when G is a nonabelian finite simple group. According to the author's knowledge it is originally due to Hall [Hal] (see also [KaL] and [Wie]).

We state an easy corollary of Lemma 7 that we will use in the proof of Theorem 1.

Corollary 8 *Let G_i ($1 \leq i \leq n$) be finite nonabelian simple groups and let*

$$H \leq G_1 \times \cdots \times G_n$$

such that the projections $\pi_i(H) = G_i$ ($1 \leq i \leq n$). Then there exists $g \in H$ such that $\pi_i(g) \neq 1$ ($1 \leq i \leq n$).

Proof. We proceed by induction on n . For $n = 1$ the lemma is trivial. By induction we have an element $g \in H$ such that $\pi_i(g) \neq 1$ ($1 \leq i < n$). If the last coordinate is automorphism dependent on some previous coordinate k then $\pi_k(g) \neq 1$ implies $\pi_n(g) \neq 1$. If it is not, then $1 \times \cdots \times 1 \times G_n \leq H$ and we can choose the last coordinate of g as we wish. ■

Now we prove Theorem 4.

Proof of Theorem 4. Let m be the number of maximal subgroups of G . Let $d > \log_2 m$ be an integer to be chosen later. The probability that d independent random elements all fall into a fixed maximal subgroup M is at most $|G : M|^{-d} \leq 2^{-d}$ so the probability that d random elements do not generate G is at most $m2^{-d} < 1$. In particular, G can be generated by d elements. Let

$$Q = \{(g_1, \dots, g_d) \in G^d \mid g_1, \dots, g_d \text{ generate } G\}$$

be the set of generating d -tuples.

Now $\text{Aut}(G)$ acts on Q by $(g_1, \dots, g_d)^\alpha = (g_1^\alpha, \dots, g_d^\alpha)$ where $\alpha \in \text{Aut}(G)$. This action is fixed-point free, as if α fixes all the elements of a generating set then it fixes every element of G . Let r be the number of $\text{Aut}(G)$ -orbits and let $t_1, \dots, t_r \in Q$ be an orbit representative system.

It is easy to see that the conditions of Lemma 7 hold for $a_{i,j} = t_j(i)$. This implies that the r -tuples

$$h_i = (t_1(i), \dots, t_r(i))$$

generate a group H which contains $N_1 \times \cdots \times N_r$.

Let $1 \neq g \in N$, let $k \leq r$ be a natural number to be chosen later and let the r -tuple h be defined by

$$h(i) = 1 \quad (1 \leq i \leq k) \quad \text{and} \quad h(i) = g \quad (k < i \leq r)$$

Then $h \in N_1 \times \cdots \times N_r \leq H$, so there exists a word $w \in F_d$ such that $w(h_1, \dots, h_d) = h$.

Now let us evaluate w on the set of possible d -tuples from G . We completely control the evaluation on generating tuples; since

$$w(g_1^\alpha, \dots, g_d^\alpha) = (w(g_1, \dots, g_d))^\alpha \quad (\alpha \in \text{Aut}(G))$$

we have

$$|\{(g_1, \dots, g_d) \in Q \mid w(g_1, \dots, g_d) = 1\}| = k |\text{Aut}(G)|.$$

On d -tuples (g_1, \dots, g_d) not generating G we do not control $w(g_1, \dots, g_d)$, but as we saw earlier, the number of these tuples is at most $m2^{-d} |G|^d$. Dividing by $|G|^d$, this gives us

$$k \frac{|\text{Aut}(G)|}{|G|^d} \leq P(G, w) \leq k \frac{|\text{Aut}(G)|}{|G|^d} + m2^{-d}$$

and for the maximal value of $k = r$ we get

$$k \frac{|\text{Aut}(G)|}{|G|^d} = \frac{r |\text{Aut}(G)|}{|G|^d} = \frac{|Q|}{|G|^d} \geq 1 - m2^{-d}.$$

Let

$$\epsilon(d) = m2^{-d} + \frac{|\text{Aut}(G)|}{|G|^d}$$

Since $k \leq r$ can be set arbitrarily, we deduce that the set

$$\{P(G, w) \mid w \in F_d\}$$

is an $\epsilon(d)$ -net in $[0, 1]$, that is, for every $a \in [0, 1]$ there exists $w \in F_d$ such that $|P(G, w) - a| < \epsilon(d)$.

Now $\lim_{d \rightarrow \infty} \epsilon(d) = 0$ which shows that the set

$$\{P(G, w) \mid w \in F_\infty\} = \bigcup_d \{P(G, w) \mid w \in F_d\}$$

is dense in $[0, 1]$. ■

The answer to Amit's question follows as an easy corollary of Theorem 4.

Corollary 9 *Let G be a finite non-solvable group. Then 0 is an accumulation point of the set*

$$\{P(G, w) \mid w \in F_\infty\}$$

Proof. Let K be a normal subgroup in G such that G/K is just non-solvable and let g_1, \dots, g_n be independent uniform random elements of G . Then g_1K, \dots, g_nK are independent uniform random elements of G/K which yields

$$P(G/K, w) = P(w(g_1, \dots, g_n) \in K) \geq P(w(g_1, \dots, g_n) = 1) = P(G, w)$$

for $w \in F_\infty$. Using Theorem 4 we get that for every $\epsilon > 0$ we have $w \in F_\infty$ such that

$$P(G, w) \leq P(G/K, w) < \epsilon$$

and so the corollary holds. ■

We are ready to prove Theorem 1.

Proof of Theorem 1. For each subgroup $H \leq G$ let us choose a homomorphism φ_H with domain H as follows. If H is solvable then let $\varphi_H = \text{Id}$ be the identity map, otherwise let φ_H be a homomorphism onto a just non-solvable quotient of H .

Let us enumerate all the n -tuples from G as t_1, t_2, \dots, t_k where $k = |G|^n$. Let $t_{i,j}$ denote the j -th element of t_i ($1 \leq j \leq n$). For $1 \leq i \leq k$ let

$$H_i = \langle t_{i,1}, t_{i,2}, \dots, t_{i,n} \rangle$$

Let $\varphi_i = \varphi_{H_i}$ and let $G_i = \varphi_i(H_i)$. Let N_i be the minimal normal subgroup of G_i if G_i is just non-solvable, otherwise let $N_i = 1$. Also let

$$u_{i,j} = \varphi_i(t_{i,j}) \quad (1 \leq i \leq k, 1 \leq j \leq n)$$

and let

$$p_j = (u_{1,j}, u_{2,j}, \dots, u_{k,j}) \in G_1 \times \dots \times G_k \quad (1 \leq j \leq n)$$

Let

$$L = \langle p_1, p_2, \dots, p_n \rangle \leq G_1 \times \dots \times G_k$$

and let

$$\pi_i : G_1 \times \dots \times G_k \rightarrow G_i \quad (1 \leq i \leq k)$$

denote the projection to the i -th coordinate. Then $\pi_i(L) = G_i$ ($1 \leq i \leq k$). Let $L^{(i)}$ denote the i -th derived subgroup of L and let r be an integer such that $M = L^{(r)} = L^{(r+1)}$. Then $\pi_i(M) \triangleleft G_i$ and $\pi_i(M)' = \pi_i(M)$ so $\pi_i(M) = N_i$. Now all the $N_i \neq 1$ are isomorphic to some direct power of a nonabelian simple group so M lies in a direct product of nonabelian simple groups and projects to each factor of the product. By Corollary 8 there exists an element $g \in M \leq L$ such that $\pi_i(g) \neq 1$ if and only if $N_i \neq 1$. Let $w \in F_n$ be a word such that $w(p_1, p_2, \dots, p_n) = g$.

We claim that this w will be good for our purposes. Indeed, we have

$$\pi_i(g) = w(u_{i,1}, \dots, u_{i,n}) = w(\varphi_i(t_{i,1}), \dots, \varphi_i(t_{i,n})) = \varphi_i(w(t_{i,1}, \dots, t_{i,n}))$$

Now if H_i is solvable then φ_i is the identity map and $\pi_i(g) = 1$, so we get $w(t_{i,1}, \dots, t_{i,n}) = 1$. If H_i is not solvable, then $\pi_i(g) \neq 1$ and since φ_i is a homomorphism we have $w(t_{i,1}, \dots, t_{i,n}) \neq 1$. The theorem holds. ■

Proof of Corollary 3. Let $n \geq 1$ and let $G = \text{Sym}(5N)$ be the symmetric group on $5N$ points. Applying Theorem 1 to G we get that there exists a word

$w \in F_n$ such that for all $g_1, g_2, \dots, g_n \in G$, the tuple (g_1, g_2, \dots, g_n) satisfies w if and only if the subgroup $\langle g_1, g_2, \dots, g_n \rangle \leq G$ is solvable. In particular, every homomorphism from the one-relator group $\Gamma = \langle F_n \mid w \rangle$ to G has solvable image. We claim that Γ has the property stated in the corollary.

Indeed, let $\Delta \leq \Gamma$ be a subgroup such that $|\Gamma : \Delta| \leq N$. Assume indirectly that Δ could be mapped homomorphically onto F_2 . Then there exists a subgroup $\Pi \leq \Delta$ of index 5 such that the left coset action of Δ on Δ/Π is isomorphic to the alternating group $\text{Alt}(5)$. This implies that the left coset action of Γ on Γ/Π is not solvable. But $|\Gamma/\Pi| \leq 5N$, so Γ has a non-solvable homomorphic image in $\text{Sym}(5N) = G$, a contradiction. ■

Remark on Question 1. Let G be a finite group for which there exists a constant $c > 0$ such that for all $w \in F_\infty$ we have $P(G, w) > c$. Then as we saw for large enough d most of the d -tuples generate G and so for every word $w \in F_d$ there exists a generating set $\langle g_1, \dots, g_d \rangle = G$ such that $w(g_1, \dots, g_d) = 1$, that is, G is a quotient of the one-relator group $\langle F_d \mid w \rangle$. In particular, Amit's result [Ami] implies an affirmative answer for Question 1 for finite nilpotent groups.

References

- [Ami] A. Amit, On equations in nilpotent groups, in preparation
- [BaP] B. Baumslag and S. Pride, Groups with two more generators than relators, *J. London Math. Soc.* (2) 17 (1978), no. 3, 425–426
- [Fla] P. Flavell, Finite groups in which every two elements generate a soluble subgroup, *Invent. Math.* 121 (1995), no. 2, 279–285
- [Hal] P. Hall, The Eulerian functions of a group, *Quart. J. Math.* 7 (1936) 134–151
- [KaL] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* 36 (1990), no. 1, 67–87
- [DPSS] J. D. Dixon, L. Pyber, Á. Seress and A. Shalev, Residual properties of free groups and probabilistic methods, *J. Reine Angew. Math.* 556 (2003), 159–172
- [Rob] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, 80. Springer-Verlag, New York-Berlin, 1982.
- [St1] J. R. Stallings, Quotients of the powers of the augmentation ideal in a group ring, *Knots, groups, and 3-manifolds* (Papers dedicated to the memory of R. H. Fox), pp. 101–118. *Ann. of Math. Studies*, No. 84, Princeton Univ. Press, Princeton, N.J., 1975
- [Tho] J. G. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, *Bull. Amer. Math. Soc.* 74, 1968, 383–437

- [Wie] J. Wiegold, Growth sequences of finite groups III., J. Austral. Math. Soc. Ser. A 25 (1978), no. 2, 142–144.