Residual properties of free groups and probabilistic methods

John D. Dixon

László Pyber

Ákos Seress

Aner Shalev

Abstract

Let w be a non-trivial word in two variables. We prove that the probability that two randomly chosen elements x, y of a nonabelian finite simple group S satisfy $w(x, y) = 1$ tends to 0 as $|S| \to \infty$. As a consequence, we obtain a new short proof of a well-known conjecture of Magnus concerning free groups, as well as some applications to profinite groups.

Research partially supported by NSERC grant A7171 for J.D., the Hungarian Academy of Sciences grant AKP 96/2-675 for L.P., NSF grants CCR-9503430, CCR-9731799 for Á. S. and a grant from the Israel Science Foundation for A. S.

1991 *Mathematics Subject Classification:* 20D06, 20E05, 20E26, 20P05.

1 Introduction

Answering a much investigated classical question of Magnus in a series of papers [29, 30, 31] T.S. Weigel proved the following.

Theorem 1 *Let $\mathcal{S}$ be an infinite set of finite simple groups and let $k \geq 2$. Then the free group F_k of rank k is residually $\mathcal{S}$.*

Recall that a group G is called residually $\mathcal{C}$, where $\mathcal{C}$ is some class of groups, if the intersection of normal subgroups N of G such that $G/N \in \mathcal{C}$ is the trivial group. By a well-known result of A. Peluso [19], any free group of rank at least 2 is residually F_2. Therefore Theorem 1 is equivalent to the following.

Theorem 2 *Let $\mathcal{S}$ be an infinite set of finite simple groups. Let w be a non-trivial element of the free group F_2 on X, Y (i.e., a word in the variables X, Y). Then there exists a group $S \in \mathcal{S}$ and elements $x, y \in S$ such that $\langle x, y \rangle = S$ and $w(x, y) \neq 1$.*

The main aim of the present paper is to give a concise proof of a much stronger result.

Theorem 3 *Let S be a finite simple group and let w be a non-trivial element of the free group F_2 on X, Y. Then the probability that two randomly chosen elements x and y of S satisfy both $\langle x, y \rangle = S$ and $w(x, y) \neq 1$ tends to 1 as $|S| \to \infty$.*

Answering another classical question [4], Liebeck and Shalev [14] (following Dixon [4] and Kantor and Lubotzky [13]) have recently obtained the following.

Theorem 4 *Let S be a finite simple group and let S_0 be a group with $S \leq S_0 \leq Aut(S)$. If $P(S_0)$ is the probability that two randomly chosen elements of S_0 generate a subgroup containing S, then $P(S_0) \to 1$ as $|S_0| \to \infty$.*

This result, in the case $S_0 = S$, will play a major role below.

What we really prove in the present paper is the following.

Theorem 5 *Let S be a finite simple group and let $w(X, Y)$ be a non-trivial element of the free group F_2 on X, Y. Then the probability that two randomly chosen elements $x, y \in S$ satisfy $w(x, y) \neq 1$ tends to 1 as $|S| \to \infty$.*

Theorem 5 holds for words w in any number of variables $X_1, \ldots, X_k$, with a similar proof.

Theorem 3 clearly follows from the above two results: the number of pairs x, y for which either $\langle x, y\rangle \neq S$ or $w(x, y) = 1$ is negligible, therefore for almost all pairs *both* properties in the theorem hold. Our proof shows the power of probabilistic ideas in group theory. It should be noted that Weigel's proof of Theorem 1 also employs some probabilistic ideas. For other applications of Erdős-type probabilistic arguments in group theory see [10, 18, 15]. We note that Theorem 5 has already been applied in [17] in the solution of some Burnside-type problems.

Let us now turn to some applications involving profinite groups. Recall that a profinite group G (and its cartesian powers G^k) can be viewed as a probability space with respect to the Haar measure. As a consequence of Theorem 5 and the remark following it, we obtain the following.

Corollary 6 *Let G be the profinite completion of any of the groups* $\mathrm{SL}(d, \mathbb{Z})$ *or* $\mathrm{Aut}(F_d)$ *($d \geq 2$). Then a random k-tuple of elements of G generates a discrete subgroup isomorphic to F_k.*

Analogues of Corollary 6 for Lie groups and for some infinite permutation groups appear in [6, 5, 2, 9]. Related questions have been considered for absolute Galois groups of certain fields, where even stronger conclusions are sometimes satisfied. See for instance Theorem 16.13 of Fried and Jarden [7]. It is noteworthy that our proof of Corollary 6 works for all profinite groups with infinitely many nonabelian finite simple quotients (by open subgroups). This suggests the following problem.

Problem 7 *Let G be a profinite group with arbitrarily large nonabelian simple upper composition factors (i.e., composition factors of quotients by open normal subgroups). Is it true that a random k-tuple of elements of G generates a subgroup isomorphic to F_k?*

Using a probabilistic argument we also obtain:

Corollary 8 *Let G be the profinite completion of* $\mathrm{SL}(d, \mathbb{Z})$*, $d \geq 3$. Then G has a dense free subgroup of finite rank.*

For further work inspired by Corollary 8, see [22, 24].

We make some comments about the proof of our main result. For a fixed word w and for alternating groups of large degree or classical groups of large rank we prove the assertion of Theorem 5 by a direct counting argument. The proof for groups of Lie type of bounded rank uses tools from algebraic geometry. It obviously implies a result of G.A. Jones [12], that a proper subvariety of groups contains at most finitely many finite simple groups. Needless to say that the proofs of all results mentioned above rely on the Classification of Finite Simple Groups.

Residual properties of various free products have also been investigated [26, 27]. Forthcoming results from [23] show that the methods of this paper can be applied in these more general situations. In particular probabilistic arguments can be used to obtain new results on residual properties of $\mathrm{PSL}(2,\mathbb{Z})$. Results concerning random generation of simple groups by restricted pairs of elements or subgroups (which are clearly needed for such an approach) appear in [15, 21]. It also turns out that the probabilistic approach is useful in the study of residual properties of free pro-p groups. Some results in this direction are obtained by Barnea in [1].

It is known [20] that there exists an infinite 2-generator group G which generates the variety of all groups such that F_2 is not residually $\{G\}$. However the following is still undecided.

Problem 9 *Let $\mathcal{G}$ be a set of finite 2-generator groups which generates the variety of all groups. Is it true that F_2 is residually $\mathcal{G}$?*

Equivalently, the question is whether a non-trivial law $w(X,Y)$ which is satisfied by all generating pairs of a finite 2-generated group G implies a non-trivial law $w'(X,Y)$ (depending only on w) satisfied by all pairs of elements of G.

We are very grateful to Udi Hrushovski for helpful suggestions regarding Section 4, and for allowing us to quote his yet unpublished paper [11].

2 The setup

Suppose that an infinite set $\mathcal{S}$ of simple groups, and a word $w = w_1 w_2 \cdots w_r$ of length r in two variables X, Y (i.e., $w_i \in \{X, X^{-1}, Y, Y^{-1}\}$ for all $1 \leq i \leq r$) are given. We can suppose that w is reduced, i.e., no consecutive X, X^{-1} and Y, Y^{-1} occur in w. Let s denote the number of occurrences of X, X^{-1} and $t := r - s$ be the number of occurrences of Y, Y^{-1} in w.

We divide $\mathcal{S}$ into finitely many subsets:

$\mathcal{S}(0)$ contains the sporadic simple groups in $\mathcal{S}$.

$\mathcal{S}(1)$ contains the alternating groups in $\mathcal{S}$.

$\mathcal{S}(2)$ contains the linear groups $\mathrm{PSL}(d, q)$ in $\mathcal{S}$ with $d > r$.

$\mathcal{S}(3)$ contains the symplectic groups $\mathrm{PSp}(d, q)$ in $\mathcal{S}$ with $d > 2r + 10$.

$\mathcal{S}(4)$ contains the unitary groups $\mathrm{PSU}(d, q)$ in $\mathcal{S}$ with $d > 2r + 10$.

$\mathcal{S}(5)$ contains the orthogonal groups $\mathrm{P}\Omega(d, q)$ in $\mathcal{S}$ with $d > 2r + 10$.

We divide the remaining Lie-type groups in $\mathcal{S}$ into finitely many categories $\mathcal{S}(i)$ $(6 \leq i \leq c)$ such that within each category, the type of group and dimension is the same; in each category, only the size of the underlying field changes.

Clearly, it is enough to prove Theorem 5 separately for each infinite set $\mathcal{S}(i)$, $i \geq 1$. Cases $\mathcal{S}(1)$–$\mathcal{S}(5)$ are handled in Section 3. The basic idea of the proofs in each category is similar. The remaining categories $\mathcal{S}(i)$, $i \geq 6$, which consist of groups with bounded rank, are handled in Section 4 using ideas from algebraic geometry. Section 5 is devoted to the proof of the corollaries.

3 Groups with large rank

3.1 Alternating groups

Let $n > r+1$, let A_n act on the set Ω, $|\Omega| = n$, and let $\alpha_0 \in \Omega$ be fixed. Let P be the set of pairs (x, y) from A_n such that the sequence $A = (\alpha_0, \alpha_1, \ldots, \alpha_r)$ defined recursively by $\alpha_i := \alpha_{i-1}^{w_i(x,y)}$ consists of distinct elements. Clearly, each pair $(x, y) \in P$ satisfies $w(x, y) \neq 1$ so it is enough to show that $|P| / |A_n|^2 \to 1$ as $n \to \infty$.

The number of sequences $A = (\alpha_0, \alpha_1, ..., \alpha_r)$ with distinct elements is $(n-1)(n-2)\cdots(n-r)$. For a fixed A, the number of $x \in A_n$ satisfying $\alpha_i = \alpha_{i-1}^{w_i(x,y)}$ in all s positions with $w_i \in \{X, X^{-1}\}$ is $(n-s)!/2$, and the number of y satisfying $\alpha_i = \alpha_{i-1}^{w_i(x,y)}$ with $w_i \in \{Y, Y^{-1}\}$ is $(n-t)!/2$. (We have used the fact that w is reduced; otherwise, there would be no such x and y.) Hence

$$\frac{|P|}{|A_n|^2} = \frac{(n-1)(n-2)\cdots(n-r)}{n(n-1)\cdots(n-s+1)\cdot n(n-1)\cdots(n-t+1)} \to 1$$

as $n \to \infty$ since $s + t = r$.

3.2 Linear groups

Let $d > r$. First we consider $\mathrm{SL}(d, q)$, acting on the vector space $V = \mathrm{GF}(q)^d$. Let $0 \neq \alpha_0 \in V$ be fixed. Let P be the set of pairs (x, y) from $\mathrm{SL}(d, q)$ such that the sequence $A = (\alpha_0, \alpha_1, \ldots, \alpha_r)$ defined recursively by $\alpha_i := \alpha_{i-1}^{w_i(x,y)}$ consists of linearly independent vectors. Again, each $(x, y) \in P$ satisfies $w(x, y) \neq 1$.

For fixed α_0 the number of sequences $A = (\alpha_0, \alpha_1, ..., \alpha_r)$ of linearly independent vectors is $\prod_{j=1}^{r}(q^d - q^j)$. For a fixed A, the number of $x \in \mathrm{SL}(d, q)$ satisfying $\alpha_i = \alpha_{i-1}^{w_i(x,y)}$ in all s positions with $w_i \in \{X, X^{-1}\}$ is $(\prod_{j=s}^{d-1}(q^d - q^j))/(q-1)$, and the number of y satisfying $\alpha_i = \alpha_{i-1}^{w_i(x,y)}$ whenever $w_i \in \{Y, Y^{-1}\}$ is $(\prod_{j=t}^{d-1}(q^d - q^j))/(q-1)$. Hence

$$\frac{|P|}{|\mathrm{SL}(d,q)|^2} = \frac{\prod_{j=1}^{r}(q^d - q^j)}{\prod_{j=0}^{s-1}(q^d - q^j)\prod_{j=0}^{t-1}(q^d - q^j)} = 1 - O(q^{-(d-r)})$$

where the implied constant depends on r, but not on d and q. This will be true for all constants in Section 3.3 as well. Note that for a fixed bound M, there are at most $M \log M$ pairs d, q with $d > r$ such that $q^{d-r} < M$.

Now we consider $\mathrm{PSL}(d,q)$. Let P^* be the number of pairs (x,y) in $\mathrm{PSL}(d,q)$ such that the sequence $A = (\langle\alpha_0\rangle, \langle\alpha_1\rangle, \ldots, \langle\alpha_r\rangle)$ defined recursively by $\langle\alpha_i\rangle := \langle\alpha_{i-1}\rangle^{w_i(x,y)}$consists of linearly independent points of the projective space. Clearly $(x,y) \in P$ implies that $(xz_1, yz_2) \in P$ for all $z_1, z_2 \in Z(\mathrm{SL}(d,q))$. Thus

$$\frac{|P^*|}{|\mathrm{PSL}(d,q)|^2} = \frac{|P|}{|\mathrm{SL}(d,q)|^2} \to 1 \text{ as } q^{d-r} \to \infty.$$

3.3 Symplectic, unitary and orthogonal groups

We treat these groups uniformly. Let $d > 2r + 10$, and let $G := \mathrm{Sp}(d,q)$, $U(d,q)$ or $\mathrm{GO}(d,q)$ acting on the space $V := \mathrm{GF}(q)^d, \mathrm{GF}(q^2)^d$ or $\mathrm{GF}(q)^d$, respectively (for general reference to these groups and the properties which we shall use below see, for example, [25]).

Let $\alpha_0 \in V$ be a fixed nonzero singular vector. Let P be the set of pairs (x,y) from G such that the sequence $A = (\alpha_0, \alpha_1, \ldots, \alpha_r)$ defined recursively by $\alpha_i := \alpha_{i-1}^{w_i(x,y)}$ consists of linearly independent singular vectors. Such a sequence A will be called a *feasible sequence.* Clearly all pairs $(x,y) \in P$ satisfy $w(x,y) \neq 1$, and we shall show that the proportion of pairs $(x,y) \in G \times G$ which lie in P tends to 1 as $q^d \to \infty$.

In order to estimate the number of feasible sequences A we need general estimates for the number of singular vectors in a subspace of V.

Proposition 10 *Let $M(W)$ denote the number of nonzero singular vectors in a subspace W of V, and suppose $m := \dim(W)$ with $m > d/2$. Then:*

Symplectic case $M(W) = q^m - 1$;

Unitary case $M(W) = q^{2m-1} + O(q^{m+d/2})$;

Orthogonal case $M(W) = q^{m-1} + O(q^{m/2+d/4})$.

Proof. The symplectic case is clear since every vector in a symplectic space is singular, so consider the unitary case. Suppose that the radical $R(W)$ of W has dimension k, and choose a subspace U of W such that $W = R(W) \perp U$.

Note that since $R(V) = 0$, $\dim R(W) \leq d/2$, and so $\dim U = m - k > 0$. Thus U is a nontrivial subspace for which the restriction of the unitary form is nonsingular. This means that the number $M(U)$ of nonzero singular vectors in U is $(q^{m-k} - (-1)^{m-k})(q^{m-k-1} - (-1)^{m-k-1})$ (see [25] Lemma 10.4). Finally, for each $w \in R(W)$ and $u \in U$, $w + u$ is singular if and only if u is singular. Hence $M(W) = q^{2k}M(U) + q^{2k} - 1 = q^{2m-1} + O(q^{m+k}) = q^{2m-1} + O(q^{m+d/2})$ as asserted.

Now consider the orthogonal case. Again we can write $W = R(W) \perp U$ with $\dim R(W) = k \leq d/2$ and $\dim U = m - k > 0$, so U is a nontrivial subspace for which the restriction of the orthogonal form is nonsingular. Thus the number $M(U)$ of nonzero singular vectors in U is $q^{m-k-1}-1$ if $m-k$ is odd, and is $q^{m-k-1}-1 \pm (q-1)q^{(m-k)/2-1}$ if $m-k$ is even, depending on the Witt index (see [25] page 140). If the totally isotropic space $R(W)$ is totally singular then, as in the unitary case, we get $M(W) = q^k M(U) + q^k - 1 = q^{m-1} + O(q^{m/2+d/4})$.

However, in the orthogonal case when q is even, it is possible for a totally isotropic subspace not to be totally singular (see [25] page 54); the set of singular vectors then forms a hyperplane of the subspace. Suppose that $R(W)$ is not totally singular, and let ϕ denote the quadratic form on V. For each $w \in R(W)$ and nonsingular $u \in U$, the vector $u + cw$ is singular if and only if $\phi(u + cw) = \phi(u) + c^2\phi(w)$ equals 0. If w is singular then there is clearly no such $c \in \mathrm{GF}(q)$; and if w is nonsingular then there is exactly one such c because each element in $\mathrm{GF}(q)$ has a unique square root (since q is even). Thus there are $M_0 := (q^{m-k} - 1 - M(U))(q^k - q^{k-1})/(q - 1) = q^{m-1} - q^{k-1}(M(U) + 1)$ singular vectors in W of the form $u + w$ where $u \in U$ is nonsingular and $w \in R(W)$. On the other hand, if $u \in U$ is singular and $w \in R(W)$ then $u + w$ is singular if and only if w is. Thus the total number of nonzero singular vectors in W is $M(W) = q^{k-1}M(U) + q^{k-1} - 1 + M_0 = q^{m-1} - 1$. This completes the orthogonal case. ∎

We estimate the number of feasible sequences $A = (\alpha_0, \alpha_1, \ldots, \alpha_r)$. Suppose that $(\alpha_0, \alpha_1, \ldots, \alpha_{i-1})$ is already defined and suppose that w_i is the jth occurence of X, X^{-1}. So far, we have $j - 1$ restrictions of the form $\alpha^x = \beta$, where $\{\alpha, \beta\} = \{\alpha_{l-1}, \alpha_l\}$ and $w_l \in \{X, X^{-1}\}$. If $w_i = X$ then let B be the subspace spanned by the $j - 1$ values of β; if $w_i = X^{-1}$ then let B be the subspace spanned by the $j - 1$ values of α.

Take a pair (x, y) from G which witnesses that the partial sequence

$(\alpha_0, \alpha_1, \ldots, \alpha_{i-1})$ is feasible. Put $\delta := \alpha_{i-1}^{w_i(x,y)}$, and consider the points of the form $\alpha_i := \delta + \beta$ where $\beta \in B^\perp$, α_i is singular, and $\alpha_i \notin \langle \alpha_0, \alpha_1, \ldots, \alpha_{i-1} \rangle$. Since δ is singular, the linear map which fixes $\alpha_0, \alpha_1, ..., \alpha_{i-1}$ and maps δ onto α_i is an isometry between two subspaces, and Witt's theorem (see [25] Theorem 7.4) shows that this can be extended to an isometry x_0 of V. Now (xx_0, y) (respectively $(x_0^{-1}x, y)$) is a witness to the feasibility of the sequence $(\alpha_0, \alpha_1, \ldots, \alpha_i)$ depending on whether $w_i = X$ or X^{-1}, respectively. Thus to estimate the number of possible extensions of $(\alpha_0, \alpha_1, \ldots, \alpha_{i-1})$ to a feasible sequence of length $i+1$ we need to estimate the number of singular vectors in $\left\{\delta + \beta | \beta \in B^\perp\right\}$.

Proposition 11 *With the notation above, the number N of singular vectors in $\left\{\delta + \beta | \beta \in B^\perp\right\}$ is:*

Symplectic case q^{d-j+1};

Unitary case $q^{2d-2\bar{j}+1}(1 + O(q^{-d/2+j}))$;

Orthogonal case $q^{d-j}(1 + O(q^{-d/4+(j+1)/2}))$.

Proof. The symplectic case follows at once since all vectors are singular and $B^\perp$ has dimension $d - j + 1$.

Now consider the unitary case. If $\langle \delta \rangle^\perp$ contains $B^\perp$, then $\delta + \beta$ is singular if and only if β is singular; then $N = M(B^\perp)$ and the result follows from Proposition 10. Thus suppose that $\langle \delta \rangle^\perp$ does not contain $B^\perp$. Now for each nonsingular $\gamma \in B^\perp \setminus \langle \delta \rangle^\perp$, there are exactly q values $c \in \mathrm{GF}(q^2)^*$ such that $\delta + c\gamma$ is singular because δ and γ define a hyperbolic line, which has $q+1$ singular points, including $\langle \delta \rangle$. On the other hand, for each singular $\gamma \in B^\perp \setminus \langle \delta \rangle^\perp$, there are exactly $q-1$ such values $c \in \mathrm{GF}(q^2)^*$ because $\langle \gamma \rangle$ itself is one of the singular points on the hyperbolic line. Hence the number of $\beta \in B^\perp$ for which $\delta + \beta$ is singular is given by:

$$\begin{aligned} N &= M(\langle \delta \rangle^\perp \cap B^\perp) + \frac{q^{2d-2j+2} - q^{2d-2j}}{q^2-1} q - \frac{(M(B^\perp) - M(\langle \delta \rangle^\perp \cap B^\perp))}{q^2-1} \\ &= q^{2d-2j+1} + \frac{q^2 M(\langle \delta \rangle^\perp \cap B^\perp) - M(B^\perp)}{q^2-1} \\ &= q^{2d-2j+1} + \frac{q^{2d-2j+1} + O(q^{3d/2-j+2}) - q^{2d-2j+1} + O(q^{3d/2-(j-1)})}{q^2-1} \\ &= q^{2d-2j+1}(1 + O(q^{-d/2+j})). \end{aligned}$$

We finally turn to the orthogonal case. Once again, if $\langle\delta\rangle^\perp$ contains $B^\perp$ then $N = M(B^\perp)$ and so the result follows from Proposition 10. Thus suppose that $\langle\delta\rangle^\perp$ does not contain $B^\perp$. Then for each nonsingular $\gamma \in B^\perp \setminus \langle\delta\rangle^\perp$, there is exactly one $c \in \mathrm{GF}(q)^*$ such that $\delta + c\gamma$ is singular because δ and γ define a hyperbolic line, which has two singular points, including $\langle\delta\rangle$. If $\gamma \in B^\perp \setminus \langle\delta\rangle^\perp$ is singular then there is no such $c \in \mathrm{GF}(q)^*$ because the other singular point on the hyperbolic line is $\langle\gamma\rangle$ itself. Hence the number of $\beta \in B^\perp$ for which $\delta + \beta$ is singular is given by:

$$\begin{aligned} N &= M(\langle\delta\rangle^\perp \cap B^\perp) + \frac{q^{d-j+1} - q^{d-j} - (M(B^\perp) - M(\langle\delta\rangle^\perp \cap B^\perp))}{q-1} \\ &= q^{d-j} + \frac{qM(\langle\delta\rangle^\perp \cap B^\perp) - M(B^\perp)}{q-1} \\ &= q^{d-j} + \frac{q^{d-j} + O(q^{3d/4-j/2+1}) - q^{d-j} + O(q^{3d/4-(j-1)/2})}{q-1} \\ &= q^{d-j}(1 + O(q^{-d/4+j/2})). \end{aligned}$$

This completes the proof for all cases. ∎

Since $\alpha_i \notin \langle\alpha_0, \alpha_1, ..., \alpha_{i-1}\rangle$, the number of extensions of a feasible partial sequence $(\alpha_0, \alpha_1, \ldots, \alpha_{i-1})$ to a feasible partial sequence $(\alpha_0, \alpha_1, \ldots, \alpha_i)$ is at least $N - q^i$ (in the symplectic and orthogonal cases) and at least $N - (q^2)^i$ (in the unitary case). The value of N given in the previous proposition was based on the assumption that $w_i = X$ or X^{-1}, but it is clear that an analogous result holds when $w_i = Y$ or Y^{-1}.

Proposition 12 *Let L be the number of feasible sequences $(\alpha_0, \alpha_1, \ldots, \alpha_r)$. Then:*

Symplectic case $L \geq q^{d(s+t)-(s^2+t^2-s-t)/2}(1 + O(q^{-d+2r-1}))$;

Unitary case $L \geq q^{2d(s+t)-(s^2+t^2)}(1 + O(q^{-d/2+r}))$;

Orthogonal case $L \geq q^{d(s+t)-(s^2+t^2+s+t)/2}(1 + O(q^{-d/4+(r+1)/2}))$.

Proof. The observations above and the value of N given in Proposition 11 show that there is some rearrangement $i_1, i_2, ..., i_s, k_1, k_2, ..., k_t$ of $1, 2, ..., r$ such that:

in the symplectic case

$$L \geq \prod_{j=1}^{s}(q^{d-j+1} - q^{i_j}) \prod_{l=1}^{t}(q^{d-l+1} - q^{k_l});$$

in the unitary case

$$L \geq \prod_{j=1}^{s}(q^{2d-2j+1}(1+O(q^{-d/2+j}))-q^{2i_j}) \prod_{l=1}^{t}(q^{2d-2l+1}(1+O(q^{-d/2+l}))-q^{2k_l});$$

and, in the orthogonal case

$$L \geq \prod_{j=1}^{s}(q^{d-j}(1 + O(q^{-d/4+(j+1)/2})) - q^{i_j}) \prod_{l=1}^{t}(q^{d-l}(1 + O(q^{-d/4+(l+1)/2})) - q^{k_l}).$$

The estimates now follow easily. ∎

Finally, since α_0 is fixed, each pair $(x, y) \in P$ has exactly one feasible sequence. On the other hand, for each feasible sequence $(\alpha_0, \alpha_1, \ldots, \alpha_r)$, the set of corresponding $(x, y) \in P$ forms a coset in $G \times G$ of the subgroup $G_1 \times G_2$ where G_1 is the pointwise stablizer in G of the subspace spanned by the s vectors α_i for which $\alpha_i^x = \alpha_{i-1}$ or α_{i+1}, and G_2 is the pointwise stabilizer of the analogous subspace for y. The following will be used to estimate the size of these pointwise stabilizers.

Proposition 13 *Let $m < d/2$ and let $I_{m,d}$ denote the set of all sequences $(\beta_1, \beta_2, ..., \beta_m)$ which form a basis of a totally singular subspace of a d-dimensional nondegenerate space V (equivalently, $\beta_1, \beta_2, ..., \beta_m$ are linearly independent, singular and pairwise orthogonal). Then:*

Symplectic case $|I_{m,d}| = q^{dm-m(m-1)/2}(1 + O(q^{-d+2m-2}))$;

Unitary case $|I_{m,d}| = q^{2dm-m^2}(1 + O(q^{-d/2+m}))$;

Orthogonal case $|I_{m,d}| = q^{dm-m(m+1)/2}(1 + O(q^{-d/4+(m+1)/2}))$.

Proof. β_1 can be chosen in $M(V)$ ways; and after $\beta_1, \beta_2, ..., \beta_{i-1}$ have been chosen, β_i can be chosen as any nonzero singular vector in $\langle \beta_1, \beta_2, ..., \beta_{i-1} \rangle^\perp$ provided $\beta_i \notin \langle \beta_1, \beta_2, ..., \beta_{i-1} \rangle$. Using Proposition 10 and the fact that $\langle \beta_1, \beta_2, ..., \beta_{i-1} \rangle \subseteq \langle \beta_1, \beta_2, ..., \beta_{i-1} \rangle^\perp$ we obtain:

in the symplectic case $|I_{m,d}| = \prod_{j=0}^{m-1}(q^{d-j} - q^j) = q^{dm-m(m-1)/2}(1+O(q^{-d+2m-2}))$;

in the unitary case $|I_{m,d}| = \prod_{j=0}^{m-1}(q^{2d-2j-1} + O(q^{3d/2-j}) - (q^2)^j) = q^{2dm-m^2}(1+O(q^{-d/2+m}))$;

in the orthogonal case $|I_{m,d}| = \prod_{j=0}^{m-1}(q^{d-j-1} + O(q^{3d/4-j/2}) - q^j) = q^{dm-m(m+1)/2}(1+O(q^{-d/4+(m+1)/2}))$. ∎

We now estimate the index of a pointwise stabilizer of a subspace W of V and show that, asymptotically, this depends only on the dimension of W.

Proposition 14 *Let W be a subspace of V of dimension m where $m < d/2$, and let H be the pointwise stabilizer of W in G. Then $|G : H| = |I_{m,d}|\,(1 + O(q^{-d/4+(m+1)/2}))$.*

Proof. Suppose that the radical $R(W)$ of W has dimension k and let U be a subspace of W such that $W = R(W) \perp U$. Then $R(U) = 0$ and so $U^\perp \cap W = R(W)$. Each isometry of $U^\perp$ which fixes $R(W)$ pointwise extends in a unique way to an isometry of V which fixes W pointwise. Thus H is isomorphic to the pointwise stabilizer H_0 of $R(W)$ in the group G_0 of isometries of $U^\perp$. Since V is nondegenerate, $U^\perp$ is also nondegenerate, and so G_0 is a symplectic, unitary or orthogonal group in the respective cases. Put $l := m - k$. Then $\dim U^\perp = \dim V - l$, and so from the order formulas (see [25] pages 70, 118 and 141) we get: $|G| \,/\, |G_0| = q^{dl-l(l-1)/2}(1 + O(q^{-d+l}))$ for the symplectic case; $q^{2dl-l^2}(1 + O(q^{-d+l}))$ in the unitary case; and $q^{dl-l(l+1)/2}(1 + O(q^{-d+l}))$ in all orthogonal cases.

Now let $I_{k,d-l}$ denote the set of all sequences which form bases of totally isotropic subspaces of dimension k in $U^\perp$. Witt's theorem shows that G_0 acts transitively on $I_{k,d-l}$, and so $|H| = |H_0| = |G_0| \,/\, |I_{k,d-l}|$. Substituting the value of $|I_{k,d-l}|$ from Proposition 13, we obtain that $|G : H| = (|G|/|G_0|)\,|I_{k,d-l}|$ as stated. ∎

The last proposition shows that the number of pairs $(x, y) \in P$ which are witnesses to a particular feasible sequence A is $|G|^2 \,/ (|I_s|\,|I_t|)(1+O(q^{-d/4+(r+1)/2}))$.

Hence $1 \geq |P| \,/\, |G|^2 \geq L/(|I_s|\,|I_t|)(1 + O(q^{-d/4+(r+1)/2}))$ where L is given in Proposition 12. Thus $|P| \,/\, |G|^2 = 1 + O(q^{-d/4+(r+1)/2})$.

Now let $P_0 = P \cap (G' \times G')$ and note that $|G : G'|$ equals 1 for the symplectic case, $q+1$ in the unitary case, and is at most 4 in the orthogonal case. Thus in all cases $|P_0| \,/\, |G'|^2 \geq (|P| - (|G|^2 - |G'|^2))/|G'|^2 = 1 + O(q^{-d/4+(r+1)/2+2}) \to 1$ as $q^d \to \infty$ since we have assumed that $d > 2r + 10$.

This shows that, as $q^d \to \infty$, almost all pairs (x, y) from the derived groups $\mathrm{Sp}(d, q)$, $\mathrm{SU}(d, q)$ and $\Omega(d, q)$ lie in P and hence satisfy $w(x, y) \neq 1$. The transition to the corresponding projective groups is now analogous to that for $\mathrm{PSL}(d, q)$.

4 Groups with bounded rank

The finite simple groups of Lie type of bounded rank (say $\leq c$) split into finitely many "horizontal" families, such that the groups in each family are of fixed type (and rank), and only the field varies. Therefore it suffices to consider groups in one horizontal family.

Each such family of finite simple groups arises from some simple algebraic group G (which can be taken to be a Chevalley group, defined over the integers $\mathbb{Z}$, and thereby over algebraically closed fields of any characteristic). While in most cases the procedure is simply taking fixed points of Frobenius automorphisms, the following generalization is needed in order to include the Ree and the Suzuki families.

Given a prime p and a power $q = p^m$ of p, let K_p be an algebraically closed field of characteristic p, endowed with the Frobenius automorphism $\phi_q : x \mapsto x^q$. Let G be a simple Chevalley group, and let $h : G \to G$ be an endomorphism (arising from a graph endomorphism) such that h^2 or h^3 equals either the identity or a Frobenius automorphism. We also permit $h = \mathrm{Id}_G$. We note that for $p \geq 5$ the endomorphism h is defined over $\mathbb{Z}$ and satisfies $h^i = \mathrm{Id}_G$ for some $i = 1, 2, 3$. If $p = 2, 3$ and h^2 or h^3 is a Frobenius automorphism then h is only defined over $\mathbb{Z}/p\mathbb{Z}$. Now consider the group

$$G_q = \{a \in G(K_p) : \phi_q(a) = h(a)\}.$$

Then the groups G_q include – as bounded index subgroups – all the horizontal families of finite simple groups.

Our main tool in this section is the following result due (among others) to Hrushovski (see [H, Lemma 2.18]). Recall that A^n denotes the n-dimensional

affine space.

Lemma 15 *Given positive integers d, e, f, n there exists a constant $B = B(d, e, f, n)$ with the following property: for every prime p and a power $q = p^m$, and for every affine variety V in A^n of dimension at most d defined over K_p by at most e polynomial equations of degree at most f, and for every endomorphism $h : V \to V$ defined (in V^2) over K_p by at most e polynomial equations of degree at most f, we have*

$$|\{a \in V : \phi_q(a) = h(a)\}| \leq Bq^d.$$

Let $d = \dim G$. It is well known that the group G_q has $(1+o(1))q^d$ points (sharper estimates can be found in [H]).

Now fix an integer $k \geq 1$ and let V be a proper subvariety of the (irreducible) variety G^k. Then $\dim V \leq kd-1$, and by Lemma 15, $V \cap (G_q)^k$ has at most Bq^{kd-1} points, where B is a constant depending only on the relevant parameters associated with G, h, V.

By a theorem of Platonv (see Theorem 10.15 in [28]), a linear group is either solvable-by-finite or generates the variety of all groups. In particular, if w is a non-trivial word in X, Y, and G is a simple algebraic group, then w cannot be identically 1 on G^2. Thus the variety V cut out by $w = 1$ is a proper subvariety of G^2, and we obtain

$$|\{(x, y) \in G_q \times G_q : w(x, y) = 1\}| \leq Bq^{2d-1}.$$

It follows that the probability that $w(x, y) = 1$ in G_q (or in some bounded index subgroup of G_q) is in $O(q^{-1})$; in particular, this probability tends to 0 as $q \to \infty$.

The reader should note that the above argument works not only when the characteristic p is fixed, but also when p tends to infinity. Indeed, in the latter case (assuming $p \geq 5$ as we may), G, h, V are all defined over $\mathbb{Z}$. Therefore the parameters d, e, f, n in Lemma 15, and with them the constant B, do not depend on p.

This completes the proof of Theorem 5. ∎

5 The corollaries

Proof of Corollary 6. Consider the following subsets of G^k:

$F := \{X \mid \langle X \rangle \text{ is a free group of rank } k\}$ and

$F(w) := \{X \mid w(X) \neq 1\}$,

where $X \in G^k$ and w is a reduced word in the free group of rank k. We want to prove that the complement F^c of the set F has measure $\mu(F^c) = 0$. Since $F = \bigcap_{w \neq 1} F(w)$, it suffices to prove that $\mu(F(w)^c) = 0$ for every $w \neq 1$.

By a result of Gilman [8], $\mathrm{Aut}(F_d)$ has arbitrarily large alternating quotients A_n. Hence the same is true for the profinite completion $G = \widehat{\mathrm{Aut}(F_d)}$.

Now $\mu(F(w)^c)$ is less than the proportion of k-tuples of A_n satisfying $w(x_1, \ldots, x_k) = 1$. As pointed out in the introduction, an obvious modification of the proof of Theorem 5 shows that this proportion tends to 0 as $n \to \infty$. Hence $\mu(F(w)^c) = 0$ as required.

For the groups $\widehat{\mathrm{SL}(d, \mathbb{Z})}$, and for any profinite group G with arbitrarily large nonabelian simple quotients modulo open subgroups, the assertion follows in a similar way.

■

Proof of Corollary 8. Let G denote the profinite group $\widehat{\mathrm{SL}(d, \mathbb{Z})}$, $d \geq 3$. As proved in [16], there is a number $k = k(d)$ such that the probability that k random elements generate a dense (discrete) subgroup of G is positive (see [3] for a much more general result). Using Corollary 6, we see that the probability that a random k-tuple of G generates a dense F_k subgroup is also positive. In particular G has a dense free subgroup of finite rank. ■

References

[1] Y. Barnea, Residual properties of free pro-p groups, in preparation.

[2] M. Bhattacharjee, The ubiquity of free subgroups in certain inverse limits of groups, *J. Algebra* **172** (1995), 134–146.

[3] A.V. Borovik, L. Pyber, A. Shalev, Maximal subgroups in finite and profinite groups, *Trans. Amer. Math. Soc.* **348** (1996), 3745–3761.

[4] J.D. Dixon, The probability of generating the symmetric group, *Math. Z.* **110** (1969), 199–205.

[5] J.D. Dixon, Most finitely generated permutation groups are free, *Bull. London Math. Soc.* **22** (1990), 222–226.

[6] D.B.A. Epstein, Almost all subgroups of a Lie group are free, *J. Algebra* **19** (1971), 261–262.

[7] M.D. Fried, M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 1986.

[8] R. Gilman, Finite quotients of the automorphism group of a free group, *Can. J. Math.* **29** (1977), 541–551.

[9] A.M.W. Glass, The ubiquity of free groups, *The Math. Intelligencer* **14** (1992), 54–57.

[10] R.M. Guralnick, W. M. Kantor, Probabilistic generation of finite simple groups, to appear in *J. Algebra*.

[11] E. Hrushovski, The first order theory of the Frobenius automorphisms, to appear.

[12] G.A. Jones, Varieties and simple groups, *J. Austr. Math. Soc.* **17** (1974), 163–173.

[13] W.M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Ded.* **36** (1990), 67–87.

[14] M.W. Liebeck, A. Shalev, The probability of generating a finite simple group, *Geom. Ded.* **56** (1995), 103–113.

[15] M.W. Liebeck, A. Shalev, Classical groups, probabilistic methods, and the $(2,3)$-generation problem, *Annals of Math.* **144** (1996), 77–125.

[16] A. Mann, Positively finitely generated groups, *Forum Math.* **8** (1996), 429–459.

[17] A. Mann and C. Martinez, The exponent of finite groups, *Arch. Math.* **67** (1996), 8–10.

[18] A.Yu. Ol'shanskii, The number of generators and orders of abelian subgroups of finite p-groups, *Math. Notes* **23** (1978), 183–185.

[19] A. Peluso, A residual property of free groups, *Comm. Pure Appl. Math.* **19** (1966), 435–437.

[20] S.J. Pride, Residual properties of free groups III, *Math. Z.* **132** (1973), 245–248.

[21] L. Pyber, Dixon-type theorems, preprint.

[22] L. Pyber, Dense free subgroups in profinite groups, in preparation.

[23] A. Shalev, Residual properties of the modular groups and other free products, in preparation.

[24] G.A. Soifer, T.N. Venkateramana, Finitely generated profinitely dense, free subgroups in higher rank semisimple groups, to appear.

[25] D.E. Taylor, *The Geometry of the Classical Groups*, Heldermann, Berlin, 1992.

[26] M.C. Tamburini, J.S. Wilson, A residual property of free products, *Math. Z.* **186** (1984), 525–530.

[27] M.C. Tamburini, J.S. Wilson, On the generation of finite simple groups by pairs of subgroups, *J. Algebra* **116** (1988), 316–333.

[28] B.A.F. Wehrfritz, *Infinite Linear Groups*, Springer, Berlin, 1973.

[29] T.S. Weigel, Residual properties of free groups, *J. Algebra* **160** (1993), 16–41.

[30] T.S. Weigel, Residual properties of free groups II, *Comm. Algebra* **20** (1992), 1395–1425.

[31] T.S. Weigel, Residual properties of free groups III, *Israel J. Math.* **77** (1992), 65–81.

Authors' addresses:

Department of Mathematics, Carleton University
Ottawa, Ontario K15 5B6, Canada
email: jdixon@math.carleton.ca

Mathematical Institute of the Hungarian Academy of Sciences
1053 Budapest, Hungary
email: pyber@math-inst.hu

Department of Mathematics, The Ohio State University
Columbus, OH 43210, USA
email: akos@math.ohio-state.edu

Institute of Mathematics, The Hebrew University
Jerusalem 91904, Israel
email: shalev@math.huji.ac.il