On a question of B.H. Neumann

Robert Guralnick
Department of Mathematics
University of Southern California
E-mail: guralnic@math.usc.edu

Igor Pak
Department of Mathematics
Massachusetts Institute of Technology
E-mail: pak@math.mit.edu

February 21, 2002

Abstract

The automorphism group of a free group $\mathrm{Aut}(F_k)$ acts on the set of generating k-tuples $(g_1, \ldots, g_k)$ of a group G. Higman showed that when $k = 2$, the union of conjugacy classes of the commutators $[g_1, g_2]$ and $[g_2, g_1]$ is an orbit invariant. We give a negative answer to a question of B.H. Neumann, as to whether there is a generalization of Higman's result for $k \geq 3$.

1 Introduction

Let G be a finite group, and let $d(G)$ be the minimum number of generators in G. For every $k \geq d(G)$, let $\mathcal{N}_k(G) = \{ (g_1, \ldots, g_k) \in G^k \,:\, \langle g_1, \ldots, g_k \rangle = G\}$ be the set of generating k-tuples in G. One can identify $\mathcal{N}_k(G)$ with the set of epimorphisms $\mathrm{Epi}(F_k \to G)$. The gives a natural action of $\mathrm{Aut}(F_k)$ on $\mathcal{N}_k(G)$ defined by $\alpha : \phi \to \phi \circ \alpha$, where $\alpha \in \mathrm{Aut}(F_k)$ and $\phi \in \mathrm{Epi}(F_k \to G)$. Consider also the diagonal action of $\mathrm{Aut}(G)$ on $\mathcal{N}_k(G)$. The orbits of $\mathrm{Aut}(F_k) \times \mathrm{Aut}(G)$ acting on $\mathcal{N}_k(G)$ are called *T-systems* (short for "systems of transitivity"), and were introduced by B.H. and H. Neumann in [NN] (see also [G, E2, N, NN, P].)

Let w be a nontrivial word in the free group F_k, and let $\varphi_w : \mathcal{N}_k \to G$ be the associated map $\varphi_w(g_1, \ldots, g_k) = w(g_1, \ldots, g_k)$. We say that w is *invariant* on T-systems in G, if the set of $\mathrm{Aut}(G)$-conjugates of $\{\varphi_w(g_1, \ldots, g_k)^{\pm 1}\}$ is invariant on all generating k-tuples in a T-system. Higman's result (which we refer to as Higman's Lemma in this paper) states that for $k = 2$, the commutator $[g_1, g_2]$ is invariant on T-systems of every group G (see [N, P]). In [N], B.H. Neumann asks whether there exists a generalization of Higman's Lemma for $k \geq 3$. We give a negative answer to this question:

Theorem 1.1 *For every nontrivial word $w \in F_k$, where $k \geq 3$, there exist a finite group G, such that w is not invariant on T-systems in G.*

The proof is based on a result by R. Gilman [G], that for each $k \geq 3$ group $\mathrm{PSL}(2,p)$ has a unique T-system. In fact, we prove that the map φ_w takes unboundedly many values on this T-system, when $p \to \infty$. The proof idea was motivated by a recent paper [LS].

We say a few words about the history of the problem. Let $\tau_k(G)$ be the number of T-systems. When $k = d(G)$, it was shown in [NN], that $\tau_k(G) > 1$ in several special cases (e.g. $G = A_5$.) In fact, $\tau_k(G)$ is unbounded, as shown in [D1]. An example of a solvable G with $\tau_k(G) > 1$ and $k = d(G)$, was found in [N], answering a question of Gaschütz. In the opposite direction, it was shown in [D2] that $\tau_k(G) = 1$ when $k > d(G)$, and G is a finite solvable group. It is conjectured that $\tau_k(G) = 1$ for all finite G and $k > d(G)$ [P]. When G is a finite simple group this is known as Wiegold's Conjecture, confirmed in several special cases, in particular for $\mathrm{PSL}(2,p)$ (see [CP, E2, G, P]). One implication of the conjecture is a positive answer to Waldhausen's question: If $G = \langle x_1, \ldots, x_k \,|\, r_1, \ldots, r_n \rangle$, and $k > d(G)$, is it true that the normal closure of $\langle r_1, \ldots, r_m \rangle$ in F_n contains a primitive element of F_n? (see [D2].)

Now, given a word w such that the map $\varphi_w : \mathcal{N}_k(G) \to G$ is invariant on T-systems, we obtain $\tau_k(G) \geq |\mathrm{Im}(\varphi_w)|/2$, where $\mathrm{Im}(\varphi_w) \subset G$ is an image of the map φ_w. This is exactly the strategy used by B.H. Neumann in [N], when $w = [x_1, x_2]$ and $k = 2$. Theorem 1.1 implies that this strategy fails when $k = 3$, by using Neumann's idea in the reverse direction. Interestingly, our proof of Theorem 1.1 can be adapted for the case $k = 2$, when it implies the following result:

Theorem 1.2 *The number of T-systems in* $\mathrm{PSL}(2,p)$ *is unbounded, when $k = 2$, and as $p \to \infty$.*

This result is due to Evans [E1], who proved it by an explicit construction. A similar result for alternating groups A_n was recently obtained in [P] by using Higman's Lemma and a simple combinatorial construction (see also [E1]).

Remark 1.3 One can ask to characterize all words w that can be used in Higman's Lemma for $k = 2$. We conjecture that w must be a conjugate of $[g_1, g_2]^m$, where $m \in \mathbb{Z}$.

Remark 1.4 It would be interesting to quantify the lower bound on the number of T-systems of $\mathrm{PSL}(2,p)$, when $k = 2$, which we obtain implicitly in the proof of Theorem 1.2. The result should be compared with that of Theorem 3.17 in [E1]. With more effort, the methods used in this paper can be adapted to prove the same result for any fixed type of Chevalley group X – i.e. the number of T-systems in $X(q)$ goes to infinity as $q \to \infty$. Different methods would be needed to prove the same result for all simple groups as the order tends to infinity.

Remark 1.5 In the recent years, much attention has been brought to the subject by the "practical" product replacement algorithm. In fact, this was our motivation for study of the number of T-systems. We refer to [P] for an extensive review of the subject, applications and references.

Acknowledgments We would like to thank Martin Evans for the reference [E1], and an anonymous referee for helpful remarks. This paper was written when the second author was a Fellow at MSRI in Berkeley, California. The first author was partially supported by an NSF grant.

2 Preliminary results

Let w be a nontrivial word in the free group of rank k, and let G be any group. The word w defines a map $\varphi_w : G^k \to G$, by $\varphi_w(g_1, \dots, g_k) \to w(g_1, \dots, g_k)$.

We now consider subgroups of $G := \mathrm{SL}(2, \mathbb{C})$ – there are obvious analogs for other Lie groups. Since G contains a free group [H], we see that φ_w is not identically 1 (or even central).

Since $G_c := \mathrm{SU}(2, \mathbb{C})$ and $\Gamma := \mathrm{SL}(2, \mathbb{Z})$ are both Zariski dense in G, it follows that w does not induce the trivial map on H^k for $H = G_c$ or Γ. Consider a map $\chi_w = \mathrm{tr} \circ \varphi_w : G_c^k \to \mathbb{C}$, defined by $\chi_w(g_1, \dots, g_k) = \mathrm{tr}(w(g_1, \dots, g_k))$, where $(g_1, \dots, g_k) \in G^k$.

Since G_c is compact, it contains only semisimple elements. Therefore, the map $\chi_w : G_c^k \to \mathbb{C}$ takes on some value other than 2 (if $\chi_w(g_1, \dots, g_k) = 2$, it follows that $w(g_1, \dots, g_k)$ is unipotent). Since the image of φ_w contains 1, the integer 2 is in the image of $\chi_w = \mathrm{tr} \circ \varphi_w$.

Since G_c^k is connected, this implies that the image of χ_w is infinite. Thus,

Lemma 2.1 *The image of w intersects infinitely many semisimple conjugacy classes of G.*

We need to record some simple facts about subgroups of G and $\mathrm{SL}(2, p)$ with respect to representations (see [C]).

Lemma 2.2 *Let H be a proper closed subgroup of G. Then H acts reducibly in any rational representation of G of dimension $d > 5$.*

Proof. Let V be any rational G-module of dimension $d > 5$. The subgroups of G are well known. If H has positive dimension, then either H is contained in a Borel subgroup of G (and so has a 1-dimensional invariant subspace) or normalizes a torus. The normalizer of a torus has no irreducible representations of dimension more than 2.

So it suffice to assume that H is finite. Let N be a minimal normal noncentral (in G) subgroup of H. If N is cyclic, then H is contained in the normalizer of a torus, a contradiction as above. If N is an extraspecial 2-group, then H/N embeds in S_3 and any irreducible representation is at most 4-dimensional. The only other possibility is that $N = SL(2,5)$. The largest irreducible representation of $SL(2,5)$ is 5-dimensional. □

The same proof (considering finite subgroups only) yields the following:

Lemma 2.3 *Let H be a proper subgroup of $SL(2,p)$. If V is a d-dimensional $SL(2,p)$-module in characteristic p with $d > 5$, then H acts reducibly.*

We next turn to generating k-tuples. We need to assume $k \geq 2$ for this (to ensure that there exist generating k-tuples.) Let π_p denote the natural map from $\Gamma = \mathrm{SL}(2,\mathbb{Z})$ to $\mathrm{SL}(2,p)$. Consider

$$X = \big\{(g_1,\ldots,g_k) \in \Gamma^k \, : \, \pi_p(\langle g_1,\ldots,g_k\rangle) = \mathrm{SL}(2,p) \text{ for almost all prime } p\big\}.$$

Lemma 2.4 *Suppose $k \geq 2$. Then X is dense in G^k.*

Proof. Let V be the six dimensional irreducible rational module for G. As we have seen above, every proper closed subgroup acts reducibly on V. Let L be an integral sublattice of V. Let $\rho : G \to \mathrm{GL}(V)$ be the corresponding representation.

Note that $\langle g_1,\ldots,g_k\rangle$ acts irreducibly on V if and only if $\mathrm{End}(V)$ is generated by the $\rho(g_i)$. This condition is equivalent to the condition that some collection of determinants of $d^2 \times d^2$ matrices do not identically vanish. Note that G can be generated (topologically) by 2 elements (eg., a pair of unipotent elements). Thus the set Y of k-tuples which generate irreducible subgroups on V form an open non-empty subvariety of G^k (in the Zariski topology). By the choice of V, Y is precisely the collection of k-tuples which generate a dense subgroup of G.

If $(g_1,\ldots,g_k) \in Y \cap \Gamma^k$, let A be the subring of $\mathrm{End}(L)$ generated by the $\rho(g_i)$ and H the subgroup generated by the $\rho(g_i)$. Since A generates $\mathrm{End}(V)$ as an algebra, A has finite index in $\mathrm{End}(L)$. In particular, for almost all primes p, H acts irreducibly on L/pL. If $p > d$, L/pL is an irreducible $\mathrm{SL}(2,p)$-module (because the high weight for V is $(d-1)\lambda$). We have seen that no proper subgroup of $\mathrm{SL}(2,p)$ acts irreducibly on this module. Thus, H maps onto $\mathrm{SL}(2,p)$ for all but finitely many p.

The same argument shows that $(g_1,\ldots,g_k) \in X \subseteq Y$ (a fact which we don't need). Therefore, $X := Y \cap \Gamma^k$ is the intersection of a nontrivial open subset and a dense subset of an irreducible variety. Thus, X is dense in G^k. □

Since χ_w is not constant on G^k, it cannot be constant on the dense subset X, whence:

Corollary 2.5 *If w is a nontrivial word in $r \geq 2$ variables, then χ_w takes on infinitely many values on X.*

Recall that the full automorphism group of $\mathrm{PSL}(2,p)$ is $\mathrm{PGL}(2,p)$ [C]. We have:

Corollary 2.6 *Let w be a nontrivial word in $k \geq 2$ variables. For any sufficiently large prime p (depending upon w), there exist $g_1,\dots,g_k$ and $h_1,\dots,h_k \in \mathrm{PSL}(2,p)$ such that $\mathrm{PSL}(2,p) = \langle g_1,\dots,g_k\rangle = \langle h_1,\dots,h_k\rangle$ and $w^{\pm 1}(g_1,\dots,g_k)$, $w^{\pm 1}(h_1,\dots,h_k) \in \mathrm{PSL}(2,p)$ are not conjugate under $\mathrm{PGL}(2,p)$.*

Proof. By the previous result, we may choose $g_1,\dots,g_k$ and $h_1,\dots,h_k \in (Y\cap\Gamma)$ such that $\mathrm{tr}(w(g_1,\dots,g_k)) \neq \pm\mathrm{tr}(w(h_1,\dots,h_k))$ and $\mathrm{PSL}(2,p) = \langle g_1,\dots,g_k\rangle = \langle h_1,\dots,h_k\rangle$ for all sufficiently large p. From here, it follows that $\mathrm{tr}(w(g_1,\dots,g_k)) \neq \mathrm{tr}(w(h_1,\dots,h_k))$ modulo p for sufficiently large p, whence the elements $w(g_1,\dots,g_k)$ and $w(h_1,\dots,h_k)$ are not conjugate under the automorphism group $\mathrm{PGL}(2,p)$. The restriction that $w^{-1}(g_1,\dots,g_k)$ and $w(h_1,\dots,h_k)$ are not conjugate under $\mathrm{PGL}(2,p)$ follows similarly. $\square$

Corollary 2.7 *Let n be any positive integer. For any sufficiently large prime p, there exist $g_1,\dots,g_n$ and $h_1,\dots,h_n \in \mathrm{PSL}(2,p)$ such that $\mathrm{PSL}(2,p) = \langle g_1,h_1\rangle = \cdots = \langle g_n,h_n\rangle$, and the commutators $[g_i,h_i]$ are not conjugate under $\mathrm{PGL}(2,p)$.*

Proof. Follows verbatim the proof of of the previous corollary. In this case we need n pairs of generators, and the word $w = [x_1,x_2] \in F_2$. From Corollary 2.3, for every fixed n and sufficiently large p we can find $\langle g_1,h_1\rangle = \ldots = \langle g_n,h_n\rangle = \mathrm{PSL}(2,p)$, with the commutators $[g_i,h_i]$, as desired. $\square$

Remark 2.8 Different versions of Lemma 2.4 are known in much greater generality. We refer to [PR] for references and details.

3 Proof of Theorems

Proof of Theorem 1.1.

Let w be a nontrivial word in F_k, $k \geq 3$, which is invariant on all T-systems of $G_p = \mathrm{PSL}(2,p)$. Recall the result of Gilman [G], that $\tau_k(\mathrm{PSL}(2,p)) = 1$ for all $k \geq 3$ and $p \geq 5$. Thus, all pairs of values $\{\varphi_w^{\pm 1}\}$ on $\mathcal{N}_k(G_p)$ are conjugate in $\mathrm{PGL}(2,p)$. This contradicts Corollary 2.6, when p is sufficiently large. $\square$

Proof of Theorem 1.2.

Fix any integer n. By Higman's Lemma [N] (see the introduction), the union of commutators $[g_1,g_2]$ and $[g_2,g_1]$ is invariant on T-systems. By Corollary 2.7, for sufficiently large primes p, the commutator $[g_1,g_2]$ takes on values in at least n different classes conjugates in $\mathrm{PSL}(2,p)$. Therefore, the number of T-systems $\tau_2(\mathrm{PSL}(2,p))$ is unbounded, as $p \to \infty$. $\square$

References

[C] R. Carter, *Simple groups of Lie type*, Reprint of the 1972 originalm Wiley Classics Library, A Wiley-Interscience Publicationm John Wiley & Sons, Inc., New York, 1989

[CP] G. Cooperman, I. Pak, The product replacement graph on generating triples of permutations, preprint, 2000

[D1] M. J. Dunwoody, On T-systems of groups, *J. Austral. Math. Soc.* **3** (1963), 172–179

[D2] M. J. Dunwoody, Nielsen Transformations, in: *Computational Problems in Abstract Algebra*, 45–46, Pergamon, Oxford, 1970

[E1] M. Evans, Ph. D. Thesis, University of Wales, 1985

[E2] M. Evans, T-systems of certain finite simple groups, *Math. Proc. Cambridge Philos. Soc.* **113** (1993), 9–22

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

[H] F. Hausdorff, *Grundzüge der Mengenlehre*, Leipzig, 1914

[LS] M. W. Liebeck, A. Shalev, Diameters of finite simple groups: sharp bounds and applications, preprint, 1999

[N] B. H. Neumann, On a question of Gaschütz, *Archiv der Math.* **7** (1956), 87–90

[NN] B. H. Neumann, H. Neumann, Zwei Klassen charakteristischer Untergruppen und ihre Faktorgruppen, *Math. Nachr.* **4** (1951), 106–125

[P] I. Pak, What do we know about the product replacement algorithm? in: *Groups ann Computation* III (W. Kantor, A. Seress, eds.), 301–347, deGruyter, Berlin, 2000

[PR] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Boston, MA, 1994