Product decompositions in finite simple groups

Martin W. Liebeck
Department of Mathematics
Imperial College
London SW7 2BZ, UK

Nikolay Nikolov
Department of Mathematics
Imperial College
London SW7 2BZ, UK

Aner Shalev
Institute of Mathematics
Hebrew University
Jerusalem 91904, Israel

July 11, 2011

Abstract

We propose a general conjecture on decompositions of finite simple groups as products of conjugates of an arbitrary subset. We prove this conjecture for bounded subsets of arbitrary finite simple groups, and for large subsets of groups of Lie type of bounded rank. Some of our arguments apply recent advances in the theory of growth in finite simple groups of Lie type, and provide a variety of new product decompositions of these groups.

In this paper we propose the following conjecture:

Conjecture *There exists an absolute constant c such that if G is a finite simple group and A is any subset of G of size at least two, then G is a product of N conjugates of A for some $N \leq c \log |G| / \log |A|$.*

Note that we must have $N \geq \log |G| / \log |A|$ by order considerations, and so the bound above is tight up to a multiplicative constant.

The above conjecture is a stronger version of a recent conjecture we posed in [6], where A was assumed to be a subgroup of G. Positive evidence for the latter conjecture is provided by [7] (when A is a Sylow subgroup) and [5, 9, 10] (when A is of type SL_n), with applications to bounded generation and expanders. Further results were proved in [6] in various cases where A is a maximal subgroup of G, but the general case is still open.

The authors are grateful for the support of an EPSRC grant. The third author is also grateful for the support of an ERC Advanced Grant 247034.

2010 *Mathematics Subject Classification:* 20D40, 20D06

In this paper we provide positive evidence for the stronger conjecture stated above, regarding subsets. One important case where the conjecture is known to be true (and widely applied) is when the subset A is a conjugacy class, or more generally, a normal subset of G; indeed, this is the main result of [8]. Note also that if G is a group of Lie type of bounded rank, and A is a bounded subset of G, then the conjecture holds, as shown in [6, 2.3].

The following easy reductions will sometimes be useful. We first claim that, in proving the conjecture for a subset A, we may assume that $1 \in A$. Indeed, let $a \in A$ and $B = a^{-1}A$. Then $1 \in B$, and if G is a product of N conjugates of B then it is also a product of N conjugates of A.

Secondly, we claim we may assume there exists $x \neq 1$ such that $1, x, x^{-1} \in A$. Indeed, suppose $1 \in A$ and let $x \in A$ be a non-identity element (whose existence follows from the assumption $|A| \geq 2$). Then $1, x, x^2 \in A^2$, hence $x^{-1}, 1, x \in x^{-1}A^2$. Assuming the conjecture holds for sets containing $x^{-1}, 1, x$ we deduce that G is a product of say $N \leq c \log |G| / \log |A^2| \leq c \log |G| / \log |A|$ conjugates of $x^{-1}A^2$, hence it is a product of N conjugates of A^2, so G is a product of $2N \leq 2c \log |G| / \log |A|$ conjugates of A.

Our first result here concerns arbitrary subsets of groups of Lie type of bounded rank, but provides a slightly weaker bound.

Theorem 1 *Let G be a finite simple group of Lie type of rank r, and let A be any subset of G of size at least 2. Then there is a constant $c = c(r)$ depending only on r, and a positive integer $N \leq \max(3, (\frac{\log |G|}{\log |A|})^c)$, such that G is a product of N conjugates of A.*

Proof. The proof is short but relies on strong tools, most importantly the recent results on growth of Cayley graphs in [1, 3, 12]. Let G and A be as in the hypothesis.

By [4, 5.3.9] there exists $\delta > 0$ depending only on r such that every non-trivial representation of G has dimension at least $|G|^{\delta}$. Hence [11, Corollary 1] shows that if $|A| > |G|^{1-\delta/3}$, then $A^3 = G$. Consequently we may assume that $|A| \leq |G|^{1-\delta/3}$.

Assume (as we may) that $1, x \in A$, where $x \neq 1$.

By [2, Theorem 2], there are $l = 8(2r+1)$ conjugates $x^{g_1}, \ldots, x^{g_l}$ of x which generate G, and hence $G = \langle A^{g_1}, \ldots, A^{g_l} \rangle$. Define $X = A^{g_1} \cdots A^{g_l}$. Then X contains A^{g_i} for all i, and so X generates G. By [12, Theorem 4] or in an equivalent formulation [1, Theorem 2.3], for any generating set Y of G, either $Y^3 = G$ or $|Y^3| > |Y|^{1+\epsilon}$, where $\epsilon > 0$ depends only on r. (Note that the statements there only say that $|Y^3| > \gamma |Y|^{1+\epsilon}$ for a positive constant γ, but as justified at the beginning of [3, Section 6], we can assume $\gamma = 1$ by taking a smaller value of ϵ.) Applying this repeatedly to $X, X^3, X^9, \ldots$, we obtain

$$|X^{3^n}| \geq \min(|G|, |X|^{(1+\epsilon)^n}) \geq \min(|G|, |A|^{(1+\epsilon)^n}).$$

Now choose n minimal such that $(1+\epsilon)^n \geq \frac{\log|G|}{\log|A|}$ and let $k = 3^n$. Then $X^k = G$, and $k \leq (\frac{\log|G|}{\log|A|})^b$ where $b = 1 + (\log 3/\log(1+\epsilon))$, hence depends only on r. As X is a product of l conjugates of A, we see that G is a product of kl conjugates of A. Set $N = kl$. Then $N \leq 8(2r+1)(\frac{\log|G|}{\log|A|})^b$. Since $|A| \leq |G|^{1-\delta/3}$, it follows that $N \leq (\frac{\log|G|}{\log|A|})^c$ for some $c > b$ depending only on r. This completes the proof. ■

Notice that Theorem 1 implies that if A is a subset of G of size at least $|G|^\alpha$ for some fixed $\alpha > 0$, and r is bounded, then G is a product of boundedly many conjugates of A, so our conjecture holds in this case (cf. [6, Theorem 2], which includes an analogous result for maximal subgroups).

In particular, this leads to a host of new product decompositions, as follows.

Corollary 2 *Let $\bar{G}$ be a simple adjoint algebraic group of rank r over the algebraic closure of $\mathbb{F}_p$, where p is a prime, and let σ be a Frobenius morphism of $\bar{G}$ such that $G(q) = (\bar{G}_\sigma)'$ is a finite simple group of Lie type over $\mathbb{F}_q$. Suppose $\bar{H}$ is a σ-stable subgroup of $\bar{G}$ of positive dimension such that $H(q) = \bar{H}_\sigma \cap G(q)$ is nontrivial. Then $G(q)$ is equal to a product of $f(r)$ conjugates of $H(q)$, for a suitable function f.*

Proof. It is well known that $|H(q)|$ is at least γq (or $\gamma q^{1/2}$ for Suzuki and Ree groups), where $\gamma = \gamma(r) > 0$. As $|H(q)| > 1$ by hypothesis, it follows that $|H(q)| > q^\delta$ with $\delta = \delta(r) > 0$. Since $|G(q)| < q^{8r^2}$, the conclusion follows from Theorem 1. ■

Various particular cases of this are of special interest. For example, it follows that a simple group $G(q)$ of rank r (not a Suzuki group) is a product of $f(r)$ conjugate subgroups isomorphic to $SL_2(q)$ or $PSL_2(q)$. This was proved in [5, 9] without the conjugacy part of the conclusion, and was one of the last steps in showing that all families of finite simple groups can be made into expanders with respect to bounded generating sets.

Moreover, various new product decompositions now follow in a similar manner. For example, $G(q)$ is a product of $f(r)$ conjugates of any nontrivial torus T, or of any centralizer $C_{G(q)}(g)$, and so on.

In the second part of this paper we prove our conjecture for finite simple groups in general, provided the subset A has bounded size. This follows from the theorem below.

Theorem 3 *There exists an absolute constant c such that if G is a finite simple group, and A is any subset of G of size at least 2, then G is a product of N conjugates of A for some $N \leq c\log|G|$.*

Proof. Since the case when G is of Lie type and bounded rank follows from [6], it suffices to prove the theorem for alternating groups and classical groups of unbounded rank.

We assume (as we may) that $1, x, x^{-1} \in A$ for some $x \neq 1$.

We start with the alternating case $G = A_n$. It is easy to choose a 3-cycle $y \in A_n$ such that $[x, y] \neq 1$ has support of size at most 5. Let $C = x^{A_n}$, the conjugacy class of x. Since $[x, y] = x^{-1}x^y \in C^{-1}C$, we see that $C^{-1}C$ contains either a 3-cycle, a 5-cycle or a double transposition. In all cases we deduce that $(C^{-1}C)^2$ contains all double transpositions in A_n.

Since $x, x^{-1} \in A$, some product of 4 conjugates of A contains $\{1, t\}$ for a double transposition $t \in A_n$. Denote by τ a fixed transposition of S_n, say $(1, 2)$. We now use our result that S_{n-2} (and therefore A_{n-2}) is contained in a product $S_2^{g_1} \cdots S_2^{g_k}$ of $k \leq 320n \log n$ conjugates of $S_2 = \{1, \tau\}$, by Lemma 3.7 with $m = 2$ in [6].

By adding the transposition $(n-1, n)$ to the transpositions τ^{g_i} we obtain a conjugate of t for any copy of $S_2^{g_i}$ and in this way we see that A_{n-2} is a product of at most $320n \log n$ conjugates of the set $\{1, t\}$. (We only get even powers of the transposition $(n-1, n)$ on the last two points since the elements of A_{n-2} always end up as products of **even** number of conjugates of τ).

Finally A_n is a product of 3 conjugates of A_{n-1} (since a product of 2 distinct conjugates of A_{n-1} can move 1 to any point in in $1, \ldots, n$). Therefore A_n is a product of 9 conjugates of A_{n-2}. Thus, setting $c = 9 \times 320 \times 4 = 11520$, we obtain A_n as a product of at most $cn \log n$ conjugates of A. This concludes the proof for alternating groups.

Now let $G = PCl_n(q)$, a projective classical group of (unbounded) dimension n over $\mathbb{F}_q$. Let x be as above. By the proof of [2, 2.2], there are elements $y_1, \ldots y_k \in G$ with $k \leq 3$ such that the element $u = [x, y_1, \ldots, y_k]$ is a non-identity long root element of G. Now u is equal to a product of $2^k \leq 8$ conjugates of $x^{\pm 1}$, hence lies in a product of at most 8 conjugates of A.

Replacing u by a conjugate, we may write $u = u_\alpha(1)$ for a long root α. Consider the subgroup $H = \langle u_{\pm\alpha}(t) : t \in \mathbb{F}_q \rangle \cong SL_2(q)$ of G. As in [6, 2.3], we see that H is equal to a product of at most $c_1 \log q$ conjugates of the set $\{1, u\}$, hence it is contained in a product of at most $c_2 \log q$ conjugates of A.

By [10], there is a Levi subgroup X of G of type SL_m such that G is a product of boundedly many conjugates of X; and by [5, 1.1], X is a product of at most $c_3 n^2$ conjugates of H. Hence G is equal to a product of $c_4 n^2$ conjugates of H. We conclude from the above that G is equal to a product of at most $c_5 n^2 \log q$ conjugates of A, completing the proof of the theorem. ∎

References

[1] E. Breuillard, B. Green and T. Tao, Approximate subgroups of linear groups, preprint, arXiv1005.1881v1.

[2] J.I. Hall, M.W. Liebeck and G.M. Seitz, Generators for finite simple groups, with applications to linear groups, *Quart. J. Math. Oxford* **43** (1992), 441–458.

[3] H.A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math.* **167** (2008), 601–623.

[4] P. Kleidman and M.W. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Series **129**, Cambridge Univ. Press, 1990.

[5] M.W. Liebeck, N. Nikolov and A. Shalev, Groups of Lie type as products of SL_2 subgroups, *J. Algebra* **326** (2011), 201–207.

[6] M.W. Liebeck, N. Nikolov and A. Shalev, A conjecture on product decompositions in simple groups, *Groups Geom. Dyn.* **4** (2010), 799–812.

[7] M.W. Liebeck and L. Pyber, Finite linear groups and bounded generation, *Duke Math. J.* **107** (2001), 159–171.

[8] M.W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Ann. of Math.* **154** (2001), 383–406.

[9] A. Lubotzky, Finite simple groups of Lie type as expanders, *J. Eur. Math. Soc.*, to appear.

[10] N. Nikolov, A product decomposition for the classical quasisimple groups, *J. Group Theory* **10** (2007), 43–53.

[11] N. Nikolov, L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem, *J. Eur. Math. Soc.* **13** (2011), 1063–1077.

[12] L. Pyber and E. Szabo, Growth in finite simple groups of Lie type of bounded rank, preprint, arXiv:1005.1858v2.