

Open Research Online

The Open University's repository of research publications and other research outputs

On the product decomposition conjecture for finite simple groups

Journal Item

How to cite:

Gill, Nick; Pyber, László; Short, Ian and Szabó, Endre (2013). On the product decomposition conjecture for finite simple groups. *Groups, Geometry, and Dynamics*, 7(4) pp. 867–882.

For guidance on citations see [FAQs](#).

© 2013 European Mathematical Society Publishing House

Version: Accepted Manuscript

Link(s) to article on publisher's website:
<http://dx.doi.org/doi:10.4171/GGD/208>

Copyright and Moral Rights for the articles on this site are retained by the individual authors and/or other copyright owners. For more information on Open Research Online's data [policy](#) on reuse of materials please consult the policies page.

oro.open.ac.uk

ON THE PRODUCT DECOMPOSITION CONJECTURE FOR FINITE SIMPLE GROUPS

N. GILL, L. PYBER, I. SHORT, E. SZABÓ

ABSTRACT. We prove that if G is a finite simple group of Lie type and S a subset of G of size at least two then G is a product of at most $c \log |G| / \log |S|$ conjugates of S , where c depends only on the Lie rank of G . This confirms a conjecture of Liebeck, Nikolov and Shalev in the case of families of simple groups of bounded rank. We also obtain various related results about products of conjugates of a set within a group.

1. INTRODUCTION

Our starting point is the following conjecture of Liebeck, Nikolov and Shalev [11].

Conjecture 1.1. *There exists an absolute constant c such that if G is a finite simple group and S is a subset of G of size at least two, then G is a product of N conjugates of S for some $N \leq c \log |G| / \log |S|$.*

Note that we must have $N \geq \log |G| / \log |S|$ by order considerations, and so the bound above is best possible up to the value of the constant c .

The conjecture is an extension of a deep (and widely applied) theorem of Liebeck and Shalev. Indeed, the main result of [16] states that the above conjecture holds when S is a conjugacy class or, more generally, a normal subset (that is, a union of conjugacy classes) of G . In [11] Conjecture 1.1 is also proved for sets of bounded size.

Somewhat earlier Liebeck, Nikolov and Shalev [12] posed the following (still unproved) weaker conjecture.

Conjecture 1.2. *There exists an absolute constant c such that if G is a finite simple group and H is any nontrivial subgroup of G , then G is a product of N conjugates of H for some $N \leq c \log |G| / \log |H|$.*

Conjecture 1.2 itself represents a dramatic generalization of a host of earlier work on product decompositions of finite simple groups, most of which prove Conjecture 1.2 for particular subgroups H . For instance, in [15] it is proved that a finite simple group of

2010 *Mathematics Subject Classification.* 20D06, 20D40, 20G40.

Key words and phrases. Conjugacy, Doubling lemma, Product theorem, simple group, width.

L.P. is supported in part by OTKA NK78439 and K84233.

E.Sz. is supported in part by OTKA NK81203 and K84233.

N.G. would like to thank Harald Helfgott for allowing the use of his research funds to facilitate a visit to the Rényi Institute during which work on this paper was initiated. He would also like to thank the University of Bristol to which he has been a regular visitor over the course of writing this paper.

N.G. is the corresponding author.

Lie type in characteristic p is a product of 25 Sylow p -subgroups (see also [1] for a recent improvement from 25 to 5).

Further positive evidence for Conjecture 1.2 is provided by [13], [17] and [18] (when H is of type SL_n). Certain results of this type are essential to prove that finite simple groups can be made into expanders (see the announcement [8]).

The main purpose of this note is to prove Conjecture 1.1 for finite simple groups of Lie type of bounded rank. Put another way, we prove a version of Conjecture 1.1 in which the constant c depends on the rank of the group G . Our main result follows.

Theorem 1.3. *Fix a positive integer r . There exists a constant $c = c(r)$ such that if G is a finite simple group of Lie type of rank r and S is a subset of G of size at least two then G is a product of N conjugates of S for some $N \leq c \log |G| / \log |S|$.*

In [11] a weaker bound of the form $N \leq (\log |G| / \log |S|)^{c(r)}$ is obtained. Also, in [12], Theorem 1.3 is proved when S is a maximal subgroup of G .

As a byproduct of our proof we obtain two results of independent interest. In these results, and throughout the paper, we denote by S^g the conjugate $g^{-1}Sg$ of a subset S of a group G by an element g of G , and, given a positive integer m , we denote by S^m the product $SS \cdots S$ of m copies of S . There should be no confusion between these two similar notations because the type of the exponent will always be given.

Theorem 1.4. *Fix a positive integer r . There exists a positive constant $\varepsilon = \varepsilon(r)$ such that if G is a finite simple group of Lie type of rank r and S is a subset of G then for some g in G we have $|SS^g| \geq |S|^{1+\varepsilon}$ or $S^3 = G$.*

The next theorem is similar, but concerns only normal subsets, in which case we obtain absolute constants.

Theorem 1.5. *There exists $\varepsilon > 0$ and a positive integer b such that if G is a finite simple group and S is a normal subset of G then $|S^2| \geq |S|^{1+\varepsilon}$ or $S^b = G$.*

Theorem 1.5 relates to a result of Shalev [27, Theorem 7.4], which we strengthen in Section 5.

Note that the theorem would not be true were we to consider sets that are not normal. For instance, take S to be a maximal parabolic subgroup in $G = PSL_n(q)$ with index $\frac{q^n-1}{q-1}$. Clearly $S^b = S$ for all positive integers b ; on the other hand, for any positive number ε , and any g in G , we have $|SS^g| \leq |G| \leq |S|^{1+\varepsilon}$ once n is large enough. We conclude that neither of the given options can hold in this more general situation.

Theorems 1.4 and 1.5, and the remarks of the previous paragraph, lead us to make the following conjecture.

Conjecture 1.6. *There exists $\varepsilon > 0$ and a positive integer b such that if S is a subset of a finite simple group G then for some g in G we have $|SS^g| \geq |S|^{1+\varepsilon}$ or G is the product of b conjugates of S .*

Note that, by Theorems 1.3 and 1.4, Conjectures 1.1, 1.2 and 1.6 hold for all exceptional simple groups. Note too that all three conjectures could be phrased in terms of *translates* of the set S , rather than conjugates. This follows from the simple fact that a product of translates of S is equal to a translate of a product of conjugates of S . Similarly a product

of conjugates of a translate of S is equal to a translate of a product of conjugates of S , a fact which will be useful in its own right.

It is possible that Conjecture 1.6 actually holds with $b = 3$. When $b = 2$ counterexamples are given by large non-real conjugacy classes (see the final section of [27] for some related issues). Further counterexamples are given by certain families of maximal subgroups (see for example [14, Corollary 2], which states that large enough simple unitary groups of odd dimension cannot be decomposed into the product of two proper subgroups).

We derive Theorems 1.3 and 1.4 as consequences of the recent Product theorem for finite simple groups, proved independently by Breuillard, Green and Tao [3], and Pyber and Szabó [23] (see Section 2). Theorem 1.5 follows from a version of Conjecture 1.1 for normal subsets due to Liebeck and Shalev [16] and an extension of Plünnecke's theorem [30, Theorem 6.27] to normal subsets of nonabelian groups (see Section 4).

In the final section we use a result of Petridis [20] to derive an analogue of the classical Doubling lemma, a special case of Plünnecke's theorem. We refer to the new result as the Skew doubling lemma; it can be thought of as a nonabelian version of the classical Doubling lemma. The Skew doubling lemma is applied to prove that Conjecture 1.1 implies Conjecture 1.6. In the other direction, a standard argument (similar to the proof of Corollary 2.8) shows that Conjecture 1.6 implies that a simple group G is a product of $(\log |G| / \log |S|)^c$ conjugates of S , a weaker version of Conjecture 1.1.

2. PROOF OF THEOREM 1.4

We begin with a result of Petridis [20, Theorem 4.4], which extends work of Helfgott, Ruzsa and Tao [7, 25, 26, 29]. It relates to the Doubling lemma for abelian groups, which we return to in Section 4.

Lemma 2.1. *Let S be a finite subset of a group G . Suppose that there exist positive numbers J and K such that $|S^2| \leq J|S|$ and $|SgS| \leq K|S|$ for each g in S . Then $|S^3| \leq J^7 K|S|$.*

Suppose now that G is a finite group. Let $\text{minclass}(G)$ denote the size of the smallest nontrivial conjugacy class in G . Given a subset S of G that is neither empty nor the trivial group, we denote by $\text{minclass}(S, G)$ the size of the smallest nontrivial conjugacy class in G that intersects S . Finally, let $\text{mindeg}(G)$ denote the dimension of the smallest nontrivial complex irreducible representation of G .

As observed in [19], a result of Gowers [4] implies the following.

Proposition 2.2. *Let G be a finite group and let $k = \text{mindeg}(G)$. Take $S \subseteq G$ such that $|S| \geq \frac{|G|}{\sqrt[3]{k}}$. Then $G = S^3$.*

Now let $G = G_r(q)$ be a simple group of Lie type of rank r over \mathbb{F}_q , the finite field of order q . We need some facts about G . The first result can be deduced, for example, from [9, Tables 5.1 and Theorem 5.2.2].

Proposition 2.3. *We have $q^r \leq \text{minclass}(G) < |G| \leq q^{8r^2}$.*

Proposition 2.4. *Let $k = \text{mindeg}(G)$. Then $|G| < k^{8r^2}$.*

Proof. We use the lower bounds on projective representations given by Landazuri and Seitz [10], allowing for the slight errors corrected in [9, Table 5.3.A]. For $G \neq PSL_2(q)$, we see that $k \geq q$, and so the result follows from Proposition 2.3.

Now suppose that $G = PSL_2(q)$; then $|G| < q^3$ and $r = 1$. For $q \geq 5$ and $q \neq 9$, $k = \frac{1}{(2,q-1)}(q-1)$ and it is clear that $k^8 > q^3$. When $q = 4$ we have $k = 2$ and the result follows; likewise when $q = 9$ we have $k = 3$ and the result follows. \square

The next result was obtained independently in [5] and [28].

Proposition 2.5. *Each finite simple group G is $\frac{3}{2}$ -generated; that is, for any nontrivial element g of G there exists h in G such that $\langle g, h \rangle = G$.*

Corollary 2.6. *Let G be a finite simple group and let S be a subset of G of size at least two. Then some translate of S generates G .*

Proof. Let u and v be distinct elements of S . Since G is $\frac{3}{2}$ -generated, there exists x in G such that $\langle vu^{-1}, x \rangle = G$. Therefore the translate $Su^{-1}x$, which contains x and $vu^{-1}x$, generates G . \square

The next result, the Product theorem, is our primary tool for proving Theorems 1.3 and 1.4. Versions of this result can be found in [3, 23]. It was first proved by Helfgott for the groups $PSL_2(p)$ and $PSL_3(p)$ in [6, 7].

Theorem 2.7. *Fix a positive integer r . There exists a positive constant $\eta = \eta(r)$ such that, for G a finite simple group of Lie type of rank r and S a generating set of G , either $S^3 = G$ or $|S^3| \geq |S|^{1+\eta}$.*

We can now prove Theorem 1.4.

Proof of Theorem 1.4. Given a positive integer r , let η be the constant from Theorem 2.7. Let $L = 8^{\frac{2}{\eta}}$.

Suppose first that $|S| \leq L$. The result holds trivially if $S = G$ or $|S| \leq 1$, so let us assume that $S \neq G$ and $|S| > 1$. We will show that there is an element g such that $|SS^g| \geq |S| + 1$. By replacing S with a translate, we may assume that S contains the identity. Therefore $S^2 \supseteq S$. If the inequality $|S^2| \geq |S| + 1$ does not hold then instead $|S^2| = |S|$, so $S^2 = S$, and hence S is a group. It is not a normal subgroup (because G is simple) so there are elements x and g in G with $x \in S^g$ but $x \notin S$. Then $SS^g \supseteq S \cup \{x\}$, so $|SS^g| \geq |S| + 1$, as required. Let $\varepsilon_1 = \log(L+1)/\log L - 1$. One can check that $|S| + 1 \geq |S|^{1+\varepsilon_1}$, and hence there is an element g of G such that $|SS^g| \geq |S|^{1+\varepsilon_1}$.

Suppose now that $|S| > L$. Since G is $\frac{3}{2}$ -generated, there exists an element g of G such that the set $T = S \cup \{g\}$ generates G . We can apply Theorem 2.7 to T to conclude that either $|T^3| \geq |S|^{1+\eta}$ or $T^3 = G$. We consider each possibility in turn.

Suppose that $|T^3| \geq |S|^{1+\eta}$. Observe that T^3 is the union of the eight sets SSS , SSg , SgS , gSS , Sgg , gSg , ggS and $\{ggg\}$. Therefore at least one of the eight sets is larger than $\frac{1}{8}|S|^{1+\eta}$. We assumed earlier that $|S| \geq 8^{\frac{2}{\eta}}$, from which it follows that $\frac{1}{8}|S|^{1+\eta} > |S|^{1+\frac{\eta}{2}}$. Therefore one of the first seven of the eight sets is larger than $|S|^{1+\frac{\eta}{2}}$. All of these seven sets except SSS are equal to a translate of the product of one or two conjugates of S , so if any of these have size at least $|S|^{1+\frac{\eta}{2}}$ then $|SS^h| \geq |S|^{1+\frac{\eta}{2}}$ for some element h of G . If,

on the other hand, $|SSS| \geq |S|^{1+\frac{\eta}{2}}$, then Lemma 2.1 (with $J = K = |S|^{\frac{\eta}{16}}$) implies that there is an element h of $S \cup \{1\}$ with $|SS^h| \geq |S|^{1+\frac{\eta}{16}}$. Therefore in both cases there is an element h with $|SS^h| \geq |S|^{1+\varepsilon_2}$, where $\varepsilon_2 = \frac{\eta}{16}$.

The remaining possibility is that $T^3 = G$. If $S^3 \neq G$ then Proposition 2.2 implies that $|S| \leq |G|/\sqrt[3]{k}$ where $k = \text{mindeg}(G)$. But Proposition 2.4 gives that $|S| \leq |G|^{1-\frac{1}{24r^2}}$, and this implies, in particular, that $|T^3| = |G| \geq |S|^{1+\frac{1}{24r^2}}$. The argument of the previous paragraph applies again, to give a positive constant ε_3 that depends only on r such that $|SS^h| \geq |S|^{1+\varepsilon_3}$ for some element h .

Let ε be the minimum of ε_1 , ε_2 and ε_3 ; this depends only on r . We have shown that if $S^3 \neq G$ then there is an element g of G with $|SS^g| \geq |S|^{1+\varepsilon}$. This completes the proof. \square

Note that we can immediately deduce the following result of [11] (which we will use later).

Corollary 2.8. *Fix a positive integer r . There exists a constant d such that if G is a finite simple group of Lie type of rank r and S is a subset of G of size at least two then G is a product of N conjugates of S for some $N \leq 3(\log |G|/\log |S|)^d$.*

Proof. Let ε be the constant from Theorem 1.4, and define $d = \log_{1+\varepsilon} 2$. Let M be the integer part of $\log_{1+\varepsilon} \frac{\log |G|}{\log |S|}$. Theorem 1.4 implies that G is the product of $3 \cdot 2^M$ conjugates of S , and

$$3 \cdot 2^M \leq 3 \left(\frac{\log |G|}{\log |S|} \right)^d.$$

\square

The results in this section motivate a common generalisation of the Product theorem (that is, Theorem 2.7) and Conjecture 1.6 for groups of Lie type.

Conjecture 2.9. *There exists $\varepsilon > 0$ and a positive integer b such that the following statement holds. For each integer r there is a positive integer $c(r)$ such that if G is a finite simple group of Lie type of rank r and S a generating set of G , then either $|SS^g| \geq |S|^{1+\varepsilon}$ for some $g \in S^{c(r)}$, or else G is the product of b conjugates S^{g_1}, \dots, S^{g_b} , where $g_1, \dots, g_b \in S^{c(r)}$.*

It would be interesting to prove Conjecture 1.6 in the case when S is a subgroup of G . A rather general qualitative result in this direction was obtained by Bergman and Lenstra [2]. They show that if H is a subgroup of a group G satisfying $|HH^g| \leq K|H|$ for all g in G , then H is ‘‘close to’’ some normal subgroup N of G , in the sense that $|H : H \cap N|$ and $|N : H \cap N|$ are both bounded in terms of K .

3. PROOF OF THEOREM 1.3

Given an element g of a group G we define

$$g^G = \{g^h : h \in G\},$$

and, for a subset Z of G ,

$$Z^G = \{Z^h : h \in G\}.$$

We begin the proof of Theorem 1.3 with a simple combinatorial lemma, which enables us to deal with “small” sets.

Lemma 3.1. *Let S be a subset of size at least two in a finite group G . There exist a positive integer m and m conjugates of S such that their product X satisfies*

$$|X| = |S|^m \geq \frac{\sqrt{\text{minclass}(SS^{-1}, G)}}{|S|} \geq \frac{\sqrt{\text{minclass}(G)}}{|S|}.$$

Proof. Define $X_1 = S$ and, if possible, choose an element g of G such that $X_1^{-1}X_1 \cap gSS^{-1}g^{-1} = \{1\}$. Define $X_2 = X_1gSg^{-1}$. Notice that if $x_L, x_R \in X_1, s_L, s_R \in S$, and $x_Lgs_Lg^{-1} = x_Rgs_Rg^{-1}$, then $x_R^{-1}x_L = gs_Rs_L^{-1}g^{-1}$. Hence $x_R^{-1}x_L \in X_1^{-1}X_1 \cap gSS^{-1}g^{-1}$, and so $x_L = x_R$ and $s_L = s_R$. It follows that $|X_2| = |X_1||S|$. Now repeat this process with X_2 replacing X_1 , and so on.

The process terminates with a set X of size $|S|^m$, which is a product of m conjugates of S , and such that $|X^{-1}X \cap gSS^{-1}g^{-1}| \geq 2$ for all g in G .

Let T be a set of smallest possible size that intersects every conjugate of $Z = SS^{-1}$ nontrivially, and write $t = |T|$. Let $n = |G : N_G(Z)|$, the number of G -conjugates of Z . By the pigeonhole principle there exists an element g of Z that lies in at least $\frac{n}{t}$ different conjugates of Z . Let us count the set

$$\Omega = \{(g', Z') \in g^G \times Z^G \mid g' \in Z'\}$$

in two different ways.

First, since every conjugate of g lies in the same number of conjugates of Z , we know that $|g^G| \frac{n}{t} \leq |\Omega|$. On the other hand it is clear that $|\Omega| \leq n|Z|$. Putting these together we obtain that $|g^G| \frac{n}{t} \leq n|Z|$. Therefore

$$t \geq \frac{|g^G|}{|Z|} \geq \frac{\text{minclass}(SS^{-1}, G)}{|S|^2}$$

and using $|X|^2 \geq |X^{-1}X| \geq t$ our statement follows. \square

Remark 3.2. Lemma 3.1 and Proposition 2.3 imply that if G is a simple group of Lie type of rank r and S a subset of size less than $q^{r/4}$ then we have $|SS^g| = |S|^2$ for some g in G .

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. As observed above, a product of conjugates of a translate of S is equal to the translate of a product of conjugates of S . By Corollary 2.6, a translate of S generates G . Therefore we assume that S generates G .

Suppose that $|S| \geq |\text{minclass}(G)|^{1/4}$; then $|G| < |S|^{32r}$ by Proposition 2.3. Now Corollary 2.8 implies that G is a product of fewer than $3(32r)^d$ conjugates of S . The theorem holds in this case with $c = 3(32r)^d$.

Suppose instead that $|S| < |\text{minclass}(G)|^{1/4}$. By Lemma 3.1 we can choose conjugates S_1, \dots, S_m of S such that the set $X = S_1 \cdots S_m$ satisfies $|X| = |S|^m$ and

$$|X| \geq \frac{\sqrt{|\text{minclass}(G)|}}{|S|} \geq |\text{minclass}(G)|^{1/4}.$$

It follows from the first part of the proof that G is a product of fewer than $c \log |G| / \log |X|$ conjugates of X . Therefore G is a product of fewer than $mc \log |G| / \log |X|$ conjugates of S and, since $\log |X| = m \log |S|$, the result follows. \square

4. PLÜNNECKE-RUZSA ESTIMATES FOR NONABELIAN GROUPS

The following basic result in additive combinatorics is due to Plünnecke [21, 22] (see also [30, Section 6.5]).

Theorem 4.1. *Let A and B be finite sets in an abelian group G and suppose that $|AB| \leq K|A|$ where K is a positive number. Then for any positive integer m there exists a nonempty subset X of A such that*

$$|XB^m| \leq K^m|X|.$$

In particular, $|B^2| \leq K|B|$ implies that $|B^m| \leq K^m|B|$ for $m = 1, 2, \dots$

The last statement (“In particular...”) is called the Doubling lemma; it does not hold for nonabelian groups, however, as we saw in Lemma 2.1, there are useful analogues in this context due to Helfgott, Petridis, Ruzsa and Tao [7, 20, 25, 26, 29]. Petridis also proved the following lemma [20, Proposition 2.1].

Lemma 4.2. *Let X and B be finite sets in a group. Suppose that*

$$\frac{|XB|}{|X|} \leq \frac{|ZB|}{|Z|}$$

for all $Z \subseteq X$. Then, for all finite sets C ,

$$|CXB| \leq \frac{|CX||XB|}{|X|}.$$

Using this lemma we can extend Plünnecke’s theorem to normal subsets of nonabelian groups. The statement and proof mimic [20, Theorem 3.1], which is a stronger version of Theorem 4.1.

Theorem 4.3. *Let A and B be finite sets in a group G with B normal in G . Suppose that $|AB| \leq K|A|$ for some positive number K . Then there exists a nonempty subset X of A such that*

$$|XB^m| \leq K^m|X|$$

for $m = 1, 2, \dots$. In particular, $|B^2| \leq K|B|$ implies that $|B^m| \leq K^m|B|$ for $m = 1, 2, \dots$

Proof. We proceed by induction on m . First choose $X \subseteq A$ such that

$$\frac{|XB|}{|X|} \leq \frac{|ZB|}{|Z|}$$

for all $Z \subseteq A$. Then

$$|XB| \leq |X| \frac{|AB|}{|A|} \leq K|X|,$$

so the result is true for $m = 1$.

Now suppose that $|XB^m| \leq K^m|X|$ for some positive integer m . Normality of B implies that $|XB^{m+1}| = |B^mXB|$, and then Lemma 4.2 gives

$$|XB^{m+1}| = |B^mXB| \leq \frac{|B^mX||XB|}{|X|} \leq K^{m+1}|X|.$$

This verifies the inductive step, and completes the proof of the theorem. \square

Following an argument of Petridis (see the proof of [20, Theorem 1.2]) we observe that the Plünnecke-Ruzsa estimates [30, Corollary 6.29] can also be generalised using Theorem 4.3.

Corollary 4.4. *Suppose that A and B are subsets of a group G , with B normal in G , and $|AB| \leq K|A|$. Then*

$$|B^mB^{-n}| \leq K^{m+n}|A|$$

for all positive integers m and n .

Theorem 4.3 suggests that certain techniques in additive combinatorics concerning subsets of abelian groups can be applied to normal subsets of nonabelian groups. The next example – which is a consequence of Plünnecke’s theorem, and generalises [25, Corollary 2.4] – supports this suggestion.

Theorem 4.5. *Let A and B be subsets of a group G with B normal in G , and suppose that $|AB^j| \leq K|A|$ for some positive integer j . If $m \geq j$ then*

$$|B^m| \leq K^{\frac{m}{j}}|A|.$$

Sketch of proof. We use the notation of [30, Section 6.5]. Construct the m -tuple of directed bipartite graphs

$$(G_{A,B}, G_{AB,B}, \dots, G_{AB^{m-1},B}).$$

This m -tuple is a Plünnecke graph. Now Plünnecke’s theorem [30, Theorem 6.27] yields the result immediately. \square

5. PROOF OF THEOREM 1.5

In this section we prove Theorem 1.5 and generalise some related results of Shalev. We will need the following theorem of Liebeck and Shalev [16].

Theorem 5.1. *There exists an absolute positive constant a such that, if G is a finite simple group and S is a nontrivial normal subset of G , then $G = S^m$, where $m \leq a \frac{\log |G|}{\log |S|}$.*

Proof of Theorem 1.5. Let a be the absolute constant from Theorem 5.1. Choose a positive integer b larger than $2a$. Suppose first that $|S| \geq \sqrt{|G|}$. Then Theorem 5.1 implies that $G = S^m$ where

$$m \leq \frac{a \log |G|}{\log |S|} \leq 2a \leq b,$$

and hence $S^b = G$.

Now suppose that $|S| \leq \sqrt{|G|}$. Then

$$\frac{\log |S|}{a \log |G|} \geq \frac{\log |S|}{2a(\log |G| - \log |S|)} = \frac{\log |S|}{2a(\log(|G|/|S|))}.$$

Theorem 5.1 implies, once again, that for some $m \leq \frac{a \log |G|}{\log |S|}$ we have $G = S^m$. Hence, applying Theorem 4.3 to the normal subset S , we see that

$$\frac{|S^2|}{|S|} \geq \left(\frac{|S^m|}{|S|} \right)^{\frac{1}{m}} \geq \left(\frac{|G|}{|S|} \right)^{\frac{\log |S|}{a \log |G|}} \geq \left(\frac{|G|}{|S|} \right)^{\frac{\log |S|}{2a(\log(|G|/|S|))}} = |S|^{\frac{1}{2a}} \geq |S|^{\frac{1}{b}},$$

and this completes the proof. \square

The next result is a strengthening of [27, Theorem 7.4].

Proposition 5.2. *For every $\delta > 0$ there exists $\varepsilon > 0$ such that for any finite simple group G and subsets A and B of G with B normal in G and $|A| \leq |G|^{1-\delta}$ we have*

$$|AB| \geq |A||B|^\varepsilon.$$

Proof. We assume that A is nonempty and B is nontrivial, otherwise the result is immediate.

By Theorem 5.1, $G = B^m$, where $m \leq a \frac{\log |G|}{\log |B|}$. Let $K = |AB|/|A|$. Then, by Theorem 4.3, there is a nonempty subset X of A such that $|XB^m| \leq K^m|X|$. It follows that

$$|G| = |B^m| = |XB^m| \leq K^m|X| \leq K^m|A|.$$

Since $|A| \leq |G|^{1-\delta}$ and $m \leq a \frac{\log |G|}{\log |B|}$ we can rearrange this inequality to give

$$|G|^\delta \leq K^{a \frac{\log |G|}{\log |B|}}.$$

This is equivalent to $|B|^{\frac{\delta}{a}} \leq K$, which, with $\varepsilon = \frac{\delta}{a}$, is the required result. \square

Proposition 5.2 constitutes the expansion result for B^2 that was partially proven in [27, Proposition 10.4]. Furthermore it goes some way towards a proof of [27, Conjecture 10.3] although what remains is the more difficult part of the conjecture.

We can strengthen [27, Proposition 10.4] in a different direction as follows.

Proposition 5.3. *For every $\delta > 0$ and positive integer r there exists $\varepsilon > 0$ such that for any finite simple group G of Lie type of rank r and any set $S \subseteq G$ such that $|S| \leq |G|^{1-\delta}$, there exists g in G such that*

$$|SS^g| \geq |S|^{1+\varepsilon}.$$

Proof. Given $\delta > 0$ and a positive integer r , let ε be the positive constant from Theorem 1.4. Now choose any subset S of G such that $|S| \leq |G|^{1-\delta}$. According to Theorem 1.4, either $|SS^g| \geq |S|^{1+\varepsilon}$ or else $S^3 = G$. In the former case the result is proven. In the latter case we apply Lemma 2.1 with $J = K = (|S^3|/|S|)^{1/10}$ to deduce the existence of an element g of G with $|SgS| > K|S|$. Then, using $S^3 = G$ and $|G| \geq |S|^{1+\delta}$, it follows that

$$|SgS| > \left(\frac{|S^3|}{|S|} \right)^{\frac{1}{10}} |S| \geq |S|^{1+\frac{\delta}{10}}.$$

Provided that ε is chosen to be smaller than $\frac{\delta}{10}$, the inequality $|SS^g| \geq |S|^{1+\varepsilon}$ is again satisfied. \square

6. THE SKEW DOUBLING LEMMA

The next result is another analogue of the Doubling lemma for nonabelian groups, which we call the *Skew doubling lemma*.

Lemma 6.1 (Skew doubling lemma). *If S is a finite subset of a group G such that, for some positive number K , $|SS^g| \leq K|S|$ for every conjugate S^g of S , then*

$$|S_1 \cdots S_m| \leq K^{14(m-1)}|S|$$

for $m = 1, 2, \dots$, where each of S_1, \dots, S_m is any conjugate of either S or S^{-1} .

To prove Lemma 6.1 we will use Lemma 2.1 and the following result, Ruzsa's triangle inequality [24] (see also [30, Section 2.3]).

Lemma 6.2. *Let U, V and W be finite subsets of a group G . Then*

$$\frac{|VW^{-1}|}{|U|} \leq \frac{|UV^{-1}|}{|U|} \frac{|UW^{-1}|}{|U|}.$$

First we prove a special case of Lemma 6.1.

Lemma 6.3. *Let S be a finite subset of a group G . Suppose that K is a positive number such that $|SS^g| \leq K|S|$ for each g in G . Then $|S_1 S_2 S_3| \leq K^{14}|S|$, where each of S_1, S_2 and S_3 is any conjugate of either S or S^{-1} .*

Proof. Choose elements a and b of G . We can apply Lemma 2.1 with $J = K$ to obtain

$$|S^3| \leq K^8|S|.$$

Using this inequality and Lemma 6.2 (with $U = S^{-1}$, $V = SS$ and $W = S$) we obtain

$$\frac{|SSS^{-1}|}{|S|} \leq \frac{|S^{-1}S^{-1}S^{-1}|}{|S|} \frac{|S^{-1}S^{-1}|}{|S|} = \frac{|S^3|}{|S|} \frac{|S^2|}{|S|} \leq K^9.$$

Using this inequality and Lemma 6.2 (with $U = S$, $V = S^{-1}$ and $W = SS^{-1}$) we obtain

$$\frac{|S^{-1}SS^{-1}|}{|S|} \leq \frac{|SS|}{|S|} \frac{|SSS^{-1}|}{|S|} \leq K^{10}.$$

Using this inequality and Lemma 6.2 (with $U = S^{-1}$, $V = SS^{-1}$ and $W = Sa$) we obtain

$$\frac{|SS^{-1}a^{-1}S^{-1}|}{|S|} \leq \frac{|S^{-1}SS^{-1}|}{|S|} \frac{|S^{-1}a^{-1}S^{-1}|}{|S|} \leq K^{11}.$$

Using this inequality and Lemma 6.2 (with $U = S$, $V = SaS$ and $W = S^{-1}b^{-1}$) we obtain

$$(6.1) \quad \frac{|SaSbS|}{|S|} \leq \frac{|SS^{-1}a^{-1}S^{-1}|}{|S|} \frac{|SbS|}{|S|} \leq K^{12}.$$

Using this inequality and Lemma 6.2 (with $U = S$, $V = S^{-1}$ and $W = S^{-1}b^{-1}S^{-1}a^{-1}$) we obtain

$$(6.2) \quad \frac{|S^{-1}aSbS|}{|S|} \leq \frac{|SS|}{|S|} \frac{|SaSbS|}{|S|} \leq K^{13}.$$

Finally, using this inequality and Lemma 6.2 (with $U = S^{-1}$, $V = S^{-1}aSb$ and $W = S$) we obtain

$$(6.3) \quad \frac{|S^{-1}aSbS^{-1}|}{|S|} \leq \frac{|S^{-1}b^{-1}S^{-1}a^{-1}S|}{|S^{-1}|} \frac{|S^{-1}S^{-1}|}{|S^{-1}|} = \frac{|S^{-1}aSbS|}{|S|} \frac{|SS|}{|S|} \leq K^{14}.$$

Equations (6.1), (6.2) and (6.3) imply that, given any conjugates S_1 , S_2 and S_3 of either S or S^{-1} , we have $|S_1S_2S_3|/|S| \leq K^{14}$, as required. \square

We need the following proposition.

Proposition 6.4. *If A and B are finite subsets of a group G such that, for some positive number K , $|BB^g| \leq K|B|$ for every conjugate B^g of B , then*

$$|AB_1B_2| \leq K^{14}|AB_3|,$$

where each of B_1 , B_2 and B_3 is any conjugate of B or B^{-1} .

Proof. By Lemma 6.3 we have

$$\frac{|B_3^{-1}B_1B_2|}{|B_3|} \leq K^{14},$$

where each of B_1 , B_2 and B_3 is any conjugate of B or B^{-1} . Applying Lemma 6.2 with $U = B_3^{-1}$, $V = A$ and $W = B_2^{-1}B_1^{-1}$ we obtain

$$\frac{|AB_1B_2|}{|AB_3|} = \frac{|AB_1B_2|}{|B_3^{-1}A^{-1}|} \leq \frac{|B_3^{-1}B_1B_2|}{|B_3|} \leq K^{14},$$

as required. \square

We can finally prove Lemma 6.1.

Proof of the Skew doubling lemma. The result holds trivially when $m = 1$ and $m = 2$. Suppose that $m \geq 3$. Apply Proposition 6.4 with $B = S$, $A = S_1 \cdots S_{n-2}$, $B_1 = B_3 = S_{n-1}$ and $B_2 = S_n$ to see that

$$\frac{|S_1 \cdots S_n|}{|S_1 \cdots S_{n-1}|} \leq K^{14}$$

for $n = 3, 4, \dots, m$. It follows that

$$\begin{aligned} \frac{|S_1 \cdots S_m|}{|S|} &= \left(\frac{|S_1 \cdots S_m|}{|S_1 \cdots S_{m-1}|} \right) \left(\frac{|S_1 \cdots S_{m-1}|}{|S_1 \cdots S_{m-2}|} \right) \cdots \left(\frac{|S_1 S_2 S_3|}{|S_1 S_2|} \right) \left(\frac{|S_1 S_2|}{|S_1|} \right) \\ &\leq (K^{14})^{m-2} K \\ &\leq K^{14(m-1)}, \end{aligned}$$

as required. \square

Using the Skew doubling lemma we can derive Conjecture 1.6 from Conjecture 1.1. The proof is similar to the proof of Theorem 1.5.

Proof that Conjecture 1.1 implies Conjecture 1.6. Let c be the absolute constant from Conjecture 1.1. We define b to be a positive integer greater than $2c$, and $\varepsilon = 1/(28c)$. Suppose first that $|S| \geq \sqrt{|G|}$. Then Conjecture 1.1 implies that $G = S_1 \cdots S_N$, for conjugates S_1, \dots, S_N of S , where

$$N \leq \frac{c \log |G|}{\log |S|} \leq 2c < b,$$

and hence G is certainly the product of b conjugates of S .

Now suppose that $|S| \leq \sqrt{|G|}$. Then

$$\frac{\log |G| - \log |S|}{c \log |G| - \log |S|} \geq \frac{\log |G| - \log |S|}{c \log |G|} \geq \frac{1}{2c}.$$

In particular observe that

$$c \log |G| - \log |S| \leq 2c(\log |G| - \log |S|) = 2c \log(|G|/|S|).$$

Conjecture 1.1 implies, once again, that for some $N \leq \frac{c \log |G|}{\log |S|}$ we have $G = S_1 \cdots S_N$, for conjugates S_1, \dots, S_N of S . Using the Skew doubling lemma, Lemma 6.1, we see that there is an element g of G for which

$$\frac{|SS^g|}{|S|} \geq \left(\frac{|S_1 \cdots S_N|}{|S|} \right)^{\frac{1}{14(N-1)}} \geq \left(\frac{|G|}{|S|} \right)^{\frac{\log |S|}{14(c \log |G| - \log |S|)}} \geq \left(\frac{|G|}{|S|} \right)^{\frac{\log |S|}{28c(\log(|G|/|S|))}} \geq |S|^{\frac{1}{28c}},$$

and this completes the proof. \square

REFERENCES

- [1] L. Babai, N. Nikolov, and L. Pyber. Product growth and mixing in finite groups. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 248–257, New York, 2008. ACM.
- [2] G. M. Bergman and H. W. Lenstra, Jr. Subgroups close to normal subgroups. *J. Algebra*, 127(1):80–97, 1989.
- [3] E. Breuillard, B. Green, and T. Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.*, 21(4):774–819, 2011.
- [4] W. T. Gowers. Quasirandom groups. *Combin. Probab. Comput.*, 17(3):363–387, 2008.
- [5] R. M. Guralnick and W. M. Kantor. Probabilistic generation of finite simple groups. *J. Algebra*, 234(2):743–792, 2000. Special issue in honor of Helmut Wielandt.
- [6] H. A. Helfgott. Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math. (2)*, 167(2):601–623, 2008.
- [7] H. A. Helfgott. Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$. *J. Eur. Math. Soc. (JEMS)*, 13(3):761–851, 2011.
- [8] M. Kassabov, A. Lubotzky, and N. Nikolov. Finite simple groups as expanders. *Proc. Natl. Acad. Sci. USA*, 103(16):6116–6119 (electronic), 2006.
- [9] P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.
- [10] V. Landazuri and G. M. Seitz. On the minimal degrees of projective representations of the finite Chevalley groups. *J. Algebra*, 32:418–443, 1974.
- [11] M. W. Liebeck, N. Nikolov, and A. Shalev. Product decompositions in finite simple groups. *Bull. London Math. Soc.* Published on-line; doi: 10.1112/blms/bdr107.
- [12] M. W. Liebeck, N. Nikolov, and A. Shalev. A conjecture on product decompositions in simple groups. *Groups Geom. Dyn.*, 4(4):799–812, 2010.
- [13] M. W. Liebeck, N. Nikolov, and A. Shalev. Groups of Lie type as products of SL_2 subgroups. *J. Algebra*, 326:201–207, 2011.
- [14] M. W. Liebeck, C. E. Praeger, and J. Saxl. The maximal factorizations of the finite simple groups and their automorphism groups. *Mem. Amer. Math. Soc.*, 86(432):iv+151, 1990.

- [15] M. W. Liebeck and L. Pyber. Finite linear groups and bounded generation. *Duke Math. J.*, 107(1):159–171, 2001.
- [16] M. W. Liebeck and A. Shalev. Diameters of finite simple groups: sharp bounds and applications. *Ann. of Math. (2)*, 154(2):383–406, 2001.
- [17] A. Lubotzky. Finite simple groups of Lie type as expanders. *J. Eur. Math. Soc. (JEMS)*, 13(5):1331–1341, 2011.
- [18] N. Nikolov. A product decomposition for the classical quasisimple groups. *J. Group Theory*, 10(1):43–53, 2007.
- [19] N. Nikolov and L. Pyber. Product decompositions of quasirandom groups and a Jordan type theorem. *J. Eur. Math. Soc. (JEMS)*, 13(4):1063–1077, 2011.
- [20] G. Petridis. New proofs of Plünnecke-type estimates for product sets in groups. 2011, Preprint available on the Math arXiv: <http://arxiv.org/abs/1101.3507>.
- [21] H. Plünnecke. *Eigenschaften und Abschätzungen von Wirkungsfunktionen*. BMwF-GMD-22. Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 1969.
- [22] H. Plünnecke. Eine zahlentheoretische Anwendung der Graphentheorie. *J. Reine Angew. Math.*, 243:171–183, 1970.
- [23] L. Pyber and E. Szabó. Growth in finite simple groups of Lie type of bounded rank. 2010, Preprint available on the Math arXiv: <http://arxiv.org/abs/1005.1858>.
- [24] I. Z. Ruzsa. Sums of finite sets. In *Number theory (New York, 1991–1995)*, pages 281–293. Springer, New York, 1996.
- [25] I. Z. Ruzsa. Sumsets and structure. In *Combinatorial number theory and additive group theory*, Adv. Courses Math. CRM Barcelona, pages 87–210. Birkhäuser Verlag, Basel, 2009.
- [26] I. Z. Ruzsa. Towards a noncommutative Plünnecke-type inequality. In *An irregular mind*, volume 21 of *Bolyai Soc. Math. Stud.*, pages 591–605. János Bolyai Math. Soc., Budapest, 2010.
- [27] A. Shalev. Word maps, conjugacy classes, and a noncommutative Waring-type theorem. *Ann. of Math. (2)*, 170(3):1383–1416, 2009.
- [28] A. Stein. $1\frac{1}{2}$ -generation of finite simple groups. *Beiträge Algebra Geom.*, 39(2):349–358, 1998.
- [29] T. Tao. Product set estimates for non-commutative groups. *Combinatorica*, 28(5):547–594, 2008.
- [30] T. Tao and V. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

LÁSZLÓ PYBER AND ENDRE SZABÓ
A. RÉNYI INSTITUTE OF MATHEMATICS
HUNGARIAN ACADEMY OF SCIENCES
P.O. BOX 127
H-1364 BUDAPEST
E-mail address: pyber@renyi.hu
E-mail address: endre@renyi.hu

NICK GILL AND IAN SHORT
DEPARTMENT OF MATHEMATICS AND STATISTICS
THE OPEN UNIVERSITY
MILTON KEYNES, MK7 6AA
UNITED KINGDOM
E-mail address: n.gill@open.ac.uk
E-mail address: i.short@open.ac.uk