A conjecture on product decompositions in 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

May 24, 2010

Abstract

We propose a conjecture concerning decompositions of finite simple groups as products of conjugate subgroups, and prove it for a large class of maximal subgroups.

1 Introduction

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 H is any nontrivial subgroup of G, then G is a product of N conjugates of H for some $N \leq c \log|G|/\log|H|$.*

Note that since a product of n conjugates of H has size at most $|H|^n$, the upper bound for N in the conjecture is best possible, up to the value of the constant c. The conjecture is in the spirit of the main result of [17], which shows that if C is a non-identity conjugacy class of the simple group G, then $G = C^N$ for some $N \leq c \log|G|/\log|C|$.

Our conjecture is a far reaching generalization of various recent results. For example, [15, Theorem 1] shows that if G is a simple group of Lie type in

The third author acknowledges the support of an EPSRC Visiting Fellowship at Imperial College London

2000 *Mathematics Subject Classification:* 20G40 characteristic p, then G is a product of at most 25 of its Sylow p-subgroups (see also [4] for a recent improvement from 25 to 5). Also [18] shows that every classical group over $\mathbb{F}_q$ is a product of at most 200 conjugate subgroups of type $SL_n(q)$. These results support the special case of the conjecture where $|H| > |G|^\epsilon$ for some fixed $\epsilon > 0$, and one has to show that G is a bounded product of conjugates of H. Particular results of this type are essential in the proof that simple groups can be made into expanders (see the announcement [8] and [14]).

In this paper we prove two results which go some way towards establishing the conjecture in the case where H is a maximal subgroup of G. The first is a proof of the conjecture in this case when G is a group of Lie type of bounded rank, and the second when $\log|G|/\log|H|$ is bounded.

Theorem 1 *If G is a finite simple group of Lie type of rank r and H is a maximal subgroup of G, then G is a product of N conjugates of H for some $N \leq c \log|G|/\log|H|$, where $c = c(r)$ depends only on r.*

Theorem 2 *There is a function $f : \mathbb{N} \to \mathbb{N}$ and an absolute constant c such that the following holds. If $k \in \mathbb{N}$, and G is a finite simple group with a maximal subgroup H such that $\log|G|/\log|H| \leq k$ and $|G| > f(k)$, then G is a product of at most $c \log|G|/\log|H|$ conjugates of H.*

In Theorem 1 the constant c is not explicit. Likewise the function f in Theorem 2 is not explicit; however our proof shows that the constant c can be taken to be less than 10^8 provided the rank of G is sufficiently large.

Our proof of Theorem 1, given in Section 2, uses a variety of tools. For the case where $|H|$ is bounded (in terms of the rank r), we use results from [3] and [6] concerning diameters of Cayley graphs. If H is of unbounded order and is not a subfield subgroup $G(q_0)$ (where $G = G(q)$ and $\mathbb{F}_{q_0}$ is a subfield of $\mathbb{F}_q$), we use [13, Theorem 1.2], which relies heavily on model theory.

The proof of Theorem 2 is divided into the case of alternating groups (Section 3) and groups of Lie type (Section 4). The alternating case is based on combinatorial arguments. For the groups of Lie type, we need to consider only classical groups of large rank by Theorem 1, and for these our arguments are mostly constructive although we also use some character theoretic methods via recent results from [19] and [23].

2 Proof of Theorem 1

First we state a result taken from [19, Corollary 1] which will be useful at several points in this section and the next.

Lemma 2.1 *Let G be a finite group and let k be the minimal degree of a nontrivial complex character of G. Suppose S is a subset of G such that $|S| > |G|/k^{1/3}$. Then $G = S^3$.*

Now we begin the proof of Theorem 1 with a general result about maximal subgroups of groups of Lie type.

Lemma 2.2 *There is a function $f : \mathbb{N} \to \mathbb{N}$ such that if $G = G_r(q)$ is a simple group of Lie type of rank r over $\mathbb{F}_q$, and H is a maximal subgroup of G, then one of the following holds:*

(i) $|H| < f(r)$;

(ii) *H is a subfield subgroup;*

(iii) $|H| \geq q - 1$;

Proof. For G of classical type this is well known, and we give a sketch proof. First, if H lies in one of the collections of Aschbacher subgroups $\mathcal{C}_i$ defined in [2], then by inspection of these subgroups (see [9] for their explicit structure), one sees that (i),(ii) or (iii) holds. Otherwise, the main theorem of [2] shows that H is almost simple, and [10] implies that either (i) holds or $F^*(H) \in \mathrm{Lie}(p)$, where p is the characteristic of $\mathbb{F}_q$; say $F^*(H) = H(q_0)$. By [22, Corollary 6], we have either $q_0 \geq q^{1/2}$ or $q_0 = q^{1/3}$ and $H(q_0) = {}^3D_4(q_0)$; in either case $|H(q_0)| > q - 1$ and (iii) holds.

Now suppose G is of exceptional Lie type. Write $G = \bar{G}'_\sigma$, where $\bar{G}$ is a simple adjoint algebraic group of the same type as G over the algebraic closure $\bar{\mathbb{F}}_q$ and σ is a Frobenius morphism of $\bar{G}$. Now [16, Corollary 8] states that if H is a maximal subgroup of G then either $|H| < c$ (an absolute constant), or H is a subfield subgroup, or $H = N_G(\bar{X}_\sigma)$ for some σ-stable closed connected subgroup $\bar{X}$ of $\bar{G}$ of positive dimension. In the latter case we establish that $|H| \geq q - 1$. This is clear if H is parabolic, so we may assume that $\bar{X}$ is reductive. If $\bar{X}$ has a nontrivial simple factor then H contains a group of Lie type over $\mathbb{F}_q$ by [16, 1.13], and this clearly has order greater than $q - 1$. Otherwise, $\bar{X}$ is a torus, and it is easily seen that the minimum possible order of a torus normalizer is at least $q-1$. This completes the proof. ∎

For the case of bounded maximal subgroups in Theorem 1 (i.e. H as in case (i) of Lemma 2.2), we prove the following result, which is rather more general than what is required.

Proposition 2.3 *Suppose G is a simple group of Lie type of rank r, let $1 \neq h \in G$ and let $S = \{1, h\}$. Then G is a product of N conjugates of S for some $N \leq c \log |G|$, where $c = c(r)$ depends only on r.*

Proof. By [3] there exists $k \leq 7$ and $g_1, \ldots, g_k \in G$ generating G, such that the diameter of the Cayley graph of G with respect to these generators is at most $b \log |G|$, where b is an absolute constant. Also, by [6] (see also [11]), if $C = h^G$ then there exists $d \leq ar$ such that $G = C^d$, where a is an absolute constant.

For each i with $1 \leq i \leq k$, write $g_i = h_{i1} \ldots h_{id}$ and $g_i^{-1} = h'_{i1} \ldots h'_{id}$ with all $h_{ij}, h'_{ij} \in C$. Consider the sequence $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$ repeated at least $b \log |G|$ times. By the above, every element of G is equal to a sub-product of elements in this sequence. Replacing each g_i by the sequence $h_{i1}, \ldots, h_{id}$ and likewise for g_i^{-1}, we see that each element of G is a sub-product of the resulting sequence. This means that G is a product of $2kdb \log |G| \leq 14arb \log |G|$ conjugates of S. The result follows. ∎

Note that the case of Theorem 1 where $|H|$ is bounded by a function of r follows immediately from Proposition 2.3, taking $1 \neq h \in H$.

Next we consider the maximal subgroups in case (iii) of Lemma 2.2, excluding subfield subgroups. The main ingredient here is [13, Theorem 1.2], which is proved using a substantial amount of model theory.

Proposition 2.4 *Let $G = G(q)$ be a finite simple group of Lie type of rank r, and suppose that H is a maximal non-subfield subgroup of G of order at least $q-1$. Then G is a product of c conjugates of H, where $c = c(r)$ depends only on r.*

Proof. Let X be the coset space G/H. Recall that an *orbital graph* is a graph with vertex set X, and edge set an orbit of G on the set of unordered pairs of elements of X; as G is primitive on X, all the orbital graphs are connected by a classical result of D.G. Higman.

By [13, Theorem 1.2], there is a constant $d = d(r)$ such that the diameters of all the orbital graphs are at most d. Each orbital consists of elements of X in double cosets $Hg^{\pm 1}H$ for some $1 \neq g \in G \backslash H$. It follows that for each $g \in G \setminus H$, every element $x \in G$ can be written as $x = h_1 g^{\epsilon_1} \cdots h_e g^{\epsilon_e}$, where $h_i \in H$, $\epsilon_i = \pm 1$ and $e \leq d$. Hence G is the union of at most $\sum_{e=0}^{d} 2^e < 2^{d+1}$ products of the form $Hg^{\epsilon_1} \cdots Hg^{\epsilon_e}$ with $e \leq d$. One of these products, say $Hg^{\epsilon_1} \cdots Hg^{\epsilon_e}$ therefore has size greater than $|G|/2^{d+1}$. This implies that there is a product S of at most d conjugates of H such that $|S| > |G|/2^{d+1}$.

We now use Lemma 2.1 to complete the proof: by [10], if q is large enough (as we may assume) then the minimal nontrivial character degree k of G satisfies $k > 2^{3(d+1)}$, so for the set S in the previous paragraph, we have $G = S^3$. It follows that G is a product of at most $3d$ conjugates of H. ∎

It remains to prove Theorem 1 in the case where H is a subfield subgroup. For this we require the following result.

Lemma 2.5 *Let $\mathbb{F}_q$ be a field and let $\mathbb{F}_{q_0}$ be a subfield with $|\mathbb{F}_q : \mathbb{F}_{q_0}| = d$. Let G be $SL_2(q)$, $Sz(q)$ or $SU_3(q)$, and let G_0 be a subfield subgroup $SL_2(q_0)$, $Sz(q_0)$ or $SU_3(q_0)$, respectively. Then G is a product of at most $26d$ conjugates of a subgroup G_0.*

Proof. First consider $G = SL_2(q)$ and let G_0 be a subgroup $SL_2(q_0)$. Take U, U_0 to be Sylow p-subgroups of G, G_0 respectively, and choose notation so that $U = \{u(\alpha) : \alpha \in \mathbb{F}_q\}$ and $U_0 = \{u(\alpha) : \alpha \in \mathbb{F}_{q_0}\}$, where

$$u(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

If $h(\lambda) = \mathrm{diag}(\lambda^{-1}, \lambda) \in G$, then $U_0^{h(\lambda)} = \{u(\lambda^2\alpha) : \alpha \in \mathbb{F}_{q_0}\}$. Choose a basis $\lambda_1, \ldots, \lambda_d$ for $\mathbb{F}_q$ over $\mathbb{F}_{q_0}$. Now every element of a finite field is a sum of two squares (since more than half of the field elements are squares). Expressing each λ_i as a sum of two squares, it follows that there is a spanning set $\alpha_1^2, \ldots, \alpha_{2d}^2$ for $\mathbb{F}_q$ over $\mathbb{F}_{q_0}$, where $\alpha_i \in \mathbb{F}_q$. Hence

$$U = U_0^{h(\alpha_1)} \cdots U_0^{h(\alpha_{2d})}. \tag{1}$$

By [15, Theorem D], G is a product of 13 conjugates of U, and the result follows.

Next consider $G = Sz(q)$. Again let U, U_0 be Sylow p-subgroups of G, G_0. By [24] (see Section 4), we have $q = 2^{2k+1}$ and $U = \{(\alpha, \beta) : \alpha, \beta \in \mathbb{F}_q\}$ with multiplication

$$(\alpha, \beta)\,(\gamma, \delta) = (\alpha + \gamma, \alpha\gamma^\theta + \beta + \delta)$$

where $\gamma^\theta = \gamma^{2^{k+1}}$. Also $U_0 = \{(\alpha, \beta) : \alpha, \beta \in \mathbb{F}_{q_0}\}$. Now $N_G(U)$ contains a subgroup $\{\phi(\zeta) : \zeta \in \mathbb{F}_q^*\}$, where

$$(\alpha, \beta)^{\phi(\zeta)} = (\zeta\alpha, \zeta^{1+\theta}\beta).$$

If $\zeta_1, \ldots, \zeta_d$ is a basis for $\mathbb{F}_q$ over $\mathbb{F}_{q_0}$, then as above we see that for any $\alpha \in \mathbb{F}_q$, there exists β such that (α, β) lies in the product $U_0^{\phi(\zeta_1)} \cdots U_0^{\phi(\zeta_d)}$. Also $1 + \theta$ is surjective on $\mathbb{F}_q$ (since $(2^{2k+1} - 1, 2^{k+1} + 1) = 1$), so there is a basis for $\mathbb{F}_q$ over $\mathbb{F}_{q_0}$ of the form $\eta_1^{1+\theta}, \ldots, \eta_d^{1+\theta}$, and any element $(0, \delta)$ ($\delta \in \mathbb{F}_q$) lies in the product $U_0^{\phi(\eta_1)} \cdots U_0^{\phi(\eta_d)}$. Since $(\alpha, \beta)\,(0, \delta) = (\alpha, \beta + \delta)$, it follows that

$$U = U_0^{\phi(\zeta_1)} \cdots U_0^{\phi(\zeta_d)} \cdot U_0^{\phi(\eta_1)} \cdots U_0^{\phi(\eta_d)}, \tag{2}$$

a product of $2d$ conjugates of U_0. Now the result follows from [15] as above.

Finally, let $G = SU_3(q)$. This is similar to the previous case. Here $d = |\mathbb{F}_q : \mathbb{F}_{q_0}|$ is odd, and from [20, p.255], a Sylow p-subgroup U of G can be taken as

$$U = \{(\alpha, \beta) \,:\, \alpha, \beta \in \mathbb{F}_{q^2}, \beta + \bar{\beta} + \alpha\bar{\alpha} = 0\}$$

where $\bar{\alpha} = \alpha^q$, and the multiplication is $(\alpha, \beta)\,(\gamma, \delta) = (\alpha + \gamma, \beta + \delta - \bar{\alpha}\gamma)$. Also $U_0 = \{(\alpha, \beta) : \alpha, \beta \in \mathbb{F}_{q_0^2}\} \in Syl_p(G_0)$. For $\lambda \in \mathbb{F}_{q^2}^*$, $N_G(U)$ contains an element $k(\lambda)$ such that

$$(\alpha, \beta)^{k(\lambda)} = (\lambda^2\bar{\lambda}^{-1}\alpha,\, \lambda\bar{\lambda}\beta).$$

We can choose $\lambda_1, \ldots, \lambda_d$ such that $\lambda_i^2\bar{\lambda}_i^{-1}$ $(1 \le i \le d)$ form a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_{q_0^2}$. Hence for any $\alpha \in \mathbb{F}_{q^2}$, there exists β such that (α, β) lies in the product $U_0^{k(\lambda_1)} \cdots U_0^{k(\lambda_d)}$. Similarly there exist $\mu_1, \ldots, \mu_d \in \mathbb{F}_{q^2}$ such that any $(0, \delta)$ $(\delta \in \mathbb{F}_{q^2},\, \delta + \bar{\delta} = 0)$ lies in the product $U_0^{k(\mu_1)} \cdots U_0^{k(\mu_d)}$. Hence

$$U = U_0^{k(\lambda_1)} \cdots U_0^{k(\lambda_d)} \cdot U_0^{k(\mu_1)} \cdots U_0^{k(\mu_d)}. \tag{3}$$

Now the result follows as in the previous cases. ■

Now we are able to prove Theorem 1 for subfield subgroups. The next result is slightly more general than we need, since it deals with arbitrary subfield subgroups, not just maximal ones.

Proposition 2.6 *Let $G = G(q)$ be a finite simple group of Lie type of rank r, and let $H = G(q_0)$ be a subfield subgroup of G, where $|\mathbb{F}_q : \mathbb{F}_{q_0}| = d$. Then G is a product of at most $100r^2d$ conjugates of H.*

Proof. First consider the case where G is an untwisted group. As in [5], take G to be generated by root groups $U_\alpha = \{x_\alpha(t) : t \in \mathbb{F}_q\}$ for α in the root system Φ of G, and H to be generated by subgroups $U_\alpha^0 = \{x_\alpha(t) : t \in \mathbb{F}_{q_0}\}$. By [5, 5.3.3], we have $U = \prod_{\alpha\in\Phi^+} U_\alpha \in Syl_p(G)$ and $U_0 = \prod_{\alpha\in\Phi^+} U_\alpha^0 \in Syl_p(G_0)$, where the product is taken over positive roots in increasing order. Since U_α is a Sylow p-subgroup of the group $\langle U_{\pm\alpha}\rangle \cong (P)SL_2(q)$, the equality (1) shows that U_α is a product of $2d$ conjugates of U_α^0. It follows that U is a product of $2d|\Phi^+|$ conjugates of U_0, and hence by [15, Theorem D], G is a product of at most $26d|\Phi^+|$ conjugates of G_0. Since $|\Phi^+| < 2r^2$, the result follows in the untwisted case.

Now suppose that G is a twisted group. Again let U, U_0 be Sylow p-subgroups of G, H respectively. Then [5, 13.6.1] shows that we can write $U = U_1 \cdots U_k$, where $k \le |\Phi^+|$ and each U_i is a Sylow p-subgroup of one of the groups $(P)SL_2(q^i)$ $(i \in \{1, 2, 3\})$, $(P)SU_3(q)$ or $Sz(q)$, with a similar expression $U_0 = U_1^0 \cdots U_k^0$ for U_0. By (1), (2), (3), each U_i is a product of at most $2d$ conjugates of U_i^0, and so U is a product of $2dk$ conjugates of U_0.

Now [15, Theorem D] shows that G is a product of at most $50dk$ conjugates of G_0. This completes the proof. ■

The proof of Theorem 1 is now complete.

3 Proof of Theorem 2 for alternating groups

Let $G = A_n$, $k \in \mathbb{N}$, and let H be a maximal subgroup of G with $|H| \geq |G|^{1/k}$.

Lemma 3.1 *For n sufficiently large in terms of k, one of the following holds:*

(i) $H = (S_m \times S_{n-m}) \cap G$ *for some m (H intransitive)*

(ii) $H = (S_m \wr S_{n/m}) \cap G$ *for some proper divisor m of n (H imprimitive).*

Proof. The only alternative to (i) and (ii) is that H is primitive on $\{1, \ldots, n\}$. If this is the case then $|H| < 4^n$ by [21], which is not possible provided $4^{nk} < n!/2$. ■

The next lemma allows us to work with S_n instead of A_n in the proof of Theorem 2, which is convenient.

Lemma 3.2 *Let H be a subgroup of S_n with $H \not\leq A_n$, and define $K = H \cap A_n$. Suppose that $S_n = \prod_{i=1}^{t} H^{a_i}$ for some $a_i \in S_n$. Then, provided $n > 2^{3t}$, A_n is a product of $3t$ conjugates of K.*

Proof. Note first that since by hypothesis H is normalized by an odd permutation, any S_n-conjugate of H is also an A_n-conjugate. Now pick an element $x \in H \backslash K$ so that $H = K \cup xK$. Then

$$\prod_{i=1}^{t} H^{a_i} = \prod_{i=1}^{t} (K \cup xK)^{a_i} = \prod_{i=1}^{t} (K^{a_i} \cup x^{a_i} K^{a_i}).$$

For any t-tuple $\mathbf{b} = (b_1, \ldots, b_t)$ with $b_i \in \{1, x^{a_i}\}$, define the set

$$X_{\mathbf{b}} = \prod_{i=1}^{t} b_i K^{a_i} = b_1 \cdots b_t \prod_{i=1}^{t} K^{g_i},$$

where $g_i = a_i b_{i+1} \cdots b_t$.

Altogether we see that A_n is a union of the 2^{t-1} sets $X_{\mathbf{b}}$ as $\mathbf{b}$ ranges over all possible t-tuples $\mathbf{b}$ with an even number of terms $b_j = 1$. By the pigeonhole principle $|X_{\mathbf{b}}| > |A_n|/2^t$ for at least one such $\mathbf{b}$. Put $X = X_{\mathbf{b}}$. Then by Lemma 2.1 and the fact that the minimal degree of a nontrivial complex representation of A_n is $n-1 \geq 2^{3t}$, we have $A_n = X^3$, and it easily follows that A_n is a product of $3t$ conjugates of K. ■

In view of Lemma 3.2, to prove Theorem 2 for alternating groups it is sufficient to express the symmetric group S_n as a product of the appropriate numbers of conjugates of the subgroups $H = S_m \times S_{n-m}$ and $H = S_m \wr S_{n/m}$ in Lemma 3.1.

In the following lemmas, the inclusions of the groups S_k and S_k^t in S_n are the natural ones: the S_k fixes $n-k$ points, and the S_k^t acts imprimitively on kt points and fixes the rest.

Lemma 3.3 *S_{4n} is a product of 6 conjugates of S_{2n}. More generally if $k \leq n \leq 2k$ then S_n is a product of at most 8 conjugates of S_k.*

Proof. We will prove the first part of the statement; the proof of the second is similar. For $i = 1, \ldots, 4$ define subsets X_i of $\{1, 2, \ldots, 4n\}$ as follows:

$$\begin{aligned} &X_1 = \{1, \ldots, 2n\}, \quad X_2 = \{2n+1, \ldots, 4n\}, \\ &X_3 = \{1, \ldots, n, 2n+1, \ldots, 3n\}, \\ &X_4 = \{n+1, n+2, \ldots, 2n, 3n+1, 3n+2, \ldots, 4n\}. \end{aligned}$$

Let J_i be the copy of S_{2n} acting on the set X_i and fixing all points outside.

Let $g \in S_{4n}$ and put $Y = gX_1 \cap X_2$, $Z = gX_2 \cap X_1$. Then $|Y| = |Z|$ and with an application of an element $h \in J_1J_2$ we can make hY and hZ to be initial segments of X_2 and X_1 respectively. Now with an application of an element $h' \in J_3J_4$ we can swap hY and hZ fixing all the other elements and thus achieve that $h'hg$ stabilizes X_1 and X_2 and so $h'hg \in J_1J_2$. Therefore $g \in J_1J_2J_3J_4J_1J_2$. ■

Lemma 3.4 *$S_{nm} = ABA$ where A is a conjugate of $(S_n)^m$ and B is a conjugate of $(S_m)^n$.*

Proof. This is the content of Lemma 4 of [1]. ■

Corollary 3.5 *For an integer $t \geq 2$ the group S_{n^t} is a product of $2t-1$ conjugates of $(S_n)^{n^{t-1}}$.*

Proof. Use induction on t. The case $t = 1$ is trivial. If the result is true for some $t \geq 1$ apply Lemma 3.4 with $m = n^t$ to get that

$$S_{n^{t+1}} = ABA, \quad A = S_n^{n^t}, \quad B \text{ conjugate to } S_{n^t}^n,$$

and apply the induction hypothesis to B. ■

Proposition 3.6 *Suppose that $n = mk$. Then S_n is a product of at most $16\frac{\log n}{\log m} + 24$ copies of $H = (S_m)^k$.*

Proof. Let l be the largest integer such that $m^l \leq n$. Then $l \leq \frac{\log n}{\log m}$ and if $a = m^l$ then $a > k$. By Corollary 3.5, S_a is a product of $2l - 1$ conjugates of $(S_m)^{m^{l-1}}$. Let b be the largest integer such that $ba \leq n$. Then $ab \geq n/2$ and also $bm^{l-1} \leq k$. Hence $(S_m)^{bm^{l-1}} \leq H$ and so $(S_a)^b$ is a product of $2l - 1$ conjugates of H.

Again using Lemma 3.4 we see that S_{ab} is a product of two conjugates of $(S_b)^a$ and a conjugate of $(S_a)^b$. We saw that $(S_a)^b$ is contained in a product of at most $2l - 1$ conjugates of H and we claim that $(S_b)^a$ is contained in a product of at most 2 conjugates of H. To see this, observe that each copy of S_m contains the direct product of at least $[m/b] \geq m/2b$ copies of S_b and so $H = (S_m)^k$ contains the direct product of at least $km/(2b) = n/2b \geq ab/2b = a/2$ copies of S_b. Therefore $(S_b)^a$ is contained in at most 2 conjugates of H, proving the claim.

Therefore S_{ab} is contained in the product of at most $2l - 1 + 4 = 2l + 3$ conjugates of H. Since $ab \geq n/2$ it follows from Lemma 3.3 that S_n is a product of 8 conjugates of S_{ab}, which proves the proposition. ■

Proposition 3.7 *For $2 \leq m \leq n$, the group S_n is a product of at most $320t$ conjugates of S_m, where $t = \frac{n \log n}{m \log m}$.*

Proof. Let n' be the largest multiple of m which is less than or equal to n. Then $n' > n/2$ and so S_n is a product of at most 8 conjugates of $S_{n'}$. Put $T = S_m^{n'/m}$. By Proposition 3.6, $S_{n'}$ is in a product of at most $16 \log n'/\log m + 24$ conjugates of T, and T is a product of n'/m copies of S_m. Altogether S_n is a product of at most

$$8\frac{n'}{m}\left(16\frac{\log n'}{\log m} + 24\right) \leq 8\frac{n}{m}\left(\frac{16 \log n}{\log m} + 24\right) < 320\frac{n \log n}{m \log m}$$

conjugates of S_m. ■

Proposition 3.8 *Suppose $n = mk$ for integers $m, k \in \mathbb{N}$. The group S_n is a product of at most $1280t$ conjugates of $L = S_m \wr S_k$, where $t = \log|S_n|/\log|L|$.*

Proof. In the case where $|S_k| < |S_m|^k$, we have

$$\log|G|/\log|L| > \frac{1}{2}\log|G|/k\log|S_m| \geq \frac{1}{4}\log n/\log m,$$

and we can apply Proposition 3.6 with subgroup $H = S_m^k$. Otherwise, $|S_k| \geq |S_m|^k$, which gives

$$\log|G|/\log|L| \geq \frac{1}{2}\log|S_n|/\log|S_k| \geq \frac{1}{4}\frac{n\log n}{k\log k}$$

and we apply Proposition 3.7 with $H = S_k$. ∎

As observed above, this proposition together with Lemmas 3.2 and 3.3 gives the bounds necessary to complete the proof of Theorem 2 for alternating groups.

4 Proof of Theorem 2 for groups of Lie type

Before embarking on the proof, we prove two lemmas we shall need concerning the generation of $SL_n(q)$. In the statement we abuse notation slightly by referring to the derived subgroup of a Levi subgroup of G also as a Levi subgroup.

Lemma 4.1 *There is an absolute constant b such that if $G = SL_n(q)$ and K is a Levi subgroup $SL_r(q)$ of G, then G is a product of at most $b(n/r)^2$ conjugates of K.*

Proof. Write $n = tr + k$ with $0 \leq k < r$. We first find a suitable product of conjugates of K containing all the upper unitriangular matrices in a Levi subgroup $SL_{tr}(q)$ of G. This is trivial if $t = 1$, so assume $t \geq 2$.

We first get all the upper unitriangular matrices in a Levi subgroup $SL_{2r}(q)$. Define

$$l = \begin{pmatrix} I & I \\ 0 & I \end{pmatrix} \in SL_{2r}(q).$$

Then for $d = \mathrm{diag}(a, I) \in K$ (where $a \in SL_r(q)$) we have

$$dld^{-1}l^{-1} = \begin{pmatrix} I & a - I \\ 0 & I \end{pmatrix}.$$

Thus the product $(KK^l)^2$ contains all matrices in $SL_{2r}(q)$ of the form

$$\begin{pmatrix} I & a + b - 2I \\ 0 & I \end{pmatrix} \quad (a, b \in SL_r(q)).$$

Now we claim that an arbitrary matrix in $M_r(q)$ (the set of all $r \times r$ matrices over $\mathbb{F}_q$) can be expressed as a sum of 3 matrices of the form $a + b - 2I$ with $a, b \in SL_r(q)$. To see this, observe first that taking a to be upper unitriangular and b lower unitriangular, we can make $a + b - 2I$ equal to any matrix with 0's on the diagonal. If $q > 2$, we can add a further matrix $a' + b' - 2I$ with a', b' diagonal to make the first $r - 1$ diagonal entries arbitrary; then we can adjust the last diagonal entry by adding a further diagonal matrix $a'' + b'' - 2I$. If $q = 2$, let $a \in SL_r(q)$ be a monomial matrix with prescribed diagonal entries, and let $b = I$; then $a + b$ can have arbitrary diagonal entries. This proves the claim.

It follows from the previous paragraph that there is a product of 12 conjugates of K which contains all the matrices $\begin{pmatrix} I & X \\ 0 & I \end{pmatrix}$ in $SL_{2r}(q)$. Adding two further conjugates to get the matrices $\mathrm{diag}(a, I)$, $\mathrm{diag}(I, a)$ ($a \in SL_r(q)$), we see that there is a product of 14 conjugates of K containing all the upper unitriangular matrices in $SL_{2r}(q)$.

To get to $SL_{3r}(q)$ we repeat the above argument to get two further products of 12 conjugates of K containing the matrices

$$\begin{pmatrix} I & 0 & X \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix}, \quad \begin{pmatrix} I & 0 & 0 \\ 0 & I & X \\ 0 & 0 & I \end{pmatrix}.$$

Similarly, to get $SL_{tr}(q)$ we choose products of 12 conjugates of K to get matrices as above with X in one of $\binom{t}{2}$ obvious $r \times r$ blocks, and a further t conjugates to get block diagonal matrices, to conclude that the group P of upper unitriangular matrices in $SL_{tr}(q)$ is contained in a product of $12\binom{t}{2} + t$ conjugates of K. By [15], $SL_{tr}(q)$ is a product of 25 conjugates of P (improved to 5 in [4]), hence of $60\binom{t}{2} + 5t$ conjugates of K.

Now let $s = [n/2]$ and take a Levi subgroup $R = SL_s(q)$ in $SL_{tr}(q)$. By the above argument, a subgroup $SL_{2s}(q)$ of G is contained in a product of $14 \cdot 5 = 70$ conjugates of R. If n is even then $SL_{2s}(q) = G$; and if n is odd then by [18, Lemma 2], G is a product of 4 conjugates of $SL_{2s}(q)$. We conclude that G is a product of

$$4 \cdot 70 \cdot (60\binom{t}{2} + 5t)$$

conjugates of K, giving the result. ■

Lemma 4.2 *Let $G = SL_n(q)$ and write $k = [n/2]$. Define T to be the subgroup*

$$\{\begin{pmatrix} I & X & (0) \\ 0 & I & (0) \\ (0) & (0) & (1) \end{pmatrix} : X \in M_k(q)\}$$

(where bracketed entries are present only if n is odd). Then G is a product of 152 conjugates of T.

Proof. It follows from [7, 2.1] that $SL_{2k}(q)$ is a product of 38 conjugates of T. And if n is odd, [18, Lemma 2] implies that G is a product of 4 conjugates of $SL_{2k}(q)$. ■

We now embark on the proof of Theorem 2 for G a simple group of Lie type. Let $k \in \mathbb{N}$ and let H be a maximal subgroup of G with $|H| \geq |G|^{1/k}$. By Theorem 1 we may assume that the rank of G is large (in terms of k), so that G is a classical group. Write $G = Cl_n(q)$, a classical group with natural module V of dimension n over $\mathbb{F} = \mathbb{F}_{q^u}$, where $u = 2$ if G is unitary and $u = 1$ otherwise.

By [2], the maximal subgroup H is either in one of the Aschbacher families $\mathcal{C}_i$ $(1 \leq i \leq 8)$ or it lies in the collection $\mathcal{S}$ of almost simple, irreducible subgroups (satisfying various other conditions); see [9] for descriptions of all these families.

In the following statement, we say a quantity is 'bounded' if it is bounded in terms of k.

Lemma 4.3 *The maximal subgroup H is of one of the following types:*

(i) *a parabolic subgroup of G*

(ii) *the stabilizer of a nonsingular subspace of V $(G \neq L_n(q))$*

(iii) *$H \in \mathcal{C}_2$: $Cl_a(q) \wr S_b$ with $ab = n$ and b bounded; or $GL_{n/2}(q^u).2$ $(G \neq L_n(q))$*

(iv) *$H \in \mathcal{C}_3$: $Cl_a(q^b)$ with $ab = n$ and b bounded; or $GU_{n/2}(q).2$ (G orthogonal or symplectic)*

(v) *$H \in \mathcal{C}_4$: $Cl_a(q) \otimes Cl_b(q)$ with $ab = n$ and b bounded*

(vi) *$H \in \mathcal{C}_5$: $Cl_n(q^{1/r})$ with r bounded, or $Sp_n(q), SO_n(q)$ (G unitary)*

(vii) *$H \in \mathcal{C}_8$: $Sp_n(q), SO_n(q), SU_n(q^{1/2})$ $(G = L_n(q))$, or $O_n(q)$ $(G = Sp_n(q)$, q even$)$.*

Proof. This follows from inspection of [9, Chap. 4], noting that subgroups in families $\mathcal{C}_6$ and $\mathcal{C}_7$ do not contain subgroups of order larger than $|G|^{1/k}$, and neither does family $\mathcal{S}$, by [12]. ■

Lemma 4.4 *Assume H is not a subfield subgroup $Cl_n(q^{1/r})$. Then H contains a subgroup $S \cong SL_r(q^u)$ with the following properties:*

(i) *n/r is bounded*

(ii) *there is a Levi subgroup $L \cong SL_s(q^u)$ of G containing S*

(iii) *the embedding of S in L takes the form*

$$\psi : A \to \text{diag}(A, \phi_2(A), \ldots, \phi_t(A), I_l) \quad (A \in SL_r(q^u)),$$

where $s = rt + l$ and the ϕ_i are automorphisms of $SL_r(q^u)$.

Proof. This is clear from Lemma 4.3 when H is not as in 4.3(iv),(v). In case (iv) of 4.3 with H of type $Cl_a(q^b)$, we take a large Levi subgroup of H of the form $SL_r(q^{bu})$, and a subgroup $S = SL_r(q^u)$ of this; then S is embedded in the required fashion in a Levi $L = SL_{br}(q^u)$ of G. Similarly in case (v), we take S to be a large Levi in the factor $Cl_a(q)$ of H. ■

Lemma 4.5 *Assume H is not a subfield subgroup $Cl_n(q^{1/r})$, and let S be as in the previous lemma. Then there is a Levi subgroup $R \cong SL_r(q^u)$ of G, and an element $x \in L$, such that $(SS^x)^3$ contains R.*

Proof. Let S, L be as in the previous lemma, and let $y \in SL_r(q^u)$ be a regular semisimple element. Define $x = \mathrm{diag}(y^{-1}, I_{s-r}) \in L$. Then for $\psi(A) = \mathrm{diag}(A, \phi_2(A), \ldots, \phi_t(A), I_l) \in S$ as in 4.4(iii), we have

$$\psi(A)^{-1}\psi(A)^x = \mathrm{diag}(A^{-1}yAy^{-1}, I_{s-r}).$$

Hence the product SS^x contains all matrices $\mathrm{diag}(y^A y^{-1}, I_{s-r}) \in L$ for $A \in SL_r(q^u)$. These matrices lie in a Levi subgroup $R \cong SL_r(q^u)$ of G. By [23, 2.3], if C is the class y^R then $C^3 = R$, and hence also $(Cy^{-1})^3 = R$. Hence $(SS^x)^3$ contains R. ■

Lemma 4.6 *Assume H is not a subfield subgroup. Then Theorem 2 holds.*

Proof. Let $R \cong SL_r(q^u)$ be as in the previous lemma, and choose a Levi subgroup L of G of type SL, maximal subject to containing R. Then $L \cong SL_m(q^u)$ with $m \geq \frac{1}{2}n - 1$. By Lemma 4.1, L is contained in a product of $b(n/r)^2$ conjugates of R; by 4.5, R is contained in a product of 6 conjugates of H; and by [18, Theorem 1], G is a product of 200 conjugates of L. We conclude that G is a product of $1200b(n/r)^2$ conjugates of H. As H contains $S \cong SL_r(q^u)$, we have $\log|G|/\log|H| \geq b'(n/r)^2$ for some positive constant b', and the conclusion follows. ■

Lemma 4.7 *Theorem 2 holds if H is a subfield subgroup.*

Proof. Assume H is a subfield subgroup $Cl_n(q^{1/r})$. We may choose a Levi subgroup $L \cong SL_{2m}(q^{u/r})$ of H with $2m \geq \frac{1}{2}n - 2$, and a Levi subgroup $L_0 \cong SL_{2m}(q^u)$ of G containing L. Define

$$M = \{\begin{pmatrix} I_m & X \\ 0 & I_m \end{pmatrix} : X \in M_m(q^{u/r})\} \leq L,$$
$$M_0 = \{\begin{pmatrix} I_m & Y \\ 0 & I_m \end{pmatrix} : Y \in M_m(q^u)\} \leq L_0.$$

Write $k = \mathbb{F}_{q^{u/r}}$, $K = \mathbb{F}_{q^u}$. There is a set of $2r$ squares $a_1^2, \ldots, a_{2r}^2$ ($a_i \in K$) which span K over k. Define $\lambda_i = \mathrm{diag}(a_i^{-1}I_m, a_i I_m) \in L$. Then

$$\begin{pmatrix} I_m & X \\ 0 & I_m \end{pmatrix}^{\lambda_i} = \begin{pmatrix} I_m & a_i^2 X \\ 0 & I_m \end{pmatrix},$$

and hence we see that the product $M^{\lambda_1} \dots M^{\lambda_{2r}} = M_0$. By Lemma 4.2, L_0 is a product of 152 (actually the proof gives 38) conjugates of M_0. Finally, G is a product of 200 conjugates of L_0 by [18]. It follows that G is a product of $2r \cdot 38 \cdot 200$ conjugates of H. This completes the proof. ■

The proof of Theorem 2 is now complete.

References

[1] M. Abert, Symmetric groups as products of abelian subgroup, *Bull. London Math. Soc.* **34** (2002), 451–456.

[2] M. Aschbacher, On the maximal subgroups of the finite classical groups, *Invent. Math.* **76** (1984), 469-514.

[3] L. Babai, W.M. Kantor and A. Lubotzky, Small diameter Cayley graphs for finite simple groups, *Europ. J. Comb.* **10** (1989), 507–522.

[4] L. Babai, N. Nikolov and L. Pyber, Expansion and product decompositions of finite groups: variations on a theme of Gowers, in preparation.

[5] R.W. Carter, *Simple groups of Lie type*, Wiley Interscience, 1972.

[6] E.W. Ellers, N. Gordeev and M. Herzog, Covering numbers for Chevalley groups, *Israel J. Math.* **111** (1999), 339–372.

[7] M. Kassabov, Universal lattices and unbounded rank expanders, *Invent. Math.* **170** (2007), 297-326.

[8] M. Kassabov, A. Lubotzky and N. Nikolov, Finite simple groups as expanders, *Proc. Nat. Acad. Sci. USA* **103** (2006), 6116–6119.

[9] 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.

[10] V. Landazuri and G.M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups, *J. Algebra* **32** (1974), 418-443.

[11] R. Lawther and M.W. Liebeck, On the diameter of a Cayley graph of a simple group of Lie type based on a conjugacy class, *J. Comb. Theory Ser. A* **83** (1998), 118–137.

[12] M.W. Liebeck, On the orders of maximal subgroups of the finite classical groups, *Proc. London Math. Soc.* **50** (1985), 426–446.

[13] M.W. Liebeck, H.D. Macpherson and K. Tent, Primitive permutation groups of bounded orbital diameter, *Proc. London Math. Soc.* **100** (2010), 216–248.

[14] M.W. Liebeck, N. Nikolov and A. Shalev, Groups of Lie type as products of SL_2 subgroups, *J. Algebra*, to appear.

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

[16] M.W. Liebeck and G.M. Seitz, On the subgroup structure of exceptional groups of Lie type, *Trans. Amer. Math. Soc.* **350** (1998), 3409–3482.

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

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

[19] N. Nikolov, L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem, *J. Europ. Math. Soc.*, to appear.

[20] M.E. O'Nan, A characterization of $U_3(q)$, *J. Algebra* **22** (1972), 254–296.

[21] C.E. Praeger and J. Saxl, On the orders of primitive permutation groups, *Bull. London Math. Soc.* **12** (1980), 303–307.

[22] G.M. Seitz, Representations and maximal subgroups of finite groups of Lie type, *Geom. Ded.* **25** (1988), 391-406.

[23] A. Shalev, Word maps, conjugacy classes, and a non-commutative Waring-type theorem, *Annals of Math.* **170** (2009), 1383–1416.

[24] M. Suzuki, On a class of doubly transitive groups, *Annals of Math.* **75** (1962), 105–145.