Groups of Lie type as products of SL_2 subgroups

Martin W. Liebeck
Imperial College
London SW7 2BZ, UK
m.liebeck@imperial.ac.uk

Nikolay Nikolov
Imperial College
London SW7 2BZ, UK
n.nikolov@imperial.ac.uk

Aner Shalev
Hebrew University
Jerusalem 91904, Israel
shalev@math.huji.ac.il

Abstract

We prove that apart from the Suzuki groups, every finite simple group of Lie type of rank r over a field of q elements can be written as a product of $C(r)$ subgroups isomorphic to $SL_2(q)$ or $PSL_2(q)$, where $C(r)$ is a quadratic function. This has an application to the theory of expander graphs.

1 Introduction

In this paper we prove that a group $G(q)$ of Lie type of rank r (not a Suzuki group) over a field of q elements is equal to a product of $C(r)$ of its subgroups $SL_2(q)$ or $PSL_2(q)$, where $C(r)$ is a quadratic function of the rank. This adds to the collection of such "width" results for simple groups. For example, in [8, Theorem D] it is shown that $G(q)$ is a product of 25 of its Sylow p-subgroups (where $q = p^a$), later improved to 5 in [2, Theorem 1.16]; in [10] it is shown that every classical group is a product of 200 subgroups of type SL_n for some n (however see Remark 1 below); and in [12] it is proved that for any nontrivial word w we have $w(G)^3 = G$, where G is a sufficiently large simple group and $w(G)$ denotes the set of w-values in G.

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

[0]2000 *Mathematics Subject Classification:* 20G40, 05C25

However our main motivation comes from [6], where the authors announce that all finite simple groups except possibly the Suzuki groups ${}^2B_2(q)$ can be made into expanders uniformly. Let us explain this in a little more detail. A collection $\mathcal{F} = \{G_i\}_{i=1}^{\infty}$ of finite groups is said to be a uniform family of expanders if there is some $k \in \mathbb{N}$, and a set of k generators S_i for each G_i, such that the Cayley graphs $\mathrm{Cay}(G_i, S_i)$ form a sequence of e-expanders for some fixed constant $e > 0$. Here, a graph X is defined to be an e-expander if, for every subset A of vertices with $|A| \leq \frac{1}{2}|X|$, we have $|\delta A| \geq e|A|$, where δA is the set of vertices at distance 1 from A; see [6] for more details. One of the key arguments in [6] is based on the following observation. Suppose $\mathcal{F}$ is a collection of groups which is a uniform expander family. Let $\mathcal{L}$ be another collection of groups and assume that there is an integer d such that every group $G \in \mathcal{L}$ has a product decomposition $G = H_1 \cdots H_d$ with each $H_i \in \mathcal{F}$. Then $\mathcal{L}$ is also a family of uniform expanders. Now one of the major results in [6] is that the groups $\mathcal{S} = \{SL_2(q) \mid q \text{ prime power}\}$ are uniform expanders. Hence, to prove the same for families of groups of Lie type of bounded rank r, it is sufficient to prove that these can be expressed as products of bounded numbers of subgroups of type SL_2. An argument for this based on model theory was outlined in [6], and has recently been completed in [9]; but this does not give explicit bounds on the number $C(r)$ of subgroups SL_2 required.

In this paper we give a short proof of this result using group theoretic arguments, which moreover produce explicit and close to best possible bounds for the function $C(r)$. This also has the advantage of giving explicit lower bounds for the expansion constants for families of groups of Lie type of bounded rank, since in the above discussion a lower bound for the expansion constant for the family $\mathcal{L}$ can be explicitly calculated in terms of k,d and the expansion constant for the family $\mathcal{F}$.

We note that, while our arguments are group theoretic, they rely in some cases on character methods and on a recent result of Gowers [5, 3.3] developed and applied further by Babai, Pyber and Nikolov [2] – see Theorem 2.4 below.

Here is our result.

Theorem 1.1. *Let $G = G(q)$ be a simple group of Lie type over $\mathbb{F}_q$, not a Suzuki group ${}^2B_2(q)$. Then G is equal to a product of N subgroups $(P)SL_2(q)$, where N is as in Table 1, a quadratic function of the rank of G.*

In the first line of the table, $|\Phi^+|$ denotes the number of positive roots in the root system of G; a list of these numbers can be found in [3, p.43].

Table 1:

$G(q)$	N
untwisted	$5\|\Phi^+\|$
${}^2A_{2m+1}(q)$	$5(m+1)(4m+1)$
${}^2A_{2m}(q)$, $m>1$	$5m(4m+7)$, $q>2$
	$30m(4m-3)$, $q=2, m>2$
${}^2A_2(q)$, $q>2$	55
${}^2D_n(q)$, $n\geq 4$	$5(n-1)(n+2)$
${}^3D_4(q)$	105
${}^2E_6(q)$	300
${}^2G_2(q)$, $q\geq 3^7$	6
${}^2F_4(q)$, $q\geq 2^7$	900

Remarks 1. In fact the result of [10] mentioned in the first paragraph is not proved there for $G = SU_3(q)$, so our result for this group (proved in Proposition 2.3 below) completes the proof in [10].

2. Since $|G(q)|$ is a polynomial in q of degree $f(r)$, a quadratic in r, our bounds are best possible, apart from reducing the constants involved.

2. A few groups $G(q)$ are omitted from the table, namely $U_5(2)$, ${}^2G_2(q)$ ($q = 3^3, 3^5$) and ${}^2F_4(q)'$ ($q = 2, 2^3, 2^5$). For these groups our proof gives upper bounds 350, 8 and 6060 for N, respectively.

3. Our proof produces subgroups which are in fact all isomorphic to $SL_2(q)$ except when $G = {}^2G_2(q)$ or $PSL_2(q)$. When G is of untwisted type they are all conjugate, but this is not the case for G twisted.

2 Ree groups and SU_3

The most difficult cases of Theorem 1.1 are those in which G is a Ree group ${}^2G_2(q)$ or ${}^2F_4(q)$, or $U_3(q)$. We handle these in this section.

Proposition 2.1. *Let $q = 3^{2n+1}$ with $n\geq 3$. The simple Ree group ${}^2G_2(q)$ is a product of 6 conjugates of a subgroup $H\cong PSL_2(q)$. If $q = 3^3$ or 3^5 then G is a product of 8 conjugates of H.*

Proposition 2.2. *Let $q = 2^{2n+1}$, $n\geq 3$ and $G = {}^2F_4(q)$ be the simple Ree group of type ${}^2F_4$. Then G is a product of 900 conjugates of a subgroup $H\cong SL_2(q)$.*

Proposition 2.3. *For $q > 2$, the group $SU_3(q)$ is a product of* 55 *conjugates of a subgroup $H \cong SL_2(q)$.*

Note that this proposition is false for $q = 2$ as $U_3(2) = 3^2 Q_8$.

The following very recent result, relating product decompositions with group representations, plays a major role in our proofs.

Theorem 2.4 ([2])**.** *Let $n > 2$ be an integer and let G be a finite group with a minimal nontrivial representation of degree k. Suppose that $A_i \subseteq G$, $i = 1, 2, \dots, n$ are such that $|A_i|/|G| \geq k^{-(n-2)/n}$. Then $G = A_1 \cdot A_2 \cdots A_n$.*

Proof of Proposition 2.1

Let $G = {}^2G_2(q)$, $q = 3^{2n+1} \geq 27$. For basic properties of G we refer to [14]. If t is an involution in G, then $C_G(t) = \langle t \rangle \times H$ where $H \cong PSL_2(q)$. Also, there is a conjugate u of t such that tu has order $q + \sqrt{3q} + 1$ and $C_G(tu) = \langle tu \rangle$. Hence $C_G(t) \cap C_G(u) = 1$, showing that there are two conjugates S, T of H in G such that $S \cap T = \{1\}$.

Hence $|ST| = |S||T| = q^2(q^2-1)^2/4$ while $|G| = q^3(q^2-1)(q^2-q+1)$. By [14] the minimal degree of a nontrivial complex representation of G is $k = q^2 - q + 1$. We see that if $q \geq 3^7$ then

$$\frac{|ST|}{|G|} = \frac{(q^2-1)}{4q(q^2-q+1)} > \frac{1}{k^{3/5}}.$$

Therefore by Theorem 2.4 with $n = 5$ we have $G = (ST)(TS)(ST)(TS)(ST) = STSTST$. If $q = 3^3$ or 3^5 an easy computation shows that then $|ST|/|G| > k^{-5/7}$ and similarly we get $G = (ST)^4$. Proposition 2.1 is proved. $\square$

Proof of Proposition 2.2

Let $G = {}^2F_4(q)$. The root groups and commutator relations in G are described in [4, 2.4.5(d)]. We follow the notation in [4, 2.4.5]. The root system has 16 roots, and correspondingly G has 16 root subgroups $X_1, \dots, X_{16}$. For even index i the group $X_i = \{x_i(t) \mid t \in \mathbb{F}_q\}$ is one-parameter, and together with its opposite X_{i+8} generates a copy of $SL_2(q)$. Let H be one of these, say $H = \langle X_8, X_{16} \rangle$. On the other hand if i is odd then $\langle X_i, X_{i+8} \rangle \cong {}^2B_2(q)$ and X_i is two-parameter. Its centre is a one-parameter subgroup denoted $Y_i = \{y_i(t) \mid t \in \mathbb{F}_q\}$.

By [4, 2.4.5(d)(2)], for i odd we have $[x_i(1), x_{i+3}(t)] = y_{i+2}(t)$. This shows that each Y_i is in the product of two conjugates of H.

Lemma 2.5. *Let S be a subgroup ${}^2B_2(q)$ of G as above, and let P and Q be the centres of its two opposite root subgroups. Then $|PQPQ| > (q-1)^4$ and $S = (PQ)^{11}$.*

Proof: We use the 4-dimensional representation of S as a subgroup of $Sp_4(q)$, conveniently described in [3, p.246]. Denote by θ the map $t \to t^{2^n}$ on $\mathbb{F}_q$. If P is parametrized by $y(t)$ and Q by $z(u)$ for parameters $t, u \in \mathbb{F}_q$, then

$$y(t) = \begin{pmatrix} 1 & 0 & t^{2\theta} & t \\ 0 & 1 & t & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad z(u) = y(u)^T.$$

Now for $t, u, a, b \in \mathbb{F}_q^*$ $(= \mathbb{F}_q \backslash \{0\}$, define a map $f : (\mathbb{F}_q^*)^{(4)} \to Sp_4(q)$ as follows:

$$f(t,u,a,b) := y(t)z(u)y(a)z(b) = \begin{pmatrix} * & * & * & * \\ & * & * & tu^{2\theta}a \\ & * & * & u^{2\theta}a \\ & ua^{2\theta}b & ua^{2\theta} & ua+1 \end{pmatrix}$$

where $*$ denote entries we are not interested in.

We claim that f is injective. Indeed, suppose $f(t,u,a,b) = f(t_0,u_0,a_0,b_0)$. Then $tu^{2\theta}a = t_0u_0^{2\theta}a_0$ and $u^{2\theta}a = u_0^{2\theta}a_0$, whence $t = t_0$, and similarly $b = b_0$. The equations $u^{2\theta}a = u_0^{2\theta}a_0$ and $ua = u_0a_0$ imply that $u^{2\theta-1} = u_0^{2\theta-1}$, hence $u = u_0$ and also $a = a_0$. So f is injective as claimed.

Adding the identity to the image of f we conclude that $|PQPQ| > (q-1)^4$. Similarly we get $|QPQP| > (q-1)^4$

Now $|S| = q^2(q-1)(q^2+1)$ and the minimal degree of a nontrivial character of S is at least $k = \sqrt{q/2}(q-1)$, by [7]. So we see that when $q \geq 2^7$

$$\frac{|PQPQ|}{|S|} > \frac{(q-1)^3}{q^2(q^2+1)} \geq k^{-5/7}.$$

By Theorem 2.4 again, this time with $n = 7$, we see that

$$S = ((PQPQ)(QPQP))^3(PQPQ) = (PQ)^{11}.$$

Lemma 2.5 is proved. □

Lemma 2.5 and the discussion before it show that each subgroup of type ${}^2B_2$ in G is contained in a product of $2 \times 22 = 44$ conjugates of H.

The positive maximal unipotent subgroup U of G is a product $X_1X_2\cdots X_8$ of eight root subgroups, half of them of type A_1 and the rest of type ${}^2B_2$. Therefore U is contained in a product of $4+4\times 44 = 180$ conjugates of the subgroup H. The same is true for the negative unipotent subgroup $V = X_9\cdots X_{16}$. Now by [2, Theorem 1.16] we have $G = UVUVU$. This shows that G is product of $5\times 180 = 900$ conjugates of H and Proposition 2.2 is proved. $\square$

Note that when $q = 2^3$ or 2^5 we need to take $n = 50$ when applying 2.4 as above at the end of the proof of 2.5, and this leads to the bound in Remark 2 after the statement of Theorem 1.1.

Proof of Proposition 2.3

It is most convenient to work with matrices for this proof. Let $G = SU_3(q)$ with $q = p^n$ (p prime, $q > 2$), and let G preserve a non-degenerate hermitean form $(\,,\,)$ on $V = V_3(q^2)$. Choose a basis e, d, f of V such that e, f are singular vectors orthogonal to d, and $(d,d) = (e,f) = 1$. Then relative to this basis, there is a Sylow p-subgroup U of G consisting of the matrices

$$u(\alpha,\beta) = \begin{pmatrix} 1 & \alpha & \beta \\ & 1 & -\bar{\alpha} \\ & & 1 \end{pmatrix}$$

where $\alpha,\beta \in \mathbb{F}_{q^2}$, $\bar{\alpha} = \alpha^q$ and $\beta+\bar{\beta}+\alpha\bar{\alpha} = 0$. Write H for the stabilizer G_d, so that $H \cong SU_2(q) \cong SL_2(q)$ and the elements $u(0,\beta)$ in U form a Sylow p-subgroup U_0 of H. Write $u = u(0,1)$.

Observe that H has a subgroup T consisting of diagonal matrices $h(t) = \mathrm{diag}(t^{-1},1,t)$ for $t \in \mathbb{F}_q^*$, and

$$u(\alpha,\beta)^{h(t)} = u(t\alpha, t^2\beta).$$

The next lemma follows from a more general result in [11, 3.5.2], but we include a proof for completeness.

Lemma 2.6. *For any $\alpha \in \mathbb{F}_{q^2}^*$, there exist four G-conjugates of $u = u(0,1)$ having product equal to $u(\alpha,\beta)$ for some β.*

Proof: This is proved by a calculation using the character table of G, which can be found in [13]. We are grateful to Claude Marion for his assistance with this calculation.

It is well known (see for example [1, p.43]) that if C_i $(1 \leq i \leq d)$ are conjugacy classes of a finite group G and $g_i \in C_i$, then for $g \in G$, the number of solutions to the equation $x_1 \cdots x_d = g$ with $x_i \in C_i$ is equal to $a_{C_1,\dots,C_d,g}|C_1|\cdots|C_d|/|G|$, where

$$a_{C_1,\dots,C_d,g} = \sum_{\chi \in Irr(G)} \frac{\chi(g_1)\cdots\chi(g_d)\chi(g^{-1})}{\chi(1)^{d-1}}.$$

taking $G = SU_3(q)$ and $C = u^G$ we calculate that

$$a_{C,C,C,C,u(\alpha,\beta)} > 0$$

and this implies the result. (Note that $a_{C,C,C,u(\alpha,\beta)} = 0$, so four is the minimal number of conjugates needed in the lemma.) $\square$

We can now prove Proposition 2.3. Let α_1, α_2 be a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. By Lemma 2.6, we can write

$$u(\alpha_1, \beta_1) = u^{g_1} \cdots u^{g_4}, \;\; u(\alpha_2, \beta_2) = u^{g_5} \cdots u^{g_8}$$

for some β_1, β_2 and some $g_i \in G$. For any $\alpha \in \mathbb{F}_{q^2}$, let $\alpha = t_1\alpha_1 + t_2\alpha_2$ with $t_i \in \mathbb{F}_q$. Without loss of generality assume that each $t_i \neq 0$ (otherwise omit the factor $u(a_i, b_i)^{h(t_i)}$ below), so that

$$u(\alpha_1, \beta_1)^{h(t_1)} u(\alpha_2, \beta_2)^{h(t_2)} = u(\alpha, \beta)$$

for some β. Hence

$$\begin{aligned} U \;\; &\subseteq TU_0^{g_1} \cdots U_0^{g_4} T U_0^{g_5} \cdots U_0^{g_8} T U_0 \\ &\subseteq H H^{g_1} \cdots H^{g_4} H H^{g_5} \cdots H^{g_8} H, \end{aligned} \tag{1}$$

a product of 11 conjugates of H. Again using [2, 1.16], it follows that G is a product of 55 conjugates of H, proving Proposition 2.3. $\square$

3 Proof of Theorem 1.1

In this section we complete the proof of Theorem 1.1. This is for the most part straightforward, given the previous section.

Lemma 3.1. *Theorem* 1.1 *holds for* $G = G(q)$ *of untwisted type.*

Proof: The assertion is trivial for $PSL_2(q)$, so assume that $G \neq PSL_2(q)$. Let Φ be the root system of G, and for $\alpha \in \Phi$ let X_α be the corresponding root subgroup of G. Then $\langle X_\alpha, X_{-\alpha}\rangle \cong SL_2(q)$ and G has maximal unipotent subgroups $U = \prod_{\alpha\in\Phi^+} X_\alpha$ and $V = \prod_{\alpha\in\Phi^-} X_\alpha$ (see [3, Chapters 5,6]). Hence U is contained in a product of $|\Phi^+|$ copies of $SL_2(q)$, and the same holds for V. By [2, 1.16] we have $G = UVUVU$, so G is equal to a product of $5|\Phi^+|$ copies of $SL_2(q)$, as required. $\square$

The twisted groups require a little more effort, using the following result.

Proposition 3.2. *Let $d \geq 1$, $q = p^a$, $G = SL_2(q^d)$ and let G_0 be a subgroup $SL_2(q)$ of G. If U, U_0 are Sylow p-subgroups of G, G_0 respectively, then U is a product of $2d$ G-conjugates of U_0.*

Proof: Take $U = \{u(\alpha) : \alpha \in \mathbb{F}_{q^d}\}$ and $U_0 = \{u(\alpha) : \alpha \in \mathbb{F}_q\}$, 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 $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$. 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 $\mathbb{F}_{q^d}$ over $\mathbb{F}_q$, where $\alpha_i \in \mathbb{F}_q$. Hence $U = U_0^{h(\alpha_1)} \cdots U_0^{h(\alpha_{2d})}$, completing the proof. $\square$

Now we embark on the proof of Theorem 1.1 for $G = G(q)$ a twisted group. Types ${}^2G_2$, ${}^2F_4$ and ${}^2A_2$ were handled in the previous section.

The strategy is similar for all cases. We refer to [3, Chapter 13] for a description of the root subgroups of G. These are denoted by X_S^1 in [3, 13.5.1]. Here S is an equivalence class in Φ (the root system of the untwisted group corresponding to G) under the action of the graph automorphism; S has type A_1, A_1^2, A_1^3 or A_2, and X_S^1 is a Sylow p-subgroup of $SL_2(q)$, $SL_2(q^2)$, $SL_2(q^3)$ or $SU_3(q)$ respectively ([3, 13.6.3]). Moreover $U^1 = \prod X_S^1$ is a Sylow p-subgroup of G, where the product is over equivalence classes S in Φ^+, and there is an opposite Sylow subgroup V^1 which is the product over classes S in Φ^-. By [2, 1.16] we have $G = U^1V^1U^1V^1U^1$.

First consider $G = {}^2A_{2m+1}(q)$. Here there are $m+1$ classes S of type A_1 and $m(m+1)$ of type A_1^2 (and none of the other types). Hence from the above, we see that U^1 is contained in a product of $m+1$ copies of $SL_2(q)$ and

$m(m+1)$ of $SL_2(q^2)$. It follows using Proposition 3.2 that U^1 is contained in a product of $m+1+4m(m+1)$ copies of $SL_2(q)$, and similarly for V^1. The factorization $G = U^1V^1U^1V^1U^1$ now gives the conclusion in this case.

Next consider $G = {}^2A_{2m}(q)$ with $m > 1$. Assume first that $q > 2$. In this case there are m classes S of type A_2 and $m(m-1)$ of type A_1^2. Hence U^1 is contained in a product of m copies of $SU_3(q)$ and $m(m-1)$ of $SL_2(q^2)$. By (1) in the proof of 2.3, for each S of type A_2, the root group X_S^1 is contained in a product of 11 copies of a subgroup $SL_2(q)$ of the corresponding group $SU_3(q)$. Hence using 3.2, we see that U_1 is contained in a product of K copies of $SL_2(q)$, where

$$K = 11m + 4m(m-1) = 4m^2 + 7m,$$

and the conclusion follows in the usual way.

For $q = 2$ the above argument does not apply, so we use a different method. Let $G = {}^2A_{2m}(2) = SU_{2m+1}(2)$ with $m > 2$. Pick two nonsingular vectors v_1, v_2 with $(v_1, v_2) = 0$, and let $H_i = G_{v_i}$ $(i = 1, 2)$. Then $H_i \cong SU_{2m}(2)$ and $H_1 \cap H_2 \cong SU_{2m-1}(2)$. Hence

$$|H_1H_2| = \frac{|SU_{2m}(2)|^2}{|SU_{2m-1}(2)|}.$$

The minimal nontrivial character degree of G is at least $k = 2(2^{2m}-1)/3$ by [7], and we check that $|G|/|H_1H_2| < k^{3/5}$ (this uses the assumption that $m > 2$ – when $m = 2$ we need to replace $3/5$ here with $2/3$, leading to the bound given in Remark 2 after 1.1). Hence Theorem 2.4 applies with $n = 5$ to give

$$G = (H_1H_2)(H_2H_1)(H_1H_2)(H_2H_1)(H_1H_2) = H_1H_2H_1H_2H_1H_2,$$

a product of 6 copies of $SU_{2m}(2)$. By the result already proved for this case, $SU_{2m}(2)$ is a product of $5m(4m-3)$ copies of $SL_2(2)$, and the conclusion follows.

Now consider $G = {}^2D_n(q)$, $n \geq 4$. Here there are $(n-1)(n-2)$ classes S of type A_1 and $n-1$ of type A_1^2. Hence U^1 is contained in a product of $(n-1)(n-2)+4(n-1)$ copies of $SL_2(q)$ and the result follows in the usual way.

For $G = {}^3D_4(q)$ there are 3 classes S of type A_1 and 3 of type A_1^3; and for $G = {}^2E_6(q)$ there are 12 classes of type A_1 and 12 of type A_1^2. The result follows as before.

This completes the proof of Theorem 1.1.

References

[1] Z. Arad and M. Herzog (eds.), *Products of Conjugacy Classes in Groups*, Springer Lecture Notes **1112**, Springer-Verlag, Berlin, 1985.

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

[3] R. Carter, *Simple groups of Lie type*, Wiley, 1972.

[4] D. Gorenstein, R. Lyons and R. Solomon, *The classification of finite simple groups*, Mathematical Surveys and Monographs, Vol. 40.3, American Mathematical Society, Providence, RI, 1998.

[5] W. T. Gowers, Quasirandom groups, preprint, http://arxiv.org/abs/0710.3877.

[6] M. Kassabov, A. Lubotzky, N. Nikolov, Finite simple groups as expanders, *Proc. Natl. Acad. Sci USA* **103** (2006), 6116 - 6119.

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

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

[9] A. Lubotzky, Simple groups of Lie type as expanders, *in preparation.*

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

[11] D.M. Rodgers, Covering and generating number for groups, PhD thesis, University of Cambridge, 2001.

[12] A. Shalev, Word maps, conjugacy classes and a non-commutative Waring-type theorem, *Annals of Math.*, to appear.

[13] W.A. Simpson and J.S. Frame, The character tables for SL(3, q), SU(3, q^2), PSL(3, q), PSU(3, q^2), *Canad. J. Math.* **25** (1973), 486–494.

[14] H.N. Ward, On Ree's series of simple groups, *Trans. Amer. Math. Soc.* **121** (1966), 62–89.