Séminaire BOURBAKI Mars 2013
65ème année, 2012-2013, n$^{\text{o}}$ 1069

# THE PROOF OF ORE'S CONJECTURE
## [after Ellers–Gordeev and Liebeck–O'Brien–Shalev–Tiep]

by **Gunter MALLE**

## INTRODUCTION

The *commutator* $[g,h] := g^{-1}h^{-1}gh$ of two elements $g,h$ of a group $G$ is introduced in every first course in group theory, as well as the *commutator subgroup*

$$[G,G] := \langle [g,h] \mid g,h \in G \rangle,$$

generated by all commutators in $G$, and usually it is stated that not all elements of $[G,G]$ need to be commutators. The first such example of finite order may have been given by Fite [Fi02]. The smallest example of a finite group $G$ for which $[G,G]$ contains non-commutators has order 96; in fact there are two non-isomorphic groups of that order in which the set of commutators does not equal the commutator subgroup, see Guralnick [Gu80].

In a 1951 paper, Oystein Ore [Ore] shows that every even element in a symmetric group of degree at least 3 is a commutator and claims that the proof can be extended to show that every element in a simple alternating group $\mathfrak{A}_n$ is a commutator. He concludes by saying that *"It is possible that a similar theorem holds for any simple group of finite order, but it seems that at present we do not have the necessary methods to investigate the question."* This has become known as *Ore's conjecture*, the recent solution of which [LOST] is the topic of this lecture:

THEOREM 0.1 (Liebeck–O'Brien–Shalev–Tiep). — *Let $G$ be a finite non-abelian simple group. Then every element of $G$ is a commutator.*

In fact, at almost the same time as Ore, Noboru Ito [Ito51] showed the same statement for the alternating groups $\mathfrak{A}_n$, but without speculating about other finite simple groups.

The proof of Ore's conjecture relies on the classification of the finite simple groups and, through Lusztig's parametrization of irreducible characters of finite reductive groups, on the Weil conjectures; the final step also required a considerable amount of computer calculation.

Note that obvious generalizations of Theorem 0.1 fail to hold. For example Guralnick [Gu10] gives a quite general construction of groups, including non-solvable ones, with the property that $[G,G]$ does not consist of commutators only: let $G = U \wr H$ be the regular wreath product of two finite groups $U, H$ with $U$ abelian. If $|U| > 2$ or $|[H,H]| > 2$

then some element of $[H, G]$ is not a commutator in $G$ (see also Isaacs [Is77] for a weaker result). Thus, for $U$ of order at least 3 and any non-abelian simple group $H$ this gives a non-solvable example $G$ with factor group $H$, and in fact one may also obtain a *perfect* one (that is, a group $G$ with $G = [G, G]$). Computer calculations show that the smallest example of a perfect group not all of whose elements are commutators is an extension of an elementary abelian group of order $2^4$ with the alternating group $\mathfrak{A}_5$. Even closer to the case of simple groups, H. I. Blau [Bl94] proved that there exist (finitely many) quasisimple groups that contain non-commutator central elements (see Theorem 6.1 below). Recall that a group $G$ is called *quasisimple* if it is perfect and the quotient $G/Z(G)$ by its center $Z(G)$ is (non-abelian) simple. The smallest such example is the exceptional 6-fold covering group of the alternating group $\mathfrak{A}_6$ (that is, a non-split central extension of the cyclic group of order 6 by $\mathfrak{A}_6$), for which the central elements of order 6 can be seen not to be commutators. So the property required by Ore's conjecture seems to be closely tied to simple groups.

We want to mention another open problem closely related to Ore's conjecture, which is concerned with the square $C^2 := \{xy \mid x, y \in C\}$ of a conjugacy class $C$, and which in the introduction to the book [AH85] is attributed to J. G. Thompson:

Conjecture 0.2 (J. G. Thompson). — *Let $G$ be a finite non-abelian simple group. Then there exists a conjugacy class $C \subseteq G$ such that $C^2 = G$.*

Clearly, if $C^2 = G$ then every element in the product $C^2$ is a commutator, so the Thompson conjecture implies the (now proven) Ore conjecture. Many papers on the Ore conjecture actually show that the stronger Thompson conjecture holds for particular families of groups, so in this survey we will consider both conjectures simultaneously.

In a broader context, the Ore conjecture can be thought of as a particular instance of the surjectivity of word maps. For any word $w$ in a free group $F_r$ on $r$ generators, and any group $G$, one can ask whether the corresponding word map is surjective, the Ore conjecture being the special case of the commutator word. This gives (non-commutative) analogues of diophantine equations on groups. For example, the representability of a group element by a product of $k$th powers, or by the $k$th power of a given word, can be considered to be analogues of Waring's problem in number theory. This point of view has been propagated by Shalev (see e.g. [Sh09, LS09, LST11]).

One attractive feature of these questions, which we will insist on throughout this survey, is the fact that they also make sense for simple algebraic groups, where more powerful methods are available and much more can be shown to hold.

Let us end this introduction with a short historical overview on the proof of Ore's conjecture. After Ore and Ito proved the conjecture for the simple alternating groups, R.C. Thompson [Th61, Th62, Th62a] established it for the finite projective special linear groups $\mathrm{PSL}_n(q) = \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q))$. The symplectic groups $\mathrm{Sp}_{2n}(q)$ with $q \equiv 1 \pmod 4$ were handled by Gow [Gow88], and Bonten [Bo93] dealt with exceptional

groups of Lie type of low rank. The case of sporadic groups was settled by Neubüser, Pahlings and Cleuvers [NPC84].

In 1998, E.W. Ellers and N.L. Gordeev [EG98] verified Ore's conjecture (and in fact Thompson's conjecture) for all finite simple groups of Lie type over a finite field $\mathbb{F}_q$, whenever $q \geq 9$. This will be explained in Section 1. Building on this result, Shalev [Sh09] then used asymptotic methods to show that for finite simple groups $G$, the proportion of commutators tends to 1 as $|G|$ tends to infinity. In that same paper he also showed that for any word $w \neq 1$, there exists $N = N(w)$ such that for every finite simple group $G$ of order $|G| > N(w)$ we have $w(G)^3 = G$. The exponent 3 was later improved to 2 by Larsen, Shalev and Tiep [LST11]. We will discuss these methods and results in Sections 4 and 5. The remaining (infinitely many) simple groups of Lie type over small fields were then treated in the paper of Liebeck, O'Brien, Shalev and Tiep [LOST]. We sketch their approach in Section 2.

## 1. THE APPROACH BY ELLERS AND GORDEEV

Ellers and Gordeev [EG98] succeeded in proving Ore's conjecture for the finite simple groups of Lie type defined over fields of order at least 9. Since there are infinitely many distinct classical groups over any given finite field, this still leaves infinitely many open cases. The approach of Ellers–Gordeev is by direct computation. To get some idea on the method, one should consider the following model case for algebraic groups. This was proved by Pasiencier–Wang [PW62] over the complex numbers (with a precursor result by Goto [Go49] for compact semisimple Lie groups), and then Ree [Ree64] noticed that their argument can be extended to arbitrary algebraically closed fields:

THEOREM 1.1 (Pasiencier–Wang, Ree). — *Let $G$ be a semisimple linear algebraic group over an algebraically closed field. Then each element of $G$ is a commutator.*

*Proof* (Sketch) — We want to show that $g \in G$ is a commutator. First note that a conjugate of a commutator is again a commutator, so we may replace $g$ by any of its conjugates. By a result of Borel, any element of $G$ lies in some Borel subgroup $B$ of $G$, so we may assume that $g \in B$. Let $U = R_u(B)$ be the unipotent radical of $B$, and $T \leq B$ a maximal torus. One now needs the following auxiliary claim, whose proof relies on a result of Kostant on the action of the Weyl group on the character group of $T$, see [Ree64, (3.1)]:

(∗) For any $s \in T$ there exists a regular element $t \in T$ (that is, with $C_G(t) = T$) and $x \in N_G(T)$ such that $x^{-1}tx = ts$.

Now let $g = su$ be the Jordan decomposition of $g$, where we may assume that $s \in T$, since all maximal tori of $B$ are conjugate. By (∗) there exists a regular element $t \in T$

and $x \in N_G(T)$ with $x^{-1}tx = ts$. By Lemma 1.2 below applied to the regular element $ts \in T$ there is $b \in B$ with $b^{-1}tsb = tsu$, so that finally

$$g = su = t^{-1}b^{-1}tsb = t^{-1}b^{-1}x^{-1}txb = [t, xb]$$

is a commutator. □

LEMMA 1.2. — *Let $B = U \cdot T$ be a semidirect product of a nilpotent normal subgroup $U$ with an abelian group $T$. Then for $t \in T$ with $C_B(t) = T$ the coset $tU$ is a single $B$-conjugacy class.*

*Proof* — By induction over a central series of $U$ one easily shows that the map $U \to U$, $u \mapsto [t, u]$, is bijective, so any $tv \in tU$ has the form $t^u$ for some $u \in U$. □

An attempt to adapt this approach to finite groups of Lie type faces several problems. First, it is no longer true that all elements lie in a Borel subgroup. So one has to consider a larger collection of subgroups. Secondly, regular semisimple elements exist in the Borel subgroup only if the underlying field is sufficiently large compared to the rank. This is the principal reason why the Ellers–Gordeev method cannot handle all simple groups of Lie type.

In a series of three papers Ellers–Gordeev show a particular form of Gauss decomposition for elements of finite reductive groups. Recall that any finite simple group of Lie type $G$ can be obtained by the following construction. (This does not apply to the Tits simple group ${}^2F_4(2)'$, which for most purposes should rather be considered as a 27th sporadic simple group.) There exist a simple linear algebraic group $\mathbf{H}$ of simply connected type over the algebraic closure of a finite field, and a Steinberg endomorphism $F : \mathbf{H} \to \mathbf{H}$, that is, a bijective morphism with finite fixed point set $H := \mathbf{H}^F$, such that $G = H/Z(H)$. Elements of $G$ will be called regular if their preimages in the algebraic group $\mathbf{H}$ are. If $\mathbf{T} \leq \mathbf{B} \leq \mathbf{H}$ is an $F$-stable maximal torus inside an $F$-stable Borel subgroup of $\mathbf{H}$, then the image in $G$ of $\mathbf{T}^F$, respectively of $\mathbf{B}^F$, is called a maximally split torus, respectively a Borel subgroup of $G$. The group of $F$-fixed points of the unipotent radical $R_u(\mathbf{B})$ is then called the unipotent radical of $\mathbf{B}^F$. Ellers–Gordeev [EG94, EG95, EG96] obtain the following statement on Gauss decompositions of elements:

THEOREM 1.3 (Ellers–Gordeev). — *Let $G$ be a finite simple group of Lie type, $T \leq B \leq G$ a maximally split torus inside a Borel subgroup of $G$, $U$ the unipotent radical of $B$ and $U^-$ the unipotent radical of the opposite Borel subgroup. Fix $t \in T$. Then for any $1 \neq g \in G$ there exists $x \in G$ such that*

$$xgx^{-1} = u_1tu_2 \quad \text{for suitable } u_1 \in U^-,\ u_2 \in U.$$

For the special linear groups this was first shown by Sourour [So86]. In fact, Ellers–Gordeev prove the statement for Chevalley groups over any field $K$. Their proof takes roughly 50 pages of explicit calculation in the various families of groups of Lie type.

COROLLARY 1.4. — *In the situation of Theorem 1.3, suppose that $t_1, t_2 \in T$ are regular elements, and write $C_1, C_2$ for their conjugacy classes. Then $C_1C_2 \cup \{1\} = G$.*

*Proof* — Let $1 \neq g \in G$, then by Theorem 1.3 some conjugate $xgx^{-1}$ of $g$ has the form $u_1t_1t_2u_2$ with $u_1 \in U^-$, $u_2 \in U$. Now by Lemma 1.2 applied to the semidirect products $B = UT$ and $U^-T$ we can write $u_1t_1 = v_1t_1v_1^{-1}$, and $t_2u_2 = v_2t_2v_2^{-1}$ for suitable $v_1 \in U^-, v_2 \in U$, whence

$$xgx^{-1} = u_1t_1t_2u_2 = v_1t_1v_1^{-1}\, v_2t_2v_2^{-1} \in C_1C_2,$$

as claimed. □

COROLLARY 1.5. — *In the situation of Theorem 1.3, assume that $T$ contains a regular element. Then the Ore conjecture holds for $G$.*

*Proof* — Let $t \in T$ be regular and let $C_1, C_2$ in the previous corollary be the class of $t$, $t^{-1}$ respectively. Then any element of $G \setminus \{1\}$ is a commutator, and $1 \in G$ trivially is. □

Now note that, given $\mathbf{H}$, $F : \mathbf{H} \to \mathbf{H}$, and a maximally split maximal torus $\mathbf{T} \leq \mathbf{H}$ as above, any regular semisimple element $s \in \mathbf{T}$ is $F^m$-stable for $m$ sufficiently large. Thus there exist regular semisimple elements in $T$ over fields of sufficiently large order. But this field size might vary with the characteristic and with the type of $G$. So more elaborate arguments are needed to establish a uniform, explicit bound:

THEOREM 1.6 (Ellers–Gordeev [EG98]). — *Let $G$ be a finite simple group of Lie type over a field of order at least 9. Then Thompson's and Ore's conjectures hold for $G$.*

In fact, for most families of groups they obtain an even smaller bound on the field size; for example, they show that Ore's conjecture holds for symplectic groups over fields of order at least 4. Note that this still leaves infinitely many open cases, namely the classical groups of unbounded rank.

In their proof, Ellers–Gordeev use the following factorization result by Lev [Lev94], which is shown by direct computation (a similar, but weaker decomposition statement had been shown by Sourour [So86] in his proof of Thompson's conjecture for $\mathrm{SL}_n(K)$):

THEOREM 1.7 (Lev). — *Let $K$ be a field, $|K| \geq 4$, and $a_1, a_2 \in \mathrm{GL}_n(K)$ with $n \geq 3$ such that all eigenvalues of $a_1, a_2$ lie in $K$. Then any non-scalar matrix $g \in \mathrm{GL}_n(K)$ with $\det a_1 \cdot \det a_2 = \det g$ can be factorized as $g = b_1b_2$ with $b_i$ conjugate to $a_i$, for $i = 1, 2$.*

Taking $a_1 = a_2$ a regular unipotent element, this implies that all non-central elements of $\mathrm{SL}_n(K)$ with $|K| \geq 4$ lie in $C^2$, where $C$ is a class of regular unipotent elements, showing Thompson's and thus Ore's conjecture for $\mathrm{SL}_n(q)$, $q \geq 4$, whence for the simple factor groups $\mathrm{PSL}_n(q)$. To treat the other simple groups of Lie type $G$, Ellers–Gordeev consider the following situation: Assume that $G$ has root system $\Phi$ with respect to a maximal torus $T$, $G_1$ is a reductive subgroup of $G$ with root system $\Phi_1 \subset \Phi$, and $U$ is

the unipotent subgroup of $G$ generated by the root subgroups for roots $\alpha \in \Phi^+ \setminus \Phi_1$. Then one has the following inductive statement (see [EG98, Prop. 5.1]):

PROPOSITION 1.8. — *Let $C \subset G$ be a real conjugacy class. Let $g \in TG_1 \cap C$ and denote by $C_1$ the union of the $TG_1$-conjugacy classes of $g$ and $g^{-1}$. Suppose that*

(1) *$T \cap G_1 \neq Z(G_1)$,*
(2) *$C_1^2 \cup Z(G_1) = G_1$, and*
(3) *$g$ acts fixed point freely on all quotients $U_i/U_{i+1}$ of the central series $(U_i)_i$ of $U$.*

*Then $C^2 \cup Z(G) = G$. If $G$ is simple, then $C^2 = G$.*

Here, an element (and its conjugacy class) is called *real* if it is conjugate to its inverse. For the proof of Theorem 1.6 it then remains to verify these technical conditions for the various families of simple groups of Lie type, where $G_1$ is usually taken to be a subgroup of type $A$, and $g$ is the product of a regular unipotent element of $G_1$ with a suitable semisimple element of $G$.

## 2. THE CHARACTER THEORETIC METHOD

In this section we sketch the approach of Liebeck–O'Brien–Shalev–Tiep [LOST] which completes the proof of Theorem 0.1. Its main ingredient is character-theoretic, relying on the following lemma of Frobenius:

LEMMA 2.1. — *Let $G$ be a finite group. Then $g \in G$ is a commutator if and only if*

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0.$$

Here, $\mathrm{Irr}(G)$ denotes the set of complex irreducible characters of $G$.

*Proof* — We want to count pairs $(x, y) \in G \times G$ with $g = [x, y] = x^{-1}y^{-1}xy = x^{-1}x^y$, that is, representations of $g$ as a product of $x^{-1}$ times a conjugate of $x$. It is a well-known result of Frobenius that for a fixed conjugacy class $C$ of $G$ the number of pairs $(x_1, x_2) \in C \times C$ with $x_1^{-1}x_2 = g$ is given by

$$n_C := \frac{|C|^2}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(x_1)|^2 \chi(g)}{\chi(1)}.$$

Conjugating $x_2$ by $y \in C_G(x_2)$ fixes the pair, so we get $|C_G(x_2)|n_C$ pairs $(x, y) \in C \times G$ with $[x, y] = g$. Summing over all conjugacy classes $C$ of $G$ (with representative $x \in C$) yields

$$\sum_{C \subseteq G} |C_G(x)| n_C = \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \sum_{C \subseteq G} |C|\,|\chi(x)|^2 = |G| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}$$

for the desired number of pairs, where for the last equality we have used the orthogonality relations for characters. The claim follows. □

This allows us to deal with the 26 sporadic simple groups, since their character tables are known, see [NPC84], and more generally with any group whose character table is explicitly available.

Liebeck–O'Brien–Shalev–Tiep's idea for applying the Frobenius formula to the remaining groups of Lie type is as follows. By the orthogonality relations for characters we have $|\chi(g)|^2 \leq |C_G(g)|$ for any $g \in G$. Splitting off the contribution by the trivial character $1_G$ of $G$ we may thus estimate

$$\Big| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \Big| \geq 1 - |C_G(g)|^{1/2} \sum_{\chi \neq 1_G} \frac{1}{\chi(1)}.$$

Thus one may hope that for elements $g$ with small enough centralizer order $|C_G(g)|$, the second term has absolute value less than 1 so that one gets the desired result for such elements. The crucial observation which makes this approach work follows easily from the orthogonality relations and an application of the Cauchy–Schwarz inequality (see [LOST, Lem. 2.6]):

Lemma 2.2. — *Let $G$ be a finite group with $k_G$ conjugacy classes. Then for all $N > 0$ and all $g \in G$*

$$\sum_{\substack{\chi \in \mathrm{Irr}(G) \\ \chi(1) \geq N}} \frac{|\chi(g)|}{\chi(1)} \leq \frac{\sqrt{k_G\,|C_G(g)|}}{N}.$$

In order to apply this formula, one needs information on the number $k_G$ of conjugacy classes in a simple group of Lie type, and on lower bounds for degrees of its non-trivial complex irreducible characters. Let us write $G = G_r(q)$ if $G$ is a simple group of Lie type of rank $r$ over the finite field $\mathbb{F}_q$. Asymptotically, the number of conjugacy classes in $G_r(q)$, for $q \to \infty$, is bounded above by a polynomial in $q$ of degree $r$; more precise upper bounds for $k_G$ were obtained by Fulman and Guralnick [FG12], for example

$$k_G \leq \frac{q^n}{q-1} + q^{n/2+1} \quad \text{for } G = \mathrm{SL}_n(q) \text{ with } n \geq 4.$$

In practice, the argument sketched above needs to be refined slightly since there often exist a few non-trivial characters of very low degree which have to be treated separately.

The question on lower bounds for the minimal dimensions of non-trivial irreducible representations of finite simple groups is a very active area of research; first general results for groups of Lie type appeared in work of Landazuri and Seitz. For the present application, only complex irreducible representations matter, and for those, sharp lower bounds have been derived by Tiep and Zalesski [TZ96] from Lusztig's classification [Lu84] of all complex irreducible characters. Often, there exist few irreducible characters of degree very close to the lower bound, and all others have degree at least roughly the square of that bound. Such gap results are crucial in many other problems in the study of finite simple groups. As one example, we cite the result for symplectic groups (see [TZ96, 5.2]):

LEMMA 2.3. — *Let $G = \mathrm{Sp}_{2n}(q)$ with $n \geq 2$ and $q$ odd. Then $G$ has four complex irreducible characters of degrees $\frac{1}{2}(q^n \pm 1)$, the so-called* Weil characters, *and*

$$\chi(1) \geq \frac{(q^n-1)(q^n-q)}{2(q+1)}$$

*for all other $1_G \neq \chi \in \mathrm{Irr}(G)$.*

It is easy to see that any non-trivial irreducible representation of $\mathrm{Sp}_{2n}(q)$ has dimension at least $(q^n-1)/2$: considering $\mathbb{F}_{q^n}$ as an $n$-dimensional vector space over $\mathbb{F}_q$ we may embed $\mathrm{SL}_2(q^n) = \mathrm{Sp}_2(q^n)$ into $\mathrm{Sp}_{2n}(q)$, and the smallest non-trivial irreducible representation of $\mathrm{SL}_2(q^n)$ over any field of characteristic not dividing $q$ has dimension $(q^n-1)/2$. Indeed, the Borel subgroup of $\mathrm{SL}_2(q)$ is an extension of the elementary abelian group $U$ of order $q$ with a cyclic group of order $q-1$ which acts with two non-trivial orbits of length $(q-1)/2$ on the set of linear characters of $U$, whence any non-trivial representation of $\mathrm{SL}_2(q)$ has at least that dimension.

It is much harder to prove the stated gap result. For symplectic groups an elementary proof is available (see [GMST02]), but for other types, the full strength of Lusztig's classification of irreducible characters [Lu84] is needed.

Returning to Ore's conjecture, for $G = \mathrm{Sp}_{2n}(q)$ we can thus show that elements with small centralizer are commutators by applying Lemma 2.2 with the bound $N = (q^n-1)(q^n-q)/(2(q+1))$ together with the known bound on $k_G$, once we control the values of the four Weil characters. This is indeed possible by the very explicit construction of those characters. Let $P$ be the derived subgroup of an end node maximal parabolic subgroup of $\mathrm{Sp}_{2n+2}(q)$. Then $P = U.\mathrm{Sp}_{2n}(q)$ where $U$ is a *special group* of order $q^{1+2n}$ (that is, the center, the derived subgroup and the Frattini subgroup of $U$ all agree and are elementary abelian). Then $U$ has $q-1$ faithful irreducible complex representations, of dimension $q^n$, and these can be shown to extend to $P$. They take absolute value $q^{N(g)/2}$ on elements $g \in \mathrm{Sp}_{2n}(q)$, where $N(g) = \dim\ker(g-1)$. Upon restriction to $\mathrm{Sp}_{2n}(q)$ these representations split into two irreducible constituents each, of dimensions $(q^n \pm 1)/2$, the above mentioned Weil representations (see [Ger77]).

Similar bounds as in Lemma 2.3 exist for the other families of groups of Lie type [TZ96]. In the case of orthogonal groups, Liebeck–O'Brien–Shalev–Tiep need to prove estimates on character values for the $q+4$ smallest irreducible characters (see [LOST, Prop. 5.12]).

It still remains to show that elements with large centralizer are commutators. For this, the authors introduce the notion of breakable element. Let $V$ be a vector space equipped with a non-degenerate symmetric bilinear or hermitean form, and denote its group of isometries of determinant 1 by $\mathrm{Cl}(V)$. Thus, depending on the type of the form, $\mathrm{Cl}(V)$ could be a symplectic, a special orthogonal or a special unitary group. An element $g \in \mathrm{Cl}(V)$ is called *breakable* if there exists a proper non-degenerate subspace $W < V$ such that $g$ lies in the corresponding product $\mathrm{Cl}(W) \times \mathrm{Cl}(W^\perp)$ of classical groups with respect to the induced forms, and either both factors $\mathrm{Cl}(W)$ and $\mathrm{Cl}(W^\perp)$

are perfect groups, or at least $\mathrm{Cl}(W)$ is perfect and the component of $g$ in $\mathrm{Cl}(W^\perp)$ is a commutator. Since Ore's conjecture can already be assumed for $\mathrm{Cl}(W)$ (and for $\mathrm{Cl}(W^\perp)$ if it is perfect) by induction, such breakable elements are also commutators. This approach is complementary to the previous one; for example the authors show that for $G = \mathrm{Sp}_{2n}(2)$, $g$ unbreakable implies that $|C_G(g)| < 2^{2n+15}$ is indeed small.

This dichotomy approach fails if the factors in the decomposition are rather small, and thus not perfect or even solvable, like $\mathrm{Cl}(W) = \mathrm{Sp}_2(2), \mathrm{Sp}_2(3), \mathrm{Sp}_4(2)$ or $\mathrm{SO}_4^+(2)$. This leads to various 'small' cases which have to be treated by ad hoc calculations with the computer algebra systems GAP and Magma, either using or constructing their character tables and applying Lemma 2.2, or by trying to construct commutators in all conjugacy classes by random methods. Some of the challenging big cases of this type are the groups $\mathrm{Sp}_{16}(2)$, $\mathrm{SU}_6(7)$, $\mathrm{SO}_{11}(3)$, of sizes roughly $6 \cdot 10^{40}$, $4 \cdot 10^{29}$, $2 \cdot 10^{26}$ respectively. In total the authors estimate that their computations used about 3 years of CPU time.

An additional complication occurs for the projective special unitary groups $\mathrm{PSU}_n(q)$ (which by [EG98] have to be treated for $q \leq 7$ when $n$ is even, and for $q \leq 3$ when $n$ is odd). Here the bounds for centralizers of unbreakable elements are much weaker than for the other classical types. Thus, the character-theoretic approach sketched above fails. Instead the authors imitate Thompson's direct approach [Th61] for the special linear groups by representing elements directly as commutators. This again leaves open several cases with small $n$ and $q$ which have to be treated separately.

For the groups of exceptional types, the small rank cases had already been handled completely by Bonten [Bo93], and for the remaining finitely many groups of type $E_n$, $n = 6, 7, 8$, the bounds on character degrees are much more favorable than in classical types, so that similar but easier arguments allow to conclude.

## 3. TOWARDS THOMPSON'S CONJECTURE

Let us now turn to Thompson's conjecture, stated in the introduction, that any finite non-abelian simple group contains a conjugacy class $C \subseteq G$ such that $C^2 = G$.

The example of $6.\mathfrak{A}_6$ mentioned in the introduction shows that there are counter-examples to an extension of Thompson's conjecture to quasisimple groups. Moreover, the quasisimple groups $\mathrm{SL}_2(q)$, $q \equiv 3 \pmod 4$, are covered by commutators by Theorem 6.1, but they can be seen not to be covered by the square of a single conjugacy class, so not all groups satisfying Ore's condition satisfy Thompson's condition.

Note that a class satisfying Thompson's conjecture must be real. Again, the orthogonality relations for group characters yield an easy character theoretic criterion:

LEMMA 3.1. — *Let $G$ be a finite group, $C \subset G$ a real conjugacy class. Then $G = C^2$ if and only if*

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(x)|^2 \chi(g)}{\chi(1)} \neq 0$$

*for all $g \in G$ (where $x \in C$ is arbitrary).*

Thompson's conjecture has been checked for the sporadic groups [NPC84] (using the above criterion), for alternating groups by C.-H. Hsü [Hs65] (see also Bertram [Ber72]), for special linear groups by Brenner [Br83] and Lev [Lev94], and for the groups of Lie type over fields of cardinality at least 9 by Ellers–Gordeev (see Theorem 1.6). Using Lemma 3.1, Guralnick and Malle showed that for groups of Lie type of rank 1, almost any class $C$ has the desired covering property, and furthermore Thompson's conjecture holds for all exceptional groups of Lie type of rank less than 4 [GM12, Thm. 7.1 and 7.3].

In these investigations one is naturally led to study pairs of conjugacy classes whose product covers all of $G$, except possibly for the identity element. In order to verify the latter, one again uses Frobenius' character theoretic formula for structure constants, saying that for conjugacy classes $C_1, C_2$ of $G$, an element $g \in G$ is a product of elements $x \in C_1, y \in C_2$ if and only if

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x)\chi(y)\chi(g^{-1})}{\chi(1)} \neq 0.$$

This sum is very hard to evaluate in general, but as was first recognized by Malle [M88] in the construction of Galois realizations with given group and then used extensively in Malle–Saxl–Weigel [MSW94], for groups of Lie type, Deligne–Lusztig theory allows to identify classes $C_1, C_2$ such that very few irreducible characters do in fact contribute to this sum.

Let $G$ be an almost simple or quasisimple group of Lie type. Following Lübeck–Malle [LM99] we say that a pair $T_1, T_2$ of maximal tori of $G$ is *strongly orthogonal*, if only one non-trivial irreducible character $\chi \in \mathrm{Irr}(G)$ has the property that $\chi(s_1)\chi(s_2) \neq 0$ for any regular elements $s_i \in T_i$. This irreducible character is then necessarily the so-called Steinberg character St of $G$.

COROLLARY 3.2. — *Let $T_1, T_2$ be a pair of strongly orthogonal tori of a finite quasisimple group of Lie type $G$, and $C_i \subseteq G$ classes of regular semisimple elements of $T_i$, $i = 1, 2$. Then $C_1 C_2 \cup Z(G) = G$.*

*Proof* — By assumption, the only non-trivial irreducible character not vanishing on either $s_i \in T_i$ is the Steinberg character St. This is known to take values $\pm 1$ on regular semisimple elements, see [Ca85, Thm. 6.5.9]. Thus the above formula for the structure constant evaluates to $1 \pm \mathrm{St}(g)/\mathrm{St}(1)$, which is non-zero whenever $g \in G$ is non-central since then $|\mathrm{St}(g)| < \mathrm{St}(1)$. □

Such pairs of maximal tori were first considered in [MSW94] in the proof that all finite non-abelian simple groups except for $\mathrm{PSU}_3(3)$ can be generated by three involutions. Perhaps rather unexpectedly it turned out in [MSW94] and [LM99, Thm. 10.1] that:

PROPOSITION 3.3. — *All families of finite simple groups of Lie type, with the possible exception of orthogonal groups of type $D_{2n}$, possess strongly orthogonal pairs of maximal tori. Moreover, one of the tori in such a pair can be chosen to contain real elements.*

The proof requires Lusztig's classification of unipotent characters as well as his results on character values on semisimple elements, see [Lu84]. As a direct consequence one obtains the following approximation to Thompson's conjecture:

COROLLARY 3.4. — *Let $G$ be a finite simple group of Lie type, not of type $D_{2n}$. Then $G$ has a conjugacy class $C$ such that $C^2 \cup C^3 = G$.*

*Proof* — By Corollary 3.2 the product $C_1C_2$ covers $G \setminus \{1\}$, for $C_i$ classes of regular elements in the two strongly orthogonal tori, where moreover we may assume that $C_2$ contains real elements. In particular, any element of $C_1$ can be written as a product of two elements in $C_2$. As elements in $C_2$ are real, the identity lies in $C_2^2$ as well, so the claim follows with $C = C_2$. □

This has recently been improved as follows (see [GT13, Cor. 1.3]):

THEOREM 3.5 (Guralnick–Tiep). — *Let $G$ be a finite simple group. Then $G$ has a conjugacy class $C$ such that $C^3 = G$.*

In order to deal with groups of type $D_{2n}$, but also in other types, it is sometimes useful to consider the following weaker concept, formalized in [LST11]: Two maximal tori $T_1, T_2$ of $G$ are called *weakly orthogonal* if the intersection of $T_1$ with any conjugate of $T_2$ only contains the identity. Examples are any pairs of maximal tori $T_1, T_2$ of mutually coprime orders. The relevance of such pairs of tori comes again from Lusztig's classification of irreducible characters of finite reductive groups in terms of semisimple elements in the dual group (see [MSW94], [LM99] or [LST11, Prop. 2.2]):

PROPOSITION 3.6. — *Let $G$ be a finite simple group of Lie type, $T_1, T_2 \leq G$ maximal tori such that the corresponding tori in the Langlands dual group are weakly orthogonal. Let $\chi \in \mathrm{Irr}(G)$ and $s_i \in T_i$ be regular elements. Then $\chi(s_1)\chi(s_2) = 0$ unless $\chi$ is a so-called unipotent character of $G$.*

Using this, the following second approximation to Thompson's conjecture can be shown (see [GM12, Thm. 1.4], and also [LST11, Thm. 1.1.4] for an asymptotic version):

THEOREM 3.7. — *Let $G$ be a finite non-abelian simple group. Then there exist conjugacy classes $C_1, C_2 \subset G$ with $G = C_1C_2 \cup \{1\}$.*

*Proof* — For alternating groups, this is the main result of [Hs65]. For groups of Lie type different from $D_{2n}$, the assertion is an immediate consequence of Proposition 3.3 in conjunction with Corollary 3.2. For type $D_{2n}$, one has to establish bounds on the values of unipotent characters on elements of a pair of weakly orthogonal tori from [MSW94, 2.5], see [GM12, Thm. 7.6] or [LST11, Prop. 7.1.1]. □

In fact, for all but the two simple groups $\mathrm{PSL}_2(7)$ and $\mathrm{PSL}_2(17)$ we can arrange so that both classes contain elements of order prime to 6, see [GM12, Thm. 1.4]. Using this one gets (see [GM12, Cor. 1.5], and [LOST3, Thm. 2] for a slightly weaker statement):

THEOREM 3.8 (Guralnick–Malle). — *Let $k$ be a prime power or a power of 6. Then every element of any finite non-abelian simple group is a product of two $k$th powers.*

We will come back to the question on representing elements as products of powers in Section 5.

For alternating groups, much better results can be obtained at least asymptotically. For example, the following is shown in [LS09, Thm. 1.1]:

THEOREM 3.9 (Larsen–Shalev). — *There exists a constant $n_0$ such that for all $n \geq n_0$ and all permutations $g \in \mathfrak{S}_n$ with at most $n^{1/128}$ orbits on $\{1, \ldots, n\}$, the $\mathfrak{S}_n$-conjugacy class $C$ of $g$ satisfies $C^2 = \mathfrak{A}_n$.*

Choosing $g \in \mathfrak{A}_n$ with not all cycle lengths distinct, this gives a solution of Thompson's conjecture for $\mathfrak{A}_n$. The proof again relies on Frobenius' formula and a careful estimate of character values on permutations with few cycles using the Murnaghan–Nakayama rule.

Thus, at the time of writing, the Thompson conjecture remains open for simple groups of Lie type defined over fields of size at most 8, and of rank at least 4. One might hope that taking for $C$ a class of regular unipotent elements should give the result. Indeed, for $G$ of adjoint Lie type in good characteristic and $x \in G$ regular unipotent, it is known that $\chi(x) \in \{0, 1, -1\}$ for all irreducible characters $\chi$ of $G$, but even with this choice the known estimates on character values are too weak to allow for an application of Lemma 3.1.

## 4. WORD MAPS FOR ALGEBRAIC GROUPS AND FINITE GROUPS OF LIE TYPE

The formulation of Ore's conjecture fits into the more general framework of word maps on groups. Here, surprisingly strong results for groups of sufficiently large order can be obtained by asymptotic arguments. Again, the approach relies on the theory of algebraic groups. In order to phrase the results, we need the concept of *word map*: Let $F_r$ be the free group on $r$ generators $x_1, \ldots, x_r$ and $w = x_{i_1} \cdots x_{i_m} \in F_r$ a word. Then for any group $G$, $w$ defines a map $f_{w,G} : G^r \to G$ by sending $(g_1, \ldots, g_r)$ to $g_{i_1} \cdots g_{i_m}$.

Slightly abusing notation we will write $w(G) := \mathrm{im}(f_{w,G})$ for the image of $G$ under this word map.

Again, let's first consider the case of algebraic groups:

THEOREM 4.1 (Borel [Bor83]). — *Let $G$ be a semisimple linear algebraic group over an algebraically closed field $K$ and $1 \neq w \in F_r$ a word. Then $f_{w,G}$ is a dominant morphism, that is, $w(G)$ contains a Zariski open dense subset of $G$.*

*Proof* (Sketch) — First note that if $\pi : H \to G$ is an isogeny, then the diagram

$$\begin{array}{ccc} H^r & \xrightarrow{f_{w,H}} & H \\ \pi^r \downarrow & & \downarrow \pi \\ G^r & \xrightarrow{f_{w,G}} & G \end{array}$$

commutes, so if the claim holds for $H$, it also holds for $G$. In particular we may take for $\pi$ the simply connected covering, so it suffices to consider semisimple groups of simply connected type. Since these are direct products of simple algebraic groups, we may even assume that $G$ is simple.

Secondly, we may reduce to the case of $\mathrm{SL}_n$. Indeed, let $H \leq G$ be a subgroup of maximal rank. Then any maximal torus of $H$ is a maximal torus of $G$. If the claim holds for $H$, then the image of $f_{w,H}$ intersects the dense open subset of regular semisimple elements of $H$ in a dense open subset and so its image is dense in a maximal torus of $H$. Hence the image of $f_{w,G}$ is dense in a maximal torus of $G$, and so in $G$, whence the claim also holds for $G$. Now any simple algebraic group contains a semisimple maximal rank subgroup all of whose simple components are of type $A$. For example, we have $\mathrm{SL}_2^n \leq \mathrm{Sp}_{2n}$, $A_2^2 \leq F_4$ and $A_4^2 \leq E_8$. Thus, we are done when the result holds for groups $\mathrm{SL}_n$.

For $\mathrm{SL}_n$ consider the morphism $\chi_n : \mathrm{SL}_n \to K^{n-1}$ sending an element to the vector of coefficients of its characteristic polynomial (except for the first and last one). By induction, the claim holds for $\mathrm{SL}_{n-1}$, so $\chi_n \circ f_{w,G}$ contains a dense open subset of the hyperplane $\{(a_1, \ldots, a_{n-1}) \mid 1 + (-1)^n + \sum a_i = 0\}$ of $K^{n-1}$ corresponding to elements with an eigenvalue 1. By going to the closure one sees that it suffices to exhibit an element in $w(G)$ without eigenvalue 1. This is achieved by working inside an anisotropic subgroup of $\mathrm{SL}_n$ (i.e., a division algebra of degree $n$ over some global subfield of $K$).□

Theorem 1.1 shows that the commutator word map is surjective, but in general, word maps on simple algebraic groups need not be surjective: already on $\mathrm{SL}_2$ in characteristic 0, the word $x^2$ is not surjective. See Mycielski [My77] for this and further examples. Similarly, in positive characteristic $p$, the image of the $p$-power word map does not contain regular unipotent elements. It is intriguing to speculate under which conditions surjectivity might hold for non-power words.

Returning to finite groups, Theorem 4.1 allows us to deduce the following:

THEOREM 4.2 (Larsen [La04]). — *Let $1 \neq w \in F_r$, and $G_1, G_2, \ldots$ be an infinite sequence of pairwise non-isomorphic finite non-abelian simple groups. Then*

$$\lim_{n\to\infty} \frac{\log |G_n|}{\log |w(G_n)|} = 1.$$

*Proof* (Rough sketch) — Since $w(G_n)$ is closed under conjugation, it suffices to exhibit an element in the image with small enough centralizer, so with large class size.

One distinguishes three cases: for a sequence of simple groups of Lie type with a fixed root system, Larsen shows that $|w(G_n)| > c|G_n|$ for some $c > 0$, basically using Theorem 4.1, but the details are quite involved. In fact, it turns out that it is sufficient to prove this for groups of type $A_1$.

As a second step, one shows the same statement for a sequence of alternating groups. For this, one decomposes $n = \sum_{i=1}^{k}(p_i+1)$ with suitable primes $p_i$, embeds the product $\mathrm{PSL}_2(p_1) \times \ldots \times \mathrm{PSL}_2(p_k)$ into $\mathfrak{A}_n$ via the natural permutation action of $\mathrm{PSL}_2(p)$ on the projective line over $\mathbb{F}_p$, and uses the first part for the factors $\mathrm{PSL}_2(p_i)$ to find an element in $w(\mathfrak{A}_n)$ with small centralizer.

Finally, for the classical groups of arbitrary rank, one uses natural embeddings like $\mathfrak{A}_n \leq \mathrm{SL}_n(q) \leq \mathrm{SO}^+_{2n}(q) \leq \mathrm{SO}_{2n+1}(q) \leq \mathrm{SL}_{2n+1}(q)$ to exhibit elements with small centralizer, starting with those for $\mathfrak{A}_n$. □

A different proof of Theorem 4.2 is given in [LS09] using the following important irreducibility property enjoyed by word maps, the proof of which would lead too far away from the topic of this lecture (see [LS09, Thm. 3.3]):

THEOREM 4.3 (Larsen–Shalev). — *Let $w_i \in F_{r_i}$, $i = 1, 2$, be non-trivial words in two disjoint sets of letters, and $w \in F_{r_1+r_2}$ their concatenation. Let $G$ be a simple algebraic group of simply connected type over an algebraically closed field. Then for all non-central elements $g \in G$, the fiber $f^{-1}_{w,G}(g)$ is irreducible.*

## 5. ASYMPTOTIC WARING TYPE RESULTS

The results stated in the previous section form a key ingredient for the study of various asymptotic Waring type questions on the image of word maps. Recall that in number theory the Waring problem, solved by Hilbert, asks whether there exists a function $f$ such that any positive integer can be represented by $f(k)$ $k$th powers. In analogy, in the setting of group theory, given any non-trivial word $w \in F_r$ one may ask whether some power $w(G) \cdots w(G)$ covers $G$ for all sufficiently large non-abelian finite simple groups $G$. (Recall that we write $w(G)$ for the image of the word map on $G^r$ associated to $w$.) Here the best and most general results are consequences of the following (see [LST11, Thm. 1.1.1]):

THEOREM 5.1 (Larsen–Shalev–Tiep). — *Let $w_1, w_2 \in F_r$ be non-trivial words. Then there exists a constant $N = N(w_1, w_2)$ such that for all finite non-abelian simple groups $G$ of order $|G| \geq N$ we have $w_1(G)\, w_2(G) = G$.*

The case of alternating groups and of groups of Lie type of bounded rank had already been established earlier by Larsen and Shalev [LS09]. Using Theorem 4.3 and suitable embeddings as in the proof of Theorem 4.2 they show, for example, that each word map on $\mathfrak{A}_n$ with $n$ large enough contains elements with few cycles in their image and then conclude by Theorem 3.9.

As an immediate consequence one has:

COROLLARY 5.2. — *For any $1 \neq w \in F_r$ there exists a constant $N = N(w)$ such that $w(G)^2 = G$ for all finite non-abelian simple groups $G$ of order $|G| \geq N$.*

Taking for $w$ the commutator word shows in particular that any element in a sufficiently large finite non-abelian simple group is the product of two commutators. Earlier, Liebeck and Shalev [LS01] had proved that for any word $w$ there exists an unspecified constant $c = c(w)$ such that if $G$ is a finite non-abelian simple group and $w(G) \neq 1$ then $w(G)^c = G$. This was then improved by Shalev [Sh09, Thm. 1.1] who showed the statement of the above corollary with 3 in place of 2. Nikolov and Pyber [NP11] reproved this using different methods. A recent result of Jambor, Liebeck and O'Brien [JLO13, Cor. 3] shows that the exponent 2 in Corollary 5.2 cannot in general be replaced by 1, even for non-power words: the word map for $w = x_1^2[x_1^{-2}, x_2]^2$ is not surjective on infinitely many groups $\mathrm{PSL}_2(q)$. It is not clear whether this also leads to a counterexample for simple algebraic groups.

The constants in all of the above statements are not explicit. Guralnick and Tiep [GT13, Thm. 1.4 and Cor. 1.5] have recently obtained the following explicit bounds for the power word $w = x_1^k$:

THEOREM 5.3 (Guralnick–Tiep). — *Let $G$ be a finite non-abelian simple group.*

(a) *Let $1 \leq k \leq m$. If $|G| \geq m^{8m^2}$, then every element of $G$ can be written as $x^k y^m$ for some $x, y \in G$.*

(b) *Let $m \geq 1$ be not divisible by the exponent of $G$. Then every element of $G$ is a product of at most $80m\sqrt{2\log_2 m} + 56$ $m$th powers in $G$.*

Recall that by Theorem 3.8, the conclusion of Theorem 5.3(a) actually holds for all non-abelian simple groups when $k = m$ is restricted to prime powers or powers of 6.

This particular question has a long history. Martínez and Zelmanov [MZ96] and independently Saxl and Wilson [SW97] showed that there exists a function $f$ such that any element in a finite non-abelian simple group $G$ is a product of $f(k)$ $k$th powers, provided there are any non-trivial $k$th powers in $G$.

Shalev [Sh09] uses Theorem 4.2 of Larsen (to deal with Lie type groups of large rank) and Theorem 1.6 of Ellers–Gordeev (to dispose of groups of bounded rank) to show the following asymptotic version of Thompson's conjecture:

THEOREM 5.4 (Shalev). — *For any sequence $(G_n)_n$ of finite simple groups of increasing order there exist conjugacy classes $C_n \subset G_n$ such that*

$$\frac{|C_n^2|}{|G_n|} \longrightarrow 1 \qquad \text{for } n \to \infty.$$

The idea of proof for Theorem 5.1 is quite simple: by the result of Larsen and Shalev [LS09] one only has to consider groups of Lie type $G$. For these, one shows that $w_i(G)$ contains (elements of) a conjugacy class $C_i$ of regular elements in a pair of (strongly or weakly) orthogonal maximal tori (as in Section 3), so that the product $C_1C_2$ covers all of $G$ except possibly for the identity element (which is clearly contained in $w_1(G)w_2(G)$). The main result guaranteeing this is [LST11, Thm. 5.3.2]:

THEOREM 5.5 (Larsen–Shalev–Tiep). — *Let $w$ be a non-trivial word. Then for any sequence of finite simple groups $G(q)$ of fixed Lie type and any maximal torus $T(q)$, we have*

$$q^{\dim G - \mathrm{rk}G} \frac{|\{(g_1, \dots, g_r) \in G(q)^r \mid w(g_1, \dots, g_r) \in T(q)\}|}{|G(q)|^r} \longrightarrow 1.$$

COROLLARY 5.6. — *Let $w$ be a non-trivial word. Then for any sequence of finite simple groups $G(q)$ of fixed Lie type of rank at most $d$ there exists $q_0$ such that $w(G(q))$ contains regular elements of any maximal torus of $G(q)$ for all $q \geq q_0$.*

*Proof* — Fix a type of group $G$. It follows from Theorem 5.5 that there exists $\delta > 0$ such that $|T(q) \cap w(G(q))| \geq \delta |T(q)|$ for any maximally split torus $T(q)$ of $G(q)$. But the number of regular elements in a maximal torus $T(q)$ is larger than $(1-\delta)|T(q)|$ for $q$ larger than a suitable $q_0$. We conclude by taking the maximum over all such $q_0$ for all classes of maximal tori and all types of groups of rank at most $d$. □

We thus obtain the conclusion of Theorem 5.1 for groups of bounded rank, a case which had already been settled (in a slightly different way) in [LS09]:

COROLLARY 5.7 (Larsen–Shalev). — *Let $w_1, w_2$ be non-trivial words and $d_0 \geq 0$. Then there exists a constant $N = N(w_1, w_2, d_0)$ such that for all simple groups of Lie type $G$ of rank $d \leq d_0$ and order $|G| \geq N$ we have $w_1(G)w_2(G) = G$.*

*Proof* — By Corollary 5.6 the image $w_i(G)$ meets (and hence contains) a conjugacy class $C_i$ of regular elements in a maximally split torus of $G$. Thus we are in the situation of Corollary 1.4, so $G \setminus \{1\}$ is covered by $C_1C_2$. Since clearly 1 is also in the image, the claim follows.

For groups $G = G_r(q)$ not of type $D_{2n}$, instead of appealing to the result of Ellers–Gordeev, one may use that there exist pairs of strongly orthogonal maximal tori $T_1, T_2$ in $G$ by Proposition 3.3, and that $w_i(G)$ contains regular semisimple elements of $T_i$ whenever $d \leq d_0$ and $q$ is large enough, again by Theorem 5.5. The claim then follows by Corollary 3.2. □

This leaves the case of (classical) groups of unbounded rank. Again, we want to exhibit regular semisimple elements in pairs of strongly or weakly orthogonal tori, but this time the argument must work for all fields $\mathbb{F}_q$. We give the details in the easiest case:

PROPOSITION 5.8. — *The claim of Theorem 5.1 holds for simple symplectic groups.*

*Proof* — Let $G = \mathrm{Sp}_{2n}(q)$. By the previous discussion we may assume that $n$ is large. Let $T_i(q)$, $i = 1, 2$, be representatives of the two classes of maximal tori of $\mathrm{SL}_2(q^n)$. Under the embedding of $\mathrm{SL}_2(q^n)$ into $\mathrm{Sp}_{2n}(q)$ discussed in Section 2, $T_1(q), T_2(q)$ are mapped onto a pair of strongly orthogonal tori of $\mathrm{Sp}_{2n}(q)$. By Corollary 5.6, for $n$ large enough, $w_i(\mathrm{SL}_2(q^n))$ contains elements of $T_i(q)$ which map to regular elements in $\mathrm{Sp}_{2n}(q)$. Thus $G$ is covered by $w_1(G)w_2(G)$ by Corollary 3.2, and passing to the quotient by the center we obtain the desired conclusion. □

A similar approach works for other families of classical groups, but here one cannot guarantee to find elements in strongly orthogonal tori. For example, in type $\mathrm{SL}_n(q)$, one uses embeddings $\mathrm{SL}_k(q^l) < \mathrm{SL}_{kl}(q)$ with $k = 2, 3$ to find regular elements in a pair of weakly orthogonal tori. It can be shown that exactly three non-trivial (unipotent) irreducible characters do not vanish on these elements, all of them of rather large degree. The non-vanishing of the relevant structure constant then follows by bounding the values of these characters. The argument for orthogonal groups is even more technically involved.

## 6. EXTENSIONS AND OPEN PROBLEMS

We now discuss possible extensions of Ore's conjecture and related open problems.

As mentioned in the introduction, Blau [Bl94] proved that there is (only) a finite number of quasisimple (but not simple) finite groups that contain non-commutator central elements, and in a follow-up paper to their proof of Ore's conjecture Liebeck–O'Brien–Shalev–Tiep [LOST2] determined all quasisimple groups containing non-commutators:

THEOREM 6.1 (Blau, Liebeck–O'Brien–Shalev–Tiep). — *If $G$ is a finite quasisimple group containing non-commutators, then*

$$G/Z(G) \in \{\mathrm{PSL}_3(4), \mathrm{PSU}_4(3), \mathrm{PSU}_6(2), {}^2E_6(2), \mathfrak{A}_6, \mathfrak{A}_7, M_{22}, Fi_{22}\}.$$

For most quasisimple groups of classical Lie type, this had essentially already been contained in their first paper [LOST], so only the spin groups, the exceptional covering groups of classical groups and the exceptional groups of type $E_6$, ${}^2E_6$ and $E_7$ had to be considered.

It turns out, though, that in all cases every element of a finite quasisimple group is a product of at most two commutators. Let us mention here that for more general groups, Nikolov and Segal [NS07] have shown the following:

THEOREM 6.2 (Nikolov–Segal). — *There exists a function $f$ such that for any group $G$ generated by at most $r$ elements, every element of its commutator subgroup $[G,G]$ is a product of at most $f(r)$ commutators.*

This was one of the key steps in their proof establishing that in a finitely generated profinite group, every subgroup of finite index is open. (The special case of finitely generated pro-$p$ groups had long ago been shown by Serre.) The proof eventually relies on a result on twisted commutators in finite quasisimple groups, which in turn uses the classification of finite simple groups.

Closely related to Thompson's conjecture is the concept of covering number. In a finite non-abelian simple group $G$, for any non-trivial conjugacy class $C \subset G$ there exists some $k = k(C)$ such that $C^k = G$. The minimal exponent $k$ which works for all non-trivial classes $C$ is called the *covering number* $cn(G)$ of $G$.

The following upper bound on covering numbers for groups of Lie type has been obtained in [EGH99] (see also Lawther and Liebeck [LL98] for closely related results on the covering number with respect to $C \cup C^{-1}$):

THEOREM 6.3 (Ellers–Gordeev–Herzog). — *There exists a constant $d$ such that for any finite simple group of Lie type $G$ of rank $r$ we have $cn(G) \leq dr$.*

The expected best possible value for $d$ is 4, but the estimates obtained in the above reference are weaker. The claim is first shown for classical groups, by embedding a type $A$ subgroup of maximal possible rank and using that $cn(\mathrm{PSL}_n(q)) = n$ for $q, n \geq 4$. For the finitely many exceptional types one can clearly assume that $q$ is large enough, in which case Theorem 1.3 of Ellers–Gordeev can be used to deduce the result.

The lecture notes of Arad and Herzog [AH85] list several further open questions on products of conjugacy classes in finite non-abelian simple groups. Let us mention one open problem, the Arad–Herzog conjecture, which claims that products of arbitrary conjugacy classes can never be too small:

CONJECTURE 6.4 (Arad–Herzog). — *Let $G$ be a finite non-abelian simple group. Then the product of two non-trivial conjugacy classes of $G$ is never a single conjugacy class.*

Note that the claim may fail for arbitrary groups: Let $G$ be a Frobenius group of order $pd$ with $d|(p-1)$. Then the product of any class of non-trivial elements of order dividing $d$ with any class of elements of order $p$ is a single conjugacy class. A more interesting example can be obtained in the extension of $\mathrm{GL}_{2n}(q)$ by the transpose-inverse automorphism, see [GMT13, Example 7.2]. So, as for the Ore conjecture, the property in question seems to be tied to simple groups.

The Arad–Herzog conjecture is open in general, but has recently been shown to hold for various classes of simple groups (see [FA87, GMT13]):

THEOREM 6.5 (Fisman–Arad, Guralnick–Malle–Tiep). — *Let $G$ be an alternating group $\mathfrak{A}_n$, $n \geq 5$, a simple group $\mathrm{PSL}_n(q)$ or a simple group of Lie type of rank less than 4. Then the Arad–Herzog Conjecture holds for $G$.*

The proofs rely on the following easy character theoretic observation, which again follows from the orthogonality relations (see [GMT13, Lem. 2.2]):

LEMMA 6.6. — *Let $G$ be a finite group, $C, D \subset G$ two conjugacy classes of $G$. If $CD$ is a single conjugacy class, then $\chi(x)\chi(y) = \chi(1)\chi(xy)$ for all irreducible complex characters $\chi$ of $G$ and $x \in C$, $y \in D$.*

For alternating groups and $\mathrm{PSL}_n(q)$ this criterion can be applied with a single well-chosen character; for the groups of Lie type of small rank, one uses the knowledge of the complete character table (see [GMT13]).

Again, the question becomes much simpler if we turn to the natural analogue for simple algebraic groups, see [GMT13, Thm. 1.1]:

THEOREM 6.7 (Guralnick–Malle–Tiep). — *Let $G$ be a simple algebraic group over an algebraically closed field and $C, D$ non-central conjugacy classes of $G$. Then the product $CD$ is never a single conjugacy class.*

In fact, the proofs show that except for a small number of well-understood situations where the product consists of two or three classes, $CD$ is the union of infinitely many conjugacy classes.

The above result has the following immediate consequence ([GMT13, Cor. 1.2]), whose analogue in the case of finite groups, formerly known as Szep's conjecture, was proved by Fisman–Arad [FA87]:

COROLLARY 6.8. — *Let $G$ be a simple algebraic group over an algebraically closed field. Let $x, y \in G$ be non-central. Then $C_G(x)C_G(y) \neq G$.*

This investigation has recently been extended to almost simple algebraic groups in [GM13]; here, in disconnected groups there exist various pairs of conjugacy classes whose product is again a single class.

**Acknowledgements:** I thank Michael Cuntz, Bob Guralnick, Radha Kessar, Michael Larsen, Martin Liebeck, Eamonn O'Brien, Aner Shalev and Pham Huu Tiep for valuable comments on a draft version.

## REFERENCES


[AH85] Z. Arad, M. Herzog (eds.) – *Products of conjugacy classes in groups*, Lecture Notes in Math., vol. 1112, Springer-Verlag, Berlin, 1985.

[Ber72] E. Bertram – *Even permutations as a product of two conjugate cycles*, J. Combinatorial Theory Ser. A **12** (1972), 368–380.

[Bl94] H. I. Blau – *A fixed-point theorem for central elements in quasisimple groups*, Proc. Amer. Math. Soc. **122** (1994), 79–84.

[Bo93] O. Bonten – *Über Kommutatoren in endlichen einfachen Gruppen*, Aachener Beiträge zur Math. **7**, Verlag der Augustinus-Buchhandlung, Aachen, 1993.

[Bor83] A. Borel – *On free subgroups of semisimple groups*, Enseign. Math. (2) **29** (1983), 151–164.

[Br83] J. L. Brenner – *Covering theorems for finasigs. X. The group $G = \mathrm{PSL}(n, q)$ had a class $C$ such that $CC = G$*, Ars Combin. **16** (1983), 57–67.

[Ca85] R. W. Carter – *Finite groups of Lie type. Conjugacy classes and complex characters*, John Wiley & Sons, Inc., New York, 1985.

[EG94] E. W. Ellers, N. L. Gordeev – *Gauss decomposition with prescribed semisimple part in classical Chevalley groups*, Comm. Algebra **22** (1994), 5935–5950.

[EG95] E. W. Ellers, N. L. Gordeev – *Gauss decomposition with prescribed semisimple part in Chevalley groups II: Exceptional cases*, Comm. Algebra **23** (1995), 3085–3098.

[EG96] E. W. Ellers, N. L. Gordeev – *Gauss decomposition with prescribed semisimple part in Chevalley groups III: Twisted groups*, Comm. Algebra **24** (1996), 4447–4475.

[EG98] E. W. Ellers, N. L. Gordeev – *On the conjectures of J. Thompson and O. Ore*, Trans. Amer. Math. Soc. **350** (1998), 3657–3671.

[EGH99] E. W. Ellers, N. L. Gordeev, M. Herzog – *Covering numbers for Chevalley groups*, Israel J. Math. **111** (1999), 339–372.

[FA87] E. Fisman, Z. Arad – *A proof of Szep's conjecture on nonsimplicity of certain finite groups*, J. Algebra **108** (1987), 340–354.

[Fi02] W. B. Fite – *On metabelian groups*, Trans. Amer. Math. Soc. **3** (1902), 331–353.

[FG12] J. Fulman, R. Guralnick – *Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements*, Trans. Amer. Math. Soc. **364** (2012), 3023–3070.

[Ger77] P. Gérardin – *Weil representations associated to finite fields*, J. Algebra **46** (1977), 54–101.

[Go49] M. Gotô – *A theorem on compact semi-simple groups*, J. Math. Soc. Japan **1** (1949), 270–272.

[Gow88] R. Gow – *Commutators in the symplectic group*, Arch. Math. (Basel) **50** (1988), 204–209.

[Gu80] R. Guralnick, – *Expressing group elements as commutators*, Rocky Mountain J. Math. **10** (1980), 651–654.

[Gu10] R. Guralnick – *Commutators and wreath products*, pp. 79–82 in: Character theory of finite groups, Contemp. Math., 524, Amer. Math. Soc., Providence, RI, 2010.

[GMST02] R. Guralnick, K. Magaard, J. Saxl, P. H. Tiep – *Cross characteristic representations of symplectic and unitary groups*, J. Algebra **257** (2002), 291–347.

[GM12] R. Guralnick, G. Malle – *Products of conjugacy classes and fixed point spaces*, J. Amer. Math. Soc. **25** (2012), 77–121.

[GM13] R. Guralnick, G. Malle – *Products and commutators of classes in algebraic groups*, submitted, arXiv:1302.0182.

[GMT13] R. Guralnick, G. Malle, P. H. Tiep – *Products of conjugacy classes in finite and algebraic simple groups*, Advances Math. **234** (2013), 618–652.

[GT13] R. Guralnick, P. H. Tiep – *The Waring problem for finite quasisimple groups II*, preprint, arXiv:1302.0333.

[Hs65] C.-H. Hsü – *The commutators of the alternating groups*, Sci. Sinica **14** (1965), 339–342.

[Is77] I. M. Isaacs – *Commutators and the commutator subgroup*, Amer. Math. Monthly **84** (1977), 720–722.

[Ito51] N. Ito – *A theorem on the alternating group* $\mathfrak{A}_n (n \geqq 5)$, Math. Japonicae **2** (1951), 59–60.

[JLO13] S. Jambor, M. W. Liebeck, E. A. O'Brien – *Some word maps that are non-surjective on infinitely many finite simple groups*, Bull. London Math. Soc. **45** (2013), 907–910.

[La04] M. Larsen – *Word maps have large image*, Israel J. Math. **139** (2004), 149–156.

[LS09] M. Larsen, A. Shalev – *Word maps and Waring type problems*, J. Amer. Math. Soc. **22** (2009), 437–466.

[LST11] M. Larsen, A. Shalev, P. H. Tiep – *The Waring problem for finite simple groups*, Ann. of Math. (2) **174** (2011), 1885–1950.

[LL98] R. Lawther, M. W. Liebeck – *On the diameter of a Cayley graph of a simple group of Lie type based on a conjugacy class*, J. Combin. Theory Ser. A **83** (1998), 118–137.

[Lev94] A. Lev – *Products of cyclic similarity classes in the groups* $\mathrm{GL}_n(F)$, Linear Algebra Appl. **202** (1994), 235–266.

[LOST] M. W. Liebeck, E. A. O'Brien, A. Shalev, P. H. Tiep – *The Ore conjecture*, J. Eur. Math. Soc. **12** (2010), 939–1008.

[LOST2] M. W. Liebeck, E. A. O'Brien, A. Shalev, P. H. Tiep – *Commutators in finite quasisimple groups*, Bull. Lond. Math. Soc. **43** (2011), 1079–1092.

[LOST3] M. W. Liebeck, E. A. O'Brien, A. Shalev, P. H. Tiep – *Products of squares in finite simple groups*, Proc. Amer. Math. Soc. **140** (2012), 21–33.

[LS01] M. W. Liebeck, A. Shalev – *Diameters of finite simple groups: sharp bounds and applications*, Ann. of Math. (2) **154** (2001), 383–406.

[LM99] F. Lübeck, G. Malle – $(2,3)$*-generation of exceptional groups*, J. London Math. Soc. **59** (1999), 109–122.

[Lu84] G. Lusztig – *Characters of reductive groups over a finite field*, Annals of Mathematics Studies, 107. Princeton Univ. Press, Princeton, NJ, 1984.

[M88] G. Malle – *Exceptional groups of Lie type as Galois groups*, J. reine angew. Math. **392** (1988), 70–109.

[MSW94] G. Malle, J. Saxl, T. Weigel – *Generation of classical groups*, Geom. Dedicata **49** (1994), 85–116.

[MZ96] C. Martínez, E. Zelmanov – *Products of powers in finite simple groups*, Israel J. Math. **96** (1996), 469–479.

[My77] J. Mycielski – *Research problems: Can one solve equations in group?*, Amer. Math. Monthly **84** (1977), 723–726.

[NPC84] J. Neubüser, H. Pahlings, E. Cleuvers – *Each sporadic finasig $G$ has a class $C$ such that $CC = G$*, Abstracts Amer. Math. Soc. **34**, 6 (1984).

[NP11] N. Nikolov, L. Pyber – *Product decompositions of quasirandom groups and a Jordan type theorem*, J. Eur. Math. Soc. **13** (2011), 1063–1077.

[NS07] N. Nikolov, D. Segal – *On finitely generated profinite groups. I. Strong completeness and uniform bounds*, Ann. of Math. (2) **165** (2007), 171–238.

[Ore] O. Ore – *Some remarks on commutators*, Proc. Amer. Math. Soc. **2** (1951), 307–314.

[PW62] S. Pasiencier, H. Wang – *Commutators in a semi-simple Lie group*, Proc. Amer. Math. Soc. **13** (1962), 907–913.

[Ree64] R. Ree – *Commutators in semi-simple algebraic groups*, Proc. Amer. Math. Soc. **15** (1964), 457–460.

[SW97] J. Saxl, J. S. Wilson – *A note on powers in simple groups*, Math. Proc. Cambridge Philos. Soc. **122** (1997), 91–94.

[Sh09] A. Shalev – *Word maps, conjugacy classes, and a noncommutative Waring-type theorem*, Ann. of Math. (2) **170** (2009), 1383–1416.

[So86] A. R. Sourour – *A factorization theorem for matrices*, Linear and Multilinear Algebra **19** (1986), 141–147.

[Th61] R. C. Thompson – *Commutators in the special and general linear groups*, Trans. Amer. Math. Soc. **101** (1961), 16–33.

[Th62] R. C. Thompson – *On matrix commutators*, Portugal. Math. **21** (1962), 143–153.

[Th62a] R. C. Thompson – *Commutators of matrices with coefficients from the field of two elements*, Duke Math. J. **29** (1962), 367–373.

[TZ96] P. H. Tiep, A. Zalesskii – *Minimal characters of the finite classical groups*, Comm. Algebra **24** (1996), 2093–2167.

Gunter MALLE

TU Kaiserslautern
Fachbereich Mathematik
Postfach 3049
D–67653 Kaiserslautern, Allemagne
*E-mail* : malle@mathematik.uni-kl.de