Turkish Journal of Mathematics

Volume 31
Number 5 *Suppl.*

Article 10

1-1-2007

Commutators, Words, Conjugacy Classes and Character Methods

ANER SHALEV

Turk J Math
31 (2007) , Suppl, 131 – 148.

Commutators, Words, Conjugacy Classes and Character Methods

*Aner Shalev**

Abstract

In this survey paper we show how character methods can be used to solve a wide range of seemingly unrelated problems. These include commutators, powers of conjugacy classes and related random walks, as well as word maps and Waring type problems. In particular we describe recent progress made on conjectures of Ore, of Thompson, and of Lulov and Pak. New open problems and conjectures are also stated.

Key Words: Finite simple groups, commutators, conjagacy classes, characters, word maps, random walks.

1. Commutators

Let G be a group, and let G' be its commutator subgroup. Then every element g of G' is a product of commutators $[x, y] = x^{-1}y^{-1}xy$. Can we bound the length of such a product independently of g?

In general the answer is negative; but it turns out to be positive in some important classes of groups. A pioneering result of Brian Hartley [19] in this context is the following.

Theorem 1.1 *Let G be a d-generated finite solvable group with Fitting height h. Then*

2000 *AMS Mathematics Subject Classification:* 20C15, 20D06, 20P05, 20C30.

Dedicated to the cherished memory of Brian Hartley.

*Supported by the Israel Science Foundation and by the Bi-National Science Foundation United States-Israel Grant 2004-052.

every element of G' can be expressed as a product of $f(d,h)$ commutators, where f is some function of d and h alone.

Brian Hartley then deduced the following important consequence.

Corollary 1.2 *Let G be a finitely generated poly-nilpotent profinite group. Then the commutator subgroup of G is closed, and every finite index subgroup of G is open.*

The first conclusion follows since by Theorem 1.1 there exists n such that $G' = C^n$, where C is the (closed) set of commutators in G, and C^n denotes the set of all products of length n of elements of C. The second conclusion is easily deduced from the first. Corollary 1.2 extends a result of Serre for the case of finitely generated pro-p groups.

The general case has been recently solved by Nikolov and Segal [38, 39], following Segal's work [43] on the pro-solvable case. Indeed we have:

Theorem 1.3 *(i) There exists a function f such that if G is a d-generated finite group then every element of G' is a product of $f(d)$ commutators.*

(ii) The commutator subgroup of a finitely generated profinite group is closed.

(iii) Every finite index subgroup of a finitely generated profinite group is open.

The proof of this result is highly non-trivial, and relies on the classification of finite simple groups, probabilistic arguments and other methods. While part (ii) above follows from part (i), the proof of part (iii) requires extra work.

There is special interest in the case where G is a finite (nonabelian) simple group. A result of Wilson [47] from 1996 shows the following.

Theorem 1.4 *There exists an absolute constant c such that every element of a finite simple group is a product of c commutators.*

Wilson's proof uses methods of mathematical logic and does not provide an explicit value for the constant c. In Theorem 2.8 of [44] we prove that, if we allow finitely many exceptions G, we may take c to be 2.

Theorem 1.5 *Every element of a sufficiently large finite simple group is a product of two commutators.*

Our proof of this theorem combines character theory with probabilistic arguments. After this theorem was proved Bob Guralnick told me he can use different methods to prove this result for *all* finite simple groups G.

An even stronger result was conjectured in 1951 by Ore [40].

Conjecture 1.6 *Every element of a finite (nonabelian) simple group is a commutator.*

This challenging longstanding conjecture has a long history. Ore himself proved it for alternating groups A_n [40]. The case of $\mathrm{PSL}(n,q)$ was settled by R.C. Thompson in the sixties. Bonten proved it for exceptional groups of Lie type of rank up to 4. It was also verified for the sporadic groups. In 1998 Ellers and Gordeev proved the conjecture for all Lie type simple groups over a field with at least 8 elements (see [10] and the references therein for the more detailed results).

In the yet unpublished paper [25] with Liebeck and O'Brien we prove the following.

Theorem 1.7 *The Ore conjecture holds for all symplectic (simple) groups and all exceptional groups of Lie type.*

It therefore remains to prove the Ore conjecture for orthogonal and unitary groups. These cases are studied in [26].

Probabilistic results related to the Ore conjecture have just been proved. In Theorem 2.9 of [44] we show the following.

Theorem 1.8 *Let G be a finite simple group, and let $x \in G$ be randomly chosen. Then the probability that x is a commutator tends to 1 as $|G| \to \infty$.*

In fact we show that for $G = X_r(q)$, a Lie type simple group of rank r over a field with q elements, this probability is at least $1 - cq^{-2r}$, where c is some absolute constant.

A more refined probabilistic result is obtained in [15]. We show there that the commutator map is almost *measure preserving* on finite simple groups. More precisely we have:

Theorem 1.9 *Let G be a finite simple group and let $\alpha : G \times G \to G$ be the map sending (x,y) to $[x,y]$. Then*

(i) For every subset $Y \subseteq G$ we have

$$|\alpha^{-1}(Y)|/|G|^2 = |Y|/|G| + o(1).$$

(ii) For every subset $X \subseteq G \times G$ we have

$$|\alpha(X)|/|G| \geq |X|/|G|^2 - o(1).$$

(iii) In particular, if X is as above and $|X|/|G|^2 = 1-o(1)$, then almost every element of G is a commutator of the form $[x, y]$ where $x, y \in X$.

Here and throughout this paper $o(1)$ denotes a real number depending on $|G|$ alone which tends to 0 as $|G| \to \infty$.

Note that this somewhat surprising theorem provides new information even for groups for which the Ore conjecture is already proved.

Applying this result for the set of generating pairs for G, which is of size $|G|^2(1-o(1))$ (see [27] and the references therein) we obtain the following.

Corollary 1.10 *Almost every element of a finite simple group G can be expressed as a commutator $[x, y]$ where x, y generate G.*

This result can be used to prove a conjecture by Guralnick and Pak [18] regarding the Product Replacement Algorithm, see [15] for more details.

We close this section posing a conjecture which seems even harder than the Ore conjecture.

Conjecture 1.11 *Let G be a finite simple group and let $g \in G$.*

(i) The number of ways g can be written as a commutator $[x, y]$ is at least $(1-o(1))|G|$.

(ii) If G is a group of Lie type of bounded rank, and $g \neq 1$, then the number of ways g can be written as a commutator $[x, y]$ is $(1 + o(1))|G|$.

Note that 1 can be expressed as a commutator in $k(G)|G|$ ways, where $k(G)$ is the number of conjugacy classes in G (which tends to ∞ as $|G| \to \infty$). Therefore the identity element is always over-represented as a commutator. Conjecture 1.11 states that there are no under-represented elements, and that in the bounded rank case the only over-represented element is the identity.

This conjecture is open even for alternating groups. It can be checked for families of groups whose character table is explicitly known (using Proposition 4.1 below). For example, it holds for $\mathrm{PSL}(2, q)$.

2. Words

By a *word* we mean an element $w = w(x_1, \dots, x_d)$ of the free group F_d on $x_1, \dots, x_d$. Given a word w and a group G we consider the *word map* $w_G : G^d \to G$ sending $(g_1, \dots, g_d)$ to $w(g_1, \dots, g_d)$. The set of all group elements of the form $w(g_1, \dots, g_d)$ (where $g_i \in G$) is denoted by $w(G)$.

A useful result proved by Borel [4] in the 1980s states that word maps on simple algebraic groups are dominant maps. This can be applied in the study of word maps on finite simple groups of Lie type.

If $w \neq 1$ and G is a finite simple group then it was already shown by Jones [20] that $w(G) \neq \{1\}$ provided G is large enough (namely $|G| \geq N_w$). Two natural questions arise: how large is $w(G)$? and can we express any element $g \in G$ as a short product of elements of $w(G)$?

The study of $w(G)$ is a natural extension of the study of commutators described in Section 1. Another much studied word is the power word $w = x_1^k$, playing a major role in Burnside-type problems and other contexts. The following interesting result was proved independently by Martinez and Zelmanov [36] in 1996 and by Saxl and Wilson [41] in 1997.

Theorem 2.1 *For each integer $k \geq 2$ there exists a number $f(k)$ depending only on k such that every element of a finite simple group G can be written as a product of $f(k)$ kth powers.*

This result can be compared with Waring problem in number theory (see for instance [37]), where we express each integer as a sum of $g(k)$ kth powers. Can we extend Theorem 2.1 for arbitrary words w? In the work [28] from 2001 with Martin Liebeck we provide such an extension.

Theorem 2.2 *For each word $w \neq 1$ there exists a number $f(w)$ depending only on w such that every element of a finite simple group G can be written as a product of $f(w)$ elements of $w(G)$.*

The proof of this result starts by showing that if G is large enough then $|w(G)| \geq |G|^\epsilon$ for some $\epsilon = \epsilon(w) > 0$. Then a general result on normal subsets of that size is obtained. Can we get better lower bounds on $|w(G)|$? In 2004 Larsen [21] provided such a bound as follows.

Theorem 2.3 *For any word $w \neq 1$ and real number $\epsilon > 0$ there exists $N = N_{w,\epsilon}$ such that if G is a finite simple group satisfying $|G| \geq N$ then $|w(G)| \geq |G|^{1-\epsilon}$.*

The proof uses the dominance of word maps and algebraic geometry. Combining these methods with refined character theoretic results we can show that the inexplicit function $f(w)$ in Theorem 2.2 can be replaced by a very small absolute constant (provided G is large enough).

Theorem 2.4 *For each word $w \neq 1$ there exists a number $N = N_w$ depending only on w such that if G is a finite simple group of order at least N then*

$$w(G)^3 = G.$$

This somewhat surprising result will appear in [44]. It shows that Waring-type problems sometimes have better solutions in non-commutative contexts. Restricting to powers we obtain the following improvement of Theorem 2.1.

Corollary 2.5 *For every integer $k \geq 1$ there is a number $N = N_k$ such that if G is a finite simple group of order at least N then every element $g \in G$ can be written as $g = g_1^k g_2^k g_3^k$.*

Is Theorem 2.4 above best possible? In the recent joint work [22] with Michael Larsen we provide a stronger result for alternating groups and Lie type groups of bounded rank.

Theorem 2.6 *Let $w \neq 1$ be a word.*

(i) We have $w(A_n)^2 = A_n$ provided $n \geq N_w$.

(ii) If G is a finite simple group of Lie type of rank r, then we have $w(G)^2 = G$ provided $|G| \geq N_{w,r}$.

We pose the following.

Conjecture 2.7 *For any word $w \neq 1$ there is a number $N = N_w$ such that if G is a finite simple group of order at least N then $w(G)^2 = G$.*

In view of Theorem 2.6 it remains to prove the conjecture for classical groups of unbounded rank. Note that if $w = [x_1, x_2]$ is the commutator word, then it satisfies the conjecture by Theorem 1.5 above. However the case $w = x_1^k$ (even when $k = 2$) is very much open.

There are some indications that the "worst" words in these contexts are the power words. For example, the word maps of power words w need not be surjective, in fact $|w(G)|$ may be much smaller than $|G|$. It might be that words w which are not proper powers of other words behave better. We quote a related conjecture of Brenner.

Conjecture 2.8 *Let $w \neq 1$ be a word which is not a proper power of another word. Then $w(A_n) = A_n$ for all $n \geq N_w$.*

This is a far reaching generalization of the Ore conjecture (and theorem) for alternating groups. We propose the following version for groups of Lie type.

Conjecture 2.9 *Let $w \neq 1$ be a word which is not a proper power of another word. Then there exists a number $N = N_w$ such that, if G is a finite simple group of Lie type of rank $r \geq N_w$, then $w(G) = G$.*

A challenging test case is the Engel word $w = [x_1, x_2, \ldots, x_2]$.

We conclude this section with yet another problem on word maps.

Problem 2.10 *Which words w induce almost measure preserving maps $w_G : G^d \to G$ on finite simple groups G?*

By Theorem 1.9 commutators $[x_1, x_2]$ have this property. As shown in [15] longer commutators in distinct variables and in any bracket arrangement also have this property, as well as the word $x_1^2 x_2^2$. On the other hand, words which are proper powers do not have this measure preserving property. For general words this problem is very much open.

Note that there is also interest in dual questions, related to the kernel of word maps w_G, and the probability that $w(g_1, \ldots, g_d) = 1$. These questions arise naturally in the contexts of residual properties of free groups [9] and of the girth of Cayley graphs [14].

3. Conjugacy Classes

Several results on properties of $w(G)$ rely on the study of conjugacy classes and their powers.

If G is a finite simple group and $C \neq \{1\}$ is a conjugacy class in G then there exists an integer k such that $C^k = G$. The minimal such k given C is the *covering number*

$cn(C,G)$ of C in G, and the minimal k which works for *all* non-trivial classes C is the covering number $cn(G)$ of G.

There has been considerable interest in the study of these covering numbers over the past decades. See the book [1] where the covering number of A_n is determined, as well as bounds for other simple groups. Much later more refined results for simple groups of Lie type were obtained in [11] and [24], so we have the following.

Theorem 3.1 *Let G be a finite simple group.*

(i) If $G = A_n$ then $cn(G) = [(n-1)/2]$.

(ii) If G is a Lie type group of rank r then $cn(G) \leq cr$ where c is some absolute constant.

In the paper [28] with Liebeck we determine the covering numbers of arbitrary classes in arbitrary simple groups up to a multiplicative constant.

Theorem 3.2 *There exists an absolute constant c such that if G is a finite simple group and $C \neq \{1\}$ is a conjugacy class in G, then*

$$cn(C,G) \leq c\frac{\log|G|}{\log|C|}.$$

However, the constant c is not given explicitly, and computing the exact covering number of classes is still very hard in many cases. One motivation for such computations is a challenging conjecture of J.G. Thompson.

Conjecture 3.3 *Every finite simple group G has a conjugacy class C such that $C^2 = G$.*

We note that the Thompson conjecture implies the Ore conjecture. Indeed, if $C^2 = G$ then $1 \in C^2$ so $C^{-1} = C$ and $G = C^{-1}C$. Since $g^{-1}g^h = [g,h]$ every element of $C^{-1}C$ is trivially a commutator, and the implication follows.

Thompson conjecture was verified for alternating groups, projective special linear groups, sporadic groups, and groups of Lie type over a field with at least 8 elements (see [10] for the latter result). Moreover, a result of Gow [17] shows that if C is a class of regular semisimple real elements in the simple group of Lie type G, then C^2 contains all semisimple elements of G.

In [44] we combine probabilistic and character methods to obtain the following approximations to Thompson conjecture.

Theorem 3.4 *There exists an absolute constant c such that every finite simple group G of order $\geq c$ has a conjugacy class C such that $C^3 = G$. Furthermore, if $x \in G$ is randomly chosen, then the probability that $(x^G)^3 = G$ tends to 1 as $|G| \to \infty$.*

The first assertion extends results obtained by Malle, Saxl and Weigel in [35].

We also show that there are classes whose square covers almost all of G.

Theorem 3.5 *In every finite simple group we can find a conjugacy class C_G with the property that*

$$|C_G^2|/|G| \to 1 \text{ as } |G| \to \infty.$$

The case of symmetric and alternating groups is particularly interesting. On the one hand there are early results showing that $C^2 = A_n$ for certain classes C (e.g. a class of an n-cycle or of two cycles, see [2] and [5] and the references therein). But very few classes like this have been found, and it remained open whether $C^2 = A_n$ is a rare or a common phenomenon.

In the recent joint work [23] with Larsen we show the following.

Theorem 3.6 *For any $\epsilon > 0$ there exists $N = N_\epsilon$ such that if $n \geq N$ and $\sigma \in S_n$ satisfies*
(i) σ consists of at most $n^{1/4-\epsilon}$ cycles, or
(ii) σ consists of at most $(1/4 - \epsilon)n$ cycles, and has no cycles of length 1 or 2,
then $(\sigma^{S_n})^2 = A_n$.

By the Erdős-Turán theory [12] a random permutation in S_n has about $\log n$ cycles. Using the preceding theorem we can readily deduce the following.

Corollary 3.7 *Let $\sigma \in A_n$ be a randomly chosen permutation. Then the probability that $(\sigma^{A_n})^2 = A_n$ tends to 1 as $n \to \infty$.*

Thus almost all classes C in A_n satisfy $C^2 = A_n$. Is it the case for the other finite simple groups? We do not know the answer to this question (obviously a positive answer would imply Thompson conjecture for all large simple groups). However, in [45] we obtain some positive indication, using the concepts of *random walks* and *mixing times*.

Random walks on finite (almost) simple groups G with respect to a conjugacy class C as a generating set have been studied extensively in the past decades. See Diaconis and Shahshahani [8] for transpositions in symmetric groups, Lulov [32] and Vishne [46]

for homogeneous classes in symmetric groups, Lulov and Pak [33] for cycles in symmetric groups, and [16], [28], [31] for groups of Lie type. A main problem investigated is determining the mixing time $T(C, G)$ of the random walk, namely the time required till we reach an almost uniform distribution on G. In most cases this mixing time is still not known. For background see also [6], [7].

The following result from [23] gives rather sharp bounds on mixing times in A_n.

Theorem 3.8 *Let $\sigma \in A_n$, and $C = \sigma^{S_n}$, and let $T = T(C, A_n)$ denote the mixing time of the associated random walk on A_n.*

(i) The mixing time T is bounded if and only if σ has at most n^α fixed points, where $\alpha < 1$ is bounded away from 1.

(ii) If σ has n^α fixed points where $\alpha < 1$ then
$(1-\alpha)^{-1} \leq T \leq 2(1-\alpha)^{-1} + 1$.

(iii) If σ is fixed-point-free or has $n^{o(1)}$ fixed points then $T \leq 3$.

(iv) If σ has at most $n^{o(1)}$ cycles of length 1 and 2 then $T = 2$.

Parts (iii) and (iv) are best possible, and extend Lulov's result [32] for permutations σ which consist of n/m m-cycles (where the mixing time is 3 if $m = 2$ and 2 if $m \geq 3$).

The main conjecture of Lulov and Pak in [33] is the following.

Conjecture 3.9 *Let $C_n \subset S_n$ be a sequence of conjugacy classes of permutations with no fixed points. Then, as $n \to \infty$, the mixing time $T(C_n, S_n)$ is 2 or 3.*

This means that in two or three steps we reach an almost uniform distribution on a suitable coset of A_n in S_n.

Part (iii) of Theorem 3.8 (with a similar variant when σ is an odd permutation) establishes Conjecture 3.9 even when there are some fixed points. We therefore have

Corollary 3.10 *The Lulov-Pak conjecture holds.*

In [45] we obtain a somewhat surprising result for general simple groups G, showing that the mixing time $T(G, C)$ is usually the smallest possible, namely 2.

Theorem 3.11 *Let G be a finite simple group, let $x \in G$ be randomly chosen, and let $C = x^G$ be its conjugacy class. Then the probability that $T(C, G) = 2$ tends to 1 as $|G| \to \infty$.*

This means that the product of two random elements of a "typical" class C is almost uniformly distributed on G.

Theorem 3.10 immediately implies the following.

Corollary 3.12 *Fix $\epsilon > 0$ and let G be a finite simple group. Let $x \in G$ be randomly chosen. Then the probability that $|(x^G)^2|/|G| \geq 1 - \epsilon$ tends to 1 as $|G| \to \infty$.*

Thus the square of a class of a random element of G covers almost all of G. This provides positive evidence towards Thompson conjecture, suggesting that C^2 might be equal to G for many classes C.

4. Characters

The proofs of the results described above require various tools, and we will not attempt to describe all of them in this survey paper. Rather, we shall highlight a major tool, namely character methods, which play an essential role in many of these proofs. Let $\mathrm{Irr}G$ denote the set of complex irreducible characters of the finite group G. To explain the connections to character theory we quote some classical results. We start with a result of Frobenius from 1896.

Proposition 4.1 *Let G be a finite group, and let $g \in G$. Then the number $N(g)$ of pairs $(x, y) \in G \times G$ such that $[x, y] = g$ satisfies*

$$N(g) = |G| \sum_{\chi \in \mathrm{Irr}G} \frac{\chi(g)}{\chi(1)}.$$

Consequently, an element $g \in G$ is a commutator if and only if $\sum_\chi \frac{\chi(g)}{\chi(1)} \neq 0$.

Now, if G is a finite simple group, and $g \in G$ is an element with a small centralizer, then one can use recent advances in representation theory (based on Deligne-Lusztig theory [34] and other tools) to show that the main contribution to the character sum in Proposition 4.1 comes from the trivial character $\chi = 1$, and all the other characters altogether contribute marginally. This means that, for such elements g we have $\sum_\chi \frac{\chi(g)}{\chi(1)} = 1 + o(1)$ and so $N(g) = |G|(1 + o(1))$ and in particular g is a commutator when G is large enough.

This argument shows that elements with a small centralizer are commutators. It can be shown that almost all elements of G have small centralizers, and this gives rise to the proof of Theorem 1.8 above.

In proving Theorem 1.7 we combine this character theoretic approach with an inductive argument. Elements with small centralizers are shown to be commutators using Proposition 4.1 and representation theory, while the remaining elements are shown to lie in some product of subgroups of Lie type of smaller dimension, which by induction already satisfy the Ore conjecture. This approach requires computational methods to verify all the base cases of the induction.

The method in [15] is more probabilistic and yields results on arbitrary finite groups whose representation growth is very small. We need some notation.

A central concept in many of our character-theoretic arguments is the so called *Witten zeta function* ζ^G encoding the character degrees of a finite group G. For a real number s define

$$\zeta^G(s) = \sum_{\chi \in \mathrm{Irr}G} \chi(1)^{-s}.$$

This function was defined by Witten [48] for real Lie groups and studied and applied extensively in [29], [30], [31], [15] for finite simple groups.

It turns out that the value of $\zeta^G(s)$ for certain numbers s encodes a key information on various properties of G. To illustrate this in the context of the commutator map, let U be the uniform distribution on G, and let P be the commutator distribution defined by

$$P(g) = N(g)/|G|^2.$$

Using non-commutative Fourier techniques one can show that

$$||P - U|| \leq (\sum_{\chi \neq 1} \chi(1)^{-2})^{1/2} = (\zeta^G(2) - 1)^{1/2},$$

where the above norm is the L_1-norm. Thus, if G is any finite group satisfying $\zeta^G(2) \leq 1 + \epsilon$ then $||P - U|| \leq \epsilon^{1/2}$ and so P is almost uniform when ϵ is close to zero. Combining this with some extra arguments we deduce that *if G is a finite group such that $\zeta^G(2)$ is very close to 1, then the commutator map from $G \times G$ to G is almost measure preserving.*

Now, in [30] we show the following.

Theorem 4.2 *Fix a real number $s > 1$, and let G be a finite simple group. Then $\zeta^G(s) \to 1$ as $|G| \to \infty$.*

Using this for $s = 2$ we finally obtain a proof of Theorem 1.9. More detailed results on the behavior of ζ^G can be found in [29, 31].

Character methods are also relevant in the context of studying powers of conjugacy classes and the Thompson conjecture in particular. Here a main tool is the following classical result (see e.g. [42], §7.2, or [1], 10.1, p. 43).

Proposition 4.3 *Let G be a finite group, $C \subset G$ a conjugacy class, and let k be a positive integer. For each element $g \in G$ let $N(C, k, g)$ be the number of k tuples $(x_1, \dots, x_k)$ where $x_i \in C$ $(i = 1, \dots, k)$ such that $x_1 \cdots x_k = g$. Then*

$$N(C, k, g) = \frac{|C|^k}{|G|} \sum_{\chi \in \mathrm{Irr}G} \frac{\chi(C)^k \chi(g^{-1})}{\chi(1)^{k-1}}.$$

Here we write $\chi(C)$ for the (common) value of $\chi(x)$ for $x \in C$.

Consequently we see that $g \in C^2$ if and only if

$$\sum_{\chi \in \mathrm{Irr}G} \frac{\chi(C)^2 \chi(g^{-1})}{\chi(1)} \neq 0.$$

In particular the Thompson conjecture amounts to saying that any finite simple group G has a class C such that the character sum above is non-zero for all $g \in G$.

In general estimating this sum for all $g \in G$ is quite a formidable task. But if C is a class of elements with small centralizers, and we assume the centralizer of g is small as well, then again one can show that the sum above is dominated by the summand at $\chi = 1$, which implies that $N(C, 2, g) = (1 + o(1))|C|^2/|G|$ and in particular $g \in C^2$ when G is large enough. The detailed arguments are much more involved, but they follow this general philosophy, and enable us to prove Theorem 3.5, showing the existence of a class $C_G \subset G$ with $|C_G^2|/|G| \to 1$.

The fact that a class x^G of a random element $x \in G$ has this property (see 3.11 and 3.12) uses again the Witten zeta function ζ^G. It is intriguing that in this context the value of $\zeta^G(s)$ at $s = 2/3$ plays a key role. We show that *if G ranges over any family of finite groups such that $\zeta^G(2/3) \to 1$, then for a random $x \in G$ the mixing time $T(x^G, G)$ is 2 for almost all G.*

Now, for most families of finite simple groups $\zeta^G(2/3) \to 1$ (see [31]), and the few remaining families (which are $L_2(q), L_3(q)$ and $U_3(q)$) are dealt with by ad-hoc methods.

Our results on classes and word maps in symmetric and alternating groups are based on new sharp bounds on character values in symmetric groups obtained in the joint work [23] with Larsen. These bounds have the form $|\chi(\sigma)| \leq \chi(1)^{E(\sigma)+o(1)}$ for all $\chi \in \mathrm{Irr}S_n$, where $0 \leq E(\sigma) \leq 1$ depends on the cycle structure of the permutation σ.

The detailed bound is quite technical, but we present here some of its main consequences.

Theorem 4.4 *Let $\sigma \in S_n$.*

(i) If σ has at most n^α fixed points, then

$$|\chi(\sigma)| \leq \chi(1)^{1/2+\alpha/2+o(1)} \text{ for all } \chi \in \mathrm{Irr}S_n.$$

(ii) If σ has at most $n^{o(1)}$ cycles of length $< m$ then

$$|\chi(\sigma)| \leq \chi(1)^{1/m+o(1)} \text{ for all } \chi \in \mathrm{Irr}S_n.$$

(iii) If σ has at most n^α cycles then

$$|\chi(\sigma)| \leq \chi(1)^{\alpha+o(1)} \text{ for all } \chi \in \mathrm{Irr}S_n.$$

These bounds are essentially best possible. Part (ii) above is a far reaching generalization of a result of Fomin and Lulov [13]. Theorem 4.4 is very useful in bounding mixing times $T(C, G)$ of random walks. Indeed, if P^t is the distribution of this walk at time t, then by the upper bound lemma of Diaconis and Shahshahani we have

$$||P_C^t - U_G||^2 \leq \sum_{1 \neq \chi \in \mathrm{Irr}G} \frac{\chi(C)^{2t}}{\chi(1)^{2t-2}}.$$

Using Theorem 4.4 we can bound $|\chi(C)|$ by $\chi(1)^\alpha$ for appropriate α, which reduces the right hand side above to the value of the Witten zeta function ζ^G at a certain point s (depending on t). We can then find the minimal integer $t > 1$ such that $\zeta^G(s)$ tends to 0, and conclude that $T(C, G) \leq t$. This is how Theorem 3.8 is proved.

Theorem 4.4 also plays a major role in the proof of Theorem 3.6, showing that $C^2 = A_n$ for many classes C. This in turn is useful in establishing our word map theorem $w(A_n)^2 = A_n$. The idea is to use embeddings of $\mathrm{PSL}(2, p)$ in A_n, then apply algebraic

geometry and analytic number theory to show that $w(A_n)$ contains a class C with few cycles. Theorem 3.6 then shows that $C^2 = A_n$, and so $w(A_n)^2 = A_n$, proving Theorem 2.6(i).

Are there analogues of Theorem 4.4 for finite groups of Lie type? Such analogues could be extremely useful in solving various outstanding problems in such groups. Some results in this direction for semisimple elements are obtained in the recent work [3] with Bezrukavnikov and Liebeck. The general theorem is too technical to state here, but we illustrate it with the following special case.

Theorem 4.5 *Let $G = GL(n,q)$ and let $g \in G$ be a diagonal matrix with eigenvalues $\lambda_1, \ldots, \lambda_m$ each occurring n/m times. Then we have*

$$|\chi(g)| \leq c\chi(1)^{1/m} \text{ for all } \chi \in \mathrm{Irr}G,$$

where c is a constant depending only on n (and not on q).

This result could be regarded as a linear analogue of 4.4(ii) above and of the Fomin-Lulov bound [13] for S_n.

References

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

[2] Bertram, E.: Even permutations as a product of two conjugate cycles, *J. Comb. Th. Ser. A* **12** (1972), 368-380.

[3] Bezrukavnikov, R., Liebeck, M.W. and Shalev, A.: Character bounds, random walks and covering in finite Chevalley groups, Preprint, 2005.

[4] Borel, A.: On free subgroups of semisimple groups, *Enseign. Math.* **29** (1983), 151-164.

[5] Brenner, J.L.: Covering theorems for finite nonabelian simple groups. IX. How the square of a class with two nontrivial orbits in S_n covers A_n, *Ars Combinatoria* **4** (1977), 151-176.

[6] Diaconis, P.: *Group Representations in Probability and Statistics*, Institute of Mathematical Statistics Lecture Notes - Monograph Series, Vol. 11, 1988.

[7] Diaconis, P.: Random walks on groups: characters and geometry, in *Groups St Andrews 2001 in Oxford, Vol.I*, 120-142, London Math. Soc. Lecture Note Series **304**, Cambridge Univ. Press, Cambridge, 2003.

[8] Diaconis, P. and Shahshahani, M.: Generating a random permutation with random transpositions, *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **57** (1981), 159-179.

[9] Dixon, J.D., Pyber, L., Seress, Á., Shalev, A.: Residual properties of free groups and probabilistic methods, *J. reine angew. Math. (Crelle's)* **556** (2003), 159-172.

[10] Ellers, E.W. and Gordeev, N.: On conjectures of J. Thompson and O. Ore, *Trans. Amer. Math. Soc.* **350**, 3657-3671.

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

[12] Erdős, P. and Turán, P.: On some problems of a statistical group theory. I, *Z. Wahrscheinlichkeitstheorie Verw. Gabiete* **4** (1965), 175-186.

[13] Fomin, S.V. and Lulov, N.: On the number of rim hook tableaux, *J. Math. Sci. (New York)* **87** (1997), 4118-4123.

[14] Gamburd, A., Hoory, S., Shahshahani, M., Shalev, A. and Virág, B.: The girth of random Cayley graphs, Preprint, 2007.

[15] Garion, S. and Shalev, A.: Commutator maps, measure preservation, and T-systems, to appear in *Trans. Amer. Math. Soc.*

[16] Gluck, D.: Characters and random walks on finite classical groups, *Adv. Math.* **129** (1997), 46-72.

[17] Gow, R.: Commutators in finite simple groups of Lie type, *Bull. London Math. Soc.* **32** (2000), 311-315.

[18] Guralnick. R.M. and Pak, I.: On a question of B.H. Neumann, *Proc. Amer. Math. Soc.* **131** (2002), 2021-2025.

[19] Hartley, B.: Subgroups of finite index in profinite groups, *Math. Z.* **168** (1979), 71-76.

[20] Jones, G.A.: Varieties and simple groups, *J. Austr. Math. Soc.* **17** (1974), 163-173.

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

[22] Larsen, M. and Shalev, A.: Word maps and Waring type problems, Preprint, 2007.

[23] Larsen, M. and Shalev, A.: Characters of symmetric groups: sharp bounds and applications, Preprint, 2007.

[24] Lawther, R. and Liebeck, M.W.: 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.

[25] Liebeck, M.W., O'Brien, E.A. and Shalev, A.: On the Ore conjecture, Preprint, 2007.

[26] Liebeck, M.W., O'Brien, E.A., Shalev A. and Tiep, P.: On the Ore conjecture, II, in preparation.

[27] Liebeck, M.W. and Shalev, A.: The probability of generating a finite simple group, *Geom. Ded.* **56** (1995), 103-113.

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

[29] Liebeck, M.W. and Shalev, A.: Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), 552-601.

[30] Liebeck, M.W. and Shalev, A.: Fuchsian groups, finite simple groups, and representation varieties, *Invent. Math.* **159** (2005), 317-367.

[31] Liebeck, M.W. and Shalev, A.:, Character degrees and random walks in finite groups of Lie type, *Proc. London Math. Soc.* **90** (2005), 61-86.

[32] Lulov, N.: Random walks on symmetric groups generated by conjugacy classes, Ph.D. Thesis, Harvard University, 1996.

[33] Lulov, N. and Pak, I.: Rapidly mixing random walks and bounds on characters of the symmetric groups, *J. Algebraic Combin.* **16** (2002), 151-163.

[34] Lusztig, G.: *Characters of reductive groups over finite fields*, Ann. of Math. Studies, Princeton University Press, Princeton, 1984.

[35] Malle, G., Saxl, J. and Weigel, T.: Generation of classical groups, *Geom. Ded.* **49** (1994), 85-116.

[36] Martinez, C. and Zelmanov, E.I.: Products of powers in finite simple groups, *Israel J. Math.* **96** (1996), 469-479.

[37] Nathanson, M.B.: *Additive Number Theory: the classical bases*, Graduate Texts in Mathematics **164**, Springer, 1996.

[38] Nikolov, N. and Segal, D.: On finitely generated profinite groups, I: strong completeness and uniform bounds, *Annals of Math.* **165** (2007), 171-238.

[39] Nikolov, N. and Segal, D.: On finitely generated profinite groups, II: product decompositions of quasisimple groups, *Annals of Math.* **165** (2007), 239-273.

[40] Ore, O.O.: Some remarks on commutators, *Proc. Amer. Math. Soc.* **272** (1951), 307-314.

[41] Saxl, J. and Wilson, J.S.: A note on powers in simple groups, *Math. Proc. Camb. Phil. Soc.* **122** (1997), 91-94.

[42] Serre, J.-P.: *Topics in Galois Theory*, Research notes in math **1**, Jones and Bartlett, Boston-London, 1992.

[43] Segal, D.: Closed subgroups of profinite groups, *Proc. London Math. Soc.* **81** (2000), 29-54.

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

[45] Shalev, A.: Mixing and generation in simple groups, to appear in *J. Algebra.*

[46] Vishne, U.: Mixing and covering in symmetric groups, *J. Algebra* **205** (1998), 119-140.

[47] Wilson, J.S.: First-order group theory, in *Infinite Groups 1994*, de Gruyter, Berlin, 1996, pp. 301-314.

[48] Witten, E.: On quantum gauge theories in two dimensions, *Comm. Math. Phys.* **141** (1991), 153-209.

Aner SHALEV
Institute of Mathematics
The Hebrew University
Jerusalem 91904 ISRAEL
e-mail: shalev@math.huji.ac.il

Received 27.09.2007