REPRESENTATIONS OF FINITE GROUPS AND APPLICATIONS

PHAM HUU TIEP

Abstract

We discuss some basic problems in representation theory of finite groups, and current approaches and recent progress on some of these problems. We will also outline some applications of these and other results in representation theory of finite groups to various problems in group theory, number theory, and algebraic geometry.

1 Introduction

Let $G$ be a finite group and $\mathbb{F}$ be a field. A (finite-dimensional) representation of $G$ over $\mathbb{F}$ is a group homomorphism $\Phi : G \rightarrow \text{GL}(V)$ for some finite-dimensional vector space $V$ over $\mathbb{F}$. Such a representation $\Phi$ is called irreducible if $\{0\}$ and $V$ are the only $\Phi(G)$-invariant subspaces of $V$.

Representation theory of finite groups started with the letter correspondence between Richard Dedekind and Ferdinand Georg Frobenius in April (12th, 17th, 26th) 1896. In the same year, Frobenius constructed the character table of $\text{PSL}_2(\mathbb{F})$, $\mathbb{F}$ any prime. Later on, the foundations of the complex representation theory (i.e. when $\mathbb{F} = \mathbb{C}$), were developed by Frobenius, Dedekind, Burnside, Schur, Noether, and others. Foundations of the modular representation theory (that is, when $p = \text{char}(\mathbb{F}) > 0$ and $p$ divides $|G|$) were (almost singlehandedly) laid out by Richard Brauer, started in 1935 and continued over the next few decades.

A natural question arises: in a more-than-century-old theory such as the representation theory of finite groups, what could still remain to be studied? By the Jordan–Hölder theorem, irreducible representations are the building blocks of any finite-dimensional representation of any finite group $G$. The main problem of representation theory of finite groups, which still remains wide open in full generality as well as for many important families of finite groups, can be formulated as follows:

The author gratefully acknowledges the support of the NSF (grants DMS-1201374 and DMS-1665014), the Simons Foundation, and the Clay Mathematics Institute.

MSC2010: primary 20C15; secondary 20C20, 20C33.
Problem 1.1. Given a finite group $G$ and a field $\mathbb{F}$, describe all irreducible representations of $G$ over $\mathbb{F}$.

Likewise, finite simple groups are building blocks of any finite group, and they are known thanks to the Classification of Finite Simple Groups (CFSG) Gorenstein, Lyons, and Solomon [1994], arguably one of the most monumental achievements of modern mathematics. So it is natural to focus our attention on studying Problem 1.1 for groups $G$ that are simple, or more generally, almost quasisimple, that is, when $S \triangleleft G/\mathbb{Z}(G) \leq \text{Aut}(S)$ for some finite non-abelian simple group $S$. Aside from the symmetric group $S_n$ and alternating group $A_n$ of degree $n$, almost quasisimple groups include the finite classical groups with natural module $V = \mathbb{F}_q^n$ (such as the special linear group $\text{SL}(V) \cong \text{SL}_n(q)$), the special unitary group $\text{SU}(V) \cong \text{SU}_n(q^{1/2})$ when $q$ is a square, the symplectic group $\text{Sp}(V) \cong \text{Sp}_n(q)$ when $2|n$, and the special orthogonal groups $\text{SO}(V)$, as well as their exceptional and twisted analogues. When $q$ is a power of a fixed prime $p$, the latter are usually referred to as finite groups of Lie type in characteristic $p$. A more precise definition and a technically convenient framework, particularly for the Deligne-Lusztig theory Lusztig [1988, 1984], are provided by viewing the latter groups as the fixed point subgroups

$$G^F := \{g \in G \mid F(g) = g\}$$

for a Steinberg endomorphism $F : G \to G$ on a connected reductive algebraic group $G$ defined over a field of characteristic $p$.

Throughout the paper, for a finite group $G$, $\text{Irr}(G)$ denotes the set of complex irreducible characters of $G$, and $\text{IBr}_p(G)$ denotes the set of irreducible $p$-Brauer characters of $G$ (that is, the Brauer characters of irreducible representations of $G$ over $\mathbb{F}_p$) for a given prime $p$.

Example 1.2. Just to see how difficult Problem 1.1 can be, let us consider the example of the symmetric group $G = S_n$.

(i) When $\mathbb{F} = \mathbb{C}$, according to the classical theory of Frobenius and Young, the complex irreducible characters $\chi = \chi^\lambda$ of $G$ are labeled by the partitions $\lambda$ of $n$, and the hook length formula gives us the degree $\chi^\lambda(1)$ for any $\lambda \vdash n$, and the Frobenius character formula determines the character values $\chi^\lambda(g)$ for all $g \in G$. Nevertheless, for a random partition $\lambda$ of a large $n$ and a random permutation $g \in S_n$, it remains a difficult problem to compute $\chi^\lambda(g)$ efficiently. Even by now one still does not know a precise formula for the largest degree $b(S_n) = \max_{\lambda \vdash n} \chi^\lambda(1)$ (which has importance in probabilistic group theory and various applications). The best until now, still asymptotic, answer to this question is given by work of Vershik and Kerov [1985] and independently of Logan and Shepp [1977] in 1977:

$$e^{-1.2826\sqrt{n} \sqrt{n!}} \leq b(S_n) \leq e^{-0.1156\sqrt{n} \sqrt{n!}}.$$
(This result implies that, in a sense, a randomly chosen partition \( \lambda \) of \( n \) already yields an irreducible character of degree close to be largest possible, and thus explains the difficulty of the question.)

(ii) For various applications, one also needs to know good exponential bounds on character values for symmetric groups. For instance, for each \( 1 \neq g \in S_n \) one would like to find an (explicit) constant \( 0 < \alpha = \alpha(g) < 1 \) such that \( |\chi(g)| \leq \chi(1)^{\alpha} \) for all \( \chi \in \text{Irr}(S_n) \). Such an \( \alpha(g) \) was found by Fomin and Lulov [1995] in the case all cycles of \( g \) have same size. The general case was settled by Larsen and Shalev [2008] only in 2008, and it led to important results in a number of applications.

(iii) Now let us keep the same group \( G = S_n \) but change \( \mathbb{F} \) to \( \mathbb{F}_2 \). Then the irreducible representations of \( G \) over \( \mathbb{F} \) are labeled by partitions of \( \lambda \) into distinct parts. But now, for a given degree, say \( n = 1000 \), and given such a partition \( \lambda \), one still does not know what is the dimension of the corresponding representation. The same story goes with the similar question for \( G = \text{GL}_{1000}(2) \) and \( \mathbb{F} = \mathbb{F}_2 \) or \( \mathbb{F} = \mathbb{F}_3 \).

Various questions mentioned in Example 1.2 also remain open, say, for most of the finite groups of Lie type.

**Problem 1.3.** Let \( G \) be a finite group of Lie type. For any \( g \in G \setminus Z(G) \), find a constant \( 0 < \alpha = \alpha(g) < 1 \), as small and explicit as possible, such that \( |\chi(g)| \leq \chi(1)^{\alpha} \) for all \( \chi \in \text{Irr}(G) \).

Given a finite group \( G \), let \( d_p(G) \) denote the smallest degree of faithful representations of \( G \) over \( \mathbb{F}_p \). We would like to study the following special instance of Problem 1.1, which turns out to be of importance for many applications:

**Problem 1.4.** Given an almost quasisimple group \( G \) and a prime \( p \),

(i) determine \( d_p(G) \), and

(ii) classify irreducible \( \mathbb{F}_p G \)-representations of degree up to \( d_p(G)^{2-\epsilon} \), for a fixed \( 0 < \epsilon < 1 \).

To formulate further conjectures, let us introduce some more notation. For a fixed group \( G \) and \( p \), let \( P \in \text{Syl}_p(G) \), and let

\[
\text{Irr}_{p'}(G) = \{ \chi \in \text{Irr}(G) \mid p \nmid \chi(1) \}.
\]

We say that \( \chi \in \text{Irr}(G) \) has \( p \)-defect 0 if \( \chi(1)_p = |G|_p \). If \( \chi \) belongs to a \( p \)-block \( B \) of \( G \) with defect group \( D \), then \( \chi \) is said to have height 0 if \( \chi(1)_p = [G : D]_p \).

Several fundamental conjectures in representation theory of finite groups follow the global-local principle, which in this case states that certain global invariants of a finite group \( G \) can be determined locally, in terms of its \( p \)-subgroups, their normalizers, etc.
The following is probably the easiest one to formulate among all the global-local conjectures:

**Conjecture 1.5 (McKay [1972]).** There exists a bijection \( \text{Irr}_{p'}(G) \leftrightarrow \text{Irr}_{p'}(N_G(P)) \).

The *Alperin-McKay conjecture* Alperin [1976] is a blockwise version of the McKay conjecture and asserts: If a \( p \)-block \( B \) of a finite group \( G \) has a defect group \( D \) and Brauer correspondent \( b \), a \( p \)-block of \( N_G(D) \), then \( B \) and \( b \) have the same number of characters of height 0. There are several recent refinements (due to Isaacs, Navarro, Turull, and others) of the McKay conjecture, which roughly say that in Conjecture 1.5 there should exist a bijection \( \pi \) that is compatible with the action of certain Galois automorphisms of \( \overline{\mathbb{Q}} \) and preserving congruences modulo \( p \), local Schur indices, etc.

Even if the Problem 1.1 remains unsolved, can one hope for a “natural” labeling of the irreducible representations of \( G \)? If \( G \) is a connected reductive algebraic group defined over \( \mathbb{F} \), then one can label the finite-dimensional rational irreducible representations of \( G \) by their highest weights. Alperin [1987] conjectured in 1986 that one should be able to do the same for any finite group \( G \). More precisely, a \( p \)-weight of \( G \) is a pair \( (Q, \delta) \), where \( Q \) is a \( p \)-subgroup of \( G \) and \( \delta \in \text{Irr}(N_G(Q)/Q) \) has \( p \)-defect 0.

**Conjecture 1.6 (Alperin).** The number of irreducible \( p \)-Brauer characters of a finite group \( G \) equals the number of \( G \)-conjugate classes of \( p \)-weights of \( G \).

Given a \( p \)-block \( B \) of \( G \), a \( p \)-weight of \( B \) is a \( p \)-weight \( (Q, \delta) \) with \( \delta \) belonging to an \( N_G(Q) \)-block \( b \) with \( b^G = B \). Then the blockwise version of the Alperin weight Conjecture 1.6 asserts that the number of irreducible \( p \)-Brauer characters of \( G \) that belong to \( B \) equals the number of \( G \)-conjugate classes of \( p \)-weights of \( B \).

Finally, we recall the *Brauer height zero conjecture* Brauer [1956], perhaps one of the oldest and deepest conjectures in the modular representation theory:

**Conjecture 1.7 (Brauer, 1955).** All complex irreducible characters in a \( p \)-block \( B \) of a finite group \( G \) have height zero if and only if the defect groups \( D \) of \( B \) are abelian.

## 2 Current Approaches and Recent Results

The aforementioned, and several other, fundamental conjectures in representation theory of finite groups have been proved to hold for many classes of finite groups, including solvable groups, \( p \)-solvable groups, as well as various families of simple groups. As important evidence in favor of these conjectures as these results are, none of the above conjectures has been proved to hold for all arbitrary finite groups.

A possible approach to tackle these conjectures, which was already one of the main ideas in Dade’s works in the ’90s, is to try to use the CFSG to reduce to *simple* groups. As
we will see, such reductions are possible, on the one hand, and they have led to important progress on some of these conjectures. On the other hand, oftentimes such reductions require one to prove much stronger statements about the simple groups, not merely the original conjecture in question. We will now discuss recent progress on various problems mentioned in §1.

2.1 The McKay conjecture. In 2007, Isaacs, Malle, and Navarro succeeded in proving the following reduction theorem for the McKay Conjecture 1.5:

**Theorem 2.1.1.** Isaacs, Malle, and Navarro [2007] Suppose that every finite non-abelian simple group $S$ is McKay-good for the prime $p$. Then the McKay conjecture holds for arbitrary finite groups (for the prime $p$).

Here, the McKay-goodness (also known as the inductive McKay condition) for the prime $p$ is much more than just satisfying the McKay conjecture. It is in fact a long and complicated list of conditions concerning representations and cohomology of certain subgroups of the universal cover of $S$, occupying a couple of pages of Isaacs, Malle, and Navarro [ibid.]. Later, a reduction theorem in the same spirit for the Alperin-McKay conjecture was obtained by Späth in Späth [2013a]. Combined efforts of Malle, Cabanes, and Späth have also led to the proof of the inductive McKay condition for all simple groups, except for simple orthogonal groups in odd characteristics and exceptional groups of type $E_6$, $2E_6$, and $E_7$. Moreover, a breakthrough has recently been achieved by Malle and Späth, showcasing the strengths of the current approach:

**Theorem 2.1.2.** Malle and Späth [2016] The McKay conjecture for $p = 2$ holds for all finite groups $G$.

Less is currently known about various refinements of the McKay conjecture, which, if true, would imply many interesting consequences. For instance, the Galois-McKay conjecture, as proposed by Navarro in Navarro [2004], implies that the character table of any finite group $G$ detects whether a Sylow $p$-subgroup of $G$ is self-normalizing. This would give a partial answer to Problem 12 in Brauer’s celebrated list Brauer [1963]: Given the character table of a group $G$ and a prime $p$ dividing $|G|$, how much information about the Sylow $p$-groups $P$ of $G$ can be obtained? In fact, an unconditional answer has been obtained, supporting the Galois-McKay conjecture:

**Theorem 2.1.3.** Let $G$ be a finite group, $p$ a prime, and let $P \in \text{Syl}_p(G)$.

(i) **Navarro, Tiep, and Turull [2007]** Suppose $p > 2$. Then $P = N_G(P)$ if and only if $\text{Irr}_{p'}(G)$ contains a unique character $\chi$ with $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\exp(2\pi i / |G|))$. 


Suppose $p = 2$ and let $\sigma$ be the automorphism of $\mathbb{Q}(\exp(2\pi i/|G|))$ that fixes every root of unity of 2-power order and squares every root of unity of odd order. Then $P = N_G(P)$ if and only if every $\chi \in \text{Irr}_{2'}(G)$ is fixed by $\sigma$.

Finite groups with self-normalizing Sylow $p$-subgroups (with $p > 2$) also stand out as one of the few cases where a canonical bijection $\pi$ satisfying the McKay Conjecture 1.5 can be found (and therefore it is compatible with the action of Galois automorphisms). As shown in Navarro, Tiep, and Vallejo [2014], in this case $\pi(\chi)$ can be taken to be the (unique) linear constituent of $\chi|_P$ for any $\chi \in \text{Irr}_{p'}(G)$. (Also see Isaacs [1973], Navarro [2003], Giannelli, Kleshchev, Navarro, and Tiep [2017], Isaacs, Navarro, Olsson, and Tiep [2017], Giannelli, Tent, and Tiep [2018] for some other occurrences of canonical McKay correspondences.) We also note the following recent result:

**Theorem 2.1.4.** Guralnick, Navarro, and Tiep [2016] Let $G$ be a finite group, $p$ be a prime, and $P \in \text{Syl}_p(G)$. Suppose that $N_G(P)$ has odd order. Then the McKay conjecture, the Alperin weight conjecture, and their blockwise versions hold for $G$ and the prime $p$.

### 2.2 The Alperin weight conjecture (AWC)

The following reduction theorem for the Alperin weight Conjecture 1.6 was proved in 2011:

**Theorem 2.2.1.** Navarro and Tiep [2011] Suppose that every finite non-abelian simple group $S$ is AWC-good for the prime $p$. Then the Alperin weight conjecture holds for arbitrary finite groups (for the prime $p$).

Another reduction theorem for the AWC was obtained by Puig [2011], and the blockwise version of the AWC was reduced to simple groups by Späth in Späth [2013b].

As it was the case with the inductive McKay condition, the AWC-goodness in Theorem 2.2.1 is much stronger than just satisfying the AWC. Nevertheless, the list of AWC-good simple groups for the prime $p$ has been shown to include the simple groups of Lie type in the same characteristic $p$, the alternating groups, and all the sporadic simple groups.

### 2.3 The Brauer height zero conjecture (BHZ)

The “if” direction of the Brauer height zero Conjecture 1.7 was reduced by Berger and Knörr [1988] in 1988 to quasisimple groups. This was a “pure” reduction; namely they showed that if the “if” direction of the BHZ holds for all blocks (with abelian defect groups) of all finite quasisimple groups, then it also holds for all blocks (with abelian defect groups) of all finite groups. The verification of (both directions of) the BHZ for quasisimple groups was completed recently by Kessar and Malle [2013, 2017]. Thus the “if” direction of the BHZ holds for arbitrary finite groups.
The “only if” direction of the BHZ is even more difficult. The Gluck–Wolf proof of this direction for $p$-solvable groups was already extraordinarily complicated. For arbitrary finite groups, the following reduction theorem was obtained in 2014:

**Theorem 2.3.1.** Navarro and Späth [2014] Suppose all of the following statements hold:

(i) The inductive Alperin-McKay condition Späth [2013a] holds for all finite simple groups $S$ for the prime $p$;

(ii) A generalized Gluck-Wolf theorem (gGW) holds; and

(iii) The “only if” direction of the BHZ holds for all finite quasisimple groups.

Then the “only if” direction of the BHZ holds for all finite groups for the prime $p$.

Another reduction theorem, with condition 2.3.1(i) replaced by the projective Dade conjecture Dade [1994], was obtained earlier by Murai in Murai [2012]. As mentioned above, condition (iii) in Theorem 2.3.1 holds, thanks to Kessar and Malle [2017]. The statement (gGW) alluded to in Theorem 2.3.1(ii) is a relative version of the BHZ, and is now also a theorem:

**Theorem 2.3.2.** Navarro and Tiep [2013] Let $G$ be a finite group with a normal subgroup $Z$, $p$ be a prime, and let $\lambda \in \text{Irr}(Z)$. Suppose that $\chi(1)/\lambda(1)$ is coprime to $p$ for all $\chi \in \text{Irr}(G)$ lying above $\lambda$. Then the Sylow $p$-subgroups of $G/Z$ are abelian.

Let us also mention

**Theorem 2.3.3.** Navarro and Tiep [2012] The Brauer height zero conjecture holds for all 2-blocks of $G$ with defect groups $P \in \text{Syl}_2(G)$.

### 2.4 Dimensions of irreducible representations and Problem 1.4.

For an almost quasisimple group $G$, let $S$ denote the unique non-abelian composition factor of $G$. In the case $S$ is a sporadic simple group, Problem 1.4 depends largely on latest developments in computational group theory. In particular, $d_p(G)$ has been completely determined Jansen [2005]. However, Problem 1.4 remains open for a number of large sporadic groups, for instance in the case where $G = M$ is the Monster and $p = 2$.

Next, let us consider the case $S = A_n$ with $n \geq 5$. Here, certainly the case of complex representations is very well understood, thanks to classical work of Frobenius and Schur. The case of modular representations of $S_n$ was settled by James in James [1983]. In particular, he showed that

$$d_p(S_n) = \begin{cases} n - 1, & p \nmid n \\ n - 2, & p \mid n \end{cases}.$$
In fact, James proved that, for a fixed \( p \)-regular partition \( \mu = (\lambda_2, \ldots, \lambda_k) \) of \( m \),
\[
\dim D^{(n-m, \lambda_2, \ldots, \lambda_k)} \approx \frac{n^m}{m!} \dim D^\mu
\]
when \( n \to \infty \) (if \( D^\lambda \) is the \( p \)-modular irreducible representation of \( S_n \) labeled by the \( p \)-regular partition \( \lambda \vdash n \)). This beautiful result gives however only an asymptotic bound on the dimension of \( D^\lambda \). For a number of applications, one needs an effective bound on \( \dim D^\lambda \), and the first such bound was obtained in Guralnick, Larsen, and Tiep [2012]. Define for \( p \neq 2 \)
\[
m_p(\lambda) := \max(\lambda_1, (\lambda^M)_1),
\]
(the longest row of partitions \( \lambda \) and \( \lambda^M \)), where \( \lambda \mapsto \lambda^M \) is the Mullineux bijection on the set of \( p \)-regular partitions of \( n \); also set \( m_2(\lambda) := \lambda_1 \).

**Theorem 2.4.1.** Guralnick, Larsen, and Tiep [ibid.] For any \( p \geq 0 \), and any \( p \)-regular partition \( \lambda \) of \( n \),
\[
\dim D^\lambda \geq \frac{2^{n-m_p(\lambda)}}{2}
\]
This effective bound was used to establish polynomial representation growth for the modular representations of \( S_n \) and \( A_n \), see Guralnick, Larsen, and Tiep [ibid., Theorem 1.1]. It also allowed to deduce quantitative results on branching rules for irreducible \( S_n \)-representations over \( A_n \), and, as a consequence, resolve Problem 1.4 for \( G = A_n \). However, the bound in Theorem 2.4.1 is not of the right magnitude. This issue has been rectified very recently:

**Theorem 2.4.2.** Kleshchev and Tiep [n.d.] Let \( p \) be a prime, \( m \geq 2 \), and let \( \lambda = (n - m, \lambda_2, \ldots, \lambda_k) \) be a \( p \)-regular partition of \( n \geq (m - 1)p + 2 \). Then
\[
\dim D^\lambda \geq \begin{cases} 
\left( \prod_{j=0}^{m-1} (n - jp) \right)/m!, & p \geq 5 \\
\left( \prod_{j=0}^{m-1} (n - 2jp) \right)/m!, & p = 2, 3
\end{cases}
\]
For spin representations, i.e. faithful representations of double covers of \( S_n \) and \( A_n \), Problem 1.4 has been studied in Kleshchev and Tiep [2004, 2012]. In particular, it was shown in Kleshchev and Tiep [2004] that
\[
\delta_p(2S_n) = \begin{cases} 
2^\lfloor (n-1)/2 \rfloor, & p \not| n \\
2^\lfloor (n-2)/2 \rfloor, & p|n
\end{cases}
\]
Furthermore, irreducible spin modular representations of degree up to \( (n/2) \cdot \delta_p(G) \) for \( G = 2S_n \) and \( 2A_n \) were determined in Kleshchev and Tiep [2012].
Now we discuss the main case of Problem 1.4 when $S$ is a simple group of Lie type in characteristic $\ell$. In the defining characteristic case, that is when $p = \text{char}(\mathbb{F}) = \ell$, Problem 1.4 can be solved using the representation theory of reductive algebraic groups (namely the theory of highest weight modules), and Premet’s theorem Premet [1987]. In fact, this was done by Liebeck for classical groups, and by Lübeck for exceptional groups.

Next we consider the cross characteristic case, that is when $p = \text{char}(\mathbb{F}) \neq \ell$. If, moreover, $p = 0$ or $0 < p \nmid |G|$, then Problem 1.4 can be solved using the Deligne-Lusztig theory Lusztig [1988, 1984]. This was done in Tiep and Zalesskii [1996] for classical groups, and by Lübeck for exceptional groups.

The remaining case ($\ell \neq p > 0$ and $p||G|$) turns out to be much harder and is still ongoing. Complete results have been obtained for groups of type $A$, that is when $G = \text{SL}_n(q)$, see Guralnick and Tiep [1999] and Brundan and Kleshchev [2000], and when $G = \text{SU}_n(q)$, see Hiss and Malle [2001] and Guralnick, Magaard, Saxl, and Tiep [2002].

**Theorem 2.4.3.** Guralnick and Tiep [1999] Assume $n \geq 4$ and $(n, q) \neq (4, 2), (4, 3)$. Then

$$b_p(\text{SL}_n(q)) = \frac{q^n - 1}{q - 1} - \begin{cases} 1, & p \nmid \frac{q^{n-1}}{q-1} \\ 2, & p|\frac{q^{n-1}}{q-1}. \end{cases}$$

Moreover, $\text{SL}_n(q)$ has one irreducible representation over $\mathbb{F}$ of degree $b_p$ and $(q-1)p' - 1$ of degree $(q^n - 1)/(q - 1)$. All other nontrivial irreducible representations have degree at least $(q^{n-1} - 1)\left(\frac{q^{n-2} - q}{q - 1} - 1\right)$.

**Theorem 2.4.4.** Guralnick, Magaard, Saxl, and Tiep [2002] Assume $n \geq 5$ and $(n, q) \neq (6, 2)$. Then

$$b_p(\text{SU}_n(q)) = \left\lfloor \frac{q^n - 1}{q + 1} \right\rfloor.$$

Moreover, $\text{SU}_n(q)$ has $(q+1)p'$ irreducible representations over $\mathbb{F}$ of degree $b_p$ or $b_p + 1$. All other nontrivial irreducible representations have degree at least \( \frac{(q^n - 1)(q^{n-1} - q^2)}{(q + 1)(q^2 - 1)} \).

The case of symplectic groups was also settled in Guralnick, Magaard, Saxl, and Tiep [ibid.] and Guralnick and Tiep [2004]; in particular,

$$b_p(\text{Sp}_{2n}(q)) = \begin{cases} (q^n - 1)/2, & q \text{ odd} \\ (q^n - 1)(q^n - q)/2(q + 1), & q \text{ even}. \end{cases}$$

Less complete results have also been obtained for other families of finite groups of Lie type, see Tiep [2003], Tiep [2006] for relevant references. All these results rely crucially on the Deligne-Lusztig theory and further important results of Broué and Michel [1989] and Bonnafé and Rouquier [2003].
As mentioned in Example 1.2, of interest is also the largest degree

\[ b(G) = \max_{\chi \in \text{Irr}(G)} \chi(1) \]

of complex irreducible characters of an almost quasisimple group \( G \). In the case \( G \) is of Lie type in characteristic \( p \), the Steinberg character \( \text{St} \) has quite a large degree, equal to \( |G|_p \). It turns out that \( b(G)/\text{St}(1) \) can grow unbounded when we fix the size \( q \) of the defining field \( \mathbb{F}_q \) and let the rank \( r \) of \( G \) grow. An upper bound for \( b(G) \) was given in Seitz [1990, Theorem 2.1], which yields the exact value of \( b(G) \) when \( q \) is large enough compared to \( r \).

**Theorem 2.4.5.** *Larsen, Malle, and Tiep [2013]* For any \( 1 > \varepsilon > 0 \), there are (explicit) constants \( A, B > 0 \) depending on \( \varepsilon \) such that, for any simple algebraic group \( \mathfrak{G} \) in characteristic \( p \) of rank \( r \) and any Steinberg endomorphism \( \mathfrak{F} : \mathfrak{G} \to \mathfrak{G} \), the largest degree \( b(G) \) of the corresponding finite group \( G := \mathfrak{G}^\mathfrak{F} \) over \( \mathbb{F}_q \) satisfies the following inequalities:

\[
A(\log q r)^{(1-\varepsilon)/\gamma} < \frac{b(G)}{|G|_p} < B(1 + \log q r)^{2.54/\gamma}
\]

if \( G \) is classical, and \( 1 \leq b(G)/|G|_p < B \) if \( G \) is an exceptional group of Lie type. Here, \( \gamma = 1 \) if \( G \) is untwisted of type \( A \), and \( \gamma = 2 \) otherwise.

A lower bound for the largest degree of modular irreducible representations of \( G = \mathfrak{G}^\mathfrak{F} \) was also given in *Larsen, Malle, and Tiep [ibid., Theorem 1.4]*. Theorem 2.4.5 implies the following, somewhat surprising, consequence which answers a question raised by D. Vogan and J. Berstein:

**Corollary 2.4.6.** Let \( q \) be any prime power and let \( n > 2q^{6815} \). Consider a non-degenerate quadratic space \( V = \mathbb{F}_q^n \), a non-degenerate subspace \( U \) of codimension 1 in \( V \), and embed the full orthogonal group \( H = \text{GO}(U) \cong \text{GO}^+_{n-1}(q) \) via \( g \mapsto \text{diag}(g, \det(g)) \) in the special orthogonal group \( G = \text{SO}(V) \cong \text{SO}^+_n(q) \). Then there exists a character \( \chi \in \text{Irr}(G) \) such that its restriction to \( H \) is not multiplicity-free (and \( \chi \) is trivial at \( Z(G) \)).

**Proof.** We give a proof for the case \( n = 2m + 1 \geq 9 \); the case \( n = 2m \) is completely similar. By *Larsen, Malle, and Tiep [ibid., Theorem 5.2]* (and its proof), there is \( \chi \in \text{Irr}(G) \) such that \( \chi \) is trivial at \( Z(G) \) and

\[
\chi(1) > q^{m^2} \cdot \frac{1}{5} (\log_q (m + 10))^{3/8}.
\]

On the other hand, \( |\text{Irr}(H)| < 15q^m \) by Theorems 3.14 and 3.21 of *Fulman and Guralnick [2012]*. Now if \( \chi|_H \) is multiplicity-free, then by Schwarz’s inequality we must have that

\[
\chi(1) \leq \sum_{\alpha \in \text{Irr}(H)} \alpha(1) \leq (|H| \cdot |\text{Irr}(H)|)^{1/2} < \sqrt{30} \cdot q^{m^2},
\]
contradicting the above lower bound on $\chi(1)$ when $m \geq q^{6815}$. \hfill \Box

In fact, Corollary 2.4.6 also holds if we take $U$ to be any nonzero proper non-degenerate subspace of $V$ and replace $H$ with $SO(V) \cap (GO(U) \times GO(U^\perp))$.

### 2.5 Bounds on character values: Problem 1.3.

For a finite group $G$, a character ratio is a complex number of the form $\chi(g)/\chi(1)$, where $g \in G$ and $\chi$ is an irreducible character of $G$. Upper bounds for absolute values of character values and character ratios have long been of interest, for various reasons; these include applications to random generation, covering numbers, mixing times of random walks, word maps, representation varieties and other areas.

The first significant bounds on character ratios for finite groups of Lie type $G$, defined over a field $\mathbb{F}_q$, were obtained by Gluck [1993, 1997]. In particular, he showed that $|\chi(g)|/\chi(1) \leq C q^{-1/2}$ for any non-central element $g \in G$ and any non-linear character $\chi \in \text{Irr}(G)$, where $C$ is an absolute constant. Another explicit character bound for finite classical groups, with natural module $V = \mathbb{F}_q^n$, was obtained in Larsen, Shalev, and Tiep [2011, Theorem 4.3.6]:

$$\frac{|\chi(g)|}{\chi(1)} < q^{-\sqrt{\text{supp}(g)}/481},$$

where $\text{supp}(g)$ is the codimension of the largest eigenspace of $g \in G$ on $V \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$.

These bounds have played a crucial role in a number of applications (some described in §3). However, in many situations of these and other applications, one needs stronger, exponential character bounds as described in Problem 1.3. Such a bound was established for $S_n$ in Larsen and Shalev [2008]. For finite groups of Lie type, it has been obtained for the first time in Bezrukavnikov, Liebeck, Shalev, and Tiep [n.d.]. For a subgroup $X$ of an algebraic group $\mathfrak{G}$, write $X_{\text{unip}}$ for the set of non-identity unipotent elements of $X$. For a fixed Steinberg endomorphism $F : \mathfrak{G} \to \mathfrak{G}$, a Levi subgroup $\mathfrak{L}$ of $\mathfrak{G}$ is called split, if it is an $F$-stable Levi subgroup of an $F$-stable proper parabolic subgroup of $\mathfrak{G}$. For an $F$-stable Levi subgroup $\mathfrak{L}$ of $\mathfrak{G}$ and $L := \mathfrak{L}^F$, we define

$$\alpha(L) := \max_{u \in L_{\text{unip}}} \frac{\dim u^\mathfrak{L}}{\dim u^\mathfrak{G}}, \quad \alpha(\mathfrak{L}) := \max_{u \in L_{\text{unip}}} \frac{\dim u^\mathfrak{L}}{\dim u^\mathfrak{G}}$$

if $\mathfrak{L}$ is not a torus, and $\alpha(L) = \alpha(\mathfrak{L}) := 0$ otherwise.

**Theorem 2.5.1.** Bezrukavnikov, Liebeck, Shalev, and Tiep [ibid.] There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that the following statement holds. Let $\mathfrak{G}$ be a connected reductive algebraic group such that $[\mathfrak{G}, \mathfrak{G}]$ is simple of rank $r$ over a field of good characteristic $p > 0$. Let $G := \mathfrak{G}^F$ for a Steinberg endomorphism $F : \mathfrak{G} \to \mathfrak{G}$. Let $g \in G$ be any
element such that $C_G(g) \leq L := \mathcal{L}^F$, where $\mathcal{L}$ is a split Levi subgroup of $G$. Then, for any character $\chi \in \text{Irr}(G)$ and $\alpha := \alpha(L)$, we have

$$|\chi(g)| \leq f(r)\chi(1)^{\alpha}.$$ 

The $\alpha$-bound in Theorem 2.5.1 is sharp in many cases; for instance, it is always optimal in the case $G = \text{SL}_n(q)$, see Bezrukavnikov, Liebeck, Shalev, and Tiep [n.d., Theorem 1.3]. Furthermore, the function $f(r)$ is given explicitly in Bezrukavnikov, Liebeck, Shalev, and Tiep [ibid., Proposition 2.7]. Explicit bounds for $\alpha(L)$ can be found in Bezrukavnikov, Liebeck, Shalev, and Tiep [ibid.]; in particular, it is shown in Bezrukavnikov, Liebeck, Shalev, and Tiep [ibid., Theorem 1.6] that

$$\alpha(L) \leq \alpha(\mathcal{L}) \leq \frac{1}{2} \left( 1 + \frac{\dim \mathcal{L}}{\dim G} \right)$$

if $G$ is a classical group. As a consequence, the following Lie-theoretic analogue of the celebrated Fomin–Lulov bound Fomin and Lulov [1995] was obtained in Bezrukavnikov, Liebeck, Shalev, and Tiep [n.d.]:

**Corollary 2.5.2.** Let $m < n$ be a divisor of $n$ and let $L \leq G = \text{GL}_n(q)$ be a Levi subgroup of the form $L = \text{GL}_n/m(q)^m$. Let $g \in G$ with $C_G(g) \leq L$. Then we have

$$|\chi(g)| \leq f(n-1)\chi(1)^{\frac{1}{m}}$$

for all $\chi \in \text{Irr}(G)$, where $f : \mathbb{N} \to \mathbb{N}$ is the function specified in Theorem 2.5.1.

Again, the exponent $1/m$ in Corollary 2.5.2 is sharp. Moreover, an exponential character bound for $\ell$-Brauer characters of $G = \text{GL}_n(q)$, $\text{SL}_n(q)$ (in the case $\ell \nmid q$ and for the elements $g \in G$ with $C_G(g)$ contained in a split Levi subgroup of $G$), has also been established in Bezrukavnikov, Liebeck, Shalev, and Tiep [ibid.].

The above results do not cover, for instance, the case where $g \in G^F$ is a unipotent element. However, a complete result covering all elements in $\text{GL}_n(q)$ and $\text{SL}_n(q)$ has been obtained in Bezrukavnikov, Liebeck, Shalev, and Tiep [ibid.]:

**Theorem 2.5.3.** There is a function $h : \mathbb{N} \to \mathbb{N}$ such that the following statement holds. For any $n \geq 5$, any prime power $q$, any irreducible complex character $\chi$ of $G := \text{GL}_n(q)$ or $\text{SL}_n(q)$, and any non-central element $g \in G$,

$$|\chi(g)| \leq h(n) \cdot \chi(1)^{1-\frac{1}{2n}}.$$ 

There is also a different approach to Problem 1.3, which so far has been worked out completely for groups of type $A$ in Guralnick, Larsen, and Tiep [n.d.]. It has long been
observed that irreducible characters of symmetric groups and of finite groups of Lie type seem to appear in “clusters”, where the characters in a given cluster have roughly the same degree (as a polynomial function of $n$ in the case of $S_n$, and of $q^r$ in the case of a Lie-type group of rank $r$ over $\mathbb{F}_q$), and display roughly the same behavior in several contexts. The main goal of this approach is to develop the concept of character level – the characters $\chi \in \text{Irr}(G)$ will then be grouped in clusters according to their level, and then prove exponential character bounds for characters (at least of not-too-large level).

Let us use the notation $GL^\epsilon$ to denote $GL$ when $\epsilon = +$ and $GU$ when $\epsilon = -$, and similarly for $SL^\epsilon$. Let $V = \mathbb{F}_Q^n$ be the natural module of $G \in \{GL^\epsilon_n(q), SL^\epsilon_n(q)\}$, where $Q = q$ when $\epsilon = +$, and $Q = q^2$ when $\epsilon = -$. It is known that the class function

$$\tau : g \mapsto \epsilon^n(\epsilon q)^{\dim_{\mathbb{F}_Q} \text{Ker}(g \cdot \nu)}$$

is a (reducible) character of $G$. The true level $l^*(\chi)$ of a character $\chi \in \text{Irr}(G)$ is then defined to be the smallest non-negative integer $j$ such that $\chi$ is an irreducible constituent of $\tau^j$; and the level $l(\chi)$ is the smallest non-negative integer $j$ such that $\lambda \chi$ is an irreducible constituent of $\tau^j$ for some character $\lambda$ of degree 1 of $G$, see Guralnick, Larsen, and Tiep [ibid.].

**Theorem 2.5.4.** Guralnick, Larsen, and Tiep [ibid.] Let $G \in \{GL^\epsilon_n(q), SL^\epsilon_n(q)\}$ with $n \geq 2$, $\epsilon = \pm$, and let $\chi \in \text{Irr}(G)$ have level $j = l(\chi)$. Then the following statements hold.

(i) $q^{j(n-j)}/2(q + 1) \leq \chi(1) \leq q^{nj}$. If furthermore $j \geq n/2$, then

$$\chi(1) > q^{n^2/4-2}/(q - \epsilon).$$

(ii) If $n \geq 7$ and $\lceil (1/n) \log_q \chi(1) \rceil < \sqrt{n-1} - 1$, then

$$l(\chi) = \left\lfloor \frac{\log_q \chi(1)}{n} \right\rfloor.$$

(iii) If $l(\chi) \leq \sqrt{8n-17)/12 - 1/2}$ for $\chi \in \text{Irr}(G)$, then $|\chi(g)| < 2.43\chi(1)^{1-1/n}$ for all $g \in G \setminus \mathbb{Z}(G)$. Moreover, if $l(\chi) \leq (\sqrt{12n-59} - 1)/6$ for $\chi \in \text{Irr}(G)$, then

$$|\chi(g)| < 2.43\chi(1)^{\max(1-1/2l(\chi),1-\text{supp}(g)/n)}$$

for all $g \in G$.

(iv) Suppose that $g \in G$ satisfies $|C_{GL^\epsilon_n(q)}(g)| \leq q^{n^2/12}$. Then $|\chi(g)| \leq \chi(1)^{8/9}$. 

Note that the exponent $1 - 1/n$ in the character bound in Theorem 2.5.4(iii) is optimal. Another feature of character level is provided by the following result, which shows that the characters of level $j < n/2$ of $\text{SL}_n^\varepsilon(q)$ are controlled by $\text{GL}_j^\varepsilon(q)$:

**Theorem 2.5.5.** Guralnick, Larsen, and Tiep [n.d.] For any $0 \leq j \leq n$, there is a canonical bijection $\alpha \mapsto \Theta(\alpha)$ between $\{\alpha \in \text{Irr}(\text{GL}_n^\varepsilon(q)) \mid I^*(\alpha) \geq 2j - n\}$ and $\{\chi \in \text{Irr}(\text{GL}_n^\varepsilon(q)) \mid I^*(\chi) = j\}$. If furthermore $j < n/2$, then the map $\alpha \mapsto \Theta(\alpha)|_S$ yields a canonical bijection between $\text{Irr}(\text{GL}_n^\varepsilon(q))$ and $\{\theta \in \text{Irr}(S) \mid I(\theta) = j\}$ for $S = \text{SL}_n^\varepsilon(q)$.

### 3 Some Recent Applications

Results on Problems 1.3, 1.4 and other have been used in the revision of the Classification of Finite Simple Groups (for instance, in the classification of quadratic modules), in computational group theory (e.g. in the recognition of permutation/matrix groups of moderate degree). They also played a key role in the proofs Guralnick and Tiep [2005], Guralnick and Tiep [2008] of Larsen’s conjecture on moments Katz [2004, 2005] and the Kollár-Larsen conjecture Balaji and Kollár [2008] on symmetric powers, and the solution Guralnick and Tiep [2012] of the Kollár-Larsen problem Kollár and Larsen [2009] on linear groups generated by elements of bounded deviation and crepant resolutions.

We will now discuss some recent applications in group theory, number theory, and algebraic geometry.

#### 3.1 Automorphy lifting and adequate groups.

For a number field $\mathbb{K}$, let $G_{\mathbb{K}}$ denote the absolute Galois group of $\mathbb{K}$. A key ingredient of Wiles’ celebrated proof of Fermat’s Last Theorem is the following modularity lifting theorem:

**Theorem 3.1.1 (Taylor-Wiles, R. Taylor and Wiles [1995]).** Let $p > 2$, $\mathcal{O}$ be the ring of integers in some finite extension of $\mathbb{Q}_p$, and let $\Phi : G_{\mathbb{Q}} \to \text{GL}_2(\mathcal{O})$ be a Galois representation such that

(i) $\Phi$ “looks like” coming from a modular form;

(ii) The associated $p$-modular representation $\overline{\Phi} : G_{\mathbb{Q}} \to \text{GL}_2(\overline{\mathbb{F}}_p)$ is modular;

(iii) $\overline{\Phi}(G_{\mathbb{Q}} \sqrt{(-1)^{(p-1)/2}p})$ is big.

Then $\Phi$ is modular.

Here, bigness means just irreducibility.

In 2010, Harris, Shepherd-Barron, and R. Taylor [2010] proved the Sato-Tate conjecture for any non-CM elliptic curve over $\mathbb{Q}$ with non-integral $j$-invariant. A key role in this important result is played by an automorphy lifting theorem, due to Clozel, Harris, and
R. Taylor [2008], that generalizes the Taylor-Wiles Theorem 3.1.1 to $GL_n$. Now, \textit{bigness} means irreducibility plus some more conditions, including a condition on the existence of a special element with a special \textit{multiplicity-one} eigenvalue. The Clozel–Harris–Taylor theorem was generalized further by Thorne [2012], removing the multiplicity-one condition, and thus replacing \textit{bigness} by \textit{adequacy}:

\textbf{Definition 3.1.2 (Thorne [2012] and Guralnick, Herzig, and Tiep [2015]).} Let $F$ be a field of characteristic $p$. A finite irreducible subgroup $G \leq GL(V) = GL_n(F)$ is called \textit{adequate}, if

- $H^1(G, F) = 0$;
- $H^1(G, \text{End}(V)/F) = 0$;
- $\text{End}(V)$ is linearly spanned by the $p'$-elements $g \in G$.

Which irreducible subgroups of $GL(V)$ are adequate? Extending Guralnick, Herzig, R. Taylor, and Thorne [2012], and using results on Problem 1.4 as well as Blau and Zhang [1993], the following adequacy theorem has recently been proved:

\textbf{Theorem 3.1.3. Guralnick, Herzig, and Tiep [2015]} Let $G < GL(V)$ be a finite irreducible subgroup and let $O^{p'}(G)$ denote the subgroup of $G$ generated by all $p'$-elements $x \in G$. Suppose that the $O^{p'}(G)$-module $V$ contains an irreducible submodule of dimension $< p$. Then, aside from a few explicitly described examples, $G$ is adequate.

This result has been extended in Guralnick, Herzig, and Tiep [2017] to include finite linear groups in dimension $p$. As a by-product, answers to a question of Serre concerning complete reducibility of subgroups in classical groups of low dimension, and a question of Mazur concerning $\dim \text{Ext}^1(V, V)$ and $\dim \text{Ext}^1(V, V^*)$ (which is of interest in deformation theory), have been obtained.

\textbf{3.2 The $\alpha$-invariant and Thompson’s conjecture.} Let $V = \mathbb{C}^n$ and let $G < GL(V)$ be a finite group. Then $G$ acts on the dual space $V^*$, and a nonzero element $f \in \text{Sym}^k(V^*)$ is said to be an \textit{invariant}, respectively a \textit{semi-invariant}, of degree $k$ for $G$ if $G$ fixes $f$, respectively if $G$ fixes the 1-dimensional space $\langle f \rangle_\mathbb{C}$. Let

\[ d(G) := \min\{k \in \mathbb{N} | G \text{ has a semi-invariant of degree } k\}. \]

In 1981, Thompson proved the following theorem:

\textbf{Theorem 3.2.1. Thompson [1981]} Let $n \in \mathbb{N}$ be any integer and $G < GL_n(\mathbb{C})$ be any finite subgroup. Then $d(G) \leq 4n^2$.

It turns out that this result also has interesting implications in algebraic geometry, in particular, in regard to the $\alpha$-invariant $\alpha_G(\mathbb{P}^{n-1})$ when $G < GL(V)$ acts on the projective space $\mathbb{P}V = \mathbb{P}^{n-1}$.
The $\alpha$-invariant $\alpha_G(X)$ for a compact group $G$ of automorphisms of a Kähler manifold $X$ was introduced by Tian in 1987 Tian [1987], Tian and Yau [1987]. This invariant is of importance in differential geometry and algebraic geometry. As shown by Demailly and Kollár Demailly and Kollár [2001], in the case $X$ is a Fano variety the $\alpha$-invariant coincides with the log-canonical threshold

$$\text{lct}(X, G) = \sup \left\{ \lambda \in \mathbb{Q} \left| \begin{array}{l} \text{the log pair } (X, \lambda D) \text{ has log-canonical singularities} \\ \text{for every } G\text{-invariant effective } \mathbb{Q}\text{-divisor } D \sim_{\mathbb{Q}} -K_X \end{array} \right. \right\}.$$ 

An important example of Fano varieties is the projective space $\mathbb{P}V = \mathbb{P}^{n-1}$, where $V = \mathbb{C}^n$. Consider the natural action of any finite subgroup $G < GL(V)$ on $\mathbb{P}^{n-1}$. Then

$$\alpha_G(\mathbb{P}V) \leq \frac{d(G)}{\dim(V)},$$

see Cheltsov and Shramov [2011, §1], and so Theorem 3.2.1 implies

**Theorem 3.2.2.** Thompson [1981] Let $n \in \mathbb{N}$ be any integer and $G < GL_n(\mathbb{C})$ be any finite subgroup. Then $\alpha_G(\mathbb{P}^{n-1}) \leq 4n$.

In the same paper Thompson [ibid.], Thompson raised (the first part of) the following conjecture:

**Conjecture 3.1 (Thompson).** There is a positive constant $C$ such that for any $n \in \mathbb{N}$ and for any finite subgroup $G < GL_n(\mathbb{C})$, the following statements hold:

(i) $d(G) \leq Cn$; and

(ii) $\alpha_G(\mathbb{P}^{n-1}) \leq C$.

This conjecture has recently been proved in Tiep [2016], relying on Aschbacher’s theorem Aschbacher [1984] and results on Problem 1.4:

**Theorem 3.2.3.** Tiep [2016] Thompson’s Conjecture 3.1 is true, with $C = 1184036$.

This implies

**Corollary 3.2.4.** Let $G \leq GL(V)$ be a finite group. Then $G$ has a nonzero polynomial invariant, of degree at most $\min(1184036 \cdot \dim(V) \cdot \exp(G/G'), |G|)$.

### 3.3 Word maps on simple groups.

The classical Waring problem, solved in 1909 by Hilbert, asks if given any $k \geq 1$, there is a (smallest) $g(k)$ such that every positive integer is a sum of at most $g(k)$ $k^{\text{th}}$ powers. Recently, there has been considerable interest in
non-commutative versions of the Waring problem, particularly for finite simple groups. Here, one asks if given any \( k \geq 1 \), there exists a (smallest) \( f(k) \) such that every element in any finite non-abelian simple group \( G \) is a product of \( f(k) k^{th} \) powers, provided that \( \exp(G) \nmid k \). It was shown by Martinez and Zelmanov [1996] and independently by Saxl and Wilson [1997] that \( f(k) \) exists (but implicitly).

More generally, given a word, i.e. an element \( w(x_1, \ldots, x_d) \) of the free group \( F(x_1, \ldots, x_d) \), and a group \( G \), one considers the word map \( w : G^d \to G \) and defines

\[
    w(G) := \{ w(g_1, \ldots, g_d) \mid g_i \in G \}
\]

to be the image of the word map \( w \) on \( G^d \). Then the non-commutative Waring problem (for simple groups) can be formulated as follows

**Problem 3.2.** *Is there any integer \( c \) (possibly depending on \( w \)) such that

\[
    w(G)^c := \{ y_1 y_2 \ldots y_c \mid y_i \in w(G) \}
\]

equals \( G \), for any finite non-abelian simple group \( G \) with \( w(G) \neq 1 \)?*

Such smallest \( c = c(w) \) is called the *width* of \( w \). Of particular interest is the case where \( w = w(x, y) = x y x^{-1} y^{-1} \), where the assertion \( c(w) = 1 \) is known as the *Ore conjecture* (1951), which is now a theorem:

**Theorem 3.3.1.** *Liebeck, O’Brien, Shalev, and Tiep [2010] Every element in any finite non-abelian simple group is a commutator.*

A particular motivation for Problem 3.2 comes from the celebrated Nikolov–Segal proof of the Serre conjecture on finitely generated profinite groups. The existence of \( c(w) \) was first established in Liebeck and Shalev [2001] (again implicitly). Note that, in general, the width of \( w \) on simple groups can grow unbounded: as shown in Kassabov and Nikolov [2013] and Guralnick and Tiep [2015], for any \( k \in \mathbb{N} \), there is a word \( w \) and a simple group \( S \) such that \( w(S) \neq 1 \) but \( w(S)^N \neq S \). So in Problem 3.2 it is natural to bound the width of \( w \) on *sufficiently large* simple groups. In this asymptotic setting, a breakthrough was achieved by Shalev [2009], where he proved that *for any \( w \neq 1 \), \( w(S)^3 = S \) for all sufficiently large simple groups \( S \).* Building on Shalev [ibid.] and Larsen and Shalev [2008, 2009], the best solution for Problem 3.2 was achieved in Larsen, Shalev, and Tiep [2011]:

**Theorem 3.3.2.** *Larsen, Shalev, and Tiep [ibid.] The following statements hold.*

(i) *For any word \( w \neq 1 \), there exists a constant \( N_w \) depending on \( w \), such that for all finite non-abelian simple groups \( S \) of order greater than \( N_w \) we have \( w(S)^2 = S \).*
(ii) For any two words \( w_1, w_2 \neq 1 \), there exists a constant \( N_{w_1,w_2} \) depending on \( w_1 \) and \( w_2 \) such that for all finite non-abelian simple groups \( S \) of order greater than \( N_{w_1,w_2} \) we have \( w_1(S)w_2(S) = S \).

As regards the Waring problem for quasisimple groups, the best solution has also been achieved:

**Theorem 3.3.3.** *Larsen, Shalev, and Tiep [2013] and Guralnick and Tiep [2015]* The following statements hold.

(i) For any \( w_1, w_2, w_3 \neq 1 \), there exists a constant \( N_{w_1,w_2,w_3} \) depending on \( w_1 \), \( w_2 \), and \( w_3 \) such that for all finite quasisimple groups \( G \) of order greater than \( N_{w_1,w_2,w_3} \) we have \( w_1(G)w_2(G)w_3(G) = G \).

(ii) For any \( w_1, w_2 \neq 1 \), there exists a constant \( N_{w_1,w_2} \) depending on \( w_1 \) and \( w_2 \) such that for all finite quasisimple groups \( G \) of order greater than \( N_{w_1,w_2} \) we have \( w_1(G)w_2(G) \geq G \triangleleft Z(G) \).

The aforementioned results on the Waring problem are mostly asymptotic and non-effective. Recently, effective versions of the main results of Martinez and Zelmanov [1996] and Saxl and Wilson [1997], as well as of Theorem 3.3.2 for power word maps, have been obtained:

**Theorem 3.3.4.** *Guralnick and Tiep [2015]*

(i) Let \( k \geq l \geq 1 \). If \( S \) is any finite simple group of order \( \geq k^{8k^2} \), then every \( g \in S \) can be written as \( x^k \cdot y^l \) for some \( x, y \in S \).

(ii) Let \( k \geq 1 \) and let \( S \) be any finite simple group such that \( \exp(S) \nmid k \). Then any element of \( S \) is a product of at most \( 80k \sqrt{2\log_2 k} + 56k^t \) powers in \( S \).

Also for power word maps, the following result has been proved, which generalizes classical theorems of Burnside and Feit–Thompson:

**Theorem 3.3.5.** *Guralnick, Liebeck, O’Brien, Shalev, and Tiep [n.d.]*

(i) Let \( p, q \) be primes, let \( a, b \) be non-negative integers, and let \( N = p^a q^b \). The word map \( (x, y) \mapsto x^N y^N \) is surjective on all finite non-abelian simple groups.

(ii) Let \( N \) be an odd positive integer. The word map \( (x, y, z) \mapsto x^N y^N z^N \) is surjective on all finite quasisimple groups.

See also Guralnick, Liebeck, O’Brien, Shalev, and Tiep [ibid., Theorems 3–5] for results concerning power word maps \( x \mapsto x^N \) for a general composite integer \( N \).
3.4 Random walks, probabilistic generation, and representation varieties of Fuchsian groups. Let \( G \) be a finite group with a generating set \( S \). Then the corresponding Cayley graph \( \Gamma = \Gamma(G, S) \) has \( G \) as its vertex set and \( \{(g, gs) \mid g \in G, s \in S\} \) as edge set. A random walk on \( \Gamma \) starts from 1, and at each step moves from a vertex \( g \) to \( gs \) chosen according to some probability distribution \( P \) on \( S \). For any \( t \in \mathbb{N} \), let \( P^t(x) \) denote the probability of reaching \( x \in G \) after \( t \) steps. A basic question is how fast \( P^t \) is converging to the uniform distribution \( U \) on \( G \) (i.e. \( U(x) = 1/|G| \) for all \( x \in G \)), in the \( l^1 \)-norm:
\[
||P^t - U|| = \sum_{x \in G} |P^t(x) - U(x)|.
\]
One then defines the mixing time \( T = T(G, S) \) as
\[
T = \min\{t \in \mathbb{N} \mid ||P^t - U|| < 1/e\}.
\]
The study of random walks is pioneered by the influential work of Diaconis. A classical random walk was studied in Diaconis and Shahshahani [1981], where we want to shuffle a deck of \( n \) cards and at each shuffle we swap cards \( i \) and \( j \) with \( i, j \) chosen uniformly at random from \( \{1, 2, \ldots, n\} \), that is, with \( G = S_n \) and \( S = \{(ij) \mid 1 \leq i \neq n\} \). It was shown in Diaconis and Shahshahani [ibid.] that \( T \approx (n \log n)/2 \) for this card shuffle.

We will consider the case where \( S = g^G = \{gzg^{-1} \mid z \in G\} \) and the distribution \( P \) is uniform: \( P(s) = 1/|S| \) for all \( s \in S \). In this case, the “Upper Bound Lemma” of Diaconis and Shahshahani [ibid.] states:

**Lemma 3.4.1.** Suppose \( G \) is generated by \( S = g^G \) and \( P \) is uniform on \( S \). Then for any \( t \in \mathbb{N} \),
\[
||P^t - U||^2 \leq \sum_{1_G \neq \chi \in \text{Irr}(G)} \left( \frac{||\chi(g)||}{\chi(1)} \right)^{2t} \chi(1)^2.
\]

Another tool allowing us to apply character-theoretic methods to these questions is provided by the following analogue of the Riemann zeta function
\[
\zeta^G(s) = \sum_{\chi \in \text{Irr}(G)} \chi(1)^{-s},
\]
first considered by Witten [1991]. Now, sharp bounds on \( \zeta^G(s) \) and exponential character bounds on \( ||\chi(g)|| \) lead to strong results on mixing time \( T(G, g^G) \), see e.g. Larsen and Shalev [2008] for the case of \( S_n \).

**Theorem 3.4.2.** Guralnick, Larsen, and Tiep [n.d.] Let \( G = \text{SL}_n^\epsilon(q) \) with \( \epsilon = \pm \) and \( n \geq 10 \). Suppose that \( g \in G \) is such that \( |C_{\text{GL}_n}(g)| \leq q^{n^2/12} \). Then \( T(G, g^G) \leq 10 \) for \( q \) sufficiently large.
Proof. According to Theorem 2.5.4(iv), $|\chi(g)| \leq \chi(1)^{8/9}$. It then follows by Lemma 3.4.1 that

$$\|P^t - U\|^2 \leq \sum_{1 \neq \chi \in \text{Irr}(G)} \left( \frac{|\chi(g)|}{\chi(1)} \right) \chi(1)^2 \leq \xi^G(2t/9 - 2) - 1.$$

Taking $t \geq 10$, we have $2t/9 - 2 \geq 2/9 > 2/n$, whence $\lim_{q \to \infty} \xi^G(2t/9 - 2) = 1$ by Liebeck and Shalev [2005a, Theorem 1.1], and the result follows.

Similarly, the character bounds in Theorem 2.5.1 imply the following results on mixing time of random walks on quasisimple groups:

**Theorem 3.4.3.** Bezrukavnikov, Liebeck, Shalev, and Tiep [n.d.] Suppose $G$ is a simple algebraic group in good characteristic, and $G = G(q) = \mathfrak{g}^F$ is a finite quasisimple group over $\mathbb{F}_q$. Let $g \in G$ be such that $C_G(g) \leq L$, where $L = \mathfrak{L}^F$ for a split Levi subgroup $\mathfrak{L}$ of $\mathfrak{g}$. Let $r = \text{rank}(\mathfrak{g})$ and let $h = (\dim \mathfrak{g})/r - 1$ be the Coxeter number of $\mathfrak{g}$.

(i) Suppose $\mathfrak{g}$ is of classical type. Then the mixing time

$$T(G, g^G) \leq \min \left\{ r + 2, \left[ (2 + \frac{2}{h}) \cdot \frac{\dim \mathfrak{g}}{\dim \mathfrak{g} - \dim \mathfrak{L}} \right] \right\}$$

for large $q$.

(ii) If $\mathfrak{g}$ is of exceptional type, then $T(G, g^G) \leq 3$ for large $q$.

Using Theorem 2.5.3, we obtain the following result covering all elements of $\text{SL}_n(q)$:

**Corollary 3.4.4.** Bezrukavnikov, Liebeck, Shalev, and Tiep [ibid.] Let $G = \text{SL}_n(q)$ with $n \geq 5$ and let $g$ be an arbitrary non-central element of $G$. Then the mixing time $T(G, g^G) \leq 2n + 3$ for large $q$.

Next we discuss some applications to the study of representation varieties of Fuchsian groups, and also to probabilistic generation of finite simple groups. Recall that Fuchsian groups are finitely generated non-elementary discrete groups of isometries of the hyperbolic plane. Fuchsian groups, which include free groups, the modular group $\text{PSL}_2(\mathbb{Z})$, surface groups, the Hurwitz group and hyperbolic triangle groups, play an important role in geometry, analysis, and algebra. Representation varieties of Fuchsian groups provide a convenient framework to generalize various results on random generation of finite simple groups (e.g. by two random elements, or by elements of orders 2 and 3). An old conjecture of G. Higman (now a theorem thanks to work of Conder, Everitt, and Liebeck and Shalev [2005b]) states that every Fuchsian group surjects onto all large enough alternating groups. Extending this, the following conjecture was raised by Liebeck and Shalev in Liebeck and Shalev [ibid.]:

Proof. According to Theorem 2.5.4(iv), $|\chi(g)| \leq \chi(1)^{8/9}$. It then follows by Lemma 3.4.1 that

$$\|P^t - U\|^2 \leq \sum_{1 \neq \chi \in \text{Irr}(G)} \left( \frac{|\chi(g)|}{\chi(1)} \right) \chi(1)^2 \leq \xi^G(2t/9 - 2) - 1.$$
**Conjecture 3.3.** For any Fuchsian group $\Gamma$ there is an integer $f(\Gamma)$, such that if $G$ is a finite simple classical group of rank at least $f(\Gamma)$, then the probability $P_G(\Gamma)$ that a randomly chosen homomorphism from $\Gamma$ to $G$ is onto tends to 1 as $|G| \to \infty$.

This conjecture was proved in Liebeck and Shalev [ibid.] for oriented Fuchsian groups of genus at least 2 and non-oriented Fuchsian groups of genus at least 3. Our new results on character bounds have allowed us to establish Conjecture 3.3 in various cases that had resisted all attacks so far.

Let $\Gamma$ be a co-compact Fuchsian group of genus $g$ having $d$ elliptic generators of orders $m_1, \ldots, m_d$ (all at least 2). Thus if $\Gamma$ is oriented, it has a presentation of the following form:

$$\langle a_1, b_1, \ldots, a_g, b_g, x_1, \ldots, x_d \mid x_1^{m_1} = \cdots = x_d^{m_d} = 1, x_1 \cdots x_d \prod_{i=1}^{g} [a_i, b_i] = 1 \rangle,$$

and if $\Gamma$ is non-oriented it has a presentation

$$\langle a_1, \ldots, a_g, x_1, \ldots, x_d \mid x_1^{m_1} = \cdots = x_d^{m_d} = 1, x_1 \cdots x_d a_1^2 \cdots a_g^2 = 1 \rangle.$$

The measure of $\Gamma$ is defined to be

$$\mu = \mu(\Gamma) := vg - 2 + \sum_{i=1}^{d} \left(1 - \frac{1}{m_i}\right) > 0,$$

where $v = 2$ if $\Gamma$ is oriented and $v = 1$ otherwise. Let

$$N(\Gamma) := \max \left(\frac{2 + \sum \frac{1}{m_i}}{\mu}, \frac{d + 16}{4(\mu - 2)}, m_1, \ldots, m_d\right) + 1.$$

**Theorem 3.4.5.** Liebeck, Shalev, and Tiep [n.d.] Let $\mathbb{K} = \overline{\mathbb{K}}$ be a field of characteristic not dividing $m_1 \cdots m_d$.

(i) If $\mu > 2$ and $n \geq N(\Gamma)$, then

$$\dim \text{Hom}(\Gamma, \text{GL}_n(\mathbb{K})) = n^2(1 + \mu) - c,$$

where $-1 \leq c \leq \mu + 1 + \sum_{i=1}^{d} m_i$.

(ii) Assume $\mu > v := \max \left(2, 1 + \sum \frac{1}{m_i}\right)$, and define

$$Q := \bigcup_{\text{primes } p} \{q : q = p^a \equiv 1 \pmod{m_i} \ \forall i\}.$$
Then for \( n \geq vN(\Gamma) + 2 \sum m_i \), we have
\[
\lim_{q \to \infty, q \in \mathbb{Q}} P_\Gamma(\text{SL}_n(q)) = 1.
\]

(iii) Let \( G(q) \) denote a simple group of exceptional Lie type over \( \mathbb{F}_q \), and suppose that \( \gcd(m_1 \cdots m_d, 30) = 1 \). Then
\[
\lim_{q \to \infty, q \in \mathbb{Q}, \gcd(q,30)=1} P_\Gamma(G(q)) = 1.
\]

Theorem 3.4.5(iii) implies, for instance, that exceptional groups of Lie type \( G(q) \), with \( q \in \mathbb{Q} \) sufficiently large and \( \gcd(m_1m_2m_3q, 30) = 1 \), are images of the triangle group
\[
T_{m_1,m_2,m_3} = \langle x_1, x_2, x_3 \mid x_1^{m_1} = x_2^{m_2} = x_3^{m_3} = x_1x_2x_3 = 1 \rangle.
\]
Results of this flavor on triangle generation were obtained by completely different methods in Larsen, Lubotzky, and Marion [2014a,b]. Further results concerning other finite groups of Lie type are also obtained in Liebeck, Shalev, and Tiep [n.d.].

References

Roman Bezrukavnikov, Martin W. Liebeck, Aner Shalev, and Pham Huu Tiep (n.d.). “Character bounds for finite groups of Lie type” (cit. on pp. 251, 252, 260).


Alexander S. Kleshchev and Pham Huu Tiep (n.d.). “Irreducible restrictions of representations of symmetric groups in small characteristics”. In preparation (cit. on p. 248).


