Simple groups, interleaved products and conjectures of Gowers and Viola

Aner Shalev
Einstein Institute of Mathematics
The Hebrew University of Jerusalem
Jerusalem 91904
Israel

Abstract

We study the distribution of products of conjugacy classes in finite simple groups. Our results, combined with work of Gowers and Viola, lead to the solution of recent conjectures they posed on interleaved products and related complexity lower bounds, extending their work on the groups $\mathrm{SL}(2,q)$ to all (nonabelian) finite simple groups.

In particular it follows that, if G is a finite simple group, and $A, B \subseteq G^2$ are subsets of fixed positive densities, then, as $a = (a_1, a_2) \in A$ and $b = (b_1, b_2) \in B$ are chosen uniformly, the interleaved product $a \bullet b := a_1 b_1 a_2 b_2$ is almost uniform on G with respect to the ℓ_∞-norm.

It also follows that the communication complexity of an old decision problem related to interleaved products of $a, b \in G^t$ is at least $\Omega(t \log |G|)$ when G is a finite simple group of Lie type of bounded rank, and at least $\Omega(t \log \log |G|)$ when G is any finite simple group. Both these bounds are best possible.

The author acknowledges the support of an Israel Science Foundation grant 1117/13 and of the Vinik Chair of Mathematics which he holds. He also thanks the organizers of the Conway Conference (November 2015) and Princeton University for their hospitality while this work was carried out.

2010 *Mathematics Subject Classification:* 20D06, 03D15, 20P05

1 Introduction

The purpose of this paper is to provide affirmative solutions to some conjectures of Gowers and Viola – see [5, 6, 7]. These papers contain interesting results in Group Theory (interleaved products) and in Computer Science (complexity lower bounds) for the family of two-dimensional special linear groups $\mathrm{SL}(2,q)$. Here we extend these results to all finite simple groups of Lie type of bounded Lie rank, and in a weaker form to all finite simple groups. In fact all our results here also apply (with similar proofs) to all finite quasisimple groups, namely finite perfect groups G such that $G/Z(G)$ is simple.

Throughout this paper simple groups are taken to be nonabelian, and we assume the Classification of finite simple groups. Since our results are of asymptotic nature we may ignore the sporadic groups and restrict our attention to simple groups of Lie type and to alternating groups A_n.

Our main contributions are Theorem 1.1 and Corollary 1.2 below, on the distribution of products of elements from two random conjugacy classes; see also [14, 15] for earlier results in this direction, which are not sufficient for the current applications. The combination of Corollary 1.2 with reductions and statements from [7] yields various applications to interleaved products and complexity, some of which are mentioned briefly in Sections 1 and 3 of this paper.

We start with some notation which we will use throughout this paper. Let G be a finite group and let $x, y, g \in G$. Let $p_{x,y}(g)$ denote the probability that $g = x'y'$, where x' is a random conjugate of x and y' is a random conjugate of y (with respect to the uniform distribution). Then $p_{x,y}$ is a probability distribution on G. Let $||p_{x,y}||_2^2$ denote the square of its ℓ_2-norm, namely

$$||p_{x,y}||_2^2 = \sum_{g \in G} p_{x,y}(g)^2.$$

By $IrrG$ we denote the set of complex irreducible characters of G. We define the Witten zeta function ζ_G of G by

$$\zeta_G(s) = \sum_{\chi \in IrrG} \chi(1)^{-s},$$

where s is a real number. This function plays a key role in our proofs.

Our main theorem below implies that for finite simple groups G, and for almost all $x, y \in G$, the distribution $p_{x,y}$ is very close to uniform in the ℓ_2 sense. For the applications we prove a rather general quantitative result, where x, y need not be independent.

Theorem 1.1 *Let G be a finite simple group. Let ν be a probability distribution on G^2 which projects to uniform distributions on each coordinate. Choose $(x, y) \in G^2$ according to the distribution ν (so that x is uniform in G and so is y, but they are not assumed to be independent).*

(i) If $G = A_n$ then, for some absolute constant c, the ν-probability that $||p_{x,y}||_2^2 \leq |G|^{-1}(1 + cn^{-2/3})$ is greater than $1 - cn^{-2/3}$.

(ii) For any $\epsilon > 0$ there is $r(\epsilon)$ such that if $r \geq r(\epsilon)$ and G is a group of Lie type of rank r over the field with q elements, then the ν-probability that $||p_{x,y}||_2^2 \leq |G|^{-1}(1 + q^{-(2/3-\epsilon)r})$ is greater than $1 - q^{-(2/3-\epsilon)r}$.

(iii) If G is a group of Lie type of rank r, then there exists $c = c(r) > 0$ such that the ν-probability that $||p_{x,y}||_2^2 \leq |G|^{-1}(1 + |G|^{-c})$ is at least $1 - |G|^{-c}$.

We can also show that if G is alternating or a group of Lie type of unbounded rank then part (iii) above does not hold for an absolute constant $c > 0$.

Theorem 1.1 applies in various situations; these include the cases where x, y are uniform and independent, when x is uniform and $y = x$, and more generally, when x is uniform and $y = f(x)$, where $f : G \to G$ is any fixed bijection.

In particular, if we fix $a \in G$ and let f be the bijection sending x to $x^{-1}a$, we obtain the following.

Corollary 1.2 *Let G be a finite simple group, let $a \in G$ be any fixed element, let $x \in G$ distribute uniformly over G and let $y = x^{-1}a$. Then $p_{x,y}$ satisfies the conclusions (i)-(iii) of Theorem 1.1.*

In the case of $G = \mathrm{SL}(2, q)$ this result is proved in [7, 1.13]. It is also stated in [7] that if Corollary 1.2 above holds for a family of finite groups G then these groups satisfy a variety of interesting results, proven earlier only for $\mathrm{SL}(2, q)$. We mention now briefly some of these applications, while some more will be discussed in Section 3.

Recall that for a group G, a positive integer $t \geq 2$, and two t-tuples $a = (a_1, \ldots, a_t), b = (b_1, \ldots, b_t) \in G^t$, the *interleaved product* $a \bullet b$ of a and b is defined by

$$a \bullet b = a_1 b_1 a_2 b_2 \cdots a_t b_t \in G.$$

The density of a subset $A \subseteq G^t$ is defined by $|A|/|G|^t$.

Theorem 1.3 *Let G be a finite simple group and $t \geq 2$ an integer. Let $A, B \subseteq G^t$ be subsets of positive densities α and β respsectively. If a and b are selected uniformly from A and B, then, for each $g \in G$, the probability that $a \bullet b = g$ is of the form $(1 + o(1))|G|^{-1}$.*

In particular, if G is sufficiently large (given α and β), then $A \bullet B = G$.

Here $o(1)$ is a real number tending to 0 as $|G|$ tends to ∞. Thus $a \bullet b$ (for $a \in A$ and $b \in B$) is almost uniformly distributed in the ℓ_∞-norm.

Theorem 1.3 above follows from stronger bounds as follows. Let $\alpha = |A|/|G|^t$ and $\beta = |B|/|G|^t$ be the densities of A and B respectively. If the simple group G above is of Lie type of bounded rank then we obtain

$$|Prob(a \bullet b = g) - |G|^{-1}| \leq (\alpha\beta)^{-1}|G|^{-1-ct},$$

where $c > 0$ depends only on the rank of G. This extends Theorem 1.7 of [6] (which is Theorem 1.8 of [7]) dealing with $\mathrm{SL}(2, q)$.

If G is any simple group of Lie type of rank r (which is not necessarily bounded) we obtain

$$|Prob(a \bullet b = g) - |G|^{-1}| \leq (\alpha\beta)^{-1}q^{-crt}|G|^{-1},$$

where $c > 0$ is an absolute constant.

Finally, if $G = A_n$ then, for some absolute positive constant c we have

$$|Prob(a \bullet b = g) - |G|^{-1}| \leq (\alpha\beta)^{-1}n^{-ct}|G|^{-1}.$$

These results generalize the case when the subsets A, B are product sets, and the related distribution can then be analyzed using Gowers' paper [4] and the paper [1] by Babai, Nikolov and Pyber.

Applications of Corollary 1.2 to certain complexity lower bounds and related conjectures of Gowers and Viola will be described in Section 3 below. In fact Corollary 1.2 also extends additional results from [5, 6, 7], and is likely to have further applications in subsequent works.

We note that while the proofs in [5, 6, 7] avoid representation theory, we use it as our main tool, which sometimes yields shorter proofs of more general results.

Acknowledgment. I am grateful to Tim Gowers for interesting conversations, for sending me the preprint [7] and for asking me about possible extensions to other simple groups.

2 Proof of Theorem 1.1

We need some preparations.

Lemma 2.1 *Let G be a finite group, and $x, y \in G$. Then we have*

$$||p_{x,y}||_2^2 = |G|^{-1} \sum_{\chi \in IrrG} |\chi(x)|^2|\chi(y)|^2/\chi(1)^2.$$

Proof. It is well known that

$$p_{x,y}(g) = |G|^{-1} \sum_{\chi \in IrrG} \chi(x)\chi(y)\chi(g^{-1})/\chi(1).$$

Therefore

$$||p_{x,y}||_2^2 = |G|^{-2} \sum_{g \in G} [\sum_{\chi \in IrrG} \chi(x)\chi(y)\chi(g^{-1})/\chi(1)]^2.$$

This yields

$$||p_{x,y}||_2^2 = |G|^{-2} \sum_{g \in G} \sum_{\chi,\psi \in IrrG} \chi(x)\chi(y)\psi(x)\psi(y)/(\chi(1)\psi(1)) \cdot \chi(g^{-1})\psi(g^{-1}).$$

Changing the order of summation we obtain

$$||p_{x,y}||_2^2 = |G|^{-2} \sum_{\chi,\psi \in IrrG} \chi(x)\chi(y)\psi(x)\psi(y)/(\chi(1)\psi(1)) \cdot \sum_{g \in G} \chi(g^{-1})\psi(g^{-1}),$$

which, by the orthogonality relations, vanishes unless $\psi = \overline{\chi}$, yielding

$$||p_{x,y}||_2^2 = |G|^{-1} \sum_{\chi \in IrrG} |\chi(x)|^2 |\chi(y)|^2 / \chi(1)^2.$$

■

Proposition 2.2 *Let G be a finite simple group. Then*

(i) For a fixed real number $s > 1$ we have $\zeta_G(s) = 1 + o(1)$.

(ii) If G is a group of Lie type and $s > 1$ then there exists $c > 0$ depending only on s and on the rank of G such that $\zeta_G(s) \leq 1 + |G|^{-c}$.

(iii) If $G = A_n$ then for any fixed real number $s > 0$ we have $\zeta_G(s) = 1 + O(n^{-s})$.

(iv) For any fixed real numbers $s, \epsilon > 0$ with $s < 1$ there is $c = c(s, \epsilon)$ such that if G is a group of Lie type of rank r over a field with q elements and $r \geq c$ we have $\zeta_G(s) \leq 1 + q^{-(s-\epsilon)r}$.

Proof. Parts (i) and (iii) are proved in [10, 2.7] for alternating groups.

The proof of part (i) for groups of Lie type (and in fact for all finite quasisimple groups) is given in [11, 1.1].

To prove part(ii), let G be a group of Lie type of rank r over the field with q elements. Let $k(G)$ be the number of conjugacy classes of G. It is known (see [3, 1.1]) that $k(G) \leq c_1 q^r$ for some absolute constant c_1. It is also known (see [9]) that there is an absolute constant $c_2 > 0$ such that

$\chi(1) \geq c_2 q^r$ for every nontrivial character $\chi \in IrrG$. It follows that, for $s > 1$,

$$\zeta_G(s) \leq 1 + c_1 q^r (c_2 q^r)^{-s} \leq 1 + c_3 q^{-r(s-1)},$$

where c_3 depends on s. Since $|G| \leq q^{4r^2}$ this yields

$$\zeta_G(s) \leq 1 + |G|^{-c},$$

where c depends on s and r.

The proof of part (iv) applies arguments from [12]. First note that it suffices to prove part (iv) for classical groups of large rank (since we may choose $r(\epsilon)$ large enough). In the proof of Theorem 1.2 of [12] for unbounded rank, it is shown that, for $s > 0$ we have

$$\zeta_G(s) \leq 1 + c_1 q^{2/s} c_2^{\sqrt{n}} q^{-s(n-1)/2} + c_3 c_4^{-s} q^{-n},$$

where n is the dimension of the natural module for the classical group G, and c_i are absolute constants. Examination of the arguments there shows that the term $q^{-s(n-1)/2}$ may be replaced by q^{-sr} where r is the rank of G.

It easily follows (focusing on the dominant terms) that for any $0 < s < 1$ and $\epsilon > 0$ there exists $c = c(s, \epsilon)$ such that for $r \geq c$ we have

$$\zeta_G(s) \leq 1 + q^{-(s-\epsilon)r}.$$

This completes the proof.

■

We note that parts (iii) and (iv) above are almost best possible, since they show that $\zeta_G(s)$ is well approximated by its two first summands.

Proposition 2.3 *Let G be a finite simple group of Lie type. Then there is a constant $c > 0$ depending only on the rank of G, such that, if x, y distribute uniformly over G (but may be dependent), then*

$$\sum_{\chi \in IrrG} |\chi(x)|^2 |\chi(y)|^2 / \chi(1)^2 \leq 1 + |G|^{-c}$$

holds with probability at least $1 - |G|^{-c}$.

Proof. Let G be of rank r over the field with q elements. It is known that the probability that $x \in G$ is regular semisimple is at least $1 - c_1/q$ for an absolute constant $c_1 > 0$ (see [8] for a more detailed result). Therefore the probability that both x and y are regular semisimple is at least $1 - 2c_1/q$. Note that the this also holds if x, y are dependent.

If $x, y \in G$ are regular semisimple then $|\chi(x)|, |\chi(y)| \leq b$, where b depends only on the rank of G (see e.g. [15, 4.4]). This yields

$$\sum_{1 \neq \chi \in IrrG} |\chi(x)|^2 |\chi(y)|^2 / \chi(1)^2 \leq b^4(\zeta(2) - 1).$$

The result follows using Proposition 2.2(ii).

■

Corollary 2.4 *Let G be a finite simple group. Let x, y distribute uniformly over G (but they may be dependent). Then for almost all $x, y \in G$ we have*

$$\sum_{\chi \in IrrG} |\chi(x)|^2 |\chi(y)|^2 / \chi(1)^2 = 1 + o(1).$$

This result will follow by combining Proposition 2.3 with the stronger quantitative result below.

Proposition 2.5 *Let G be a finite simple group. Let x, y distribute uniformly over G (but they may be dependent).*

(i) If $G = A_n$ then there is an absolute constant c such that the probability that

$$\sum_{\chi \in IrrG} |\chi(x)|^2 |\chi(y)|^2 / \chi(1)^2 \leq 1 + cn^{-2/3}$$

is at least $1 - cn^{-2/3}$.

(ii) If G is a finite simple group of Lie type of rank r over the field with q elements, then the probability that

$$\sum_{\chi \in IrrG} |\chi(x)|^2 |\chi(y)|^2 / \chi(1)^2 \leq 1 + q^{-(2/3-\epsilon)r}$$

is at least $1 - q^{-(2/3-\epsilon)r}$, for any $\epsilon > 0$ and $r \geq r(\epsilon)$.

Proof. In [14, 2.2] it is shown that, for any finite group G, a fixed $s > 0$ and a uniformly distributed $x \in G$, the probability that

$$|\chi(x)| \leq \chi(1)^s$$

for all $\chi \in IrrG$ is greater than $2 - \zeta_G(2s) = 1 - (\zeta_G(2s) - 1)$.

We apply this for $s = 1/3$. It follows that for uniform (possibly dependent) $x, y \in G$, the probability that $|\chi(x)| \leq \chi(1)^{1/3}$ and $|\chi(y)| \leq \chi(1)^{1/3}$ for all $\chi \in IrrG$ is greater than $3 - 2\zeta_G(2/3) = 1 - 2(\zeta_G(2/3) - 1)$. Hence the inequality

$$\sum_{\chi \in IrrG} |\chi(x)|^2 |\chi(y)|^2 / \chi(1)^2 \leq \zeta_G(2/3)$$

holds with probability greater than $3 - 2\zeta_G(2/3)$.

We now apply Proposition 2.2. If $G = A_n$ then by part (iii) of this result we have

$$\zeta_G(2/3) \leq 1 + cn^{-2/3},$$

where c is an absolute constant. Plugging this in the previous probability estimate proves part (i).

Now let G be a group of Lie type of rank r over the field with q elements. Then part (iv) of Proposition 2.2 yields

$$\zeta_G(2/3) \leq 1 + q^{-(2/3-\epsilon)r},$$

for any $\epsilon > 0$ and $r \geq r(\epsilon)$.

Part (ii) follows from this and the above discussion.

■

Note that Corollary 2.4 now follows easily. Indeed, the case of groups of Lie type of bounded rank follows from Proposition 2.3. We may therefore assume that G is alternating of unbounded degree, or of Lie type of unbounded rank, and then the result follows from Proposition 2.5.

Proof of Theorem 1.1: Parts (i) and (ii) of the theorem follow immediately from Lemma 2.1 and Proposition 2.5 above. Part (iii) of the theorem follows from Lemma 2.1 and Proposition 2.3 above.

3 Complexity applications

In this section we briefly describe applications of our main results to complexity lower bounds related to interleaved products. We follow definitions and statements from [5, 6, 7].

Consider the following promise problem introduced in 1984 in [2]. Let G be a finite group and $t \geq 2$ an integer. Suppose Alice receives a t-tuple $a \in G^t$ and Bob receives a t-tuple $b \in G^t$. Suppose we are promised that the interleaved product $a \bullet b \in G$ is one of two given elements $g, h \in G$. The task of Alice and Bob is to decide whether $a \bullet b = g$ or $a \bullet b = h$. What can we say about the communication complexity of this problem?

Recall that $O(n)$ denotes numbers bounded above by cn for some constant c, while $\Omega(n)$ denotes numbers bounded below by cn for some positive constant c.

Note that a trivial upper bound for the communication complexity above is $O(t \log |G|)$. It is shown in [5, 6, 7] that this upper bound is tight for $G = \mathrm{SL}(2, q)$, namely, in this case the communication complexity is at least $\Omega(t \log |G|)$. Corollary 1.2 combined with reductions and statements from [7] extend this as follows.

Theorem 3.1 *The above communication complexity is at least* $\Omega(t \log |G|)$ *whenever* G *is a finite simple group of Lie type of bounded rank.*

For general finite simple groups we obtain the following.

Theorem 3.2 *The above communication complexity is at least* $\Omega(t \log \log |G|)$ *whenever* G *is a finite simple group. If* G *is a finite simple group of Lie type, then the communication complexity is at least* $\Omega(t\sqrt{\log |G|})$.

The first assertion in Theorem 3.2 was conjectured by Gowers and Viola (see [5, 6, 7]). This complexity lower bound is tight for alternating groups (see [13]).

The next result easily implies the complexity bounds in Theorems 3.1 and 3.2; it extends Theorem 1.2 of [6, 7] which deals with $G = \mathrm{SL}(2, q)$.

Theorem 3.3 *Let* G *be a finite simple group and let* $t \geq 2$ *be an integer. Let* $P : G^t \times G^t \to \{0, 1\}$ *be a (randomized public-coin) c-bit communication protocol. For* $g \in G$ *let* p_g *denote the probability that* $P(a, b) = 1$ *assuming* $a \bullet b = g$. *Then for any* $g, h \in G$ *we have*

(i) $|p_g - p_h| \leq 2^c |G|^{-\Omega(t)}$ *if* G *is a group of Lie type of bounded rank.*

(ii) $|p_g - p_h| \leq 2^c q^{-\Omega(rt)}$ *if* G *is a group of Lie type of rank* r.

(iii) $|p_g - p_h| \leq 2^c n^{-\Omega(t)}$ *if* $G = A_n$.

This result follows from Corollary 1.2 combined with statements from [7].

The following is an immediate consequence of Theorem 3.3.

Corollary 3.4 *With the above notation we have* $|p_g - p_h| \leq 2^c (\log |G|)^{-\Omega(t)}$ *for all finite simple groups* G.

This proves Conjecture 1.3 in [6, 7].

References

[1] L. Babai, N. Nikolov and L. Pyber, Product growth and mixing in finite groups, *ACM-SIAM Symp. on Discrete Algorithms (SODA)* (2008), 248–257.

[2] S. Even, A.L. Selman and Y. Yacobi, The complexity of promise problems with applications to public-key cryptography, *Information and Control* **61(2)** (1984), 159–173.

[3] J. Fulman and R. Guralnick, Bounds on the number and sizes of conjugacy classes in finite Chevalley groups with applications to derangements, *Trans. Amer. Math. Soc.* **364** (2012), no. 6, 3023-3070.

[4] W.T. Gowers, Quasirandom groups, *Combinatorics, Probability and Computing* **17** (2008), 363–387.

[5] W.T. Gowers and E. Viola, The communication complexity of interleaved group products, *ACM Symp. on the Theory of Computing (STOC)*, 2015.

[6] W.T. Gowers and E. Viola, The communication complexity of interleaved group products, *Electronic Colloquium on Computational Complexity*, Report No. 44 (2015).

[7] W.T. Gowers and E. Viola, The communication complexity of interleaved group products, Preprint, August 2015.

[8] R.M. Guralnick and F. Lübeck, On p-singular elements in Chevalley groups in characteristic p, *Groups and Computation, III* (Columbus, OH, 1999), 169–182, Ohio State Univ. Math. Res. Inst. Publ., **8**, de Gruyter, Berlin, 2001.

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

[10] M.W. Liebeck and A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), no. 2, 552–601.

[11] M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups and representation varieties, *Invent. Math.* **159** (2005), no. 2, 317–367.

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

[13] E. Miles and E. Viola, Shielding circuits with groups, *ACM Symp. on the Theory of Computing (STOC)*, 2013.

[14] A. Shalev, Mixing and generation in simple groups, *J. Algebra* **319** (2008), no. 7, 3075–3086.

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