ON THE GOWERS TRICK FOR CLASSICAL SIMPLE GROUPS

FRANCESCO FUMAGALLI AND ATTILA MARÓTI

ABSTRACT. If A, B, C are subsets in a finite simple group of Lie type G at least two of which are normal with $|A||B||C|$ relatively large, then we establish a stronger conclusion than $ABC = G$. This is related to a theorem of Gowers and is a generalization of a theorem of Larsen, Shalev, Tiep and the second author and Pyber.

1. INTRODUCTION

Let A, B, C be subsets of a finite group G. Let $\mathrm{Prob}(A, B, C)$ be the probability that if a and b are uniformly and randomly chosen elements from A and B respectively, then $ab \in C$. Recall that a subset of G is normal if it is invariant under conjugation by every element of G.

Theorem 1.1. *There exists a universal constant $\delta > 0$ such that whenever G is a finite simple group of Lie type and whenever A, B, C are subsets in G such that*

(1) at least two of the three subsets A, B, C are normal in G and
(2) $|A||B||C| > |G|^{3-\delta}/\eta^2$ for some given η with $0 < \eta < 1/4$,

then

$$(1-\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A, B, C) < (1+\eta)\frac{|C|}{|G|}$$

and, for any $g \in G$, the number N of triples $(a, b, c) \in A \times B \times C$ such that $abc = g$ satisfies

$$(1-\eta)\frac{|A||B||C|}{|G|} < N < (1+\eta)\frac{|A||B||C|}{|G|}.$$

Larsen, Shalev, Tiep [7, Theorem 7.4] and the second author and Pyber [11, Theorem 1.3] proved that there exists a universal constant $\delta > 0$ such that whenever A, B, C are normal subsets in a finite simple group of Lie type G, each of size at least $|G|^{1-\delta}$, then $ABC = G$. Theorem 1.1 is an improvement of this result. Theorem 1.1 is also related to a theorem of Gowers. See the next section.

2020 *Mathematics Subject Classification.* 20D06, 20D40, 20G05.

Key words and phrases. Gowers trick, simple group, character bounds.

The first author is partially supported by the Italian INdAM-GNSAGA. The second author thanks the hospitality of the Department of Mathematics at the University of Florence. He was also supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K138596, No. K132951 and Grant No. K138828.

2. A theorem of Gowers and the Gowers trick

Let G be a finite group and let A, B, C be subsets of G. As in the Introduction, let $\mathrm{Prob}(A,B,C)$ be the probability that if a and b are uniformly and randomly chosen elements from A and B respectively, then $ab \in C$. Let k be the minimal degree of a non-trivial complex irreducible character of G. Gowers proved the following stronger form of [5, Theorem 3.3], which is implicit in its proof and which may be considered as the main result of [5].

Theorem 2.1 (Gowers). *If $\eta > 0$ is such that $|A||B||C| > |G|^3/\eta^2 k$, then*

$$(1-\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A,B,C) < (1+\eta)\frac{|C|}{|G|}.$$

The Gowers trick was obtained by Nikolov and Pyber [12, Corollary 1]. We state it in the following form.

Theorem 2.2. *If $\eta > 0$ is such that $|A||B||C| > |G|^3/\eta^2 k$, then for any $g \in G$, the number N of triples $(a,b,c) \in A \times B \times C$ such that $abc = g$ satisfies*

$$(1-\eta)\frac{|A||B||C|}{|G|} < N < (1+\eta)\frac{|A||B||C|}{|G|}.$$

In the next paragraph we will show that, in the statement of Theorem 1.1, we may assume that G is a classical simple group $\mathrm{Cl}(n,q)$ where n is the dimension of the natural module for the lift of G over the field of size q unless G is a unitary group when the field has size q^2. Furthermore, we will show that we may also assume that in the statement of Theorem 1.1 this n is sufficiently large.

Let G be a finite simple group of Lie type of rank r. We have $k > |G|^{1/8r^2}$ by [4, Proposition 2.3]. Choose δ to be less than $1/8r^2$. In this case $k > |G|^{\delta}$ and so $|G|^{3-\delta}/\eta^2 > |G|^3/\eta^2 k$ for any given $\eta > 0$. Thus Theorem 1.1 follows from Theorem 2.1 and Theorem 2.2 when r is bounded. Therefore we may assume that r is unbounded, that is, G is a finite simple classical group $\mathrm{Cl}(n,q)$, where n is unbounded.

3. Sets permuted

The aim of this section is to reduce the proof of Theorem 1.1 to the case when A and B are normal in G (see Proposition 3.4).

Let G be an arbitrary group. For arbitrary subsets X, Y, Z of G, let $\mathcal{N}(X,Y,Z)$ be $\{(x,y) \in X \times Y | xy \in Z\}$ and let $X^{-1} = \{x^{-1} | x \in X\}$.

Lemma 3.1. *For arbitrary subsets X, Y, Z of a group G, the three sets $\mathcal{N}(X,Y,Z)$, $\mathcal{N}(Y,Z^{-1},X^{-1})$, $\mathcal{N}(Z^{-1},X,Y^{-1})$ have the same cardinality.*

Proof. Let ϕ_1 be the map from the set $\mathcal{N}(X,Y,Z)$ to the set $\mathcal{N}(Y,Z^{-1},X^{-1})$ defined by $\phi_1(x,y) = (y,(xy)^{-1})$, for every $(x,y) \in \mathcal{N}(X,Y,Z)$. Let ϕ_2 be the map from $\mathcal{N}(Y,Z^{-1},X^{-1})$ to $\mathcal{N}(X,Y,Z)$ defined by $\phi_2(y,z^{-1}) = (zy^{-1},y)$, for every $(y,z^{-1}) \in \mathcal{N}(Y,Z^{-1},X^{-1})$. We claim that both ϕ_1 and ϕ_2 are bijections and that they are inverses of one another. For this it is sufficient to see that the maps

$\phi_2 \circ \phi_1$ and $\phi_1 \circ \phi_2$ are the identity maps on $\mathcal{N}(X, Y, Z)$ and on $\mathcal{N}(Y, Z^{-1}, X^{-1})$ respectively. Indeed, for arbitrary $(x, y) \in \mathcal{N}(X, Y, Z)$, we have

$$(\phi_2 \circ \phi_1)(x, y) = \phi_2(\phi_1(x, y)) = \phi_2((y, (xy)^{-1})) = ((xy)y^{-1}, y) = (x, y)$$

and for arbitrary $(y, z^{-1}) \in \mathcal{N}(Y, Z^{-1}, X^{-1})$, we have

$$(\phi_1 \circ \phi_2)(y, z^{-1}) = \phi_1(\phi_2(y, z^{-1})) = \phi_1((zy^{-1}, y)) = (y, (zy^{-1}y)^{-1}) = (y, z^{-1}).$$

This shows that $\mathcal{N}(X, Y, Z)$ and $\mathcal{N}(Y, Z^{-1}, X^{-1})$ are in bijection.

Finally, to prove that $\mathcal{N}(Y, Z^{-1}, X^{-1})$ is in bijection with $\mathcal{N}(Z^{-1}, X, Y^{-1})$, it is enough to repeat the argument above with (Y, Z^{-1}, X^{-1}) in place of (X, Y, Z). □

A consequence of Lemma 3.1 is the following.

Corollary 3.2. *Let G be a finite group and let A, B, C be non-empty subsets of G. Then*

$$N(B, C^{-1}, A^{-1}) = N(A, B, C) = N(C^{-1}, A, B^{-1}) \tag{1}$$

and

$$\frac{|C|}{|A|} \cdot \mathrm{Prob}(B, C^{-1}, A^{-1}) = \mathrm{Prob}(A, B, C) = \frac{|C|}{|B|} \cdot \mathrm{Prob}(C^{-1}, A, B^{-1}). \tag{2}$$

Proof. Recall that for arbitrary non-empty subsets X, Y, Z in a finite group G, we defined $N(X, Y, Z)$ to be $|\mathcal{N}(X, Y, Z)|$ and $\mathrm{Prob}(X, Y, Z)$ to be $N(X, Y, Z)/|X||Y|$. Conclusion (1) is a direct consequence of Lemma 3.1 and (2) follows from (1). □

We introduce some more notation. Fix $g \in G$. For subsets X, Y, Z of G, set

$$\mathcal{N}(X, Y, Z, g) = \{(x, y, z) \in X \times Y \times Z | xyz = g\}.$$

Lemma 3.3. *Let G be a group, let X, Y, Z be subsets of G and let $g \in G$. Let Z be normal in G. The following hold.*

(i) *The sets $\mathcal{N}(X, Y, Z, g)$ and $\mathcal{N}(X, Z, Y, g)$ have the same cardinality.*
(ii) *If Y is a normal subset in G, then the sets $\mathcal{N}(X, Y, Z, g)$ and $\mathcal{N}(Y, Z, X, g)$ have the same cardinality.*

Proof. (i) Let η_1 be the map from the set $\mathcal{N}(X, Y, Z, g)$ to the set $\mathcal{N}(X, Z, Y, g)$ defined by $\eta_1(x, y, z) = (x, yzy^{-1}, y)$ for every $(x, y, z) \in \mathcal{N}(X, Y, Z, g)$ and let η_2 be the map from $\mathcal{N}(X, Z, Y, g)$ to $\mathcal{N}(X, Y, Z, g)$ defined by $\eta_2(x, z, y) = (x, y, y^{-1}zy)$ for every $(x, z, y) \in \mathcal{N}(X, Z, Y, g)$. We claim that $\eta_2 \circ \eta_1$ is the identity map on $\mathcal{N}(X, Y, Z, g)$ and that $\eta_1 \circ \eta_2$ is the identity map on $\mathcal{N}(X, Z, Y, g)$. For arbitrary $(x, y, z) \in \mathcal{N}(X, Y, Z, g)$, we have

$$\begin{aligned}(\eta_2 \circ \eta_1)(x, y, z) &= \eta_2(\eta_1(x, y, z)) = \eta_2((x, yzy^{-1}, y)) \\ &= (x, y, y^{-1}(yzy^{-1})y) = (x, y, z)\end{aligned}$$

and for arbitrary $(x, z, y) \in \mathcal{N}(X, Z, Y, g)$, we have

$$\begin{aligned}(\eta_1 \circ \eta_2)(x, z, y) &= \eta_1(\eta_2(x, z, y)) = \eta_1((x, y, y^{-1}zy)) \\ &= (x, y(y^{-1}zy)y^{-1}, y) = (x, z, y).\end{aligned}$$

(ii) Let θ_1 be the map from the set $\mathcal{N}(X,Y,Z,g)$ to the set $\mathcal{N}(Y,Z,X,g)$ defined by $\theta_1(x,y,z) = (xyx^{-1}, xzx^{-1}, x)$ for every $(x,y,z) \in \mathcal{N}(X,Y,Z,g)$ and let θ_2 be the map from the set $\mathcal{N}(Y,Z,X,g)$ to the set $\mathcal{N}(X,Y,Z,g)$ defined by $\theta_2(y,z,x) = (x, x^{-1}yx, x^{-1}zx)$ for every $(y,z,x) \in \mathcal{N}(Y,Z,X,g)$. We claim that $\theta_2 \circ \theta_1$ is the identity map on the set $\mathcal{N}(X,Y,Z,g)$ and that $\theta_1 \circ \theta_2$ is the identity map on the set $\mathcal{N}(Y,Z,X,g)$. For arbitrary $(x,y,z) \in \mathcal{N}(X,Y,Z,g)$, we have

$$\begin{aligned}(\theta_2 \circ \theta_1)(x,y,z) &= \theta_2(\theta_1(x,y,z)) = \theta_2((xyx^{-1}, xzx^{-1}, x)) \\ &= (x, x^{-1}(xyx^{-1})x, x^{-1}(xzx^{-1})x) = (x,y,z)\end{aligned}$$

and for arbitrary $(y,z,x) \in \mathcal{N}(Y,Z,X,g)$, we have

$$\begin{aligned}(\theta_1 \circ \theta_2)(y,z,x) &= \theta_1(\theta_2(y,z,x)) = \theta_1((x, x^{-1}yx, x^{-1}zx)) \\ &= (x(x^{-1}yx)x^{-1}, x(x^{-1}zx)x^{-1}, x) = (y,z,x).\end{aligned}$$

□

Note that if G is finite, then $|\mathcal{N}(X,Y,Z,g)| = N(X,Y,gZ^{-1})$.

Proposition 3.4. *If Theorem 1.1 is true in the special case when A and B are normal, then Theorem 1.1 is true in general.*

Proof. Let A, B, C be subsets of G satisfying conditions (1) and (2) of Theorem 1.1. We have two cases to consider: (i) A and C are normal in G and (ii) B and C are normal in G. Observe that if X is a normal set in G then X^{-1} is also normal in G.

If A and C are normal in G, then our hypothesis gives

$$(1-\eta)\frac{|B|}{|G|} < \mathrm{Prob}(C^{-1}, A, B^{-1}) < (1+\eta)\frac{|B|}{|G|}. \tag{3}$$

Applying (2), we deduce that

$$(1-\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A, B, C) < (1+\eta)\frac{|C|}{|G|},$$

which is the first conclusion of Theorem 1.1. Fix g in G. Let $N = |\mathcal{N}(A,B,C,g)|$. This is equal to $N(A,B,gC^{-1})$. By applying our hypothesis to the triple (A,C,B), we deduce that

$$(1-\eta)\frac{|A||B||C|}{|G|} < |\mathcal{N}(A,C,B,g)| < (1+\eta)\frac{|A||B||C|}{|G|}.$$

But

$$|\mathcal{N}(A,C,B,g)| = |\mathcal{N}(A,B,C,g)| = N$$

by Lemma 3.3, and this proves the second conclusion of Theorem 1.1 in this special case.

If B and C are normal in G, then by applying our hypothesis to the triple (B, C^{-1}, A^{-1}) in place of (A,B,C), we deduce that

$$(1-\eta)\frac{|A|}{|G|} < \mathrm{Prob}(B, C^{-1}, A^{-1}) < (1+\eta)\frac{|A|}{|G|}. \tag{4}$$

We get

$$(1-\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A,B,C) < (1+\eta)\frac{|C|}{|G|},$$

by applying (2). Fix $g \in G$. Our hypothesis for the triple (B,C,A) implies that

$$(1-\eta)\frac{|A||B||C|}{|G|} < |\mathcal{N}(B,C,A,g)| < (1+\eta)\frac{|A||B||C|}{|G|}.$$

But

$$|\mathcal{N}(B,C,A,g)| = |\mathcal{N}(A,B,C,g)| = N$$

by Lemma 3.3, and this proves the second conclusion of Theorem 1.1 in this special case too. □

From now on, in order to prove our main result, we may assume that in the statement of Theorem 1.1, A and B are normal.

4. The second conclusion of Theorem 1.1

We claim that the second conclusion of Theorem 1.1 follows from the first. For this we may assume that A and B are normal in G. Fix $g \in G$. The number N of triples $(a,b,c) \in A \times B \times C$ such that $abc = g$ is equal to $N(A,B,gC^{-1})$. Observe that $|gC^{-1}| = |C|$ (and C need not be normal). We get

$$(1-\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A,B,gC^{-1}) < (1+\eta)\frac{|C|}{|G|}$$

by the first conclusion. The second conclusion now follows from the fact that $\mathrm{Prob}(A,B,gC^{-1}) = N(A,B,gC^{-1})/|A||B|$.

From now on, we focus on the first conclusion of Theorem 1.1.

5. Changing Hypothesis (2)

We will show that we may replace Hypothesis (2) of Theorem 1.1 by (2') below. Let A, B, C be subsets in G. Let $\eta > 0$ and let $\delta > 0$ be as in the statement of Theorem 1.1. Hypothesis (2) of Theorem 1.1 states that $|A||B||C|$ is larger than $|G|^{3-\delta}/\eta^2$. This implies that $|A|$, $|B|$, $|C|$ are larger than $|G|^{1-\delta}/\eta^2$. On the other hand, if $|A|$, $|B|$, $|C|$ are larger than $|G|^{1-(\delta/3)}/\eta^2$, then Hypothesis (2) of Theorem 1.1 holds. By changing δ to $\delta/3$, in the rest of the paper we will replace Hypothesis (2) by the following.

(2') The subsets A, B, C have size larger than $|G|^{1-\delta}/\eta^2$.

6. Three conjugacy classes

We will prove Theorem 1.1 in the case when A, B, C are conjugacy classes.

Let G be a finite group and let $\mathrm{Irr}(G)$ be the set of complex irreducible characters of G. For an element $g \in G$ and a character $\chi \in \mathrm{Irr}(G)$, it is useful to bound $|\chi(g)|$ in terms of a fixed power of $\chi(1)$. Such character bounds were first used in the fundamental paper by Diaconis and Shahshahani [2] where they were applied to random walks on symmetric groups. The following is a special case of an important theorem of Guralnick, Larsen, Tiep [6, Theorem 1.3].

Theorem 6.1 (Guralnick, Larsen, Tiep)**.** *There exists a universal constant $\mu > 0$ such that whenever G is a classical simple group and $g \in G$ satisfies $|C_G(g)| \leq |G|^{\mu}$, then $|\chi(g)| \leq \chi(1)^{1/10}$ for every $\chi \in \mathrm{Irr}(G)$.*

Let A, B, C be conjugacy classes of a finite group G and let a, b, c be representatives in A, B, C respectively. We have

$$N(A,B,C) = \frac{|A||B||C|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(a)\chi(b)\overline{\chi(c)}}{\chi(1)} \tag{5}$$

by [1, p. 43-44].

For any positive number x, the well-known Witten zeta function $\zeta^G(x)$ is defined to be $\sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^{-x}$. A special case of an important theorem of Liebeck and Shalev [10, Theorem 1.1] is the following.

Theorem 6.2 (Liebeck, Shalev)**.** *For any sequence of non-abelian finite simple groups $G \neq \mathrm{PSL}(2,q)$ (for any prime power q) and any $x > 2/3$, $\zeta^G(x) \to 1$ as $|G| \to \infty$.*

We are now in the position to prove Theorem 1.1 in the special case when the sets A, B, C are conjugacy classes in G. For this, we may assume that G is a classical simple group $\mathrm{Cl}(n,q)$ where n is sufficiently large and we may replace Hypothesis (2) by (2').

Theorem 6.3. *Let G be a classical simple group $\mathrm{Cl}(n,q)$. Fix $\eta > 0$. There is a δ with $0 < \delta < 1$ such that whenever A, B, C are conjugacy classes of G each of size larger than $|G|^{1-\delta}/\eta^2$, then*

$$(1-\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A,B,C) < (1+\eta)\frac{|C|}{|G|}.$$

Proof. We may choose n large enough by the last paragraph of Section 2. Let μ be as in Theorem 6.1. Let A, B, C be conjugacy classes of G each of size larger than $|G|^{1-\delta}/\eta^2 > |G|^{1-\mu}$ for some δ. As n may be chosen large enough, we may assume that $\zeta^G(7/10) - 1 < \eta$ by Theorem 6.2. Let $a \in A$, $b \in B$ and $c \in C$. We have by

(5) that

$$\begin{aligned}\left|N(A,B,C)-\frac{|A||B||C|}{|G|}\right| &= \frac{|A||B||C|}{|G|}\left|\sum_{1\neq\chi\in\mathrm{Irr}(G)}\frac{\chi(a)\chi(b)\overline{\chi(c)}}{\chi(1)}\right|\\ &\leq \frac{|A||B||C|}{|G|}\sum_{1\neq\chi\in\mathrm{Irr}(G)}\frac{|\chi(a)||\chi(b)||\overline{\chi(c)}|}{|\chi(1)|}\\ &\leq \frac{|A||B||C|}{|G|}\sum_{1\neq\chi\in\mathrm{Irr}(G)}\chi(1)^{-7/10}\\ &= \frac{|A||B||C|}{|G|}(\zeta^G(7/10)-1)\\ &< \frac{|A||B||C|}{|G|}\eta.\end{aligned}$$

The result follows. □

7. Three normal sets

We will prove Theorem 1.1 in the case when the subsets A, B, C are normal.

Lemma 7.1. *Let $G=\mathrm{Cl}(n,q)$. There exists a universal constant c such that*

$$k(G)\leq |G|^{c/n}.$$

Proof. We have $k(G)\leq q^{c_1 n}$ for some universal constant c_1 by [8, Theorem 1.1] (see also [3, Corollary 1.2]). By the order formulas for finite simple classical groups, there exists a universal constant $c_2>0$ such that $|G|=|\mathrm{Cl}(n,q)|\geq q^{c_2n^2}$. We get

$$k(G)\leq q^{c_1n}=\left(q^{c_2n^2}\right)^{c_1/(c_2n)}\leq |G|^{c/n},$$

where $c=c_1/c_2$. □

Lemma 7.2. *Let $G=\mathrm{Cl}(n,q)$. Fix $\eta>0$ and $\delta>0$. Let X be a normal subset of G with $|X|>|G|^{1-\delta}/\eta^2$. For any fixed $\alpha>\delta$, the set X contains a conjugacy class Y of G with $|Y|>|G|^{1-\alpha}/\eta^2$, provided that n is sufficiently large.*

Proof. If no such conjugacy class Y of G is contained in the normal subset X of G, then

$$|G|^{1-\delta}/\eta^2<|X|\leq k(G)|G|^{1-\alpha}/\eta^2\leq |G|^{1+(c/n)-\alpha}/\eta^2$$

by Lemma 7.1. Thus $c/n>\alpha-\delta$. This is a contradiction since c/n tends to 0 as n goes to infinity. □

Let $G=\mathrm{Cl}(n,q)$. Fix η with $0<\eta<1$. Let $\delta>0$ later to be specified. Let A, B, C be normal subsets of G each of size larger than $|G|^{1-\delta}/\eta^2$. Let $X\in\{A,B,C\}$. Let X_1 be the union of all conjugacy classes in G which are contained in X and each of which have size larger than $|G|^{1-\alpha}/\eta^2$ for some fixed $\alpha>\delta$ soon to be determined (in the end of the proof we will require $\delta>0$ to be small and $\alpha>0$ such that $\alpha>3\delta$). Let us call such conjugacy classes large. Since n may be taken to be sufficiently large, the normal set X_1 is non-empty by Lemma 7.2.

Let $K_{a_1}, \dots, K_{a_r}$ be the list of (distinct) large conjugacy classes of G contained in A_1. Similarly, let $K_{b_1}, \dots, K_{b_s}$ be the list of large conjugacy classes of G contained in B_1, and let $K_{c_1}, \dots, K_{c_t}$ be the list of large conjugacy classes of G contained in C_1. Let a_i, b_j, c_l be fixed indices such that $1 \leq i \leq r$, $1 \leq j \leq s$, $1 \leq l \leq t$. There is a choice of $\delta > 0$ in Theorem 6.3 with $\eta/2$ such that

$$(1-(\eta/2))\frac{|K_{a_i}||K_{b_j}||K_{c_l}|}{|G|} < N(K_{a_i}, K_{b_j}, K_{c_l}) < (1+(\eta/2))\frac{|K_{a_i}||K_{b_j}||K_{c_l}|}{|G|}.$$

This immediately implies that

$$(1-(\eta/2))\frac{|A_1||B_1||C_1|}{|G|} < \sum_{i=1}^{r}\sum_{j=1}^{s}\sum_{l=1}^{t} N(K_{a_i}, K_{b_j}, K_{c_l}) < (1+(\eta/2))\frac{|A_1||B_1||C_1|}{|G|}.$$

Since

$$N(A_1, B_1, C_1) = \sum_{i=1}^{r}\sum_{j=1}^{s}\sum_{l=1}^{t} N(K_{a_i}, K_{b_j}, K_{c_l}),$$

it follows that

$$(1-(\eta/2))\frac{|A_1||B_1||C_1|}{|G|} < N(A_1, B_1, C_1) < (1+(\eta/2))\frac{|A_1||B_1||C_1|}{|G|}. \tag{6}$$

For $X_2 = X \setminus X_1$, we have, by Lemma 7.1, that

$$|X_2| \leq k(G)|G|^{1-\alpha}/\eta^2 \leq |G|^{1+(c/n)-\alpha}/\eta^2 \leq \beta|G|^{1-\delta}/\eta^2 < \beta|X| \tag{7}$$

for any fixed $\beta > 0$, provided that n is sufficiently large. It follows that

$$|X_1| > (1-\beta)|X|. \tag{8}$$

Let $i, j, l \in \{1, 2\}$. Observe that $N(A_i, B_j, C_l) \leq |G| \min\{|A_i|, |B_j|, |C_l|\}$. We have

$$N(A, B, C) = \sum_{i=1, j=1, l=1}^{2} N(A_i, B_j, C_l) \leq N(A_1, B_1, C_1) + 7|G| \max\{|A_2|, |B_2|, |C_2|\}.$$

Since $7|G| \max\{|A_2|, |B_2|, |C_2|\} \leq 7|G|^{2+(c/n)-\alpha}/\eta^2$ by (7), it follows from this that

$$N(A_1, B_1, C_1) \leq N(A, B, C) \leq N(A_1, B_1, C_1) + 7|G|^{2+(c/n)-\alpha}/\eta^2. \tag{9}$$

Formulas (9), (6), and (8) give

$$N(A, B, C) \geq N(A_1, B_1, C_1) > (1-(\eta/2))\frac{|A_1||B_1||C_1|}{|G|} > (1-(\eta/2))(1-\beta)^3\frac{|A||B||C|}{|G|}.$$

For $\beta < 1 - (2(1-\eta)/(2-\eta))^{1/3}$, we have $(1-(\eta/2))(1-\beta)^3 > 1-\eta$, that is,

$$N(A, B, C) > (1-\eta)\frac{|A||B||C|}{|G|}. \tag{10}$$

On the other hand, (9) and (6) provide

$$N(A, B, C) < (1+(\eta/2))\frac{|A||B||C|}{|G|} + 7|G|^{2+(c/n)-\alpha}/\eta^2. \tag{11}$$

Now

$$7|G|^{2+(c/n)-\alpha}/\eta^2 \leq |G|^{2-3\delta}/(2\eta) \leq (\eta/2)\frac{|A||B||C|}{|G|}, \tag{12}$$

provided that $\alpha > 3\delta$ and n is sufficiently large. Formulas (11) and (12) give

$$N(A,B,C) < (1+\eta)\frac{|A||B||C|}{|G|}. \tag{13}$$

Finally, (10) and (13) provide (the first conclusion of) Theorem 1.1 in the case when A, B, C are normal subsets in G.

8. Product mixing

For positive numbers ϵ and η, Lifshitz and Marmor [9, Section 2.3] defined a finite group G to be an (ϵ,η)-mixer if for all subsets A, B, C of G with $|A|$, $|B|$, $|C|$ all at least $\epsilon|G|$, we have

$$(1-\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A,B,C) < (1+\eta)\frac{|C|}{|G|}.$$

They also say that G is normally an (ϵ,η)-mixer if the same holds for all such normal subsets A, B, C. (We remark that these properties were defined for $\eta = 0.01$.) Theorem 2.1 implies that the alternating group A_n is an (ϵ,η)-mixer for $\epsilon = Cn^{-1/3}$ where $C = C(\eta)$ is a constant depending only on η. For normal subsets, this result was improved exponentially. The following may be found in [9, Theorem 2.5].

Theorem 8.1 (Lifshitz, Marmor)**.** *For any $\eta > 0$, there exists an absolute constant $c > 0$, such that A_n is normally an $(n^{-cn^{1/3}},\eta)$-mixer.*

It is shown in [9, Theorem 8.1] that Theorem 8.1 is best possible in the sense that there exists an absolute constant C (depending on η) such that A_n is not normally an $(n^{-Cn^{1/3}},\eta)$-mixer.

It would be interesting to extend Theorem 8.1 in the spirit of Theorem 1.1, however with our current method this is not possible.

In the rest of the paper we will work with the following definition.

Definition 8.2. *Let ϵ and η be positive real numbers less than 1. Let $i \in \{1,2,3\}$. The finite group G is an (ϵ,η,i)-mixer if whenever A, B, C are subsets of G each of size at least $\epsilon|G|$ and i of these subsets are normal in G, then*

$$(1-\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A,B,C) < (1+\eta)\frac{|C|}{|G|}.$$

For a positive real number ϵ less than 1 and for a finite group G, let $k_\epsilon(G) \geq 1$ denote the number of conjugacy classes K of G such that $|K| < \epsilon|G|$.

Proposition 8.3. *Let η and ϵ be positive real numbers satisfying the inequalities $\eta < 1/2$ and $\epsilon < \min\{1, \eta \cdot k_\epsilon(G)^{-1}(1-\eta)^{-2}\}$. Let G be a finite group which is an $(\epsilon,\eta,3)$-mixer. Let $\epsilon' = (\epsilon \cdot k_\epsilon(G)/\eta)^{1/2} < 1$. If A, B, C are subsets of G each of size at least $\epsilon'|G|$ with A and B normal in G, then*

$$(1-2\eta)\frac{|C|}{|G|} < \mathrm{Prob}(A,B,C) < (1+2\eta)\frac{|C|}{|G|}.$$

Proof. Let A, B, C be subsets of G each of size at least $\epsilon'|G|$ with A and B normal in G. Since $N(A,B,C) = \sum_{c \in C} N(A,B,\{c\})$, we have

$$\mathrm{Prob}(A,B,C) = \frac{1}{|A||B|} \sum_{c \in C} N(A,B,\{c\}). \tag{14}$$

Let m be the number of conjugacy classes of G. Let the list of conjugacy classes of G be $K_1, \ldots, K_m$ arranged in such a way that the conjugacy classes $K_1, \ldots, K_t$ have sizes at least $\epsilon|G|$ and the conjugacy classes $K_{t+1}, \ldots, K_m$ have sizes less than $\epsilon|G|$. Let K be the union of the conjugacy classes $K_{t+1}, \ldots, K_m$. For each $i \in \{1, \ldots, m\}$, let c_i be an element from K_i.

Since A and B are normal in G, the number $N(A,B,\{c_i\})$ is independent from the choice of c_i in K_i. This gives

$$\sum_{c \in C} N(A,B,\{c\}) = \sum_{i=1}^{m} |C \cap K_i| \cdot N(A,B,\{c_i\}) = \sum_{i=1}^{m} |C \cap K_i| \cdot \frac{N(A,B,K_i)}{|K_i|}. \tag{15}$$

From (14) and (15) we get

$$\begin{aligned} \mathrm{Prob}(A,B,C) &= \frac{1}{|A||B|} \Big(\sum_{i=1}^{m} |C \cap K_i| \cdot \frac{N(A,B,K_i)}{|K_i|} \Big) = \\ &= \frac{1}{|A||B|} \Big(\sum_{i=1}^{t} |C \cap K_i| \cdot \frac{N(A,B,K_i)}{|K_i|} + \sum_{i=t+1}^{m} |C \cap K_i| \cdot \frac{N(A,B,K_i)}{|K_i|} \Big). \end{aligned} \tag{16}$$

Since $N(A,B,K_i) \leq |A||K_i|$ for every i in $\{1, \ldots, m\}$ and $|B|, |C| \geq \epsilon'|G|$, we have

$$\begin{aligned} \frac{1}{|A||B|} \sum_{i=t+1}^{m} |C \cap K_i| \cdot \frac{N(A,B,K_i)}{|K_i|} &\leq \frac{1}{|B|} \sum_{i=t+1}^{m} |C \cap K_i| \\ &\leq \frac{|C \cap K|}{|B|} \leq \frac{|C \cap K|}{\epsilon'|G|} \leq \frac{|K|}{\epsilon'|G|} \\ &\leq \frac{k_\epsilon(G)\epsilon|G|}{\epsilon'|G|} = k_\epsilon(G)(\epsilon/\epsilon') = \eta\epsilon' \\ &\leq \eta \frac{|C|}{|G|}. \end{aligned} \tag{17}$$

Formulas (16) and (17) give

$$0 \leq \mathrm{Prob}(A,B,C) - \Big(\sum_{i=1}^{t} \frac{|C \cap K_i|}{|K_i|} \cdot \mathrm{Prob}(A,B,K_i) \Big) \leq \eta \frac{|C|}{|G|}. \tag{18}$$

Observe that $\epsilon' \geq \epsilon$ (since $k_\epsilon(G) \geq 1 > \eta/(1-\eta)$). Since G is an $(\epsilon, \eta, 3)$-mixer, we have

$$(1-\eta)\frac{|K_i|}{|G|} < \mathrm{Prob}(A,B,K_i) < (1+\eta)\frac{|K_i|}{|G|} \tag{19}$$

for every $i \in \{1, \ldots, t\}$. Inequalities (18) and (19) give the required upper bound

$$\begin{aligned}\mathrm{Prob}(A,B,C) &< (1+\eta)\Big(\sum_{i=1}^{t} \frac{|C \cap K_i|}{|G|}\Big) + \eta\frac{|C|}{|G|}\\ &= (1+\eta)\frac{|C \cap (G \setminus K)|}{|G|} + \eta\frac{|C|}{|G|}\\ &\leq (1+2\eta)\frac{|C|}{|G|}.\end{aligned}$$

Inequalities (18) and (19) also give

$$\begin{aligned}\mathrm{Prob}(A,B,C) &\geq \sum_{i=1}^{t} \frac{|C \cap K_i|}{|K_i|} \cdot \mathrm{Prob}(A,B,K_i)\\ &> (1-\eta)\sum_{i=1}^{t} \frac{|C \cap K_i|}{|G|}\\ &= (1-\eta)\frac{|C \cap (G \setminus K)|}{|G|}\\ &\geq (1-\eta)\Big(\frac{|C|-|K|}{|G|}\Big). \qquad (20)\end{aligned}$$

Since $|K| \leq k_\epsilon(G)\epsilon|G|$, inequality (20) gives

$$\mathrm{Prob}(A,B,C) > (1-\eta)\frac{|C|}{|G|} - (1-\eta)\frac{|K|}{|G|} \geq (1-\eta)\frac{|C|}{|G|} - (1-\eta)k_\epsilon(G)\epsilon. \qquad (21)$$

Since $|C| \geq \epsilon'|G|$, we have $\eta|C|/|G| \geq \eta\epsilon'$. Since $\epsilon' = (\epsilon k_\epsilon(G)/\eta)^{1/2}$, we get $\eta|C|/|G| \geq (\eta\epsilon k_\epsilon(G))^{1/2}$. In view of this and (21), in order to complete the proof of the lemma, it is sufficient to show that $(\eta\epsilon k_\epsilon(G))^{1/2} \geq (1-\eta)k_\epsilon(G)\epsilon$. This inequality is equivalent to the inequality $\epsilon \leq \eta(1-\eta)^{-2}k_\epsilon(G)^{-1}$. But this is part of the conditions of our lemma. □

We deduce the following consequence of Proposition 8.3. This is not needed for the proof of Theorem 1.1.

Theorem 8.4. *Let η and ϵ be positive real numbers satisfying the inequalities $\eta < 1/2$ and $\epsilon < \min\{1, \eta \cdot k_\epsilon(G)^{-1}(1-\eta)^{-2}\}$. Let G be a finite group which is an $(\epsilon,\eta,3)$-mixer. Let $\epsilon' = (\epsilon \cdot k_\epsilon(G)/\eta)^{1/2} < 1$. If a finite group G is an $(\epsilon,\eta,3)$-mixer, then it is also an $(\epsilon',2\eta,2)$-mixer.*

Proof. Let G be an $(\epsilon,\eta,3)$-mixer. Let A, B, C be subsets of G each of size at least $\epsilon'|G|$. Assume that two of the sets A, B, C are normal in G. If A and B are normal in G, then the result follows by Proposition 8.3. Let A and C be normal in G. Then

$$(1-2\eta)\frac{|B^{-1}|}{|G|} < \mathrm{Prob}(C^{-1},A,B^{-1}) < (1+2\eta)\frac{|B^{-1}|}{|G|}$$

by Proposition 8.3. Thus

$$(1-2\eta)\frac{|C|}{|G|} < \frac{|C|}{|B|} \cdot \mathrm{Prob}(C^{-1},A,B^{-1}) < (1+2\eta)\frac{|C|}{|G|}.$$

Since

$$\frac{|C|}{|B|} \cdot \mathrm{Prob}(C^{-1}, A, B^{-1}) = \mathrm{Prob}(A, B, C)$$

by Corollary 3.2, the result follows. Finally, let B and C be normal in G. Then

$$(1-2\eta)\frac{|A^{-1}|}{|G|} < \mathrm{Prob}(B, C^{-1}, A^{-1}) < (1+2\eta)\frac{|A^{-1}|}{|G|}$$

by Proposition 8.3. Thus

$$(1-2\eta)\frac{|C|}{|G|} < \frac{|C|}{|A|} \cdot \mathrm{Prob}(B, C^{-1}, A^{-1}) < (1+2\eta)\frac{|C|}{|G|}.$$

Since

$$\frac{|C|}{|A|} \cdot \mathrm{Prob}(B, C^{-1}, A^{-1}) = \mathrm{Prob}(A, B, C)$$

by Corollary 3.2, the result follows in this case too. The proof is complete. □

9. Proof of Theorem 1.1

In Section 2 we showed that, in order to prove Theorem 1.1, we may assume that G is a finite simple classical group $\mathrm{Cl}(n, q)$ with n large enough. Given η with $0 < \eta < 1/4$ and $\delta > 0$, we may also replace Hypothesis (2) by (2'). In Section 4 we also showed that it is sufficient to establish the first conclusion of Theorem 1.1. We may assume that A and B are normal in G by Proposition 3.4. If C is normal in G, Theorem 1.1 follows from Section 6. In the language of Definition 8.2, G is an $(\epsilon, \eta, 3)$-mixer where $\epsilon = |G|^{-\delta}/\eta^2$. By changing η to $\eta/2$, we also have that G is an $(\epsilon, \eta/2, 3)$-mixer where $\epsilon = 4|G|^{-\delta}/\eta^2$. Finally, assume that C is not normal in G. Observe that $k_\epsilon(G) \geq 1$ since $\epsilon|G| = 4|G|^{1-\delta}/\eta^2 > 1$ for n large enough. We have $k_\epsilon(G) \leq k(G) \leq |G|^{c/n}$ by Lemma 7.1. It follows that

$$\epsilon = 4|G|^{-\delta}/\eta^2 < \min\{1, \eta(1-\eta)^{-2}|G|^{-c/n}\},$$

for any given $\delta > 0$, provided that n is sufficiently large. Now G is an $(\epsilon', \eta, 2)$-mixer by Proposition 8.3, where

$$\epsilon' = (\epsilon \cdot k_\epsilon(G)/\eta)^{1/2} \leq (2/\eta^{3/2})|G|^{((c/n)-\delta)/2}.$$

This is at most $|G|^{-\delta/3}/\eta^2$ provided that n is sufficiently large. In this case the first conclusion of Theorem 1.1 holds with $\delta/3$ in place of δ.

References

[1] Z. Arad, J. Stavi, M. Herzog, Powers and products of conjugacy classes in groups. Lecture Notes in Math., 1112 Springer-Verlag, Berlin, 1985, 6–51.

[2] P. Diaconis, M. Shahshahani, Generating a random permutation with random transpositions. *Z. Wahrsch. Verw. Gebiete* **57** (1981), no. 2, 159–179.

[3] J. Fulman, R. M. 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] N. Gill, L. Pyber, E. Szabó, A generalization of a theorem of Rodgers and Saxl for simple groups of bounded rank. *Bull. Lond. Math. Soc.* **52** (2020), no. 3, 464–471.

[5] T. W. Gowers, Quasirandom groups. *Combin. Probab. Comput.* **17** (2008), no.3, 363–387.

[6] R. M. Guralnick, M. Larsen, P. H. Tiep, Character levels and character bounds for finite classical groups. *Invent. Math.* **235** (2024), no. 1, 151–210.

[7] M. Larsen, A. Shalev, P. H. Tiep, Products of normal subsets. *Trans. Amer. Math. Soc.* **377** (2024), no. 2, 863–885.

[8] M. W. Liebeck, L. Pyber, Upper bounds for the number of conjugacy classes of a finite group. *J. Algebra* **198** (1997), no. 2, 538–562.

[9] N. Lifshitz, A. Marmor, Bounds for Characters of the Symmetric Group: A Hypercontractive Approach. ArXiv:2308.08694.

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

[11] A. Maróti, L. Pyber, A generalization of the diameter bound of Liebeck and Shalev for finite simple groups. *Acta Math. Hungar.* **164** (2021), no. 2, 350–359.

[12] N. Nikolov, L. Pyber, Product decompositions of quasirandom groups and a Jordan type theorem. *J. Eur. Math. Soc. (JEMS)* **13** (2011), no. 4, 1063–1077.

Dipartimento di Matematica e Informatica 'Ulisse Dini', Viale Morgagni 67/A, 50134 Firenze, Italy

Email address: francesco.fumagalli@unifi.it

Hun-Ren Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary

Email address: maroti.attila@renyi.hu