

Ultraproducts of quasirandom groups with small cosocles

Yilong Yang

Communicated by Robert M. Guralnick

Abstract. A D -quasirandom group is a group without any non-trivial unitary representation of dimension less than D . Given a sequence of groups with increasing quasirandomness, it is natural to ask if the ultraproduct will end up with no finite dimensional unitary representation at all. This is not true in general, but we answer this question in the affirmative when the groups in question have uniform small cosocles, i.e., their quotients by small kernels are direct products of finite simple groups.

Two applications of our results are given, one in triangle patterns inside quasirandom groups and one in self-bohrifying groups. Our main tools are some variations of the covering number for groups, different kinds of length functions on groups, and the classification of finite simple groups.

1 Introduction

As an indirect consequence of Kassabov, Lubotzky and Nikolov's paper [12], the following theorem about non-abelian finite simple groups is true.

Theorem 1.1. *An ultraproduct of non-abelian finite simple groups is either finite simple, or has no finite-dimensional unitary representation other than the trivial one.*

Definitions related to ultraproducts are presented in Section 2 for those unfamiliar with them.

In this paper, we shall show that non-abelian finite simple groups are not the only kind of groups exhibiting such behavior. It turns out that such behavior has a very close link to the notion of quasirandom groups, defined by Gowers [7], and the notion of minimally almost periodic groups, defined by von Neumann and Wigner [13]. All representations considered in this paper are over $\mathbb{C}$. We shall informally say that a group is quasirandom when the group is D -quasirandom for some large D .

Definition 1.2. For a positive integer D , a group G is D -quasirandom if it has no non-trivial unitary representation of dimension less than D .

Definition 1.3. An infinite group is *minimally almost periodic* if it has no non-trivial finite dimensional unitary representation.

A group is minimally almost periodic iff it is D -quasirandom for all D . Then it is natural to wonder whether some sort of limit of increasingly quasirandom groups would give us a minimally almost periodic group. One such limit to consider is the ultraproduct.

We will prove the existence of classes of groups with similar results to Theorem 1.1. The main theorem is the following Theorem 1.5.

Definition 1.4. For a group G , we define its *cosocle* $\text{Cos}(G)$ to be the intersection of all maximal normal subgroups of G .

Let n be any positive integer. Let $\mathcal{C}_n$ be the class of groups that are arbitrary direct products (not necessarily finite) of finite quasisimple groups and finite groups G whose cosocles contain at most n conjugacy classes of G .

Theorem 1.5. *For any sequence of groups in $\mathcal{C}_n$ with quasirandom degree going to infinity, their non-principal ultraproducts will be minimally almost periodic.*

Quasirandom groups were first introduced by Gowers to find groups with no large product-free subset. They can be seen as stronger versions of perfect groups.

Example 1.6 (Gowers [7]). (i) A group (not necessarily finite) is 2-quasirandom iff it is perfect. The reason is that a non-perfect group has a non-trivial abelian quotient, which in turn has a non-trivial homomorphism into $U_1(\mathbb{C})$. A perfect group, on the other hand, can only have the trivial homomorphism into the abelian group $U_1(\mathbb{C})$.

- (ii) A finite perfect group with no normal subgroup of index less than n is at least $\sqrt{\log n}/2$ -quasirandom. In fact, using a form of Jordan's theorem [6], a finite perfect group with no normal subgroup of index less than n is at least $c \log n$ -quasirandom for some constant c .
- (iii) In particular, a non-abelian finite simple group G is at least $c \log n$ -quasirandom if it has n elements.
- (iv) Conversely, any D -quasirandom group must have more than $(D - 1)^2$ elements.
- (v) The alternating group A_n is $(n - 1)$ -quasirandom for $n > 5$, and the special linear group $SL_2(F_p)$ is $\frac{p-1}{2}$ -quasirandom for any prime p .

Morally, ultraproducts preserve all local properties at the scale of elements. In particular, all element-wise identities are preserved. But global properties of

a group, like being finite or finitely generated, might be lost after taking ultraproducts. So one may wonder if a non-principal ultraproduct of increasingly quasirandom groups is always minimally almost periodic. In other words, we want to investigate if quasirandomness can be captured by element-wise properties. This turns out to be false. In particular, we have the following counterexample, pointed out by László Pyber.

Example 1.7. We recall that a group G (not necessarily finite) is 2-quasirandom iff G is perfect. We claim that there is a sequence of D_i -quasirandom groups $(G_i)_{i \in \mathbb{Z}^+}$ with $\lim_{i \rightarrow \infty} D_i = \infty$, whose ultraproduct by any non-principal ultrafilter is not even perfect.

Using the construction of Holt and Plesken [11, Lemma 2.1.10], one may construct a finite perfect group $G_{p,n}$ for each prime $p \geq 5$ and positive integer n , such that an element of $G_{p,n}$ cannot be written as a product of less than n commutators, and that the only simple quotient of $G_{p,n}$ is $\mathrm{PSL}_2(\mathbb{F}_p)$, the projective special linear group of 2×2 matrices over the field of p elements. Then by Example 1.6 (ii), for any D , $G_{p,n}$ is D -quasirandom for large enough p .

Let G_i be $G_{p_i,i}$, where $(p_i)_{i \in \mathbb{Z}^+}$ is a strictly increasing sequence of primes. Then G_i is D_i -quasirandom for some D_i with $\lim_{i \rightarrow \infty} D_i = \infty$. Let $g_i \in G_i$ be an element which cannot be written as a product of less than i commutators. Then $g = (g_i)_{i \in \mathbb{N}}$ corresponds to an element of the ultraproduct $G = \prod_{i \rightarrow \omega} G_i$ by any ultrafilter ω . When ω is non-principal, clearly g cannot be written as a product of finite number of commutators in G . So g is not in the commutator subgroup of G , and thus G is not perfect.

However, a recent paper by Bergelson and Tao [3] proved the following theorem, which sheds some new light on this inquiry:

Theorem 1.8 ([3, Theorem 49 (i)]). *The ultraproduct $\prod_{i \rightarrow \omega} \mathrm{SL}_2(\mathbb{F}_{p_i})$ by a non-principal ultrafilter ω is minimally almost periodic.*

Inspired by this, we make the following definitions:

Definition 1.9. A class $\mathcal{F}$ of groups is a *q.u.p. (quasirandom ultraproduct property) class* if for any sequence of groups in $\mathcal{F}$ with quasirandom degree going to infinity, their non-principal ultraproducts will be minimally almost periodic.

Definition 1.10. A class $\mathcal{F}$ of groups is a *Q.U.P. class* if there is an unbounded non-decreasing function $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ such that any ultraproduct of any sequence of D -quasirandom groups in $\mathcal{F}$ is $f(D)$ -quasirandom.

Remark 1.11. A Q.U.P class is automatically a q.u.p. class. It is like an effective version of q.u.p. class, where we are able to keep track of the amount of quasirandomness passed down to the ultraproduct.

In this paper, the proof of Theorem 1.5 in fact shows that the class $\mathcal{C}_n$ is a Q.U.P. class. And we immediately have the following corollary:

Corollary 1.12. *The following classes are Q.U.P.*

- (i) *The class $\mathcal{C}_{QS}$ of finite quasisimple groups.*
- (ii) *The class $\mathcal{C}_{SS}$ of finite semisimple groups.*
- (iii) *The class $\mathcal{C}_{CS(n)}$ of finite groups with at most n conjugacy classes in their cosocles.*

All Q.U.P. classes must have a uniformly bounded commutator width, i.e., every element can be written as a product of uniformly bounded number of commutators. In view of this, the following conjecture was suggested by László Pyber.

Conjecture 1.13. For any integer n , the class of perfect groups with commutator width $\leq n$ (i.e., every element of these groups can be written as a product of at most n commutators) is Q.U.P.

So far, we do not know if there is a non-Q.U.P but q.u.p. class of groups.

Some applications of our results have already been found. In a paper in preparation by Bergelson, Robertson and Zorin-Kranich [2, Theorem 1.12], it is shown that a sufficiently quasirandom group in a q.u.p. class will have many “triangles”. As another application, one may also use our method to find many examples of self-bohrifying groups. Both applications will be explained in Section 8 of this paper.

Here we shall briefly outline the sections of this article:

- (i) A model case of the alternating groups to illustrate the general idea (Section 3).
- (ii) A group with a nice covering property is very quasirandom (Section 4).
- (iii) Covering properties can ignore small cosocles (Section 5).
- (iv) Quasirandom finite quasisimple groups have nice covering properties (Section 6).
- (v) Proof of Theorem 1.5 (Section 7).
- (vi) Applications of our results (Section 8).

2 Definitions relating to ultraproducts

Definition 2.1. A *filter* on $\mathbb{N}$ is a collection ω of subsets of $\mathbb{N}$ such that:

- (i) $\emptyset \notin \omega$,
- (ii) if $X \in \omega$ and $X \subseteq Y$, then $Y \in \omega$,
- (iii) if $X, Y \in \omega$, then $X \cap Y \in \omega$.

An *ultrafilter* is a filter that is maximal with respect to the containment order. A *non-principal ultrafilter* is an ultrafilter that contains no finite subset of $\mathbb{N}$.

Definition 2.2. Given a sequence of groups $(G_i)_{i \in \mathbb{N}}$, let G be their direct product. Given an ultrafilter ω on $\mathbb{N}$, let

$$N := \{g = (g_i)_{i \in \mathbb{N}} \in G : \{i \in \mathbb{N} : g_i = e\} \in \omega\},$$

which is clearly a normal subgroup of G . Then we call G/N the *ultraproduct* of the groups $(G_i)_{i \in \mathbb{N}}$ by ω , denoted by $\prod_{i \rightarrow \omega} G_i$.

Remark 2.1. An ultrafilter ω is principal (i.e., not non-principal) iff we can find an element $n \in \mathbb{N}$ such that for all subsets $A \subseteq \mathbb{N}$, we have $A \in \omega$ iff $n \in A$. In this case, the corresponding ultraproduct of groups $(G_i)_{i \in \mathbb{N}}$ is isomorphic to G_n . Therefore, in practice, the useful ultrafilters are usually non-principal.

The particular choice of ultrafilter is not that important. As long as we fix a non-principal ultrafilter, then all the discussion in the rest of the paper will be true for the ultraproduct of this ultrafilter.

Ultraproducts have an interesting property, given by Łoś' Theorem. Given an ultraproduct $G = \prod_{i \rightarrow \omega} G_i$ for an ultrafilter ω , any first-order statement ϕ in the language of groups is true for G iff it is true for most of the G_i , i.e.,

$$\{i \in \mathbb{N} : \phi \text{ is true for } G_i\} \in \omega.$$

In particular, this implies that behaviors at the scale of elements are preserved. We shall not need Łoś' Theorem in this paper, but it could be used as an alternative to Proposition 7.3.

3 The class of alternating groups

Let A_n denote the alternating group of rank n , and S_n the symmetry group of rank n . We shall show that the class of alternating groups is a Q.U.P. class, as a simple illustration of the general idea to attack Theorem 1.5.

3.1 Quasirandom alternating groups have nice covering properties

Definition 3.1. (i) For any subsets A, B of a group G , we define the product set

$$AB = \{ab \in G : a \in A, b \in B\}.$$

And we define $A^n := \{a_1 a_2 \dots a_n : a_1, \dots, a_n \in A\}$.

- (ii) An element g of a group G is said to have *covering number* K if its conjugacy class $C(g)$ has $C(g)^K = G$.
- (iii) Let m be any positive integer or ∞ . Then an element $g \in G$ has *the covering property* (K, m) if g^i has covering number K for all $1 \leq i \leq m$.
- (iv) A group G has *the covering property* (K, m) if it has an element with the covering property (K, m) .

Remark 3.2. Note that we use A^n to denote the set of elements that can be expressed as products of *exactly* n elements of A . For example, the cyclic group of order 2 has no covering property at all. The identity is always an even power of the generator, while the generator is always an odd power of itself. There is no uniform choice of K where every element is a product of K conjugates of the generator.

Definition 3.3. An even permutation $\sigma \in A_n$ is *exceptional* if its cycles in the cycle decomposition have distinct odd lengths, or equivalently, if its conjugacy class in A_n is different from its conjugacy class in S_n .

Lemma 3.4 (Brenner [4, Lemma 3.05]). *If an even permutation $\sigma \in A_n$ is fixed-point free and non-exceptional, then $A_n = C(\sigma)^4$.*

Proposition 3.5. *For any $m \in \mathbb{Z}^+$, A_n has the covering property $(4, m)$ for large enough n .*

Proof. Pick any odd prime $p > m$, and pick another prime $q > p$.

Since p, q are necessarily coprime, for any large enough integer n , we can find positive integers a, b such that $n = ap + bq$. Let $\sigma \in S_n$ be a permutation composed of a p -cycles and b q -cycles, where all cycles are disjoint.

Since p, q are odd, σ is an even permutation in A_n . Further, for large enough n , a or b can be chosen to be larger than 1, so σ will be non-exceptional. Since σ is also fixed-point free by construction, Lemma 3.4 implies that $A_n = C(\sigma)^4$.

Now clearly σ^i will also have a cycle decomposition of a p -cycles and b q -cycles for all $1 \leq i \leq p-1$, and this implies that $A_n = C(\sigma^i)^4$ for all $1 \leq i \leq p-1$. So A_n has the covering property $(4, p-1)$. Since $p-1 \geq m$, A_n has the covering property $(4, m)$. $\square$

Corollary 3.6. *For any $m \in \mathbb{Z}^+$, any D' -quasirandom alternating group has the covering property $(4, m)$ for large enough D' .*

3.2 Covering properties passes to ultraproducts and implies quasirandomness

Lemma 3.7. *Let G_i be a sequence of groups such that all but finitely many of them have the covering property (K, m) . Then any ultraproduct of them by a non-principal ultrafilter will have the covering property (K, m) .*

Proof. Since non-principal ultraproducts ignore finitely many exceptions in the sequence G_i , without loss of generality we may assume all G_i have the covering property (K, m) .

For each G_i , let g_i be the element of G_i with the covering property (K, m) . Then we claim that in any ultraproduct of G_i , the element represented by the sequence (g_i) would have the covering property (K, m) .

Pick any $1 \leq j \leq m$. Then any element of G_i is a product of conjugates of g_i^j by $a_{i,1}, \dots, a_{i,K} \in G_i$. As a result, any element of the ultraproduct is a product of conjugates of $(g_i)^j$ by $(a_{i,1}), \dots, (a_{i,K})$. Here we use a sequence of elements (a_i) to represent an element in the ultraproduct. $\square$

We now state a special case of Proposition 4.4, proven in Section 4.

Lemma 3.8. *There is a function $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ such that for any $m, K \in \mathbb{Z}^+$ with $m > f(D)K^{D^2}$, any group G (not necessarily finite) with the covering property (K, m) is D -quasirandom.*

Proposition 3.9. *The class of alternating groups is a Q.U.P. class.*

Proof. For any $D \in \mathbb{Z}^+$, find $m > f(D)4^{D^2}$ and find $D' \in \mathbb{Z}$ such that any D' -quasirandom alternating group has the covering property $(4, m)$. Let G be an ultraproduct of D' -quasirandom alternating groups. Then G will also have the covering property $(4, m)$. Then by Lemma 3.8, G is D -quasirandom. $\square$

4 Covering properties imply quasirandomness

This section is devoted to obtaining some element-scale properties that guarantee the quasirandomness of a group.

Definition 4.1. (i) An element g of a group G is said to have *symmetric covering number K* if $C(g)^K C(g^{-1})^K = G$.

- (ii) Let m be a positive integer or ∞ . Then an element $g \in G$ has *the symmetric covering property* (K, m) if g^i has symmetric covering number K for all $1 \leq i \leq m$.
- (iii) A group G has *the symmetric covering property* (K, m) if it has an element $g \in G$ with the symmetric covering property (K, m) .
- (iv) A group G has *the (symmetric) covering property* (K, m) mod N for some normal subgroup N if G/N has the (symmetric) covering property (K, m) .

Definition 4.2. (i) A pair of elements (g_1, g_2) of a group G is said to have *symmetric double covering number* (K_1, K_2) if we have

$$C(g_1)^{K_1} C(g_1^{-1})^{K_1} C(g_2)^{K_2} C(g_2^{-1})^{K_2} = G.$$

- (ii) Let m_1, m_2 be positive integers or ∞ . A pair of elements (g_1, g_2) in G has *the symmetric double covering property* $[(K_1, m_1), (K_2, m_2)]$ if (g_1^i, g_2^j) has symmetric double covering number (K_1, K_2) for all $1 \leq i \leq m_1, 1 \leq j \leq m_2$.
- (iii) A group G has *the symmetric double covering property* $[(K_1, m_1), (K_2, m_2)]$ if it has a pair of elements (g_1, g_2) in G with the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$.
- (iv) A group G has *the symmetric double covering property* $[(K_1, m_1), (K_2, m_2)]$ mod N for some normal subgroup N if G/N has the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$.

Remark 4.3. (i) Suppose $K < K'$. Then an element with covering number K has covering number K' . In general, the (symmetric) covering property (K, m) implies the (symmetric) covering property (K', m') when $K' \geq K, m' \leq m$. A similar statement is also true for the symmetric double covering properties.

- (ii) Any symmetric covering property is always weaker than the corresponding non-symmetric covering property.
- (iii) Any group with the symmetric covering property (K, m) has the symmetric double covering property $[(1, \infty), (K, m)]$. This is easily seen by taking g_1 to be the identity, and taking g_2 to be the element with the symmetric covering property (K, m) .
- (iv) In our definition of the symmetric double covering properties, since $C(g_1)$ and $C(g_2)$ are conjugate invariant subsets of G , they necessarily commute, i.e., $C(g_1)C(g_2) = C(g_2)C(g_1)$. So the order of (K_1, m_1) and (K_2, m_2) does not matter.

- (v) By imitating the definition of the symmetric double covering properties, one can in fact define the symmetric n -tuple covering properties for groups. As n grows larger and larger, the corresponding covering properties will become weaker and weaker. Note that most results throughout this paper would still hold by replacing the symmetric double covering properties by the symmetric n -tuple covering properties, though for our purpose here, the symmetric double covering properties are enough.

The proof of Proposition 4.4 will be the main part of this section. Let us first state the proposition and some corollaries.

Proposition 4.4 (Local criterion for quasirandomness). *There is a function*

$$f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$$

such that, for any $K_1, m_1, K_2, m_2 \in \mathbb{Z}^+$ with $m_i > f(D)K_i^{D^2}$ for $i = 1, 2$, any group G (not necessarily finite) with the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$ is D -quasirandom.

We shall fix this function f from now on.

Corollary 4.5. *For any $K, m \in \mathbb{Z}^+$ with $m > f(D)K^{D^2}$, any group G (not necessarily finite) with the symmetric double covering property (K, m) is D -quasirandom.*

Corollary 4.6. *For any $K, m \in \mathbb{Z}^+$ with $m > f(D)K^{D^2}$, any group G (not necessarily finite) with the covering property (K, m) is D -quasirandom.*

Remark 4.7. We note here that a partial converse, Corollary 7.5, of the above result is true. That is, quasirandomness implies a nice covering property mod cosocle. The proof of this converse will be presented in Section 7.

We shall first explore some geometric structures of $U_D(\mathbb{C})$.

Definition 4.8. The *Hilbert–Schmidt norm* of an n -by- n complex matrix A is

$$\|A\| = \sqrt{\text{Tr}(A^*A)}.$$

Lemma 4.9. *The following statements hold.*

- (i) *The Lie group $U_D(\mathbb{C})$ has a Riemannian metric $d : U_D(\mathbb{C}) \times U_D(\mathbb{C}) \rightarrow \mathbb{R}$ such that $d(A, B) = \|B - A\|$ for all $A, B \in U_D(\mathbb{C})$. The norm here is the Hilbert–Schmidt norm.*

(ii) This metric is bi-invariant in the sense that

$$d(AB, AC) = d(BA, CA) = d(B, C)$$

for all $A, B, C \in U_D(\mathbb{C})$.

(iii) This metric induces a Haar measure, and the volume of $U_D(\mathbb{C})$ under this Haar measure is finite, and

$$\text{vol}(U_D(\mathbb{C})) = \frac{(2\pi)^{D(D+1)/2}}{1!2! \dots (D-1)!}.$$

We shall denote this constant by v_D from now on.

(iv) Under the metric d , $U_D(\mathbb{C})$ has non-negative Ricci curvature everywhere.

(v) There is a function $c : \mathbb{Z}^+ \rightarrow \mathbb{R}^+$, such that a geodesic ball of radius r in $U_D(\mathbb{C})$ will have volume bounded by $c(D)r^{D^2}$. We shall fix this function c from now on.

Proof. These are very standard facts. See, e.g., [14] and [5]. □

Definition 4.10. Let G be any group. A non-negative function $\ell : G \rightarrow \mathbb{R}$ is called a *length function* if it has the following properties:

- (i) $\ell(g) = 0$ iff g is the identity element.
- (ii) ℓ is symmetric, i.e., $\ell(g) = \ell(g^{-1})$ for all $g \in G$.
- (iii) ℓ is conjugate invariant, i.e., $\ell(ghg^{-1}) = \ell(h)$ for all $g, h \in G$.
- (iv) ℓ satisfies the triangle inequality, i.e., $\ell(gh) \leq \ell(g) + \ell(h)$ for all $g, h \in G$.

A *pseudo-length function* is a non-negative function $\ell : G \rightarrow \mathbb{R}$ satisfying (ii), (iii) and (iv) above.

Lemma 4.11. Let G be a group, and suppose $g_1, g_2 \in G$ have symmetric double covering number (K_1, K_2) . Let $\phi : G \rightarrow H$ be any homomorphism and let ℓ be a length function of H . Then for all $g \in G$, we have

$$\ell(\phi(g)) \leq 2K_1\ell(\phi(g_1)) + 2K_2\ell(\phi(g_2)).$$

Proof. For any $g \in G$, g can be written as the product of K_1 conjugates of g_1 , K_1 conjugates of g_1^{-1} , K_2 conjugates of g_2 and K_2 conjugates of g_2^{-1} . So by the triangle inequality and the conjugate invariance of ℓ , we have

$$\begin{aligned} \ell(\phi(g)) &\leq K_1\ell(\phi(g_1)) + K_1\ell(\phi(g_1^{-1})) + K_2\ell(\phi(g_2)) + K_2\ell(\phi(g_2^{-1})) \\ &\leq 2K_1\ell(\phi(g_1)) + 2K_2\ell(\phi(g_2)). \end{aligned} \quad \square$$

Proposition 4.12. The function $\ell : U_D(\mathbb{C}) \rightarrow \mathbb{R}$ defined by $\ell(A) = d(A, I)$ is a length function.

Proof. Let A, B be any unitary matrices.

Positivity: Clearly $\ell(A) = d(A, I) \geq 0$. And we have

$$\ell(A) = 0 \iff d(A, I) = 0 \iff A = I.$$

Symmetry: We have

$$\ell(A) = d(A, I) = d(AA^{-1}, IA^{-1}) = d(I, A^{-1}) = \ell(A^{-1}).$$

Conjugate invariance: We have

$$\ell(BAB^{-1}) = d(BAB^{-1}, I) = d(BA, B) = d(A, I) = \ell(A).$$

Triangle inequality: We have

$$\begin{aligned} \ell(AB) &= d(AB, I) \leq d(AB, B) + d(B, I) \\ &= d(A, I) + d(B, I) = \ell(A) + \ell(B). \end{aligned} \quad \square$$

We shall use ℓ to denote this length function from now on.

Lemma 4.13. *For any $\epsilon > 0$ and any integer $m > v_D/(c(D)\epsilon^{D^2})$, any m points in $U_D(\mathbb{C})$ will have two points with distance smaller than ϵ . Here v_D and $c(D)$ are as in Lemma 4.9.*

Proof. This follows from a volume packing argument.

Since our metric is bi-invariant, each ball of radius $\frac{\epsilon}{2}$ in $U_D(\mathbb{C})$ has the same volume $\text{vol}(B_{\epsilon/2})$. So by our assumption on m , we have

$$m > \frac{v_D}{c(D)\epsilon^{D^2}} \geq \frac{\text{vol}(U_D(\mathbb{C}))}{\text{vol}(B_{\epsilon/2})}.$$

Now for any m points in $U_D(\mathbb{C})$, suppose any two of them have distance larger than ϵ . Then the balls of radius $\frac{\epsilon}{2}$ centered at these m points will be disjoint and contained in $U_D(\mathbb{C})$, which is impossible. So two of the points have distance smaller than ϵ . $\square$

Lemma 4.14. *Any non-trivial cyclic subgroup of $U_D(\mathbb{C})$ contains an element of length larger than $\sqrt{2}$.*

Proof. Let A be any non-trivial element of $U_D(\mathbb{C})$ of finite order. Let $\lambda_1, \dots, \lambda_D$ be its eigenvalues, and, without loss of generality, say $\lambda_1 \neq 1$. Then λ_1 is a primitive n -th root of unity for some n . Replacing A by a proper power of itself, we may assume that λ_1 is an n -th root of unity closest to -1 . Then in particular, $|\lambda_1 - 1| > \sqrt{2}$.

Then we know

$$\ell(A)^2 = \text{Tr}(A - I)^*(A - I) = \sum_{i=1}^D |\lambda_i - 1|^2 \geq |\lambda_1 - 1|^2 > 2.$$

Now suppose A has infinite order. Let $\lambda_1, \dots, \lambda_D$ be its eigenvalues, and without loss of generality say $\lambda_1 \neq 1$. Then λ_1 is an element of infinite order on the unit circle. Replacing A by a proper power of itself, we may assume that λ_1 is arbitrarily close to -1 . Then in particular, $|\lambda_1 - 1| > \sqrt{2}$. Then we are done by the same computation. $\square$

Proof of Proposition 4.4. For any $\epsilon_1, \epsilon_2 > 0$, pick

$$m_1 > \frac{v_D}{c(D)\epsilon_1^{D^2}} \quad \text{and} \quad m_2 > \frac{v_D}{c(D)\epsilon_2^{D^2}}.$$

For any unitary representation $\phi : G \rightarrow \text{U}_D(\mathbb{C})$ of a group G with the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$, we may find elements $g_1, g_2 \in G$ for this symmetric double covering property.

Now consider the points $I, \phi(g_1), \phi(g_1^2), \dots, \phi(g_1^{m_1})$. By Lemma 4.13, since $m_1 > v_D/(c(D)\epsilon_1^{D^2})$, we can find two points with distance less than ϵ_1 . Say $d(\phi(g_1^s), \phi(g_1^t)) < \epsilon_1$ for some $1 \leq s < t \leq m_1$. Then

$$\ell(\phi(g_1^{t-s})) = d(\phi(g_1^{t-s}), I) = d(\phi(g_1^t), \phi(g_1^s)) < \epsilon_1.$$

So we have $\ell(\phi(g_1^i)) < \epsilon_1$ for some $1 \leq i \leq m_1$. Similarly we have $\ell(\phi(g_2^j)) < \epsilon_2$ for some $1 \leq j \leq m_2$.

To sum up, there are elements $g_1^i, g_2^j \in G$ with symmetric double covering number (K_1, K_2) , and $\ell(\phi(g_1^i)) < \epsilon_1, \ell(\phi(g_2^j)) < \epsilon_2$. So by Lemma 4.11, all elements of $\phi(G)$ would have length smaller than $2K_1\epsilon_1 + 2K_2\epsilon_2$.

Now pick ϵ_1, ϵ_2 small enough so that

$$2K_1\epsilon_1 + 2K_2\epsilon_2 \leq \sqrt{2}.$$

(Say $\epsilon_1 \leq \sqrt{2}/(4K_1)$ and $\epsilon_2 \leq \sqrt{2}/(4K_2)$.) Then all elements of $\phi(G)$ would have length at most $\sqrt{2}$. But by Lemma 4.14, this means $\phi(G)$ is trivial.

So, a group with the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$ will be D -quasirandom if $m_1 \geq f(D)K_1^{D^2}$ and $m_2 \geq f(D)K_2^{D^2}$, where

$$f(D) = \frac{v_D}{c(D)}(2\sqrt{2})^{D^2}. \quad \square$$

Remark 4.15. Note that the above argument proves Proposition 4.4 for all groups, not necessarily finite. However, if one only needs to prove Proposition 4.4 for finite groups, and only for the covering property (K, m) , then a group is D -quasirandom

if $\frac{m}{K} \gg$ the length ratio of the longest and the shortest closed geodesics of $U_n(\mathbb{C})$. So one can interpret the optimal value of $\frac{m}{K}$ as a measure of the “shape” of the finite group. The smaller this optimal value is, the “more rounded” the finite group looks like.

5 Covering properties and the cosocle

In this section, we will show that a certain nice covering property mod cosocle is equivalent to a weaker covering property of the whole group.

Lemma 5.1. *Let G be a group, and let N be a normal subgroup of G contained in its cosocle. Let C be a conjugate invariant symmetric subset of G such that $CN = G$. Then for any non-empty conjugate invariant subset $S \subseteq G$, $SC = S$ iff $S = G$.*

Proof. Suppose $SC = S$ and $S \neq G$. Then we have $SC^i = S$ for any positive integer i . So S must contain the subgroup generated by C . Since C is conjugate invariant, the subgroup generated by C is a normal subgroup, and it is a proper normal subgroup since it is contained in $S \neq G$. In particular, C is contained in a maximal normal subgroup M of G .

But since N is in the cosocle, it is contained in M . So

$$CN \subseteq MN = M \subsetneq G.$$

This is a contradiction. □

Proposition 5.2. *Let G be a group with the symmetric double covering property $[(K_1, m_1), (K_2, m_2)] \bmod N$ for a normal subgroup N contained in the cosocle, and suppose that N contains exactly n conjugacy classes of G . Then G has the symmetric double covering property $[((3n-2)K_1, m_1), ((3n-2)K_2, m_2)]$.*

Proof. Find $g_1, g_2 \in G$ such that (g_1N, g_2N) has symmetric double covering number (K_1, K_2) in G/N . Let

$$C := C(g_1)^{K_1} C(g_1^{-1})^{K_1} C(g_2)^{K_2} C(g_2^{-1})^{K_2}.$$

Then by assumption, C is mapped surjectively onto G/N through the quotient map. So $CN = G$.

Now N contains exactly n conjugacy classes of G . I claim that C^{3^t} contains at least $t+1$ conjugacy classes of G in N , which would imply that $C^{3^{n-3}} \supseteq N$. Then $C^{3^{n-2}} \supseteq CN = G$, finishing our proof.

We proceed by induction. As a convention we define C^0 to be $\{e\}$. Then the claim is true when $t = 0$.

Now assume the statement is true for some $t < n$. Then C^{3t} contains $t + 1$ conjugacy classes of G in N . Let them be $C_1, \dots, C_{t+1}$. Then we have

$$C^{3t+1} \supseteq C \left(\bigcup_{i=1}^{t+1} C_i \right).$$

Suppose for contradiction that C^{3t+2} is disjoint from $C(N - \bigcup_{i=1}^{t+1} C_i)$. Then we observe that

$$\begin{aligned} C \left(N - \bigcup_{i=1}^{t+1} C_i \right) &\supseteq CN - C \left(\bigcup_{i=1}^{t+1} C_i \right) \\ &= G - C \left(\bigcup_{i=1}^{t+1} C_i \right) \supseteq G - C^{3t+1}. \end{aligned}$$

So $C^{3t+2} \subseteq C^{3t+1}$. Then Lemma 5.1 implies that $C^{3t+2} = C^{3t+1} = G$. This contradicts the assumption that C^{3t+2} is disjoint from $C(N - \bigcup_{i=1}^{t+1} C_i)$.

So, C^{3t+2} intersects with $C(N - \bigcup_{i=1}^{t+1} C_i)$. Let g be an element in this intersection. Then $g \in CC_{t+2}$ for some conjugacy class C_{t+2} of G in N disjoint from $C_1, \dots, C_{t+1}$. Find $h \in C_{t+2}$ such that $g \in Ch$. Then since C is symmetric, we have $h \in Cg \subseteq C^{3t+3}$. So C^{3t+3} intersects with C_{t+2} . Since C^{3t+3} is conjugate invariant, we conclude that C^{3t+3} contains C_{t+2} .

Finally, since $e \in C$, we see that C^{3t+3} also contains $C_1, C_2, \dots, C_{t+1}$. So C^{3t+3} contains $t + 2$ conjugacy classes of G in N . $\square$

Proposition 5.3. *Let G be a group with the symmetric covering property (K, m) mod N for a normal subgroup N contained in the cosocle, and suppose that N contains exactly n conjugacy classes of G . Then G has the symmetric covering property $((3n - 2)K, m)$.*

Proof. Same strategy as Proposition 5.2. $\square$

6 Quasirandom finite simple groups have nice covering properties

In this section we shall show that, for finite quasisimple groups, large quasirandomness will imply a nice covering property. We shall first deal with finite simple groups of bounded ranks in Section 6.1. Then we shall deal with the case of alternating groups in Section 6.2. Finally, we shall deal with finite simple groups of large ranks by embedding alternating groups into them in Section 6.3. The classification of finite simple groups is used in this section.

Definition 6.1. For a finite quasisimple group G , we define its *rank* $r(G)$ as the following:

- (i) When the only simple quotient of G is abelian or sporadic, then $r(G) = 1$.
- (ii) When the only simple quotient of G is A_n , then $r(G) = n$.
- (iii) When the only simple quotient of G is a group of Lie type, then $r(G)$ is the (twisted) rank of that finite simple group as an algebraic group.

6.1 Finite simple groups of bounded ranks

Lemma 6.2 (Stolz and Thom [15, Proposition 3.8]). *There is a function*

$$K : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$$

such that, in any finite simple group of Lie type of rank $\leq r$, any non-identity element will have covering number $K(r)$.

We shall fix this function $K(r)$ from now on.

Lemma 6.3 (Babai, Goodman and Pyber [1, Proposition 5.4]). *Let k be any positive integer. Then for any finite simple group G , if $|G| \geq k^{k^2}$, then $|G|$ has a prime divisor greater than k .*

Proposition 6.4. *Let G be a finite simple group of rank $\leq r$. For any $m < \infty$, G has the covering property $(K(r), m)$ if G is D -quasirandom for large enough D .*

Proof. By choosing D to be larger than some absolute constant, a D -quasirandom group G cannot be an abelian group, a sporadic group, or an alternating group of rank $\leq r$. So we only need to consider finite simple groups of Lie type.

Recall that any D -quasirandom group must have more than $(D - 1)^2$ elements. For any $m \in \mathbb{Z}^+$, let D be an integer $> 1 + \sqrt{m^2}$. Then all D -quasirandom finite simple groups will have order $> m^{m^2}$, and thus have an element g of prime order $p > m$. Then g^i are non-identity for all $1 \leq i \leq p - 1$. Then Lemma 6.2 states that all these elements have covering number $K(r)$. So G has the covering property $(K(r), m)$. $\square$

Corollary 6.5. *Let G be a finite quasisimple group of rank $\leq r$. For any $m < \infty$, G has the symmetric covering property $(K(r) \max(3r + 1, 34), m)$ if G is D -quasirandom for large enough D .*

Proof. If a quasisimple group is D -quasirandom, then the simple group it covers is D -quasirandom. Therefore, it is enough to show that, if a finite simple group G has the covering property (K, m) , then any perfect central extension G' of it will have the covering property $(K \max(3r + 1, 34), m)$.

Let Z be the center of G' . Then Z will be the cosocle of G' , and the Schur multiplier of the simple group G would provide an upper bound for $|Z|$. Since G has a rank at most r , by going through the list of finite simple groups, its Schur multiplier has a size at most $\max(3r + 1, 34)$. So if G has the covering property (K, m) , Proposition 5.3 implies that G' has the symmetric covering property $(K \max(3r + 1, 34), m)$. $\square$

6.2 Alternating groups

Proposition 6.6. *Let G be a quasisimple group over an alternating group. Then for any $m < \infty$, G has the symmetric covering property $(20, m)$ if G is D -quasirandom for large enough D .*

Proof. If G is D -quasirandom for some large D , then the alternating group it covers must be A_n for some large n . Then Proposition 3.5 implies that A_n has the covering property $(4, m)$. Now when $n > 7$, A_n will have a Schur multiplier of 2. So G has the covering property $(20, m)$. $\square$

6.3 Finite simple groups of large ranks

The goal of this subsection is to prove the following proposition.

Proposition 6.7. *There is an absolute constant K_0 such that for any $m < \infty$, all finite quasisimple groups of ranks $\geq r$ will have the symmetric covering property (K_0, m) for large enough r .*

By the classification of finite simple groups, a finite simple group of rank larger than some absolute constant will have to be a classical finite simple group of Lie type or an alternating group. Any classical finite simple group of Lie type is in one of the following four classes:

- (i) The projective special linear groups $\mathrm{PSL}_n(\mathbb{F}_q)$. For large enough n , $\mathrm{SL}_n(\mathbb{F}_q)$ are their universal perfect central extensions.
- (ii) The projective symplectic groups $\mathrm{PSp}_n(\mathbb{F}_q)$. For large enough n , $\mathrm{Sp}_n(\mathbb{F}_q)$ are their universal perfect central extensions.
- (iii) The projective special unitary groups $\mathrm{PSU}_n(\mathbb{F}_q)$. For large enough n , $\mathrm{SU}_n(\mathbb{F}_q)$ are their universal perfect central extensions.
- (iv) The projective Omega groups $\mathrm{P}\Omega_{2n}^+(\mathbb{F}_q)$, $\mathrm{P}\Omega_{2n}^-(\mathbb{F}_q)$, or $\mathrm{P}\Omega_{2n+1}(\mathbb{F}_q)$. Here $\Omega_n(\mathbb{F}_q)$ are the commutator subgroups of the special orthogonal groups $\mathrm{SO}_n(\mathbb{F}_q)$, and

$$\mathrm{P}\Omega_n(\mathbb{F}_q) = \Omega_n(\mathbb{F}_q) / Z(\Omega_n(\mathbb{F}_q)).$$

The plus or minus signs indicate different quadratic forms used to obtain the groups in even dimensions. For large enough n , $\Omega_n(\mathbb{F}_q)$ are the universal perfect central extensions of $\mathrm{P}\Omega_n(\mathbb{F}_q)$.

The above statements can be found in any standard textbook in classical groups (e.g., see [8]). It is enough to show Proposition 6.7 for $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{Sp}_n(\mathbb{F}_q)$, $\mathrm{SU}_n(\mathbb{F}_q)$, and $\Omega_n(\mathbb{F}_q)$, since they are the universal perfect central extensions of the simple groups they cover, and since the order of the Schur multipliers of these groups are bounded above by a function of r .

We start by analyzing a length function for groups of Lie type over finite fields.

Definition 6.8. Let g be an $n \times n$ matrix over a finite field F . Let

$$m_g := \sup_{a \in F^\times} \dim(\ker(a - g)).$$

Then the *Jordan length* of g is $\ell_J(g) := \frac{n - m_g}{n}$.

Proposition 6.9. Let G be any subgroup of $\mathrm{GL}_n(F)$ for some finite field F . The function ℓ_J on G is a pseudo-length function.

Proof. *Non-negativity:* For any $g \in G$,

$$m_g = \sup_{a \in F^\times} \dim(\ker(a - g)) \leq n.$$

So $\ell_J(g) = \frac{n - m_g}{n} \geq 0$.

Symmetry: For any $g \in G$, any $a \in F^\times$, and any vector $v \in F^n$, we have

$$\begin{aligned} v \in \ker(a - g) &\iff av = gv \\ &\iff g^{-1}v = a^{-1}v \\ &\iff v \in \ker(a^{-1} - g^{-1}). \end{aligned}$$

As a result,

$$m_g = \sup_{a \in F^\times} \dim(\ker(a - g)) = \sup_{a \in F^\times} \dim(\ker(a^{-1} - g^{-1})) = m_{g^{-1}}.$$

So $\ell_J(g) = \ell_J(g^{-1})$.

Conjugate-invariance: For any $g, h \in G$, any $a \in F^\times$, and any vector $v \in F^n$, we have

$$\begin{aligned} v \in \ker(a - g) &\iff av = gv \\ &\iff ahv = (hgh^{-1})hv \\ &\iff hv \in \ker(a - hgh^{-1}). \end{aligned}$$

As a result,

$$m_g = \sup_{a \in F^\times} \dim(\ker(a - g)) = \sup_{a \in F^\times} \dim(\ker(a - hgh^{-1})) = m_{hgh^{-1}}.$$

So $\ell_J(g) = \ell_J(hgh^{-1})$.

Triangle inequality: For any $g, h \in G$, any $a, b \in F^\times$, and any vector $v \in F^n$, we have

$$\begin{aligned} v \in \ker(a - g) \cap \ker(a - abh^{-1}) &\implies gv = av = abh^{-1}v \\ &\implies v \in \ker(abh^{-1} - g). \end{aligned}$$

So we know $\ker(a - g) \cap \ker(a - abh^{-1}) \subseteq \ker(abh^{-1} - g)$. As a result, we have

$$\begin{aligned} m_{gh} &\geq \dim \ker(ab - gh) \\ &\geq \dim \ker(abh^{-1} - g) \\ &\geq \dim(\ker(a - g) \cap \ker(a - abh^{-1})) \\ &\geq \dim(\ker(a - g)) + \dim(\ker(a - abh^{-1})) - n \\ &\geq \dim(\ker(a - g)) + \dim(\ker(b - h)) - n. \end{aligned}$$

Since this is true for all $a, b \in F^\times$, therefore

$$m_g + m_h - n \leq m_{gh}.$$

So $\ell_J(gh) \leq \ell_J(g) + \ell_J(h)$. □

Lemma 6.10. *Given an $n_1 \times n_1$ matrix A over a finite field F , and an $n_2 \times n_2$ matrix B over the same finite field, then $\ell_J(A \oplus B) \geq \frac{n_1}{n_1+n_2} \ell_J(A) + \frac{n_2}{n_1+n_2} \ell_J(B)$.*

Proof. For any $a \in F^\times$, we have

$$\ker(a - A \oplus B) = \ker((a - A) \oplus (a - B)) = \ker(a - A) \oplus \ker(a - B).$$

So $\dim \ker(a - A \oplus B) \leq m_A + m_B$. Since this is true for all $a \in F^\times$, therefore $m_{A \oplus B} \leq m_A + m_B$. So we have

$$\begin{aligned} \ell_J(A \oplus B) &= \frac{n_1 + n_2 - m_{A \oplus B}}{n_1 + n_2} \\ &\geq \frac{n_1 + n_2 - m_A - m_B}{n_1 + n_2} \\ &\geq \frac{n_1 - m_A}{n_1 + n_2} + \frac{n_2 - m_B}{n_1 + n_2} \\ &\geq \frac{n_1}{n_1 + n_2} \ell_J(A) + \frac{n_2}{n_1 + n_2} \ell_J(B). \end{aligned} \quad \square$$

Lemma 6.11 (Stolz and Thom [15, Lemma 3.11]). *There is an absolute constant c_0 such that for any finite classical quasisimple group of Lie type G , and for any $g \in G \setminus Z(G)$, where $Z(G)$ is the center of G , then $C(g)^K = G$ for all $K \geq \frac{c}{\ell_J(g)}$.*

In short, elements of large Jordan length will automatically have small covering number.

The next step is to identify subgroups of these quasisimple groups of Lie type isomorphic to the alternating groups. A key step is to treat elements in alternating groups as matrices, namely permutation matrices. These are the matrices with exactly one entry of value 1 in each column and in each row, and 0 for all other entries. Such an $n \times n$ matrix will act on the standard orthonormal basis of an n -dimensional vector space by permutation, and thus will provide an embedding of S_n into $\mathrm{GL}_n(F)$ for any field F . Any such matrix is in A_n iff it has determinant 1.

Lemma 6.12. *If P is an $n \times n$ permutation matrix where its cycle decomposition has k cycles, then we have $\ell_J(P) \geq \frac{n-k}{n}$.*

Proof. By cycle decomposition, after a change of basis in the vector space, P will be a direct sum of many cyclic permutation matrices. By Lemma 6.10, it is enough to prove the case when P is a single cycle of length n , and show that $\ell_J(P) \geq \frac{n-1}{n}$.

Since P is a single cycle of length n , its eigenvalues in the algebraic closure of F are precisely all the n -th roots of unity, with multiplicity 1 for each root of unity. So $\dim \ker(a - P) \leq 1$ for all $a \in F^\times$. So $\ell_J(P) \geq \frac{n-1}{n}$. $\square$

Proposition 6.13. *There is an absolute constant K_0 such that, for any $m < \infty$, for any finite quasisimple group of Lie type of $n \times n$ matrices, if it contains A_n as permutation matrices, then it will have the covering property (K_0, m) for large enough n .*

Proof. Let $K_0 > 3c_0$ for the absolute constant c_0 in Lemma 6.11. Then any element A of Jordan length $\geq \frac{1}{3}$ will have covering number K_0 in any finite quasisimple group of Lie type.

Pick any odd prime $p > m$, and pick another prime $q > p$. For any large enough n , we have $n = ap + bq$ for some integers $a > 1$, $0 < b < p + 1$. Then find $\sigma \in A_n$ made up of exactly a p -cycles and b q -cycles, where all cycles are disjoint. This element will be fixed-point free and non-exceptional, and it will have at most $a + b \leq \frac{n}{p} + p$ cycles.

For any finite quasisimple group of Lie type of $n \times n$ matrices, suppose it contains A_n as permutation matrices. Let P be the matrix corresponding to σ . Then

we have

$$\ell_J(P) \geq \frac{n - \frac{n}{p} - p}{n} = 1 - \frac{1}{p} - \frac{p}{n} > \frac{1}{3}.$$

The last inequality follows because $p \geq 3$ and $n \geq 2p + q > 3p$.

So this element will have covering number K_0 in G . It clearly has order pq , and all of its powers coprime to pq will also have the same covering number. So G has the covering property $(K_0, p - 1)$. $\square$

Corollary 6.14. *For any $m < \infty$, all finite special linear groups of rank r for large enough r will have the covering property (K_0, m) . Here K_0 is the absolute constant in Proposition 6.13.*

Proposition 6.15. *There is an absolute constant K_0 , such that for any $m < \infty$, we have the following:*

- (i) *For any finite quasisimple group of Lie type of $2n \times 2n$ matrices, if it contains A_n as $\{P \oplus P : P \in A_n \text{ is a permutation } n \times n \text{ matrix}\}$, then it will have the covering property (K_0, m) for large enough n .*
- (ii) *Let I_1 be the 1×1 identity matrix. For any finite quasisimple group of Lie type of $(2n+1) \times (2n+1)$ matrices, if it contains A_n as $\{P \oplus P \oplus I_1 : P \in A_n \text{ is a permutation } n \times n \text{ matrix}\}$, then it will have the covering property (K_0, m) for large enough n .*
- (iii) *Let I_2 be the 2×2 identity matrix. For any finite quasisimple group of Lie type of $(2n+2) \times (2n+2)$ matrices, if it contains A_n as $\{P \oplus P \oplus I_2 : P \in A_n \text{ is a permutation } n \times n \text{ matrix}\}$, then it will have the covering property (K_0, m) for large enough n .*

Proof. The strategy is identical to Proposition 6.13. Just take $\sigma \oplus \sigma, \sigma \oplus \sigma \oplus I_1$ or $\sigma \oplus \sigma \oplus I_2$ instead of σ , and use Lemma 6.10. $\square$

Definition 6.16. A vector space V is a *non-degenerate formed space* if it has a non-degenerate quadratic form Q (the orthogonal case), or a non-degenerate alternating bilinear form B (the symplectic case), or a non-degenerate Hermitian form B (the unitary case).

Lemma 6.17 (Witt's Decomposition Theorem). *Let V be any non-degenerate formed space over a finite field F . Then we have an orthogonal decomposition $V = W \oplus (\bigoplus_{i=1}^n H_i)$, where W is anisotropic of dimension at most 2, and H_i are hyperbolic planes.*

Proof. These are standard facts in the geometry of classical groups (see [8]). $\square$

Proposition 6.18. *For a non-degenerate formed space, the special isometry group, i.e., the group of isometries of determinant 1, contains an alternating group in one of the ways described by Proposition 6.15.*

Proof. Let V be any finite-dimensional non-degenerate formed space over any finite field F . Then we have an orthogonal decomposition $V = W \oplus H$ with an anisotropic space W of dimension at most 2, and an orthogonal sum of hyperbolic planes $H = \bigoplus_{i=1}^n H_i$.

Then let (v_i, w_i) be a hyperbolic pair generating H_i for each i . For any $\sigma \in A_n$, we can let σ act by permutation on the set $\{v_1, \dots, v_n, w_1, \dots, w_n\}$ such that $\sigma(v_i) = v_{\sigma(i)}$ and $\sigma(w_i) = w_{\sigma(i)}$.

Now clearly $\{v_1, \dots, v_n, w_1, \dots, w_n\}$ is a basis of H . So the above action of σ induces a linear transformation $P \oplus P$ on H , where P is the $n \times n$ permutation matrix for σ . And this $P \oplus P$ is clearly an isometry on H by construction. Now taking the direct sum of $P \oplus P$ on H and the identity matrix on W , we shall obtain our desired embedding of A_n into the full isometry group.

Finally, since P is a permutation matrix for an even permutation, it has determinant 1. Therefore the above embedding of A_n is in the special isometry group. $\square$

Corollary 6.19. *For any $m < \infty$, any finite symplectic or special unitary group of rank r has the covering property (K_0, m) for large enough r . Here K_0 is the absolute constant in Proposition 6.15.*

Corollary 6.20. *For any $m < \infty$, any $\Omega_{2n}^+(\mathbb{F}_q)$, $\Omega_{2n+1}(\mathbb{F}_q)$ or $\Omega_{2n}^-(\mathbb{F}_q)$ has the covering property (K_0, m) for large enough n . Here K_0 is the absolute constant in Proposition 6.15.*

Proof. Embed A_n in $\text{SO}_{2n}^+(q)$, $\text{SO}_{2n}^-(q)$ and $\text{SO}_{2n+1}(q)$ in the ways described by Proposition 6.15. After taking the commutator subgroup, the groups $\Omega_{2n}^+(q)$, $\Omega_{2n}^-(q)$ and $\Omega_{2n+1}(q)$ will still contain A_n through this embedding, because A_n is its own commutator subgroup. So we may apply Proposition 6.15 to $\Omega_{2n}^+(q)$, $\Omega_{2n}^-(q)$ and $\Omega_{2n+1}(q)$ and obtain the desired result. $\square$

Proposition 6.7 is proven by putting Corollary 6.14, Corollary 6.19 and Corollary 6.20 together.

7 Proof of Theorem 1.5

The results of Section 6 can be summarized into the following useful lemma.

Lemma 7.1. *For any integer D and any constant c , we can find integers D' , K_1 , K_2 , m_1 , m_2 such that all D' -quasirandom finite quasisimple groups have the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$ such that $m_1 > cK_1^{D^2}$, $m_2 > cK^{D^2}$.*

Proof. Let K_1 be $\max(20, K_0)$, where the absolute constant K_0 is as in Proposition 6.7. Pick some integer $m_1 > cK_1^{D^2}$. Find large enough r such that, according to Proposition 6.7 and Proposition 6.6, all finite quasisimple groups (including the alternating case) of ranks $\geq r$ will have the symmetric covering property (K_1, m_1) .

Set $K_2 := K(r) \max(3r + 1, 34)$ as in Corollary 6.5, and pick some integer $m_2 > cK_2^{D^2}$. Then for large enough D' , all D' -quasirandom finite quasisimple groups will have the symmetric covering property (K_2, m_2) .

In all cases, a D' -quasirandom finite quasisimple group will have the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$. $\square$

Remark 7.2. In the above proof, one cannot substitute the double covering properties with the covering properties. To have a covering property (K, m) , a finite simple group must either have a large enough rank to accommodate the large m , according to Proposition 6.7, or it must have a small enough rank to accommodate the small K , according to Proposition 6.5. So there might be a gap between the “large enough rank” and the “small enough rank”, where the finite simple subgroups in the gap would fail to have the covering property (K, m) , no matter how quasirandom they are.

In short, the covering properties of finite quasisimple groups are not necessarily uniform. It is uniform when obtained through increasing ranks, and it is uniform when obtained through base fields of increasing sizes. At least with the techniques in this paper, we cannot combine the two uniformities into one. So we must use the double covering properties.

Proposition 7.3. *Let G be a group with the symmetric double covering property for some parameters, and let $(G_i)_{i \in I}$ be an arbitrary family of groups with the symmetric double covering property for some uniform parameters. Then the following are true:*

- (i) *For any normal subgroup N , G has the symmetric double covering property for the same parameters mod N .*
- (ii) *Any quotient group of G has the symmetric double covering property for the same parameters.*
- (iii) *The group $\prod_{i \in I} G_i$ has the symmetric double covering property for the same parameters.*

(iv) As a result of (ii) and (iii), any ultraproduct $\prod_{i \rightarrow \omega} G_i$ has the symmetric double covering property for the same parameters.

Proof. Statements (i), (ii) and (iv) are straightforward.

To see (iii), let $g_{i,1}, g_{i,2} \in G_i$ be the pairs giving G_i the symmetric double covering property. Then we claim that $(g_{i,1})_{i \in I}, (g_{i,2})_{i \in I} \in \prod_{i \in I} G_i$ is the pair giving the desired symmetric double covering property.

For any element $(g_i)_{i \in I} \in \prod_{i \in I} G_i$, then each g_i is in G_i . And by its symmetric double covering property, we know

$$G_i = C(g_{i,1})^{K_1} C(g_{i,1}^{-1})^{K_1} C(g_{i,2})^{K_2} C(g_{i,2}^{-1})^{K_2}.$$

So we can find $a_{i,j}, b_{i,j} \in G_i$ for $i \in I$ and $1 \leq j \leq K_1$, and $c_{i,j}, d_{i,j} \in G_i$ for $i \in I$ and $1 \leq j \leq K_2$, such that

$$\begin{aligned} g_i = & \left(\prod_{1 \leq j \leq K_1} (a_{i,j} g_{i,1} a_{i,j}^{-1}) (b_{i,j} g_{i,1}^{-1} b_{i,j}^{-1}) \right) \\ & \times \left(\prod_{1 \leq j \leq K_2} (c_{i,j} g_{i,2} c_{i,j}^{-1}) (d_{i,j} (g_{i,2})^{-1} d_{i,j}^{-1}) \right). \end{aligned}$$

Since the above identity is true for all $i \in I$, we have

$$\begin{aligned} (g_i)_{i \in I} = & \left(\prod_{1 \leq j \leq K_1} ((a_{i,j})_{i \in I} (g_{i,1})_{i \in I} (a_{i,j})_{i \in I}^{-1}) \right. \\ & \times \left. ((b_{i,j})_{i \in I} (g_{i,1})_{i \in I}^{-1} (b_{i,j})_{i \in I}^{-1}) \right) \\ & \times \left(\prod_{1 \leq j \leq K_2} ((c_{i,j})_{i \in I} (g_{i,2})_{i \in I} (c_{i,j})_{i \in I}^{-1}) \right. \\ & \times \left. ((d_{i,j})_{i \in I} (g_{i,2})_{i \in I}^{-1} (d_{i,j})_{i \in I}^{-1}) \right). \end{aligned}$$

So we have proven (iii). $\square$

Corollary 7.4. Let $\mathcal{C}_{\text{QS}}$ be the class of finite quasisimple groups. Then $\mathcal{C}_{\text{QS}}$ is a Q.U.P. class.

Proof. For any integer D , and for the constant $c = f(D)$ as in Proposition 4.4, we can find D', K_1, K_2, m_1, m_2 as in Lemma 7.1.

Let G_i be a sequence of D' -quasirandom groups in $\mathcal{C}_{\text{QS}}$. Then G_i all have the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$. Then any ultraproduct

$$G = \prod_{i \rightarrow \omega} G_i$$

will have the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$ by Proposition 7.3. Since $m_1 > f(D)K_1^{D^2}$ and $m_2 > f(D)K_2^{D^2}$, G is D -quasirandom by Proposition 4.4. $\square$

Corollary 7.5 (Quasirandomness implies a nice covering property mod cosocle). *For any integer D , and any constant c , we can find integers D', K_1, K_2, m_1, m_2 such that all finite D' -quasirandom groups have the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$ mod cosocle, with $m_1 > cK_1^{D^2}$, $m_2 > cK_2^{D^2}$.*

Proof. Let D', K_1, K_2, m_1, m_2 be exactly as in Lemma 7.1. Let G be any finite D' -quasirandom group.

Let N be the cosocle of G . Then G/N is a direct product of D' -quasirandom finite simple groups. These simple groups all have the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$. So by Proposition 7.3, their product G/N will have this same symmetric double covering property. $\square$

Corollary 7.6. *Let $\mathcal{C}_{\text{CS}(n)}$ be the class of finite groups with at most n conjugacy classes in their cosocles. Then $\mathcal{C}_{\text{CS}(n)}$ is a Q.U.P. class.*

Proof. Let $c = f(D)(3n - 2)^{D^2}$.

For any integer D , and for the constant c , we can find D', K_1, K_2, m_1, m_2 as in Corollary 7.5.

Let G_i be a sequence of D' -quasirandom groups in $\mathcal{C}_{\text{CS}(n)}$. Then G_i all have the symmetric double covering property $[(K_1, m_1), (K_2, m_2)]$ mod cosocles. Since the cosocles contain at most n conjugacy classes, by Proposition 5.2, G_i all have the symmetric double covering property $[((3n - 2)K_1, m_1), ((3n - 2)K_2, m_2)]$. Then any ultraproduct $G = \prod_{i \rightarrow \omega} G_i$ will have the symmetric double covering property $[((3n - 2)K_1, m_1), ((3n - 2)K_2, m_2)]$ by Proposition 7.3.

Since $m_1 > f(D)[(3n - 2)K_1]^{D^2}$, $m_2 > f(D)[(3n - 2)K_2]^{D^2}$, G is D -quasirandom by Proposition 4.4. $\square$

Proof of Theorem 1.5. For any integer D , let $c = f(D)(3n - 2)^{D^2}$. We can find D', K_1, K_2, m_1, m_2 as in Corollary 7.5 and Lemma 7.1.

Let G_i be a sequence of D' -quasirandom groups in $\mathcal{C}_n$. So each G_i is a direct product of D' -quasirandom groups in $\mathcal{C}_{\text{QS}} \cup \mathcal{C}_{\text{CS}(n)}$. These factor groups must have the symmetric double covering property $[((3n - 2)K_1, m_1), ((3n - 2)K_2, m_2)]$.

By Proposition 7.3, G_i must also have this symmetric double covering property $[((3n-2)K_1, m_1), ((3n-2)K_2, m_2)]$. Then any ultraproduct $G = \prod_{i \rightarrow \omega} G_i$ will have the symmetric double covering property $[((3n-2)K_1, m_1), ((3n-2)K_2, m_2)]$ by Proposition 7.3.

Since $m_1 > f(D)[(3n-2)K_1]^{D^2}$ and $m_2 > f(D)[(3n-2)K]^{D^2}$, it follows from Proposition 4.4 that G is D -quasirandom. $\square$

8 Applications

8.1 Triangles in a quasirandom group

A quasirandom group usually contains many patterns. For example, Gowers has shown the following result:

Theorem 8.1 (Gowers [7, Theorem 5.1]). *Pick any $\epsilon_1, \epsilon_2 > 0, 0 < \alpha < 1$. If G is a D -quasirandom group for some large enough D , then for any subset A of G such that $|A| \geq \alpha|G|$, there are more than $(1 - \epsilon_1)\alpha^2|G|$ elements $x \in G$ such that $|A \cap xA| \geq (1 - \epsilon_2)\alpha^2|G|$.*

Morally, if we define an x -pair to be a set $\{y, xy\}$ for some $y \in G$, then this theorem means that any large enough subset of a quasirandom group G will contain many x -pairs for many x .

Now given a q.u.p. class, we can obtain minimally almost periodic groups via ultraproducts of sequences of increasingly quasirandom groups. Then by applying ergodic theory on the ultraproduct, more patterns similar to that of Theorem 8.1 might emerge. It is proven by Bergelson, Robertson and Zorin-Kranich [2] that, for a quasirandom group G in a q.u.p class, any large enough subset of $G \times G$ will contain many x -triangle for many x .

Definition 8.2. Let g be an element of a group G . Then a g -triangle is the set $\{(x, y), (gx, y), (gx, gy)\} \subseteq G \times G$ for some $x, y \in G$.

Theorem 8.3 (Bergelson, Robertson and Zorin-Kranich [2, Theorem 1.12]). *Let G be contained in a q.u.p. class. For any $\epsilon > 0, 0 < \alpha < 1$, there are integers D and K such that, if G is D -quasirandom, then for any subset A of $G \times G$ with $|A| \geq \alpha|G|^2$, the set $T_A = \{g \in G : A \text{ contains more than } (\alpha^4 - \epsilon)|G|^2 \text{ triangles}\}$ can cover G with at most K left translates of itself.*

8.2 Self-bohrifying groups

The application in this section is related to topological groups. We shall treat all groups in previous sections as discrete groups.

Definition 8.4. A *Bohr compactification* of a topological group G is a continuous homomorphism $b : G \rightarrow bG$ such that any continuous homomorphism from G to a compact group factors uniquely through b .

Remark 8.5. (i) The Bohr compactification exists for any group by the work of Holm [10]. It is obviously unique up to a unique isomorphism.
(ii) Clearly, a discrete group is minimally almost periodic iff it has trivial Bohr compactification. Note that for a discrete group, any abstract homomorphism from it to another topological group is automatically continuous.

Definition 8.6. A topological group G is said to be *self-bohrifying* if its Bohr compactification bG is the same abstract group as G , but with a compact topology.

By the results and techniques of this paper, one can find many examples of self-bohrifying groups. In particular, we have the following theorem.

Theorem 8.7. *Let n be a positive integer. Let G_i be a sequence of increasingly quasirandom groups in $\mathcal{C}_n$, the class defined as in Theorem 1.5. Then $\prod_{i \in \mathbb{N}} G_i$ is self-bohrifying as a discrete group.*

Corollary 8.8. *Let G_i be a sequence of non-abelian finite simple groups of increasing order. Then $\prod_{i \in \mathbb{N}} G_i$ is self-bohrifying as a discrete group.*

We will prove Theorem 8.7 by first showing that $\prod_{i \in \mathbb{N}} G_i / \coprod_{i \in \mathbb{N}} G_i$ is minimally almost periodic, and then using a lemma by Hart and Kunen [9].

Definition 8.9. Let G_i be a sequence of groups.

- (i) Their *sum* is the group $\coprod_{i \in \mathbb{N}} G_i = \{g \in \prod_{i \in \mathbb{N}} G_i : \text{only finitely many coordinates of } g \text{ is non-trivial}\}$.
- (ii) Their *reduced product* is the group $\prod_{i \in \mathbb{N}} G_i / \coprod_{i \in \mathbb{N}} G_i$.

Lemma 8.10 (Hart and Kunen [9, Lemma 3.8]). *Let $\{G_i\}_{i \in \mathbb{N}}$ be a sequence of finite groups. Then $\prod_{i \in \mathbb{N}} G_i$ is self-bohrifying if all but finitely many G_i are perfect groups, and $\prod_{i \in \mathbb{N}} G_i / \coprod_{i \in \mathbb{N}} G_i$ has trivial Bohr compactification, i.e., $\prod_{i \in \mathbb{N}} G_i / \coprod_{i \in \mathbb{N}} G_i$ is minimally almost periodic.*

Proof of Theorem 8.7. All 2-quasirandom groups are perfect. So it is enough to show that the reduced product of G_i is minimally almost periodic, i.e., it is D -quasirandom for all D .

For any integer D , let $c = f(D)(3n - 2)^{D^2}$. We can find D', K_1, K_2, m_1, m_2 as in Corollary 7.5 and Lemma 7.1.

Let G_i be a sequence of increasingly quasirandom groups in $\mathcal{C}_n$. Then all but finitely many G_i will be D' -quasirandom. Since we are interested in the reduced product, which is invariant under the change of finitely many coordinates, we may without loss of generality assume that all G_i are D' -quasirandom.

Since $G_i \in \mathcal{C}_n$, each G_i is a direct product of D' -quasirandom groups in $\mathcal{C}_{QS} \cup \mathcal{C}_{CS(n)}$. These factor groups must have the symmetric double covering property $[((3n-2)K_1, m_1), ((3n-2)K_2, m_2)]$. By Proposition 7.3, G_i must also have this symmetric double covering property $[((3n-2)K_1, m_1), ((3n-2)K_2, m_2)]$.

Now by Proposition 7.3, covering properties are preserved by arbitrary products and quotients. So $\prod_{i \in \mathbb{N}} G_i$ will have this covering property, and the reduced product $\prod_{i \in \mathbb{N}} G_i / \coprod_{i \in \mathbb{N}} G_i$ will also have this covering property.

Since $m_1 > c[(3n-2)K_1]^{D^2}$ and $m_2 > c[(3n-2)K]^{D^2}$, the reduced product is D -quasirandom by Proposition 4.4. So we are done by Lemma 8.10. $\square$

Acknowledgments. I would like to thank Professor Terence Tao for introducing me to this area and for his patient guidance. I would also like to thank Professor Richard Schwartz, Professor Vitaly Bergelson, Professor Emmanuel Breuillard and Professor Nikolay Nikolov for their helpful inputs, and thank Professor László Pyber for his helpful inputs and for pointing me to a number of very useful references.

Bibliography

- [1] L. Babai, A. J. Goodman and L. Pyber, Groups without faithful transitive permutation: Representations of small degree, *J. Algebra* **195** (1997), 1–29.
- [2] V. Bergelson, D. Robertson and P. Zorin-Kranich, Triangles in Cartesian squares of quasirandom groups, preprint (2014), <http://arxiv.org/abs/1410.5385>.
- [3] V. Bergelson and T. Tao, Multiple recurrence in quasirandom groups, *Geom. Funct. Anal.* **24** (2014), no. 1, 1–48.
- [4] J. L. Brenner, Covering theorems for FINASIGs. VIII: Almost all conjugacy classes in A_n have exponent ≤ 4 , *J. Aust. Math. Soc. Ser. A* **25** (1978), no. 2, 210–214.
- [5] J. Cheeger and D. G. Ebin, *Comparison Theorems in Riemannian Geometry*, American Mathematical Society, Providence, 1975.
- [6] M. Collins, On Jordan’s theorem for complex linear groups, *J. Group Theory* **10** (2007), no. 4, 411–423.
- [7] W. T. Gowers, Quasirandom groups, *Combin. Probab. Comput.* **17** (2008), no. 3, 363–387.

- [8] L. C. Grove, *Classical Groups and Geometric Algebra*, American Mathematical Society, Providence, 2002.
- [9] J. E. Hart and K. Kunen, Bohr compactifications of non-abelian groups, *Topology Proc.* **26** (2002), no. 2, 593–626.
- [10] P. Holm, On the Bohr compactification, *Math. Ann.* **156** (1964), 34–46.
- [11] D. Holt and W. Plesken, *Perfect Groups*, Clarendon Press, Oxford, 1989.
- [12] M. Kassabov, A. Lubotzky and N. Nikolov, Finite simple groups as expanders, *Proc. Natl. Acad. Sci. USA* **103** (2006), no. 16, 6116–6119.
- [13] J. von Neumann and E. P. Wigner, Minimally almost periodic groups, *Ann. of Math. (2)* **41** (1940), no. 4, 746–750.
- [14] M. R. Sepanski, *Compact Lie Group*, Springer Sci. Bus. Media 235, Springer, New York, 2007.
- [15] A. Stolz and A. Thom, On the lattice of normal subgroups in ultraproducts of compact simple groups, *Proc. Lond. Math. Soc. (3)* **108** (2013), no. 1, 73–102.

Received May 18, 2015; revised February 15, 2016.

Author information

Yilong Yang, UCLA Mathematics Department,
Box 951555, Los Angeles, CA 90095-1555, USA.
E-mail: yy26@math.ucla.edu