Groups Geom. Dyn. 19 (2025), 647–660
DOI 10.4171/GGD/892

Groups with property (T) and many alternating group quotients

Laurent Bartholdi and Martin Kassabov

Abstract. We prove that, for the free algebra over a sufficiently rich operad $\mathcal{O}$, a large subgroup of its group of tame automorphisms has Kazhdan's property (T). We deduce that there exists a group with property (T) that maps onto large powers of alternating groups.

To our teacher, mentor and friend Slava Grigorchuk on the occasion of his 70th birthday – Многая літа!

1. Introduction

Property (T), introduced by Kazhdan in [11], may be thought of as a strong, analytic form of finite generation – it remains the most direct path to proving that lattices in higher-rank Lie groups are finitely generated. In this spirit, one should expect groups with this property to have tight restrictions on their quotients. In particular, the Cayley graphs of their quotients form so-called *expander graphs*, characterized, for example, by a spectral gap in their combinatorial Laplacian. Conversely, families of expander graphs are conveniently "explained" by their being Cayley graphs of quotients of a single group with property (T). The performance of the "product replacement algorithm" (producing almost uniform samplings of black box groups) is thus explained by property (T) of automorphism groups of free groups [7].

It remained for long an open question whether there exists a group with property (T) that admits all (or at least infinitely many) alternating groups as quotients; see, for example, [12, Problems 10.3.2–10.3.4]. A hint that this might be possible appears in [8], proving that alternating groups admit generating sets turning them into expander graphs. The question was settled in [7]: Kaluba, Nowak and Ozawa prove that $\mathrm{Aut}(F_5)$ has property (T), while Gilman [5] had previously shown that $\mathrm{Aut}(F_5)$ maps onto infinitely many alternating groups. Another example of (T) group mapping onto infinitely many alternating groups appears in [2], while a (τ) group (see below) mapping onto all alternating groups appears earlier in [4, Theorem 9.17].

Mathematics Subject Classification 2020: 22D55 (primary); 08A35, 17A36 (secondary).
Keywords: Kazhdan's property T, tame algebra automorphisms, generation of powers of symmetric groups, operads.

In a completely different direction, Philip Hall proved that, for every finite simple group G, the minimal number of generators of the direct power G^n grows logarithmically in n and may remain bounded for unbounded exponents provided that the size of the simple group G grows sufficiently fast. In fact, for every $k \geq 2$, there exists a superexponential function $f_k(n)$ such that $\mathrm{Alt}(n)^{\times f_k(n)}$ is k-generated. For instance, for Alt(5) the alternating group on 5 letters, $\mathrm{Alt}(5)^{\times 19}$ is 2-generated while $\mathrm{Alt}(5)^{\times 20}$ requires 3 generators; see [6, Section 1.6].

It is thus theoretically possible that there exists a group with property (T), mapping onto large powers of alternating groups. We achieve a result of this kind in this article, with a superpolynomial exponent.

Main theorem (= Corollary 14). *For every $d \geq 2$, there is a group Γ_d with property (T) that surjects onto $\mathrm{Alt}(p^{(d+2)k} - 1)^{\times p^{k^{d+1}}}$ for all primes $p > 3 + d + 4\sqrt{d-1}$ and all $k \geq 1$.*

The group Γ_d constructed in Corollary 14 is generated by $d + 4$ elements; it is not difficult to slightly modify these groups and make them all 4-generated.

This implies that for every d, there is a group with property (T) that surjects onto $\mathrm{Alt}(n)^{\times f(n)}$ for infinitely many n, with $f(n) \approx \exp((\log n)^d)$. We leave as an open question whether there exists a group with property (T) that surjects onto $\mathrm{Alt}(n)^{\times f(n)}$ for infinitely many n, with $f(n) \approx \exp(n)$, or at least $f(n) \gtrsim \exp(n^\alpha)$ for some $\alpha > 0$.

1.1. Prior work

It could already be derived, using the techniques from [8] and some extra work, that the Cayley graphs of $\mathrm{Alt}(n)^{\times n^k}$ may form a family of expander graphs of bounded degree, for arbitrary $k \in \mathbb{N}$, and using [4] that there exists a group with property (τ) mapping onto all $\mathrm{Alt}(n)^{\times n^{\log n}}$.

The idea of considering "large" finite quotients of a group is classical, as we mentioned above: combining [5, 7], the group $\mathrm{Aut}(F_5)$ has property (T) and permutes the collection of normal subgroups of F_5 with quotient isomorphic to $\mathrm{PSL}(2, p)$ as an alternating or symmetric group. Since there are roughly p^{15} such subgroups, each given by a generating 5-tuple of elements of $\mathrm{PSL}(2, p)$, this shows that $\mathrm{Alt}(p^{15})$ or $\mathrm{Sym}(p^{15})$ form expanders for a uniform generating set coming from the generators of $\mathrm{Aut}(F_5)$. It follows from Corollary 14 that the estimate p^{15} can be sharpened to p^4, and it may even be brought down to p^3 using [2].

1.2. Property (T)

We recall only very briefly the definition of property (T) (for details, see, e.g., [1]). A discrete group Γ has *property (T)* if its trivial representation is isolated within unitary representations; this means the following. A representation of Γ on a Hilbert space $\mathcal{H}$ *almost has invariant vectors* if for every $\epsilon > 0$ and every finite $S \subseteq \Gamma$, there is $v \in \mathcal{H}$ with

$\|sv - v\| < \epsilon\|v\|$ for all $s \in S$. The group Γ has property (T) if every unitary representation of Γ that almost has invariant vectors actually has Γ-invariant vectors.

We shall also make use of a relative version of (T): the pair (Γ, H) with $H \leq \Gamma$ has *relative property (T)* if every unitary Γ-representation that almost has invariant vectors has H-invariant vectors. Thus, Γ has property (T) if and only if (Γ, Γ) has relative property (T), and if H is finite, then (Γ, H) always has relative property (T). This relative property often appeared as a stepping stone in the proof that a group has property (T), and this article is no exception. Briefly, if (Γ, H_i) has property (T) for a collection of subgroups (H_i), the invariant subspaces of the H_i have well-controlled, large enough angles, and G is generated by $\bigcup_i H_i$, then Γ has (T) (see [9]). We shall review more precisely the required condition in the course of the proofs.

Margulis realized in [13] that property (T) leads to explicit constructions of expander graphs, namely the Cayley graphs of finite quotients. A weaker property, called *property* (τ) by Lubotzky, already yields this conclusion: it suffices that the trivial representation be isolated among those representations of Γ that factor through a finite quotient of Γ.

2. Universal algebra

Let $\mathcal{O}$ be an *operad*: a collection $(\mathcal{O}(n))_{n\in\mathbb{N}}$ of abstract operations, with compositions $\circ_i\colon \mathcal{O}(m) \times \mathcal{O}(n) \to \mathcal{O}(m+n-1)$ for $1 \leq i \leq n$, thought of as composing an arity-m operation with an arity-n operation by feeding the output of the former as ith input of the latter. These composition maps obey the obvious associativity law. There is also an action of the symmetric group on $\mathcal{O}(n)$, permuting each operation's inputs, and compatible with the compositions.

The operad $\mathcal{O}$ is *generated* by the set S if each operation in $\mathcal{O}(n)$ can be obtained as a composition of operations in S. For simplicity, we will not allow operations of arity zero (i.e., constants) in our operads; however, we do not put any other restrictions, so, for example, operations of arity 1 (namely maps) are allowed.

We shall not need much from the theory of operads, so we concentrate immediately on a special case that serves our purposes: the *free operad* on a finite-graded set S, which can be defined by the usual universal property and also has the following concrete description. Let S be a finite set of abstract operations $\{\star_s : s \in S\}$, each with its *arity* $\mathsf{ar}(s) \in \mathbb{N}$. We denote by $\mathsf{ar}(S) = \max\{\mathsf{ar}(s) : s \in S\}$ the maximal arity of S. The *free operad* $\mathcal{O}_S$ on S consists of all compositions of operations in S, with an ordering of their inputs. The elements of $\mathcal{O}_S(n)$ are rooted trees with n leaves numbered $1, \dots, n$, with at each non-leaf vertex a label $s \in S$ and $\mathsf{ar}(s)$ descendants in a given order.

Definition 1. Let R be a commutative ring, and let $\mathcal{O}$ be an operad. An *$\mathcal{O}$-algebra over R* is an R-module A endowed with a family of R-multilinear maps $A^n \to A$, one for each element of $\mathcal{O}(n)$, satisfying the usual operad axioms.

If $\mathcal{O}$ is the free operad on S, this is equivalent to being given a family of R-multilinear maps $\star_s\colon A^{\mathsf{ar}(s)} \to A$, one for each $s \in S$.

In the category of $\mathcal{O}$-algebras over R, there is a free object on any set X which we denote by $R\langle X\rangle_{\mathcal{O}}$. As an R-module, it is generated by all rooted trees of height 1 with leaves labeled by X and an element in $\mathcal{O}(n)$ labeling the root, where n is the number of leaves in the tree.

Note that $R\langle X\rangle_{\mathcal{O}}$ has a natural grading in which all variables have degree 1 and all operations have degree 0. If X is finite and $\mathcal{O}$ is finitely generated and does not contain any operations of arity 1, then the homogeneous components of $R\langle X\rangle_{\mathcal{O}}$ are finitely generated R-modules. In the case of a free operad $\mathcal{O}_S$, the free algebra $R\langle X\rangle_{\mathcal{O}_S}$ has homogeneous components of arbitrarily large degrees provided that S contains at least one operation of arity ≥ 2.

3. Tame automorphisms

Let $\mathcal{O}$ be an operad generated by a finite set S of operations as in the previous section. Consider a commutative ring R, and let $F = R\langle X\rangle_{\mathcal{O}}$ denote the free $\mathcal{O}$-algebra on $X = \{x_0, \dots, x_{n-1}\}$. We shall consider a certain subgroup $\Gamma_{n,N,\mathcal{O}}$ of the group of *tame* automorphisms of F.

For $0 \leq i < n$ and $f \in R\langle x_0, \dots, \widehat{x_i}, \dots, x_{n-1}\rangle_{\mathcal{O}}$, consider the *transvection*

$$t_i(f)\colon F \to F, \quad t_i(f)(x_j) = \begin{cases} x_j + f & \text{if } i = j, \\ x_j & \text{otherwise.} \end{cases}$$

Evidently, $t_i(f)$ is an automorphism of F, with inverse $t_i(-f)$. By definition, the group of *tame automorphisms* of F is the group generated by all such transvections.

Definition 2. Let S be a generating set of an operad $\mathcal{O}$, and choose $n > \max\{\mathsf{ar}(S), 2\}$. Let $N \in \mathbb{N}$ be any, and consider the ring $R = \mathbb{Z}[1/N]$. The group $\Gamma_{n,N,\mathcal{O}}$ is defined as the subgroup of $\mathrm{Aut}(F)$ generated by[1]

$$\begin{aligned} \alpha_i &:= t_{i-1}(x_i) && \text{for } 1 \leq i < n, \\ \alpha_n &:= t_{n-1}(x_0/N), \\ \beta_s &:= t_0(\star_s(x_1, \dots, x_{\mathsf{ar}(s)})) && \text{for } s \in S. \end{aligned}$$

For brevity, we write it simply Γ_n when the dependency on N and $\mathcal{O}$ is irrelevant.

[1] By its construction, the group depends not only on the operad $\mathcal{O}$ but also on the choice of the generating set S. This dependence is very mild as we will show in Theorem 5 and is not reflected in the notation.

Our first main result is that the group Γ_n has property (T) as soon as the parameter N is large enough.

Theorem 3. *If N is divisible by all primes $p \leq 3 + \mathsf{ar}(S) + 4\sqrt{\mathsf{ar}(S) - 1}$, then $\Gamma_{n,N,\mathcal{O}}$ has Kazhdan's property (T).*

Proof. Notice first that the automorphisms $\alpha_1, \dots, \alpha_n$ generate $\mathrm{SL}_n(R)$, and recall that $\mathrm{SL}_n(R)$ has property (T) since $n \geq 3$.

Therefore, there exists a constant δ such that, for any representation of Γ_n on a Hilbert space $\mathcal{H}$, any $\epsilon > 0$ and any vector $v \in \mathcal{H}$ which is ϵ-almost invariant under the action of the generators of Γ_n, we have that v is $\delta\epsilon$-almost invariant under $\mathrm{SL}_n(R)$, and in particular under all $t_i(rx_j)$ with $0 \leq i \neq j < n$ and $r \in R$, and also under all $t_0(r \star_s (x_1, \dots, x_{\mathsf{ar}(s)}))$ with $r \in R$ and $s \in S$ since these are words of bounded length in $\mathrm{SL}_n(R)$ and the generators of Γ_n.

Consider the following abelian subgroups of Γ_n:

$$\begin{aligned} G_0 &= \langle t_0(rx_1), t_0(r \star_s (x_1, \dots, x_{\mathsf{ar}(s)})) : r \in R, s \in S \rangle, \\ G_i &= \{t_i(rx_{i+1 \bmod n}) : r \in R\} \quad \text{for } 1 \leq i < n. \end{aligned}$$

Then by the previous paragraph, the pairs (Γ_n, G_i) all have relative property (T).

For all $i < j$, the group generated by G_i and G_j is either abelian or nilpotent of class 2: if $0 < i < j - 1$, then it is abelian, isomorphic to R^2; if $0 < i = j - 1$, then it is isomorphic to the Heisenberg group of upper-triangular 3×3 matrices over R; and if $i = 0$, then it is isomorphic to a subgroup of a product, over $s \in S$, of either R^2 (if $\mathsf{ar}(S) < j < n - 1$) or the Heisenberg group (if $j \leq \mathsf{ar}(S)$ or $j = n - 1$).

It follows that, in a representation as above, the Friedrichs angles between invariant subspaces for G_i, G_j satisfy

$$0 \leq \cos \sphericalangle(\mathcal{H}^{G_i}, \mathcal{H}^{G_j}) \leq \begin{cases} 0 & \text{if } \langle G_i, G_j \rangle \text{ is abelian,} \\ p^{-1/2} & \text{otherwise,} \end{cases}$$

where p is the smallest prime not dividing N. (Recall that the angle between two subspaces $V, W \leq \mathcal{H}$ is the smallest angle between vectors in $V \cap (V \cap W)^{\perp}$ and $W \cap (W \cap V)^{\perp}$.) Indeed, it suffices to consider representations of the Heisenberg group over $\mathbb{Z}/p$, which have dimension 1 or $\geq p$; and then the bound on the cosine of the angles is $1/\sqrt{p}$ (see [3, Theorem 4.4]).

To apply [9, Theorem 1.2], it remains to prove that the following matrix is positive definite:

$$\Delta := \begin{pmatrix} 1 & -\varepsilon & \cdots & -\varepsilon & 0 & \cdots & 0 & -\varepsilon \\ -\varepsilon & 1 & \ddots & & & & & 0 \\ \vdots & \ddots & \ddots & -\varepsilon & & & & \vdots \\ -\varepsilon & 0 & -\varepsilon & 1 & -\varepsilon & & & \\ 0 & & & -\varepsilon & 1 & \ddots & & \vdots \\ \vdots & & & & \ddots & \ddots & -\varepsilon & 0 \\ 0 & & & & & -\varepsilon & 1 & -\varepsilon \\ -\varepsilon & 0 & \cdots & & \cdots & 0 & -\varepsilon & 1 \end{pmatrix}$$

for $\varepsilon = p^{-1/2}$, with terms "$-\varepsilon$" appearing one step away from the diagonal and in the second to $1 + \mathsf{ar}(S)$th entries of the first row and column.

We can decompose Δ as the sum of a circulant matrix Δ_1 with 2ε on the diagonal and $-\varepsilon$ off the diagonal, and a matrix Δ_2 with $1 - 2\varepsilon$ on the diagonal and $-\varepsilon$ on the third to $1 + \mathsf{ar}(S)$th entries of the first row and column.

The matrix Δ_1 is positive semidefinite when $\varepsilon > 0$, while Δ_2 has eigenvalues $1 - 2\varepsilon$ (with multiplicity $n - 2$) and $1 - 2\varepsilon \pm \sqrt{\mathsf{ar}(S) - 1}\varepsilon$ (with multiplicity 1). Thus, Δ_2 is positive definite when $\sqrt{\mathsf{ar}(S) - 1}\varepsilon < 1 - 2\varepsilon$. We deduce that Δ is positive definite when $\varepsilon < 1/(2 + \sqrt{\mathsf{ar}(S) - 1})$. ■

Remark 4. The bound for p in Theorem 3 is not optimal, but it cannot be improved significantly. It can be shown that Δ is not positive definite when $\varepsilon > 1/\max(2, \sqrt{\mathsf{ar}(S) - 1})$, so the best bound is at least $\max(4, \mathsf{ar}(S) - 1)$.

Our next result is that the group Γ_n contains a substantial part of the tame automorphism group of the free $\mathcal{O}$-algebra F and really depends on $\mathcal{O}$ (as the notation suggests) and only mildly on the choice of its generating set S.

Theorem 5. *For all $f \in R\langle x_1, \dots, x_{n-1-\mathsf{ar}(S)}\rangle_{\mathcal{O}}$, the group $\Gamma_{n,N,\mathcal{O}}$ contains the transvection $t_0(f)$.*

Proof. By linearity, it is sufficient to prove this for elements of the free S-magma, namely for rooted tree. We proceed by induction on the tree's height, the base case being a single leaf and no internal vertices; it is dealt with by elementary matrices in $\mathrm{SL}_n(R) \subset \Gamma_{n,N,\mathcal{O}}$.

Consider therefore $s \in S$, write $k = \mathsf{ar}(s)$ and consider a term $f = \star_s(f_1, \dots, f_k)$ with $f_1, \dots, f_k \in R\langle x_1, \dots, x_\ell\rangle_{\mathcal{O}}$ for some $\ell \in \mathbb{N}$ satisfying $k + \ell < n$. By induction, there are transvections $t_0(f_i)$ in Γ_n, and since Γ_n contains all even permutations of the variables, we may assume by induction that Γ_n contains the transvections

$$\gamma_j := t_{\ell+j}(f_j) \quad \text{for } 1 \le j \le k.$$

Note that the γ_j all commute with each other. There is also in Γ_n a conjugate β'_s of β_s, that is, the transvection

$$\beta'_s := t_0(\star_s(x_{\ell+1}, \dots, x_{\ell+k})).$$

By a direct computation,

$$\begin{aligned}[\beta'_s, \gamma_j] &= (\beta'_s)^{-1}(\beta'_s)^{\gamma_j} \\ &= t_0(-\star_s(x_{\ell+1}, \dots, x_{\ell+k}))\, t_0(\star_s(x_{\ell+1}, \dots, x_{\ell+j} + f_j, \dots, x_{\ell+k})) \\ &= t_0(\star_s(x_{\ell+1}, \dots, f_j, \dots, x_{\ell+k})),\end{aligned}$$

so the iterated commutator $[\dots[\beta'_s, \gamma_1], \dots, \gamma_k]$ is the transvection $t_0(f)$ which thus belongs to Γ. ∎

4. Representations

For an $\mathcal{O}$-algebra A and $X = \{x_0, \dots, x_{n-1}\}$, consider the set $\mathcal{R}_{n,A}$ of $\mathcal{O}$-algebra homomorphisms $R\langle X\rangle_{\mathcal{O}} \to A$. Such a homomorphism is uniquely determined by the images of $x_0, \dots, x_{n-1}$, which are arbitrary elements of A since $R\langle X\rangle_{\mathcal{O}}$ is free. We may therefore naturally identify $\mathcal{R}_{n,A}$ with A^n.

The automorphism group of $R\langle X\rangle_{\mathcal{O}}$ naturally acts on $\mathcal{R}_{n,A}$ by pre-composition. Under the identification of $\mathcal{R}_{n,A}$ with A^n, the generators α_i (for $1 \leq i < n$) act as $(a_0, \dots, a_{n-1}) \mapsto (a_0, \dots, a_i - a_{i+1}, \dots, a_{n-1})$, etc.

Furthermore, the action of $R\langle X\rangle_{\mathcal{O}}$ commutes with the action of the automorphism group of A by post-composition. Again choosing $R = \mathbb{Z}[1/N]$, we obtain an action of $\Gamma_{n,N,\mathcal{O}}$ on $A^n/\mathrm{Aut}(A)$.

Definition 6. An $\mathcal{O}$-algebra A over R is called *minimal* if its only subalgebras are A and the 0-submodule. Here by a subalgebra of A, we mean an R-submodule which is closed under all operad operations.

Theorem 7. *Let A be an $\mathcal{O}$-algebra, and choose $n \geq \mathsf{ar}(S) + 2$.*

(1) *If A is minimal and non-trivial, then the action of $\Gamma_{n,N,\mathcal{O}}$ on A^n has two orbits: the fixed point 0^n and a large orbit consisting of all other points.*

(2) *If A is minimal, then the induced action of Γ_n on $\Omega_{n,A} := (A^n \setminus 0^n)/\mathrm{Aut}(A)$ is k-transitive, for all k less than the number of $\mathrm{Aut}(A)$-orbits in A. In particular, if A is finite and $|\Omega| > 25$ and $\mathrm{Aut}(A)$ has at least 6 orbits on A, then Γ_n acts on Ω as a full alternating or symmetric group.*

(3) *If A, A' are two non-isomorphic minimal algebras, then the actions of Γ_n on $\Omega_{n,A}$ and on $\Omega_{n,A'}$ are not isomorphic.*

We begin by an analogue of the Chinese remainder theorem for minimal algebras.

Lemma 8. *Let the $\mathcal{O}$-algebra A be minimal. For any elements $a_1, \dots, a_k \in A \setminus 0$ in distinct* $\operatorname{Aut}(A)$*-orbits and for every $b_1, \dots, b_k \in A$, there exists $v \in R\langle x\rangle_{\mathcal{O}}$ such that the substitution $x \mapsto a_i$ maps v to b_i, that is, $\mathsf{ev}_{a_i}(v) = b_i$ where $\mathsf{ev}_a \colon R\langle x\rangle_{\mathcal{O}} \to A$ is the evaluation map $x \mapsto a$.*

Proof. The proof is by induction on k. The base case $k = 1$ follows from the minimality of A which implies that the evaluation map ev_{a_1} is a surjective map $R\langle x\rangle_{\mathcal{O}} \to A$. Assuming the statement for k, the evaluation maps at $a_1, \dots, a_k$ yield a surjection

$$\mathsf{ev}_{a_1} \times \cdots \times \mathsf{ev}_{a_k} \colon R\langle x\rangle_{\mathcal{O}} \to A^k.$$

The kernel V of this map is a subalgebra of $R\langle x\rangle_{\mathcal{O}}$ because $\mathcal{O}$ has no constants; and the evaluation at a_{k+1} maps V to a subalgebra of A. Since A is minimal, the image is either the whole of A, proving the induction step, or is 0. In the last case, $\mathsf{ev}_{a_{k+1}}$ is identically zero on V, so induces a (still surjective) algebra homomorphism $A^k \to A$. Pre-composing this homomorphism with the ith embedding $A \to A^k$, we obtain a homomorphism $\phi_i \colon A \to A$ mapping a_i to a_{k+1}; and ϕ_i is non-zero, so its kernel is 0 and its image is A, that is, ϕ_i is an automorphism of A; therefore, a_i and a_{k+1} are in the same orbit of $\operatorname{Aut}(A)$. ∎

Proof of Theorem 7. (1) Consider A a minimal algebra and $a \in A$ a non-zero element. Since A is minimal, a generates the whole algebra A, and we will show that the Γ_n-orbit of $(a, 0, \dots, 0)$ contains every non-zero element of A^n.

Consider $(a_0, \dots, a_{n-1}) \in A^n \setminus 0^n$. Since Γ contains the group of even permutations, we can assume that $a_{n-1} \neq 0$. Thus, each of $a_0 - a, a_1, a_2, \dots, a_{n-2}$ may be, respectively, written as an expression $v_i(a_{n-1})$ since a_{n-1} is non-zero and thus generates the algebra A. By Theorem 5 and conjugation, the transvection $t_i(v_i)$ belongs to Γ_n for all $1 \leq i < n$. Applying them in sequence, we see that $(a, 0, \dots, 0, a_{n-1})$ is in the same orbit as $(a_0, a_1, \dots, a_{n-1})$. Finally, a_{n-1} may be written as an expression in a and another transvection from Γ_n sends $(a, 0, \dots, 0, a_{n-1})$ to $(a, 0, \dots, 0)$.

(2) For the second statement, we shall prove that the action of Γ_n is k-transitive whenever k is at most the number of $\operatorname{Aut}(A)$-orbits on $A \setminus 0$. Using Lemma 8, the proof of k-transitivity is standard. Consider $a_1, \dots, a_k \in A \setminus 0$ in different orbits under $\operatorname{Aut}(A)$. Let $v_1, \dots, v_k$ be vectors in $A^n \setminus 0^n$ which are in different $\operatorname{Aut}(A)$-orbits under the diagonal action. We use induction on k to show that there is an element in Γ which sends v_i to $(a_i, 0, \dots, 0)$ for all $i = 1, \dots, k$. The base case $k = 1$ is the first statement of the theorem. For the induction step, we can assume that $v_i = (a_i, 0, \dots, 0)$ for $i = 1, \dots, k$. If some coordinate $b_{k+1,j}$ of v_{k+1} is non-zero for some $j > 0$, then we can find a transvection which changes the zeroth coordinate of v_{k+1} to a_{k+1} and fixes v_i for $i = 1, \dots, k$ and then uses Lemma 8 to move the resulting vector to $(a_{k+1}, 0, \dots, 0)$. Otherwise, the zeroth coordinate of v_{k+1} is in a different $\operatorname{Aut}(A)$-orbit than $a_1, \dots, a_m$, and again by Lemma 8, we can find a transvection which fixes $v_1, \dots, v_k$ and makes some other coordinate of v_{k+1} non-zero.

The final claim in (2) follows from the well-known fact that there are no highly transitive groups acting on large finite sets except the alternating and the symmetric group.

(3) For the last statement, let us assume that the actions of Γ_n on $\Omega_{n,A}$ and on $\Omega_{n,A'}$ are isomorphic. Then, using the language of group theory, we can characterize the respective subsets $(A \setminus 0) \times 0^{n-1}$ and $(A \setminus 0) \times 0^{n-1}$ as the fixed sets of all transvections $t_i(a)$ with $1 \leq i < n$. The action of transvections $t_0(a)$ being isomorphic on these two sets then directly lets us reconstruct the $\mathcal{O}$-algebra structure on A, A' from the Γ_n-action. ■

Remark 9. It is likely that the minimality assumption on A can be replaced with a weaker one, such as simplicity, plus a small extra assumption (such as a bound on the number of generators of the subalgebras of A). This will slightly change the statement to a claim that there is one large orbit consisting of all generating tuples of A. However, this will significantly complicate the proof (see [2]).

Remark 10. The last conclusion of (2) relies on the classification of finite simple groups. This dependence can be avoided when $\mathrm{Aut}(A)$ is much smaller than A, since it can be shown without using the classification that there are no non-trivial k-transitive groups on n points for $k \gg \log n$ and n sufficiently large.

It may seem that Theorem 7 requires a too strong assumption – minimality of A – rather than, say, simplicity. For example, in the category of associative algebras, there are very few minimal algebras (since every minimal algebra is commutative). However, for the free operad $\mathcal{O}_S$ as soon as S contains enough operations, minimal algebras are the norm rather than the exception.

Theorem 11. *Assume that S contains at least two operations and that $\mathcal{O}$ is free on S. Then, for every finite-dimensional vector space V over a field $\mathbb{K}$, the collection of minimal $\mathcal{O}$-algebra structures on V is Zariski-dense among all $\mathcal{O}$-algebra structures.*

In particular, for every prime p, the proportion of minimal algebras among all $\mathcal{O}$-algebra structures on $(\mathbb{Z}/p)^k$ is at least $1 - 6p^{(1-|S|)(k-1)}$.

Proof. Let us first write $V = \mathbb{K}^k$, a k-dimensional vector space.

A multilinear operation $\star_s$ on V, of arity $\mathsf{ar}(s)$, is a linear map $V^{\otimes \mathsf{ar}(s)} \to V$, and the space of such maps has dimension $k^{\mathsf{ar}(s)+1}$. The set Σ of $\mathcal{O}$-algebra structures on V is therefore a vector space of dimension $\sum_{s\in S} k^{\mathsf{ar}(s)+1}$.

For any choice of a subspace $W \leq V$, say of dimension d, the fact that $\star_s$ maps $W^{\otimes \mathsf{ar}(s)}$ back to W is a linear condition imposing $d^{\mathsf{ar}(s)}(k-d)$ independent constraints. The subspace of Σ consisting of algebras for which W is a subalgebra therefore has codimension $\sum_{s\in S} d^{\mathsf{ar}(s)}(k-d)$.

The union of all these subspaces, as W varies over the Grassmann variety of d-dimensional subspaces, is thus a variety of codimension at least

$$\sum_{s\in S} d^{\mathsf{ar}(s)}(k-d) - d(k-d),$$

which is positive as soon as S contains at least two operations.

In the case of $\mathcal{O}$-algebra structures on $(\mathbb{Z}/p)^k$, the above arguments show that the probability of a non-minimal structure is bounded by

$$\sum_{d=1}^{k-1} \binom{k}{d}_p p^{-\sum_{s\in S} d^{\operatorname{ar}(s)}(k-d)},$$

where the p-binomial coefficient $\binom{k}{d}_p = (p)_k/(p)_d(p)_{k-d}$ is the number of subspaces of $(\mathbb{Z}/p)^k$ of dimension d; here $(p)_k = (1-p)\cdots(1-p^k)$. Since all operations have arity at least 1 and there are $|S|$ operations, we have the following obvious upper bound:

$$\sum_{d=1}^{k-1} \binom{k}{d}_p p^{-|S|d(k-d)}.$$

It is not difficult to see that the contribution of the terms for $d = 1$ and $d = k-1$ is bounded above by $2\frac{p}{p-1}p^{(1-|S|)(k-1)}$, which is $\leq 3p^{(1-|S|)(k-1)}$ for $p > 2$. For all other terms, we can use

$$\binom{k}{d}_p \leq \binom{k}{d} p^{d(k-d)},$$

since $\binom{k}{d}_p$ counts strings $\sigma \in \{0,1\}^k$ with d ones and weighted by $p^{|\{i<j:\sigma_i>\sigma_j\}|}$; this gives that the contribution of all other terms is bounded above by

$$\sum_{d=2}^{k-2} \binom{k}{d} p^{-(|S|-1)2(k-2)}, \quad \text{which is } \leq (2^k - 2 - 2k)p^{-2(|S|-1)(k-2)} \text{ if } k \geq 3.$$

These bounds are sufficient to prove the desired inequality for $p \geq 3$ or $k \geq 6$, and the remaining cases can be verified directly. ∎

Remark 12. The probability that a random $\mathcal{O}$-structure on $(\mathbb{Z}/p)^k$ has a 1-dimensional subalgebra is approximately $p^{(1-|S|)(k-1)}$, so the above bound is close to optimal. It can be improved to $1-(2+\epsilon)p^{(1-|S|)(k-1)}/(1-p^{1-|S|})$ for every $\epsilon > 0$ and large enough p. Of course, all these bounds say nothing in case $k = 1$, when every algebra structure is clearly minimal.

The next issue before applying Theorem 7 is to show that generically the automorphism group of an $\mathcal{O}_S$-algebra is very small. It is reasonable to assume that generically the only automorphisms are scalars – a quick computation shows that $\lambda\mathsf{Id}$ is an automorphism of an algebra A if and only if $\lambda^{\operatorname{ar}(s)-1} = 1$ for all $s \in S$. Indeed, this is the case.

Theorem 13. *Assume that S contains at least two operations. Then for any prime $p \geq 2$, most minimal $\mathcal{O}_S$-algebra structures on $(\mathbb{Z}/p)^k$ have "trivial" automorphism group, namely*

$$\operatorname{Aut}(A) = \{\lambda\mathsf{Id} : \lambda^{\operatorname{ar}(s)-1} = 1,\ \forall s \in S\}.$$

More precisely, the number of minimal algebras with non-trivial automorphism groups is less than $1/p^k$ *of all possible algebra structures* $p^{\sum_{s\in S} k^{\mathrm{ar}(s)+1}}$.

Proof. Consider $\phi \in \mathrm{Aut}(A)$; it is a linear map, so is given by a $k \times k$ matrix. Up to passing to a field extension, there is an eigenvector $a \in A \otimes K$ with eigenvalue $\lambda \in K$.

Since a generates $A \otimes K$, we have that $A \otimes K$ is a quotient of $K\langle x\rangle_{\mathcal{O}}$, so ϕ is uniquely determined by a and λ. Moreover, since $K\langle x\rangle_{\mathcal{O}}$ is graded, the operator ϕ is diagonalizable with eigenvalues λ^i. Furthermore, if all operations in S have arity 1, then ϕ is scalar since the whole algebra $K\langle x\rangle_{\mathcal{O}}$ lies in degree 1; while if there are higher-arity operations, then λ is a root of unity. In the first case, we are done; in the second case, let n be the order of λ, and for all $i \in \mathbb{Z}/n$, let V_i be the eigenspace of ϕ with eigenvalue λ^i, say of dimension d_i.

Let us compute the linear conditions imposed on ϕ by the fact that it commutes with each operation $\star_s$. It must map $V_{i_1} \otimes \cdots \otimes V_{i_{\mathrm{ar}(s)}}$ to $V_{i_1+\cdots+i_s}$, so the dimension of the space of $\mathcal{O}$-algebra structures which commute with ϕ is

$$\sum_{s\in S}\ \sum_{i_1,\ldots,i_{\mathrm{ar}(s)}\in\mathbb{Z}/n} d_{i_1}\cdots d_{i_{\mathrm{ar}(s)}} d_{i_1+\cdots+i_{\mathrm{ar}(s)}}.$$

Since the space $V_{i_1+\cdots+i_s}$ is not the full space, its dimension is less than or equal to $k-1$. Therefore, for each $s \in S$, we have

$$\begin{aligned}\sum_{i_1,\ldots,i_{\mathrm{ar}(s)}\in\mathbb{Z}/n} & d_{i_1}\cdots d_{i_{\mathrm{ar}(s)}} d_{i_1+\cdots+i_{\mathrm{ar}(s)}} \\ &\le \sum_{i_1,\ldots,i_{\mathrm{ar}(s)}\in\mathbb{Z}/n} d_{i_1}\cdots d_{i_{\mathrm{ar}(s)}}(k-1) = k^{\mathrm{ar}(s)+1} - k^{\mathrm{ar}(s)}.\end{aligned}$$

Thus, the total sum is less than

$$\sum_{s\in S} k^{\mathrm{ar}(s)+1} - \sum_{s\in S} k^{\mathrm{ar}(s)} \le \sum_{s\in S} k^{\mathrm{ar}(s)+1} - k^2 - k,$$

since by assumption that there are at least 2 operations in S and one has arity at least 2.

This shows that each candidate ϕ is an automorphism of a minimal algebra structure with probability at most p^{-k^2-k}. Since the number of possibilities for ϕ is less than p^{k^2}, the probability that an algebra structure is minimal and has a non-trivial automorphism is less than p^{-k}. ■

Corollary 14. *Let* S *consist of one binary operation and one operation of arity* $d \ge 2$. *Then the group* $\Gamma_{d+2,N,\mathcal{O}_S}$ *has property (T) provided that* N *is divisible by all primes less than* $3 + d + 4\sqrt{d-1} < 5d$. *Moreover, this group surjects onto* $\mathrm{Alt}(p^{(d+2)k}-1)^{\times p^{k^{d+1}}}$ *for all primes* $p > 3 + d + 4\sqrt{d-1}$ *and all* $k \ge 1$.

Proof. Property (T) for the group $\Gamma_{d+2,N,\mathcal{O}_S}$ is a direct consequence of Theorem 3.

For $k \geq 2$, there are $p^{k^{d+1}}$ choices for an operation of arity d on $(\mathbb{Z}/p)^k$. By Theorems 11 and 13, almost all of the operations yield minimal $\mathcal{O}$-algebra structure A on $(\mathbb{Z}/p)^k$ with trivial automorphism group. In order to count to non-isomorphic ones, we need to divide by the size of the group $\mathrm{GL}_k(\mathbb{Z}/p)$. At the end, it is easy to see that there are at least

$$p^{\sum_s k^{\mathrm{ar}(s)+1}}(1 - 6p^{-(|S|-1)(k-1)} - p^{-k})/|\mathrm{GL}_k(\mathbb{Z}/p)|$$
$$\geq p^{k^{d+1}+k^3-k^2}(1 - 5p^{-(d-1)(k-1)} - p^{-k}) > p^{k^{d+1}}$$

non-isomorphic minimal $\mathcal{O}_S$ algebra structures on $(\mathbb{Z}/p)^k$ with trivial automorphism group. When $k = 1$, it is easy to see that there are at least $p = p^{k^{d+1}}$ non-isomorphic $\mathcal{O}_S$-structures on $\mathbb{Z}/p$. By Theorem 7 (2), each of these algebras yields a highly transitive action of $\Gamma := \Gamma_{d+2,N,\mathcal{O}_S}$ on $p^{(d+2)k} - 1$ points, yielding an alternating or symmetric quotient of Γ on that many points. Furthermore, all generators of Γ have order p, which is odd by our restrictions, so this quotient is alternating. Since these actions are non-isomorphic, they can be combined into a surjection from Γ to $\mathrm{Alt}(p^{(d+2)k} - 1)^{\times p^{k^{d+1}}}$. ∎

Using results from [10], we can deduce the following.

Corollary 15. *For every d, there is a group with property (τ) whose profinite completion is*

$$\prod_n \mathrm{Alt}(n)^{\times n^{(\log n)^d}}.$$

Idea of the proof. For any fixed $d \geq 2$, the previous construction produces a group with property (T) which maps onto $\prod_k \mathrm{Alt}(p^{(d+2)k} - 1)^{\times p^{k^{d+1}}}$ for some fixed prime p. This can be combined with the results from [10] to produce a group with (τ) and profinite completion $\prod_k \mathrm{Alt}(p^{(d+2)k} - 1)^{\times p^{k^{d+1}}}$. Finally, use that

$$\prod_{n=p^{(d+2)k}-1}^{p^{(d+2)(k+1)}-2} \mathrm{Alt}(n)^{\times n^{(\log n)^d}}$$

can be boundedly generated by p^{d+2} copies of $\mathrm{Alt}(p^{(d+2)k} - 1)^{\times p^{k^{d+1}}}$. ∎

We do not know for which functions $f(n)$ there exists a finitely generated group with property (T) or (τ) which maps onto $\mathrm{Alt}(n)^{\times f(n)}$ for all n – the above construction shows that this is possible for $\log f(n) \approx (\log n)^d$ for any fixed d, and on the other side, one needs $\log f(n) \precsim O(n \log n)$; otherwise, the minimal number of generators of $\mathrm{Alt}(n)^{\times f(n)}$ would be unbounded. This question is roughly equivalent to the question for which functions $f(n)$ it is possible to turn the Cayley graphs of $\mathrm{Alt}(n)^{\times f(n)}$ in bounded degree expanders.

Acknowledgments. The second author is grateful to the organizers and participants of the workshop on profinite rigidity at ICMAT in June 2023 for the stimulating discussions. The first author is grateful to the second author for having sparked his interest in this question. Both authors are grateful to the anonymous referee for careful reading and valuable suggestions.

Funding. L.B. is supported in part by the ERC AdG grant 101097307. M.K. is supported in part by the Simons Foundation grant 713557 and National Science Foundation grant DMS-2319371.

References

[1] B. Bekka, P. de la Harpe, and A. Valette, *Kazhdan's property (T)*. New Math. Monogr. 11, Cambridge University Press, Cambridge, 2008 Zbl 1146.22009 MR 2415834

[2] P.-E. Caprace and M. Kassabov, Tame automorphism groups of polynomial rings with property (T) and infinitely many alternating group quotients. *Trans. Amer. Math. Soc.* **376** (2023), no. 11, 7983–8021 Zbl 1535.22019 MR 4657226

[3] M. Ershov and A. Jaikin-Zapirain, Property (T) for noncommutative universal lattices. *Invent. Math.* **179** (2010), no. 2, 303–347 Zbl 1205.22003 MR 2570119

[4] M. Ershov, A. Jaikin-Zapirain, and M. Kassabov, Property (T) for groups graded by root systems. *Mem. Amer. Math. Soc.* **249** (2017), no. 1186, 135 p. Zbl 1375.22005 MR 3724373

[5] R. Gilman, Finite quotients of the automorphism group of a free group. *Canad. J. Math.* **29** (1977), no. 3, 541–551 Zbl 0332.20010 MR 0435226

[6] P. Hall, The Eulerian functions of a group. *Q. J. Math.* **os-7** (1936), no. 1, 134–151 Zbl 0014.10402

[7] M. Kaluba, P. W. Nowak, and N. Ozawa, $\mathrm{Aut}(\mathbb{F}_5)$ has property (T). *Math. Ann.* **375** (2019), no. 3–4, 1169–1191 Zbl 1494.22004 MR 4023374

[8] M. Kassabov, Symmetric groups and expander graphs. *Invent. Math.* **170** (2007), no. 2, 327–354 Zbl 1191.20002 MR 2342639

[9] M. Kassabov, Subspace arrangements and property T. *Groups Geom. Dyn.* **5** (2011), no. 2, 445–477 Zbl 1244.20041 MR 2782180

[10] M. Kassabov and N. Nikolov, Property tau is not a profinite property. 2023, Preprint

[11] D. A. Kazhdan, Connection of the dual space of a group with the structure of its close subgroups (in Russian). *Funkcional. Anal. i Priložen.* **1** (1967), no. 1, 71–74 English translation: *Funct. Anal. Appl.* **1** (1967), no. 1, 63–65 Zbl 0168.27602 MR 0209390

[12] A. Lubotzky, *Discrete groups, expanding graphs and invariant measures*. Progr. Math. 125, Birkhäuser, Basel, 1994 Zbl 0826.22012 MR 1308046

[13] G. A. Margulis, Explicit constructions of concentrators (in Russian). *Problemy Peredači Informatsii* **9** (1973), no. 4, 71–80 English translation: *Probl. Inf. Transm.* **9** (1973), no. 4, 325–332 Zbl 0312.22011 MR 0484767

Received 13 September 2023.

Laurent Bartholdi
Institut Camille Jordan, Université Claude Bernard Lyon 1, 21, avenue Claude Bernard,
69100 Villeurbanne, France; secretariat-ICJ@math.univ-lyon1.fr

Martin Kassabov
Department of Mathematics, Cornell University, Malott Hall, Ithaca, NY 14853, USA;
kassabov@math.cornell.edu, martin.kassabov@gmail.com