WHAT IS . . .

Property (τ)?

Alex Lubotzky

Property (τ) is a baby version of Kazhdan's property (T) from the representation theory of semisimple Lie groups. It is the crucial ingredient in Margulis's construction of expanders—graphs that are basic building blocks in many communication network constructions. Property (τ) appears also in the theory of automorphic forms and in hyperbolic geometry and found its way to applications in computational group theory and in the combinatorics of finite simple groups.

So what is property (τ)? The story begins with (T) as a property of a locally compact (e.g., discrete) group G. Property (T) requires that the trivial one-dimensional representation of G is "bounded away" from all other irreducible unitary representations of G. For a group like $\Gamma = \mathrm{SL}_n(\mathbb{Z})$ generated by a finite set S, it means that whenever Γ acts nontrivially and irreducibly on a Hilbert space H, every vector v of H is moved by "at least ε" away from v for some $\varepsilon > 0$ independent of H and v.

In 1973 Margulis realized that this "pushing property" is exactly what is needed to construct expanding graphs. These graphs—expanders—are highly connected sparse graphs that play an important role in combinatorics and computer science (see [3]). Loosely speaking, they are "fat and round": One cannot cut them into two large subsets without cutting a lot of edges. Or, equivalently, for every subset A of the vertices of the graphs, its boundary, i.e., the vertices outside A that are connected to A, form a fairly large set compared to A. Such graphs were known to exist by random consideration (á la Erdős), but explicit constructions are desired.

Property (T) gave them: Let Γ be a group generated by a finite set S and $\mathcal{L} = \{N_m\}_{m\in I}$ a family of finite index normal subgroups of Γ. The finite quotients Γ/N_m give rise to a family of Cayley graphs $X_m = \mathrm{Cay}(\Gamma/N_m; S)$, where the vertices of X_m are the elements of Γ/N_m, and two vertices a and b are connected if there exists $s \in S$ such that either $b = sa$ or $a = sb$.

Alex Lubotzky is professor of mathematics at the Hebrew University of Jerusalem, Einstein Institute of Mathematics. His email address is alexlub@math.huji.ac.il.

Now the group Γ acts on Γ/N_m, and hence we have a unitary representation on $L^2(\Gamma/N_m)$. Property (T) now implies that for every subset A of Γ/N_m, the characteristic function χ_A of A is "pushed by at least ε" by one of the elements in S. This means that sA is "substantially different" from A and implies that the boundary of A is large. Hence $\mathrm{Cay}(\Gamma/N_m; S)$ form a family of expanders.

A more careful look at the above argument shows that we were not using the full power of (T); property (T) says that all the representations have the "pushing" property, but we have used (T) only with respect to those unitary representations that factor through the finite quotients Γ/N_m; they are, in particular, finite dimensional. This led to the definition of (τ):

Definition. Let Γ be a group and $\mathcal{L} = \{N_m\}_{m\in I}$ a family of finite index normal subgroups in Γ. Then **Γ has property (τ) with respect to $\mathcal{L}$** if the nontrivial irreducible representations of Γ factoring through Γ/N_m (for some $m \in I$) are bounded away from the trivial representation. We say that **Γ has (τ)** if $\mathcal{L}$ is the family of all finite index normal subgroups.

In fact, (τ) is exactly what is needed to make $\mathrm{Cay}(\Gamma/N_m; S)$ expanders; they are expanders if and only if Γ has (τ) with respect to $\mathcal{L}$.

So the representation-theoretic property (τ) has an equivalent combinatorial form. But this is not the only one: Property (τ) can be expressed in equivalent analytic, geometric, and even measure-theoretic formulations. For example, assume $\Gamma = \pi_1(M)$ is the fundamental group of a compact Riemannian manifold M and M_m $(m \in I)$ is the finite sheeted covers of M corresponding to N_m $(m \in I)$. Let $\lambda_1(M_m)$ be the smallest positive eigenvalue of the Laplacian (= Laplace-Beltrami operator) of M_m. Then Γ has (τ) with respect to $\mathcal{L} = \{N_m | m \in I\}$ if and only if there exists $\varepsilon > 0$ such that $\lambda_1(M_m) \geq \varepsilon$ for every $m \in I$. The point of this equivalence is that the Cayley graphs of Γ/N_m are discrete approximations of the manifolds M_m. The graphs are expanders if and only if their λ_1's are bounded away from zero and their λ_1's approximate those of M_m.

The various equivalent forms of property (τ) not only indicate its intrinsic interest but also allow

some quite diverse and unexpected applications. Let us mention a few of them.

A celebrated theorem of Selberg from 1965 asserts that $\lambda_1(\Gamma(m)\backslash\mathbb{H}) \geq \frac{3}{16}$ when $\mathbb{H}$ is the upper half-plane $\{z = x + yi \mid x, y \in \mathbb{R}, y > 0\}$ on which $SL_2(\mathbb{R})$ (and hence also $SL_2(\mathbb{Z})$) acts by Möbius transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}.$$

Here $\Gamma(m)$ is the congruence subgroup $\Gamma(m) = \mathrm{Ker}\,(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/m\mathbb{Z}))$, and as before $\lambda_1(\Gamma(m)\backslash\mathbb{H})$ is the bottom of the positive spectrum of the Laplacian. This is a deep result whose proof involves analysis of the Riemann surface $\Gamma(m)\backslash\mathbb{H}$ as well as Weil's estimates on Kloosterman sums, which in turn boil down to the Riemann hypothesis over finite fields.

In light of the above, Selberg's theorem implies that $SL_2(\mathbb{Z})$ (which has neither (T) nor (τ)) does have (τ) *with respect to the family of congruence subgroups*. Selberg's results have been generalized by various authors, and recently Clozel showed that the same holds for all (characteristic zero) S-arithmetic subgroups of semisimple groups.

Since $SL_2(\mathbb{Z})$ is generated by $a = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, we can deduce that the Cayley graphs of $SL_2(\mathbb{Z}/p\mathbb{Z})$ with respect to these generators a and b form a family of expanding graphs. It is not difficult to see that the diameter of expanders is logarithmic in their size. From this one deduces

Corollary. *The matrix*

$$u_p = \begin{pmatrix} 1 & \frac{p-1}{2} \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}/p\mathbb{Z})$$

can be written as a word of length $O(\log p)$ using the generators a and b and their inverses.

Note that $u_p = a^{(p-1)/2}$. It is, however, not at all clear how b can help us to write u_p as a shorter word. In fact, the proof of the corollary is not constructive, and no such explicit word is known. The only known proof of this elementary statement is via the Selberg theorem and property (τ).

The above types of arguments were the starting point of an elaborate study of the diameter of finite simple groups with respect to various choices of generators.

Another surprising connection to computing arises in computational (finite) group theory. In this area the goal is to design algorithms to study specific groups. Here is a typical example to keep in mind: Given two invertible 100×100 matrices A and B over the field of two elements $\mathbb{F}_2$, find the order of the group G generated by them. A basic subroutine in many of these algorithms is one that provides a random element from the group G. Finding such a random element in G (before G has been computed or before its order is known) is an interesting challenge. The naive approach—to take a random long word in A and B—can be nicely analyzed theoretically but gives poor (i.e., slow) results. A new method was presented ten years ago called "the product replacement algorithm" (PRA, for short), which is a kind of noncommutative Gaussian elimination. Its implementation showed outstanding results. In computation—as in physics—if something works, everyone uses it. Still, its rigorous justification was somewhat mysterious. Surprisingly, (τ) came into the picture: The analysis of the PRA boils down to analyzing random walks on some graphs. These graphs turned out to be Cayley graphs of some finite quotients of $\mathrm{Aut}(F)$—the automorphism group of the free group. So if $\mathrm{Aut}(F)$ has (τ), these graphs are expanders and the random walks on them converge very fast to the uniform distribution, giving a full explanation of the outstanding performance of the PRA. As of now, the question of whether $\mathrm{Aut}(F)$ has (τ) is still open—but enough is known to get some partial results and new insight on the PRA.

Also (τ) has found its way into geometry. A well-known conjecture attributed to Thurston asserts that an n-dimensional closed hyperbolic manifold has a finite sheeted cover with positive first Betti number. The conjecture, if true, would reveal a lot of the geometry and topology of these manifolds. Property (τ) came unexpectedly into a proof of this conjecture for the subfamily of arithmetic manifolds.

The case of hyperbolic 3-manifolds is of special interest. Recent work of Lackenby may open the door to an even more dramatic application of (τ) to geometry: Lubotzky and Sarnak conjectured that the fundamental group of a compact hyperbolic 3-manifold does not have property (τ) (it is well known that it does not have the stronger property (T)). Lackenby shows that this conjecture (together with another quite plausible conjecture on the Heegard splitting) would imply the "virtual Haken conjecture". This last conjecture falls short of Thurston's conjecture but gives essentially all the geometric and topological corollaries. This work shows that property (τ) may play a significant role in the theory of hyperbolic 3-manifolds.

References

[1] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Prog. in Math. **125**, Birkhäuser, Basel, 1994.

[2] A. Lubotzky and A. Zuk, On property (τ) and its application, `http://www.ma.huji.ac.il/~alexlub/` (see BOOKS, On Property. ps or On Property.pdf).

[3] P. Sarnak, What is an expander?, *Notices Amer. Math. Soc.* **51** (2004), 762–63.