Proving Kazhdan's Property (T) with Semidefinite Programming

Tim Netzer

TU Dresden

Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory

Universität Osnabrück, September 2015

A countable group G has Kazhdan's Property (T), if

A countable group G has Kazhdan's Property (T), if

- the trivial unitary representation of G is an isolated point in the set of all irreducible unitary representations, with respect to the Fell topology

A countable group G has Kazhdan's Property (T), if

- the trivial unitary representation of G is an isolated point in the set of all irreducible unitary representations, with respect to the Fell topology
- or, if any unitary representation that has almost invariant vectors, has an invariant vector.

A countable group G has Kazhdan's Property (T), if

- the trivial unitary representation of G is an isolated point in the set of all irreducible unitary representations, with respect to the Fell topology
- or, if any unitary representation that has almost invariant vectors, has an invariant vector.

David Kazhdan introduced this notion in the 1960's, to show that certain lattices are finitely generated. In fact, each countable group with Property (T) is finitely generated.

A countable group G has Kazhdan's Property (T), if

- the trivial unitary representation of G is an isolated point in the set of all irreducible unitary representations, with respect to the Fell topology
- or, if any unitary representation that has almost invariant vectors, has an invariant vector.

David Kazhdan introduced this notion in the 1960's, to show that certain lattices are finitely generated. In fact, each countable group with Property (T) is finitely generated.The notions plays an important role in many context, as it turned out.

A countable group G has Kazhdan's Property (T), if

- the trivial unitary representation of G is an isolated point in the set of all irreducible unitary representations, with respect to the Fell topology
- or, if any unitary representation that has almost invariant vectors, has an invariant vector.

David Kazhdan introduced this notion in the 1960's, to show that certain lattices are finitely generated. In fact, each countable group with Property (T) is finitely generated.The notions plays an important role in many context, as it turned out.

Finite groups have property (T).

A countable group G has Kazhdan's Property (T), if

- the trivial unitary representation of G is an isolated point in the set of all irreducible unitary representations, with respect to the Fell topology
- or, if any unitary representation that has almost invariant vectors, has an invariant vector.

David Kazhdan introduced this notion in the 1960's, to show that certain lattices are finitely generated. In fact, each countable group with Property (T) is finitely generated.The notions plays an important role in many context, as it turned out.

Finite groups have property (T). Non-finite examples are $\mathrm{SL}_n(\mathbb{Z})$ for $n \geq 3$.

A countable group G has Kazhdan's Property (T), if

- the trivial unitary representation of G is an isolated point in the set of all irreducible unitary representations, with respect to the Fell topology
- or, if any unitary representation that has almost invariant vectors, has an invariant vector.

David Kazhdan introduced this notion in the 1960's, to show that certain lattices are finitely generated. In fact, each countable group with Property (T) is finitely generated.The notions plays an important role in many context, as it turned out.

Finite groups have property (T). Non-finite examples are $\mathrm{SL}_n(\mathbb{Z})$ for $n \geq 3$. Amenable groups have Property (T) only if they are finite,

A countable group G has Kazhdan's Property (T), if

- the trivial unitary representation of G is an isolated point in the set of all irreducible unitary representations, with respect to the Fell topology
- or, if any unitary representation that has almost invariant vectors, has an invariant vector.

David Kazhdan introduced this notion in the 1960's, to show that certain lattices are finitely generated. In fact, each countable group with Property (T) is finitely generated.The notions plays an important role in many context, as it turned out.

Finite groups have property (T). Non-finite examples are $\mathrm{SL}_n(\mathbb{Z})$ for $n \geq 3$. Amenable groups have Property (T) only if they are finite, so $\mathbb{Z}^n$ does not have Property (T).

Let G be finitely generated by $S \subseteq G$ (assume $S^{-1} = S$, $n := |S|$). Let $\mathbb{R}[G]$ be the real group algebra of G.

Let G be finitely generated by $S \subseteq G$ (assume $S^{-1} = S$, $n := |S|$). Let $\mathbb{R}[G]$ be the real group algebra of G. Then

$$\rho := \frac{1}{n} \cdot \sum_{s \in S} s \in \mathbb{R}[G]$$

is called the Random Walk Operator associated with S.

Let G be finitely generated by $S \subseteq G$ (assume $S^{-1} = S$, $n := |S|$). Let $\mathbb{R}[G]$ be the real group algebra of G. Then

$$\rho := \frac{1}{n} \cdot \sum_{s \in S} s \in \mathbb{R}[G]$$

is called the Random Walk Operator associated with S.

In fact the multiplication with ρ on $\mathbb{R}[G]$ (or $\ell^2(G)$) models the random walk on the Cayley graph of (G, S).

Let G be finitely generated by $S \subseteq G$ (assume $S^{-1} = S$, $n := |S|$). Let $\mathbb{R}[G]$ be the real group algebra of G. Then

$$\rho := \frac{1}{n} \cdot \sum_{s \in S} s \in \mathbb{R}[G]$$

is called the Random Walk Operator associated with S.

In fact the multiplication with ρ on $\mathbb{R}[G]$ (or $\ell^2(G)$) models the random walk on the Cayley graph of (G, S).

- G has Property (T), if in any unitary representation π of G, the operator $\pi(\rho)$ has a spectral gap at 1.

Let G be finitely generated by $S \subseteq G$ (assume $S^{-1} = S$, $n := |S|$). Let $\mathbb{R}[G]$ be the real group algebra of G. Then

$$\rho := \frac{1}{n} \cdot \sum_{s \in S} s \in \mathbb{R}[G]$$

is called the Random Walk Operator associated with S.

In fact the multiplication with ρ on $\mathbb{R}[G]$ (or $\ell^2(G)$) models the random walk on the Cayley graph of (G, S).

- G has Property (T), if in any unitary representation π of G, the operator $\pi(\rho)$ has a spectral gap at 1.

If you apply this to ρ operating on $\ell^2(G)$, it yields:

Let G be finitely generated by $S \subseteq G$ (assume $S^{-1} = S$, $n := |S|$). Let $\mathbb{R}[G]$ be the real group algebra of G. Then

$$\rho := \frac{1}{n} \cdot \sum_{s \in S} s \in \mathbb{R}[G]$$

is called the Random Walk Operator associated with S.

In fact the multiplication with ρ on $\mathbb{R}[G]$ (or $\ell^2(G)$) models the random walk on the Cayley graph of (G, S).

- G has Property (T), if in any unitary representation π of G, the operator $\pi(\rho)$ has a spectral gap at 1.

If you apply this to ρ operating on $\ell^2(G)$, it yields:

The random walk on G converges much faster than expected to a normal distribution.

The product replacement algorithm is a method for producing random elements in a finitely generated group.

The product replacement algorithm is a method for producing random elements in a finitely generated group. For abelian groups, there is random walk on some $\mathrm{SL}_n(\mathbb{Z})$ in the background.

The product replacement algorithm is a method for producing random elements in a finitely generated group. For abelian groups, there is random walk on some $\mathrm{SL}_n(\mathbb{Z})$ in the background. Since these groups have Property (T), this random walk converges fast.

The product replacement algorithm is a method for producing random elements in a finitely generated group. For abelian groups, there is random walk on some $\mathrm{SL}_n(\mathbb{Z})$ in the background. Since these groups have Property (T), this random walk converges fast. This explains why the product replacement algorithm for abelian groups works so well.

The product replacement algorithm is a method for producing random elements in a finitely generated group. For abelian groups, there is random walk on some $\mathrm{SL}_n(\mathbb{Z})$ in the background. Since these groups have Property (T), this random walk converges fast. This explains why the product replacement algorithm for abelian groups works so well.

Conclusion:

- Property (T) is a rather abstract property that a group may have.

The product replacement algorithm is a method for producing random elements in a finitely generated group. For abelian groups, there is random walk on some $\mathrm{SL}_n(\mathbb{Z})$ in the background. Since these groups have Property (T), this random walk converges fast. This explains why the product replacement algorithm for abelian groups works so well.

Conclusion:

- Property (T) is a rather abstract property that a group may have.
- It has interesting consequences, and appears in several contexts.

The product replacement algorithm is a method for producing random elements in a finitely generated group. For abelian groups, there is random walk on some $\mathrm{SL}_n(\mathbb{Z})$ in the background. Since these groups have Property (T), this random walk converges fast. This explains why the product replacement algorithm for abelian groups works so well.

Conclusion:

- Property (T) is a rather abstract property that a group may have.
- It has interesting consequences, and appears in several contexts.
- Proving Property (T) for a group is notoriously hard.

The product replacement algorithm is a method for producing random elements in a finitely generated group. For abelian groups, there is random walk on some $\mathrm{SL}_n(\mathbb{Z})$ in the background. Since these groups have Property (T), this random walk converges fast. This explains why the product replacement algorithm for abelian groups works so well.

Conclusion:

- Property (T) is a rather abstract property that a group may have.
- It has interesting consequences, and appears in several contexts.
- Proving Property (T) for a group is notoriously hard.

Our new approach uses a sums-of-squares approach and semidefinite programming.

Let A be an $\mathbb{R}$-algebra with involution.

Let A be an $\mathbb{R}$-algebra with involution. An element of the form

$$a = a_1^* a_1 + \cdots + a_n^* a_n$$

with $a_i \in A$ is called a sum of (hermitian) squares.

Let A be an $\mathbb{R}$-algebra with involution. An element of the form

$$a = a_1^* a_1 + \cdots + a_n^* a_n$$

with $a_i \in A$ is called a sum of (hermitian) squares.

Fix elements $b_1, \ldots, b_r \in A$. Checking whether some element $a \in A$ is a sum of squares of elements from $\mathrm{span}_{\mathbb{R}}\{b_1, \ldots, b_r\}$ means finding a positive semidefinite matrix $M \in \mathrm{Sym}_r(\mathbb{R})$ with

$$a = (b_1^*, \ldots, b_r^*) M \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}.$$

Let A be an $\mathbb{R}$-algebra with involution. An element of the form

$$a = a_1^* a_1 + \cdots + a_n^* a_n$$

with $a_i \in A$ is called a sum of (hermitian) squares.

Fix elements $b_1, \ldots, b_r \in A$. Checking whether some element $a \in A$ is a sum of squares of elements from $\mathrm{span}_{\mathbb{R}}\{b_1, \ldots, b_r\}$ means finding a positive semidefinite matrix $M \in \mathrm{Sym}_r(\mathbb{R})$ with

$$a = (b_1^*, \ldots, b_r^*) M \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}.$$

Finding a positive semidefinite matrix with linear constaints on the entries is a semidefinite program.

Let A be an $\mathbb{R}$-algebra with involution. An element of the form

$$a = a_1^* a_1 + \cdots + a_n^* a_n$$

with $a_i \in A$ is called a sum of (hermitian) squares.

Fix elements $b_1, \ldots, b_r \in A$. Checking whether some element $a \in A$ is a sum of squares of elements from $\mathrm{span}_{\mathbb{R}}\{b_1, \ldots, b_r\}$ means finding a positive semidefinite matrix $M \in \mathrm{Sym}_r(\mathbb{R})$ with

$$a = (b_1^*, \ldots, b_r^*) M \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}.$$

Finding a positive semidefinite matrix with linear constaints on the entries is a semidefinite program. Such programs admit quite efficient numerical algorithms.

Back to property (T):

Back to property (T):

For a group G are equivalent:

- Property (T)

Back to property (T):

For a group G are equivalent:

- Property (T)
- ρ has a spectral gap at 1 in each representation

Back to property (T):

For a group G are equivalent:

- Property (T)
- ρ has a spectral gap at 1 in each representation
- $\Delta := 1 - \rho$ has a spectral gap at 0 in each representation

Back to property (T):

For a group G are equivalent:

- Property (T)
- ρ has a spectral gap at 1 in each representation
- $\Delta := 1 - \rho$ has a spectral gap at 0 in each representation
- $\Delta^2 - \epsilon\Delta$ is positive semidefinite in each representation (for some $\epsilon > 0$)

Back to property (T):

For a group G are equivalent:

- Property (T)
- ρ has a spectral gap at 1 in each representation
- $\Delta := 1 - \rho$ has a spectral gap at 0 in each representation
- $\Delta^2 - \epsilon\Delta$ is positive semidefinite in each representation (for some $\epsilon > 0$)
- $\Delta^2 - \epsilon\Delta$ is a sum of squares in $\mathbb{R}[G]$, for some $\epsilon > 0$

Back to property (T):

For a group G are equivalent:

- Property (T)
- ρ has a spectral gap at 1 in each representation
- $\Delta := 1 - \rho$ has a spectral gap at 0 in each representation
- $\Delta^2 - \epsilon\Delta$ is positive semidefinite in each representation (for some $\epsilon > 0$)
- $\Delta^2 - \epsilon\Delta$ is a sum of squares in $\mathbb{R}[G]$, for some $\epsilon > 0$

The last formulation is due to Ozawa, 2014.

Back to property (T):

For a group G are equivalent:

- Property (T)
- ρ has a spectral gap at 1 in each representation
- $\Delta := 1 - \rho$ has a spectral gap at 0 in each representation
- $\Delta^2 - \epsilon\Delta$ is positive semidefinite in each representation (for some $\epsilon > 0$)
- $\Delta^2 - \epsilon\Delta$ is a sum of squares in $\mathbb{R}[G]$, for some $\epsilon > 0$

The last formulation is due to Ozawa, 2014.

It can be checked with semidefinite programming!

Theorem (N. & Thom, to appear in *Experimental Mathematics*)

For $G = \mathrm{SL}_3(\mathbb{Z})$ *the element*

$$\Delta^2 - \frac{1}{72} \cdot \Delta$$

is a sum of squares in $\mathbb{R}[G]$.

Theorem (N. & Thom, to appear in *Experimental Mathematics*)

For $G = \mathrm{SL}_3(\mathbb{Z})$ *the element*

$$\Delta^2 - \frac{1}{72} \cdot \Delta$$

is a sum of squares in $\mathbb{R}[G]$.

- new and easy proof of Property (T) for $\mathrm{SL}_3(\mathbb{Z})$, based on semidefinite programming

Theorem (N. & Thom, to appear in *Experimental Mathematics*)

For $G = \mathrm{SL}_3(\mathbb{Z})$ *the element*

$$\Delta^2 - \frac{1}{72} \cdot \Delta$$

is a sum of squares in $\mathbb{R}[G]$.

- new and easy proof of Property (T) for $\mathrm{SL}_3(\mathbb{Z})$, based on semidefinite programming
- proof is exact; the numerically computed sums-of-squares representation is rounded to rational coefficients, the error is removed with a theoretical argument

Theorem (N. & Thom, to appear in *Experimental Mathematics*)

For $G = \mathrm{SL}_3(\mathbb{Z})$ the element

$$\Delta^2 - \frac{1}{72} \cdot \Delta$$

is a sum of squares in $\mathbb{R}[G]$.

- new and easy proof of Property (T) for $\mathrm{SL}_3(\mathbb{Z})$, based on semidefinite programming
- proof is exact; the numerically computed sums-of-squares representation is rounded to rational coefficients, the error is removed with a theoretical argument
- $\epsilon = \frac{1}{72}$ improves upon the former results on the spectral gap by a factor of about 2000.

Theorem (N. & Thom, to appear in *Experimental Mathematics*)

For $G = \mathrm{SL}_3(\mathbb{Z})$ the element

$$\Delta^2 - \frac{1}{72} \cdot \Delta$$

is a sum of squares in $\mathbb{R}[G]$.

- new and easy proof of Property (T) for $\mathrm{SL}_3(\mathbb{Z})$, based on semidefinite programming
- proof is exact; the numerically computed sums-of-squares representation is rounded to rational coefficients, the error is removed with a theoretical argument
- $\epsilon = \frac{1}{72}$ improves upon the former results on the spectral gap by a factor of about 2000. Can probably still be impoved a lot

Theorem (N. & Thom, to appear in *Experimental Mathematics*)

For $G = \mathrm{SL}_3(\mathbb{Z})$ *the element*

$$\Delta^2 - \frac{1}{72} \cdot \Delta$$

is a sum of squares in $\mathbb{R}[G]$.

- new and easy proof of Property (T) for $\mathrm{SL}_3(\mathbb{Z})$, based on semidefinite programming
- proof is exact; the numerically computed sums-of-squares representation is rounded to rational coefficients, the error is removed with a theoretical argument
- $\epsilon = \frac{1}{72}$ improves upon the former results on the spectral gap by a factor of about 2000. Can probably still be impoved a lot
- shows that numerical methods can attack the abstract group theoretic question

Future:

Future:

- Property (T) for $G = \mathrm{Aut}(\mathbb{F}_4)$?

Future:

- Property (T) for $G = \mathrm{Aut}(\mathbb{F}_4)$? Unknown, experiments with the product replacement algorithm for non-abelian groups suggest yes.

Future:

- Property (T) for $G = \mathrm{Aut}(\mathbb{F}_4)$? Unknown, experiments with the product replacement algorithm for non-abelian groups suggest yes. Numerically intractable for us, so far.

Future:

- Property (T) for $G = \mathrm{Aut}(\mathbb{F}_4)$? Unknown, experiments with the product replacement algorithm for non-abelian groups suggest yes. Numerically intractable for us, so far.
- Other groups of course....

Future:

- Property (T) for $G = \mathrm{Aut}(\mathbb{F}_4)$? Unknown, experiments with the product replacement algorithm for non-abelian groups suggest yes. Numerically intractable for us, so far.
- Other groups of course....
- Other spectral-gap problems via sums of squares.

Thank you for your attention!