

Kazhdan's property (T) and semidefinite programming

小沢登高*

京都大学数理解析研究所, 2018 年 2 月

始めに:

Kazhdan の性質 (T) は従順性と並んで解析的群論において最も重要な性質である ([1]). 性質 (T) を持つ群の代表例として $SL(n \geq 3, \mathbb{Z})$ などの高階数実 Lie 群の格子が挙げられる (Kazhdan 1967) が, 性質 (T) を持つ無限群が存在すること自体が非自明な定理であり幾つもの応用が存在する重要な数学的事実である. この講演では与えられた群が性質 (T) を持つことを, 半正定値計画問題 (SDP) を利用して電子計算機により数学的に厳密に確認するためのアルゴリズムについて述べる ([8, 7, 2, 3]). 特に, 有限群の表現論を利用してアルゴリズムを高速化することで, 幾何学的に興味深い幾つかの新しい例に対して性質 (T) を確認できたことを報告する ([4]). 自然に現れる群のなかで性質 (T) を持つものは希少・特別であると考えられてきたが, 実はそうでもないということが計算機により確かめられる日が来るかもしれない. 特に幾何学的群論において著名な未解決問題である $\text{Aut}(F_d)$ の場合に, 性質 (T) を $d = 5$ に対して確認した.

この講演では数学の実験科学的側面についても述べたい. 一般的に言って, 自然科学では観察された事実が先にありそれを説明する理論が後に来るが, 数学では理論が先にありその帰結として事実を得る. こうした転倒は数学的事実に至る手段が人間の精神活動による他ないから起きていると考えられる. (数学的事実というものが数学的に厳密に証明されたものとして定義されていることから起きているともいえる. 物理学等に導かれた数学理論は数多く存在するが物理的事実は数学的理論・証明抜きには数学的事実をもたらさない.) しかし計算機科学の発展に伴い, 数学研究における実験器具である計算機器・アルゴリズムが強力になるにつれ, 今後は数学的事実がまず観察され, それを説明する理論が次に求められるということがより多く起こることになるだろうと推測される. (その結果, 四色問題のように人間に理解可能な証明が (見つから) ないということも多く起こるはずである.)

*narutaka@kurims.kyoto-u.ac.jp

Kazhdan の性質 (T) [1, 5]:

群 G が Kazhdan の性質 (T) を持つことを口語的に言うと、任意の直交表現 (π, H) に対して任意のほとんど G -不変なベクトル $v \in H$ が真に G -不変なベクトルに近いときをいう。厳密には、

$$\exists S \subseteq G \exists \kappa > 0 \text{ such that } \forall (\pi, H) \forall v \in H \quad d(v, H^G) \leq \kappa^{-1} \max_{s \in S} \|v - \pi_s v\|$$

が成り立つときをいう。この条件は $\max_{s \in S} \|v - \pi_s v\| < \kappa \|v\|$ なる $v \in H$ が存在すれば G -不変ベクトルの成す部分空間 H^G が非零であるということを主張する（実は同値）。上の条件が成り立つとき、有限集合 S は G の生成系となる。さらに、 G が性質 (T) を持つなら、任意の有限生成系 S に対して上の条件を満たす $\kappa = \kappa(S) > 0$ が存在し、**Kazhdan 定数**と呼ばれる。性質 (T) は商群及び有限指数部分群・拡大に遺伝するが、擬等長不変量ではないことが知られている。一方、群 G が従順であるとは、 $\ell_2 G$ 上 $(\lambda_g v)(x) = v(g^{-1}x)$ で定義される正則表現がほとんど G -不変ベクトルを持つときをいう： $\exists v_n \in \ell_2 G$ such that $\|v_n\| = 1$ and $\forall g \in G \quad \|v_n - \lambda_g v_n\| \rightarrow 0$ 。従順群のクラスは可換群及び劣指数増大度を持つ群を含み、部分群、商群、拡大をとる操作に閉じている。特に任意の可解群は従順である。 $\ell_2(G)^G \neq 0$ となるのは G が有限のときに限るので、性質 (T) を持つ従順群は有限群に限ることが分かる。従って、性質 (T) を持つ群は有限生成かつ有限可換化を持つことが分かる。性質 (T) は局所コンパクト群に対しても同様に定義され、格子（離散部分群で余体積が有限なもの）に遺伝する。D. Kazhdan(1967) は高階数単純連結 Lie 群が性質 (T) を持つことを示すことにより、そのような群の任意の格子が有限生成かつ有限可換化を持つことを示した。

エクспанダーグラフ [1, 5]:

性質 (T) の重要な応用にエクспанダーグラフの構成がある。エクспанダーグラフは数学、計算機科学、工業などで幅広く使われている。性質 (T) を持つ群 $G = \langle S \rangle$ が有限集合 X に推移的に作用しているとする。このとき、辺集合を $\{\{x, sx\} : x \in X, s \in S\}$ で定めることにより X をグラフと見なせる（Schreier グラフと呼ばれる）。各頂点の位数は X のサイズに依らず高々 $|S|$ である。任意の $A \subset X$ に対して、ベクトル $|A^c|1_A - |A|1_{A^c} \in \ell_2 X \ominus (\ell_2 X)^G$ を考えれば、

$$|\partial A| \geq \frac{\kappa^2}{2} |A| \left(1 - \frac{|A|}{|X|}\right)$$

が成り立つことが分かる。このようなグラフは $(|S|, \frac{\kappa^2}{2})$ -エクспанダーと呼ばれる。任意の部分集合 $A \subset X$ が与えられたとき、その k 近傍 $\mathcal{N}_k(A)$ のサイズは $\frac{|X|}{2}$ になるまで k について指数的に増大する（ $\frac{|X|}{2}$ になった後はその余集合のサイズが指数的に減少する）。頂点の位数とエクспанダー定数が一定で幾らでもサイズの大きいエクспанダーが存在することは確率論的手法により古くから知られていたが、始めて具体的に構成したの

は G. Margulis (1972) である．剰余有限群 $G = \mathrm{SL}(3, \mathbb{Z})$ が性質 (T) を持つことから，任意の生成系 S に対して， $\mathrm{SL}(3, \mathbb{Z}/n\mathbb{Z})$ がエクспанダー列となる．(Margulis は実際には包含 $\mathbb{Z}^2 \leq \mathrm{SL}(2, \mathbb{Z}) \ltimes \mathbb{Z}^2$ が包含に対する性質 (T) を持つことを利用して $\mathrm{SL}(2, \mathbb{Z}) \ltimes \mathbb{Z}^2 \curvearrowright (\mathbb{Z}/n\mathbb{Z})^2$ のグラフがエクспанダー列となることを示した．こちらの方がグラフをより具体的に記述できる．)

Product Replacement Algorithm [6]:

与えられた有限群から「ランダムな元」を選ぶことは，工業的応用上も重要である．例えば，置換 $\sigma_1, \dots, \sigma_d \in \mathfrak{S}(N)$ (ここで N は巨大， d は固定の数) が与えられたときに生成される部分群 $\langle \sigma_1, \dots, \sigma_d \rangle$ の位数を (部分群を特定することなしに) 推定する際に使われたりする．ランダムな元を得るために現在よく使われているアルゴリズムである **Product Replacement Algorithm** (PRA) について述べる．有限群 Γ と $d \in \mathbb{N}$ に対して，

$$\Gamma(d) := \{(g_1, \dots, g_d) \in \Gamma^d : \Gamma = \langle g_1, \dots, g_d \rangle\}$$

とおく． $\Gamma(d) \neq \emptyset$ を仮定する． $\Gamma(d)$ の元 $\underline{g} = (g_1, \dots, g_d)$ に 4 種の基本変形

$$\begin{aligned} R_{i,j}^{\pm} &: (g_1, \dots, g_d) \mapsto (g_1, \dots, \overbrace{g_i g_j^{\pm 1}}^{i\text{-th}}, \dots, g_d) \\ L_{i,j}^{\pm} &: (g_1, \dots, g_d) \mapsto (g_1, \dots, g_j^{\pm 1} g_i, \dots, g_d) \end{aligned} \quad (*)$$

をランダムに繰り返し m 回適用し，結果として得られた $\underline{g}$ の成分をランダムに一つ選ぶ試行 ν が PRA である．PRA は GAP や MAGMA といった群論を扱える数式処理プログラムに実装され，実用上とてもよい性能を示しているが，その数学的な裏付けは不明である．A. Lubotzky と I. Pak([6]) は $\mathrm{Aut}(F_d)$ が性質 (T) を持つならこの現象に説明がつくことを見抜いた．つまり， d に余裕があり， $\Gamma(d)$ の各連結成分 (上述のの基本変形に関して) がエクспанダーであるなら $m = O(\log |\Gamma|)$ でランダムな元が得られる (つまり， ν が Γ 上の一様分布に近い) ことが分かる．式 (*) において $g_1, \dots, g_d$ を階数 d の自由群 F_d の標準生成系と見なすとき， $R_{i,j}^{\pm}, L_{i,j}^{\pm}$ は自由群の自己同型と見なせる． $S = \{R_{i,j}^{\pm}, L_{i,j}^{\pm}\}$ は指数 2 の部分群 $\mathrm{SAut}(F_d) := \ker(\det: \mathrm{Aut}(F_d) \rightarrow \mathbb{Z}/2)$ を生成することが知られている．よって前節の議論により， $\mathrm{SAut}(F_d)$ が性質 (T) を持つなら， $\Gamma(d)$ の各連結成分が $(4d(d-1), \kappa^2/2)$ -エクспанダーとなることがわかるのである．ここで重要なのは，エクспанダー係数が有限群 Γ に依存しないことである．

性質 (T) と半正定値計画問題:

非可換実代数幾何により性質 (T) を代数的に特徴づけることを考える．非可換実代数幾何は非可換代数における等式や不等式を扱う分野である．(なお「非可換」は可換とは限らないという意味である．) 古典的な実代数幾何学を代表する初期の業績として，

Hilbert の第 17 問題 (= Artin の定理, 1927) が挙げられる: もし多項式 $f \in \mathbb{R}[x_1, \dots, x_d]$ が $\forall t \in \mathbb{R}^d f(t) \geq 0$ であるなら, 有理多項式 $g_1, \dots, g_n \in \mathbb{R}(x_1, \dots, x_d)$ が存在して $f = \sum g_i^2$ を満たす. この問題は多項式環 $\mathbb{R}[x_1, \dots, x_d]$ を完備化した連続関数環においては単に平方根 $f^{1/2}$ をとればよいだけなので trivial である. あとは完備化された環において得られた解をいかにもとの多項式環に移すかである. 非可換実代数幾何においても, 不等式を解くにあたって, 与えられた非可換環を完備化して作用素環 (C^* 環) を作り, そこで解析学により問題を解いてからもとの環に得られた解を移すといったことを考える.

今回は群 G の実群環 $\mathbb{R}[G]$ を考える. 積は合成積である. また対合 $(\sum_x f(x)x)^* = \sum_x f(x)x^{-1}$ が存在する. このとき G の直交表現 (π, H) と $\mathbb{R}[G]$ の Hilbert 空間 H 上の $*$ -表現の間には自然な 1 対 1 対応が存在し, $\mathbb{R}[G]$ の完備化 (包絡作用素環) は群 C^* 環と呼ばれる. 実群環 $\mathbb{R}[G]$ の正錐

$$\Sigma^2 \mathbb{R}[G] = \{ \sum_i f_i^* f_i : f_i \in \mathbb{R}[G] \} = \{ \sum_{x,y} P_{x,y} x^{-1} y : P \in \mathbb{M}_G^+(\mathbb{R}) \}$$

を考える. ここで $\mathbb{M}_G^+(\mathbb{R})$ は G の元を添字とする半正定値行列で高々有限個の非零成分を持つものを意味する. 群 G は有限生成であるとし, 有限生成系 S で $S = S^{-1}$ を満たすものを考え, 組合せ論的 Laplacian を次で定義する:

$$\Delta = \frac{1}{2} \sum_{s \in S} (1 - s)^* (1 - s) = |S| - \sum_{s \in S} s \in \Sigma^2 \mathbb{R}[G].$$

群 C^* 環におけるスペクトル理論を使うと, G が性質 (T) を持つのは適当な $\varepsilon > 0$ に対して不等式 $\Delta^2 - \varepsilon \Delta \geq 0$ が群 C^* 環内で成り立つことと同値であることが分かる. この事実には非可換実代数幾何学的考察を加えて次の性質 (T) の代数的な特徴づけを得られる.

定理 (Ozawa [8])

G が性質 (T) を持つ $\iff \exists \varepsilon > 0$ such that $\Delta^2 - \varepsilon \Delta \in \Sigma^2 \mathbb{R}[G]$ (or $\mathbb{Q}[G]$).
さらに右が成り立つとき, $\kappa(S) \geq (2\varepsilon/|S|)^{1/2}$.

ここで, $E \subseteq G$ を有限部分集合とし, 探索域を制限して $P \in \mathbb{M}_G^+(\mathbb{R})$ から $P \in \mathbb{M}_E^+(\mathbb{R})$ にすると不等式 $\Delta^2 - \varepsilon \Delta \in \Sigma^2 \mathbb{R}[G]$ は半正定値計画問題 (SDP)

minimize $-\varepsilon$

subject to $\exists P \in \mathbb{M}_E^+(\mathbb{R})$ such that $\Delta^2 - \varepsilon \Delta = \sum_{x,y \in E} P_{x,y} x^{-1} y$ in $\mathbb{R}[G]$

となる. (右辺の $\sum P_{x,y} x^{-1} y$ は $\sum P_{x,y} (1 - x)^* (1 - y)$ とした方が良いかもしれない.) この SDP の解が $\varepsilon > 0$ であれば性質 (T) を持つことが分かるが, 探索域を制限しているためその逆が成り立つことは保証されない. (なお本稿では G の元を同定するための語問題は無視することにする.) 実用上大抵は E として半径 2 の球 $B(2) := S \cup S^2$ を使う. なぜなら半径 3 の球はほとんどの場合計算機で実行可能でないからである. $|B(2)| \approx |S|^2$ であるから, 解くべき SDP のサイズは次元 $\approx |S|^4$, 制約条件 $|E^{-1}E| \approx |S|^4$ となる. これを実際に計算機で実行しようとするとき $|S|$ が数十のときに限界があるようである. 半径 2 の球というといかにも小さく感じるが, それでも幾つかの場合に性質 (T) が確認できるということは驚くべき経験的事実である ([7, 2, 3]). 計算機による証明からは新た

なこと学ぶことができないという人も世の中にはいるが、なぜそれが正しいのかを学ぶことはできずとも、それが正しいことをどうやったら確認できるのかを学ぶことができるのである。解答を求めるにあたってどこを探せばいいのかどうやって探せばいいのかといったことである。こうしたことも重要な数学的知見であろう。また計算機による証明は $SL(3, \mathbb{Z})$ などの良く知られた群の Kazhdan 定数の人手による評価を大幅に更新することにもなった。

仮に計算機が

$$\Delta^2 - \varepsilon_0 \Delta \approx \sum_{x,y \in E} P_{x,y} x^{-1} y$$

という解を見つけたとする。ここから厳密解の存在を保証するためには、任意の $f \in I[G]^h := \{f \in \mathbb{R}[G] : f = f^*, \sum_x f(x) = 0\}$ に対して、 $\|f\| \Delta - f \in \Sigma^2 \mathbb{R}[G]$ であることを使う。ここで $\|f\|$ は具体的に計算できる適当な重み付き ℓ_1 ノルムである。従って G が性質 (T) を持つことを示すには、 $P \approx LL^T$ と近似した後、精度保証付き計算により

$$\varepsilon_0 \gg \|\Delta^2 - \varepsilon_0 \Delta - \sum_z (\sum_x L_{x,z} x)^* (\sum_y L_{y,z} y)\|$$

であることを確認すればよいのである。一般的に言って、解を見つけることは難しくとも、与えられた解の検証は（計算機的に）たやすい。

この手法により $SL(d, \mathbb{Z})$, $d = 3, 4$, などの既に性質 (T) が示されている群について計算機による証明が得られた ([7, 2, 3]) が、 $\text{Aut}(F_d)$ のような「大きな」群に対しては計算機的能力不足により、アルゴリズムを完了することが出来なかった。

群対称 SDP:

(G, S) の対称群 $\Sigma := \{\alpha \in \text{Aut}(G) : \alpha(S) = S\}$ は $E = B(2)$ にも自然に作用する。このとき SDP の探索域を $P \in \mathbb{M}_E^+(\mathbb{R})$ から Σ の不動点環 $\mathbb{M}_E^+(\mathbb{R})^\Sigma$ に制限しても良く、 Σ のサイズが大きければ SDP の次元と制約条件を大幅に小さくできる。私は M. Kaluba と P. Nowak との共同研究 ([4]) で $G = \text{SAut}(F_5)$ を扱った。この場合、対称群 $\Sigma = (\bigoplus_{i=1}^5 \mathbb{Z}/2) \rtimes \mathfrak{S}_5$ が比較的大きいので ($|\Sigma| = 2^5 \cdot 5! = 3840$)、群対称 SDP により計算量を 100 分の 1 くらいにすることができ、結果、 $\text{SAut}(F_5)$ が性質 (T) を持つことを確認できた。これには Σ の表現論（有限次元 C^* 環 $\mathbb{M}_E(\mathbb{R})^\Sigma$ の既約分解を具体的に書き下すこと）及びポーランドのスーパーコンピューター (PL-Grid, それほどたいしたものじゃない) を使った。なお得られた解が実際に性質 (T) の条件を満たすことを検証するのは市販のデスクトップコンピューター (with 32GB RAM) でも可能である。（証明の検証にも高性能コンピューターが必要となると、誰にでも検証可能というわけにはいなくなる。こうした事態は将来多く起こるようになるであろうから、数学研究における厳密性の概念も、少なくとも部分的には、実験科学のそれに近づいていくということが予測される。）

まとめ：

問題

$\text{Aut}(F_d)$ は性質 (T) を持つか？

は前述の Lubotzky–Pak の論文 [6] の他にも Kazhdan の性質 (T) に関する標準的な教科書である [1, 7.1] や [5, 10.3] などに未解決問題として言及されている有名未解決問題である． $\text{Aut}(F_d)$ は $d \leq 3$ のとき性質 (T) を持たないことが既に知られている．今回の仕事で $d = 5$ の場合に性質 (T) を持つことが分かった．

定理 (Kaluba–Nowak–Ozawa [4])

$\text{Aut}(F_5)$ は性質 (T) を持つ．

これとそのほかの状況証拠を合わせて、上の「問題」は「予想」にアップグレードされた．

予想

$d \geq 5$ のとき $\text{Aut}(F_d)$ は性質 (T) を持つ．

数学研究の際に問題を解くに当たって、特定の答えが確実であるとの確信が役に立つことは非常に多い．今回の定理は問題の部分的解決であるばかりでなく、より一般の場合を「問題」から「予想」にしたという意義もある． $\text{Aut}(F_4)$ については今回の手法では性質 (T) を確認できなかった．（これは恐らく解が半径 2 の球 $B(2)$ 上に存在しないことを意味する．）その他の群に対するアルゴリズムの挙動から推測するに、 $\text{Aut}(F_4)$ について予想を立てるためには半径 3 の球 $B(3)$ でアルゴリズムを実行する必要があると思われる．これには今回使った計算機の 100 倍程度の能力が必要なので 10 年ほど待つ必要がある．また、 $\text{Aut}(F_6)$ についてアルゴリズムを $B(2)$ で実行するにもやはり同程度の能力が必要なので 10 年ほど待つ必要がある．もしこの研究を 5 年前に始めていたら恐らく計算機の能力不足により $\text{Aut}(F_5)$ について結果を出すことができず、研究は何ら新成果を挙げられずに挫折したものと考えられる．逆にもしこの研究を 5 年後に始めていたら群対称 SDP を使うまでもなく簡単に結果を出せていたはずである．

計算機の発展はハード・ソフトともに著しい．囲碁や将棋の世界では既に人間をはるかに上回る能力を見せているが、数学においても同様のことが私の生きているうちに起きるとは私は考えていない．しかし、正しい枠組みさえ与えられれば計算機がとてつもない能力を発揮するのは確かなことなので、今後、人間と計算機のタッグによる数学がより頻繁に、そしてより深刻に行われるようになるのは間違いのないと思われる．私は専門が作用素環論と関数解析的群論という抽象度の高い数学であることもあり、これまで研究に計算機を使う機会は一切なかった（論文・メールの読み書き等も研究の本質的な一部分ではあるがこれは除く）．今回の共同研究で私が部分的に解決した問題も計算機に関わりがあるとは 2, 3 年前まで誰も考えていなかったものである．計算機の能

力は時を追うごとに指数関数的に増大するので、ゴキブリの例えではないが、計算機で解ける問題が自分の周りに1つ見つかったということは実は既に30は存在しているのだと思う。数理新人の皆様には、計算機を扱えない数学者は今後大きなハンデを背負うことになるであろうと警告してこの話を終えることにしたい。

参考文献

- [1] B. Bekka, P. de la Harpe, and A. Valette; Kazhdan's property (T). *New Mathematical Monographs*, **11**. Cambridge University Press, Cambridge, 2008. xiv+472 pp.
- [2] K. Fujiwara and Y. Kabaya; Computing Kazhdan constants by semidefinite programming. *Experimental Mathematics*, to appear. arXiv:1703.04555
- [3] M. Kaluba and P. Nowak; Certifying Numerical Estimates of Spectral Gaps. *Groups Complexity Cryptology*, to appear. arXiv:1703.09680
- [4] M. Kaluba, P. Nowak and N. Ozawa; $\text{Aut}(\mathbb{F}_5)$ has property (T). *Preprint*. arXiv:1712.07167
- [5] A. Lubotzky; Discrete groups, expanding graphs and invariant measures. *Progress in Mathematics*, **125**. Birkhäuser Verlag, Basel, 1994. xii+195 pp.
- [6] A. Lubotzky and I. Pak; The product replacement algorithm and Kazhdan's property (T). *Journal of the American Mathematical Society* **14** (2001), 347–363.
- [7] T. Netzer and A. Thom; Kazhdan's property (T) via semidefinite optimization. *Experimental Mathematics* **24** (2015), 371–374.
- [8] N. Ozawa; Noncommutative real algebraic geometry of Kazhdan's property (T). *Journal of the Institute of Mathematics of Jussieu* **15** (2016), 85–90.