# **Numerical analysis** in the age of **data science** through the **Solvability Complexity Index Hierarchy**

**Matthew Colbrook**
(m.colbrook@damtp.cam.ac.uk)

University of Cambridge
+ École Normale Supérieure

www.damtp.cam.ac.uk/user/mjc249/home.html

# Special thanks to my collaborators!


Vegard Antun
Oslo


Lorna Ayton
Cambridge


Jonathan Ben-Artzi
Cardiff


Anders Hansen
Cambridge


Andrew Horning
MIT


Olavi Nevanlinna
Aalto


Bogdan Roman
Cambridge


Markus Seidel
West Saxon


Máté Szőke
Virginia Tech


Alex Townsend
Cornell


Marcus Webb
Manchester


Shmuel Weinberger
Chicago

# When can algorithms be trusted?

- **Ex1: Data-driven dynamical systems** **Error control and verification?**
- **Ex2: Trustworthiness in AI** **Stability and accuracy guarantees?**

# When can algorithms be trusted?

- **Ex1: Data-driven dynamical systems** — **Error control and verification?**
- **Ex2: Trustworthiness in AI** — **Stability and accuracy guarantees?**

**Why is this question essential?**

- Bedrock of numerical analysis.
- Reliable computations to back-up and test theories.
- Computed “solutions” meaningless without understanding error.

# When can algorithms be trusted?

- **Ex1: Data-driven dynamical systems** **Error control and verification?**
- **Ex2: Trustworthiness in AI** **Stability and accuracy guarantees?**

**Why is this question essential?**

- Bedrock of numerical analysis.
- Reliable computations to back-up and test theories.
- Computed “solutions” meaningless without understanding error.

**Toolkit** for classifying the difficulty of computational problems and proving the optimality of algorithms.

# Talk outline

- **Example 1:** Rigorous and verifiable data-driven dynamical systems
  - **Upper bounds (on difficulty):** Positive results on what’s possible.
- **A toolkit:** Solvability Complexity Index Hierarchy
  - Classification for infinite-dimensional spectral problems and beyond.
- **Example 2:** Smale's 18th problem, “What are the limits of AI?”
  - **Lower bounds (on difficulty):** Use SCI techniques to prove impossibility results.

**Toolkit** for classifying the difficulty of computational problems and proving the optimality of algorithms.

# Example 1: Rigorous and verifiable data-driven dynamical systems

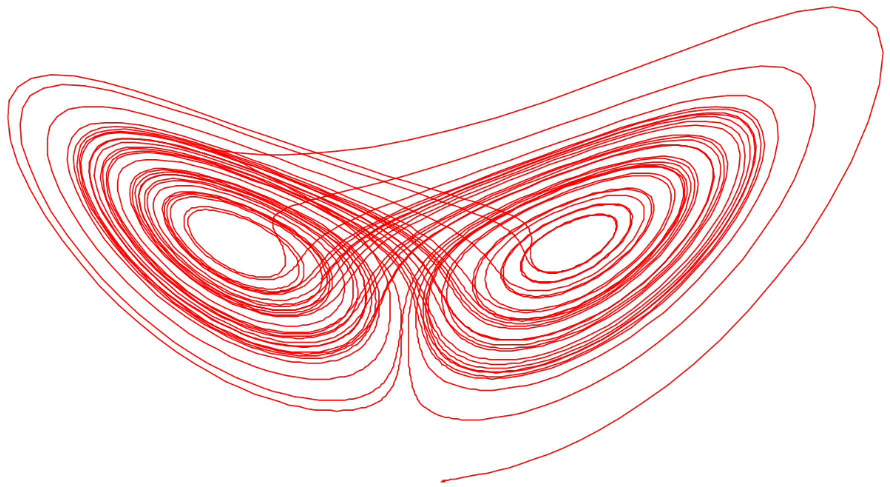
**Upper bounds:** Positive results on what's possible.

# Data-driven dynamical systems

- State $x \in \Omega \subseteq \mathbb{R}^d$, ***unknown*** function $F: \Omega \to \Omega$ governs dynamics

$$x_{n+1} = F(x_n)$$

- **Goal:** Learn about system from data $\{x^{(m)}, y^{(m)} = F(x^{(m)})\}_{m=1}^{M}$
  - E.g., **data from** trajectories, experimental measurements, simulations, …
  - E.g., **used for** forecasting, control, design, understanding, …
- **Applications:** chemistry, climatology, electronics, epidemiology, finance, fluids, molecular dynamics, neuroscience, plasmas, robotics, video processing, …



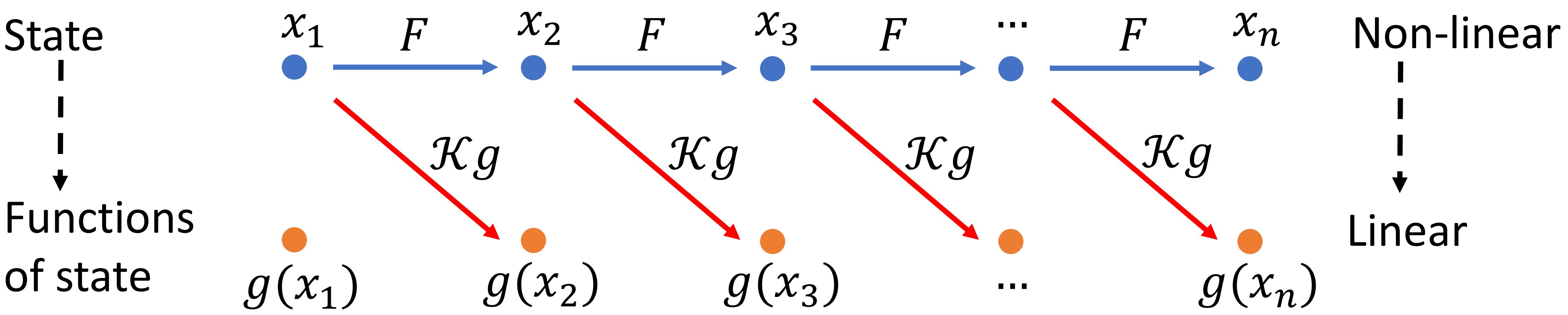
**Can we develop verified methods?**

# Operator viewpoint

- **Koopman operator** $\mathcal{K}$ acts on <u>functions</u> $g: \Omega \to \mathbb{C}$

$$[\mathcal{K}g](x) = g(F(x))$$

- $\mathcal{K}$ is ***linear*** but acts on an ***infinite-dimensional*** space.




- Work in $L^2(\Omega, \omega)$ for positive measure $\omega$, with inner product $\langle \cdot, \cdot \rangle$.


- Koopman, "*Hamiltonian systems and transformation in Hilbert space*," **PNAS**, 1931.
- Koopman, v. Neumann, "*Dynamical systems of continuous spectra*," **PNAS**, 1932.

# Koopman mode decomposition

$x_{n+1} = F(x_n)$

$[\mathcal{K}g](x) = g(F(x))$

eigenfunction of $\mathcal{K}$

generalised eigenfunction of $\mathcal{K}$

$$g(x) = \sum_{\text{eigenvalues } \lambda_j} c_{\lambda_j} \varphi_{\lambda_j}(x) + \int_{-\pi}^{\pi} \phi_{\theta,g}(x)\, \mathrm{d}\theta$$

$$g(x_n) = [\mathcal{K}^n g](x_0) = \sum_{\text{eigenvalues } \lambda_j} c_{\lambda_j} {\lambda_j}^n \varphi_{\lambda_j}(x_0) + \int_{-\pi}^{\pi} e^{in\theta} \phi_{\theta,g}(x_0)\, \mathrm{d}\theta$$

**Encodes:** geometric features, invariant measures, transient behaviour, long-time behaviour, coherent structures, quasiperiodicity, etc.

**GOAL: Data-driven approximation of $\mathcal{K}$ and its spectral properties.**


- Mezić, "*Spectral properties of dynamical systems, model reduction and decompositions,*" **Nonlinear Dynamics**, 2005.

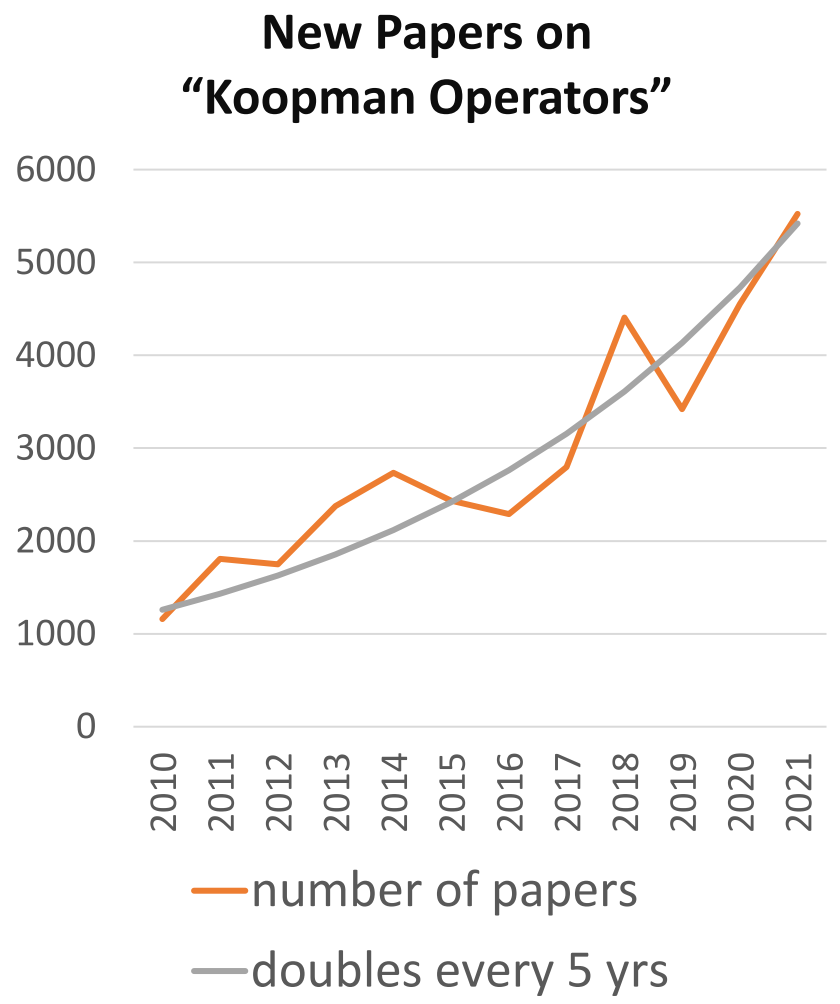
# Koopmania*: a revolution in the big data era

≈35,000 papers over last decade!

***Very* little on convergence guarantees or verification.**

**Why is this lacking?**

- K. operators have been distinct from NA community.
- Dealing with infinite dim. is notoriously hard …




**Wikipedia*: *"its wild surge in popularity is sometimes jokingly called 'Koopmania'"*

# Can we compute spectral properties in inf. dim.?

$$\mathrm{Spec}(\mathcal{K}) = \{\lambda \in \mathbb{C} : \mathcal{K} - \lambda I \text{ is not invertible}\}$$

*"Operators that arise in practice are not **diagonalized**, and it is often very hard to locate the spectrum. Thus, one has to settle for numerical approximations. Unfortunately, there are **no proven general techniques**."* W. Arveson, Berkeley (1994)

**Naïve:** $\mathcal{K} \longrightarrow \mathbb{K} \in \mathbb{C}^{N\times N}$ + compute e-values, **problems:**

1) **"Too much":** Approximate spurious modes $\lambda \notin \mathrm{Spec}(\mathcal{K})$ - "spectral pollution"
2) **"Too little":** Miss parts of $\mathrm{Spec}(\mathcal{K})$
3) **Continuous spectra**
4) **Verification:** Which part of an approximation can we trust?


- Arveson, *"The role of $C^*$-algebras in infinite dimensional numerical linear algebra,"* **Contemp. Math.**, 1994.
- Davies, *"Linear operators and their spectra,"* **CUP**, 2007.
- Brunton, Kutz, *"Data-driven Science and Engineering: Machine learning, Dynamical systems, and Control,"* **CUP**, 2019.

# Dynamic Mode Decomposition (DMD)

$$\{x^{(m)}, y^{(m)} = F(x^{(m)})\}_{m=1}^{M}$$

Given dictionary $\{\psi_1, \dots, \psi_N\}$ of functions $\psi_j : \Omega \to \mathbb{C}$

$$\langle \psi_k, \psi_j \rangle \approx \sum_{m=1}^{M} w_m \overline{\psi_j(x^{(m)})} \psi_k(x^{(m)}) = \Bigg[ \underbrace{\begin{pmatrix} \psi_1(x^{(1)}) & \cdots & \psi_N(x^{(1)}) \\ \vdots & \ddots & \vdots \\ \psi_1(x^{(M)}) & \cdots & \psi_N(x^{(M)}) \end{pmatrix}^*}_{\Psi_X} \underbrace{\begin{pmatrix} w_1 & & \\ & \ddots & \\ & & w_M \end{pmatrix}}_{W} \underbrace{\begin{pmatrix} \psi_1(x^{(1)}) & \cdots & \psi_N(x^{(1)}) \\ \vdots & \ddots & \vdots \\ \psi_1(x^{(M)}) & \cdots & \psi_N(x^{(M)}) \end{pmatrix}}_{\Psi_X} \Bigg]_{jk}$$

$$\langle \mathcal{K}\psi_k, \psi_j \rangle \approx \sum_{m=1}^{M} w_m \overline{\psi_j(x^{(m)})} \underbrace{\psi_k(y^{(m)})}_{[\mathcal{K}\psi_k](x^{(m)})} = \Bigg[ \underbrace{\begin{pmatrix} \psi_1(x^{(1)}) & \cdots & \psi_N(x^{(1)}) \\ \vdots & \ddots & \vdots \\ \psi_1(x^{(M)}) & \cdots & \psi_N(x^{(M)}) \end{pmatrix}^*}_{\Psi_X} \underbrace{\begin{pmatrix} w_1 & & \\ & \ddots & \\ & & w_M \end{pmatrix}}_{W} \underbrace{\begin{pmatrix} \psi_1(y^{(1)}) & \cdots & \psi_N(y^{(1)}) \\ \vdots & \ddots & \vdots \\ \psi_1(y^{(M)}) & \cdots & \psi_N(y^{(M)}) \end{pmatrix}}_{\Psi_Y} \Bigg]_{jk}$$

$$\mathcal{K} \longrightarrow \quad \mathbb{K} = (\Psi_X{}^* W \Psi_X)^{-1} \Psi_X{}^* W \Psi_Y \in \mathbb{C}^{N \times N}$$


- Schmid, “*Dynamic mode decomposition of numerical and experimental data,*” **Journal of fluid mechanics**, 2010.
- Kutz, Brunton, Brunton, Proctor, “*Dynamic mode decomposition: data-driven modeling of complex systems,*” **SIAM**, 2016.
- Williams, Kevrekidis, Rowley “*A data-driven approximation of the Koopman operator: Extending dynamic mode decomposition,*” **Journal of Nonlinear Science**, 2015.

# Residual DMD (ResDMD): Approx. $\mathcal{K}$ and $\mathcal{K}^*\mathcal{K}$

$$\langle \psi_k, \psi_j \rangle \approx \sum_{m=1}^{M} w_m \overline{\psi_j(x^{(m)})}\, \psi_k(x^{(m)}) = [\underbrace{\Psi_X{}^* W \Psi_X}_{G}]_{jk}$$

$$\langle \mathcal{K}\psi_k, \psi_j \rangle \approx \sum_{m=1}^{M} w_m \overline{\psi_j(x^{(m)})}\, \underbrace{\psi_k(y^{(m)})}_{[\mathcal{K}\psi_k](x^{(m)})} = [\underbrace{\Psi_X{}^* W \Psi_Y}_{K_1}]_{jk}$$

Error control

$$\langle \mathcal{K}\psi_k, \mathcal{K}\psi_j \rangle \approx \sum_{m=1}^{M} w_m \overline{\psi_j(y^{(m)})}\, \psi_k(y^{(m)}) = [\underbrace{\Psi_Y{}^* W \Psi_Y}_{K_2}]_{jk}$$

**Residuals:** $g = \sum_{j=1}^{N} \mathbf{g}_j \psi_j,\ \|\mathcal{K}g - \lambda g\|^2 \approx \mathbf{g}^*[K_2 - \lambda K_1{}^* - \bar{\lambda} K_1 + |\lambda|^2 G]\mathbf{g}$


- C., Townsend, "*Rigorous data-driven computation of spectral properties of Koopman operators for dynamical systems,*" **Communications on Pure and Applied Mathematics**, under review.
- C., Ayton, Szőke, "*Residual Dynamic Mode Decomposition,*" **Journal of Fluid Mechanics**, under review.

# Example of an upper bound

$$\mathrm{res}(\lambda, \mathbf{g}) = \sqrt{\frac{\mathbf{g}^*\left[K_2 - \lambda {K_1}^* - \bar{\lambda} K_1 + |\lambda|^2 G\right]\mathbf{g}}{\mathbf{g}^* G \mathbf{g}}}, \qquad \mathrm{Spec}_\varepsilon(\mathcal{K}) = \cup_{\|\mathcal{B}\| \le \varepsilon} \mathrm{Spec}(\mathcal{K} + \mathcal{B})$$

1. Compute $G, K_1, K_2 \in \mathbb{C}^{N\times N}$.
2. For $z_k$ in comp. grid, compute $\tau_k = \min_{g=\sum_{j=1}^{N} \mathbf{g}_j \psi_j} \mathrm{res}(z_k, g)$, corresponding $g_k$ (gen. SVD).
3. **Output:** $\{z_k : \tau_k < \varepsilon\}$ (approx. of $\mathrm{Spec}_\varepsilon(\mathcal{K})$), $\{g_k : \tau_k < \varepsilon\}$ ($\varepsilon$-pseudo-eigenfunctions).

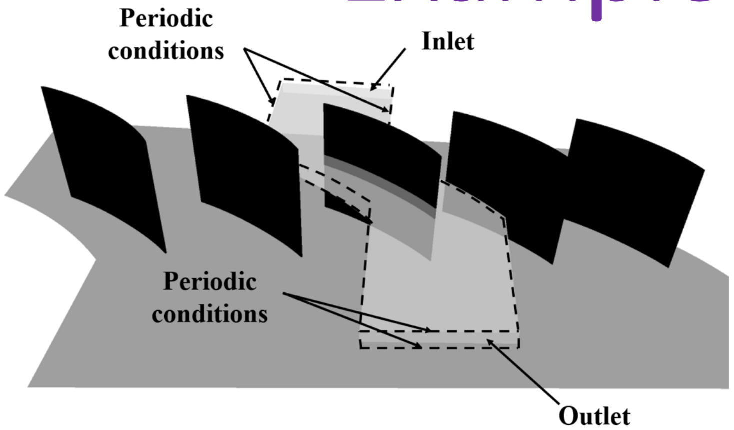
**First convergent method for general $\mathcal{K}$**

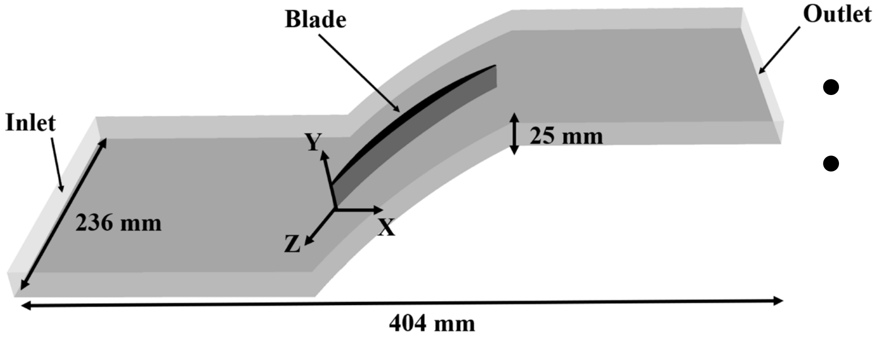
**Theorem**: Suppose the quadrature rule converges.
- **Error control:** $\{z_k : \tau_k < \varepsilon\} \subseteq \mathrm{Spec}_\varepsilon(\mathcal{K})$ (as $M \to \infty$)
- **Convergence:** Converges locally uniformly to $\mathrm{Spec}_\varepsilon(\mathcal{K})$ (as $N \to \infty$)

Similarly, overcome: **1) "too much", 2) "too little", 3) cts spectra, 4) verification.**

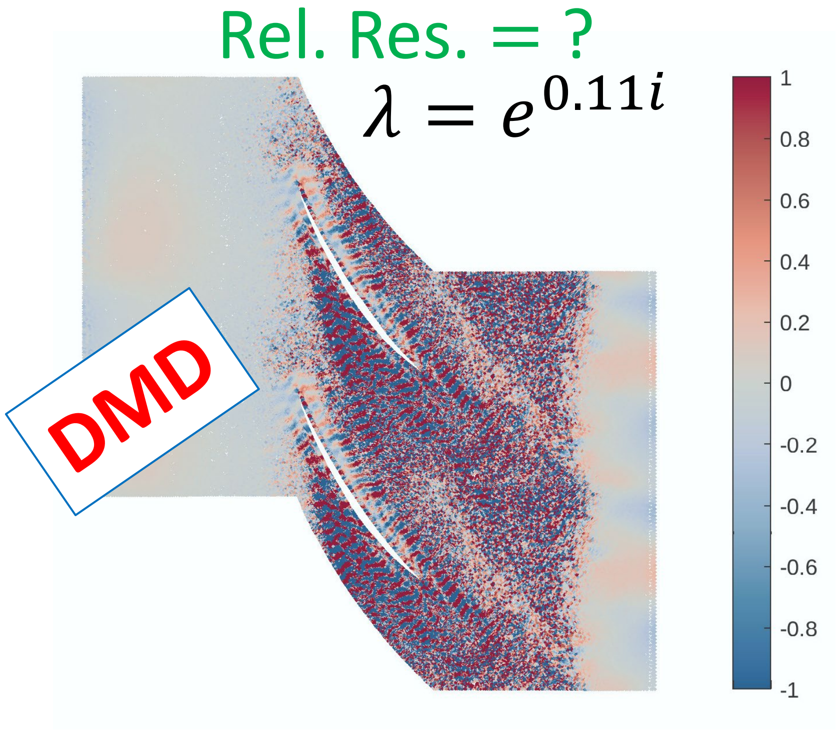
**Paves the way for rigorous data-driven Koopmania!**

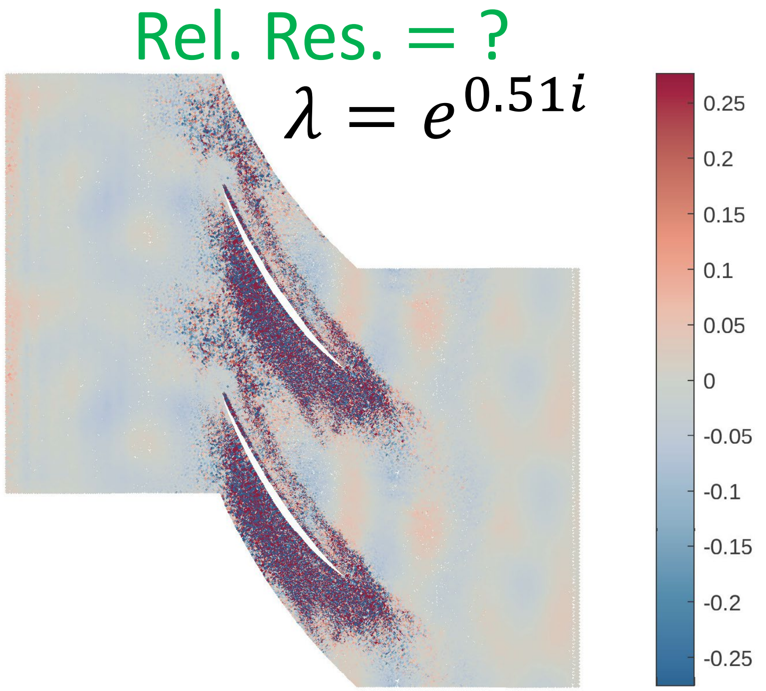
# Example: pressure field of turbulent flow

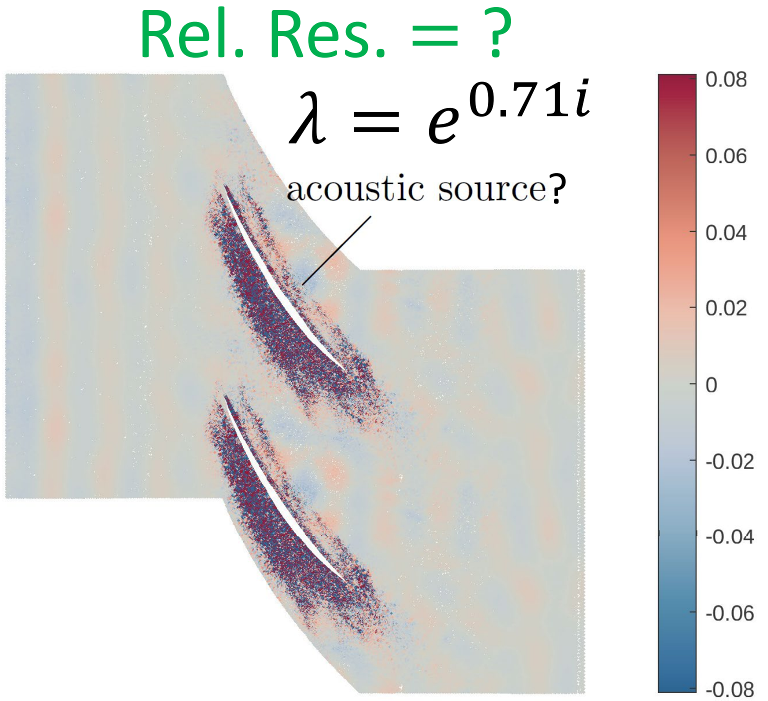


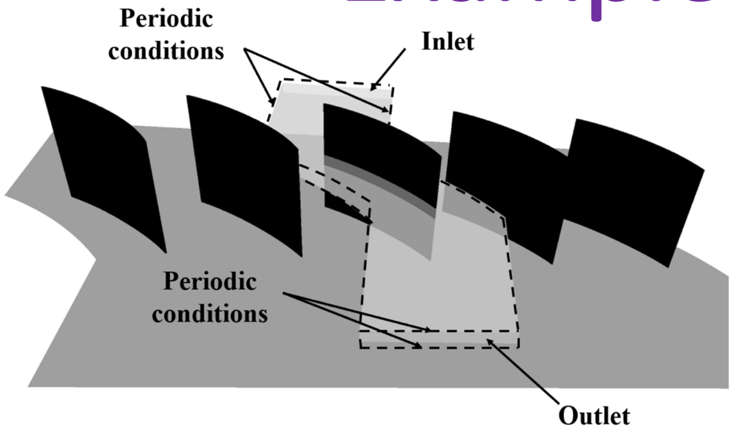

- Reynolds number $\approx 3.9 \times 10^5$
- Ambient dimension $\approx 300{,}000$ (number of measurement points)

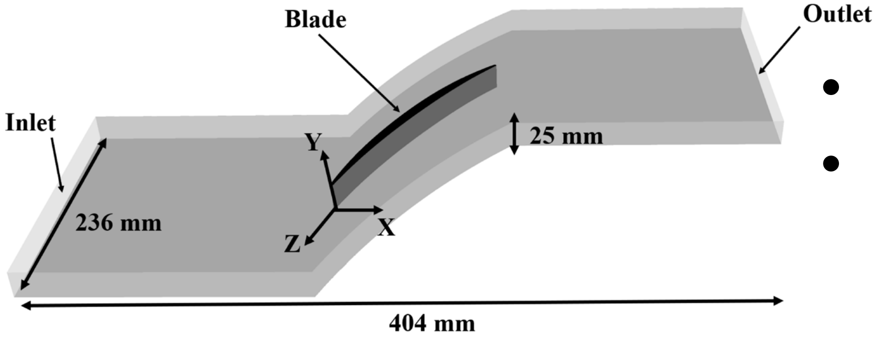


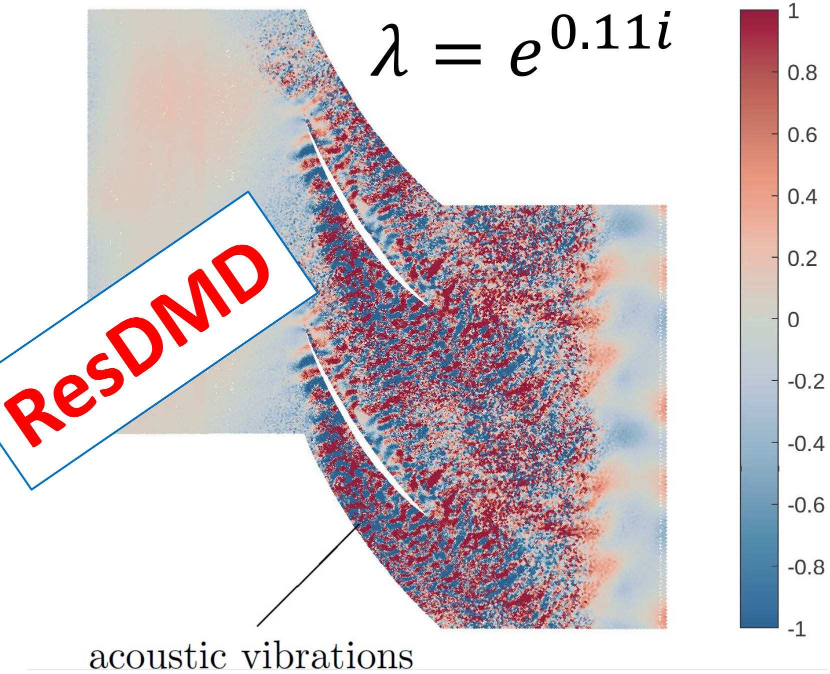
# Example: pressure field of turbulent flow



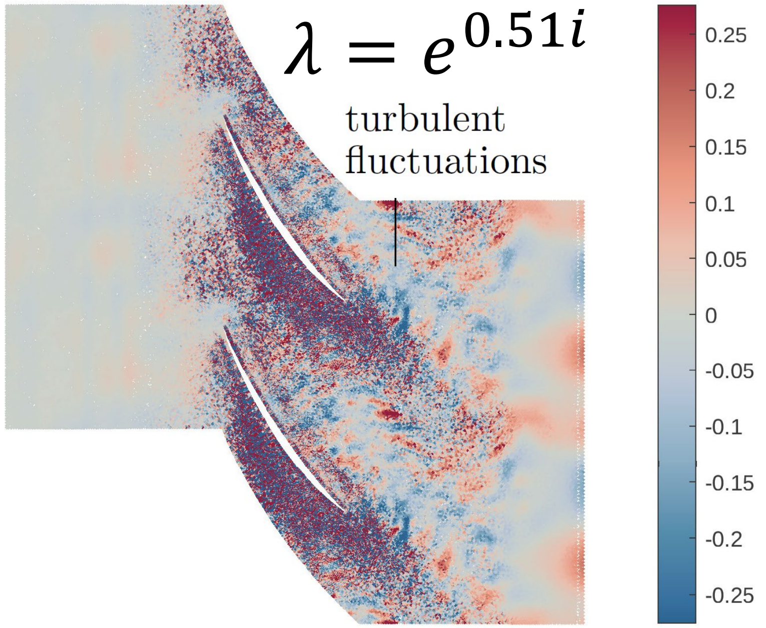




- Reynolds number $\approx 3.9 \times 10^5$
- Ambient dimension $\approx 300{,}000$ (number of measurement points)

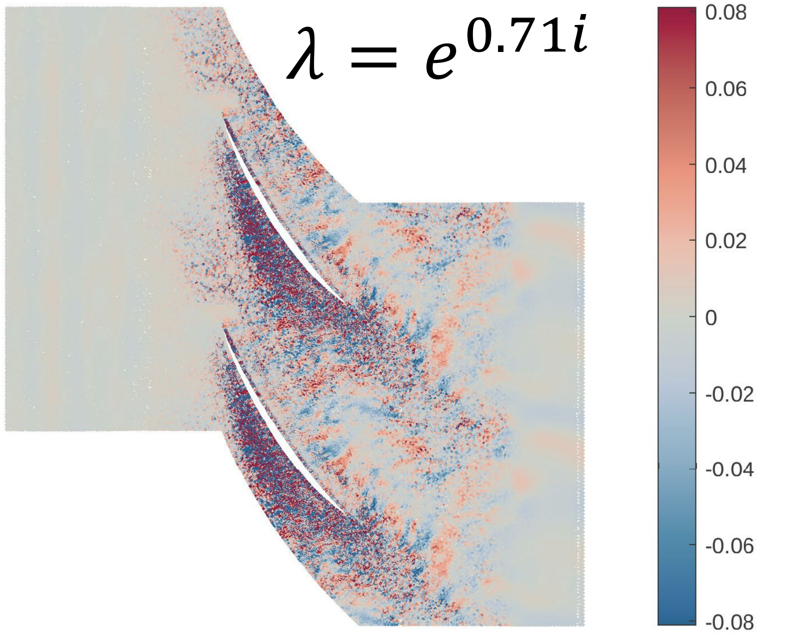
Rel. Res. $\leq 0.0054$




Rel. Res. $\leq 0.0128$




Rel. Res. $\leq 0.0196$



Previous algorithm $\Gamma_M$ (with adaptive $N = N(M)$):

$$\lim_{\varepsilon\downarrow 0}\lim_{M\to\infty}\Gamma_M\left(\left\{x^{(m)}, y^{(m)} = F\left(x^{(m)}\right)\right\}_{m=1}^{M}, \varepsilon\right) = \mathrm{Spec}(\mathcal{K})$$

Phenomena of "successive limits" widespread…

# A toolkit: Solvability Complexity Index Hierarchy

# Solvability Complexity Index Hierarchy

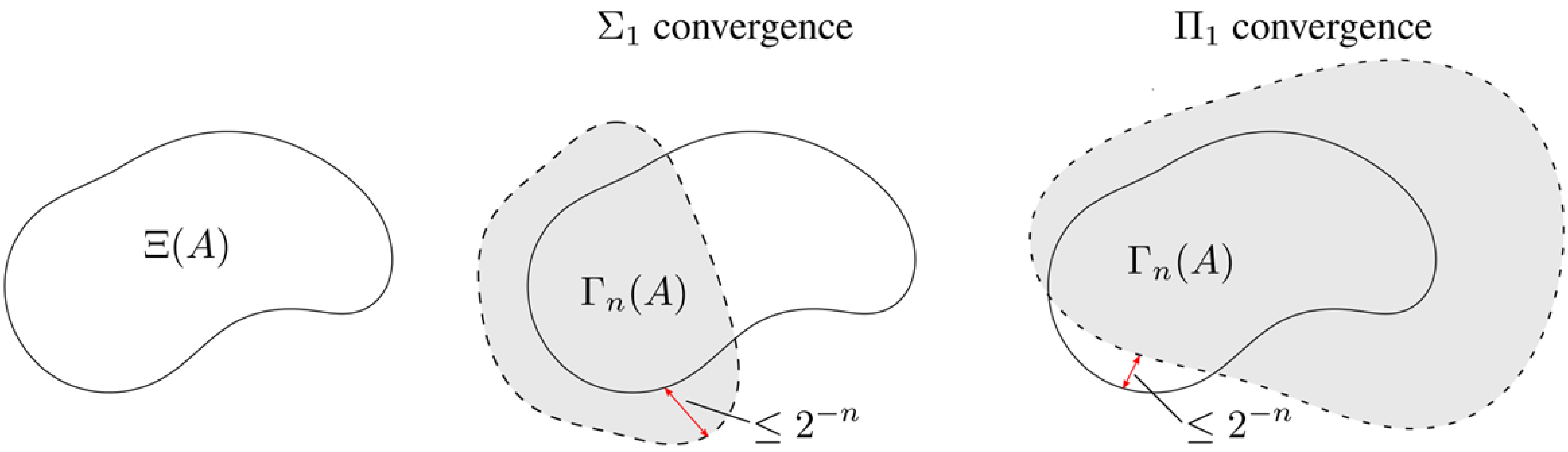
For $A \in \Omega$, want to compute $\Xi\colon \Omega \to (\mathcal{M}, d)$ metric space

- $\Delta_0$: Problems solved in finite time (v. rare).
- $\Delta_1$: Problems solved in "one limit" with full error control:
$$d(\Gamma_n(A), \Xi(A)) \leq 2^{-n}$$
- $\Delta_2$: Problems solved in "one limit" (SCI=1):
$$\lim_{n\to\infty} \Gamma_n(A) = \Xi(A)$$
- $\Delta_3$: Problems solved in "two successive limits" (SCI=2):
$$\lim_{n\to\infty} \lim_{m\to\infty} \Gamma_{n,m}(A) = \Xi(A)$$

and so on…


- C., *"The Foundations of Infinite-Dimensional Spectral Computations,"* **Cambridge**, PhD thesis.
- Ben-Artzi, C., Hansen, Nevanlinna, Seidel, *"On the solvability complexity index hierarchy and towers of algorithms."*
- Hansen, *"On the solvability complexity index, the $n$-pseudospectrum and approximations of spectra of operators,"* **JAMS**, 2011.
- McMullen, *"Families of rational maps and iterative root-finding algorithms,"* **Annals of Mathematics**, 1987.
- Smale, *"The fundamental theorem of algebra and complexity theory,"* **Bulletin of the AMS**, 1981.

# Error control for spectral problems




- $\Sigma_1 \subsetneq \Delta_2$: $\lim_{n\to\infty} \Gamma_n(A) = \Xi(A)$, $\max_{z\in\Gamma_n(A)} \mathrm{dist}\big(z, \Xi(A)\big) \leq 2^{-n}$
- $\Pi_1 \subsetneq \Delta_2$: $\lim_{n\to\infty} \Gamma_n(A) = \Xi(A)$, $\max_{z\in\Xi(A)} \mathrm{dist}(z, \Gamma_n(A)) \leq 2^{-n}$

**NB: Typically, eigensolvers for PDEs prove $\Delta_2$, not optimal $\Sigma_1$…**

# $\Sigma_1$ example: e-values with guaranteed error bounds

$$A = -\nabla^2 + x^2 + V(x) \text{ on } \mathbb{R}^1$$

| $V$ | $\cos(x)$ | $\tanh(x)$ | $\exp(-x^2)$ | $1/(1+x^2)$ |
|---|---|---|---|---|
| $E_0$ | 1.7561051579 | 0.8703478514 | 1.6882809272 | 1.7468178026 |
| $E_1$ | 3.3447026910 | 2.9666370800 | 3.3395578680 | 3.4757613534 |
| $E_2$ | 5.0606547136 | 4.9825969775 | 5.2703748823 | 5.4115076464 |
| $E_3$ | 6.8649969390 | 6.9898951678 | 7.2225903394 | 7.3503220313 |
| $E_4$ | 8.7353069954 | 8.9931317537 | 9.1953373991 | 9.3168983920 |

Can deal with mix of cts and discrete spectra, other domains, other PDEs etc.

# Small sample of classification theorems

Increasing difficulty →

**Error control**

$$
\begin{array}{ccccccccccccccc}
\Pi_0 & & & & \Pi_1 & & & & \Pi_2 & & & & \Pi_3 & & \\
\| & & & \rotatebox{45}{$\subsetneq$} & & \rotatebox{-45}{$\subsetneq$} & & \rotatebox{45}{$\subsetneq$} & & \rotatebox{-45}{$\subsetneq$} & & \rotatebox{45}{$\subsetneq$} & & \cdot^{\cdot^{\cdot}} & \\
\Delta_0 & \subsetneq & \Delta_1 & \subsetneq & \Sigma_1 \cup \Pi_1 & \subsetneq & \Delta_2 & \subsetneq & \Sigma_2 \cup \Pi_2 & \subsetneq & \Delta_3 & \subsetneq & \Sigma_3 \cup \Pi_3 & \ldots & \\
\| & & & \rotatebox{-45}{$\subsetneq$} & & \rotatebox{45}{$\subsetneq$} & & \rotatebox{-45}{$\subsetneq$} & & \rotatebox{45}{$\subsetneq$} & & \rotatebox{-45}{$\subsetneq$} & & \ddots & \\
\Sigma_0 & & & & \Sigma_1 & & & & \Sigma_2 & & & & \Sigma_3 & &
\end{array}
$$

# Small sample of classification theorems

Increasing difficulty

**Error control**

$$\begin{array}{ccccccccccccccc}
\Pi_0 & & & & & \Pi_1 & & & & \Pi_2 & & & & \Pi_3 & \\
\| & & & & \rotatebox{45}{$\subsetneq$} & & \rotatebox{-45}{$\subsetneq$} & & \rotatebox{45}{$\subsetneq$} & & \rotatebox{-45}{$\subsetneq$} & & \rotatebox{45}{$\subsetneq$} & & \ddots \\
\Delta_0 & \subsetneq & \Delta_1 & \subsetneq & \Sigma_1 \cup \Pi_1 & & \subsetneq & \Delta_2 & \subsetneq \Sigma_2 \cup \Pi_2 \subsetneq & & & \Delta_3 & \subsetneq \Sigma_3 \cup \Pi_3 & \ldots & \\
\| & & & & \rotatebox{-45}{$\subsetneq$} & & \rotatebox{45}{$\subsetneq$} & & \rotatebox{-45}{$\subsetneq$} & & \rotatebox{45}{$\subsetneq$} & & \rotatebox{-45}{$\subsetneq$} & & \iddots \\
\Sigma_0 & & & & & \Sigma_1 & & & & \Sigma_2 & & & & \Sigma_3 &
\end{array}$$

Spectra of $\mathcal{K}$

Continuous spectra of $\mathcal{K}$ (different regularity assumptions)

# Small sample of classification theorems

Increasing difficulty

**Error control**

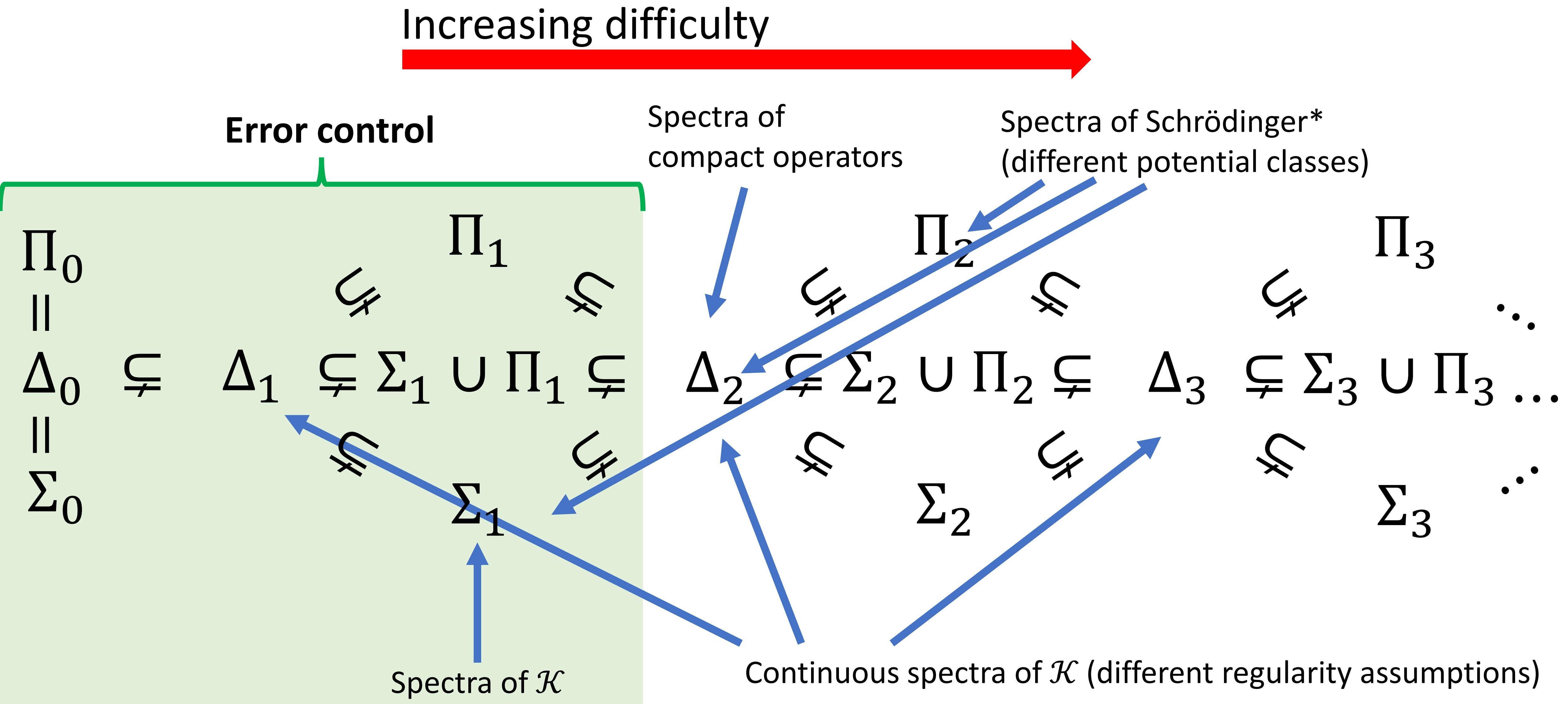
Spectra of compact operators

$$
\begin{tikzcd}
\Pi_0 \arrow[d, phantom, "\Vert"] & & \Pi_1 \arrow[dr, phantom, "\subsetneq"] & & \Pi_2 \arrow[dr, phantom, "\subsetneq"] & & \Pi_3 \arrow[dr, phantom, "\iddots"] & \\
\Delta_0 \arrow[r, phantom, "\subsetneq"] \arrow[d, phantom, "\Vert"] & \Delta_1 \arrow[ur, phantom, "\subsetneq"] \arrow[dr, phantom, "\subsetneq"] & \Sigma_1 \cup \Pi_1 \arrow[l, phantom, "\supsetneq"] \arrow[r, phantom, "\subsetneq"] & \Delta_2 \arrow[ur, phantom, "\subsetneq"] \arrow[dr, phantom, "\subsetneq"] & \Sigma_2 \cup \Pi_2 \arrow[l, phantom, "\supsetneq"] \arrow[r, phantom, "\subsetneq"] & \Delta_3 \arrow[ur, phantom, "\subsetneq"] \arrow[dr, phantom, "\subsetneq"] & \Sigma_3 \cup \Pi_3 \arrow[l, phantom, "\supsetneq"] & \dots \\
\Sigma_0 & & \Sigma_1 \arrow[ur, phantom, "\subsetneq"] & & \Sigma_2 \arrow[ur, phantom, "\subsetneq"] & & \Sigma_3 \arrow[ur, phantom, "\ddots"] &
\end{tikzcd}
$$

Spectra of $\mathcal{K}$

Continuous spectra of $\mathcal{K}$ (different regularity assumptions)

# Small sample of classification theorems




*Open problem of Schwinger*: “The special canonical group,” “Unitary operator bases,” PNAS, 1960.

# Small sample of classification theorems

Increasing difficulty

**Error control**

Spectra of compact operators

Spectra of Schrödinger* (different potential classes)

$$\Pi_0 = \Delta_0 = \Sigma_0$$

$$\Delta_0 \subsetneq \Delta_1 \subsetneq \Sigma_1 \cup \Pi_1 \subsetneq \Delta_2 \subsetneq \Sigma_2 \cup \Pi_2 \subsetneq \Delta_3 \subsetneq \Sigma_3 \cup \Pi_3 \ldots$$

$$\Delta_1 \subsetneq \Pi_1 \subsetneq \Delta_2, \quad \Delta_1 \subsetneq \Sigma_1 \subsetneq \Delta_2, \quad \Delta_2 \subsetneq \Pi_2 \subsetneq \Delta_3, \quad \Delta_2 \subsetneq \Sigma_2 \subsetneq \Delta_3, \quad \Delta_3 \subsetneq \Pi_3 \ldots, \quad \Delta_3 \subsetneq \Sigma_3 \ldots$$

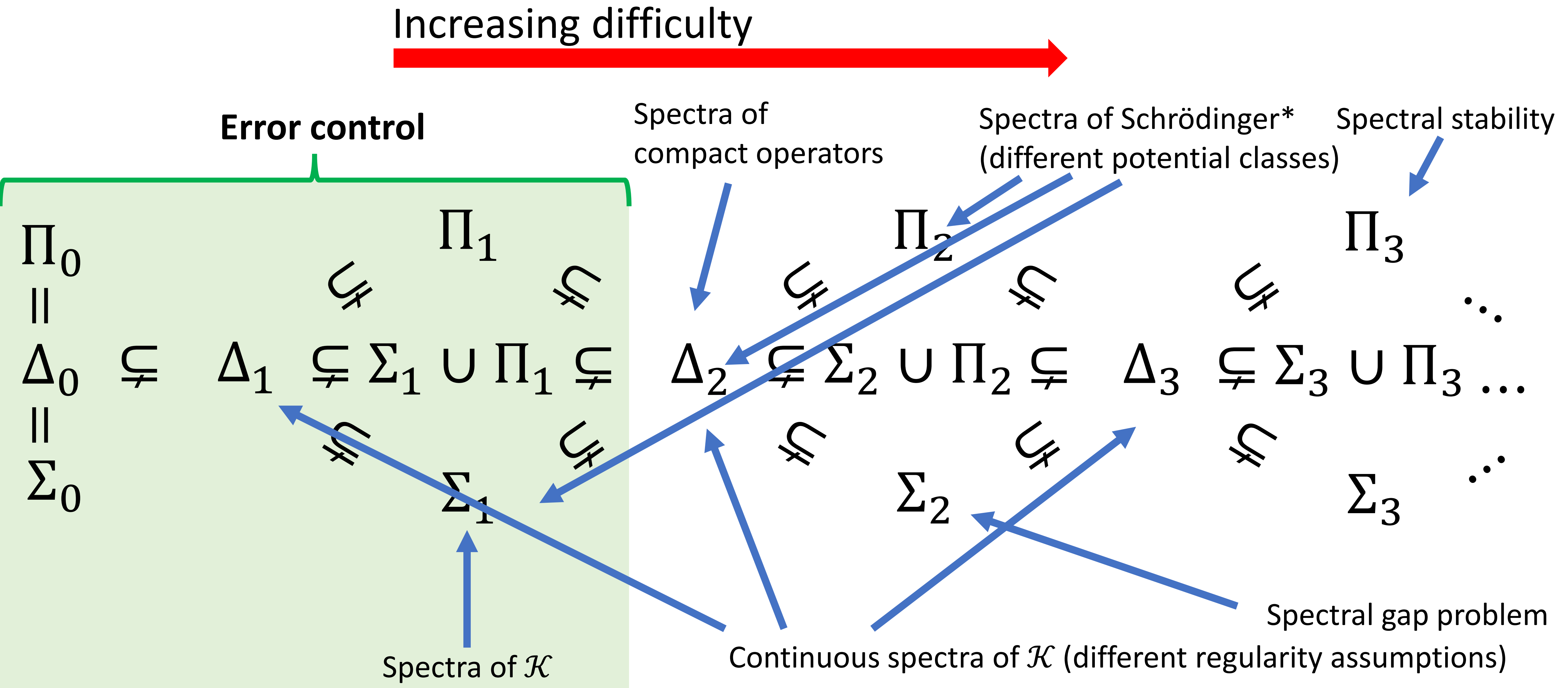
Spectra of $\mathcal{K}$

Spectral gap problem

Continuous spectra of $\mathcal{K}$ (different regularity assumptions)

*_Open problem of Schwinger_: "The special canonical group," "Unitary operator bases," PNAS, 1960.

# Small sample of classification theorems




**Open problem of Schwinger*: “The special canonical group,” “Unitary operator bases,” PNAS, 1960.

# Some success stories in inf. dim. spec. comp.

- Spectra with $\Sigma_1$ error control (v. large class of disc. ops and PDEs)
  - C., Roman, Hansen, *"How to compute spectra with error control,"* **PRL**, 2019.
  - C., Hansen, *"The foundations of spectral computations via the solvability complexity index hierarchy,"* **JEMS**, under revisions.
- Spectral measures and type (classification varies from $\Delta_1$ to $\Sigma_3$)
  - Webb, Olver, *"Spectra of Jacobi operators via connection coefficient matrices,"* **CIMP**, 2021.
  - C., *"Computing spectral measures and spectral types,"* **CIMP,** 2021.
  - C., Horning, Townsend, *"Computing spectral measures of self-adjoint operators,"* **SIAM Rev**, 2021.
- Resonances ($\Delta_2 \backslash \Sigma_1 \cup \Pi_1$)
  - Ben-Artzi, Marletta, Rösler, *"Computing scattering resonances,"* **JEMS**, 2022.
  - Ben-Artzi, Marletta, Rösler, *"Computing the sound of the sea in a seashell,"* **FOCM**, 2022.
- Zoo of problems (e.g., fractal dims, capacity, radii etc.) – up to $\Sigma_6$!!!!
  - C., *"On the computation of geometric features of spectra of linear operators on Hilbert spaces,"* **FOCM**, under revisions.

**General technique for lower bounds by embedding combinatorial problems.**


E.g., ground state of quasicrystal


E.g., continuous spectra of graphene

# Remarks

- Any model of computation.
  (lower bds universal, upper bds can be realized via interval arith.)
- Practical: “Spot” info or subclass needed to lower difficulty.
- Tells us what we can or cannot do.
- Existing hierarchies become special cases.
- **Extends beyond spectral problems:** Foundations of AI, PDEs (e.g., time-dep. Schrödinger eq. on $L^2(\mathbb{R}^d)$ with error control), optimisation (e.g., guarantees), computer-assisted proofs, …

# Example 2: Smale's 18th problem “What are the limits of AI?”

*“Very often, the creation of a technological artifact precedes the science that goes with it. The steam engine was invented before thermodynamics. Thermodynamics was invented to explain the steam engine, essentially the* ***limitations*** *of it.* ***What we are after is the equivalent of thermodynamics for intelligence.****”* Yann LeCun

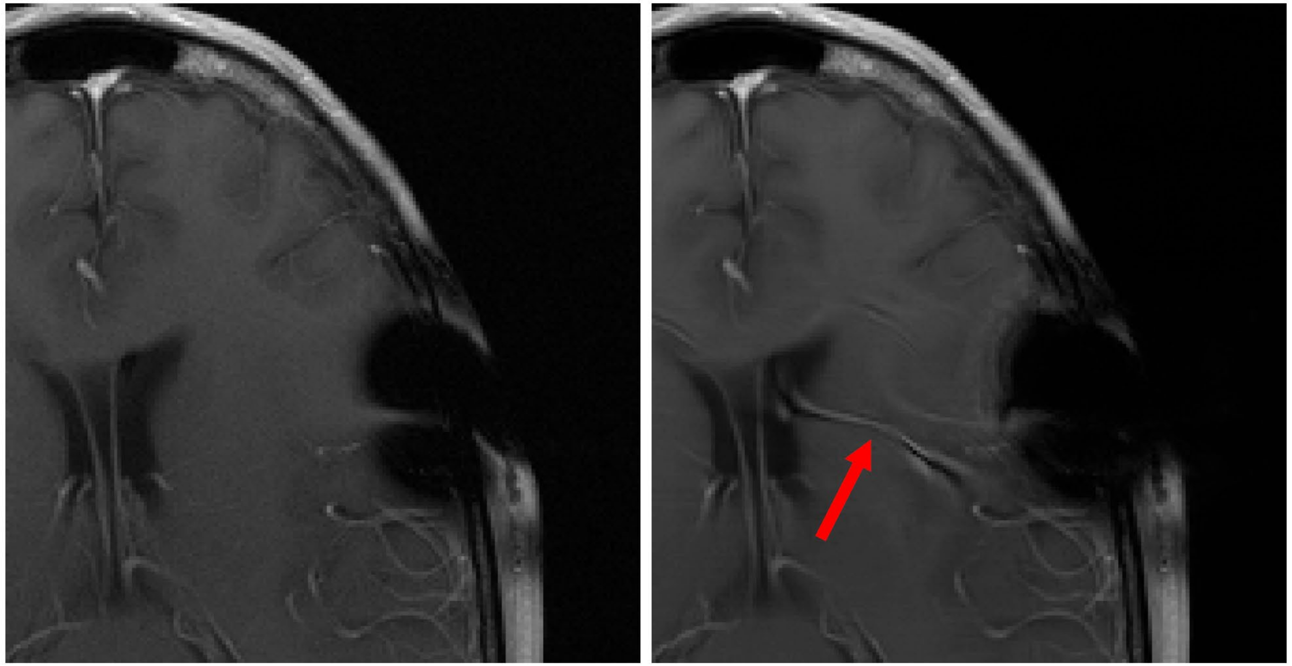
**Lower bounds:** Use SCI techniques to prove impossibility results.

(Different techniques needed for training problems.)

**S. Smale’s list of problems for the 21st century (requested by V. Arnold), inspired by Hilbert’s list*

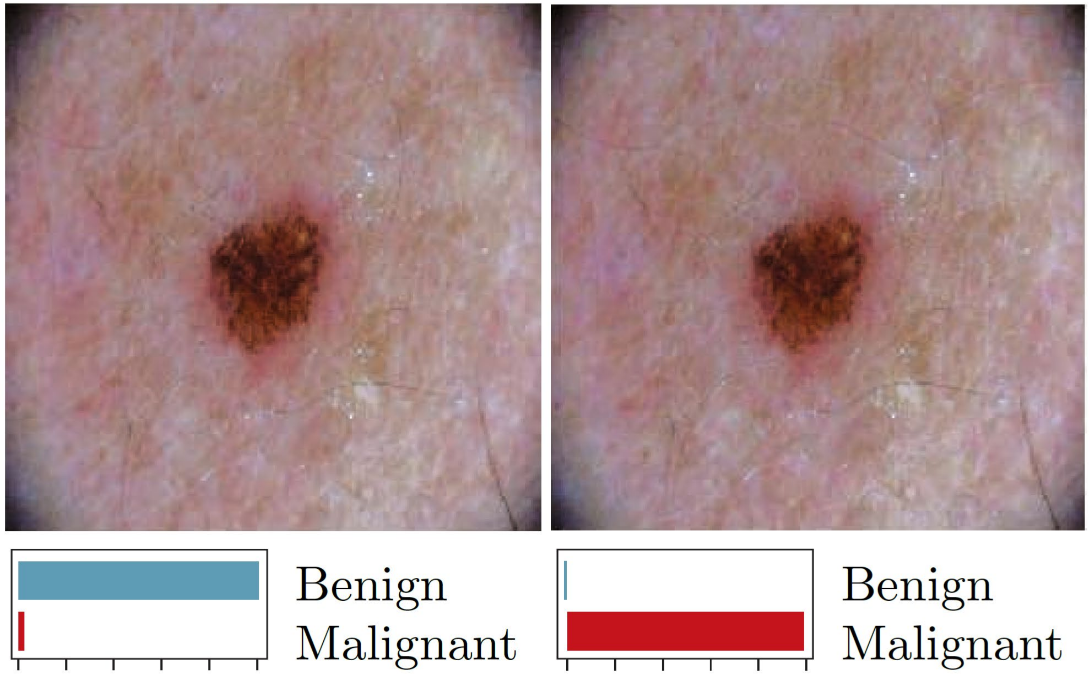
# Problem: hallucinations and instability

## Hallucinations in image reconstruction




“**AI generated hallucination**”, from Facebook and NYU’s ***FastMRI challenge*** 2020

## Instabilities in medical diagnosis




From Finlayson et al., “*Adversarial attacks on medical machine learning,*” **Science**, 2019.

**When can we make AI robust and trustworthy?**

# Example of the limits of deep learning

**Paradox:** “Nice” linear inverse problems where a *stable* and *accurate* neural network for image reconstruction exists, but it can never be trained!

E.g., suppose we want to solve (holds for much more general problems)

$$\min_{x \in \mathbb{C}^N} \|x\|_{l^1} + \lambda \|Ax - y\|_{l_2}^2$$

$$A \in \mathbb{C}^{m \times N} \text{ (modality}, m < N), \qquad S = \{y_j\}_{j=1}^{R} \text{ (samples)}$$

Arises when given $y \approx Ax + e$.

Allow arbitrary precision of training data.

Enforce condition numbers bounded by 1.

# Example of the limits of deep learning

**Paradox:** "Nice" linear inverse problems where a *stable* and *accurate* neural network for image reconstruction exists, but it can never be trained!

**Theorem**: Pick positive integers $n \geq 3$ and $M$. Class of problems such that:

- (**Not trainable**) No algorithm (even random) can train a neural network with $\boldsymbol{n}$ **digits** of accuracy over the dataset with probability greater than 1/2.
- (**Not practical**) $\boldsymbol{n-1}$ **digits** of accuracy possible over the dataset, but any training algorithm requires **arbitrarily large training data**.
- (**Trainable and practical**) $\boldsymbol{n-2}$ digits of accuracy possible over the dataset via training algorithm using $\boldsymbol{M}$ **training data**.

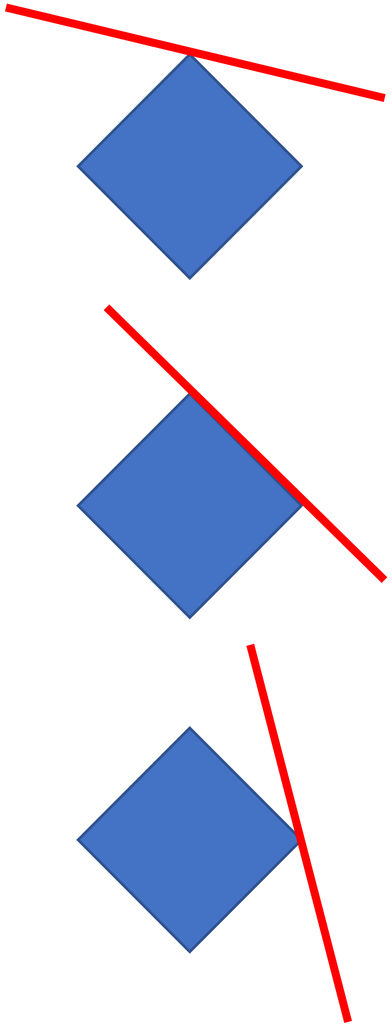
Holds for any architecture, any precision of training data.

$\Longrightarrow$ **Classification theory telling us what can and cannot be done**


- C., Antun, Hansen, "*The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18th problem,*" **PNAS**, 2022.
- Antun, C., Hansen, *"Proving Existence Is Not Enough: : Mathematical Paradoxes Unravel the Limits of Neural Networks in Artificial Intelligence,"* **SIAM News**, May 2022.
- Choi, *"Some AI Systems May Be Impossible to Compute,"* **IEEE Spectrum**, March 2022.

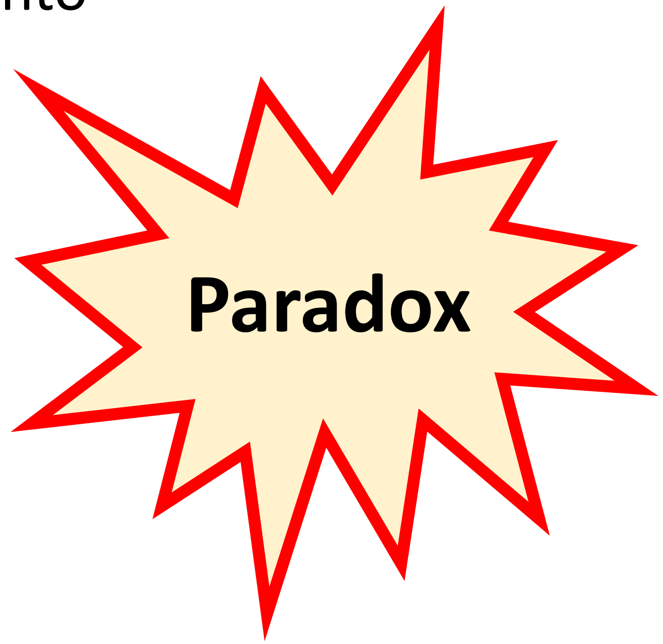
# Idea of mechanism

Phase transitions

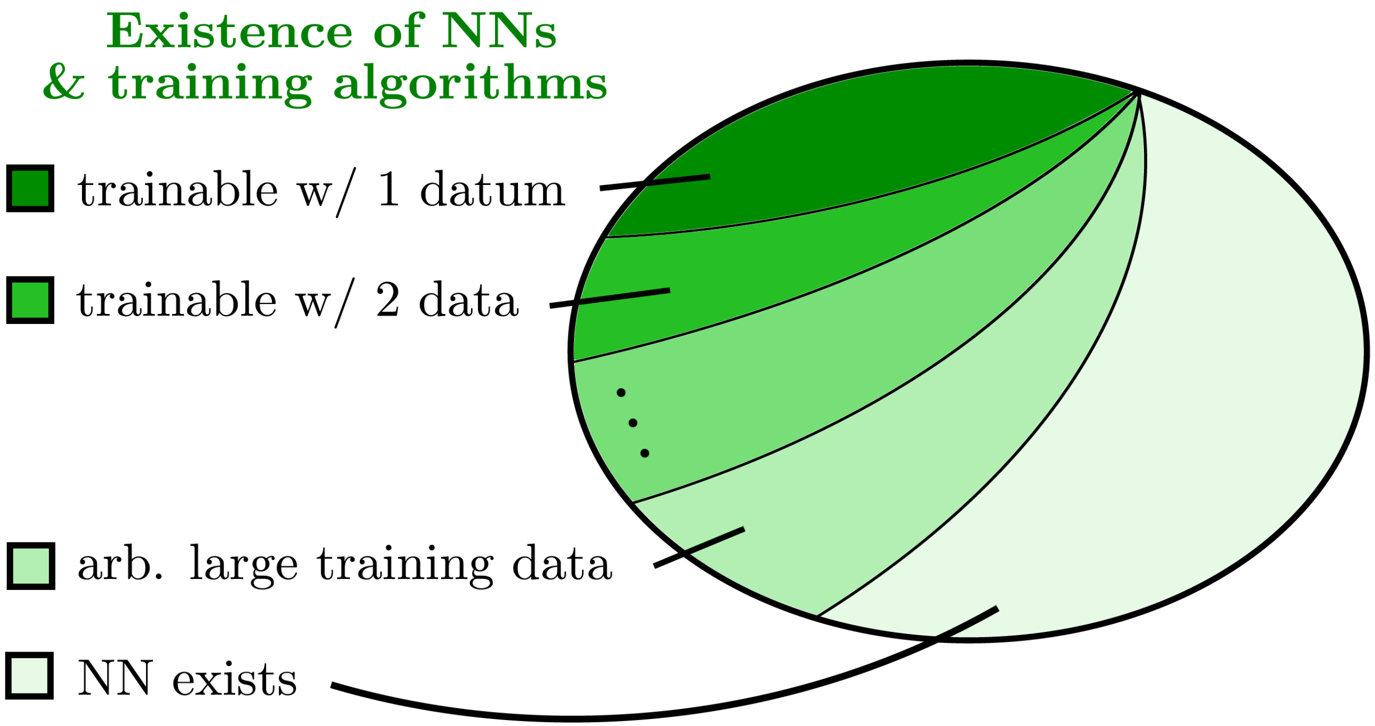


SCI machinery for embedding into
<u>well-conditioned</u> problems

General lemma
(works in other scenarios)

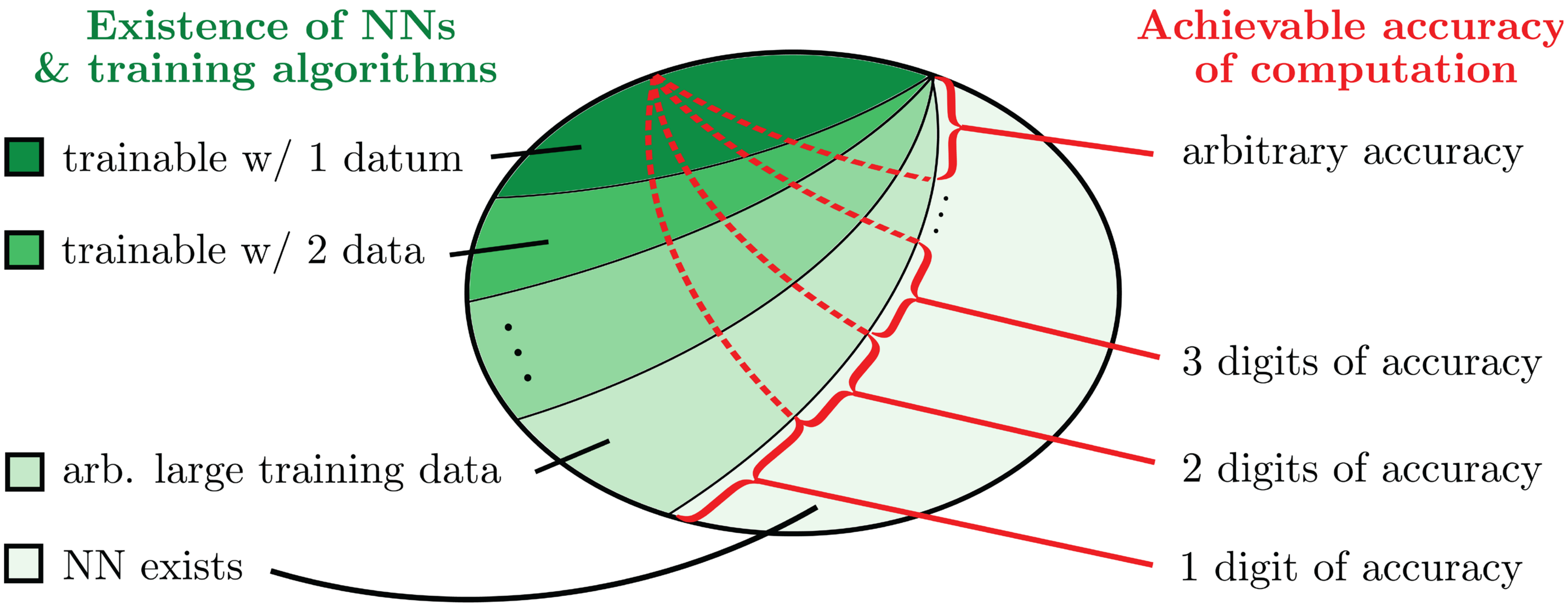


# The world of neural networks




**Given a problem and conditions, where does it sit in this diagram?**

# The world of neural networks




**Given a problem and conditions, where does it sit in this diagram?**

# Example counterpart theorem

**Certain conditions:** stable neural networks trained with exponential accuracy.
E.g., *approximate Łojasiewicz-type inequality*:

$$(1) \quad \min_{x \in \mathbb{C}^N} f(x) \quad \text{s.t.} \quad \|Ax - y\| \leq \varepsilon$$

$$\text{dist}(x, \text{solution}) \leq \alpha([f(x) - f^*] + [\|Ax - y\| - \varepsilon] + \delta)$$

**F**ast **I**terative **RE**started **NET**works (FIRENETs)
(unrolled primal-dual with novel restart scheme)

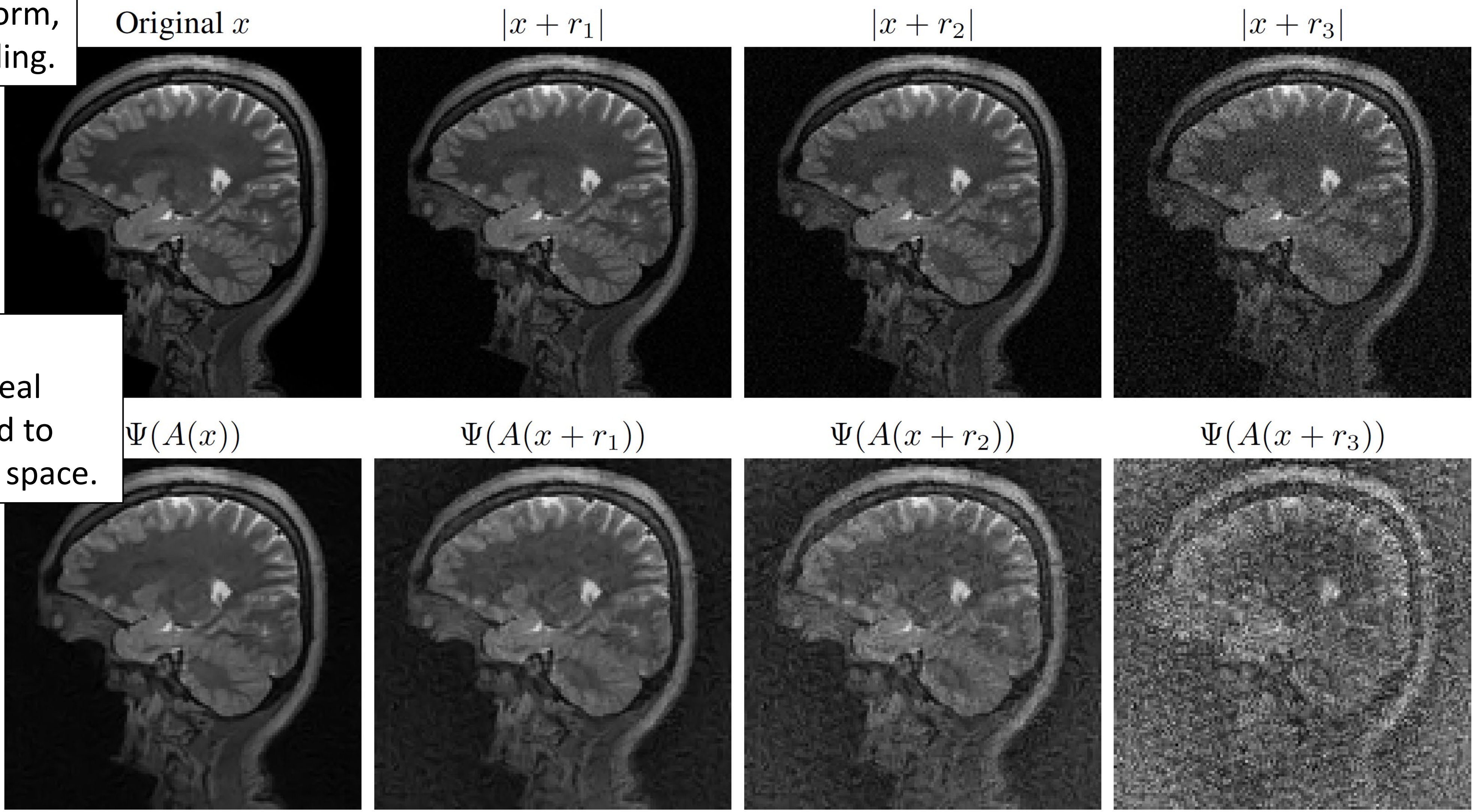
**Theorem**: Training algorithm that, under above assumption, produces *stable* neural networks $\varphi_n$ of width $O(N)$, depth $O(n)$, guaranteed worst bound

$$\text{dist}(\varphi_n(y), \text{solution}) \lesssim e^{-n} + \delta$$


- C., Antun, Hansen, "*The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18th problem,*" **PNAS**, 2022.
- C., "*WARPd: A linearly convergent first-order method for inverse problems with approximate sharpness conditions,*" **SIIMS**, to appear.

# Example of severe instability

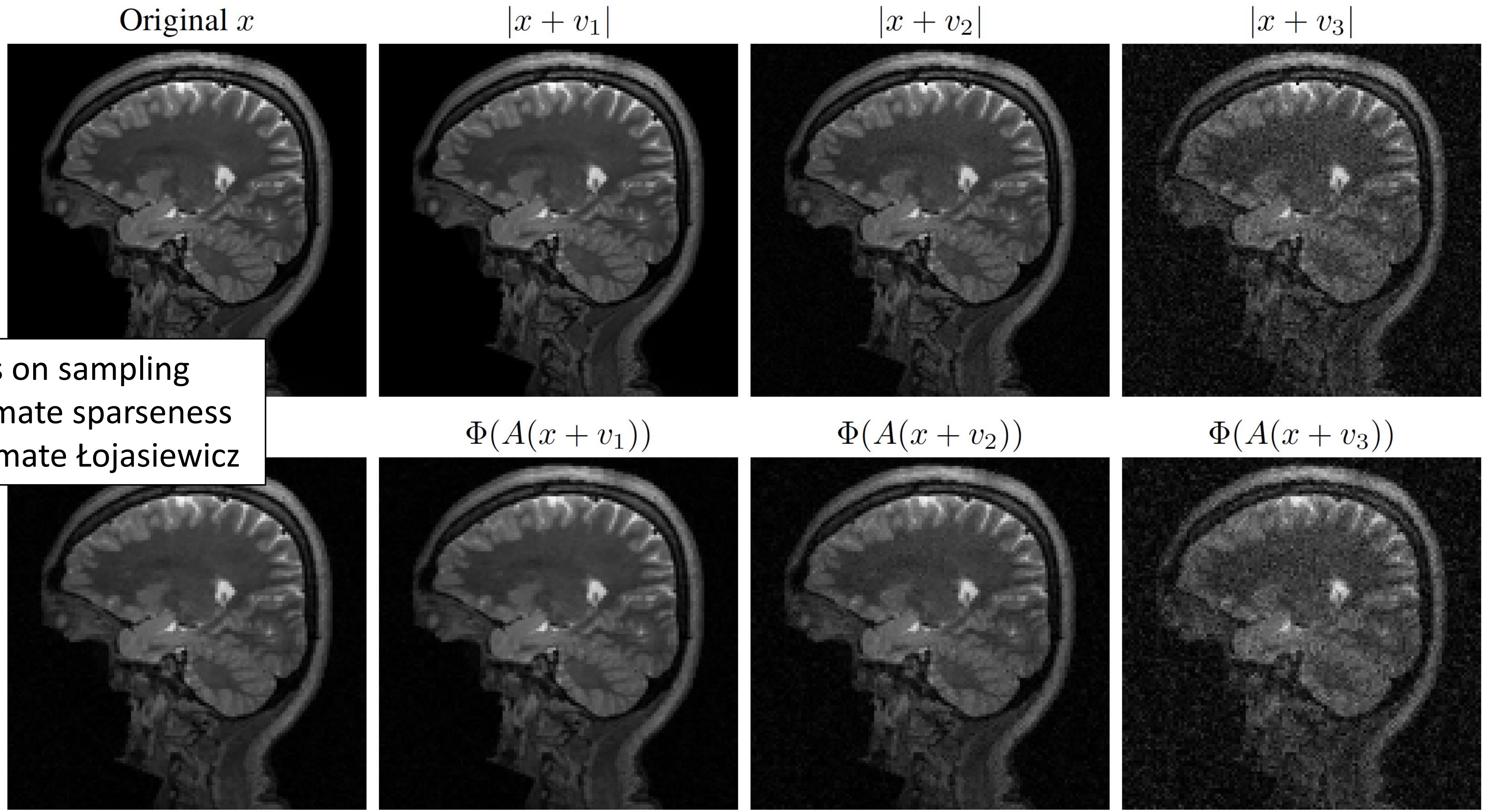
MRI: discrete 2D Fourier transform, 60% subsampling.




Perturbations computed in real space, mapped to measurement space.

- Zhu et al., *"Image reconstruction by domain-transform manifold learning,"* **Nature,** 2018.
- Antun et al., *"On instabilities of deep learning in image reconstruction and the potential costs of AI,"* **PNAS**, 2020.

# FIRENET: provably stable (even to adversarial examples) and accurate




Assumptions on sampling and approximate sparseness give approximate Łojasiewicz

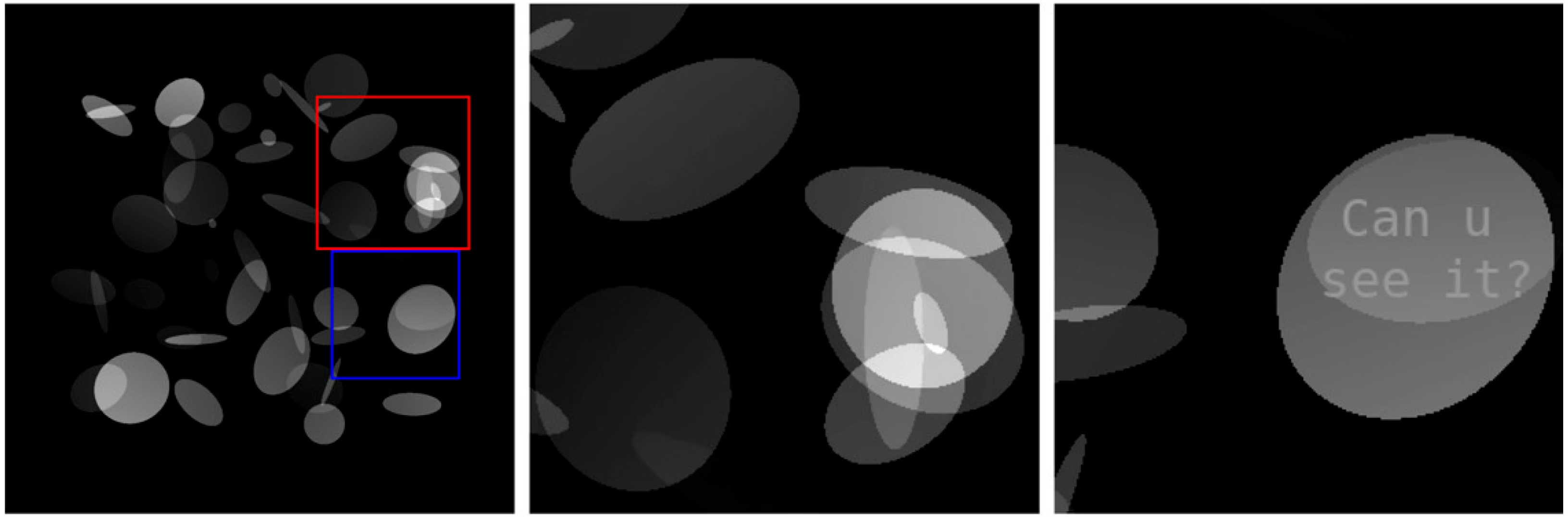
- C., Antun, Hansen, "*The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18th problem*," **PNAS**, 2022.

# Key pillars: stability and accuracy

MRI: discrete 2D Fourier transform, 15% subsampling.

All networks trained on 5000 images of ellipses

Original $x$ (full size) | Original (cropped, red frame) | Original + detail $(x + h_1)$ (cropped, blue frame)

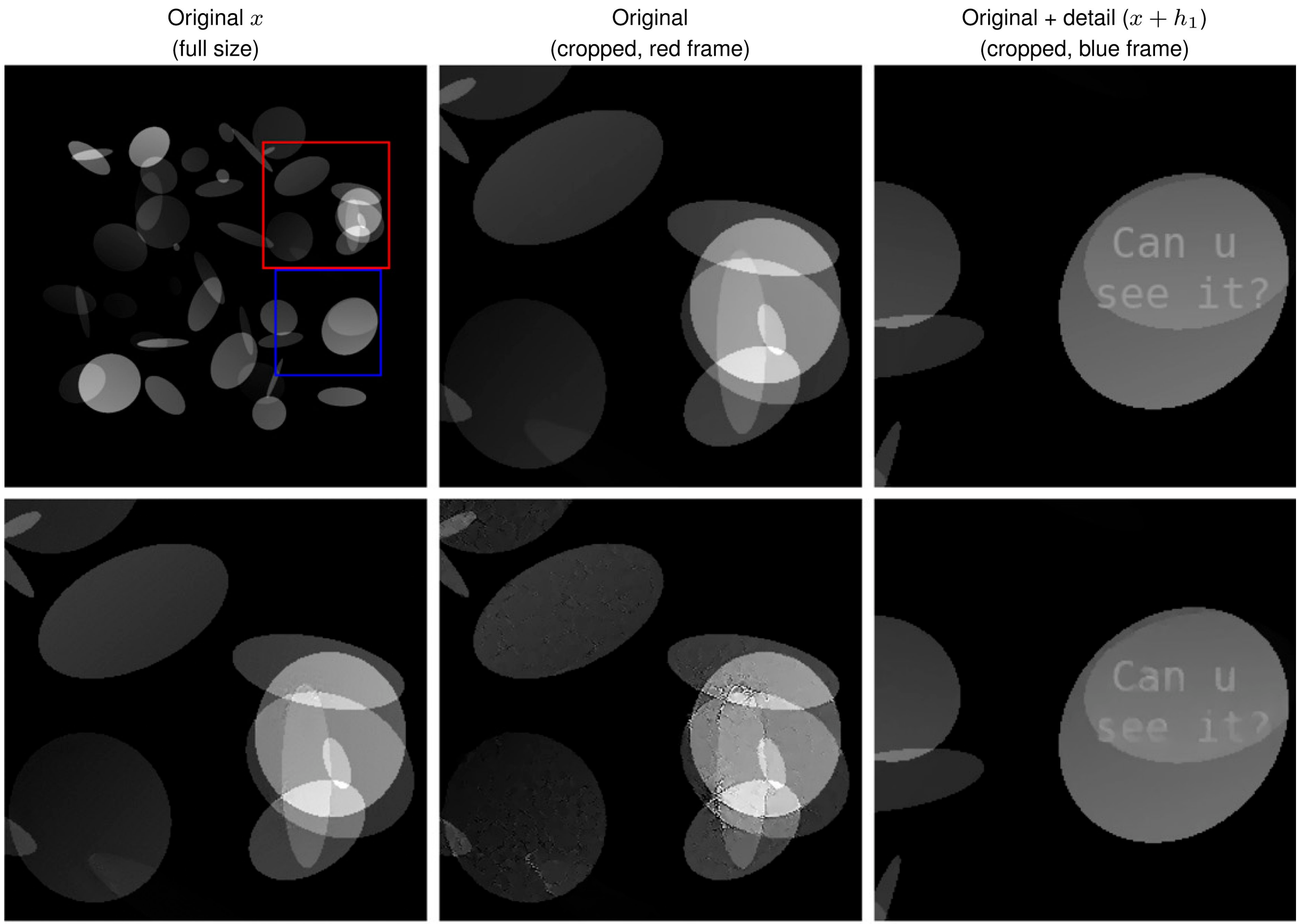



- C., Antun, Hansen, "*The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18th problem,*" **PNAS**, 2022.

# U-Net with no noise: accurate but unstable



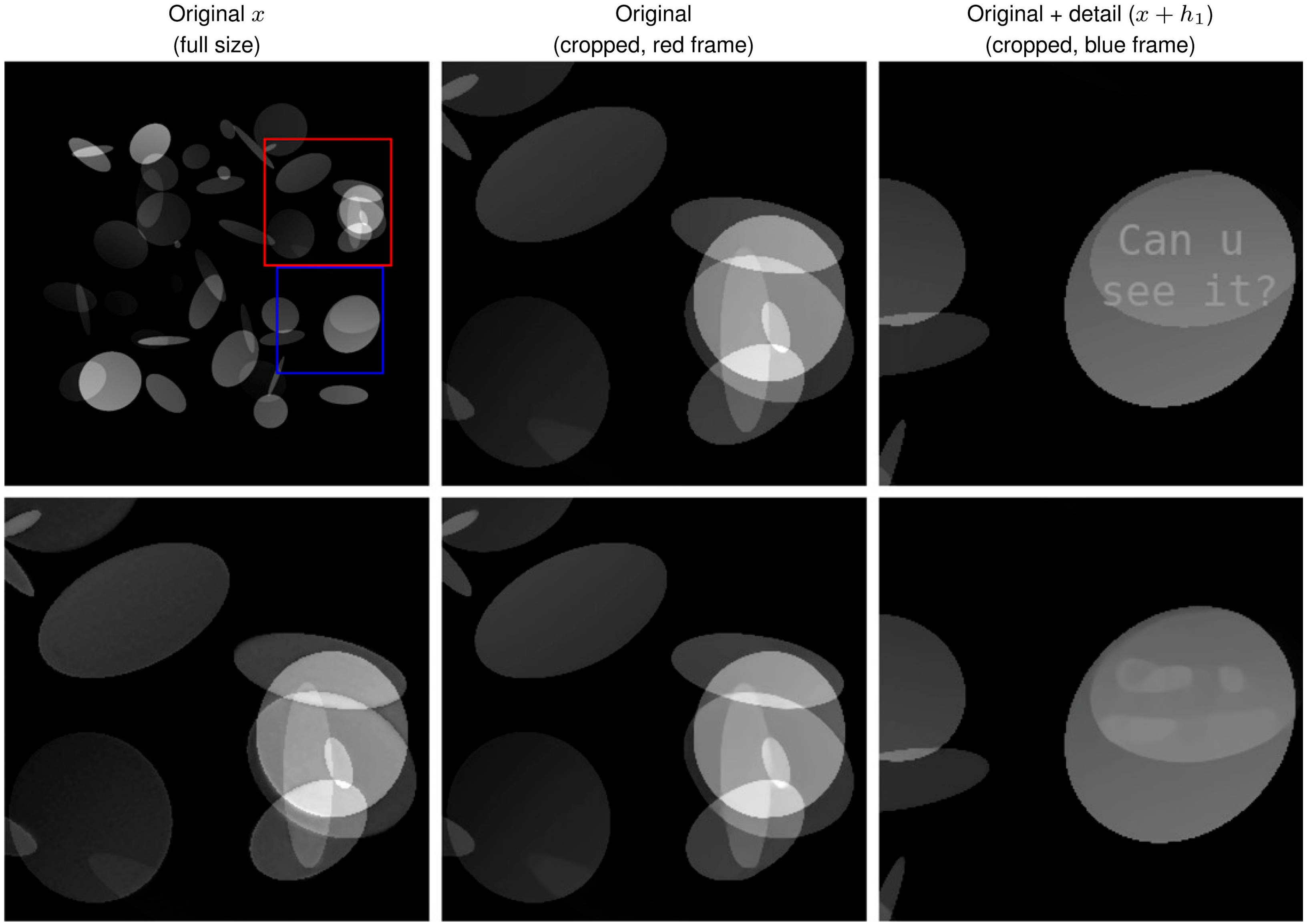
U-Net: standard neural network architecture for imaging. Approx 4 million parameters.




- C., Antun, Hansen, "*The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18th problem,*" **PNAS**, 2022.

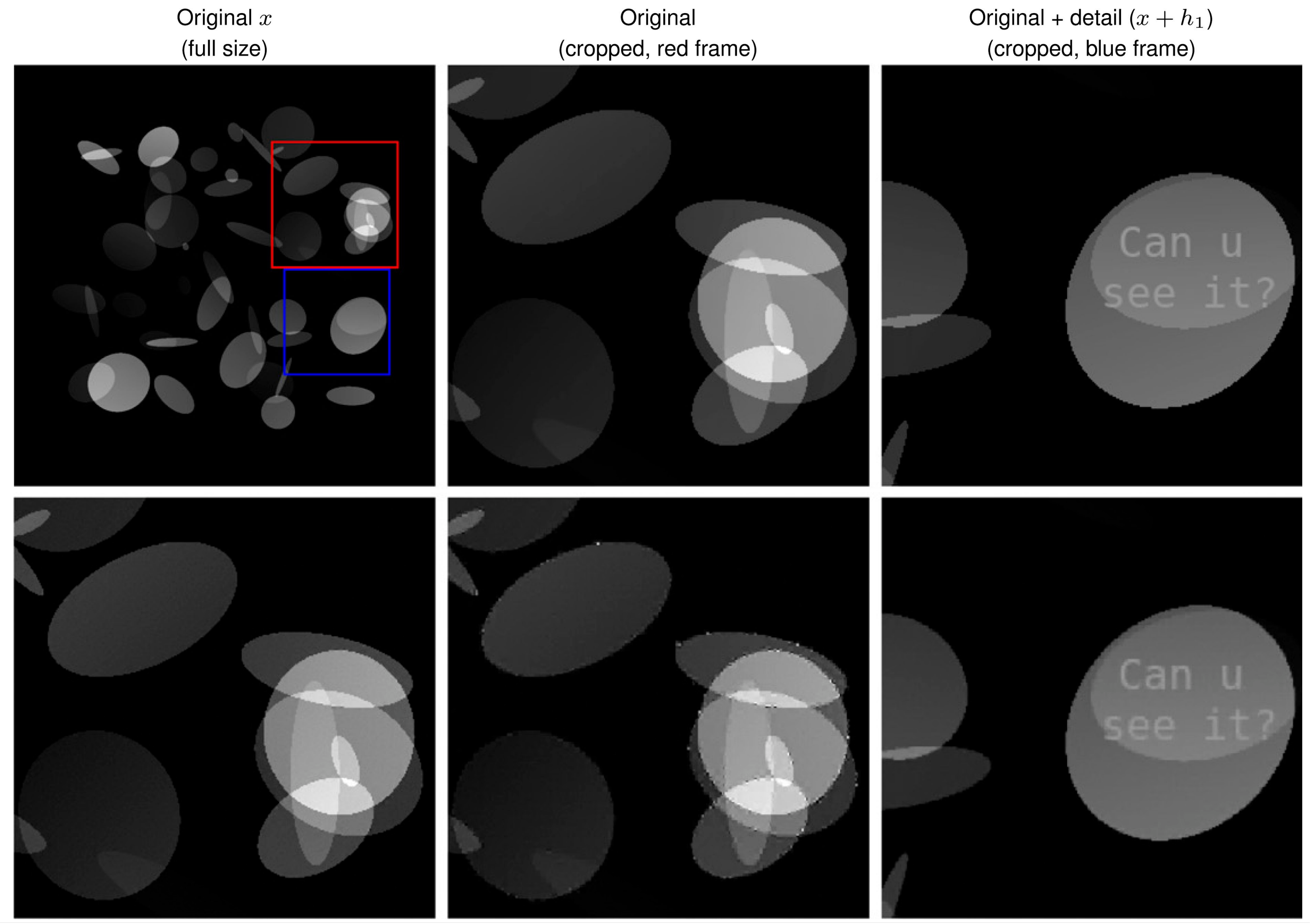
# U-Net with noise: stable but inaccurate






- C., Antun, Hansen, "*The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18th problem,*" **PNAS**, 2022.

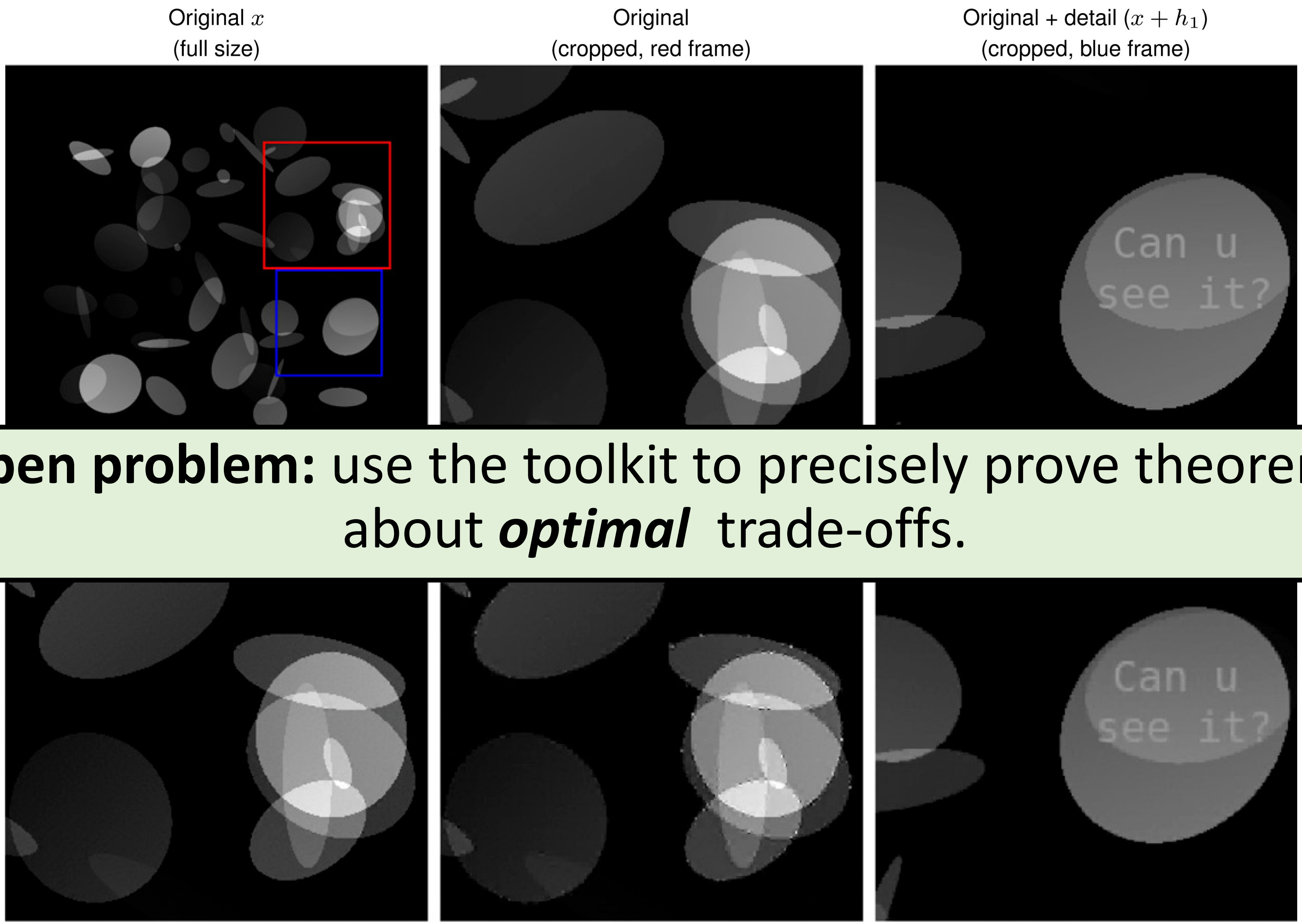
# FIRENET: balances stability and accuracy?




- C., Antun, Hansen, "*The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18th problem,*" **PNAS**, 2022.

# FIRENET: balances stability and accuracy?






**Open problem:** use the toolkit to precisely prove theorems about ***optimal*** trade-offs.

• C., Antun, Hansen, "*The difficulty of computing stable and accurate neural networks: On the barriers of deep learning and Smale's 18th problem*," **PNAS**, 2022.

# Summary: When can algorithms be trusted?

**Toolkit** + **programme**:

- Classifying the difficulty of computational problems
- Proving the optimality of algorithms.

Two **examples**:

- Rigorous and verifiable data-driven dynamical systems: <u>use the residual!</u>
- Computational boundaries in AI: <u>we need foundations!</u>

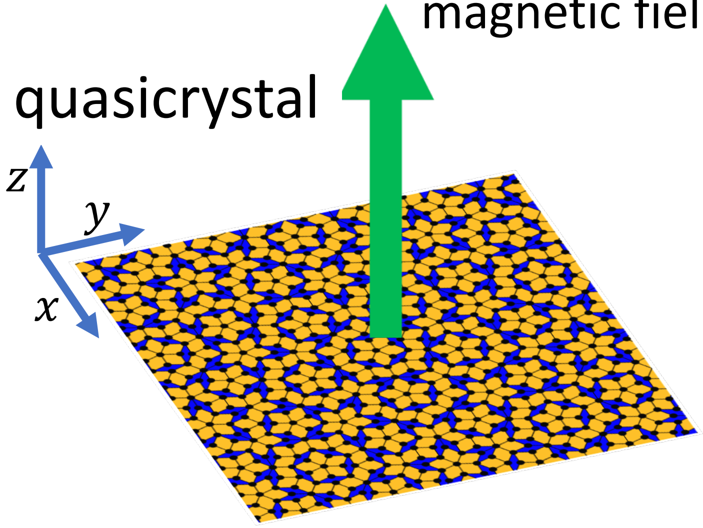
Building blocks for further problems in data analysis and beyond …

# Additional slides

# Example of “too much” (spectral pollution)

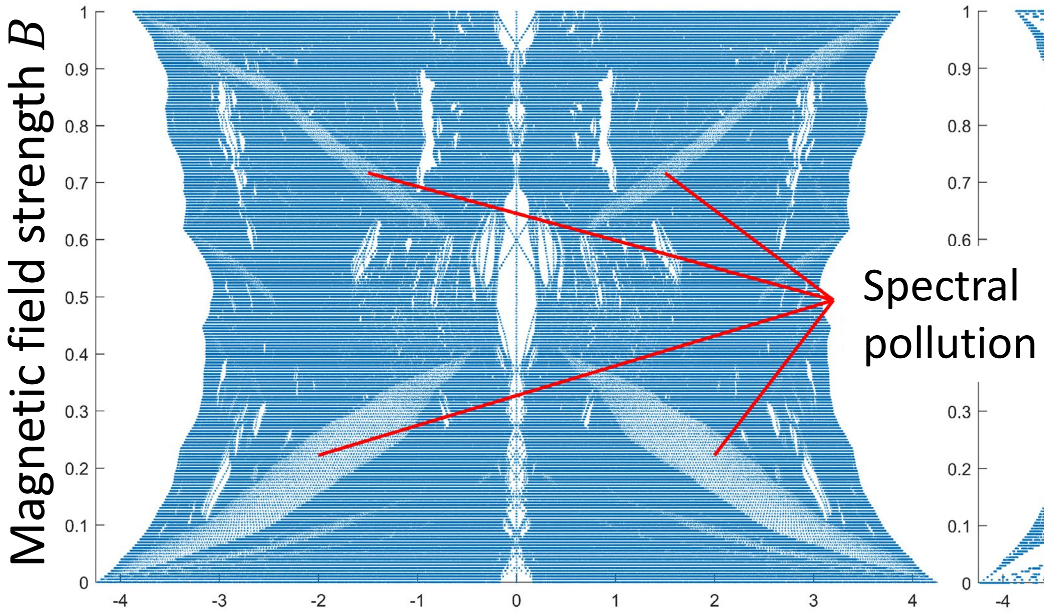
$B$: perpendicular magnetic field

quasicrystal




Infinite matrix: discrete Schrödinger operator

**Naïve method**

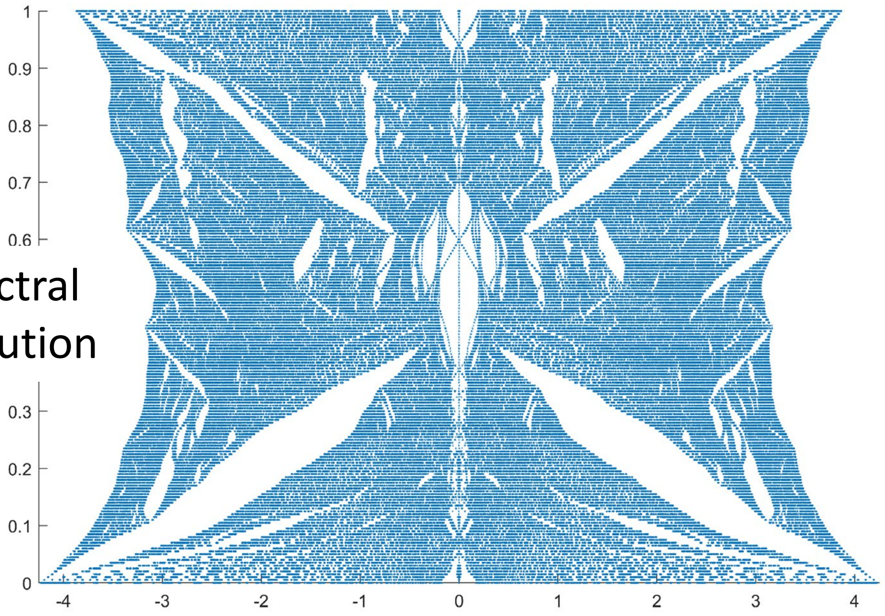



Approx. of spectrum (energy)

**Spectral pollution**

**No error control**

**“Infinite-dimensional” method**




Approx. of spectrum (energy)

**Convergent computation**

**Error control**

- C., Roman, Hansen, *“How to compute spectra with error control,”* **Physical Review Letters**, 2019.

# Convergence of quadrature

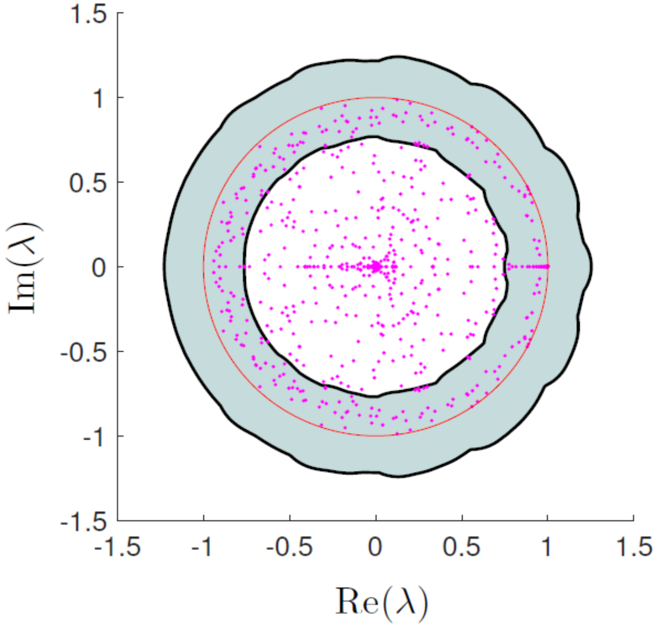
E.g., $\langle \mathcal{K}\psi_k, \psi_j \rangle = \lim_{M\to\infty} \sum_{m=1}^{M} w_m \overline{\psi_j(x^{(m)})}\, \underbrace{\psi_k(y^{(m)})}_{[\mathcal{K}\psi_k](x^{(m)})}$

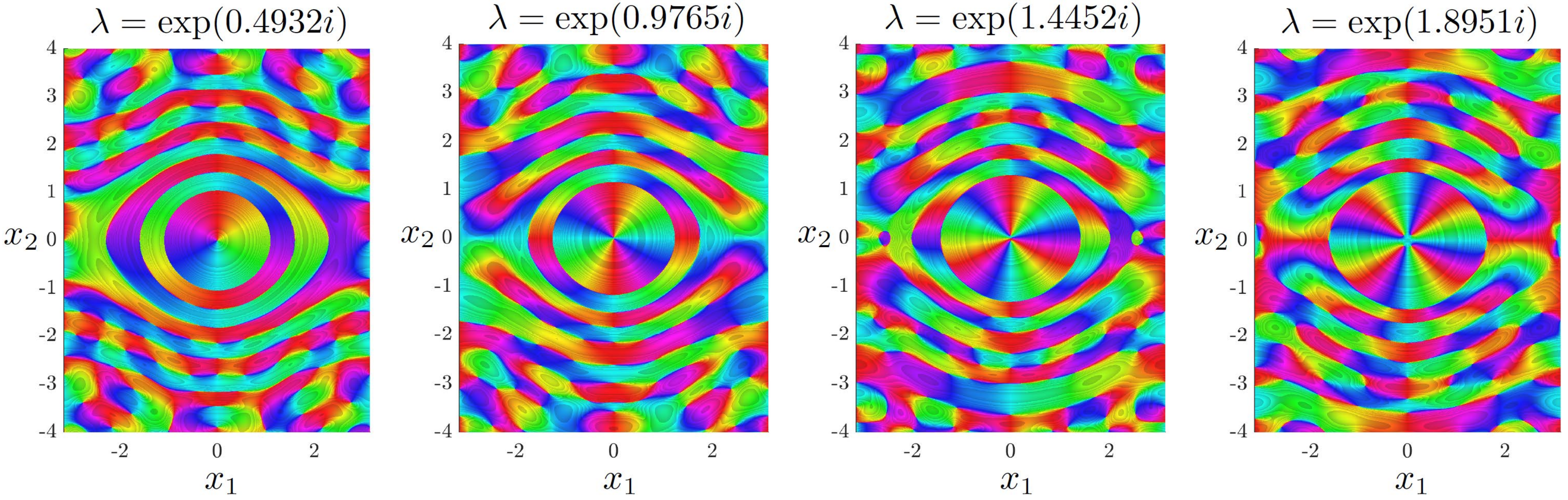
Three examples:

- **High-order quadrature:** $\{x^{(m)}, w_m\}_{m=1}^{M}$ $M$-point quadrature rule.
  Rapid convergence. Requires free choice of $\{x^{(m)}\}_{m=1}^{M}$ and small $d$.
- **Random sampling:** $\{x^{(m)}\}_{m=1}^{M}$ selected at random.
  Large $d$. Slow Monte Carlo $O(M^{-1/2})$ rate of convergence.
- **Ergodic sampling:** $x^{(m+1)} = F(x^{(m)})$.
  Single trajectory, large $d$. Requires ergodicity, convergence can be slow.

Most common

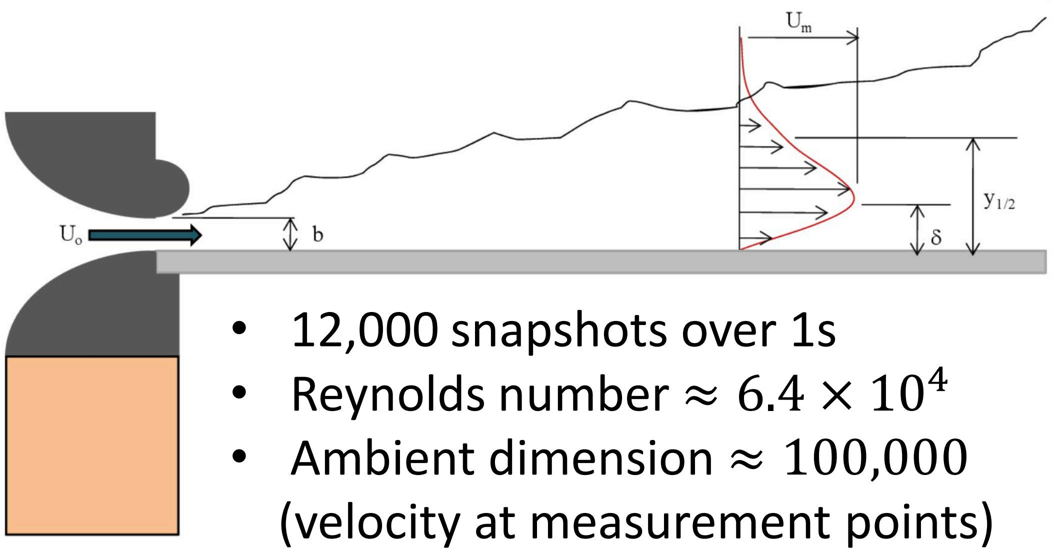
# Example: pendulum

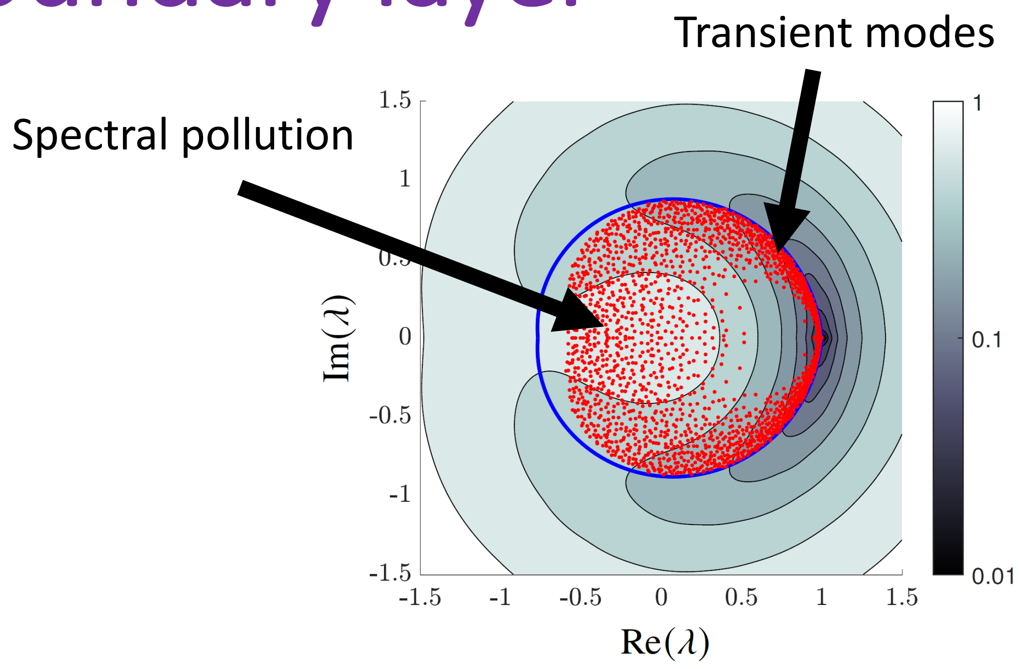



- C., Townsend, *"Rigorous data-driven computation of spectral properties of Koopman operators for dynamical systems,"* **Communications on Pure and Applied Mathematics**, under review.

# Example: wall-jet boundary layer

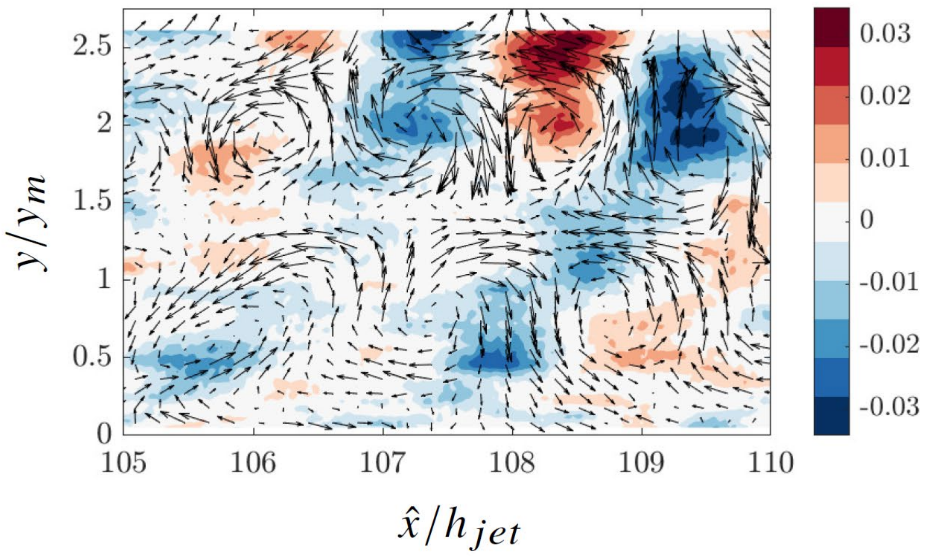


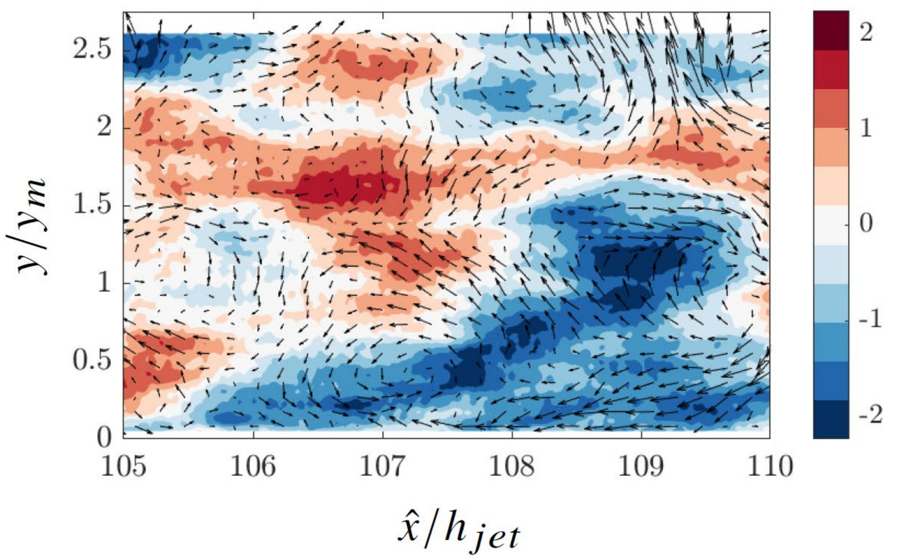

- 12,000 snapshots over 1s
- Reynolds number $\approx 6.4 \times 10^4$
- Ambient dimension $\approx 100{,}000$ (velocity at measurement points)

*Raw measurements provided by Máté Szőke (Virginia Tech)

$\lambda = 0.9439 + 0.2458i$, error $\leq 0.0765$




$\lambda = 0.8948 + 0.1065i$, error $\leq 0.1105$



# Koopman mode decomposition ($\mathbb{K}V = V\Lambda$)

Standard Koopman mode decomposition (order modes by $|\Lambda|$):

$$g(x) \approx \underbrace{[\psi_1(x) \quad \cdots \quad \psi_{N_K}(x)]V}_{\text{approx Koopman e-functions}} \underbrace{\left(V\sqrt{W}\Psi_X\right)^{\dagger}\sqrt{W}[g(x^{(1)}) \quad \cdots \quad g(x^{(M)})]^{\mathrm{T}}}_{\text{Koopman modes}}$$

$$\overset{?}{\Rightarrow} g(x_n) \approx \underbrace{[\psi_1(x) \quad \cdots \quad \psi_{N_K}(x)]V}_{\text{approx Koopman e-functions}} \Lambda^n \underbrace{\left(V\sqrt{W}\Psi_X\right)^{\dagger}\sqrt{W}[g(x^{(1)}) \quad \cdots \quad g(x^{(M)})]^{\mathrm{T}}}_{\text{Koopman modes}}$$

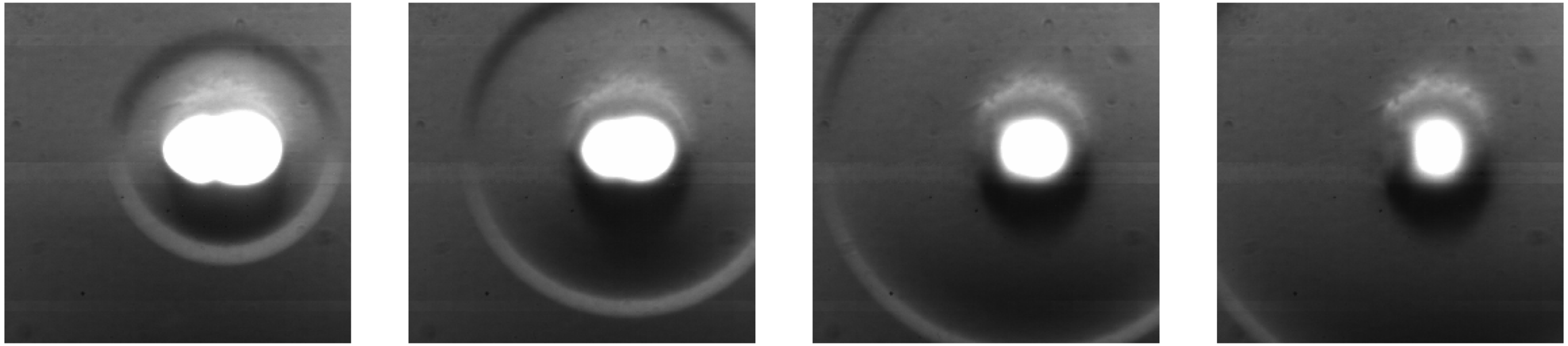
Residual Koopman mode decomposition (order modes by $\mathrm{res}(\lambda, \mathbf{v})$):

Controllable error

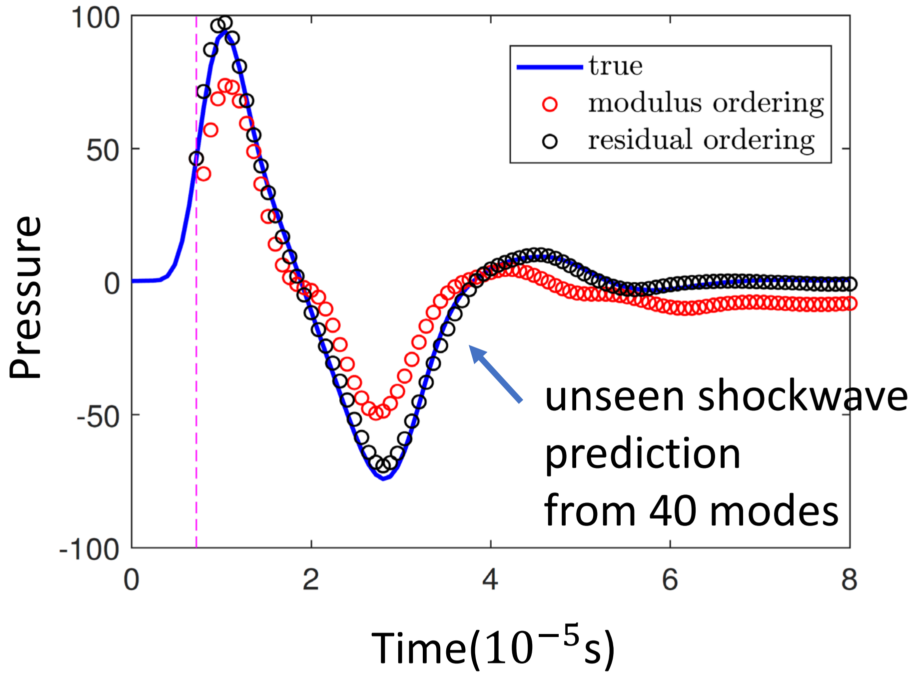
$$g(x) \approx \underbrace{[\psi_1(x) \quad \cdots \quad \psi_{N_K}(x)]V_{(\varepsilon)}}_{\text{approx Koopman e-functions}} \underbrace{\left(V_{(\varepsilon)}\sqrt{W}\Psi_X\right)^{\dagger}\sqrt{W}[g(x^{(1)}) \quad \cdots \quad g(x^{(M)})]^{\mathrm{T}}}_{\text{Koopman modes}}$$

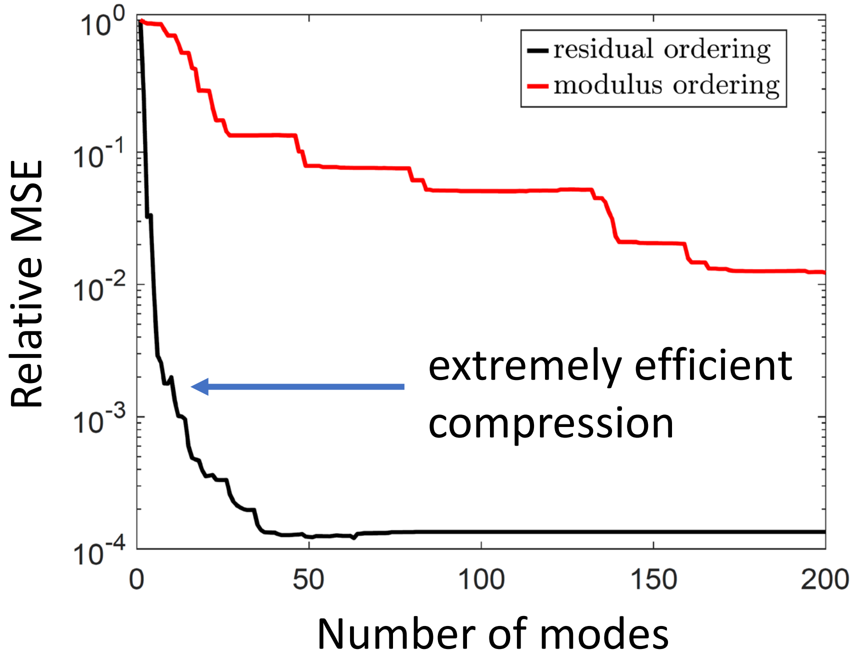
$$g(x_n) \approx \underbrace{[\psi_1(x_0) \quad \cdots \quad \psi_{N_K}(x_0)]V_{(\varepsilon)}}_{\text{approx Koopman e-functions}} \Lambda_{(\varepsilon)}^n \underbrace{\left(V_{(\varepsilon)}\sqrt{W}\Psi_X\right)^{\dagger}\sqrt{W}[g(x^{(1)}) \quad \cdots \quad g(x^{(M)})]^{\mathrm{T}}}_{\text{Koopman modes}}$$

# Example: laser-induced plasma



a) $t = 5\ \mu s$ b) $t = 10\ \mu s$ c) $t = 15\ \mu s$ d) $t = 20\ \mu s$



# Example: ionization probabilities in < 1 second

$$[Au](r) = -\frac{d^2u}{dr^2}(r) + \left(\frac{l(l+1)}{r^2} + \frac{e^{-r}-1}{r}\right)u(r), \qquad r > 0$$

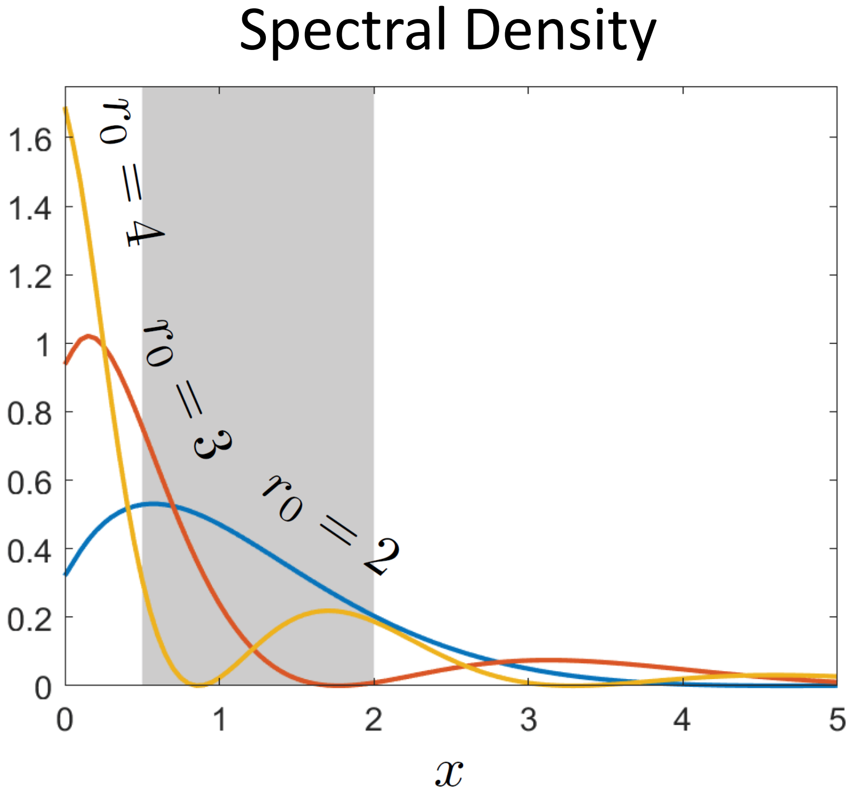
Hellman potential

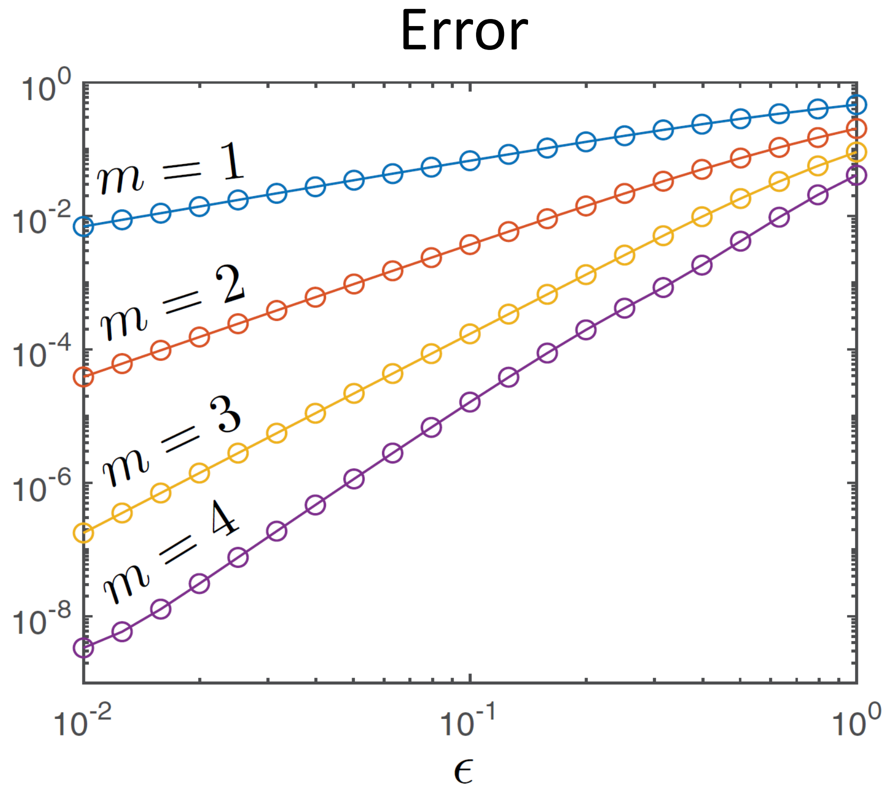
```
c = sqrt(pi/8)*(2-igamma(1/2,8)/gamma(1/2));      % Norm squared
g = @(r) exp(-(r-2).^2)/sqrt(c);                  % Measure wrt g(r)
V={@(r) 0, @(r) exp(-r)-1, 1};                    % Potential, l=1
[xi, wi] = chebpts(20,  [1/2 2]);                 % Quadrature rule
nu = rseMeas(V, g, xi, 0.1, 'Order', 4);          % epsilon=0.1, m=4
ion_prob = wi * nu;                               % Ionization prob
```

# Example: ionization probabilities in < 1 second

$$[Au](r) = -\frac{d^2u}{dr^2}(r) + \left(\frac{l(l+1)}{r^2} + \frac{e^{-r}-1}{r}\right)u(r), \qquad r > 0$$

Hellman potential



# Extensions to PDEs

- Operator A on $\mathbb{R}^d$ of form

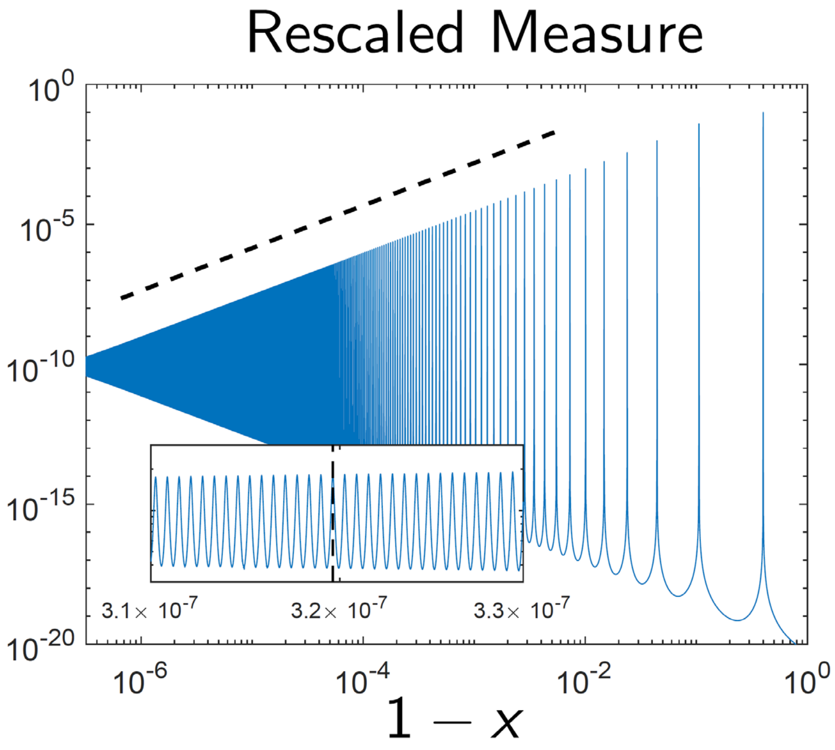
$$[Au] = \sum_{k \in \mathbb{Z}_{\geq 0}^d, |k| \leq N} c_k(x)[\partial^k u](x)$$

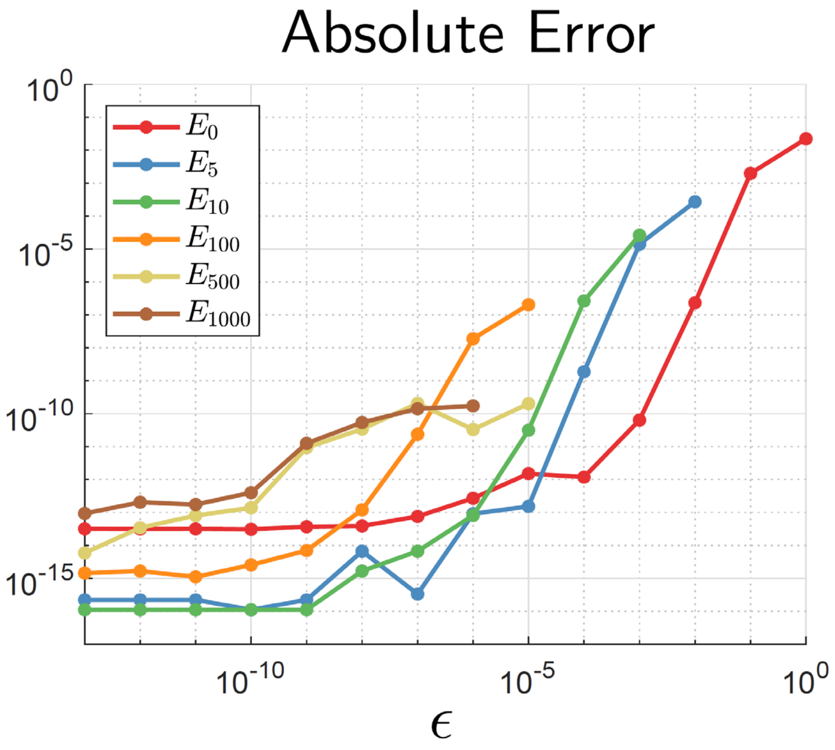
- Assume coefficients are
  - Polynomially bounded
  - Locally bounded total variation
- Build matrix representation using quasi-Monte Carlo integration.

$\rightarrow$ Sample coefficients to compute $\mathrm{Spec}(A)$ with error control!

**NB:** works for spectral methods, FEM, etc.

# Eigenvalues of Dirac operator



# Example of impossibility theorem for subsampled discrete cosine transform

| $\min_k \operatorname{dist}(\Psi_n(y_k), \Xi(A, y_k))$ | $\min_k \operatorname{dist}(\Phi_n(y_k), \Xi(A, y_k))$ | prec. of training data | $10^{-n}$ |
|---|---|---|---|
| 0.2999690 | 0.2597827 | $m = 10$ | $10^{-1}$ |
| 0.3000000 | 0.2598050 | $m = 20$ | $10^{-1}$ |
| 0.3000000 | 0.2598052 | $m = 30$ | $10^{-1}$ |
| 0.0030000 | 0.0025980 | $m = 10$ | $10^{-3}$ |
| 0.0030000 | 0.0025980 | $m = 20$ | $10^{-3}$ |
| 0.0030000 | 0.0025980 | $m = 30$ | $10^{-3}$ |
| 0.0000030 | 0.0000015 | $m = 10$ | $10^{-6}$ |
| 0.0000030 | 0.0000015 | $m = 20$ | $10^{-6}$ |
| 0.0000030 | 0.0000015 | $m = 30$ | $10^{-6}$ |

Impossibility of computing approximations of the neural network to arbitrary accuracy. We demonstrate the impossibility statement on fast iterative restarted networks $\Phi_n$ and learned iterative shrinkage thresholding algorithm networks $\Psi_n$. The table reveals the shortest $l_2$ distance between the networks' output and the problem's true solution for different values of $m$ (precision of training data is $2^{-m}$). Neither of the trained neural networks can compute the existing correct neural network to accuracy $10^{-n}$, but both compute approximations that are accurate to $10^{-n+1}$.

# Stabilising unstable neural networks

$\Psi(\tilde{y}),\ \tilde{y} = Ax + e_3$ | $\Phi\left(\tilde{y}, \Psi(\tilde{y})\right)$ | FIRENET rec. from $y = Ax + \tilde{e}_3$ | AUTOMAP+FIRENET rec. from $y = Ax + \hat{e}_3$