Instance-Optimal Quantum State Certification with Entangled Measurements

Chirag Wadhwa (University of Edinburgh)

Joint work with Ryan O'Donnell (CMU)

arxiv:2507.06010

Outline

Outline

Quantum State Certification

- A tester is given the **complete description** of a quantum state $\sigma \in \mathbb{C}^{d \times d}$ and n **copies** of an unknown state $\rho \in \mathbb{C}^{d \times d}$.
- Promised that $\rho = \sigma$ or $\|\rho - \sigma\|_1 \geq \epsilon$.
- ϵ-**certifying** σ: distinguishing between these cases with high probability.

Motivation

- Benchmarking quantum devices.
- Verifying heuristic quantum learning algorithms.

Also, a direct quantum analogue of **identity testing** in classical distribution testing:

Given the description of a distribution q, and n samples from an unknown distribution p, test whether $p = q$ or $\|p - q\|_1 \geq \epsilon$.

Worst-Case Bounds

What is the optimal copy complexity of state certification?

Worst-Case Bounds

What is the optimal copy complexity of state certification?

- [OW15] established a $\Omega(d/\epsilon^2)$ lower bound for **mixedness testing**, i.e., when $\sigma = \mathbb{1}/d$.

[OW15]: Quantum spectrum testing; O'Donnell-Wright 2015.

Worst-Case Bounds

What is the optimal copy complexity of state certification?

- [OW15] established a $\Omega(d/\epsilon^2)$ lower bound for **mixedness testing**, i.e., when $\sigma = \mathbb{1}/d$.
- [BOW19] developed an algorithm using $\mathcal{O}(d/\epsilon^2)$ copies to certify any state.
- This establishes a tight **worst-case** complexity: $\Theta(d/\epsilon^2)$.

[OW15]: Quantum spectrum testing; O'Donnell-Wright 2015.
[BOW19]: Quantum state certification; Bădescu-O'Donnell-Wright 2019.

Worst-Case Bounds

What is the optimal copy complexity of state certification?

- [OW15] established a $\Omega(d/\epsilon^2)$ lower bound for **mixedness testing**, i.e., when $\sigma = \mathbb{1}/d$.
- [BOW19] developed an algorithm using $\mathcal{O}(d/\epsilon^2)$ copies to certify any state.
- This establishes a tight **worst-case** complexity: $\Theta(d/\epsilon^2)$.
- But the problem could be much easier for other choices of σ!

[OW15]: Quantum spectrum testing; O'Donnell-Wright 2015.
[BOW19]: Quantum state certification; Bădescu-O'Donnell-Wright 2019.

Worst-Case Bounds

What is the optimal copy complexity of state certification?

- [OW15] established a $\Omega(d/\epsilon^2)$ lower bound for **mixedness testing**, i.e., when $\sigma = \mathbb{1}/d$.
- [BOW19] developed an algorithm using $\mathcal{O}(d/\epsilon^2)$ copies to certify any state.
- This establishes a tight **worst-case** complexity: $\Theta(d/\epsilon^2)$.
- But the problem could be much easier for other choices of σ!
- For e.g., when σ is pure, $\mathcal{O}(1/\epsilon^2)$ copies suffice [MdW16].

[OW15]: Quantum spectrum testing; O'Donnell-Wright 2015.
[BOW19]: Quantum state certification; Bădescu-O'Donnell-Wright 2019.
[MdW16]: A survey of quantum property testing; Montanaro-de Wolf 2016.

Instance-Optimal State Certification

How does the optimal copy complexity depend on σ?

Instance-Optimal State Certification

How does the optimal copy complexity depend on σ?

- [CLO22,CLHL22] have answered this question when testers can only perform **single-copy** measurements.

[CLO22]: Toward instance-optimal state certification with incoherent measurements; Chen-Li-O'Donnell 2022
[CLHL22]: Tight bounds for quantum state certification with incoherent measurements; Chen-Li-Huang-Liu 2022

Instance-Optimal State Certification

How does the optimal copy complexity depend on σ?

- [CLO22,CLHL22] have answered this question when testers can only perform **single-copy** measurements.
- We even have classical bounds for instance-optimal identity testing in various forms [**VV17, DK16, BCG19**].

[VV17]: An automatic inequality prover and instance optimal identity testing; Valiant-Valiant 2017.
[DK16]: A new approach for testing properties of discrete distributions; Diakonikolas-Kane 2016.
[BCG19]: Distribution testing lower bounds via reductions from communication complexity; Blais-Canonne-Gur 2019.

Instance-Optimal State Certification

How does the optimal copy complexity depend on σ?

- [CLO22,CLHL22] have answered this question when testers can only perform **single-copy** measurements.
- We even have classical bounds for instance-optimal identity testing in various forms [**VV17, DK16, BCG19**].
- However, when quantum testers are unrestricted, instance-optimal bounds were not known.

Outline

Nearly Instance-Optimal Bounds

Theorem (Main Result)

With fully entangled measurements, the copy complexity n of ϵ-certifying σ satisfies

$$\tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right) \leq n \leq \tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right).$$

$\underline{\sigma}, \overline{\sigma}$ are variants of σ constructed by zeroing out suitable eigenvalues adding up to $\mathcal{O}(\epsilon), \mathcal{O}(\epsilon^2)$ respectively.

Nearly Instance-Optimal Bounds

Theorem (Main Result)

With fully entangled measurements, the copy complexity n of ϵ-certifying σ satisfies

$$\tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right) \leq n \leq \tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right).$$

$\underline{\sigma}, \overline{\sigma}$ are variants of σ constructed by zeroing out suitable eigenvalues adding up to $\mathcal{O}(\epsilon), \mathcal{O}(\epsilon^2)$ respectively.

- For $\sigma = \mathbb{1}/d$, $n = \tilde{\Theta}(d/\epsilon^2)$.

Nearly Instance-Optimal Bounds

Theorem (Main Result)

With fully entangled measurements, the copy complexity n of ϵ-certifying σ satisfies

$$\tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right) \leq n \leq \tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right).$$

$\underline{\sigma}, \overline{\sigma}$ are variants of σ constructed by zeroing out suitable eigenvalues adding up to $\mathcal{O}(\epsilon), \mathcal{O}(\epsilon^2)$ respectively.

- For $\sigma = \mathbb{1}/d$, $n = \tilde{\Theta}(d/\epsilon^2)$.
- For pure σ, $n = \tilde{\Theta}(1/\epsilon^2)$.

Mixedness Testing Lower Bound

- Our main theorem recovers the mixedness testing bounds up to $\log(d/\epsilon)$ factors.
- Directly applying our techniques to mixedness testing, we actually recover $\Omega(d/\epsilon^2)$ without any log factors!
- With our new lower bound technique, this proof is much simpler than that of [**OW15**]!

Outline

Mixedness Testing: Prior Techniques

Mixedness Testing: Prior Techniques

- $\mathrm{d}_{\mathrm{tr}}(\sigma, \mathbb{1}/d)$ depends only on σ's eigenvalues.
- For such **spectrum tests**, weak Schur sampling is known to be optimal [**CHW07,MdW16**].
- [**OW15**] then prove the mixedness testing lower bound by analyzing the resulting Schur-Weyl distributions.

[**CHW07**]: Weak Fourier-Schur sampling, the hidden subgroup problem, and the quantum collision problem; Childs-Harrow-Wocjan 2007.

Mixedness Testing: Prior Techniques

- $\mathrm{d}_{\mathrm{tr}}(\sigma, \mathbb{1}/d)$ depends only on σ's eigenvalues.
- For such **spectrum tests**, weak Schur sampling is known to be optimal [**CHW07,MdW16**].
- [**OW15**] then prove the mixedness testing lower bound by analyzing the resulting Schur-Weyl distributions.
- Can't even be used for certifying **nearly** maximally mixed states: e.g. states with spectrum

$$\Big(\underbrace{\frac{1}{2d},\cdots\frac{1}{2d}}_{2d/3},\underbrace{\frac{2}{d},\cdots\frac{2}{d}}_{d/3}\Big).$$

Mixedness Testing: Prior Techniques

- $\mathrm{d}_{\mathrm{tr}}(\sigma, \mathbb{1}/d)$ depends only on σ's eigenvalues.
- For such **spectrum tests**, weak Schur sampling is known to be optimal [**CHW07,MdW16**].
- [**OW15**] then prove the mixedness testing lower bound by analyzing the resulting Schur-Weyl distributions.
- Can't even be used for certifying **nearly** maximally mixed states: e.g. states with spectrum

$$\Big(\underbrace{\frac{1}{2d}, \dots \frac{1}{2d}}_{2d/3}, \underbrace{\frac{2}{d}, \dots \frac{2}{d}}_{d/3}\Big).$$

We need a new way to prove the mixedness testing lower bound!

Classical Lower Bound Techniques

Classical Lower Bound Techniques

- Given n samples from an unknown distribution, distinguish between the following equally likely cases:
  1. All n samples are drawn from some fixed distribution q.
  2. A random parameter θ is drawn, then n samples are drawn from q_θ.

Classical Lower Bound Techniques

- Given n samples from an unknown distribution, distinguish between the following equally likely cases:
  1. All n samples are drawn from some fixed distribution q.
  2. A random parameter θ is drawn, then n samples are drawn from q_θ.
- Any algorithm succeeds at this task w/ prob at most

$$\frac{1}{2} + \frac{1}{2} \cdot \mathrm{d_{TV}}(\mathbb{E}_\theta[q_\theta^{\otimes n}], q^{\otimes n}).$$

Classical Lower Bound Techniques

- Given n samples from an unknown distribution, distinguish between the following equally likely cases:
  1. All n samples are drawn from some fixed distribution q.
  2. A random parameter θ is drawn, then n samples are drawn from q_θ.
- Any algorithm succeeds at this task w/ prob at most
$$\frac{1}{2} + \frac{1}{2} \cdot \mathrm{d}_{\mathrm{TV}}(\mathbb{E}_\theta[q_\theta^{\otimes n}], q^{\otimes n}).$$
- Relate to χ^2-divergence: $\mathrm{d}_{\mathrm{TV}} \leq \frac{1}{2}\sqrt{\mathrm{d}_{\chi^2}}$.
- n must be large enough so that $\mathrm{d}_{\chi^2}(\mathbb{E}_\theta[q_\theta^{\otimes n}] \| q^{\otimes n}) \geq c$.
- Use the *Ingster-Suslina method* [IS12] to explicitly compute d_{χ^2} and easily upper bound it.

[IS12]: Nonparametric goodness-of-fit testing under Gaussian models; Ingster-Suslina 2012.

Our Lower Bound Techniques

Our Lower Bound Techniques

- Given n copies of an unknown state, distinguish between the following equally likely cases:
  1. We receive n copies of a fixed state σ.
  2. A random parameter θ is drawn, then we receive n copies of some state σ_θ.

Our Lower Bound Techniques

- Given n copies of an unknown state, distinguish between the following equally likely cases:
  1. We receive n copies of a fixed state σ.
  2. A random parameter $\boldsymbol{\theta}$ is drawn, then we receive n copies of some state $\sigma_{\boldsymbol{\theta}}$.
- Any algorithm succeeds at this task w/ prob at most

$$\tfrac{1}{2} + \tfrac{1}{2} \cdot \mathrm{d}_{\mathrm{tr}}(\mathbb{E}_{\theta}[\sigma_{\boldsymbol{\theta}}^{\otimes n}], \sigma^{\otimes n}).$$

Our Lower Bound Techniques

- Given n copies of an unknown state, distinguish between the following equally likely cases:
  1. We receive n copies of a fixed state σ.
  2. A random parameter $\boldsymbol{\theta}$ is drawn, then we receive n copies of some state $\sigma_{\boldsymbol{\theta}}$.
- Any algorithm succeeds at this task w/ prob at most
$$\tfrac{1}{2} + \tfrac{1}{2} \cdot \mathrm{d}_{\mathrm{tr}}(\mathbb{E}_{\theta}[\sigma_{\boldsymbol{\theta}}^{\otimes n}], \sigma^{\otimes n}).$$
- Relate to quantum χ^2-divergence: $\mathrm{d}_{\mathrm{tr}} \leq \frac{1}{2}\sqrt{\mathrm{D}_{\chi^2}}$.
- n must be large enough so that $\mathrm{D}_{\chi^2}(\mathbb{E}_{\theta}[\sigma_{\boldsymbol{\theta}}^{\otimes n}] \| \sigma^{\otimes n}) \geq c$.

Our Lower Bound Techniques

- Given n copies of an unknown state, distinguish between the following equally likely cases:
  1. We receive n copies of a fixed state σ.
  2. A random parameter $\boldsymbol{\theta}$ is drawn, then we receive n copies of some state $\sigma_{\boldsymbol{\theta}}$.
- Any algorithm succeeds at this task w/ prob at most
$$\tfrac{1}{2} + \tfrac{1}{2} \cdot \mathrm{d}_{\mathrm{tr}}(\mathbb{E}_{\theta}[\sigma_{\boldsymbol{\theta}}^{\otimes n}], \sigma^{\otimes n}).$$
- Relate to quantum χ^2-divergence: $\mathrm{d}_{\mathrm{tr}} \leq \frac{1}{2}\sqrt{\mathrm{D}_{\chi^2}}$.
- n must be large enough so that $\mathrm{D}_{\chi^2}(\mathbb{E}_{\theta}[\sigma_{\boldsymbol{\theta}}^{\otimes n}] \| \sigma^{\otimes n}) \geq c$.
- **New Tool:** A quantum Ingster-Suslina method to explicitly compute D_{χ^2} and easily upper bound it!

Quantum χ^2-divergence

Given two states ρ, σ, let $\Delta = \rho - \sigma$. Then,

$$\mathrm{D}_{\chi^2}(\rho\|\sigma) = \mathrm{tr}\left(\sigma^{-1}\Delta^2\right) = \mathrm{tr}\left(\sigma^{-1}\rho^2\right) - 1.$$

Quantum χ^2-divergence

Given two states ρ, σ, let $\Delta = \rho - \sigma$. Then,

$$\mathrm{D}_{\chi^2}(\rho\|\sigma) = \mathrm{tr}\left(\sigma^{-1}\Delta^2\right) = \mathrm{tr}\left(\sigma^{-1}\rho^2\right) - 1.$$

Want to upper bound $\mathrm{D}_{\chi^2}(\mathbb{E}_\theta[\sigma_{\boldsymbol{\theta}}^{\otimes n}]\|\sigma^{\otimes n})$.

A Quantum Ingster-Suslina Method

We show:

$$\mathrm{D}_{\chi^2}(\mathbb{E}_\theta[\sigma_{\boldsymbol{\theta}}^{\otimes n}]\|\sigma^{\otimes n}) + 1 = \mathbb{E}_{\boldsymbol{\theta},\boldsymbol{\theta'}}(1 + Z(\boldsymbol{\theta},\boldsymbol{\theta'}))^n$$

where

$$Z(\boldsymbol{\theta},\boldsymbol{\theta'}) = \mathrm{tr}\left(\sigma^{-1}\Delta_{\boldsymbol{\theta}}\Delta_{\boldsymbol{\theta'}}\right) \quad \text{and} \quad \Delta_{\boldsymbol{\theta}} = \sigma_{\boldsymbol{\theta}} - \sigma.$$

A Quantum Ingster-Suslina Method

We show:

$$\mathrm{D}_{\chi^2}(\mathbb{E}_\theta[\sigma_{\boldsymbol{\theta}}^{\otimes n}]\|\sigma^{\otimes n})+1 = \mathbb{E}_{\boldsymbol{\theta},\boldsymbol{\theta}'}(1+Z(\boldsymbol{\theta},\boldsymbol{\theta}'))^n \leq \mathbb{E}_{\boldsymbol{\theta},\boldsymbol{\theta}'} \exp\big(nZ(\boldsymbol{\theta},\boldsymbol{\theta}')\big),$$

where

$$Z(\boldsymbol{\theta},\boldsymbol{\theta}') = \mathrm{tr}\Big(\sigma^{-1}\Delta_{\boldsymbol{\theta}}\Delta_{\boldsymbol{\theta}'}\Big) \quad \text{and} \quad \Delta_{\boldsymbol{\theta}} = \sigma_{\boldsymbol{\theta}} - \sigma.$$

A Quantum Ingster-Suslina Method

We show:

$$\mathrm{D}_{\chi^2}(\mathbb{E}_\theta[\sigma_{\boldsymbol{\theta}}^{\otimes n}]\|\sigma^{\otimes n})+1 = \mathbb{E}_{\boldsymbol{\theta},\boldsymbol{\theta}'}(1+Z(\boldsymbol{\theta},\boldsymbol{\theta}'))^n \leq \mathbb{E}_{\boldsymbol{\theta},\boldsymbol{\theta}'} \exp\big(nZ(\boldsymbol{\theta},\boldsymbol{\theta}')\big),$$

where

$$Z(\boldsymbol{\theta},\boldsymbol{\theta}') = \mathrm{tr}\Big(\sigma^{-1}\Delta_{\boldsymbol{\theta}}\Delta_{\boldsymbol{\theta}'}\Big) \quad \text{and} \quad \Delta_{\boldsymbol{\theta}} = \sigma_{\boldsymbol{\theta}} - \sigma.$$

Usage for certification lower bounds:

1. Construct a suitable mixture of alternatives $\{\sigma_{\boldsymbol{\theta}}\}_{\boldsymbol{\theta}}$.
2. Upper bound $\mathbb{E}_{\boldsymbol{\theta},\boldsymbol{\theta}'} \exp\big(nZ(\boldsymbol{\theta},\boldsymbol{\theta}')\big)$.

Mixedness Testing

Want a lower bound for testing $\rho = \mathbb{1}/d$ or $\|\rho - \mathbb{1}/d\|_1 \geq \epsilon$.

Mixedness Testing

Want a lower bound for testing $\rho = \mathbb{1}/d$ or $\|\rho - \mathbb{1}/d\|_1 \geq \epsilon$.

- Quantum Paninski Construction:

$$\sigma_{\boldsymbol{U}} \triangleq \frac{\mathbb{1}}{d} + \frac{\epsilon}{d}\boldsymbol{U}\Sigma\boldsymbol{U}^\dagger,$$

where $\Sigma = \mathrm{diag}(+1, -1, \ldots, +1, -1)$ and $\boldsymbol{U} \sim U(d)$.

Mixedness Testing

Want a lower bound for testing $\rho = \mathbb{1}/d$ or $\|\rho - \mathbb{1}/d\|_1 \geq \epsilon$.

- Quantum Paninski Construction:

$$\sigma_{\boldsymbol{U}} \triangleq \frac{\mathbb{1}}{d} + \frac{\epsilon}{d}\boldsymbol{U}\Sigma\boldsymbol{U}^\dagger,$$

  where $\Sigma = \mathrm{diag}(+1, -1, \ldots, +1, -1)$ and $\boldsymbol{U} \sim U(d)$.

- $Z(\boldsymbol{U}, \boldsymbol{V}) = \mathrm{tr}\left(\sigma^{-1}\Delta_{\boldsymbol{U}}\Delta_{\boldsymbol{V}}\right)$

Mixedness Testing

Want a lower bound for testing $\rho = \mathbb{1}/d$ or $\|\rho - \mathbb{1}/d\|_1 \geq \epsilon$.

- Quantum Paninski Construction:

$$\sigma_{\boldsymbol{U}} \triangleq \frac{\mathbb{1}}{d} + \frac{\epsilon}{d}\boldsymbol{U}\Sigma\boldsymbol{U}^\dagger,$$

  where $\Sigma = \mathrm{diag}(+1, -1, \ldots, +1, -1)$ and $\boldsymbol{U} \sim U(d)$.

- $Z(\boldsymbol{U}, \boldsymbol{V}) = \mathrm{tr}\left(\sigma^{-1}\Delta_{\boldsymbol{U}}\Delta_{\boldsymbol{V}}\right) = \frac{\epsilon^2}{d}\,\mathrm{tr}\Big(\boldsymbol{U}\Sigma\boldsymbol{U}^\dagger\boldsymbol{V}\Sigma\boldsymbol{V}^\dagger\Big)$.

Mixedness Testing

Want a lower bound for testing $\rho = \mathbb{1}/d$ or $\|\rho - \mathbb{1}/d\|_1 \geq \epsilon$.

- Quantum Paninski Construction:

$$\sigma_{\boldsymbol{U}} \triangleq \frac{\mathbb{1}}{d} + \frac{\epsilon}{d}\boldsymbol{U}\Sigma\boldsymbol{U}^\dagger,$$

  where $\Sigma = \mathrm{diag}(+1, -1, \ldots, +1, -1)$ and $\boldsymbol{U} \sim U(d)$.

- $Z(\boldsymbol{U}, \boldsymbol{V}) = \mathrm{tr}\left(\sigma^{-1}\Delta_{\boldsymbol{U}}\Delta_{\boldsymbol{V}}\right) = \frac{\epsilon^2}{d}\,\mathrm{tr}\Big(\boldsymbol{U}\Sigma\boldsymbol{U}^\dagger\boldsymbol{V}\Sigma\boldsymbol{V}^\dagger\Big)$.
- We use standard Haar-measure concentration inequalities to bound $\mathbb{E}_{\boldsymbol{U},\boldsymbol{V}} \exp\big(nZ(\boldsymbol{U}, \boldsymbol{V})\big)$ and get:

$$\mathrm{D}_{\chi^2}(\mathbb{E}_{\boldsymbol{U}}[\sigma_{\boldsymbol{U}}^{\otimes n}] \| \sigma^{\otimes n}) \leq \exp\left(\frac{C \cdot n^2\epsilon^4}{d^2}\right) - 1.$$

Mixedness Testing

Want a lower bound for testing $\rho = \mathbb{1}/d$ or $\|\rho - \mathbb{1}/d\|_1 \geq \epsilon$.

- Quantum Paninski Construction:

$$\sigma_{\boldsymbol{U}} \triangleq \frac{\mathbb{1}}{d} + \frac{\epsilon}{d}\boldsymbol{U}\Sigma\boldsymbol{U}^\dagger,$$

  where $\Sigma = \mathrm{diag}(+1, -1, \ldots, +1, -1)$ and $\boldsymbol{U} \sim U(d)$.

- $Z(\boldsymbol{U}, \boldsymbol{V}) = \mathrm{tr}\left(\sigma^{-1}\Delta_{\boldsymbol{U}}\Delta_{\boldsymbol{V}}\right) = \frac{\epsilon^2}{d}\,\mathrm{tr}\left(\boldsymbol{U}\Sigma\boldsymbol{U}^\dagger\boldsymbol{V}\Sigma\boldsymbol{V}^\dagger\right)$.
- We use standard Haar-measure concentration inequalities to bound $\mathbb{E}_{\boldsymbol{U},\boldsymbol{V}} \exp\left(nZ(\boldsymbol{U}, \boldsymbol{V})\right)$ and get:

$$\mathrm{D}_{\chi^2}(\mathbb{E}_{\boldsymbol{U}}[\sigma_{\boldsymbol{U}}^{\otimes n}] \| \sigma^{\otimes n}) \leq \exp\left(\frac{C \cdot n^2\epsilon^4}{d^2}\right) - 1.$$

  This is $\Omega(1)$ only if $n = \Omega(d/\epsilon^2)$.

Lower Bounds for Nearly Mixed States

The same technique also works for nearly maximally mixed states! In general, for well-conditioned states σ, we show:

$$n \geq \Omega\left(\frac{d^{5/2}}{\epsilon^2 \cdot \|\sigma^{-1}\|_2}\right).$$

Lower Bounds for Nearly Mixed States

The same technique also works for nearly maximally mixed states! In general, for well-conditioned states σ, we show:

$$n \geq \Omega\left(\frac{d^{5/2}}{\epsilon^2 \cdot \|\sigma^{-1}\|_2}\right).$$

For nearly mixed σ, $\|\sigma^{-1}\|_2^2 = d \times \mathcal{O}(d^2) = \mathcal{O}(d^3)$.

Lower Bounds for Nearly Mixed States

The same technique also works for nearly maximally mixed states! In general, for well-conditioned states σ, we show:

$$n \geq \Omega\left(\frac{d^{5/2}}{\epsilon^2 \cdot \|\sigma^{-1}\|_2}\right).$$

For nearly mixed σ, $\|\sigma^{-1}\|_2^2 = d \times \mathcal{O}(d^2) = \mathcal{O}(d^3)$.

$$\implies n \geq \Omega(d/\epsilon^2).$$

Small Eigenvalues

$$n \geq \Omega\left(\frac{d^{5/2}}{\epsilon^2 \cdot \|\sigma^{-1}\|_2}\right).$$

But this bound is not always strong enough!

Consider, e.g., σ with spectrum $= (\Omega(1/d), \ldots, \Omega(1/d), 1/d^2)$.

Small Eigenvalues

$$n \geq \Omega\left(\frac{d^{5/2}}{\epsilon^2 \cdot \|\sigma^{-1}\|_2}\right).$$

But this bound is not always strong enough!

Consider, e.g., σ with spectrum $= (\Omega(1/d), \ldots, \Omega(1/d), 1/d^2)$.

Such a state has

$$\|\sigma^{-1}\|_2^2 = \mathcal{O}((d-1) \cdot d^2) + d^4 = \mathcal{O}(d^4).$$

This only results in a $\Omega(\sqrt{d}/\epsilon^2)$ bound.

Small Eigenvalues

$$n \geq \Omega\left(\frac{d^{5/2}}{\epsilon^2 \cdot \|\sigma^{-1}\|_2}\right).$$

But this bound is not always strong enough!

Consider, e.g., σ with spectrum $= (\Omega(1/d), \ldots, \Omega(1/d), 1/d^2)$.

Such a state has

$$\|\sigma^{-1}\|_2^2 = \mathcal{O}((d-1) \cdot d^2) + d^4 = \mathcal{O}(d^4).$$

This only results in a $\Omega(\sqrt{d}/\epsilon^2)$ bound.

$\Rightarrow$ We place too much emphasis on the smallest eigenvalues!

Bucketing and Mass Removal

- WLOG, we assume $\sigma = \mathrm{diag}(\lambda_1, \ldots \lambda_d)$.

Bucketing and Mass Removal

- WLOG, we assume $\sigma = \mathrm{diag}(\lambda_1, \ldots \lambda_d)$.

$$\begin{pmatrix} 1/7 & & & & & & \\ & 1/8 & & & & & \\ & & \ddots & & & & \\ & & & 1/16 & & & \\ & & & & 1/17 & & \\ & & & & & 1/32 & \\ & & & & & & \epsilon/2 \\ & & & & & & & \epsilon/4 \end{pmatrix}$$

Bucketing and Mass Removal

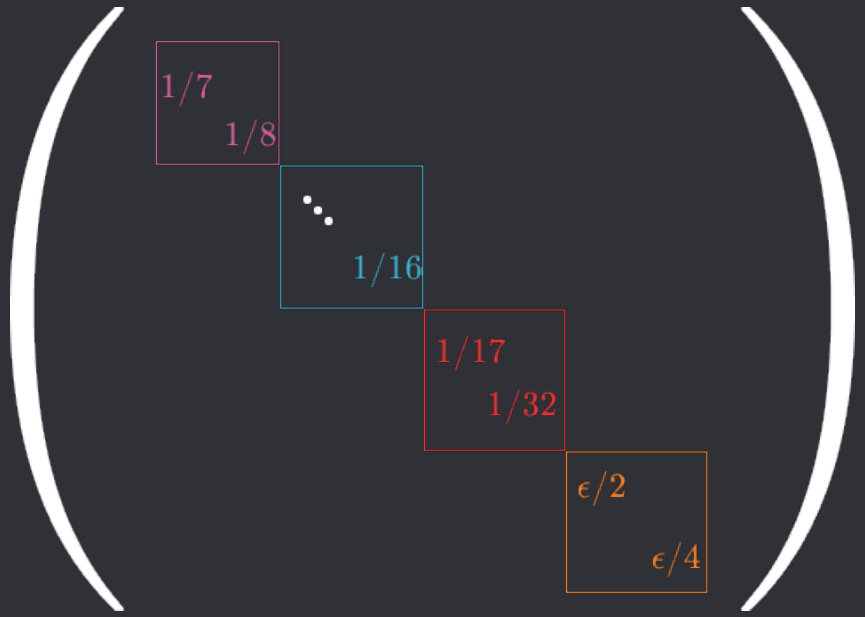
- WLOG, we assume $\sigma = \mathrm{diag}(\lambda_1, \ldots \lambda_d)$.
- Group λ_is into buckets: $i \in S_j$ if $\lambda_i \in [2^{-j-1}, 2^{-j})$.
- Group some small λ_is adding up to $\mathcal{O}(\epsilon)$ into S_{tail}.

Bucketing and Mass Removal

- WLOG, we assume $\sigma = \mathrm{diag}(\lambda_1, \ldots \lambda_d)$.
- Group λ_is into buckets: $i \in S_j$ if $\lambda_i \in [2^{-j-1}, 2^{-j})$.
- Group some small λ_is adding up to $\mathcal{O}(\epsilon)$ into S_{tail}.

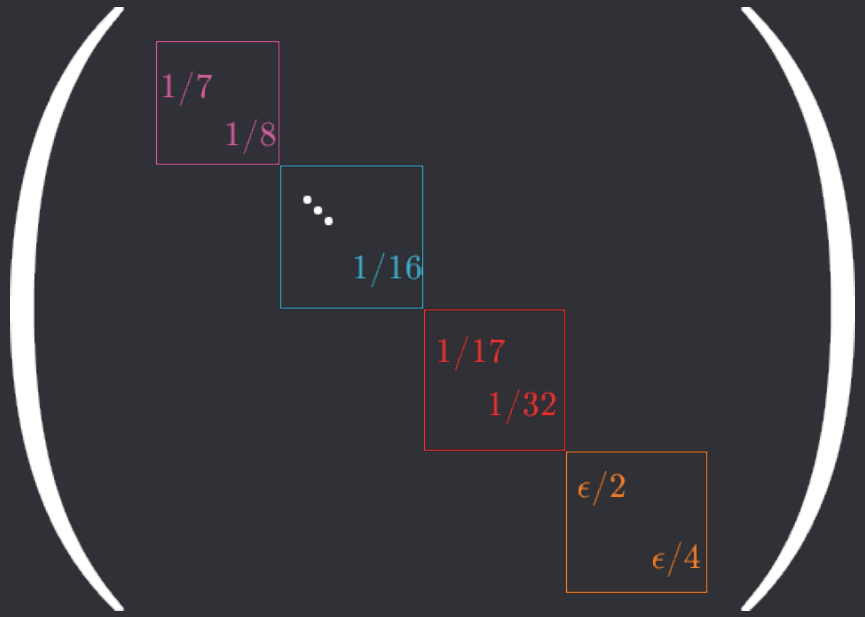
Bucketing and Mass Removal

- WLOG, we assume $\sigma = \mathrm{diag}(\lambda_1, \ldots \lambda_d)$.
- Group λ_is into buckets: $i \in S_j$ if $\lambda_i \in [2^{-j-1}, 2^{-j})$.
- Group some small λ_is adding up to $\mathcal{O}(\epsilon)$ into S_{tail}.



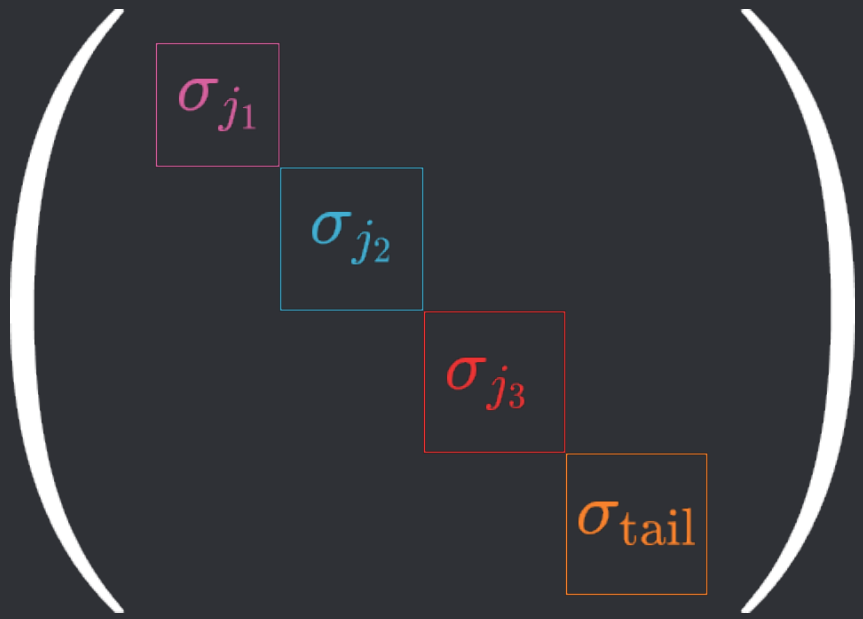
Bucketing and Mass Removal

- WLOG, we assume $\sigma = \mathrm{diag}(\lambda_1, \ldots \lambda_d)$.
- Group λ_is into buckets: $i \in S_j$ if $\lambda_i \in [2^{-j-1}, 2^{-j})$.
- Group some small λ_is adding up to $\mathcal{O}(\epsilon)$ into S_{tail}.
- $\sigma = \sigma_{\mathrm{tail}} \oplus \bigoplus_j \sigma_j$.

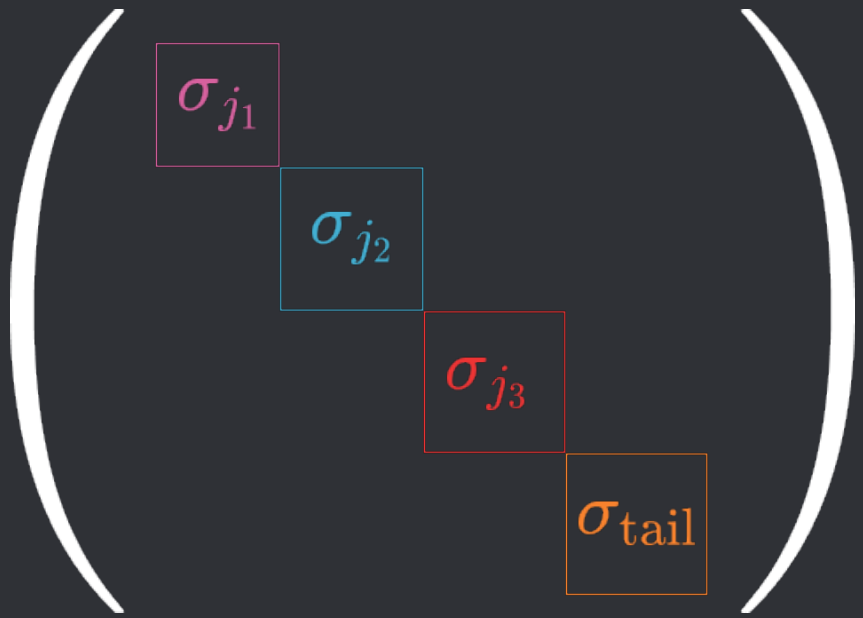


Bucketing and Mass Removal

- WLOG, we assume $\sigma = \mathrm{diag}(\lambda_1, \ldots \lambda_d)$.
- Group λ_is into buckets: $i \in S_j$ if $\lambda_i \in [2^{-j-1}, 2^{-j})$.
- Group some small λ_is adding up to $\mathcal{O}(\epsilon)$ into S_{tail}.
- $\sigma = \sigma_{\mathrm{tail}} \oplus \bigoplus_j \sigma_j$.

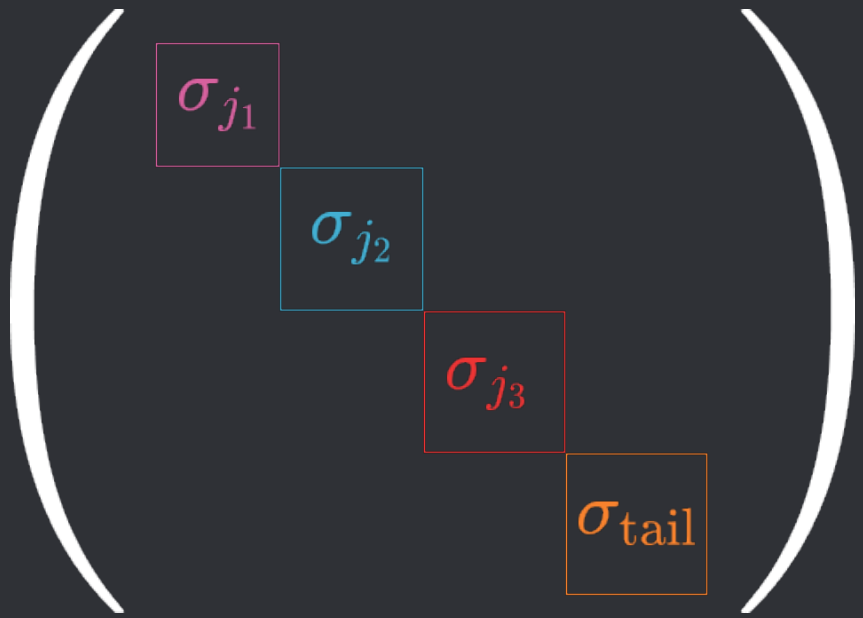


Mixture of Alternatives



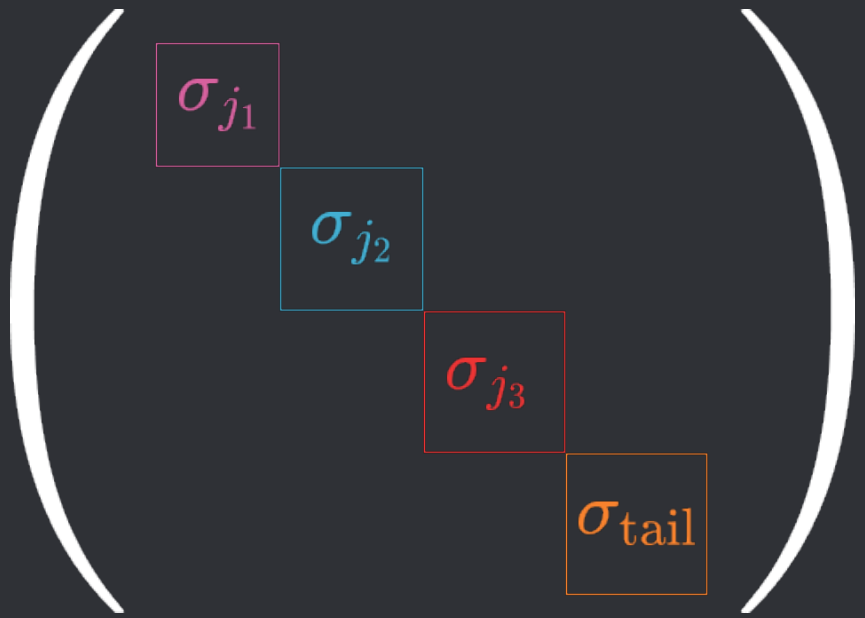
Mixture of Alternatives

- $\mathbb{C}^{d_j \times d_j} \ni \Sigma_j \triangleq \operatorname{diag}(+1, -1, \ldots, +1, -1).$



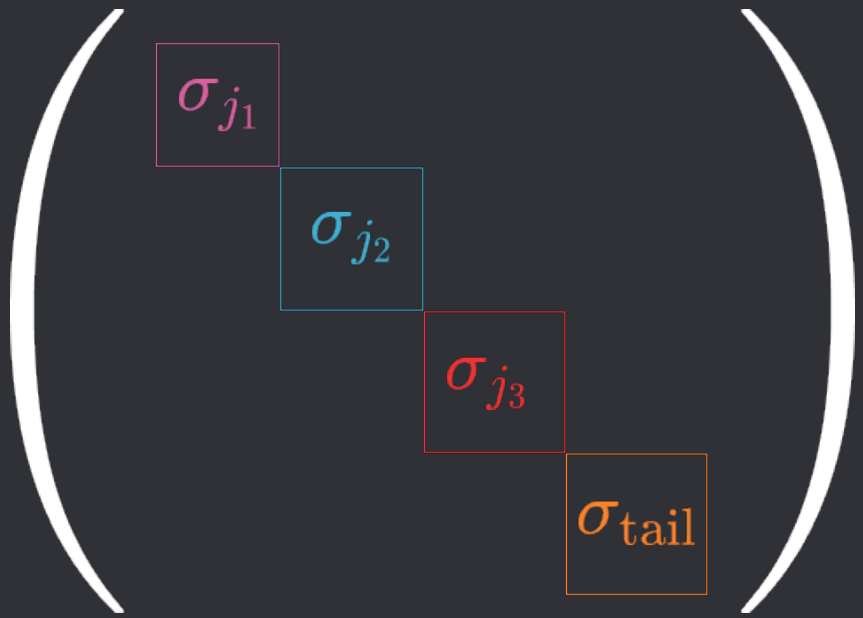
Mixture of Alternatives

- $\mathbb{C}^{d_j \times d_j} \ni \Sigma_j \triangleq \mathrm{diag}(+1, -1, \ldots, +1, -1)$.
- $\Delta_j \triangleq \epsilon_j \boldsymbol{U}_j \Sigma_j \boldsymbol{U}_j^\dagger$, where $\epsilon_j \leq 2^{-j-1}$, $\boldsymbol{U}_j \sim U(d_j)$ and $\sum_j \epsilon_j d_j \geq \epsilon$.



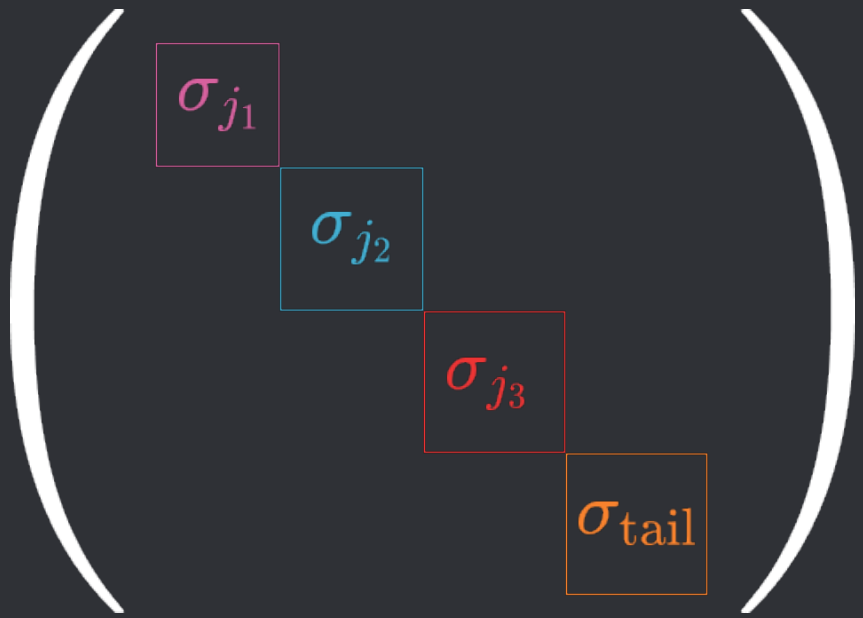
Mixture of Alternatives

- $\mathbb{C}^{d_j \times d_j} \ni \Sigma_j \triangleq \mathrm{diag}(+1, -1, \ldots, +1, -1)$.
- $\Delta_j \triangleq \epsilon_j \boldsymbol{U}_j \Sigma_j \boldsymbol{U}_j^\dagger$, where $\epsilon_j \leq 2^{-j-1}$, $\boldsymbol{U}_j \sim U(d_j)$ and $\sum_j \epsilon_j d_j \geq \epsilon$.
- Let $\vec{\boldsymbol{U}} = (\boldsymbol{U}_1, \ldots, \boldsymbol{U}_m)$.



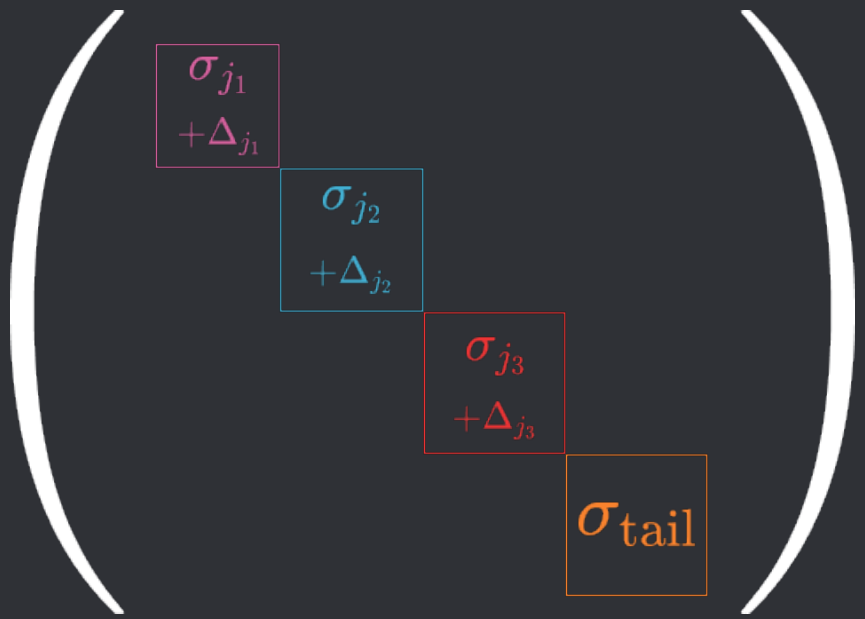
Mixture of Alternatives

- $\mathbb{C}^{d_j \times d_j} \ni \Sigma_j \triangleq \mathrm{diag}(+1, -1, \ldots, +1, -1)$.
- $\Delta_j \triangleq \epsilon_j \boldsymbol{U}_j \Sigma_j \boldsymbol{U}_j^\dagger$, where $\epsilon_j \leq 2^{-j-1}$, $\boldsymbol{U}_j \sim U(d_j)$ and $\sum_j \epsilon_j d_j \geq \epsilon$.
- Let $\vec{\boldsymbol{U}} = (\boldsymbol{U}_1, \ldots, \boldsymbol{U}_m)$.
- $\sigma_{\vec{\boldsymbol{U}}} \triangleq \sigma_{\mathrm{tail}} \oplus \bigoplus_j (\sigma_j + \Delta_j)$.



Mixture of Alternatives

- $\mathbb{C}^{d_j \times d_j} \ni \Sigma_j \triangleq \mathrm{diag}(+1, -1, \ldots, +1, -1)$.
- $\Delta_j \triangleq \epsilon_j \boldsymbol{U}_j \Sigma_j \boldsymbol{U}_j^\dagger$, where $\epsilon_j \leq 2^{-j-1}$, $\boldsymbol{U}_j \sim U(d_j)$ and $\sum_j \epsilon_j d_j \geq \epsilon$.
- Let $\vec{\boldsymbol{U}} = (\boldsymbol{U}_1, \ldots, \boldsymbol{U}_m)$.
- $\sigma_{\vec{\boldsymbol{U}}} \triangleq \sigma_{\mathrm{tail}} \oplus \bigoplus_j (\sigma_j + \Delta_j)$.



Decomposition into Independent RVs

$$\mathrm{D}_{\chi^2}(\mathbb{E}_{\vec{\boldsymbol{U}}}[\sigma_{\vec{\boldsymbol{U}}}^{\otimes n}]\|\sigma^{\otimes n}) = \mathbb{E}_{\vec{\boldsymbol{U}},\vec{\boldsymbol{V}}}\left[(1+Z(\vec{\boldsymbol{U}},\vec{\boldsymbol{V}}))^n\right] - 1,$$

Decomposition into Independent RVs

$$\mathrm{D}_{\chi^2}(\mathbb{E}_{\vec{\boldsymbol{U}}}[\sigma_{\vec{\boldsymbol{U}}}^{\otimes n}]\|\sigma^{\otimes n}) = \mathbb{E}_{\vec{\boldsymbol{U}},\vec{\boldsymbol{V}}}\left[(1+Z(\vec{\boldsymbol{U}},\vec{\boldsymbol{V}}))^n\right] - 1,$$

where

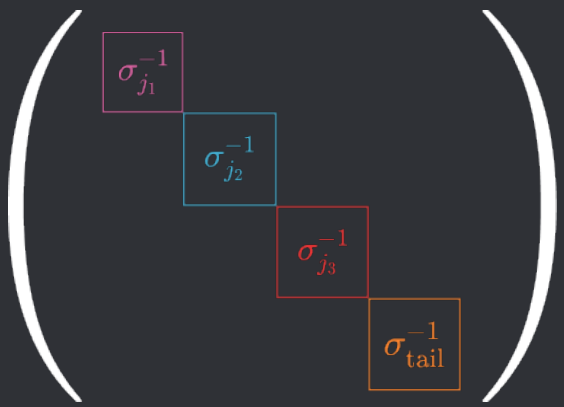
$$Z(\vec{\boldsymbol{U}},\vec{\boldsymbol{V}}) = \mathrm{tr}\left(\sigma^{-1}\Delta_{\vec{\boldsymbol{U}}}\Delta_{\vec{\boldsymbol{V}}}\right).$$

Decomposition into Independent RVs

$$Z(\vec{\boldsymbol{U}}, \vec{\boldsymbol{V}}) = \operatorname{tr}\left(\sigma^{-1}\Delta_{\vec{\boldsymbol{U}}}\Delta_{\vec{\boldsymbol{V}}}\right).$$

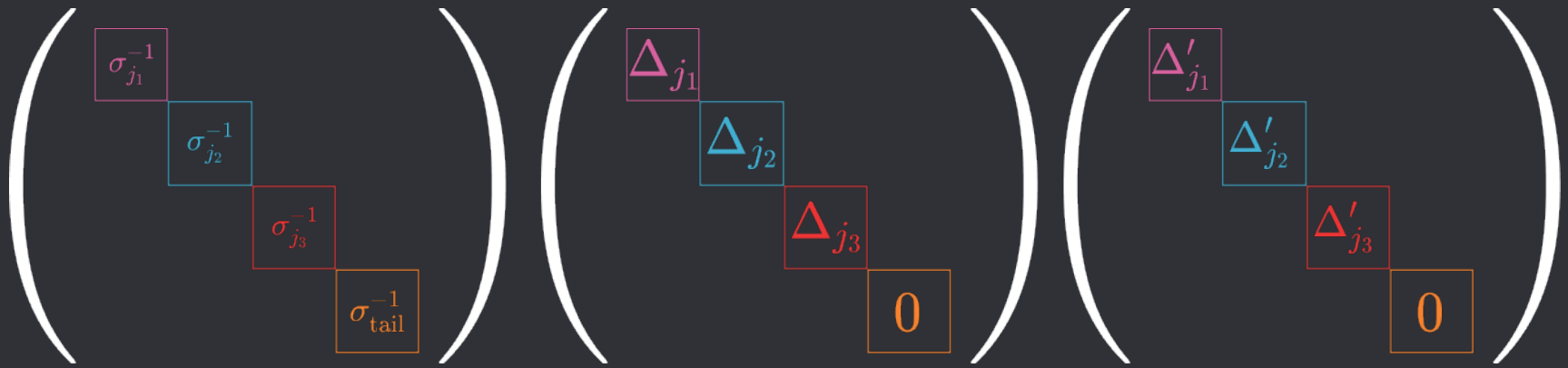
Decomposition into Independent RVs

$$\sigma^{-1}$$



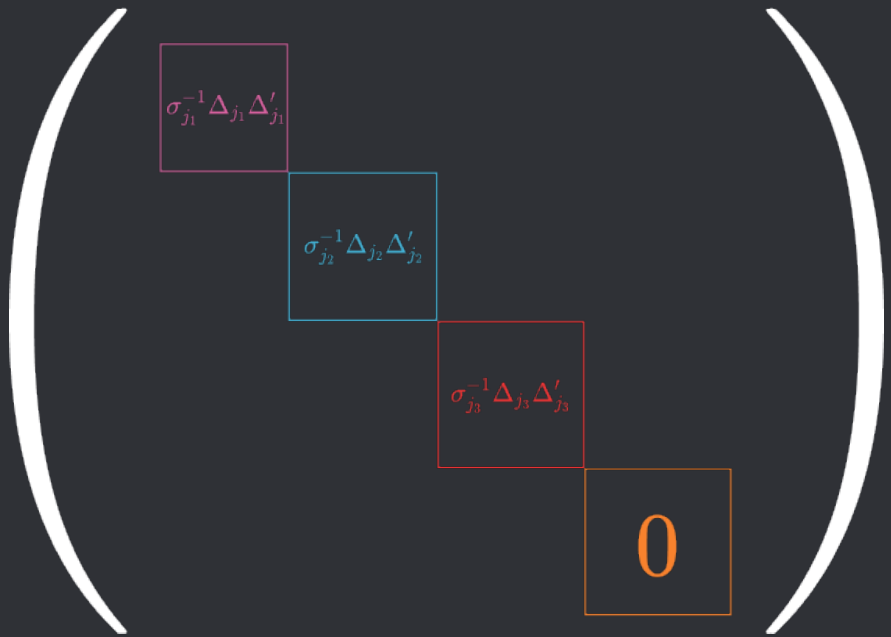
Decomposition into Independent RVs

$$\sigma^{-1}\Delta_{\vec{u}}\Delta_{\vec{v}}$$



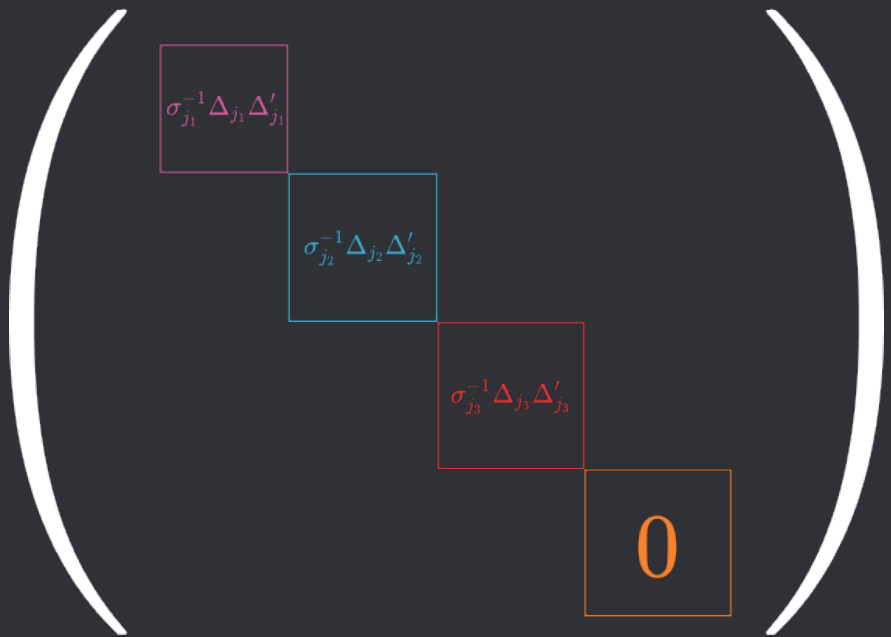
Decomposition into Independent RVs

$$\sigma^{-1}\Delta_{\vec{u}}\Delta_{\vec{v}}$$



Decomposition into Independent RVs

$$Z(\vec{\boldsymbol{U}}, \vec{\boldsymbol{V}}) = \mathrm{tr}\left(\sigma^{-1}\Delta_{\vec{\boldsymbol{U}}}\Delta_{\vec{\boldsymbol{V}}}\right) = \sum_j \mathrm{tr}\left(\sigma_j^{-1}\Delta_j\Delta_j'\right).$$



Final Steps

$$
\begin{aligned}
\mathrm{D}_{\chi^2} + 1 &\leq \mathbb{E}_{\vec{\boldsymbol{U}},\vec{\boldsymbol{V}}} \exp\Big(n \cdot Z(\vec{\boldsymbol{U}},\vec{\boldsymbol{V}})\Big) \\
&= \mathbb{E}_{\vec{\boldsymbol{U}},\vec{\boldsymbol{V}}} \exp\left(\sum_j n \cdot \mathrm{tr}\Big(\sigma_j^{-1}\Delta_j\Delta_j'\Big)\right) \\
&= \prod_j \mathbb{E}_{\boldsymbol{U}_j,\boldsymbol{V}_j} \exp\left(n \cdot \mathrm{tr}\Big(\sigma_j^{-1}\Delta_j\Delta_j'\Big)\right).
\end{aligned}
$$

Final Steps

$$\mathrm{D}_{\chi^2} + 1 \leq \prod_j \mathbb{E}_{\boldsymbol{u}_j, \boldsymbol{v}_j} \exp\left(n \cdot \mathrm{tr}\left(\sigma_j^{-1} \Delta_j \Delta_j' \right) \right).$$

$\Rightarrow$ We just need to bound each expectation!

Final Steps

$$\mathrm{D}_{\chi^2} + 1 \leq \prod_j \mathbb{E}_{\boldsymbol{u}_j, \boldsymbol{v}_j} \exp\left(n \cdot \mathrm{tr}\left(\sigma_j^{-1} \Delta_j \Delta_j' \right) \right).$$

$\Rightarrow$ We just need to bound each expectation!

This yields

$$n = \Omega\left(\sum_j \epsilon_j^4 2^{2j} \right)^{-1/2}.$$

Final Steps

$$\mathrm{D}_{\chi^2} + 1 \leq \prod_j \mathbb{E}_{\boldsymbol{U}_j, \boldsymbol{V}_j} \exp\left(n \cdot \mathrm{tr}\left(\sigma_j^{-1} \Delta_j \Delta_j' \right) \right).$$

$\Rightarrow$ We just need to bound each expectation!

This yields

$$n = \Omega\left(\sum_j \epsilon_j^4 2^{2j} \right)^{-1/2}.$$

This does give $n \geq \tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2} \right)$, but takes some work:

Final Steps

$$\mathrm{D}_{\chi^2} + 1 \leq \prod_j \mathbb{E}_{\boldsymbol{u}_j, \boldsymbol{v}_j} \exp\left(n \cdot \mathrm{tr}\left(\sigma_j^{-1} \Delta_j \Delta_j' \right) \right).$$

$\Rightarrow$ We just need to bound each expectation!

This yields

$$n = \Omega\left(\sum_j \epsilon_j^4 2^{2j} \right)^{-1/2}.$$

This does give $n \geq \tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2} \right)$, but takes some work:

- Pick $\{\epsilon_j\}$.
- Corner cases: all buckets have $d_j = 1$ or $\|\rho\|_\infty \geq \frac{1}{2}$.

Details in the paper (Section 5)

Outline

Tools from Prior Work

Tools from Prior Work

[CLO22] showed that if $\|\rho - \sigma\|_1 \geq \epsilon$, then there are a few "simpler" ways in which these states can be far.

Tools from Prior Work

[CLO22] showed that if $\|\rho - \sigma\|_1 \geq \epsilon$, then there are a few "simpler" ways in which these states can be far.

$\Rightarrow$ They test for each such case with an unentangled-measurement Hilbert-Schmidt certifier.

Tools from Prior Work

[CLO22] showed that if $\|\rho - \sigma\|_1 \geq \epsilon$, then there are a few "simpler" ways in which these states can be far.

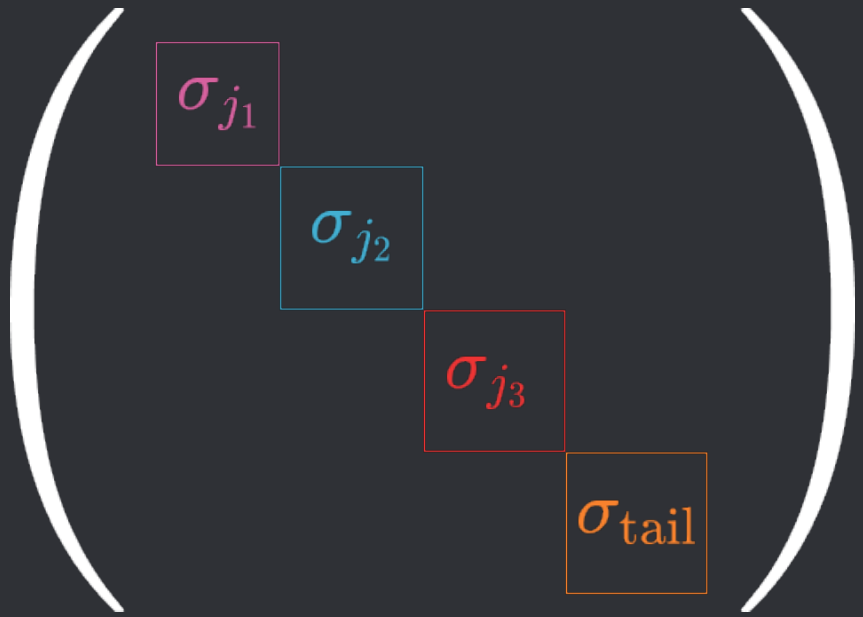
$\Rightarrow$ They test for each such case with an unentangled-measurement Hilbert-Schmidt certifier.

$\Rightarrow$ We replace this with an entangled-measurement certifier.

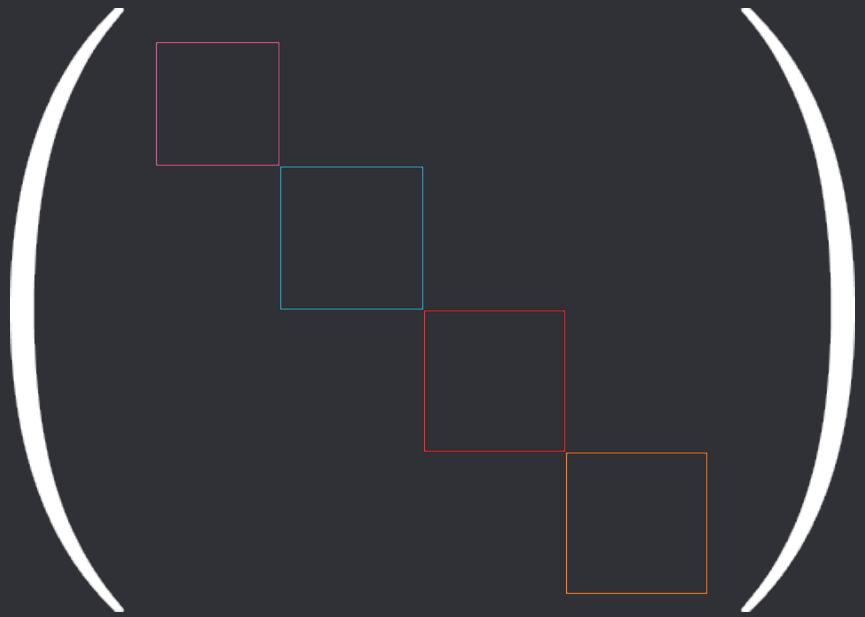
Theorem (Hilbert-Schmidt Tester from [BOW19])

There exists an algorithm HSCertify *that can distinguish between* $\rho = \sigma$ *and* $\|\rho - \sigma\|_2 \geq \epsilon$ *using* $\mathcal{O}(1/\epsilon^2)$ *copies of* ρ.

Upper Bound

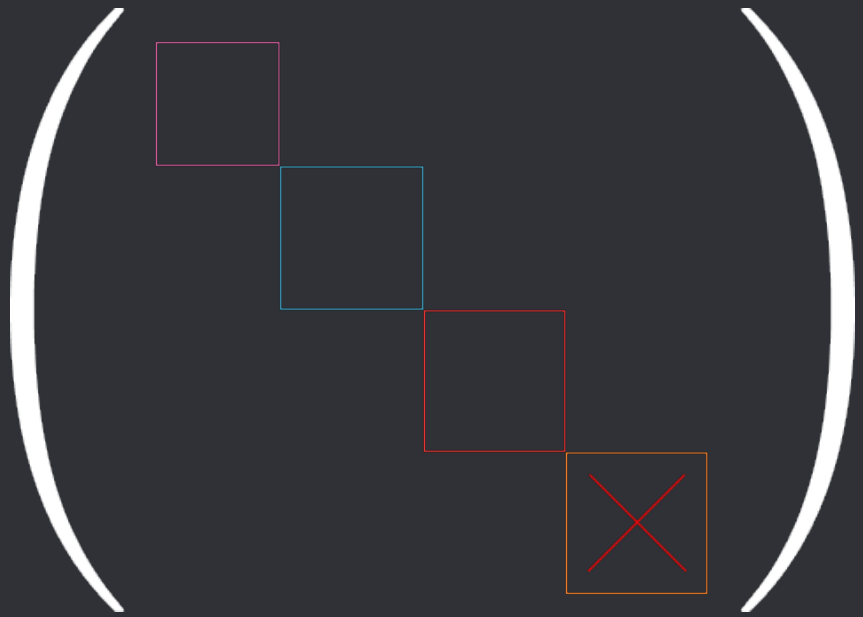


Upper Bound



Upper Bound: Case 1

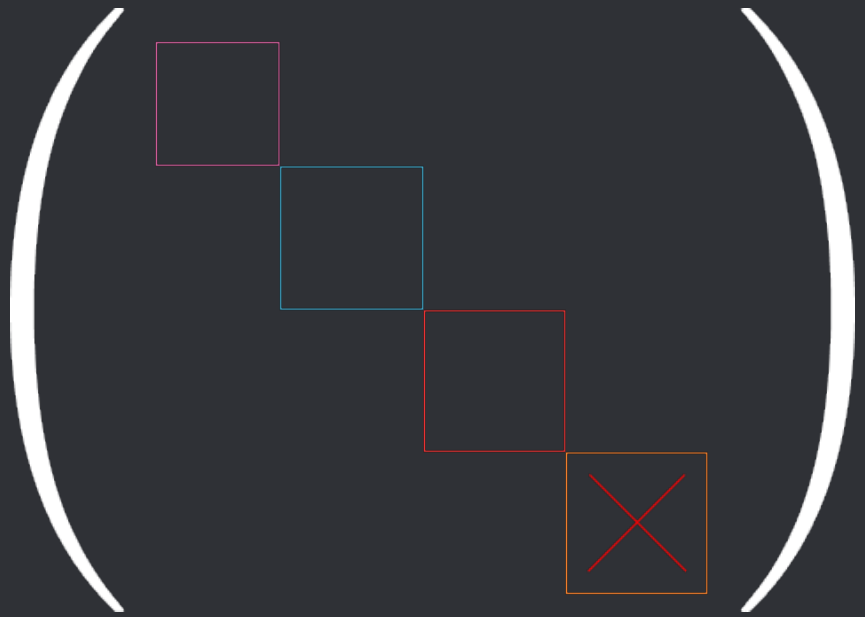
Case 1: The unknown state has too much weight on the tail.



Upper Bound: Case 1

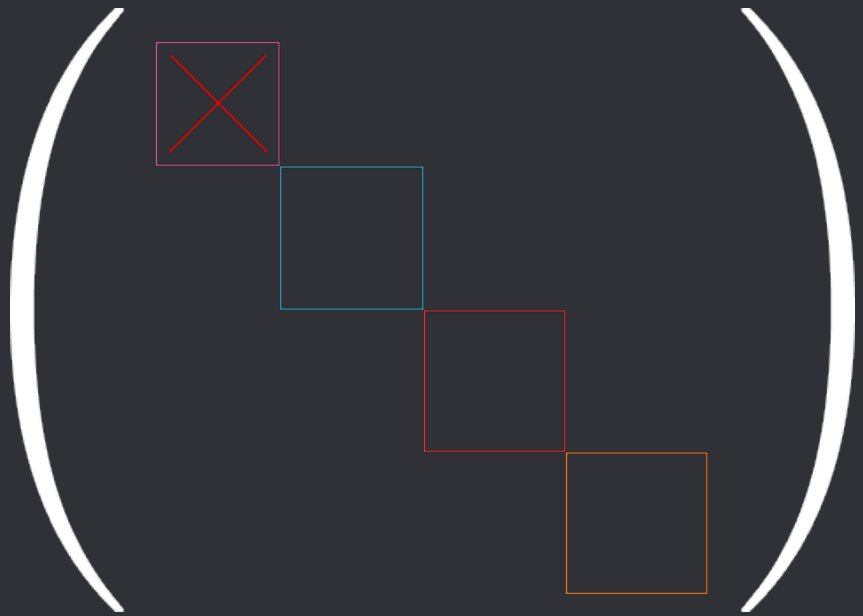
Case 1: The unknown state has too much weight on the tail.

Can be tested for with $\mathcal{O}(1/\epsilon^2)$ (unentangled!) measurements (from [**CLO22**]).



Upper Bound: Case 2

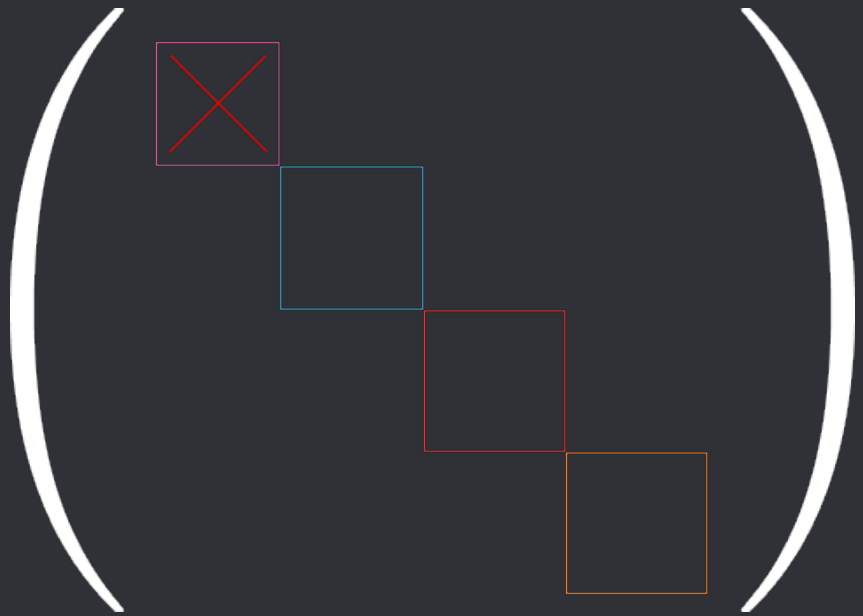
Case 2: For some bucket j, $\|\rho_j - \sigma_j\|_1$ is too large.



Upper Bound: Case 2

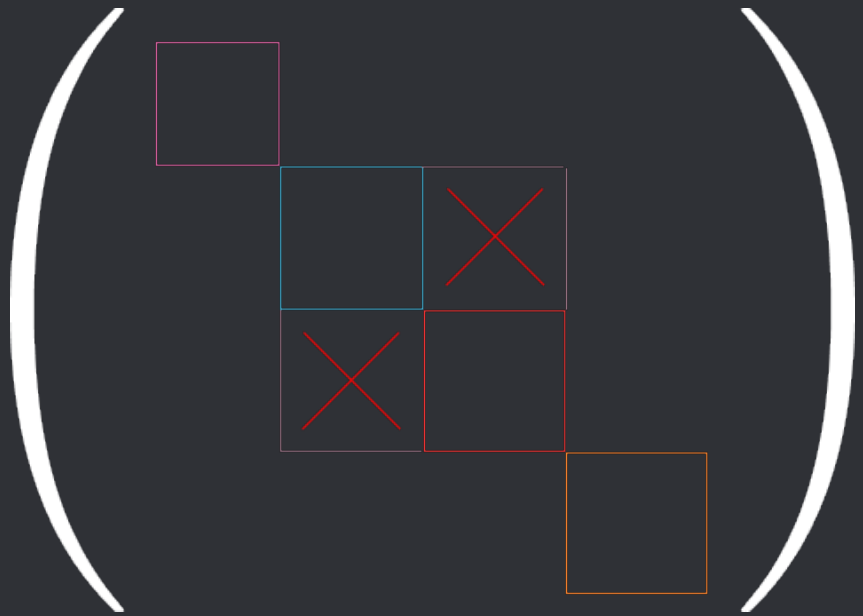
Case 2: For some bucket j, $\|\rho_j - \sigma_j\|_1$ is too large.

After simple pre-processing, projecting and then passing to HSCertify, this can be handled with $\tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right)$ copies of ρ.



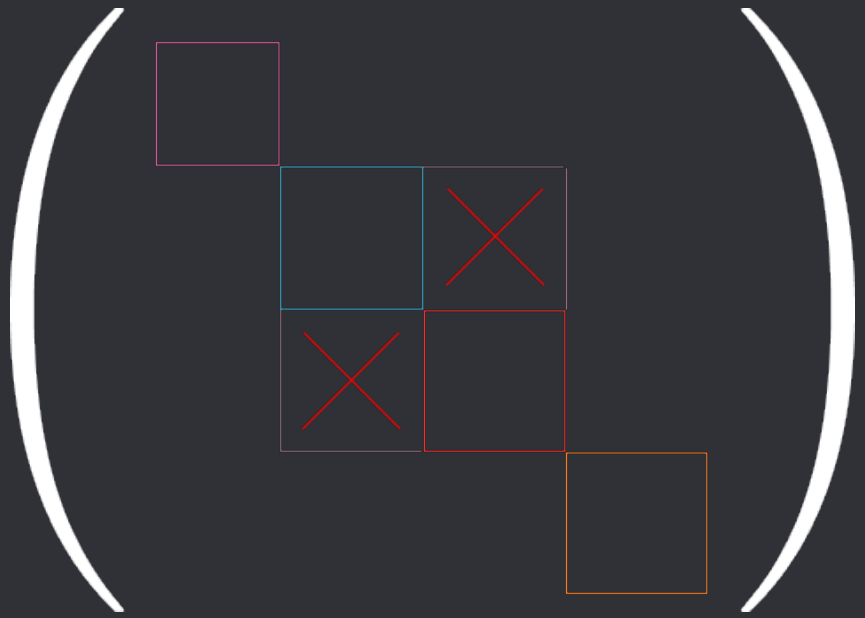
Upper Bound: Case 3

Case 3: For some buckets j, j', the non-principal submatrices are too far.



Upper Bound: Case 3

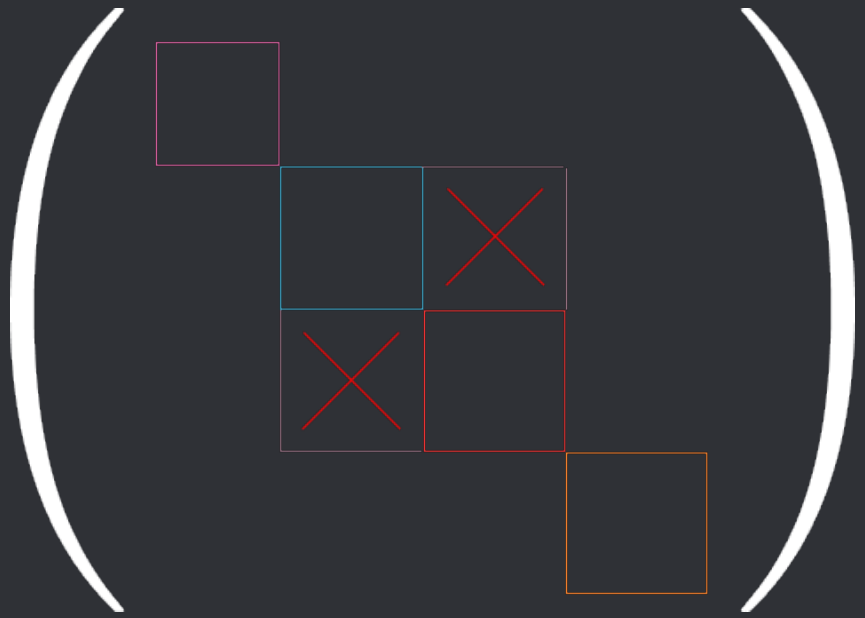
Case 3: For some buckets j, j', the non-principal submatrices are too far.



Assuming Case 2 does not hold, this can again be handled with $\tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right)$ copies of ρ.

Upper Bound: Case 3

Case 3: For some buckets j, j', the non-principal submatrices are too far.



Assuming Case 2 does not hold, this can again be handled with $\tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right)$ copies of ρ.

Total complexity: Case 1 + Case 2 + Case 3 $= \tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right)$

Discussion

We have shown nearly instance-optimal bounds for state certification with entangled measurements:

$$\tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right) \leq n \leq \tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right).$$

Discussion

We have shown nearly instance-optimal bounds for state certification with entangled measurements:

$$\tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right) \leq n \leq \tilde{O}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right).$$

Open Questions:

Discussion

We have shown nearly instance-optimal bounds for state certification with entangled measurements:

$$\tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right) \leq n \leq \tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right).$$

Open Questions:

- The amounts of mass removed to get $\underline{\sigma}, \overline{\sigma}$ do not match; can this be overcome?
- What about state certification with t-copy measurements, with $1 < t \ll d/\epsilon^2$? [CCHL21] have some partial results, but even worst-case bounds remain open.

[CCHL21]: A hierarchy for replica quantum advantage; Chen-Cotler-Huang-Li 2021.

Discussion

We have shown nearly instance-optimal bounds for state certification with entangled measurements:

$$\tilde{\Omega}\left(\frac{d \cdot F(\underline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right) \leq n \leq \tilde{\mathcal{O}}\left(\frac{d \cdot F(\overline{\sigma}, \mathbb{1}/d)}{\epsilon^2}\right).$$

Open Questions:

- The amounts of mass removed to get $\underline{\sigma}, \overline{\sigma}$ do not match; can this be overcome?
- What about state certification with t-copy measurements, with $1 < t \ll d/\epsilon^2$? [CCHL21] have some partial results, but even worst-case bounds remain open.

Thank you!

arxiv:2507.06010

chirag.wadhwa@ed.ac.uk