

Distributed Quantum Property Testing with Communication Constraints

Chirag Wadhwa (University of Edinburgh)

QCOW2, 23/04/2026

arXiv:2604.05962

Joint work with Mina Doosti (UoE) & Ryan Sweke (AIMS)

Outline

Setup

Our Results

Upper Bound Ideas

Lower Bound Ideas

Future Directions

Outline

Setup

Our Results

Upper Bound Ideas

Lower Bound Ideas

Future Directions

Quantum State Inference

Given m copies of an unknown quantum state $\rho \in \mathbb{C}^{d \times d}$, one may be interested in solving:

Quantum State Inference

Given m copies of an unknown quantum state $\rho \in \mathbb{C}^{d \times d}$, one may be interested in solving:

- **State Tomography**: Output a hypothesis state $\hat{\rho}$ with $d(\rho, \hat{\rho}) \leq \epsilon$.

Quantum State Inference

Given m copies of an unknown quantum state $\rho \in \mathbb{C}^{d \times d}$, one may be interested in solving:

- **State Tomography:** Output a hypothesis state $\hat{\rho}$ with $d(\rho, \hat{\rho}) \leq \epsilon$.
- **Property Estimation:** Estimate some function $f(\rho)$ within error ϵ .

Quantum State Inference

Given m copies of an unknown quantum state $\rho \in \mathbb{C}^{d \times d}$, one may be interested in solving:

- **State Tomography**: Output a hypothesis state $\hat{\rho}$ with $d(\rho, \hat{\rho}) \leq \epsilon$.
- **Property Estimation**: Estimate some function $f(\rho)$ within error ϵ . e.g., Shadow Tomography: $f(\rho) = \text{tr}(O\rho)$; Moment Estimation: $f(\rho) = \text{tr}(\rho^k)$.

Quantum State Inference

Given m copies of an unknown quantum state $\rho \in \mathbb{C}^{d \times d}$, one may be interested in solving:

- **State Tomography**: Output a hypothesis state $\hat{\rho}$ with $d(\rho, \hat{\rho}) \leq \epsilon$.
- **Property Estimation**: Estimate some function $f(\rho)$ within error ϵ . e.g., Shadow Tomography: $f(\rho) = \text{tr}(O\rho)$; Moment Estimation: $f(\rho) = \text{tr}(\rho^k)$.
- **Property Testing**: Check whether ρ satisfies a property $\mathcal{P}$ or is at least ϵ -far from all such states. e.g., state certification.

Quantum State Certification

Quantum State Certification

- **State Certification:** Given $\rho^{\otimes m}$ and the full description of a hypothesis state σ , determine whether $\rho = \sigma$ or if $d(\rho, \sigma) \geq \epsilon$.

Quantum State Certification

- **State Certification:** Given $\rho^{\otimes m}$ and the full description of a hypothesis state σ , determine whether $\rho = \sigma$ or if $d(\rho, \sigma) \geq \epsilon$.
- **Optimal Bounds:** With respect to the trace distance, $m = \Theta(d/\epsilon^2)$ copies are necessary [OW15] and sufficient [BOW19].

[OW15]: Quantum Spectrum Testing; O'Donnell-Wright 2015.

[BOW19]: Quantum State Certification; Bădescu-O'Donnell-Wright 2019.

Quantum State Certification

- **State Certification:** Given $\rho^{\otimes m}$ and the full description of a hypothesis state σ , determine whether $\rho = \sigma$ or if $d(\rho, \sigma) \geq \epsilon$.
- **Optimal Bounds:** With respect to the trace distance, $m = \Theta(d/\epsilon^2)$ copies are necessary [OW15] and sufficient [BOW19].
- [BOW19] show that $\mathcal{O}(1/\epsilon^2)$ copies suffice to test w.r.t $\|\cdot\|_2$.

[OW15]: Quantum Spectrum Testing; O'Donnell-Wright 2015.

[BOW19]: Quantum State Certification; Bădescu-O'Donnell-Wright 2019.

Quantum State Certification

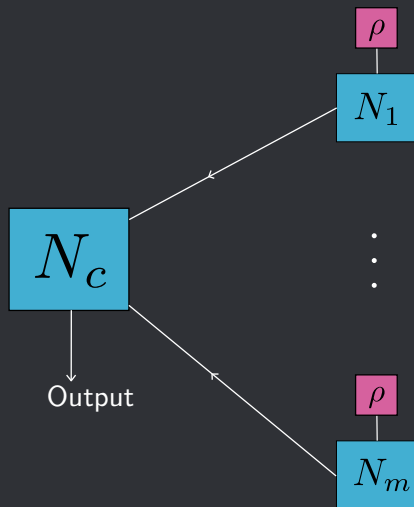
- **State Certification:** Given $\rho^{\otimes m}$ and the full description of a hypothesis state σ , determine whether $\rho = \sigma$ or if $d(\rho, \sigma) \geq \epsilon$.
- **Optimal Bounds:** With respect to the trace distance, $m = \Theta(d/\epsilon^2)$ copies are necessary [OW15] and sufficient [BOW19].
- [BOW19] show that $\mathcal{O}(1/\epsilon^2)$ copies suffice to test w.r.t $\|\cdot\|_2$.
- This problem has been studied under various constraints: e.g., limited entanglement, lack of adaptivity, lack of shared randomness.

[OW15]: Quantum Spectrum Testing; O'Donnell-Wright 2015.

[BOW19]: Quantum State Certification; Bădescu-O'Donnell-Wright 2019.

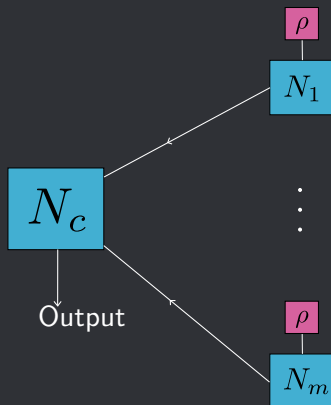
Our Distributed Setting

Our Distributed Setting



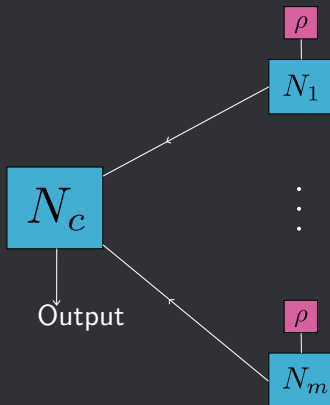
- m distributed nodes $N_1, \dots, N_m$.
- Each receives a copy of an unknown state ρ .
- Send one-way messages to a central node N_c .
- N_c uses this info to solve an inference task.

Related Settings



Related Settings

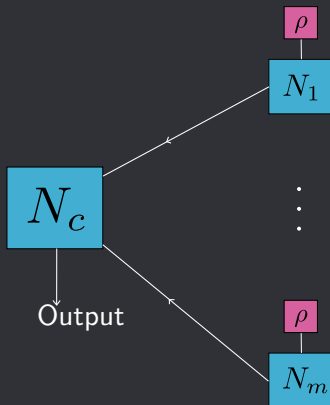
- Generalization of classical setting for learning/testing distributions [ACT19,ACT20].



[ACT19]: Inference under Information Constraints: Lower Bounds from Chi-Square Contraction; Acharya-Canonne-Tyagi 2019

[ACT20]: Inference under Information Constraints II: Communication Constraints and Shared Randomness; Acharya-Canonne-Tyagi 2019

Related Settings

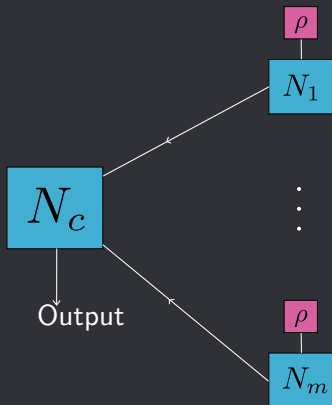


- Generalization of classical setting for learning/testing distributions [ACT19,ACT20].
- With unbounded quantum communication, equivalent to centralized setting.

[ACT19]: Inference under Information Constraints: Lower Bounds from Chi-Square Contraction; Acharya-Canonne-Tyagi 2019

[ACT20]: Inference under Information Constraints II: Communication Constraints and Shared Randomness; Acharya-Canonne-Tyagi 2019

Related Settings

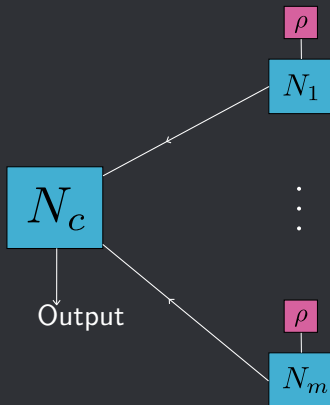


- Generalization of classical setting for learning/testing distributions [ACT19,ACT20].
- With unbounded quantum communication, equivalent to centralized setting.
- Unbounded classical communication equivalent to centralized setting with non-adaptive single-copy measurements.

[ACT19]: Inference under Information Constraints: Lower Bounds from Chi-Square Contraction; Acharya-Canonne-Tyagi 2019

[ACT20]: Inference under Information Constraints II: Communication Constraints and Shared Randomness; Acharya-Canonne-Tyagi 2019

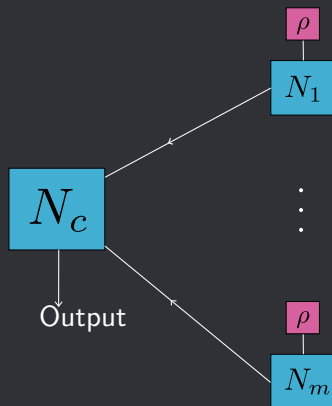
Related Settings



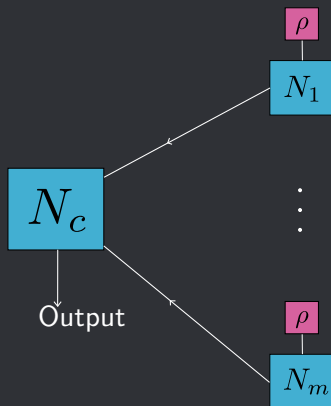
- Generalization of classical setting for learning/testing distributions [ACT19,ACT20].
- With unbounded quantum communication, equivalent to centralized setting.
- Unbounded classical communication equivalent to centralized setting with non-adaptive single-copy measurements.
- Bounds for limited classical communication implied by [LA24].

[LA24]: Quantum State Testing with Restricted Measurements; Liu-Acharya 2024.

Main Problem



Main Problem

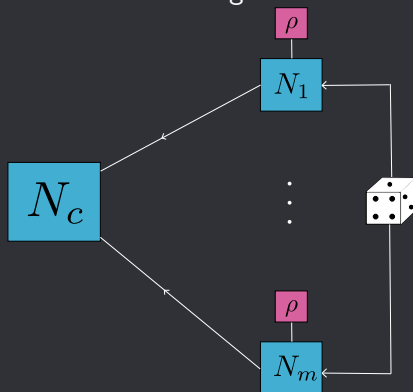


We will thus focus on quantum state certification in this setting with *limited quantum communication*.

Public versus Private Randomness

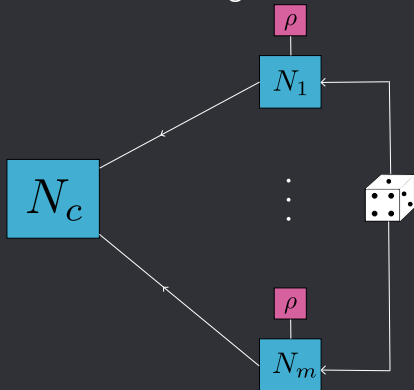
Public versus Private Randomness

Public-Coin Setting

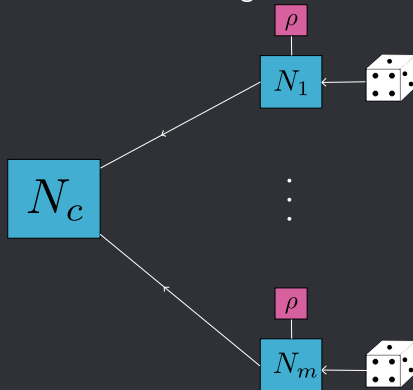


Public versus Private Randomness

Public-Coin Setting



Private-Coin Setting



A Helpful Perspective

- Suppose each node can send q qubits.

A Helpful Perspective

- Suppose each node can send q qubits.
- Can imagine action of node N_i as a quantum channel $\Phi_i : \mathbb{C}^{d \times d} \mapsto \mathbb{C}^{2^q \times 2^q}$.

A Helpful Perspective

- Suppose each node can send q qubits.
- Can imagine action of node N_i as a quantum channel $\Phi_i : \mathbb{C}^{d \times d} \mapsto \mathbb{C}^{2^q \times 2^q}$.
- N_c receives $\Phi_1(\rho), \dots, \Phi_m(\rho)$, and uses only these to solve the task.

A Helpful Perspective

- Suppose each node can send q qubits.
- Can imagine action of node N_i as a quantum channel $\Phi_i : \mathbb{C}^{d \times d} \mapsto \mathbb{C}^{2^q \times 2^q}$.
- N_c receives $\Phi_1(\rho), \dots, \Phi_m(\rho)$, and uses only these to solve the task.
- In the public-coin setting, each channel depends on the shared randomness.

A Helpful Perspective

- Suppose each node can send q qubits.
- Can imagine action of node N_i as a quantum channel $\Phi_i : \mathbb{C}^{d \times d} \mapsto \mathbb{C}^{2^q \times 2^q}$.
- N_c receives $\Phi_1(\rho), \dots, \Phi_m(\rho)$, and uses only these to solve the task.
- In the public-coin setting, each channel depends on the shared randomness.
- In the private-coin setting, each channel is independent.

Outline

Setup

Our Results

Upper Bound Ideas

Lower Bound Ideas

Future Directions

Public-Coin Bounds

Public-Coin Bounds

Theorem (Public-Coin Complexity)

In the public-coin setting with $q < \lceil \log_2(d) \rceil$ qubits of quantum communication per distributed node,

$$\mathcal{O}\left(\frac{d}{\epsilon^2} \cdot \frac{d}{2^q}\right) = \mathcal{O}\left(\frac{d^2}{2^q \epsilon^2}\right)$$

copies are sufficient for state certification.

Public-Coin Bounds

Theorem (Public-Coin Complexity)

In the public-coin setting with $q < \lceil \log_2(d) \rceil$ qubits of quantum communication per distributed node,

$$\mathcal{O}\left(\frac{d}{\epsilon^2} \cdot \frac{d}{2^q}\right) = \mathcal{O}\left(\frac{d^2}{2^q \epsilon^2}\right)$$

copies are sufficient for state certification. Moreover, if the channels used by the distributed nodes are mixedness preserving, then $\Omega\left(\frac{d^2}{2^q \epsilon^2}\right)$ copies are also necessary.

Public-Coin Bounds

Theorem (Public-Coin Complexity)

In the public-coin setting with $q < \lceil \log_2(d) \rceil$ qubits of quantum communication per distributed node,

$$\mathcal{O}\left(\frac{d}{\epsilon^2} \cdot \frac{d}{2^q}\right) = \mathcal{O}\left(\frac{d^2}{2^q \epsilon^2}\right)$$

copies are sufficient for state certification. Moreover, if the channels used by the distributed nodes are mixedness preserving, then $\Omega\left(\frac{d^2}{2^q \epsilon^2}\right)$ copies are also necessary.

- When $2^q \approx d$, we recover the $\mathcal{O}(d/\epsilon^2)$ centralized complexity.

[LA24]: Quantum State Testing with Restricted Measurements; Liu-Acharya 2024.

Public-Coin Bounds

Theorem (Public-Coin Complexity)

In the public-coin setting with $q < \lceil \log_2(d) \rceil$ qubits of quantum communication per distributed node,

$$\mathcal{O}\left(\frac{d}{\epsilon^2} \cdot \frac{d}{2^q}\right) = \mathcal{O}\left(\frac{d^2}{2^q \epsilon^2}\right)$$

copies are sufficient for state certification. Moreover, if the channels used by the distributed nodes are mixedness preserving, then $\Omega\left(\frac{d^2}{2^q \epsilon^2}\right)$ copies are also necessary.

- When $2^q \approx d$, we recover the $\mathcal{O}(d/\epsilon^2)$ centralized complexity.
- With only c classical bits, $\Theta\left(\frac{d^2}{2^{c/2} \epsilon^2}\right)$ copies are optimal [LA24].

[LA24]: Quantum State Testing with Restricted Measurements; Liu-Acharya 2024.

Private-Coin Bound

We also show that shared randomness is necessary to achieve the previous complexity:

Private-Coin Bound

We also show that shared randomness is necessary to achieve the previous complexity:

Theorem (Private-Coin Lower Bound)

In the private-coin setting with q -qubit communication, if the channels used by the distributed nodes are mixedness preserving, then

$$\Omega\left(\frac{d}{\epsilon^2} \cdot \left(\frac{d}{2^q}\right)^2\right) = \Omega\left(\frac{d^3}{4^q \epsilon^2}\right)$$

copies are necessary for state certification.

Private-Coin Bound

We also show that shared randomness is necessary to achieve the previous complexity:

Theorem (Private-Coin Lower Bound)

In the private-coin setting with q -qubit communication, if the channels used by the distributed nodes are mixedness preserving, then

$$\Omega\left(\frac{d}{\epsilon^2} \cdot \left(\frac{d}{2^q}\right)^2\right) = \Omega\left(\frac{d^3}{4^q \epsilon^2}\right)$$

copies are necessary for state certification.

- With only c classical bits and private randomness, $\Theta\left(\frac{d^3}{2^c \epsilon^2}\right)$ copies are optimal [LA24].

Outline

Setup

Our Results

Upper Bound Ideas

Lower Bound Ideas

Future Directions

Testing Algorithm

- No matter the choice of channels,
$$\|\Phi(\rho) - \Phi(\sigma)\|_1 \leq \|\rho - \sigma\|_1.$$

Testing Algorithm

- No matter the choice of channels,

$$\|\Phi(\rho) - \Phi(\sigma)\|_1 \leq \|\rho - \sigma\|_1.$$

- Can we quantify how much distance can be preserved? Similar to the JL-lemma or distortion bounds.

Testing Algorithm

- No matter the choice of channels,
$$\|\Phi(\rho) - \Phi(\sigma)\|_1 \leq \|\rho - \sigma\|_1.$$
- Can we quantify how much distance can be preserved? Similar to the JL-lemma or distortion bounds.
- Each node N_i will use a random channel Φ_U that satisfies

$$\|\Phi_U(\rho) - \Phi_U(\sigma)\|_2 \geq \frac{1}{2} \sqrt{\frac{2^q}{d}} \|\rho - \sigma\|_2$$

with constant probability.

Testing Algorithm

- No matter the choice of channels,

$$\|\Phi(\rho) - \Phi(\sigma)\|_1 \leq \|\rho - \sigma\|_1.$$

- Can we quantify how much distance can be preserved? Similar to the JL-lemma or distortion bounds.
- Each node N_i will use a random channel Φ_U that satisfies

$$\|\Phi_U(\rho) - \Phi_U(\sigma)\|_2 \geq \frac{1}{2} \sqrt{\frac{2^q}{d}} \|\rho - \sigma\|_2$$

with constant probability.

- N_c picks an appropriate parameter ϵ' and then applies the $\|\cdot\|_2$ -testing algorithm of [BOW19].
- Can achieve any desirable success probability $1 - \delta$ by repeating across $\mathcal{O}(\log(1/\delta))$ batches of nodes.

Compression Channel

Compression Channel

- Apply a random unitary $\mathbf{U} \sim U(d)$ to ρ .
- Trace out all but the first q qubits.

Compression Channel

- Apply a random unitary $\mathbf{U} \sim U(d)$ to ρ .
- Trace out all but the first q qubits.

$$\Phi_{\mathbf{U}}(\rho) = \text{tr}_B(\mathbf{U}\rho\mathbf{U}^\dagger).$$

Outline

Setup

Our Results

Upper Bound Ideas

Lower Bound Ideas

Future Directions

Lower Bounds via quantum χ^2 -divergence

Lower Bounds via quantum χ^2 -divergence

- To prove testing lower bounds, we will consider distinguishing between $\rho_{\text{mm}} \triangleq \frac{\mathbb{1}}{d}$ and $\rho \sim \mathcal{D}$.

Lower Bounds via quantum χ^2 -divergence

- To prove testing lower bounds, we will consider distinguishing between $\rho_{\text{mm}} \triangleq \frac{\mathbb{1}}{d}$ and $\rho \sim \mathcal{D}$.
- We will show that no matter the choice of $\Phi_1, \dots, \Phi_m$ implemented by $N_1, \dots, N_m$, the resulting states received by N_c are statistically indistinguishable, unless m is large.

Lower Bounds via quantum χ^2 -divergence

- To prove testing lower bounds, we will consider distinguishing between $\rho_{\text{mm}} \triangleq \frac{\mathbb{1}}{d}$ and $\rho \sim \mathcal{D}$.
- We will show that no matter the choice of $\Phi_1, \dots, \Phi_m$ implemented by $N_1, \dots, N_m$, the resulting states received by N_c are statistically indistinguishable, unless m is large.
- We want to show $\mathbb{E}_{\rho \sim \mathcal{D}} [\bigotimes_{i=1}^m \Phi_i(\rho)]$ and $\bigotimes_{i=1}^m \Phi_i(\rho_{\text{mm}})$ are close.

Lower Bounds via quantum χ^2 -divergence

- To prove testing lower bounds, we will consider distinguishing between $\rho_{\text{mm}} \triangleq \frac{\mathbb{1}}{d}$ and $\rho \sim \mathcal{D}$.
- We will show that no matter the choice of $\Phi_1, \dots, \Phi_m$ implemented by $N_1, \dots, N_m$, the resulting states received by N_c are statistically indistinguishable, unless m is large.
- We want to show $\mathbb{E}_{\rho \sim \mathcal{D}} [\bigotimes_{i=1}^m \Phi_i(\rho)]$ and $\bigotimes_{i=1}^m \Phi_i(\rho_{\text{mm}})$ are close.
- Use the “quantum Ingster-Suslina method” [[OW25](#)], which allows us to bound the quantum χ^2 -divergence between such states.

[[OW25](#)]: Instance-Optimal Quantum State Certification with Entangled Measurements; O’Donnell-W. 2025.

Lower Bounds via quantum χ^2 -divergence

- To prove testing lower bounds, we will consider distinguishing between $\rho_{\text{mm}} \triangleq \frac{\mathbb{1}}{d}$ and $\rho \sim \mathcal{D}$.
- We will show that no matter the choice of $\Phi_1, \dots, \Phi_m$ implemented by $N_1, \dots, N_m$, the resulting states received by N_c are statistically indistinguishable, unless m is large.
- We want to show $\mathbb{E}_{\rho \sim \mathcal{D}} [\bigotimes_{i=1}^m \Phi_i(\rho)]$ and $\bigotimes_{i=1}^m \Phi_i(\rho_{\text{mm}})$ are close.
- Use the “quantum Ingster-Suslina method” [OW25], which allows us to bound the quantum χ^2 -divergence between such states.
- This is enough to obtain the public-coin lower bound.
- For the private-coin lower bound, choose $\mathcal{D}$ adversarially based on the choice of $\Phi_1, \dots, \Phi_m$.

[OW25]: Instance-Optimal Quantum State Certification with Entangled Measurements; O’Donnell-W. 2025.

Outline

Setup

Our Results

Upper Bound Ideas

Lower Bound Ideas

Future Directions

Open questions within our model

Open questions within our model

- Is the private-coin lower bound optimal?

Open questions within our model

- Is the private-coin lower bound optimal?
- Can we remove the mixedness-preserving assumption from our lower bounds?

Open questions within our model

- Is the private-coin lower bound optimal?
- Can we remove the mixedness-preserving assumption from our lower bounds?
- What is the complexity of tomography in our setting?

Open questions within our model

- Is the private-coin lower bound optimal?
- Can we remove the mixedness-preserving assumption from our lower bounds?
- What is the complexity of tomography in our setting?
- Can we trade off classical and quantum communication?

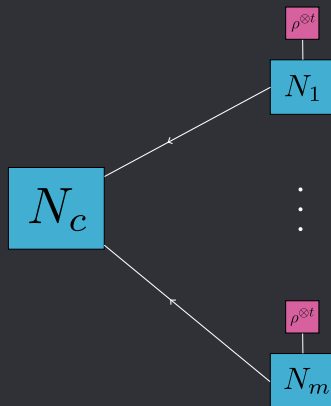
Open questions within our model

- Is the private-coin lower bound optimal?
- Can we remove the mixedness-preserving assumption from our lower bounds?
- What is the complexity of tomography in our setting?
- Can we trade off classical and quantum communication?

Extending our model

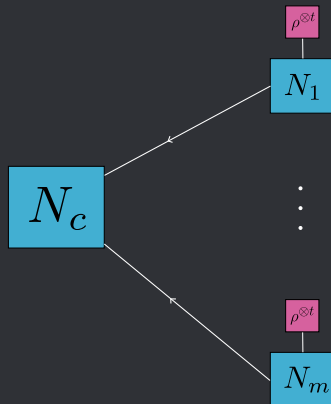
Extending our model

- What if each distributed node received $t > 1$ copies instead?



Extending our model

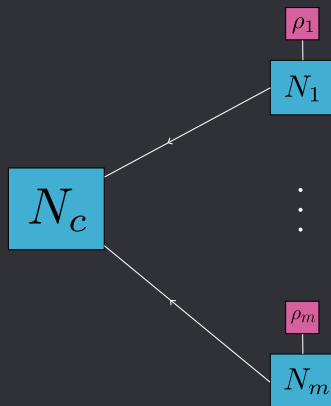
- What if each distributed node received $t > 1$ copies instead? This generalizes the centralized setting of [WC26].



[WC26]: Optimal Quantum State Testing Even with Limited Entanglement;
W.-Chen 2026.

Extending our model

- What if each distributed node received $t > 1$ copies instead? This generalizes the centralized setting of [WC26].
- What about the non-iid setting [DFMO25]? Here, we want to test the average of the m states.

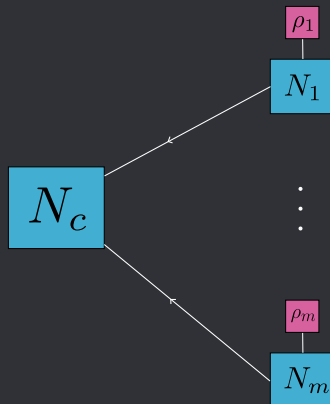


[WC26]: Optimal Quantum State Testing Even with Limited Entanglement; W.-Chen 2026.

[DFMO25]: Non-iid Hypothesis Testing: from Classical to Quantum; De Palma-Fanizza-Mowry-O'Donnell 2025.

Extending our model

- What if each distributed node received $t > 1$ copies instead? This generalizes the centralized setting of [WC26].
- What about the non-iid setting [DFMO25]? Here, we want to test the average of the m states.
- What if we allow interactivity? What if some of the nodes are adversarial?



Thank you! [arXiv:2604.05962](#)

[WC26]: Optimal Quantum State Testing Even with Limited Entanglement; W.-Chen 2026.

[DFMO25]: Non-iid Hypothesis Testing: from Classical to Quantum; De Palma-Fanizza-Mowry-O'Donnell 2025.