Optimal Verification of Two-Qubit Pure States

Kun Wang

Shenzhen Institute for Quantum Science and Engineering,
Southern University of Science and Technology

Joint work with Masahito HAYASHI

Phys. Rev. A **100**, 032315 (2019)

May 22, 2020

Outline

The state verification task

- Consider a quantum device $\mathcal{D}$ designed to produce a multipartite state $|\Psi\rangle$
- Practically, it may produce $\sigma_1, \cdots, \sigma_N$ in N uses satisfying *i.i.d.*
- It is guaranteed that $\mathcal{D}$ is in either of the following two cases

Good Case: $\sigma_i = |\Psi\rangle\langle\Psi|$ for all i;

Bad Case: For some fixed $\varepsilon > 0$, $\langle\Psi|\sigma_i|\Psi\rangle \leqslant 1 - \varepsilon$ for all i.

Task: to verify which is the case, using the device as less as possible

The state verification task

- Consider a quantum device $\mathcal{D}$ designed to produce a multipartite state $|\Psi\rangle$
- Practically, it may produce $\sigma_1, \cdots, \sigma_N$ in N uses satisfying *i.i.d.*
- It is guaranteed that $\mathcal{D}$ is in either of the following two cases

Good Case: $\sigma_i = |\Psi\rangle\langle\Psi|$ for all i;
Bad Case: For some fixed $\varepsilon > 0$, $\langle\Psi|\,\sigma_i\,|\Psi\rangle \leqslant 1 - \varepsilon$ for all i.

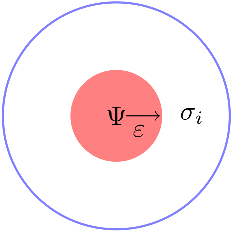
Task: to verify which is the case, using the device as less as possible

The state verification task

- Consider a quantum device $\mathcal{D}$ designed to produce a multipartite state $|\Psi\rangle$
- Practically, it may produce $\sigma_1, \cdots, \sigma_N$ in N uses satisfying *i.i.d.*
- It is guaranteed that $\mathcal{D}$ is in either of the following two cases

  Good Case: $\sigma_i = |\Psi\rangle\langle\Psi|$ for all i;

  Bad Case: For some fixed $\varepsilon > 0$, $\langle\Psi|\, \sigma_i \,|\Psi\rangle \leqslant 1 - \varepsilon$ for all i.



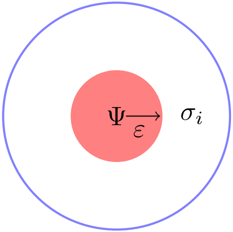
Task: to verify which is the case, using the device as less as possible

The state verification task

- Consider a quantum device $\mathcal{D}$ designed to produce a multipartite state $|\Psi\rangle$
- Practically, it may produce $\sigma_1, \cdots, \sigma_N$ in N uses satisfying *i.i.d.*
- It is guaranteed that $\mathcal{D}$ is in either of the following two cases

  Good Case: $\sigma_i = |\Psi\rangle\langle\Psi|$ for all i;

  Bad Case: For some fixed $\varepsilon > 0$, $\langle\Psi|\,\sigma_i\,|\Psi\rangle \leqslant 1 - \varepsilon$ for all i.



Task: to verify which is the case, using the device as less as possible

General strategy

- The verifier has access to a set of available measurements $\mathfrak{M}$
- For each output σ_i, he performs a binary measurement $\{T_l, \mathbb{1} - T_l\}$, chosen randomly from $\mathfrak{M}$
- Commonly, we use T_l to represent the binary measurement
- We require that $T_l \left|\Psi\right\rangle = \left|\Psi\right\rangle$
  - the measurement detects the **Good Case** with certainty
  - Reasonable since we avoid misclassifying good as bad
- Measure σ_i with T_l:
  - If $\mathbb{1} - T_l$ ticks, concludes the device is in **Bad Case**
  - If T_l ticks, continues to test next state

$$\begin{array}{ccc} & \sigma_i & \\ \swarrow & & \searrow \\ \mathbb{1}-T_l & & T_l \\ \downarrow & & \downarrow \\ \text{bad case} & & ? \end{array}$$

	Good Case	**Bad Case**
T_l	✓	✗
$\mathbb{1} - T_l$	impossible	✓

- Need to minimize the probability of event "✗"

General strategy

- The verifier has access to a set of available measurements $\mathfrak{M}$
- For each output σ_i, he performs a binary measurement $\{T_l, \mathbb{1} - T_l\}$, chosen randomly from $\mathfrak{M}$
- Commonly, we use T_l to represent the binary measurement
- We require that $T_l \left|\Psi\right\rangle = \left|\Psi\right\rangle$
  - the measurement detects the **Good Case** with certainty
  - Reasonable since we avoid misclassifying good as bad
- Measure σ_i with T_l:
  - If $\mathbb{1} - T_l$ ticks, concludes the device is in **Bad Case**
  - If T_l ticks, continues to test next state

$$\begin{tikzcd} & \sigma_i \arrow[dl] \arrow[dr] & \\ \mathbb{1} - T_l \arrow[d] & & T_l \arrow[d] \\ \text{bad case} & & ? \end{tikzcd}$$

	Good Case	**Bad Case**
T_l	✓	✗
$\mathbb{1} - T_l$	impossible	✓

- Need to minimize the probability of event "✗"

General strategy

- The verifier has access to a set of available measurements $\mathfrak{M}$
- For each output σ_i, he performs a binary measurement $\{T_l, \mathbb{1} - T_l\}$, chosen randomly from $\mathfrak{M}$
- Commonly, we use T_l to represent the binary measurement
- We require that $T_l \left|\Psi\right\rangle = \left|\Psi\right\rangle$
  - the measurement detects the **Good Case** with certainty
  - Reasonable since we avoid misclassifying good as bad
- Measure σ_i with T_l:
  - If $\mathbb{1} - T_l$ ticks, concludes the device is in **Bad Case**
  - If T_l ticks, continues to test next state

$$\begin{tikzcd} & \sigma_i \arrow[dl] \arrow[dr] & \\ \mathbb{1} - T_l \arrow[d] & & T_l \arrow[d] \\ \text{bad case} & & ? \end{tikzcd}$$

	Good Case	**Bad Case**
T_l	✓	✗
$\mathbb{1} - T_l$	impossible	✓

- Need to minimize the probability of event "✗"

General strategy

- The verifier has access to a set of available measurements $\mathfrak{M}$
- For each output σ_i, he performs a binary measurement $\{T_l, \mathbb{1} - T_l\}$, chosen randomly from $\mathfrak{M}$
- Commonly, we use T_l to represent the binary measurement
- We require that $T_l \left|\Psi\right\rangle = \left|\Psi\right\rangle$
  - the measurement detects the **Good Case** with certainty
  - Reasonable since we avoid misclassifying good as bad
- Measure σ_i with T_l:
  - If $\mathbb{1} - T_l$ ticks, concludes the device is in **Bad Case**
  - If T_l ticks, continues to test next state

$$\begin{tikzcd} & \sigma_i \arrow[dl] \arrow[dr] & \\ \mathbb{1} - T_l \arrow[d] & & T_l \arrow[d] \\ \text{bad case} & & ? \end{tikzcd}$$

	Good Case	**Bad Case**
T_l	✓	✗
$\mathbb{1} - T_l$	impossible	✓

- Need to minimize the probability of event "✗"

General strategy

- The verifier has access to a set of available measurements $\mathfrak{M}$
- For each output σ_i, he performs a binary measurement $\{T_l, \mathbb{1} - T_l\}$, chosen randomly from $\mathfrak{M}$
- Commonly, we use T_l to represent the binary measurement
- We require that $T_l \left|\Psi\right\rangle = \left|\Psi\right\rangle$
  - the measurement detects the **Good Case** with certainty
  - Reasonable since we avoid misclassifying good as bad
- Measure σ_i with T_l:
  - If $\mathbb{1} - T_l$ ticks, concludes the device is in **Bad Case**
  - If T_l ticks, continues to test next state

$$\begin{array}{ccc} & \sigma_i & \\ \swarrow & & \searrow \\ \mathbb{1} - T_l & & T_l \\ \downarrow & & \downarrow \\ \text{bad case} & & ? \end{array}$$

	Good Case	**Bad Case**
T_l	✓	✗
$\mathbb{1} - T_l$	impossible	✓

- Need to minimize the probability of event "✗"

General strategy

- The verifier has access to a set of available measurements $\mathfrak{M}$
- For each output σ_i, he performs a binary measurement $\{T_l, \mathbb{1} - T_l\}$, chosen randomly from $\mathfrak{M}$
- Commonly, we use T_l to represent the binary measurement
- We require that $T_l |\Psi\rangle = |\Psi\rangle$
  - the measurement detects the **Good Case** with certainty
  - Reasonable since we avoid misclassifying good as bad
- Measure σ_i with T_l:
  - If $\mathbb{1} - T_l$ ticks, concludes the device is in **Bad Case**
  - If T_l ticks, continues to test next state

$$\begin{array}{ccc} & \sigma_i & \\ \mathbb{1} - T_l & & T_l \\ \downarrow & & \downarrow \\ \text{bad case} & & ? \end{array}$$

	Good Case	**Bad Case**
T_l	✓	✗
$\mathbb{1} - T_l$	impossible	✓

- Need to minimize the probability of event "✗"

General strategy (cont.)

Algorithm 1: Quantum state verification framework

Input: a sequence of states σ_i

Output: the device is in "good case" or "bad case"

for $i = 1$ **to** N **do**

    Choose randomly $\{T_l, \mathbb{1} - T_l\}$ from $\mathfrak{M}$ satisfying $T_l \left|\Psi\right\rangle = \left|\Psi\right\rangle$

    Perform the measurement on σ_i

    if $\mathbb{1} - T_l$ *is returned* **then**

        Output the device is in "bad case"

    end

end

Output the device is in "good case"

Accepting probability

- $\Omega = \sum_l p_l T_l$ is called a *strategy*
- What's the largest probability of event ✗?

$$\begin{aligned} \Pr\{✗\} &\leqslant \max_{\langle\Psi|\sigma|\Psi\rangle \leqslant 1-\varepsilon} \sum_l p_l \operatorname{Tr}[T_l \sigma] \\ &= \max_{\langle\Psi|\sigma|\Psi\rangle \leqslant 1-\varepsilon} \operatorname{Tr}[\Omega\sigma] \\ &= 1 - [1 - \lambda_2^{\downarrow}(\Omega)]\varepsilon, \end{aligned}$$

where $\lambda_2^{\downarrow}(\Omega)$ is the second largest eigenvalue of Ω[1]

- This is the probability that a fake state σ is wrongly accepted
- To achieve a given confidence δ, we require

$$\underbrace{\Big(1 - [1 - \lambda_2^{\downarrow}(\Omega)]\varepsilon\Big)^N}_{\textit{the device is accepted for } N \textit{ tests}} \leqslant \delta \quad \Rightarrow \quad N \geqslant \frac{1}{[1 - \lambda_2^{\downarrow}(\Omega)]\varepsilon} \log \frac{1}{\delta}$$

[1] S. Pallister *et al.*, *PRL* (2018), H. Zhu, M. Hayashi, *PRL* (2019).

Optimization task

Minimize the second largest eigenvalue w.r.t. available measurements

$$\begin{aligned} \min \quad & \lambda_2^{\downarrow}(\Omega) \\ \mathrm{s.\,t.} \quad & \Omega = \sum_l p_l T_l,\ T_l \left|\Psi\right\rangle = \left|\Psi\right\rangle \\ & \sum_l p_l = 1,\ p_l \geqslant 0 \\ & \{T_l, \mathbb{1} - T_l\} \in \mathfrak{M} \end{aligned}$$

Experimentally motivated measurements $\mathfrak{M}$:

LO: local operations; **LOCC**: local operations and classical communication; **SEP**: separable measurements

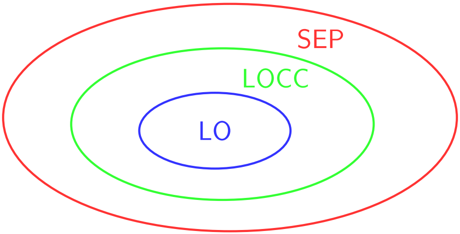
Optimization task

Minimize the second largest eigenvalue w.r.t. available measurements

$$
\begin{aligned}
\min \quad & \lambda_2^{\downarrow}(\Omega) \\
\text{s.t.} \quad & \Omega = \sum_l p_l T_l,\ T_l \left|\Psi\right\rangle = \left|\Psi\right\rangle \\
& \sum_l p_l = 1,\ p_l \geqslant 0 \\
& \{T_l, \mathbb{1} - T_l\} \in \mathfrak{M}
\end{aligned}
$$

Experimentally motivated measurements $\mathfrak{M}$:

LO: local operations; **LOCC**: local operations and classical communication; **SEP**: separable measurements



Outline

Two-qubit pure state verification

- We aim to verify the two-qubit pure state Ψ of the form

$$|\Psi\rangle = \sqrt{1-\lambda}\,|00\rangle + \sqrt{\lambda}\,|11\rangle\,,\ \lambda \in (0, 1/2)$$

- Any two-qubit pure state is locally equivalent to $|\Psi\rangle$

Known results

- The maximally entangled state case ($\lambda = 1/2$) is solved in[2]
- The product state case ($\lambda = 0$) is trivial
- The locally projective measurement case is solved in[3]
- The global measurement case is trivial[3]

Our results

- We solve this problem completely by deriving *optimal* strategies for
  1. Local operations and one-way classical communication (one-way LOCC);
  2. Local operations and two-way classical communication (two-way LOCC); and
  3. Separable measurements.

[2] M. Owari, M. Hayashi, *NJP* (2008).

[3] S. Pallister *et al.*, *PRL* (2018).

Two-qubit pure state verification

- We aim to verify the two-qubit pure state Ψ of the form

$$|\Psi\rangle = \sqrt{1-\lambda}\,|00\rangle + \sqrt{\lambda}\,|11\rangle\,,\ \lambda \in (0, 1/2)$$

- Any two-qubit pure state is locally equivalent to $|\Psi\rangle$

Known results

- The maximally entangled state case ($\lambda = 1/2$) is solved in[2]
- The product state case ($\lambda = 0$) is trivial
- The locally projective measurement case is solved in[3]
- The global measurement case is trivial[3]

Our results

- We solve this problem completely by deriving *optimal* strategies for
  1. Local operations and one-way classical communication (one-way LOCC);
  2. Local operations and two-way classical communication (two-way LOCC); and
  3. Separable measurements.

[2] M. Owari, M. Hayashi, *NJP* (2008).

[3] S. Pallister *et al.*, *PRL* (2018).

Two-qubit pure state verification

- We aim to verify the two-qubit pure state Ψ of the form

$$|\Psi\rangle = \sqrt{1-\lambda}\,|00\rangle + \sqrt{\lambda}\,|11\rangle\,,\ \lambda \in (0, 1/2)$$

- Any two-qubit pure state is locally equivalent to $|\Psi\rangle$

Known results

- The maximally entangled state case ($\lambda = 1/2$) is solved in[2]
- The product state case ($\lambda = 0$) is trivial
- The locally projective measurement case is solved in[3]
- The global measurement case is trivial[3]

Our results

- We solve this problem completely by deriving *optimal* strategies for
  1. Local operations and one-way classical communication (one-way LOCC);
  2. Local operations and two-way classical communication (two-way LOCC); and
  3. Separable measurements.

[2] M. Owari, M. Hayashi, *NJP* (2008).

[3] S. Pallister *et al.*, *PRL* (2018).

Optimal strategy using one-way LOCC measurements

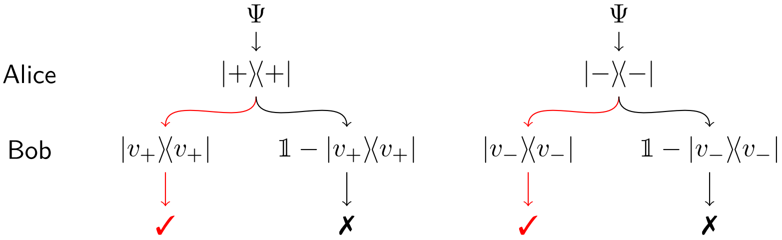
One-way LOCC measurements

Step 1. Alice performs the X measurement and sends $i \in \{0, 1\}$ to Bob

Step 2. Conditioning on i, Bob does the following

- If $i = 0$, he performs the measurement $|v_+\rangle\langle v_+|$;
- If $i = 1$, he performs the measurement $|v_-\rangle\langle v_-|$, where

$$|v_\pm\rangle := \sqrt{1-\lambda}\,|0\rangle \pm \sqrt{\lambda}\,|1\rangle$$



- Denote this measurement by T_x, then

$$T_x = |+\rangle\langle+| \otimes |v_+\rangle\langle v_+| + |-\rangle\langle-| \otimes |v_-\rangle\langle v_-|$$

- Substituting X with Y and Z, we get T_y and T_z, respectively

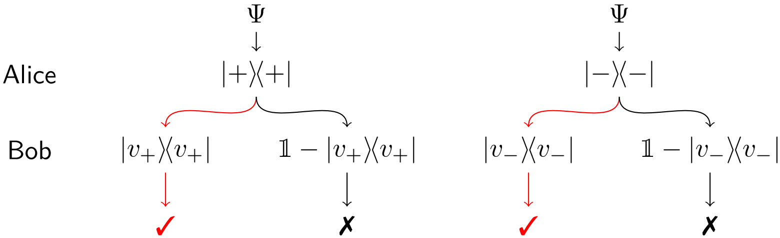
One-way LOCC measurements

Step 1. Alice performs the X measurement and sends $i \in \{0, 1\}$ to Bob

Step 2. Conditioning on i, Bob does the following

- If $i = 0$, he performs the measurement $|v_+\rangle\langle v_+|$;
- If $i = 1$, he performs the measurement $|v_-\rangle\langle v_-|$, where

$$|v_\pm\rangle := \sqrt{1-\lambda}\,|0\rangle \pm \sqrt{\lambda}\,|1\rangle$$



- Denote this measurement by T_x, then

$$T_x = |+\rangle\langle +| \otimes |v_+\rangle\langle v_+| + |-\rangle\langle -| \otimes |v_-\rangle\langle v_-|$$

- Substituting X with Y and Z, we get T_y and T_z, respectively

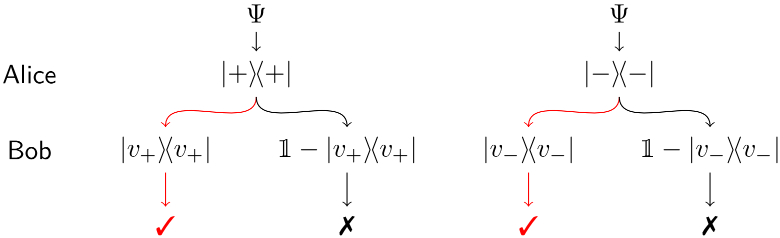
One-way LOCC measurements

Step 1. Alice performs the X measurement and sends $i \in \{0,1\}$ to Bob

Step 2. Conditioning on i, Bob does the following

- If $i = 0$, he performs the measurement $|v_+\rangle\langle v_+|$;
- If $i = 1$, he performs the measurement $|v_-\rangle\langle v_-|$, where

$$|v_\pm\rangle := \sqrt{1-\lambda}\,|0\rangle \pm \sqrt{\lambda}\,|1\rangle$$



- Denote this measurement by T_x, then

$$T_x = |+\rangle\langle +| \otimes |v_+\rangle\langle v_+| + |-\rangle\langle -| \otimes |v_-\rangle\langle v_-|$$

- Substituting X with Y and Z, we get T_y and T_z, respectively

An one-way strategy

- Let $p := \frac{1-\lambda}{2-\lambda}$. In each round, Alice chooses a measurement from

$$\{T_x, T_y, T_z\}$$

  with *a priori* probability $\{\frac{1-p}{2}, \frac{1-p}{2}, p\}$ to test the state
- The strategy has the form

$$\begin{aligned}\Omega_{\rightarrow} &= \frac{1-p}{2} T_x + \frac{1-p}{2} T_y + p T_z \\ &= |\Psi\rangle\langle\Psi| + \frac{1-\lambda}{2-\lambda} |\Psi^+\rangle\langle\Psi^+| + \frac{\lambda}{2-\lambda} \left(|01\rangle\langle 01| + |10\rangle\langle 10|\right)\end{aligned}$$

Optimality of $\Omega_{\rightarrow}$

$$\Psi \to |t,s\rangle \to \begin{cases} |t,s,B\rangle \to ✓ \\ \mathbb{1} - |t,s,B\rangle \to ✗ \end{cases}$$

- Let $|t,s\rangle := \sqrt{t}\,|0\rangle + e^{is}\sqrt{1-t}\,|1\rangle$
- The most general one-way LOCC strategy

$$\Omega = 2\int \underbrace{|t,s\rangle\langle t,s|}_{\text{Alice's outcome}} \otimes \underbrace{|t,s,B\rangle\langle t,s,B|}_{\text{Bob's measurement conditioned on the outcome}} P_{TS}(dtds)$$

where $|t,s,B\rangle := \sqrt{t(1-\lambda)}\,|0\rangle + e^{-is}\,|(1-t)\lambda\rangle\,|1\rangle$

- Alice's operation must be a POVM, imposing the constraint

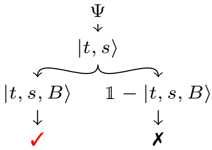
$$2\int |t,s\rangle\langle t,s| P_{TS}(dtds) = \mathbb{1} \quad \Rightarrow \quad \mathbb{E}_T[T] = \frac{1}{2}$$

- Applying the averaging technique, the eigenvalues of Ω can be computed

$$\lambda_2(\Omega) = 1 - \Xi,\ \lambda_3(\Omega) = \Xi(1-\lambda),\ \lambda_4(\Omega) = \Xi\lambda,\ \Xi := 2\mathbb{E}_T \frac{T(1-T)}{T+\lambda-2\lambda T}$$

- $\lambda_2^{\downarrow}(\Omega)$ is achieved when $\lambda_2(\Omega) = \lambda_3(\Omega)$, resulting $\lambda_2^{\downarrow}(\Omega) = \frac{1-\lambda}{2-\lambda}$

Optimality of $\Omega_{\rightarrow}$



- Let $|t, s\rangle := \sqrt{t}\,|0\rangle + e^{is}\sqrt{1-t}\,|1\rangle$
- The most general one-way LOCC strategy

$$\Omega = 2\int \underbrace{|t, s\rangle\langle t, s|}_{\text{Alice's outcome}} \otimes \underbrace{|t, s, B\rangle\langle t, s, B|}_{\text{Bob's measurement conditioned on the outcome}} P_{TS}(dtds)$$

where $|t, s, B\rangle := \sqrt{t(1-\lambda)}\,|0\rangle + e^{-is}\,|(1-t)\lambda\rangle\,|1\rangle$

- Alice's operation must be a POVM, imposing the constraint

$$2\int |t, s\rangle\langle t, s| P_{TS}(dtds) = \mathbb{1} \quad \Rightarrow \quad \mathbb{E}_T[T] = \frac{1}{2}$$

- Applying the averaging technique, the eigenvalues of Ω can be computed

$$\lambda_2(\Omega) = 1 - \Xi,\ \lambda_3(\Omega) = \Xi(1-\lambda),\ \lambda_4(\Omega) = \Xi\lambda,\ \Xi := 2\mathbb{E}_T\frac{T(1-T)}{T + \lambda - 2\lambda T}$$

- $\lambda_2^{\downarrow}(\Omega)$ is achieved when $\lambda_2(\Omega) = \lambda_3(\Omega)$, resulting $\lambda_2^{\downarrow}(\Omega) = \frac{1-\lambda}{2-\lambda}$

Optimality of $\Omega_{\rightarrow}$

$$\begin{tikzcd} & \Psi \arrow[d] & \\ & |t,s\rangle \arrow[dl] \arrow[dr] & \\ |t,s,B\rangle \arrow[d] & & \mathbb{1} - |t,s,B\rangle \arrow[d] \\ \checkmark & & \text{✗} \end{tikzcd}$$

- Let $|t,s\rangle := \sqrt{t}\,|0\rangle + e^{is}\sqrt{1-t}\,|1\rangle$
- The most general one-way LOCC strategy

$$\Omega = 2\int \underbrace{|t,s\rangle\langle t,s|}_{\text{Alice's outcome}} \otimes \underbrace{|t,s,B\rangle\langle t,s,B|}_{\text{Bob's measurement conditioned on the outcome}} P_{TS}(dtds)$$

where $|t,s,B\rangle := \sqrt{t(1-\lambda)}\,|0\rangle + e^{-is}\,|(1-t)\lambda\rangle\,|1\rangle$

- Alice's operation must be a POVM, imposing the constraint

$$2\int |t,s\rangle\langle t,s| P_{TS}(dtds) = \mathbb{1} \quad \Rightarrow \quad \mathbb{E}_T[T] = \frac{1}{2}$$

- Applying the averaging technique, the eigenvalues of Ω can be computed

$$\lambda_2(\Omega) = 1 - \Xi,\ \lambda_3(\Omega) = \Xi(1-\lambda),\ \lambda_4(\Omega) = \Xi\lambda,\ \Xi := 2\mathbb{E}_T\frac{T(1-T)}{T+\lambda-2\lambda T}$$

- $\lambda_2^{\downarrow}(\Omega)$ is achieved when $\lambda_2(\Omega) = \lambda_3(\Omega)$, resulting $\lambda_2^{\downarrow}(\Omega) = \frac{1-\lambda}{2-\lambda}$

Optimality of $\Omega_{\rightarrow}$

$$\begin{array}{ccc} & \Psi & \\ & \downarrow & \\ & |t,s\rangle & \\ \swarrow & & \searrow \\ |t,s,B\rangle & & \mathbb{1} - |t,s,B\rangle \\ \downarrow & & \downarrow \\ \checkmark & & \times \end{array}$$

- Let $|t,s\rangle := \sqrt{t}\,|0\rangle + e^{is}\sqrt{1-t}\,|1\rangle$
- The most general one-way LOCC strategy

$$\Omega = 2\int \underbrace{|t,s\rangle\langle t,s|}_{\text{Alice's outcome}} \otimes \underbrace{|t,s,B\rangle\langle t,s,B|}_{\text{Bob's measurement conditioned on the outcome}} P_{TS}(dtds)$$

where $|t,s,B\rangle := \sqrt{t(1-\lambda)}\,|0\rangle + e^{-is}\,|(1-t)\lambda\rangle\,|1\rangle$

- Alice's operation must be a POVM, imposing the constraint

$$2\int |t,s\rangle\langle t,s| P_{TS}(dtds) = \mathbb{1} \quad \Rightarrow \quad \mathbb{E}_T[T] = \frac{1}{2}$$

- Applying the averaging technique, the eigenvalues of Ω can be computed

$$\lambda_2(\Omega) = 1 - \Xi,\ \lambda_3(\Omega) = \Xi(1-\lambda),\ \lambda_4(\Omega) = \Xi\lambda,\ \Xi := 2\mathbb{E}_T\frac{T(1-T)}{T+\lambda-2\lambda T}$$

- $\lambda_2^{\downarrow}(\Omega)$ is achieved when $\lambda_2(\Omega) = \lambda_3(\Omega)$, resulting $\lambda_2^{\downarrow}(\Omega) = \frac{1-\lambda}{2-\lambda}$

Optimal strategy using two-way LOCC measurements

A two-way LOCC measurement

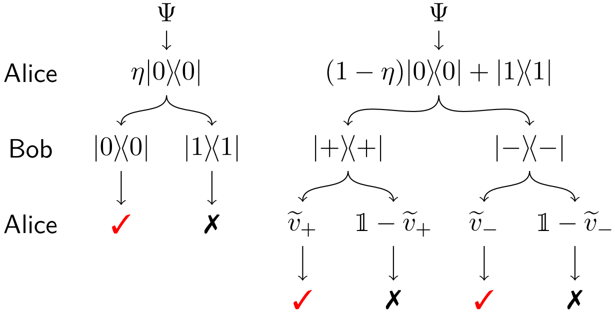
Step 1. Alice performs measurement $\eta|0\rangle\langle 0|$ and sends outcome i to Bob

Step 2. Conditioning on i, Bob does the following

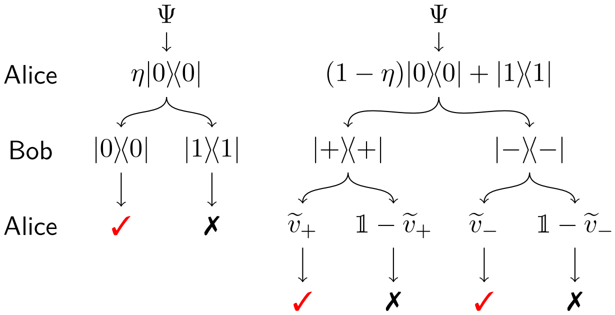
- If $i = 0$, performs Z measurement and accepts if outcome is 0
- If $i = 1$, performs X measurement and sends outcome j to Alice

Step 3. Conditioning on j, Alice does the following

- If $j = 0$, performs $\widetilde{v}_+$ and accepts if outcome is $\widetilde{v}_+$
- If $j = 1$, performs $\widetilde{v}_-$ and accepts if outcome is $\widetilde{v}_-$



A two-way LOCC measurement (cont.)



- Denote this measurement by $T_x^{A\to B}$, then

$$T_x^{A\to B} = \eta|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |\widetilde{v}_+\rangle\langle\widetilde{v}_+| \otimes |+\rangle\langle +| + |\widetilde{v}_-\rangle\langle\widetilde{v}_-| \otimes |-\rangle\langle -|$$

- Switching the role between Alice and Bob, we get $T_x^{B\to A}$
- Substituting X with Y and Z, we get $T_y^{A\to B/B\to A}$ and $T_z^{A\to B/B\to A}$

A two-way strategy

- Let $\eta := 1 - \sqrt{\frac{\lambda}{1-\lambda}}$ and $p := \frac{\lambda}{1+\sqrt{\lambda(1-\lambda)}}$
- In each round, Alice chooses a measurement from

$$\{T_x^{A\to B}, T_x^{B\to A}, T_y^{A\to B}, T_y^{B\to A}, T_z\}$$

  with *a priori* probability $\{\frac{1-p}{4}, \frac{1-p}{4}, \frac{1-p}{4}, \frac{1-p}{4}, p\}$ to test the state
- The strategy has the form

$$\begin{aligned}\Omega_{\leftrightarrow} &= \frac{1-p}{4}\left(T_x^{A\to B} + T_x^{B\to A} + T_y^{A\to B} + T_y^{B\to A}\right) + pT_z \\ &= |\Psi\rangle\langle\Psi| + \frac{\sqrt{\lambda(1-\lambda)}}{1+\sqrt{\lambda(1-\lambda)}}\left(\mathbb{1} - |\Psi\rangle\langle\Psi|\right)\end{aligned}$$

- This strategy uses up-to three step classical communication
- We prove its optimality by showing that it is optimal even if separable measurements are allowed

Optimal strategy using separable measurements

Optimal strategy is always homogeneous

- A strategy Ω is *homogeneous* if it has the form[4]

$$\Omega = |\Psi\rangle\langle\Psi| + \eta\,(\mathbb{1} - |\Psi\rangle\langle\Psi|)$$

- Our constructed strategy $\Omega_{\leftrightarrow}$ is homogeneous, but $\Omega_{\rightarrow}$ is not
- We show the following[5]

Lemma 1.

The optimal separable strategy is always homogeneous.

[4] H. Zhu, M. Hayashi, *PRL* (2019).

[5] K. Wang, M. Hayashi, *PRA* (2019).

Optimal homogeneous strategy

- We are interested in the optimization problem

$$\begin{aligned} \min \quad & \eta \\ \text{s.t.} \quad & \Omega = |\Psi\rangle\langle\Psi| + \eta\,(\mathbb{1} - |\Psi\rangle\langle\Psi|) \\ & \Omega \text{ is a separable operator} \end{aligned}$$

- Separability is equivalent to the positive partial transpose for 2×2 space[6]

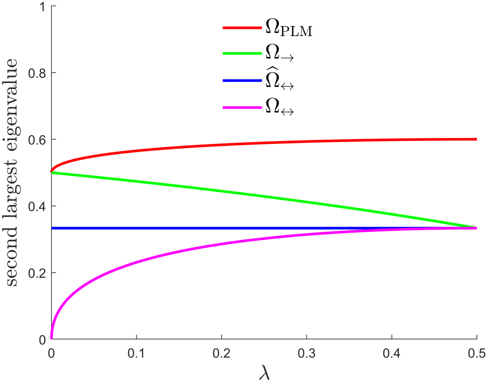
$$\begin{aligned} \Omega \text{ is a separable operator } &\Leftrightarrow \Omega^{T_B} \geqslant 0 \\ &\Leftrightarrow \lambda_4(\Omega) = \eta - (1-\eta)\sqrt{\lambda(1-\lambda)} \geqslant 0 \\ &\Leftrightarrow \eta \geqslant \eta_{\text{sep}} = \frac{\sqrt{\lambda(1-\lambda)}}{1+\sqrt{\lambda(1-\lambda)}} \end{aligned}$$

- The optimal homogeneous separable strategy satisfies

$$\Omega_{\text{sep}} = |\Psi\rangle\langle\Psi| + \eta_{\text{sep}}\,(\mathbb{1} - |\Psi\rangle\langle\Psi|) = \Omega_{\leftrightarrow}$$

[6] E. Størmer, *Acta Mathematica* (1963), S. L. Woronowicz, *Reports on Mathematical Physics* (1976).

Comparison of the strategies



- Our proposed strategies witness the power of *adaptivity*: allowing classical communication remarkably improves the verification efficiency
- Up to three steps of communication is enough to achieve optimality

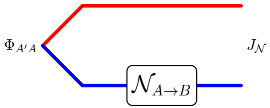
Outline

Notions on quantum channels

- A quantum channel $\mathcal{N}_{A\to B}$ maps quantum states to quantum states
- Quantum gates (unitary channels) are those of the form $\mathcal{U} \equiv U(\cdot)U^\dagger$
- Choi isomorphism[7]: there exists an one-one mapping between quantum channels and quantum states, via

$$J_{\mathcal{N}} := (\mathrm{id}_{A'} \otimes \mathcal{N}_{A\to B}) \left|\Phi\right\rangle_{A'A},$$
$$\mathcal{N}(\rho) := d\,\mathrm{Tr}_A\left[(\rho^T \otimes \mathbb{1}_B) J_{\mathcal{N}}\right].$$

$\Phi_{A'A}$ the maximally entangled state; $J_{\mathcal{N}}$ the (bipartite) Choi state



- Average gate fidelity between two quantum channels:

$$F_A(\mathcal{N},\mathcal{U}) := \int_\psi \mathrm{Tr}\left[\mathcal{N}(|\psi\rangle\langle\psi|)\mathcal{U}(|\psi\rangle\langle\psi|)\right] d\psi$$

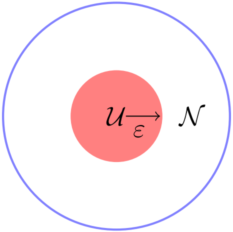
[7] M.-D. Choi, *Linear algebra and Its Applications* (1975).

The quantum gate verification task

- Consider a quantum device $\mathcal{D}$ designed to implement a unitary $\mathcal{U}$
- Practically, it may realize an unknown channel $\mathcal{N}$
- It is guaranteed that $\mathcal{D}$ is in either of the following two cases

  Good Case: implements the unitary gate $\mathcal{U}$;

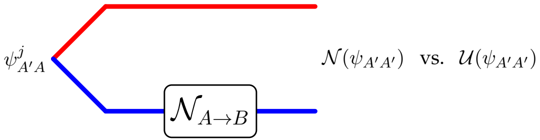
  Bad Case: implements the channel $\mathcal{N}$ st $F_A(\mathcal{N},\mathcal{U}) \leqslant 1 - \varepsilon$



Task: to verify which is the case, using the device as less as possible

From gate verification to state verification: Method I

- The verifier prepares a set of bipartite pure test states $\{p_j, |\psi^j_{A'A}\rangle\}$ as inputs



- Quantum state verification between $\mathcal{U}(\psi^j)$ or $\{\mathcal{N}(\psi^j)\}$
- However, pure bipartite quantum state preparation is difficult!

From gate verification to state verification: Method II

- The verifier prepares a set of test states $\{p_j, \rho_j\}$ as inputs

$$\rho_j \longrightarrow \boxed{\mathcal{N}_{A\to B}} \longrightarrow \mathcal{N}(\rho_j) \;\text{ vs. }\; \mathcal{U}(\rho_j)$$

- For each ρ_j, prepares a binary measurement $\{T_j, \mathbb{1} - T_j\}$
- We require T_j always identify the good case: $\operatorname{Tr}[T_j \mathcal{U}(\rho_j)] = 1$

	Good Case	**Bad Case**
T_l	✓	✗
$\mathbb{1} - T_l$	impossible	✓

- What's the probability of event ✗[8]?

$$\Pr\{✗\} = \sum_j p_j \operatorname{Tr}[T_j \mathcal{N}(\rho_j)] \equiv \operatorname{Tr}[\Omega J_{\mathcal{N}}], \quad \Omega := d \sum_j p_j \left(\rho_j^T \otimes T_j\right)$$

- Equivalent to quantum state verification of $J_{\mathcal{U}}$

Target: Minimize $\Pr\{✗\}$ – equivalent to finding optimal Ω

[8] H. Zhu, H. Zhang, *PRA* (2020), Y.-C. Liu *et al.*, *PRA* (2020).

Outline

Concluding remarks

- What we have done?
  1. Studied the two-qubit pure state verification problem comprehensively
  2. Obtained optimal strategies for each available class of measurements

- What we have learnt?
  1. Mutually unbiased bases play an important role in state verification
  2. They can extract much more information
  3. Classical communication helps a lot

- What to do next?
  1. Optimal/efficient strategies for verifying high-dimensional pure states[9]
  2. Quantum measurement/channel verification[10]
  3. Experimental verification[11]

[9] X.-D. Yu *et al.*, *npjQI* (2019), Z. Li *et al.*, *PRA* (2019), Y.-C. Liu *et al.*, *PRApplied* (2019).
[10] P. Sekatski *et al.*, *PRL* (2018), J.-D. Bancal *et al.*, *PRL* (2018).
[11] W.-H. Zhang *et al.*, *arXiv:1905.12175* (2019), X. Jiang *et al.*, *arXiv:2002.00640* (2020).

Concluding remarks

- What we have done?
  1. Studied the two-qubit pure state verification problem comprehensively
  2. Obtained optimal strategies for each available class of measurements

- What we have learnt?
  1. Mutually unbiased bases play an important role in state verification
  2. They can extract much more information
  3. Classical communication helps a lot

- What to do next?
  1. Optimal/efficient strategies for verifying high-dimensional pure states[9]
  2. Quantum measurement/channel verification[10]
  3. Experimental verification[11]

[9] X.-D. Yu *et al.*, *npjQI* (2019), Z. Li *et al.*, *PRA* (2019), Y.-C. Liu *et al.*, *PRApplied* (2019).
[10] P. Sekatski *et al.*, *PRL* (2018), J.-D. Bancal *et al.*, *PRL* (2018).
[11] W.-H. Zhang *et al.*, *arXiv:1905.12175* (2019), X. Jiang *et al.*, *arXiv:2002.00640* (2020).

Concluding remarks

- What we have done?
  1. Studied the two-qubit pure state verification problem comprehensively
  2. Obtained optimal strategies for each available class of measurements

- What we have learnt?
  1. Mutually unbiased bases play an important role in state verification
  2. They can extract much more information
  3. Classical communication helps a lot

- What to do next?
  1. Optimal/efficient strategies for verifying high-dimensional pure states[9]
  2. Quantum measurement/channel verification[10]
  3. Experimental verification[11]

[9] X.-D. Yu *et al.*, *npjQI* (2019), Z. Li *et al.*, *PRA* (2019), Y.-C. Liu *et al.*, *PRApplied* (2019).

[10] P. Sekatski *et al.*, *PRL* (2018), J.-D. Bancal *et al.*, *PRL* (2018).

[11] W.-H. Zhang *et al.*, *arXiv:1905.12175* (2019), X. Jiang *et al.*, *arXiv:2002.00640* (2020).

Q & A

Thank you !

Any questions ?

Bibliography I

- S. Pallister, N. Linden, A. Montanaro, *PRL* (2018).
- H. Zhu, M. Hayashi, *PRL* (2019).
- M. Owari, M. Hayashi, *NJP* (2008).
- K. Wang, M. Hayashi, *PRA* (2019).
- E. Størmer, *Acta Mathematica* (1963).
- S. L. Woronowicz, *Reports on Mathematical Physics* (1976).
- M.-D. Choi, *Linear algebra and Its Applications* (1975).
- H. Zhu, H. Zhang, *PRA* (2020).
- Y.-C. Liu, J. Shang, X.-D. Yu, X. Zhang, *PRA* (2020).
- X.-D. Yu, J. Shang, O. Gühne, *npjQI* (2019).
- Z. Li, Y.-G. Han, H. Zhu, *PRA* (2019).
- Y.-C. Liu, X.-D. Yu, J. Shang, H. Zhu, X. Zhang, *PRApplied* (2019).

Bibliography II

P. Sekatski, J.-D. Bancal, S. Wagner, N. Sangouard, *PRL* (2018).

J.-D. Bancal, N. Sangouard, P. Sekatski, *PRL* (2018).

W.-H. Zhang *et al.*, *arXiv:1905.12175* (2019).

X. Jiang *et al.*, *arXiv:2002.00640* (2020).