Rigidity of quantum steering and 1sDI verifiable quantum computation

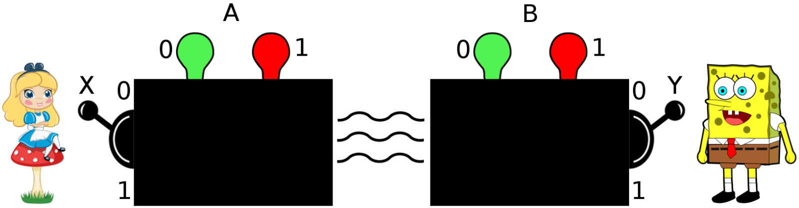
[arXiv:1512.07401]

Alexandru Gheorghiu, Petros Wallden, Elham Kashefi

8 June 2016

QPL 2016, Glasgow

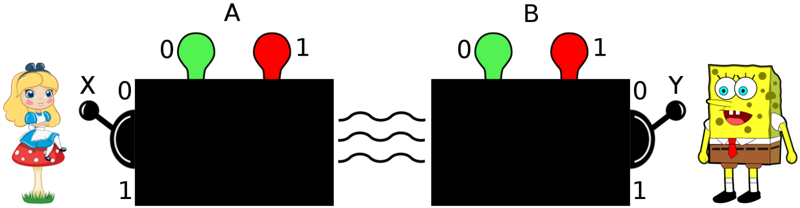
Nonlocal correlations



$$p(a, b|x, y) \neq \sum_{\lambda} p(a|x, \lambda)p(b|y, \lambda)p(\lambda)$$

$$S = |\, \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \,| \geq 2$$

Nonlocal correlations



$$p(a,b|x,y) \neq \sum_{\lambda} p(a|x,\lambda)p(b|y,\lambda)p(\lambda)$$

$$S = |\,\langle A_0 B_0\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle\,| \geq 2$$

Tsirelson's theorem (1980)

$S = 2\sqrt{2}$ is the maximum that can be achieved by QM. E.g. by having Alice and Bob share $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and measure:

$$A_0 = X,\ A_1 = Z,\ B_0 = (X+Z)/\sqrt{2},\ B_1 = (X-Z)/\sqrt{2}$$

Rigidity

Reichardt Unger Vazirani [RUV] (2012)

Robust converse of Tsirelson's theorem is also true.

Rigidity

Reichardt Unger Vazirani [RUV] (2012)

Robust converse of Tsirelson's theorem is also true.

$$S = |\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle| \geq 2\sqrt{2} - \epsilon$$

ρ_{AB} is the shared state of Alice and Bob

Rigidity

Reichardt Unger Vazirani [RUV] (2012)

Robust converse of Tsirelson's theorem is also true.

$$S = |\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle| \geq 2\sqrt{2} - \epsilon$$

ρ_{AB} is the shared state of Alice and Bob

There exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$

Rigidity

Reichardt Unger Vazirani [RUV] (2012)

Robust converse of Tsirelson's theorem is also true.

$$S = |\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle| \geq 2\sqrt{2} - \epsilon$$

ρ_{AB} is the shared state of Alice and Bob

There exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$

$$\Phi(\rho_{AB}) \approx |\phi_+\rangle \otimes |\phi_+\rangle \otimes ... \otimes |\phi_+\rangle \otimes |junk\rangle$$

Rigidity

Reichardt Unger Vazirani [RUV] (2012)

Robust converse of Tsirelson's theorem is also true.

$$S = |\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle| \geq 2\sqrt{2} - \epsilon$$

ρ_{AB} is the shared state of Alice and Bob

There exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$

$$\Phi(\rho_{AB}) \approx |\phi_+\rangle \otimes |\phi_+\rangle \otimes ... \otimes |\phi_+\rangle \otimes |junk\rangle$$

$$\Phi(A_0) \approx X \qquad \Phi(A_1) \approx Z$$

$$\Phi(B_0) \approx (X + Z)/\sqrt{2} \qquad \Phi(B_1) \approx (X - Z)/\sqrt{2}$$

Rigidity

Reichardt Unger Vazirani [RUV] (2012)

Robust converse of Tsirelson's theorem is also true.

$$S = |\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle| \geq 2\sqrt{2} - \epsilon$$

ρ_{AB} is the shared state of Alice and Bob

There exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$

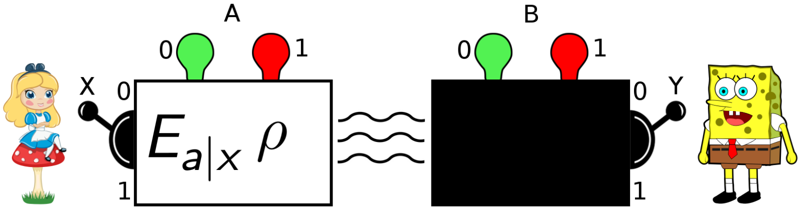
$$\Phi(\rho_{AB}) \approx |\phi_+\rangle \otimes |\phi_+\rangle \otimes ... \otimes |\phi_+\rangle \otimes |junk\rangle$$

$$\Phi(A_0) \approx X \qquad \Phi(A_1) \approx Z$$

$$\Phi(B_0) \approx (X + Z)/\sqrt{2} \qquad \Phi(B_1) \approx (X - Z)/\sqrt{2}$$

Saturating nonlocal correlations determines state and strategy!

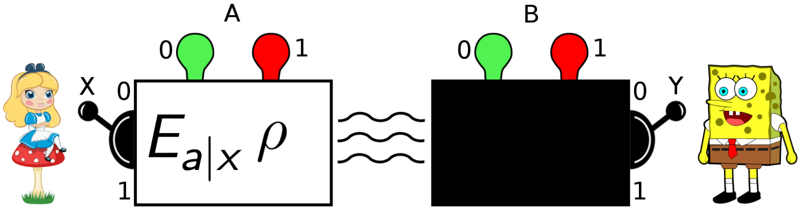
Steering correlations



$$p(a,b|x,y) \neq \sum_{\lambda} Tr(\rho_{AB}(\lambda)(E_{a|x} \otimes I))p(b|y,\lambda)p(\lambda)$$

$$S = |\,\langle A_0 B_0\rangle + \langle A_1 B_1\rangle\,| \geq \sqrt{2}$$

Steering correlations



$$p(a, b|x, y) \neq \sum_{\lambda} Tr(\rho_{AB}(\lambda)(E_{a|x} \otimes I)) p(b|y, \lambda) p(\lambda)$$

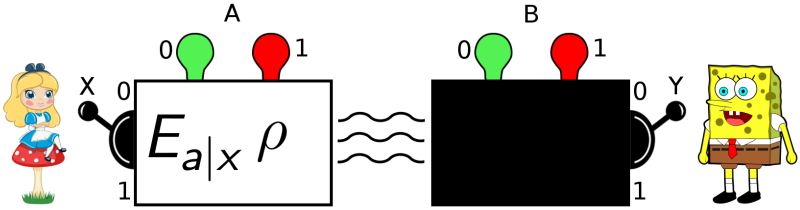
$$S = |\, \langle A_0 B_0 \rangle + \langle A_1 B_1 \rangle \,| \geq \sqrt{2}$$

Theorem

$S = 2$ is the maximum that can be achieved. E.g. by having Alice and Bob share $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and measure:

$$A_0 = X,\ A_1 = Z,\ B_0 = X,\ B_1 = Z$$

Steering correlations



$$p(a,b|x,y) \neq \sum_{\lambda} Tr(\rho_{AB}(\lambda)(E_{a|x} \otimes I))p(b|y,\lambda)p(\lambda)$$

$$S = |\,\langle A_0 B_0 \rangle + \langle A_1 B_1 \rangle\,| \geq \sqrt{2}$$

Theorem

$S = 2$ is the maximum that can be achieved. E.g. by having Alice and Bob share $|\phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and measure:

$$A_0 = X,\ A_1 = Z,\ B_0 = X,\ B_1 = Z$$

Our main result: Converse is also true!

Assumptions

- Quantum mechanics is true/correct
  (no supra-quantum correlations)

Assumptions

- Quantum mechanics is true/correct
  (no supra-quantum correlations)

- Alice is trusted to measure anticommuting A_0 and A_1
  (e.g. $A_0 = X$, $A_1 = Z$)

Assumptions

- Quantum mechanics is true/correct
  (no supra-quantum correlations)
- Alice is trusted to measure anticommuting A_0 and A_1
  (e.g. $A_0 = X$, $A_1 = Z$)
- Bob is untrusted. Measures B'_0 and B'_1

Assumptions

- Quantum mechanics is true/correct
(no supra-quantum correlations)
- Alice is trusted to measure anticommuting A_0 and A_1
(e.g. $A_0 = X$, $A_1 = Z$)
- Bob is untrusted. Measures B_0' and B_1'
- Observables have 2 outcomes ± 1 and are also unitary

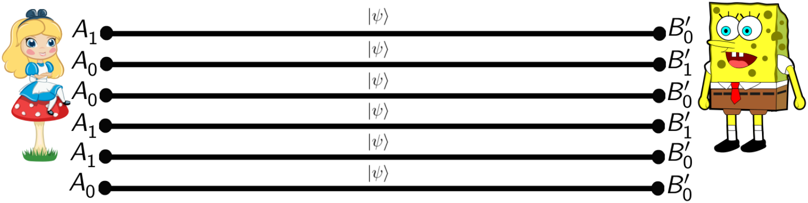
Assumptions

- Quantum mechanics is true/correct
(no supra-quantum correlations)
- Alice is trusted to measure anticommuting A_0 and A_1
(e.g. $A_0 = X$, $A_1 = Z$)
- Bob is untrusted. Measures B_0' and B_1'
- Observables have 2 outcomes ± 1 and are also unitary
- Shared state ρ_{AB}, prepared by Bob (untrusted)

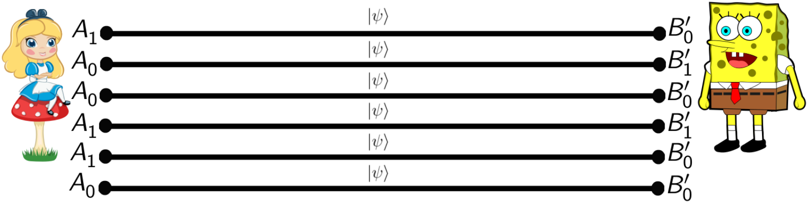
Assumptions

- Quantum mechanics is true/correct (no supra-quantum correlations)
- Alice is trusted to measure anticommuting A_0 and A_1 (e.g. $A_0 = X$, $A_1 = Z$)
- Bob is untrusted. Measures B_0' and B_1'
- Observables have 2 outcomes ± 1 and are also unitary
- Shared state ρ_{AB}, prepared by Bob (untrusted)
- In each round Alice and Bob measure the same state $|\psi\rangle$ (**i.i.d.**)

Self-testing i.i.d. states

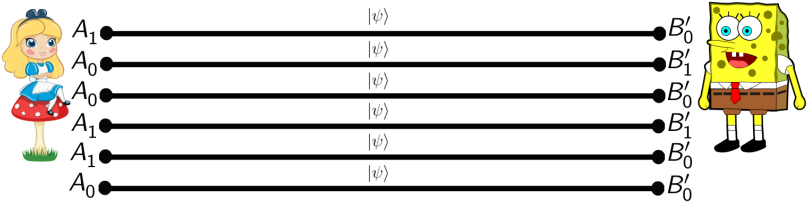


Self-testing i.i.d. states



$$|\langle A_0 B'_0 \rangle + \langle A_1 B'_1 \rangle| \geq 2 - \epsilon \tag{1}$$

Self-testing i.i.d. states



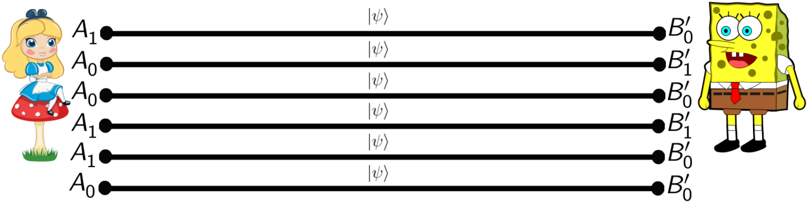
$$| \langle A_0 B'_0 \rangle + \langle A_1 B'_1 \rangle | \geq 2 - \epsilon \tag{1}$$

I.i.d. self-testing theorem

If inequality 1 is satisfied, then there exists a local isometry $\Phi = I \otimes \Phi_B$ such that, for all $M_A \in \{I, A_0, A_1\}$, $N'_B \in \{I, B'_0, B'_1\}$:

$$||\Phi(M_A N'_B |\psi\rangle) - |junk\rangle M_A N_B |\phi_+\rangle || \leq O(\sqrt{\epsilon})$$

Self-testing i.i.d. states



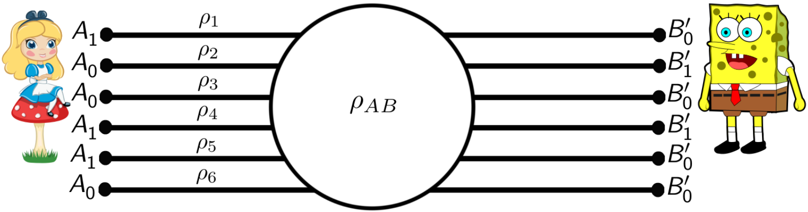
$$|\langle A_0 B'_0 \rangle + \langle A_1 B'_1 \rangle| \geq 2 - \epsilon \tag{1}$$

I.i.d. self-testing theorem

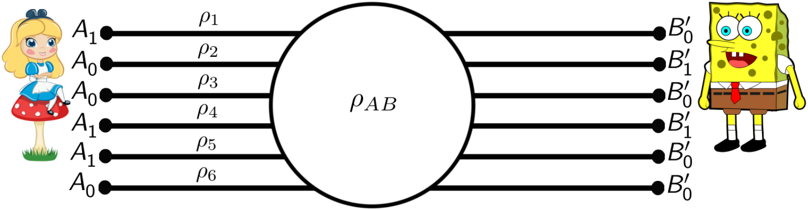
If inequality 1 is satisfied, then there exists a local isometry $\Phi = I \otimes \Phi_B$ such that, for all $M_A \in \{I, A_0, A_1\}$, $N'_B \in \{I, B'_0, B'_1\}$:

$$|| \Phi(M_A N'_B |\psi\rangle) - |junk\rangle M_A N_B |\phi_+\rangle || \leq O(\sqrt{\epsilon})$$

Cannot do better than $O(\sqrt{\epsilon})$!

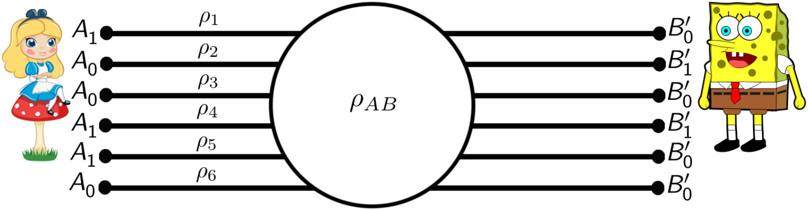

A_1
A_0
A_0
A_1
A_1
A_0
ρ_1
ρ_2
ρ_3
ρ_4
ρ_5
ρ_6
ρ_{AB}
B'_0
B'_1
B'_0
B'_1
B'_0
B'_0

Removing i.i.d.



$$|\langle A_0 B'_0 \rangle + \langle A_1 B'_1 \rangle| \geq 2 - \epsilon \quad (1)$$

Removing i.i.d.



$$|\langle A_0 B'_0 \rangle + \langle A_1 B'_1 \rangle| \geq 2 - \epsilon \tag{1}$$

Non-i.i.d. self-testing theorem

If inequality 1 is satisfied, then there exists a local isometry $\Phi = I \otimes \Phi_B$ such that, for $\mathcal{E}_{AB'}$ having the role of M_A, N'_B from before, we have for a randomly chosen ρ_i:

$$||\Phi(\mathcal{E}_{AB'}(\rho_i)) - \mathcal{E}_{AB}(|\phi_+\rangle\langle\phi_+|)|| \leq O(\epsilon^{1/6})$$

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

Do NK rounds of measurement certify N states?

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

Do NK rounds of measurement certify N states?

Not implicitly, because of overlap/adaptiveness!

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

Do NK rounds of measurement certify N states?

Not implicitly, because of overlap/adaptiveness!

- $\mathcal{S}_{real} = (\rho_{AB}, \mathcal{E}_A, \mathcal{E}'_B)$ denotes the <u>real</u> strategy

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

Do NK rounds of measurement certify N states?

Not implicitly, because of overlap/adaptiveness!

- $\mathcal{S}_{real} = (\rho_{AB}, \mathcal{E}_A, \mathcal{E}'_B)$ denotes the real strategy
- $\mathcal{S}_{ideal} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{E}_B)$ denotes the ideal strategy

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

Do NK rounds of measurement certify N states?

Not implicitly, because of overlap/adaptiveness!

- $\mathcal{S}_{real} = (\rho_{AB}, \mathcal{E}_A, \mathcal{E}'_B)$ denotes the real strategy
- $\mathcal{S}_{ideal} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{E}_B)$ denotes the ideal strategy
- $\mathcal{S}_{guess} = (\rho_{AB}, \mathcal{E}_A, \mathcal{G}_B)$ denotes a guessing strategy

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

Do NK rounds of measurement certify N states?

Not implicitly, because of overlap/adaptiveness!

- $\mathcal{S}_{real} = (\rho_{AB}, \mathcal{E}_A, \mathcal{E}'_B)$ denotes the real strategy
- $\mathcal{S}_{ideal} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{E}_B)$ denotes the ideal strategy
- $\mathcal{S}_{guess} = (\rho_{AB}, \mathcal{E}_A, \mathcal{G}_B)$ denotes a guessing strategy
- $\mathcal{S}'_{guess} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{G}_B)$ second guessing strategy

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

Do NK rounds of measurement certify N states?

Not implicitly, because of overlap/adaptiveness!

- $\mathcal{S}_{real} = (\rho_{AB}, \mathcal{E}_A, \mathcal{E}'_B)$ denotes the real strategy
- $\mathcal{S}_{ideal} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{E}_B)$ denotes the ideal strategy
- $\mathcal{S}_{guess} = (\rho_{AB}, \mathcal{E}_A, \mathcal{G}_B)$ denotes a guessing strategy
- $\mathcal{S}'_{guess} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{G}_B)$ second guessing strategy
- $\mathcal{S}$ is ϵ-structured $\leftrightarrow$ observed correlation is greater than $2 - \epsilon$

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

Do NK rounds of measurement certify N states?

Not implicitly, because of overlap/adaptiveness!

- $\mathcal{S}_{real} = (\rho_{AB}, \mathcal{E}_A, \mathcal{E}'_B)$ denotes the real strategy
- $\mathcal{S}_{ideal} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{E}_B)$ denotes the ideal strategy
- $\mathcal{S}_{guess} = (\rho_{AB}, \mathcal{E}_A, \mathcal{G}_B)$ denotes a guessing strategy
- $\mathcal{S}'_{guess} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{G}_B)$ second guessing strategy
- $\mathcal{S}$ is ϵ-structured $\leftrightarrow$ observed correlation is greater than $2 - \epsilon$
- $\mathcal{S}_1 \approx \mathcal{S}_2 \leftrightarrow \rho_1 \approx \rho_2$, $\mathcal{E}_{A,1} \approx \mathcal{E}_{A,2}$, $\mathcal{E}_{B,1} \approx \mathcal{E}_{B,2}$

State and strategy determination

Suppose we do K rounds of measurement to certify one Bell state.

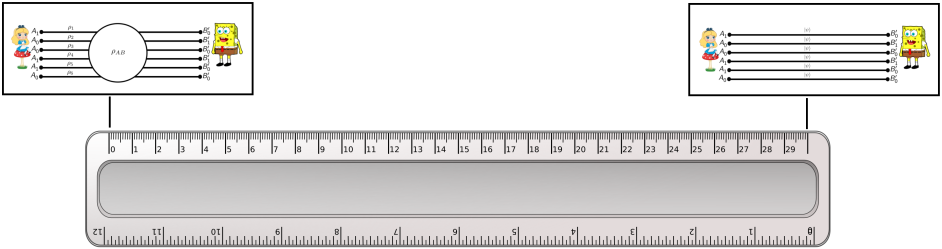
Do NK rounds of measurement certify N states?

Not implicitly, because of overlap/adaptiveness!

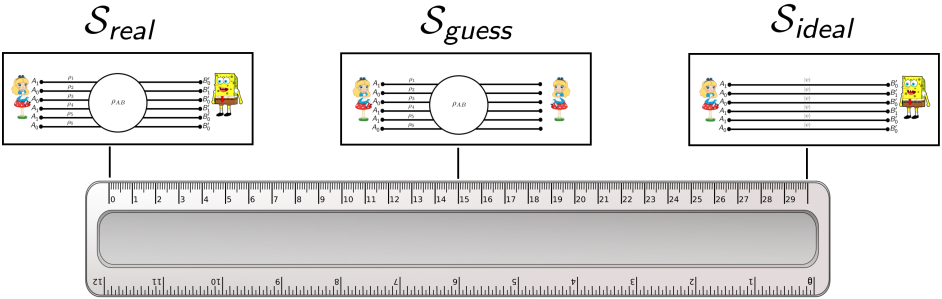
- $\mathcal{S}_{real} = (\rho_{AB}, \mathcal{E}_A, \mathcal{E}'_B)$ denotes the real strategy
- $\mathcal{S}_{ideal} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{E}_B)$ denotes the ideal strategy
- $\mathcal{S}_{guess} = (\rho_{AB}, \mathcal{E}_A, \mathcal{G}_B)$ denotes a guessing strategy
- $\mathcal{S}'_{guess} = (|\phi_+\rangle \otimes ... \otimes |\phi_+\rangle, \mathcal{E}_A, \mathcal{G}_B)$ second guessing strategy
- $\mathcal{S}$ is ϵ-structured $\leftrightarrow$ observed correlation is greater than $2 - \epsilon$
- $\mathcal{S}_1 \approx \mathcal{S}_2 \leftrightarrow \rho_1 \approx \rho_2$, $\mathcal{E}_{A,1} \approx \mathcal{E}_{A,2}$, $\mathcal{E}_{B,1} \approx \mathcal{E}_{B,2}$

Objective: $\mathcal{S}_{real} \approx \mathcal{S}_{ideal}$

$\mathcal{S}_{real}$ $\mathcal{S}_{ideal}$

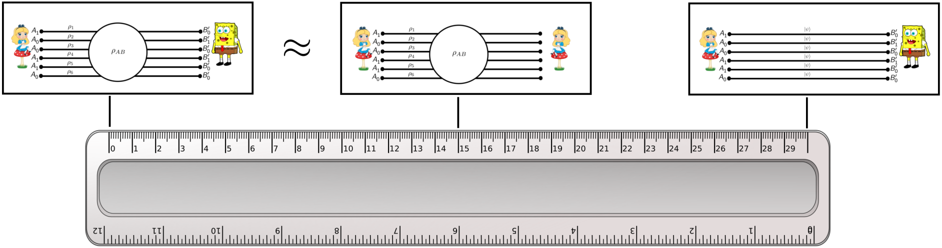


State and strategy determination - Proof sketch

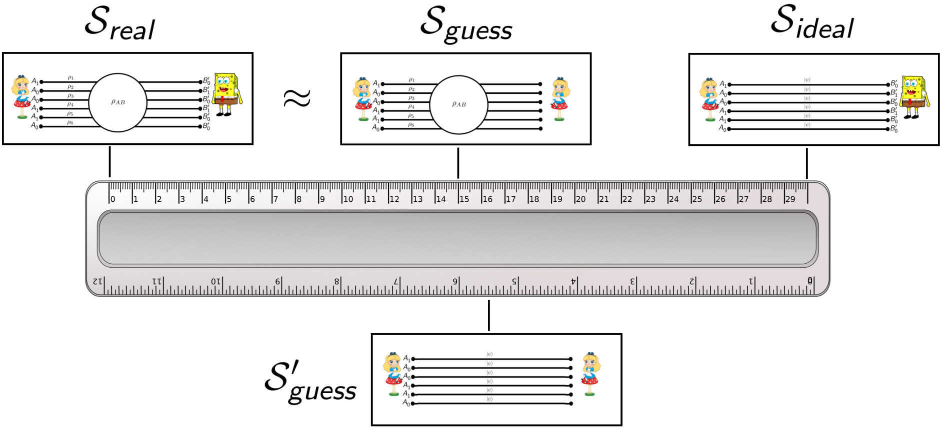


State and strategy determination - Proof sketch

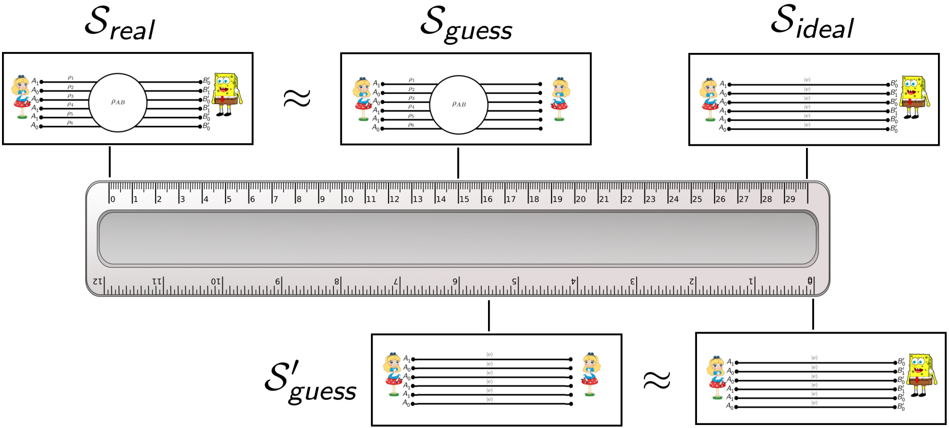
$\mathcal{S}_{real}$ $\mathcal{S}_{guess}$ $\mathcal{S}_{ideal}$



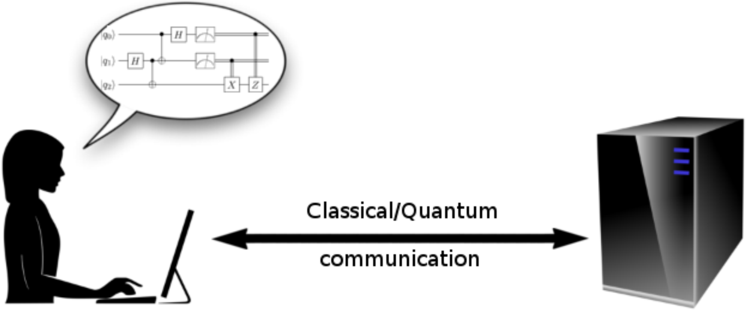
State and strategy determination - Proof sketch



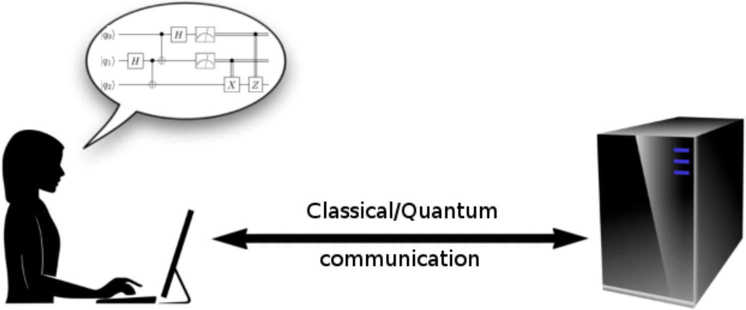
State and strategy determination - Proof sketch



Application: verification of quantum computation

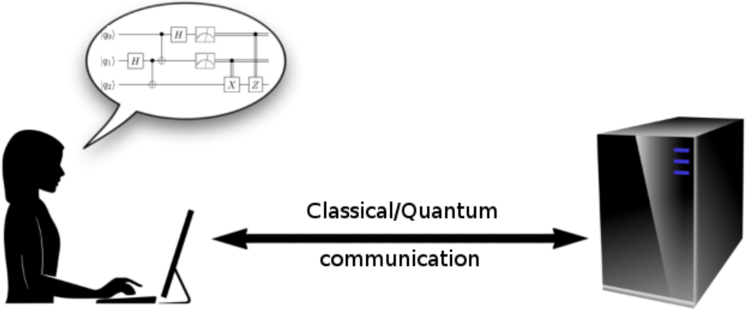


Application: verification of quantum computation



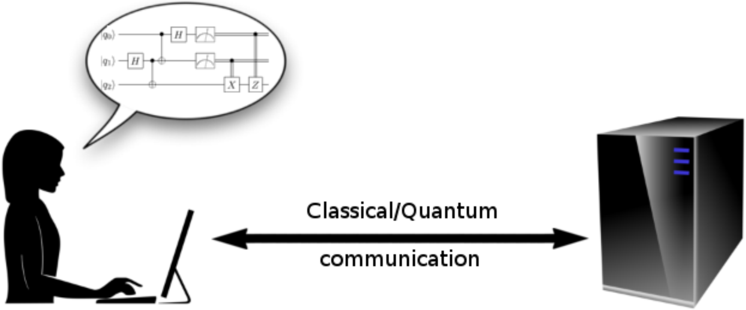
- Computationally limited, trusted verifier

Application: verification of quantum computation



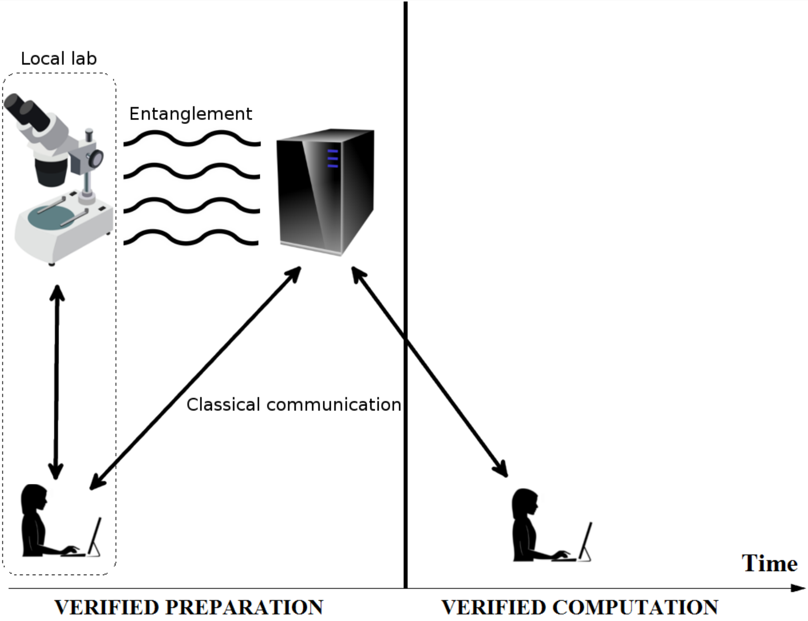
- Computationally limited, trusted verifier
- Powerful, untrusted quantum server(s)

Application: verification of quantum computation



- Computationally limited, trusted verifier
- Powerful, untrusted quantum server(s)
- Alice = verifier, Bob = server

Application: verification of quantum computation



Conclusions

- Saturating correlations $\leftrightarrow$ ideal states and measurements
- I.i.d. self-testing $\rightarrow$ Non-i.i.d. self-testing $\rightarrow$ Rigidity
- Lower bounded $\Omega(\sqrt{\epsilon})$ closeness
- Tight bounds for non-i.i.d. and rigidity?
- Most natural application is quantum verification

Related work and references

Presentation based primarily on this work:
[Gheorghiu, Kashefi, Wallden, '15] - arXiv:1512.07401

Related works on **self-testing** and **rigidity**:
[Hoban, Šupić '16] - arXiv:1601.01552
[Bancal, Navascués, Scarani, Vértesi, Yang '13] - arXiv:1307.7053
[Reichardt, Unger, Vazirani '12] - arXiv:1209.0448
[McKague, Yang, Scarani '12] - arXiv:1203.2976

Related works on **verification**:
[Gheorghiu, Kashefi, Wallden '15] - arXiv:1502.02571
[Kashefi, Wallden '15] - arXiv:1510.07408
[McKague '15] - arXiv:1309.5675

Thank you!