A Quantum Pigeonhole Principle and Two Semidefinite Relaxations of Communication Complexity

Pavel Dvořák — Charles University

Bruno Loff, Suhail Sherif — University of Lisbon

Why?

Why?

- Interested in communication complexity lower bounds.

Why?

- Interested in communication complexity lower bounds.

But computing CC is NP-hard!

("The relation R has a communication protocol of cost $\leq k$")

Why?

- Interested in communication complexity lower bounds.

But computing CC is NP-hard!

("The relation R has a communication protocol of cost $\leq k$")

("The relation R needs $>k$ communication" is coNP-hard!

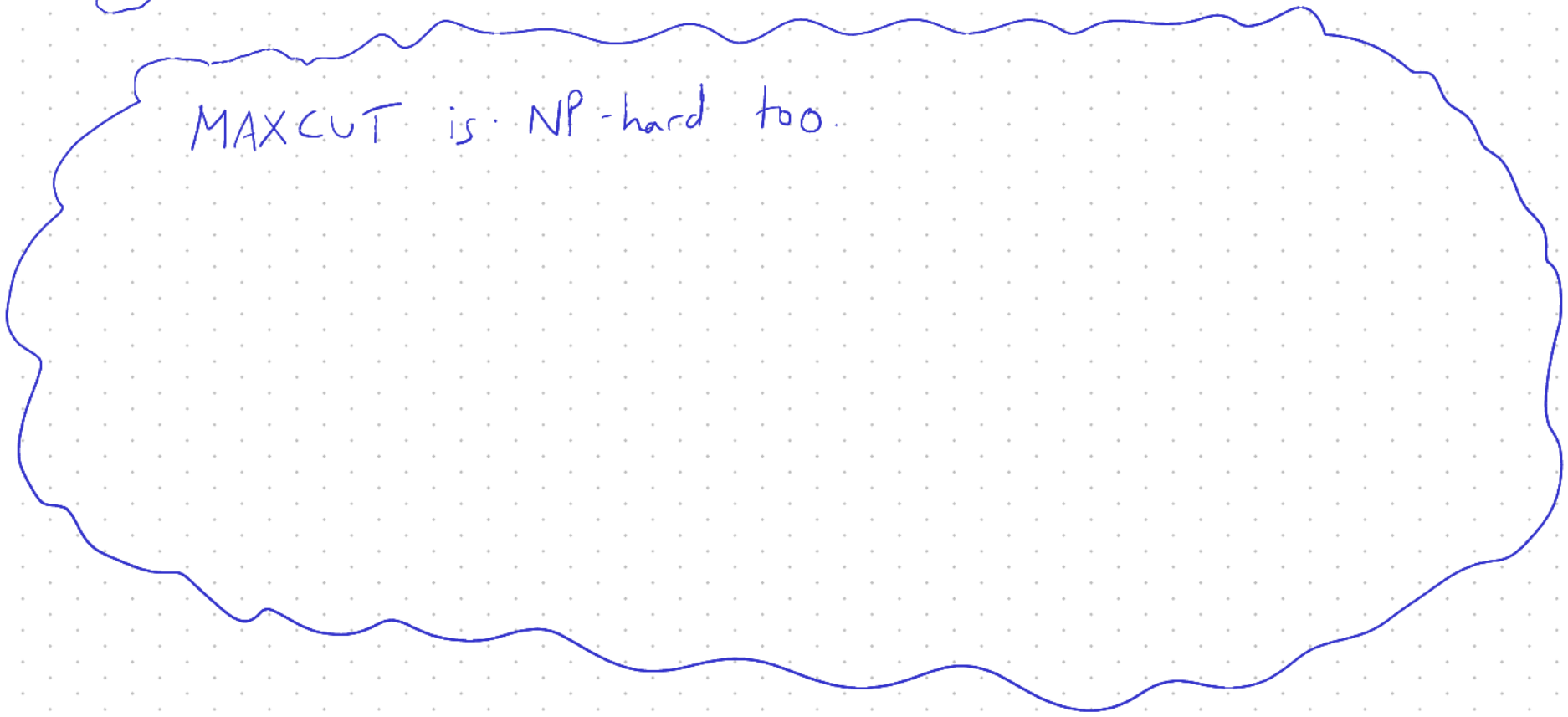
No guarantee that short proofs even exist!

Why?

- Interested in communication complexity lower bounds.

  ⋮

  But computing CC is NP-hard!



Why?

- Interested in communication complexity lower bounds.

  ⋮

  But computing CC is NP-hard!

MAXCUT is NP-hard too.

SDP-MAXCUT is easy though.

Why?

- Interested in communication complexity lower bounds.

  ⋮

  But computing CC is NP-hard!

MAXCUT is NP-hard too.

SDP-MAXCUT is easy though.

And the output of both are close, so that's great!

Can something like this work for us too?

What can this look like?

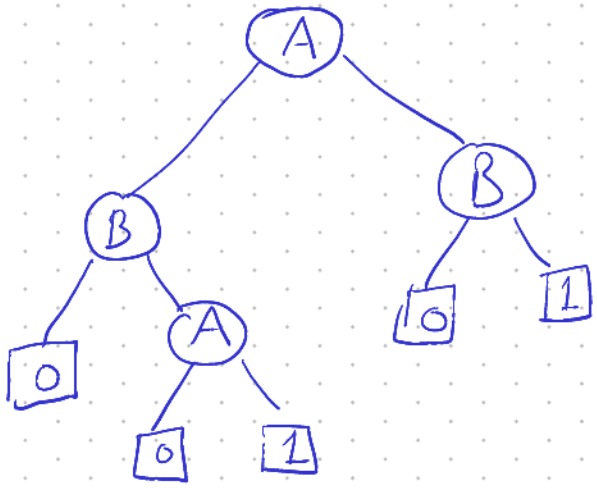
What can this look like?

We were able to come up with a quadratic feasibility problem capturing "Does the relation R have a Comm. protocol of a specific structure?"

What can this look like?

We were able to come up with a quadratic feasibility problem capturing "Does the relation R have a Comm. protocol of a specific structure?"

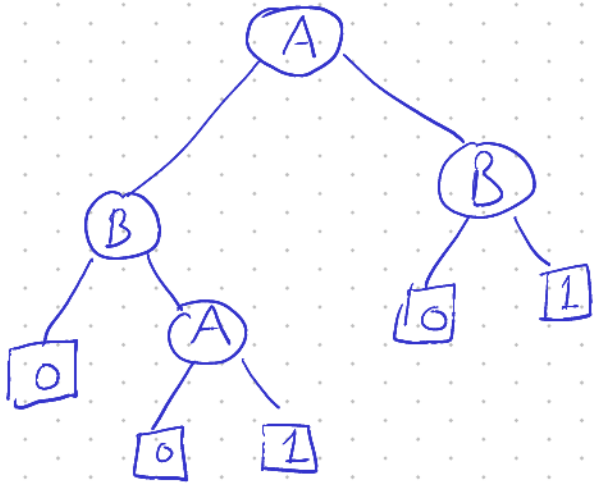
Example structure =



What can this look like?

We were able to come up with a quadratic feasibility problem capturing "Does the relation R have a Comm. protocol of a specific structure?"

Example structure:



Quadratic feasibility:

Is there a setting $\phi: V \to \{0,1\}$ satisfying certain constraints of the form

$$\sum \alpha_{ij} v_i v_j = \beta \; ?$$

What can this look like?

Quadratic feasibility:

Is there a setting $\phi : V \to \{0,1\}$ satisfying certain constraints of the form $\sum \alpha_{ij} v_i v_j = \beta$?

Semidefinite feasibility:

Is there $d \in \mathbb{N}$, a setting $\phi : V \to \mathbb{R}^d$ satisfying certain constraints of the form $\sum \alpha_{ij} \langle v_i, v_j \rangle = \beta$?

What becomes easy?

What becomes easy?

- We now have a SDFP asking "Does the relation R have a relaxed protocol of a specific structure?"

What becomes easy?

- We now have a SDFP asking "Does the relation R have a relaxed protocol of a specific structure?"
- There is an efficient algorithm that can answer this.

What becomes easy?

- We now have a SDFP asking "Does the relation R have a relaxed protocol of a specific structure?"
- There is an efficient (practical?) algorithm that can answer this.

What becomes easy?

- We now have a SDFP asking "Does the relation R have a relaxed protocol of a specific structure?"
- There is an efficient algorithm that can answer this. (practical?)
- There are simple certificates for both
  - YES instances ← the satisfying assignment ϕ
  - &
  - NO instances ← the satisfying assignment for the dual SDFP.

What becomes easy?

- We now have a SDFP asking "Does the relation R have a relaxed protocol of a specific structure?"
- There is an efficient (practical?) algorithm that can answer this.
- There are simple certificates for both

  YES instances ← the satisfying assignment ϕ

  &

  NO instances ← the satisfying assignment for the dual SDFP.

i.e. a new kind of guaranteed lower bound. (maybe even bypasses a natural proof barrier)

The Other Ingredient

MAXCUT is NP-hard too. ✓

SDP-MAXCUT is easy though. ✓ ?

And the output of both are close, so that's great!

Can something like this work for us too?

The Other Ingredient

MAXCUT is NP-hard too. ✓

SDP-MAXCUT is easy though. ✓

And the output of both are close, so that's great!

Can something like this work for us too?

Show that $SDP\text{-}CC(R) \geq CC(R)^{\Omega(1)}$ for all R?

The Other Ingredient

MAXCUT is NP-hard too ✓

SDP-MAXCUT is easy though ✓

And the output of both are close ?, so that's great!

Can something like this work for us too?

Show that $SDP\text{-}CC(R) \geq CC(R)^{\Omega(1)}$ for all R?

Show $SDP\text{-}CC(R)$ is large for some R's where we know $CC(R)$ is large?

$$R = \text{EQUALITY} : \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}$$

$$R = \text{EQUALITY} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

▷ Our actual goal : formula lower bounds via CC lower bounds for KW relations

$$R = \text{EQUALITY} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

▷ Our actual goal: formula lower bounds via CC lower bounds for KW relations (via SDP-CC lower bounds)

$$R = \text{EQUALITY} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

▷ Our actual goal : formula lower bounds via CC lower bounds for KW relations (via SDP-CC lower bounds)

Lower bound for any KW relation

$\Downarrow$

Lower bound for EQUALITY

$$R = \text{EQUALITY} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$$

▷ Our actual goal : formula lower bounds via CC lower bounds for KW relations (via SDP-CC lower bounds)

Lower bound for any KW relation

$\Downarrow$

Lower bound for EQUALITY

[The CC lower bound for Eq is just a simple application of the pigeonhole principle]

What happened next:

What happened next:

- SPP-CC #1: Structured γ_2 protocols
- SPP-CC #2: Quantum Lab protocols

What happened next:

- SDP-CC #1: Structured γ_2 protocols
- SDP-CC #2: Quantum Lab protocols
- SDP-PHP: A Quantum Pigeonhole Principle

What happened next:

- SDP-CC #1: Structured γ_2 protocols
- SDP-CC #2: Quantum Lab protocols
- SDP-PHP: A Quantum Pigeonhole Principle
- 2-round $\Omega(n)$ lower bound for QuantumLab(EQ)

What happened next:

- SDP-CC #1: Structured γ_2 protocols
- SDP-CC #2: Quantum Lab protocols
- SDP-PHP: A Quantum Pigeonhole Principle
- 2-round $\Omega(n)$ lower bound for QuantumLab(EQ)
- Cheap EQUALITY Protocols for both SDP-CCs !!!

What happened next:

- SDP-CC #1: Structured γ_2 protocols
- SDP-CC #2: Quantum Lab protocols
- SDP-PHP: A Quantum Pigeonhole Principle
- 2-round $\Omega(n)$ lower bound for QuantumLab(EQ)
- Cheap EQUALITY Protocols for both SDP-CCs !!!
- No KW lower bounds for ANY simple SDP-CC!

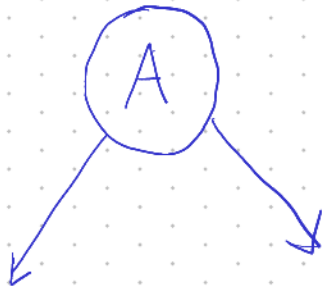
[Austrin-Risse '23]

↑

No SoS formula lower bounds

Quantum Lab Protocols

Quantum Lab Protocols

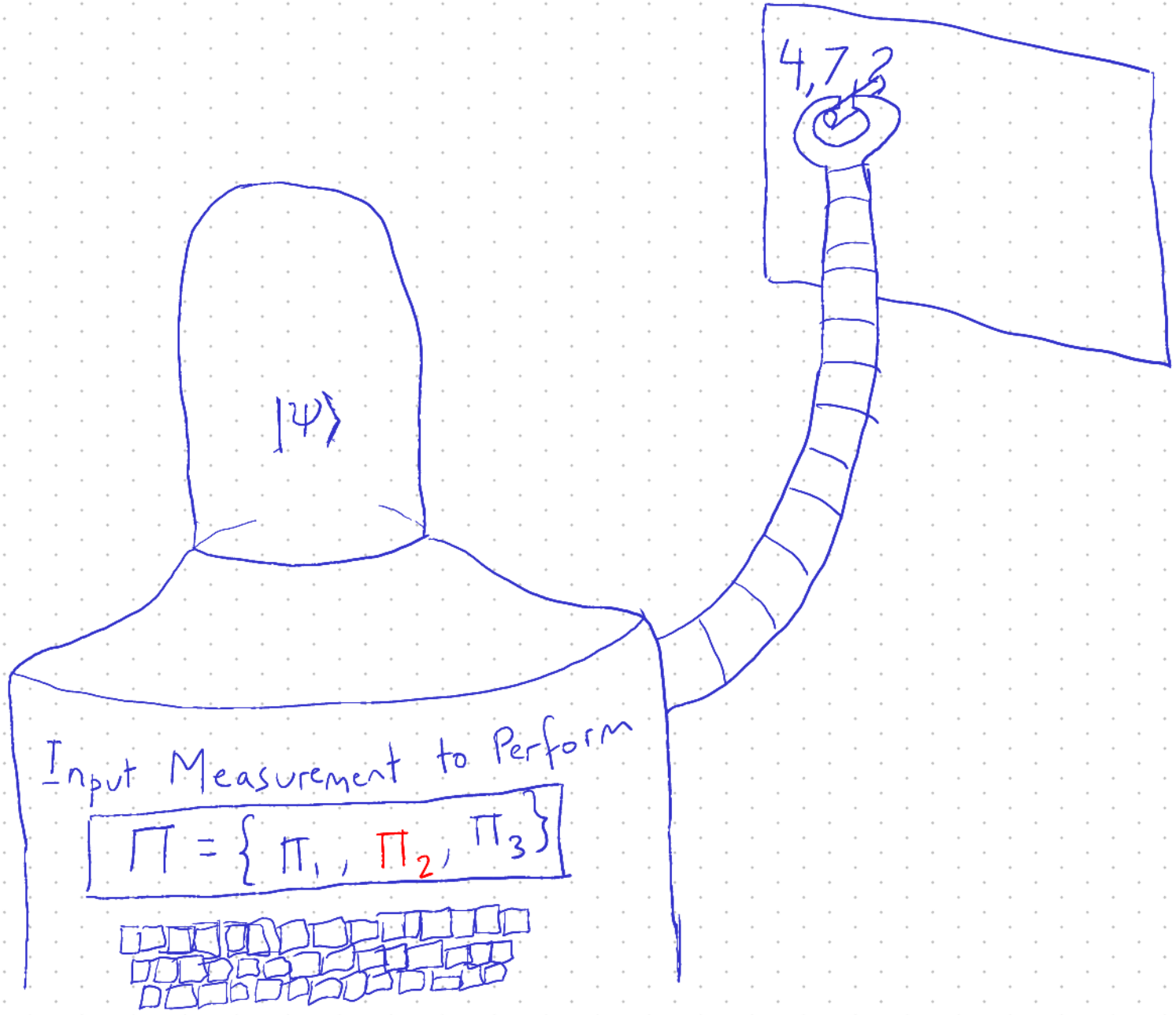


At a node u, on input x,

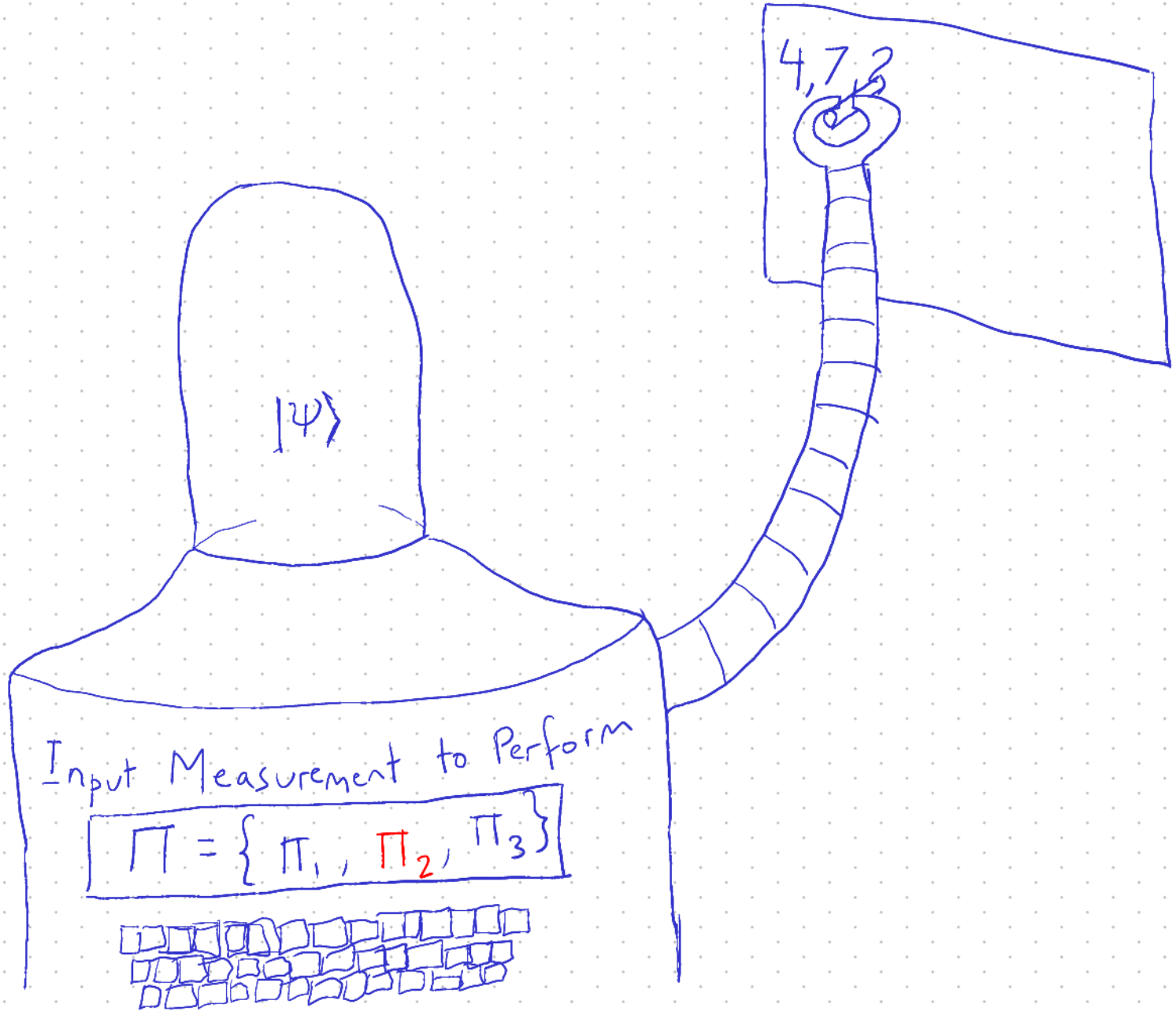
Alice has to decide which child to proceed to.

$$V_{u,x} \in \{0,1\}$$

Quantum Lab Protocols

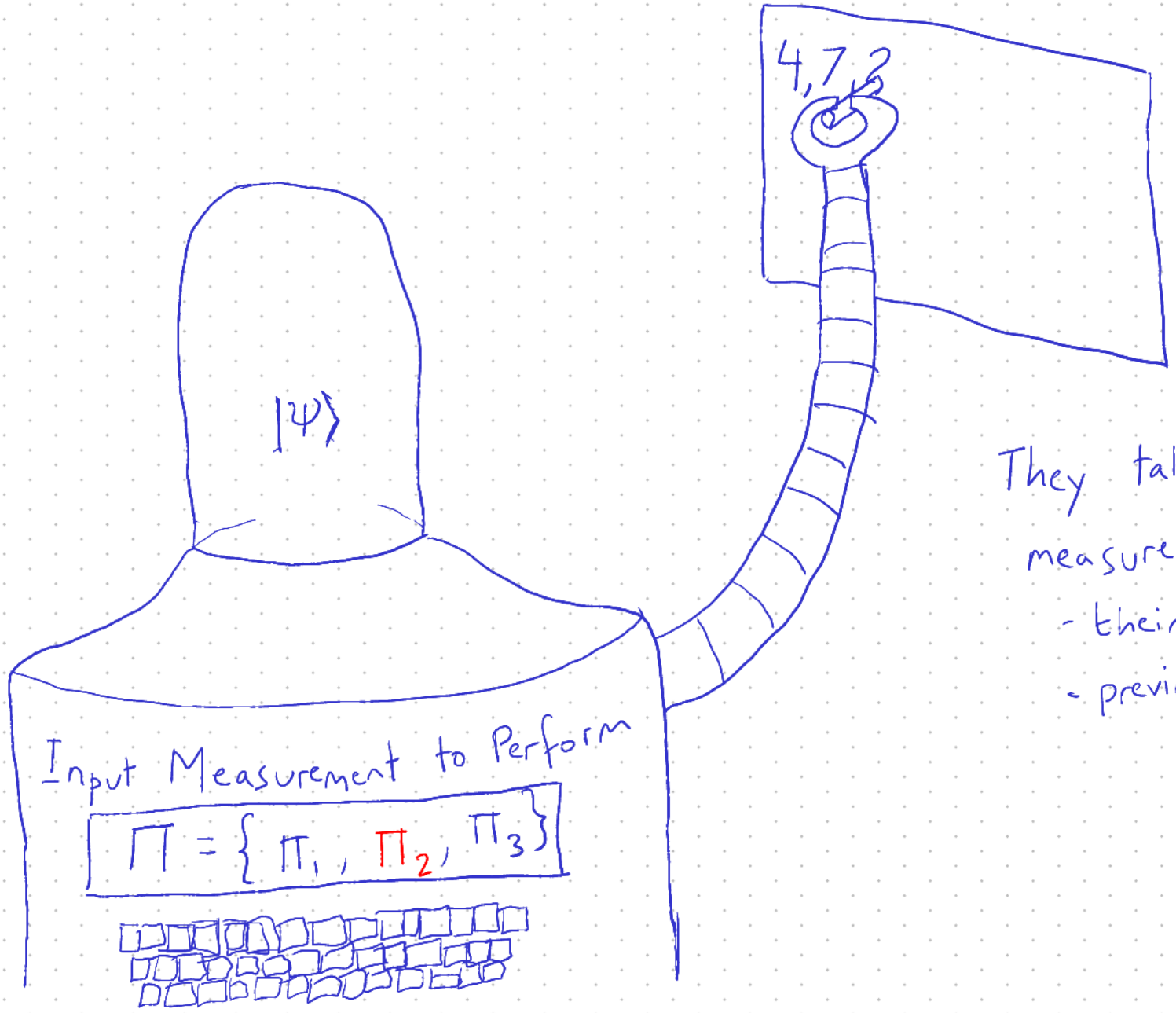


Quantum Lab Protocols



Alice, Bob agree on initial state $|\phi\rangle$.

Quantum Lab Protocols

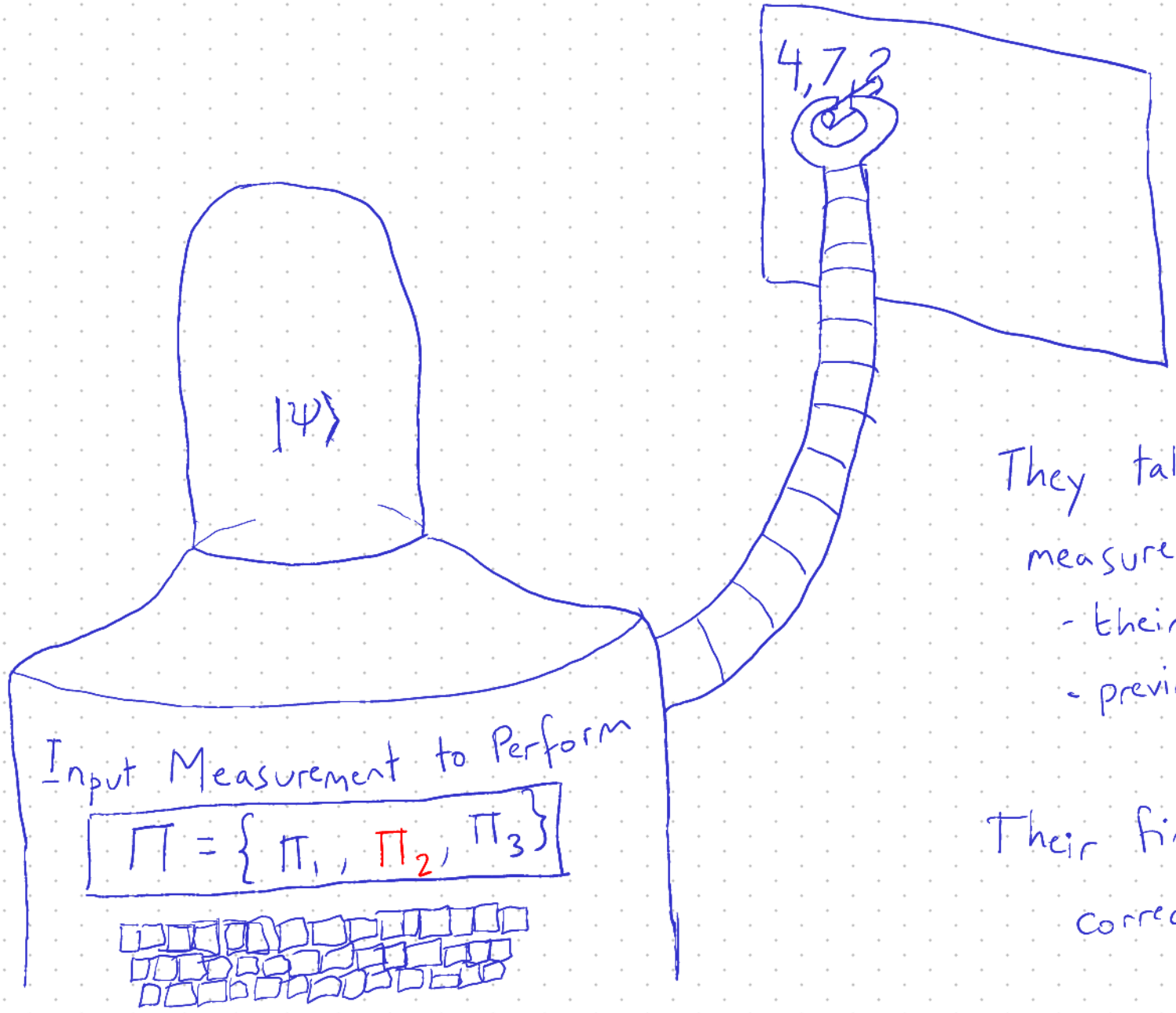


Alice, Bob agree on initial state $|\phi\rangle$.

They take turns making measurements based on:

- their input
- previous measurement results.

Quantum Lab Protocols



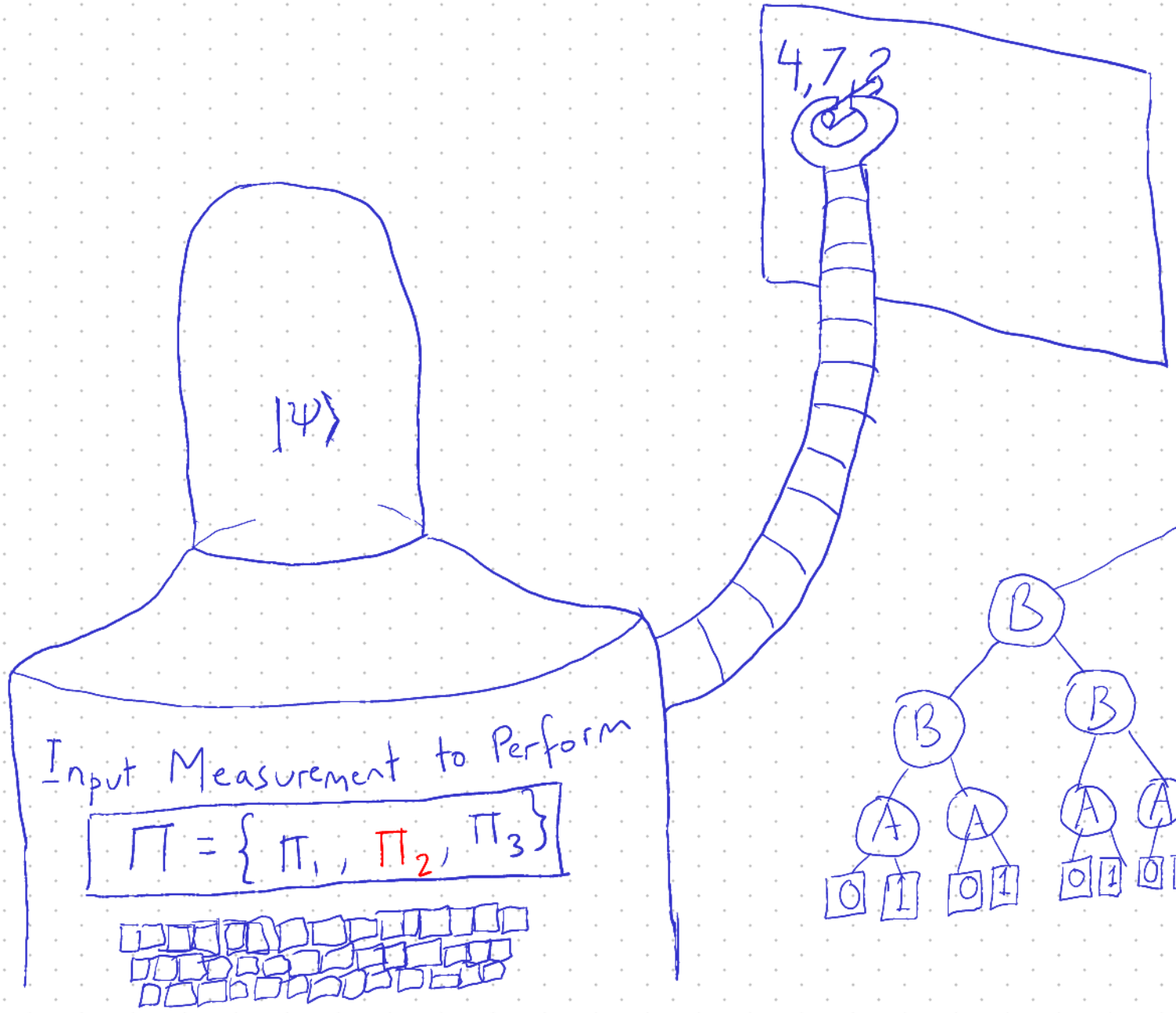
Alice, Bob agree on initial state $|\phi\rangle$.

They take turns making measurements based on:

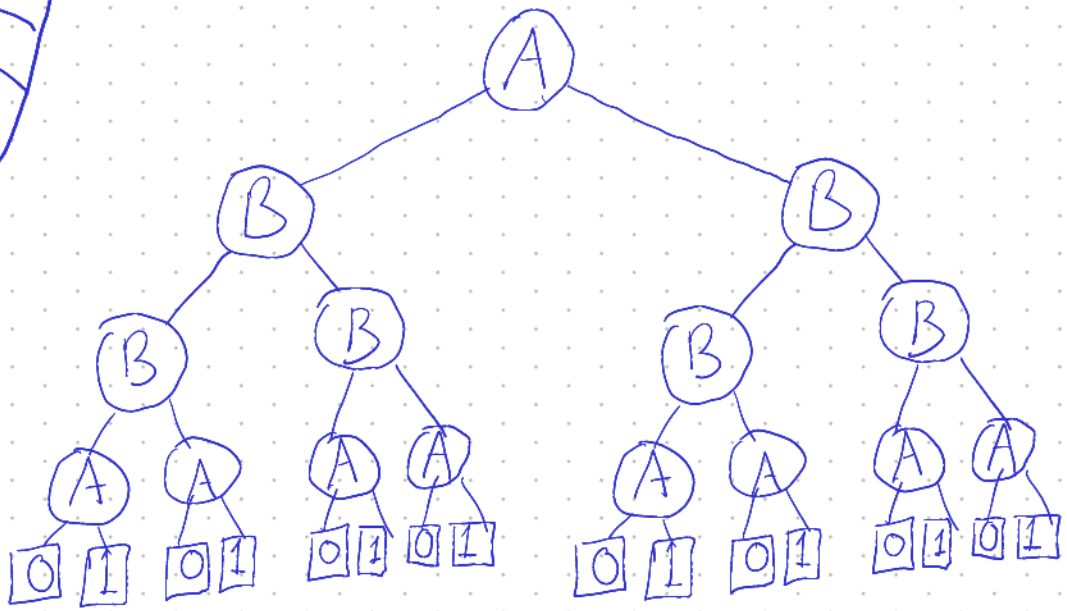
- their input
- previous measurement results.

Their final output must be correct always.

Quantum Lab Protocols - Results



EVERY function has a 3-round, 4-bit quantum lab protocol.



Quantum Pigeonhole Principle

Quantum Pigeonhole Principle

$|\psi\rangle$

Quantum Pigeonhole Principle

$|\psi\rangle$

$|\psi\rangle$

$|\psi\rangle$

$|\psi\rangle$

$|\psi\rangle$

Quantum Pigeonhole Principle

$$|\psi\rangle = |\psi_{1,1}\rangle + |\psi_{1,2}\rangle + |\psi_{1,3}\rangle + |\psi_{1,4}\rangle$$

$$|\psi\rangle = |\psi_{2,1}\rangle + |\psi_{2,2}\rangle + |\psi_{2,3}\rangle + |\psi_{2,4}\rangle$$

$$|\psi\rangle = |\psi_{3,1}\rangle + |\psi_{3,2}\rangle + |\psi_{3,3}\rangle + |\psi_{3,4}\rangle$$

$$|\psi\rangle = |\psi_{4,1}\rangle + |\psi_{4,2}\rangle + |\psi_{4,3}\rangle + |\psi_{4,4}\rangle$$

$$|\psi\rangle = |\psi_{5,1}\rangle + |\psi_{5,2}\rangle + |\psi_{5,3}\rangle + |\psi_{5,4}\rangle$$

orthogonal decompositions

Quantum Pigeonhole Principle

$$|\psi\rangle = |\psi_{1,1}\rangle + |\psi_{1,2}\rangle + |\psi_{1,3}\rangle + |\psi_{1,4}\rangle$$

$$|\psi\rangle = |\psi_{2,1}\rangle + |\psi_{2,2}\rangle + |\psi_{2,3}\rangle + |\psi_{2,4}\rangle$$

$$|\psi\rangle = |\psi_{3,1}\rangle + |\psi_{3,2}\rangle + |\psi_{3,3}\rangle + |\psi_{3,4}\rangle$$

$$|\psi\rangle = |\psi_{4,1}\rangle + |\psi_{4,2}\rangle + |\psi_{4,3}\rangle + |\psi_{4,4}\rangle$$

$$|\psi\rangle = |\psi_{5,1}\rangle + |\psi_{5,2}\rangle + |\psi_{5,3}\rangle + |\psi_{5,4}\rangle$$

orthogonal decompositions

Quantum Pigeonhole Principle

$$|\psi\rangle = |\psi_{1,1}\rangle + |\psi_{1,2}\rangle + |\psi_{1,3}\rangle + |\psi_{1,4}\rangle$$

$$|\psi\rangle = |\psi_{2,1}\rangle + |\psi_{2,2}\rangle + |\psi_{2,3}\rangle + |\psi_{2,4}\rangle$$

$$|\psi\rangle = |\psi_{3,1}\rangle + |\psi_{3,2}\rangle + |\psi_{3,3}\rangle + |\psi_{3,4}\rangle$$

$$|\psi\rangle = |\psi_{4,1}\rangle + |\psi_{4,2}\rangle + |\psi_{4,3}\rangle + |\psi_{4,4}\rangle$$

$$|\psi\rangle = |\psi_{5,1}\rangle + |\psi_{5,2}\rangle + |\psi_{5,3}\rangle + |\psi_{5,4}\rangle$$

orthogonal decompositions

} box w/ 2 non-orthogonal vectors.

Quantum Pigeonhole Principle

$$\sum_{i=1}^{p} |i\rangle_A \otimes |\psi\rangle_B$$

$\downarrow$ "classical-quantum" measurement with h outcomes

$$\sum |i\rangle_A |\phi_i\rangle_B$$

if $p > h$,

w.p. > 0 $\nexists$ measurement on B that decouples A

(like measuring A does)

Quantum Pigeonhole Principle - Results

Quantum Pigeonhole Principle - Results

▷ It is true.

Quantum Pigeonhole Principle - Results

- It is true.
- Found "simple" proof via duality

Quantum Pigeonhole Principle - Results

- It is true.
- Found "simple" proof via duality
- Proved stronger quantitative variant:

  ∃ hole j & pigeons i, i' such that

$$\langle \psi_{i,j} | \psi_{i',j} \rangle \geq \frac{1}{h^2}\left(\beta - \frac{h-1}{p-1}\right)$$

  if average initial pigeon overlap $\frac{1}{p(p-1)} \sum_{i \neq i'} \langle \psi_i | \psi_{i'} \rangle = \beta$

Quantum Pigeonhole Principle - Results

- It is true.
- Found "simple" proof via duality
- Proved stronger quantitative variant:

  $\exists$ hole j & pigeons i, i' such that

$$\langle \psi_{i,j} | \psi_{i',j} \rangle \geq \frac{1}{h^2}\left(\beta - \frac{h-1}{p-1}\right)$$

  if average initial pigeon overlap $\frac{1}{p(p-1)} \sum_{i \neq i'} \langle \psi_i | \psi_{i'} \rangle = \beta$

Open: Find "simple" proof of stronger variant?

Structured γ_2 Protocols (Γ_2^{cc})

Structured γ_2 Protocols (Γ_2^{cc})

At a node u, a relevant question:

"Does the input (x,y) reach the node u?"

$$V_{u,x,y} \in \{0,1\}$$

Structured γ_2 Protocols (Γ_2^{cc})

- Requires leaves to "have" γ_2 norm at most 1.

Structured γ_2 Protocols (Γ_2^{cc})

- Requires leaves to "have" γ_2 norm at most 1.
- $\Gamma_2^{cc}(f) \geq \log \gamma_2(M_f)$

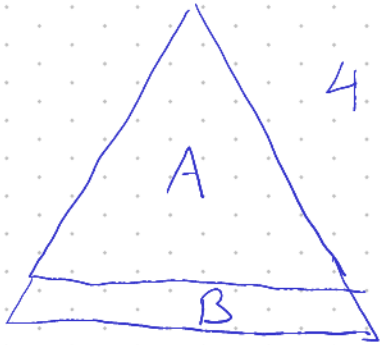
$\therefore \quad \Gamma_2^{cc}(IP) \geq \Omega(n)$

Structured γ_2 Protocols (Γ_2^{cc})

- Requires leaves to "have" γ_2 norm at most 1.
- $\Gamma_2^{cc}(f) \geq \log \gamma_2(M_f)$

$\therefore \quad \Gamma_2^{cc}(IP) \geq \Omega(n)$

But $\Gamma_2^{cc}(EQ) \leq 5.$



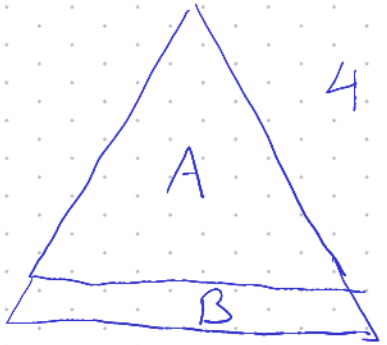
4 layers of Alice nodes

1 layer of Bob nodes

Structured γ_2 Protocols (Γ_2^{cc})

- Requires leaves to "have" γ_2 norm at most 1.
- $\Gamma_2^{cc}(f) \geq \log \gamma_2(M_f)$

$\therefore \quad \Gamma_2^{cc}(IP) \geq \Omega(n)$



4 layers of Alice nodes

1 layer of Bob nodes

But $\Gamma_2^{cc}(EQ) \leq 5$.

Is it essentially just $\log \gamma_2$?

Open Problems:

- Find "simple" proof of stronger variant of QPHP?
- Do SDP variants of other principles also hold?

Open Problems:

- Find "simple" proof of stronger variant of QPHP?
- Do SDP variants of other principles also hold?

Thank you

Questions are welcome.