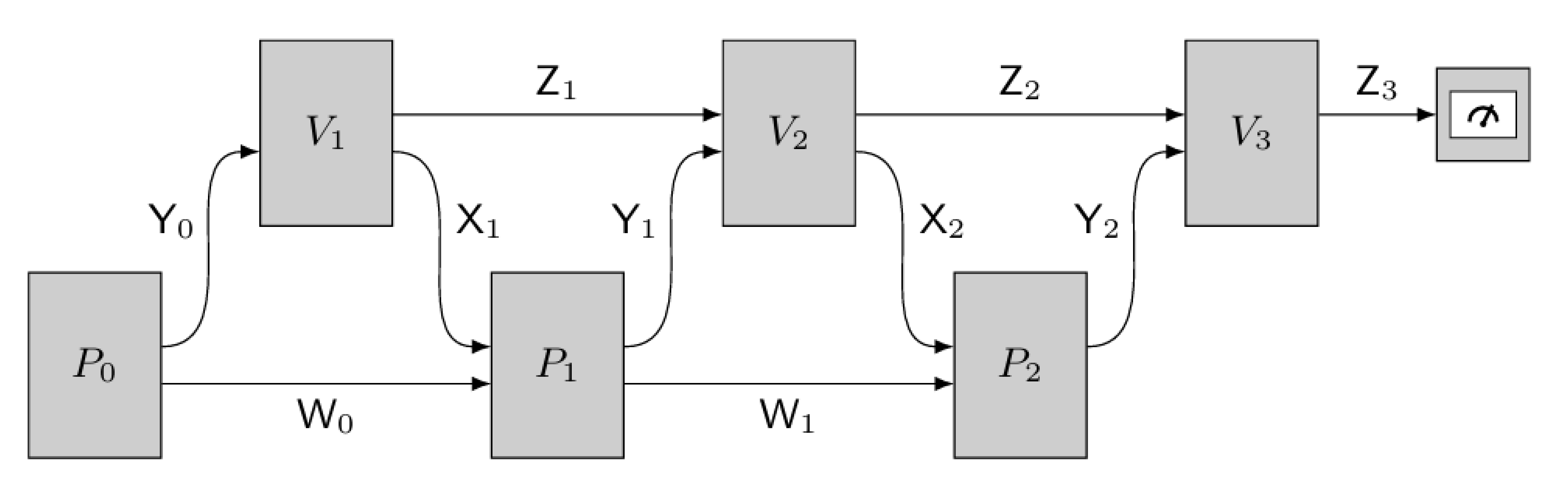
Quantum Complexity Theory

Quantum Interactive Proofs



Anant Gupta & Kevin Xie

Recap

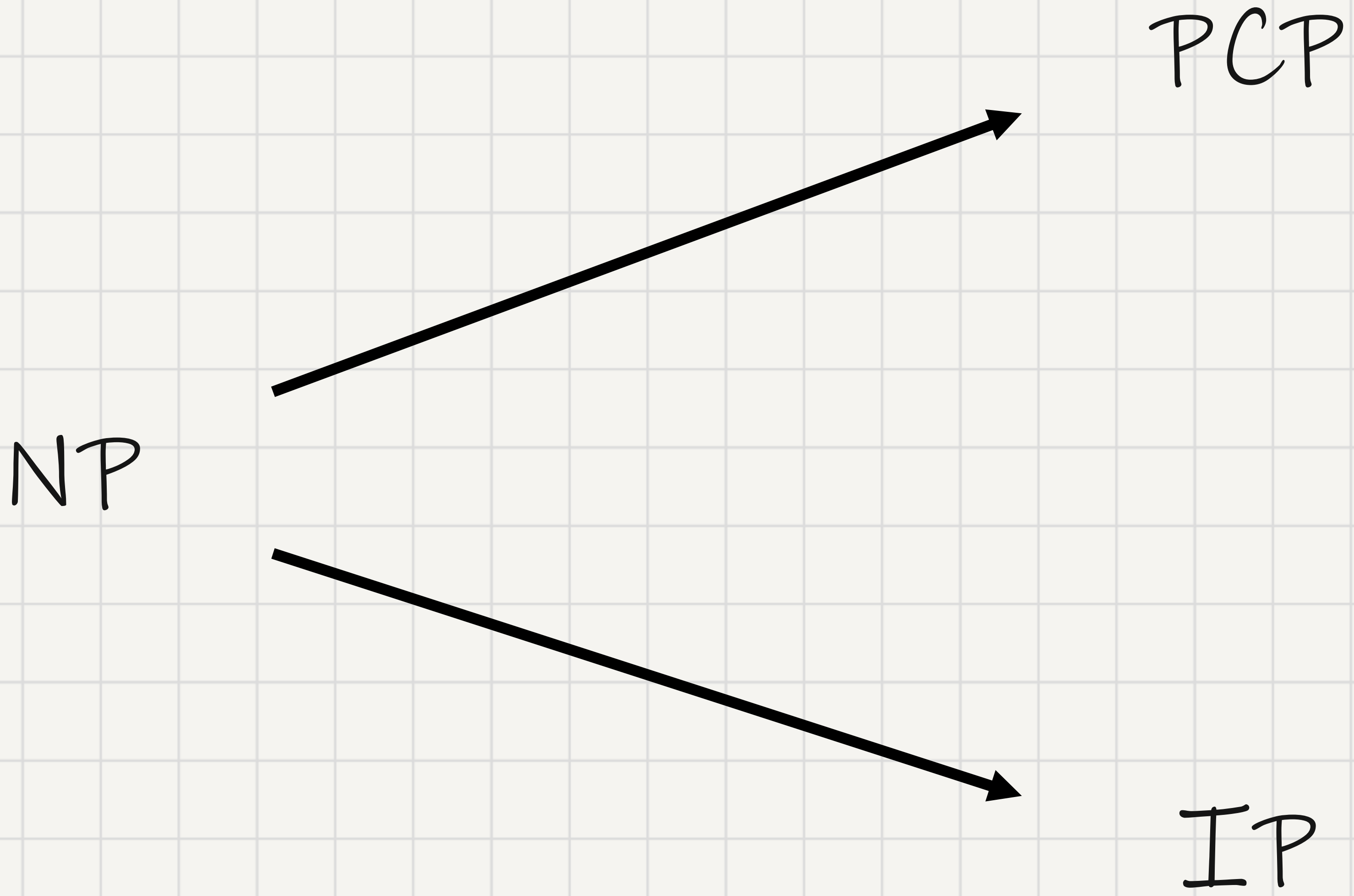
QMA: Set of all problems for which there exists a BQP verifier V such that:

- If x is in L, there exists a 'proof object' $|\psi\rangle$ which V accepts with probability $\geq 2/3$
- If x is not in L, for all 'proof objects' $|\psi\rangle$, V accepts with probability $\leq 1/3$

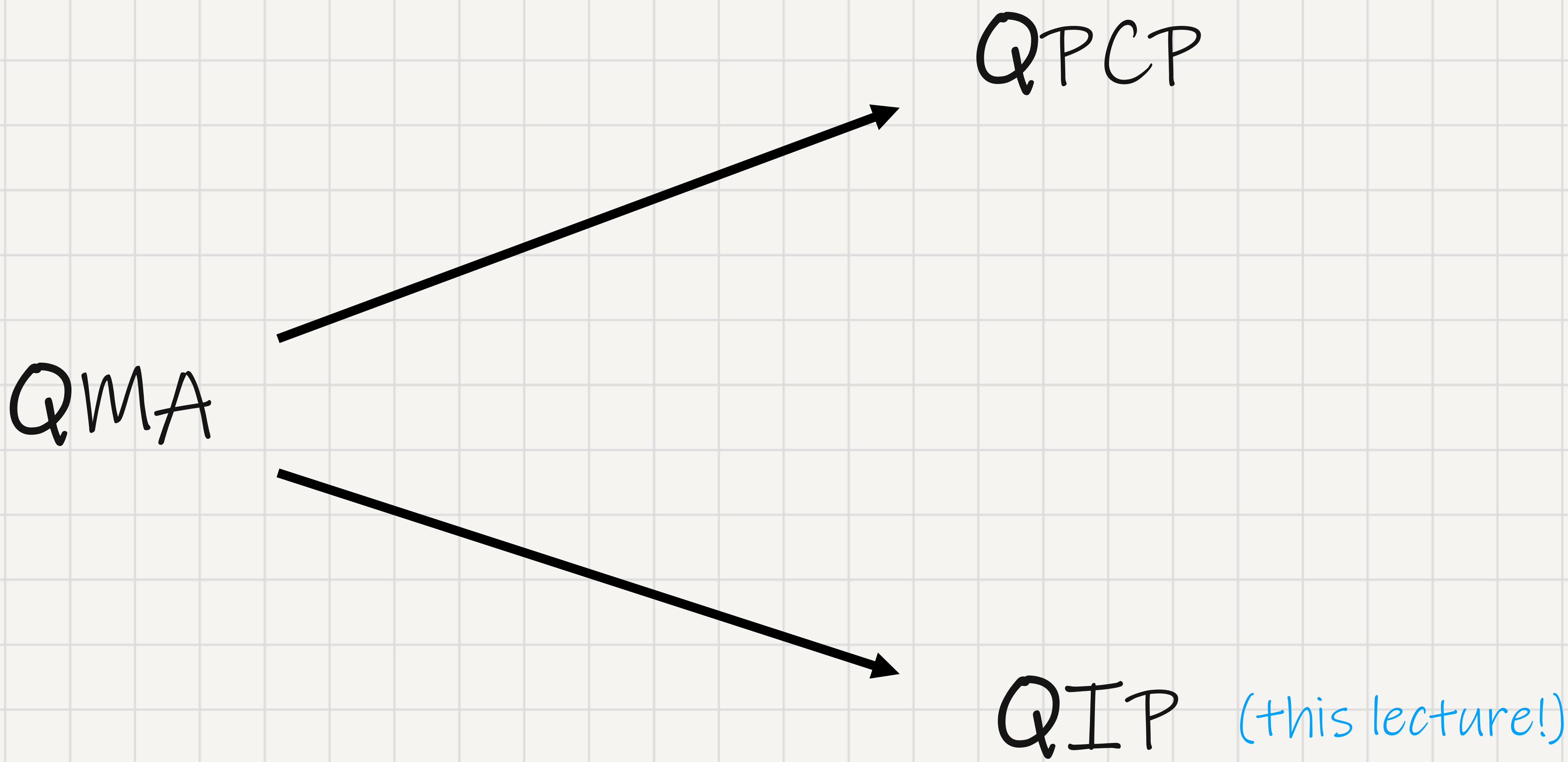
"quantum analogue of NP"

$$\text{NP} \longrightarrow \text{MA} \longrightarrow \text{QMA}$$

The classical complexity situation

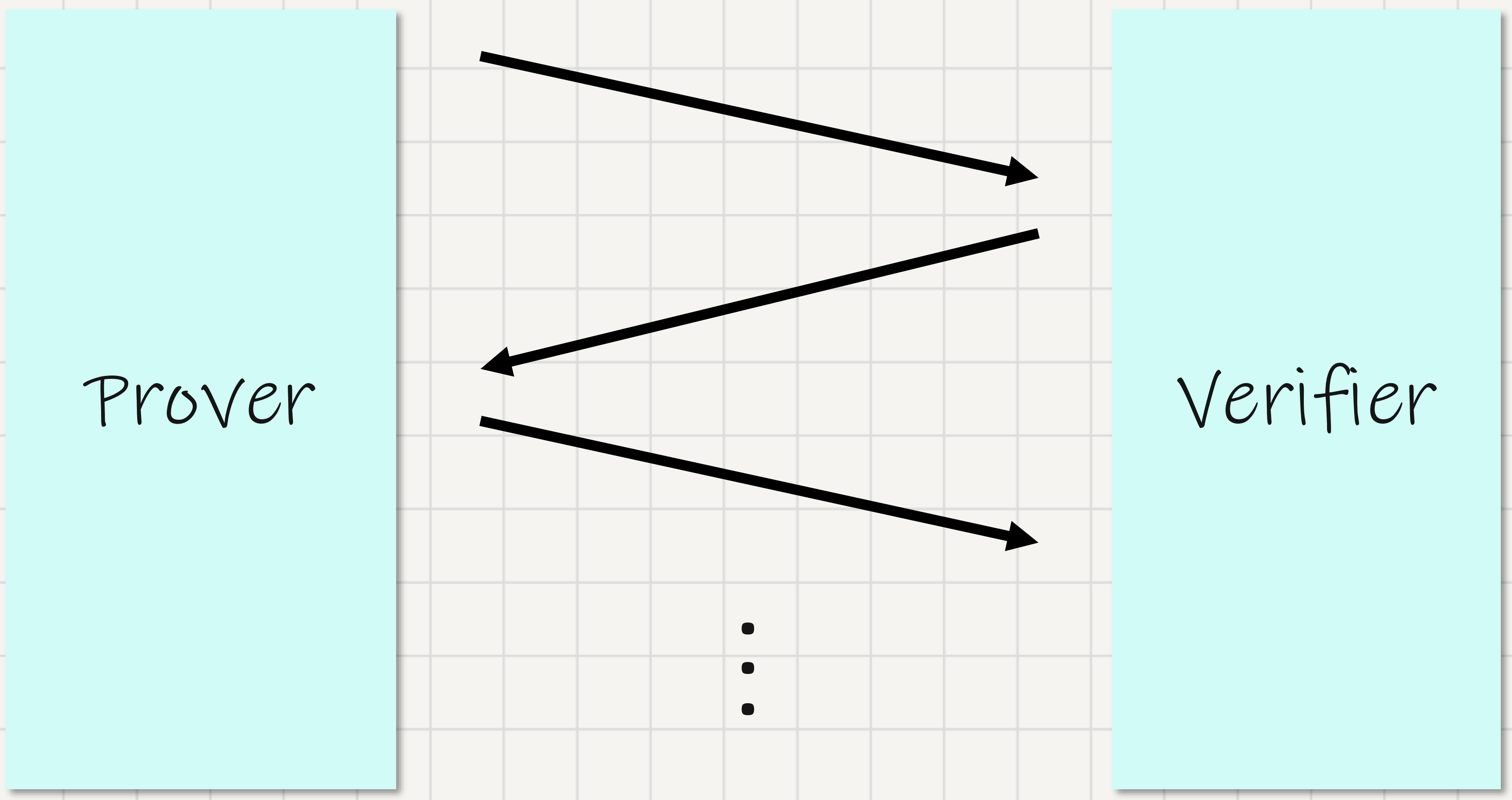


The **quantum** complexity situation



Interactive proof systems

2 parties:



Computationally **unbounded**
(but untrustworthy)

Computationally **bounded**
(but trustworthy)

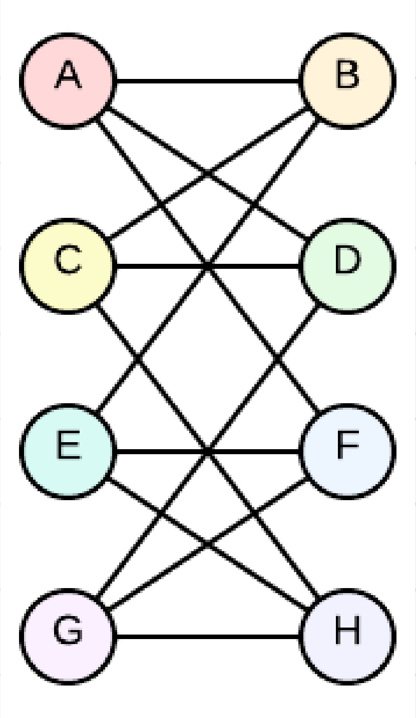
Interactive proof systems

Key idea:
Reformulate complexity classes in the interactive proof system framework

- P: polytime, deterministic, 0-turn verifier
- NP: polytime, deterministic, 1-turn verifier
- IP: polytime, probabilistic, poly-turn verifier

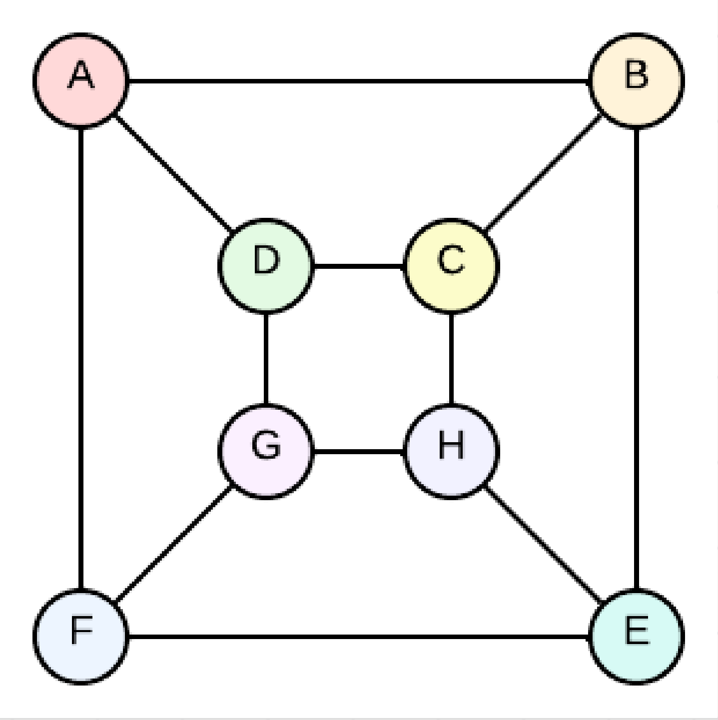
Example: Graph Isomorphism

$\overline{ISO}$: Given two graphs G and H, decide whether G and H are **not** isomorphic



Key idea:
Verifier selects G or H randomly, permutes the vertices, and asks prover which graph the result came from

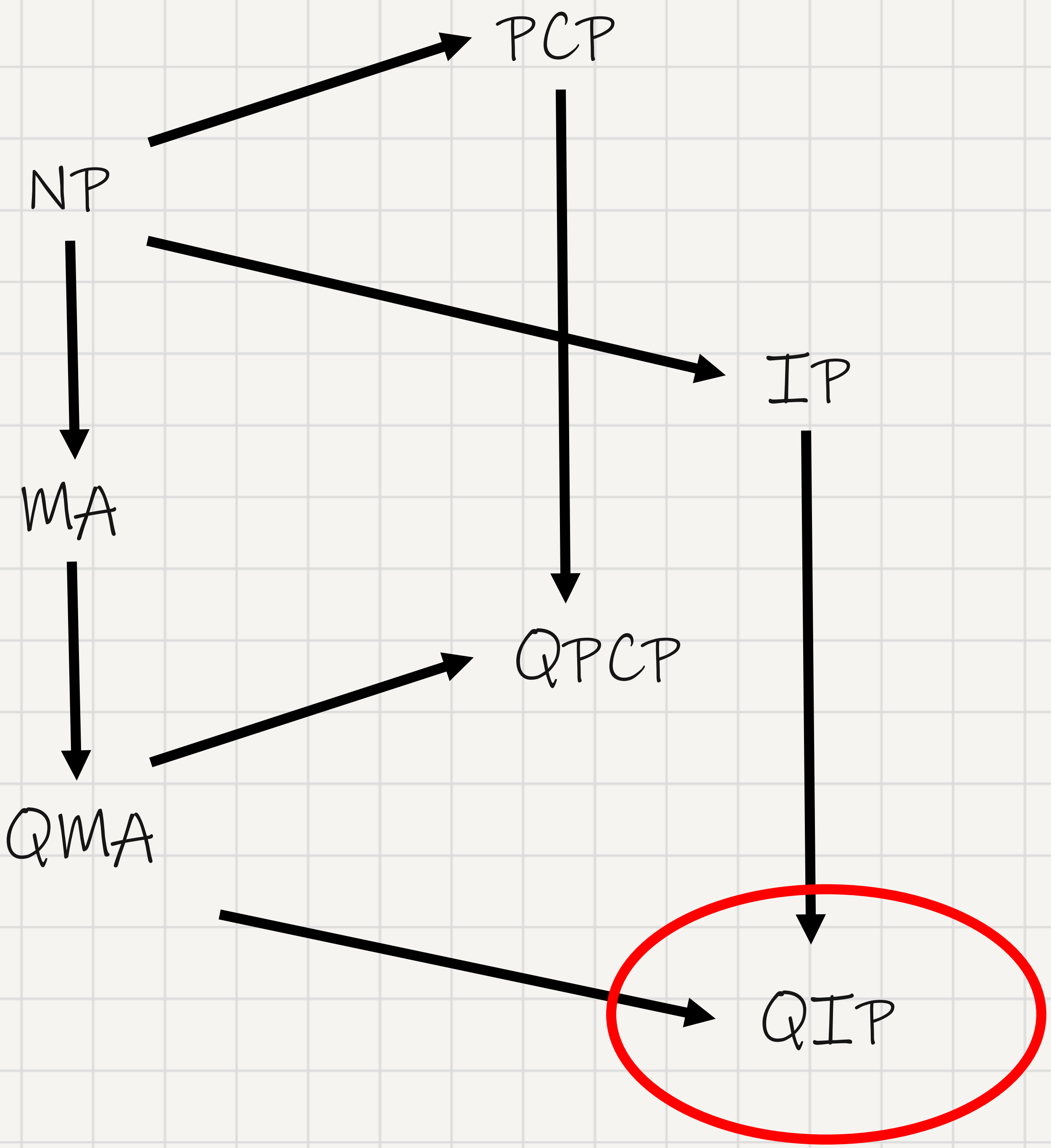
Multiple 'interactions'

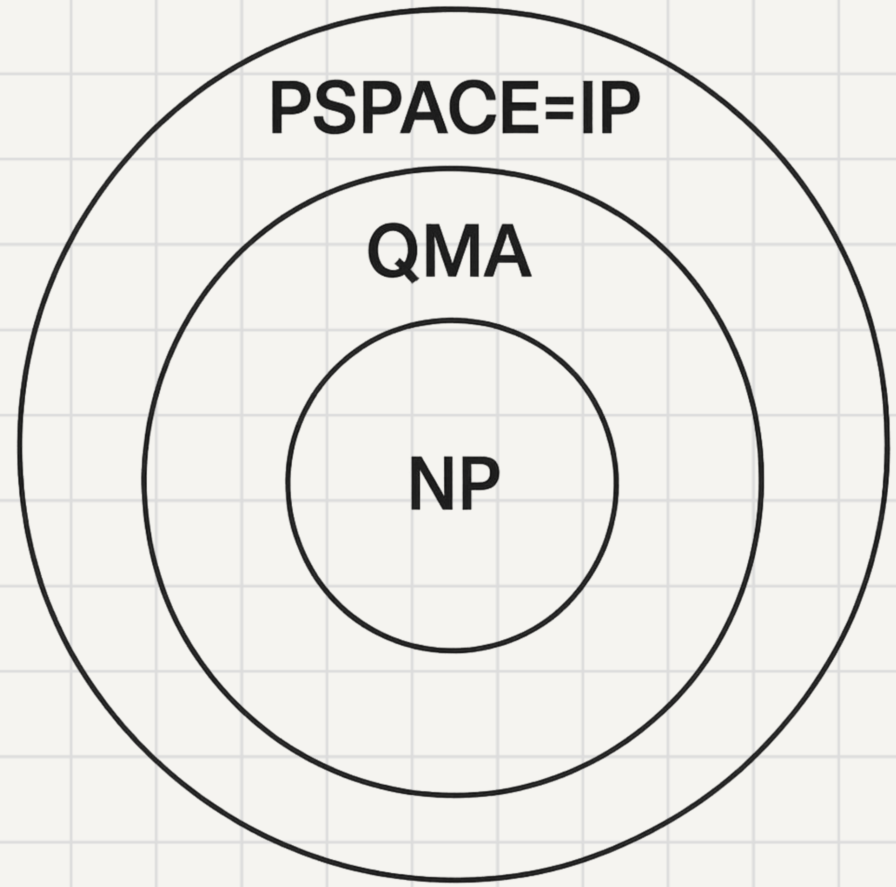


Isomorphic: Prover can do no better than guessing

Non-isomorphic: Prover always give the right answer

The big picture (so far)





Where does QIP go?

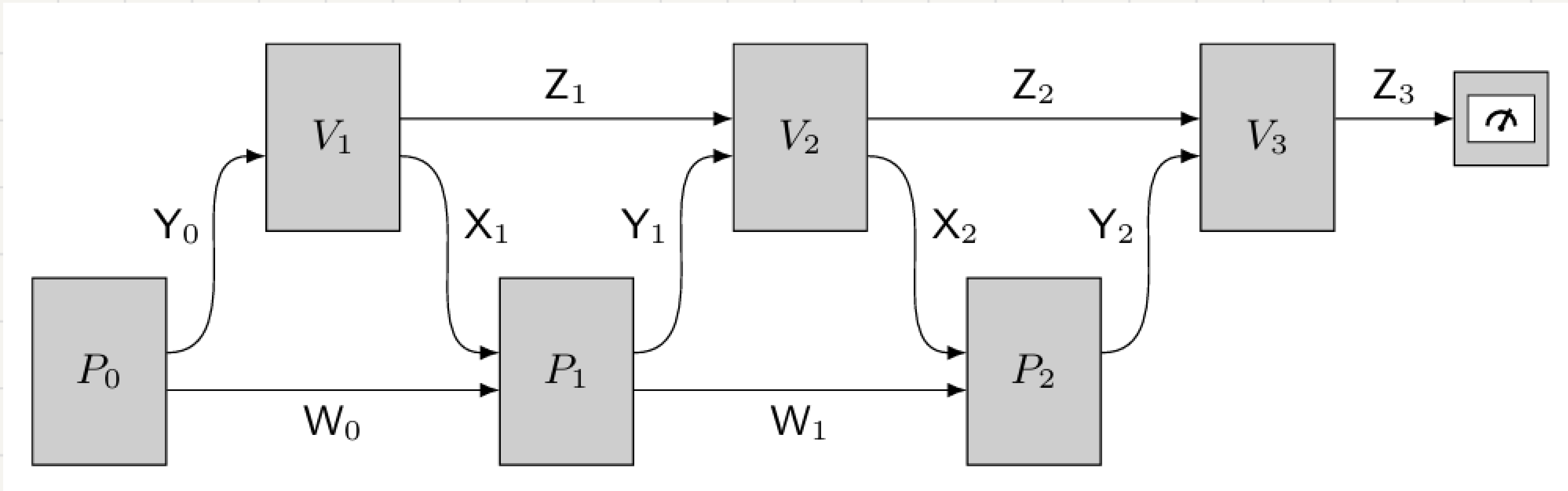
Quantum Interactive Proofs (QIP)

- Instead of sending bits, we sent *qubits*
- Sounds easy enough but...
- We cannot "read" the superposition without measuring

- How do we process between interactions?
  - Apply unitary to received state?
  - Generate a new state?
  - Generate a random state?

- Robustness of definition! All (reasonable) definitions are included in QIP

Quantum Interactive Proofs (QIP)… More formally



We can think of each turn as applying a function

$$P_i\colon \mathcal{W}_{\mathrm{i}-1} \otimes \mathcal{X}_{\mathrm{i}} \longrightarrow \mathcal{W}_{\mathrm{i}} \otimes \mathcal{Y}_{\mathrm{i}} V_i\colon \mathcal{Z}_{\mathrm{i}-1} \otimes \mathcal{Y}_{\mathrm{i}-1} \rightarrow \mathcal{Z}_{\mathrm{i}} \otimes \mathcal{X}_{\mathrm{i}}$$

No requirements on the dimensions! Only need to be physically valid

$QIP_{a,b}[m]$:

1. There is a m-turn verifier that
2. If $\mathbf{x} \in \mathbf{Accept}$, there exist P that $\omega(V) \geq a$
3. If $\mathbf{x} \notin \mathbf{Accept}$, for all P we have $\omega(V) \leq b$

Quote of the Day

I cannot define the real problem, therefore I suspect there's no real problem, but I'm not sure there's no real problem.

- Richard Feynman

Good and bad news

- Bad news: $\mathrm{QIP} = \mathrm{IP}$

  No quantum computational advantage :(

- Good news: $\mathrm{QIP} = \mathrm{QIP}[3]$

  Quantum practical advantage!

QIP = IP: Proof sketch

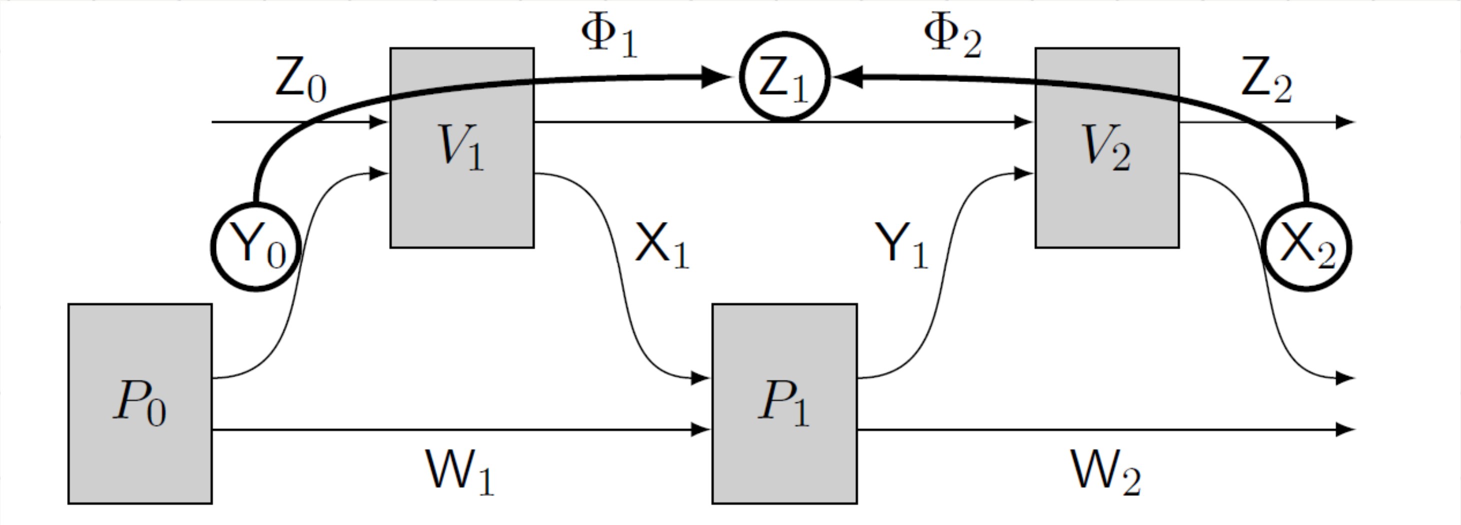
- IP $\subseteq$ QIP: straightforward
- QIP $\subseteq$ IP: less so; occurs by QIP $\subseteq$ PSPACE

Key steps:

1. Restrict attention to 3-turn quantum verifiers
2. Convert to min-max semi-definite programming problem
3. Approximate with matrix multiplicative weights update
4. (Show that all steps are implementable in PSPACE)

QIP = IP: Proof sketch (cont'd)

2. Convert to min-max semi-definite programming problem



$$\Psi_1, \Psi_2 \in \mathrm{C}(\mathcal{Y}_0, \mathcal{X}_2)$$

$$\Psi_1 = \Phi_1 \otimes \mathrm{Tr}$$

$$\Psi_2 = \mathrm{Tr} \otimes \Phi_2$$

$$\Xi = \Psi_2 - \Psi_1$$

$$\eta = \min_{\rho \in \mathrm{D}(\mathcal{Y}_0, \mathcal{X}_2)} \max_{\Pi \in \mathrm{Proj}(\mathcal{Z}_1)} \langle \Pi, \Xi \rangle$$

3. Approximate with matrix multiplicative weights update

Accept if $\eta = 0$ Reject if $\eta \geq 1/2$

QIP = QIP[3]: proof sketch

Key Steps:

1. Prove $QIP_{a,b}[m] \subseteq QIP_{1,c}[m+2]$ (Perfect completeness)
2. Prove $QIP_{1,c}[m] \subseteq QIP_{1,d}[3]$ (Parallelization)
3. Prove $QIP_{1,d}[3] \subseteq QIP_{1,d^k}[3]$ (Parallel repetition)

1. Perfect completeness: The three-step gadget

First m rounds: Behave the same, but don't measure

After round m: Pseudo-copy with isometry $|00\rangle\langle 0| + |11\rangle\langle 1|$

Send all qubits except one from pseudo-copy to P

After round m+1: V receives one qubit, combine with one it has

Measure against $\sqrt{1-\alpha}|00\rangle + \sqrt{\alpha}|11\rangle$

QIP = QIP[3]: proof sketch (cont'd)

2. Parallelization of interactions

Assuming the interaction is purified and we have perfect completeness...

$$U_{PV} = V_m P_m V_{m-1} P_{m-1} \cdots V_1 P_1$$
$$p_{acc} = Tr\left(\Pi_{acc} U_{PV} \rho_0 U_{PV}^{\dagger}\right).$$

Splitting into "forward" and "backward"

$$V_{fwd} = V_m V_{m-1} \cdots V_1, \qquad V_{bwd} = V_1^{\dagger} V_2^{\dagger} \cdots V_m^{\dagger}$$

"Verifier steps are reversible", therefore

$$\max_{U_P} Tr\left(\Pi_{acc} V_{bwd} U_P V_{fwd} \rho_0 V_{fwd}^{\dagger} U_P^{\dagger} V_{bwd}^{\dagger}\right) = p_{acc}$$

QIP = QIP[3]: proof sketch (cont'd)

3. Parallel Repetition

Classically... Run multiple interactions/experiments

How do we repeat runs in quantum?
Run k copies in parallel!

$$p_{acc}^{(k)} = \max_{U_P} Tr\left(\Pi_{acc}^{\otimes k} U_{PV}^{\otimes k} \rho_0^{\otimes k} U_{PV}^{\otimes k \dagger}\right)$$

Claim: this satisfies $\omega\left(V^{\otimes k}\right) = \omega(V)^k$

Therefore: $QIP_{a,b}[m] \subseteq QIP_{a^k,b^k}[m]$

Summary

- Interactive Proof System
- **Quantum** Interactive Proof System

- QIP = PSPACE = IP
- QIP = QIP[3]

What's next

- MIP*
- QZK

The end

Any questions?

(we are not limited to 3 rounds of interactions)