Quantum vs Classical Proofs

Shelby Kimmel (Middlebury College)
Bill Fefferman (U. Chicago)

Proceedings of MFCS 2018
Arxiv/1510.06750

Middlebury

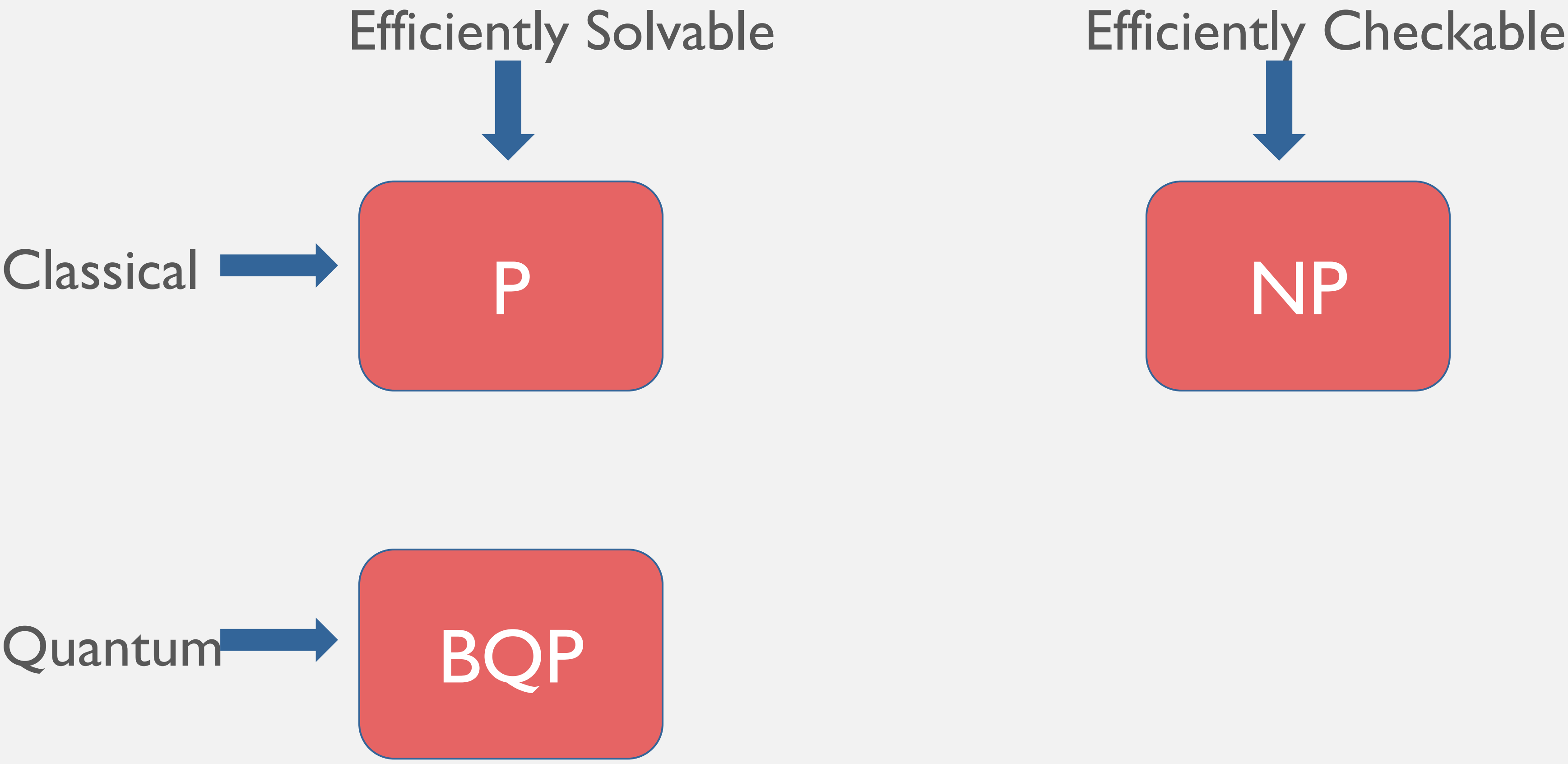
P vs NP vs BQP

P

NP

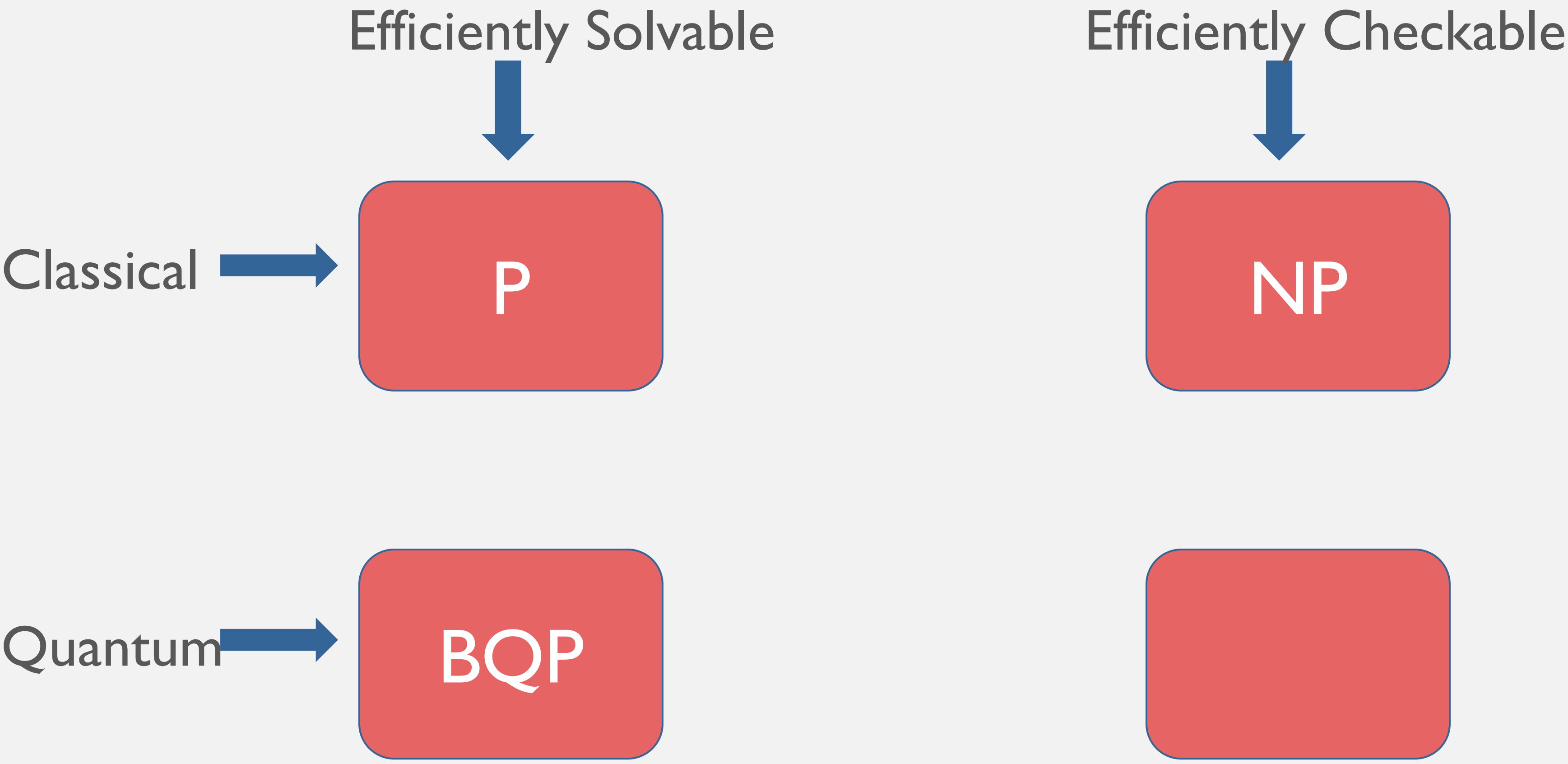
BQP

P vs NP vs BQP



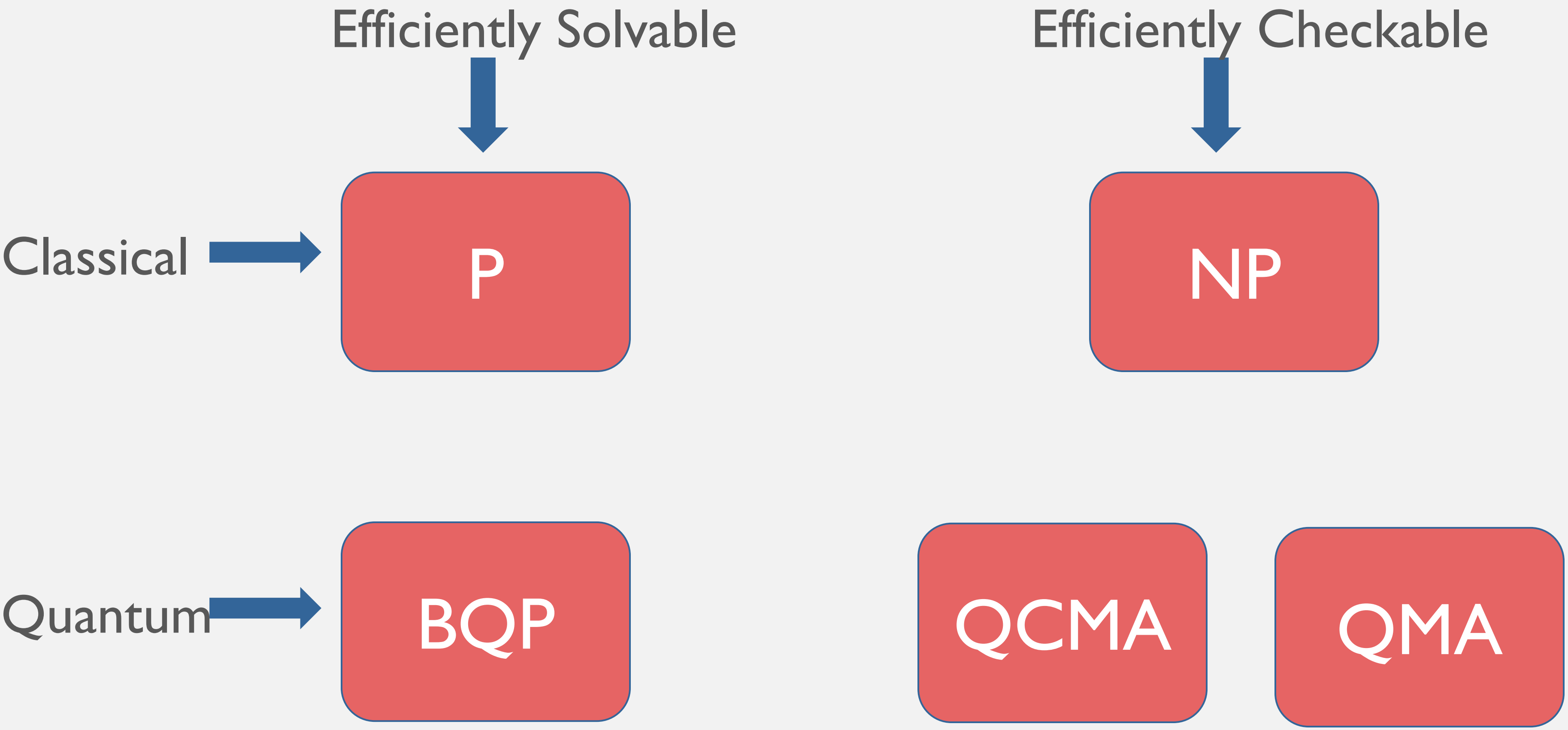
Efficiently Solvable
Efficiently Checkable
Classical
P
NP
Quantum
BQP

P vs NP vs BQP

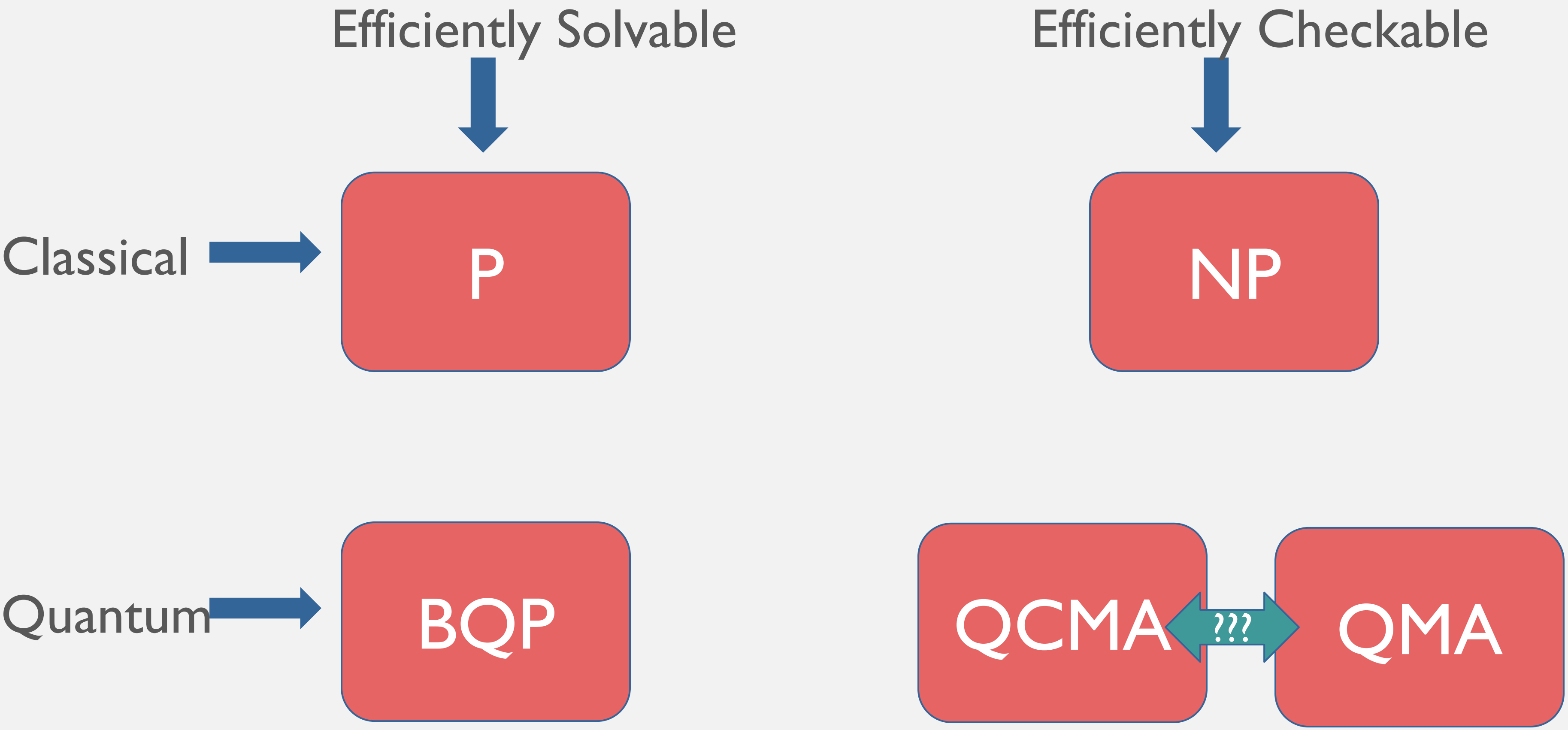


Efficiently Solvable
Efficiently Checkable
Classical
Quantum
P
NP
BQP

P vs NP vs BQP


Efficiently Solvable
Efficiently Checkable
Classical
Quantum
P
NP
BQP
QCMA
QMA

P vs NP vs BQP



Computational power of quantum state vs classical state?

Outline

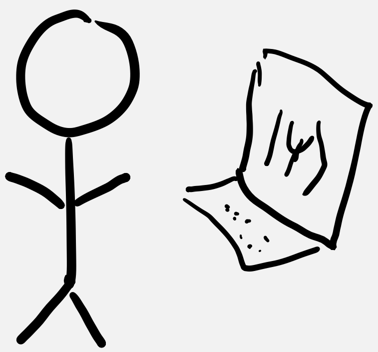
1. QMA and QCMA (what? why?)
2. Our approach to differentiating them

Informal Definitions

- QMA (Quantum Merlin Arthur)

Arthur
"I have a question – is the answer yes or no?"

e.g. Does this local Hamiltonian have a low energy state?



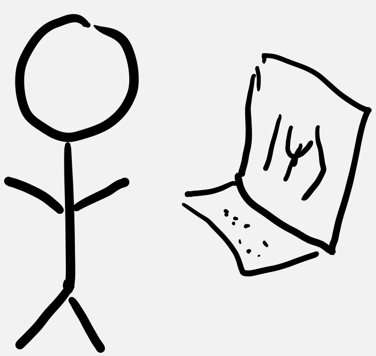
Informal Definitions

- QMA (Quantum Merlin Arthur)

Arthur
"I have a question – is the answer yes or no?"

e.g. Does this local Hamiltonian have a low energy state?

Merlin
"The answer is *yes*. Here is a quantum state (proof) to convince you."



$|\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$

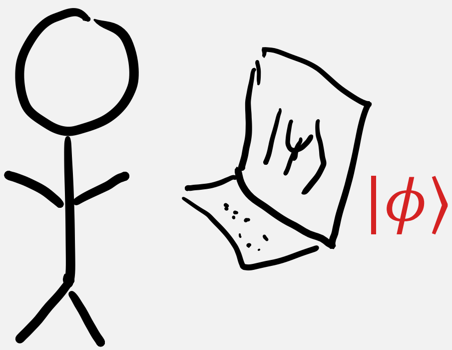
$n \sim$ size of problem

Informal Definitions

- QMA (Quantum Merlin Arthur)

Arthur
"I have a question – is the answer yes or no?"

e.g. Does this local Hamiltonian have a low energy state?



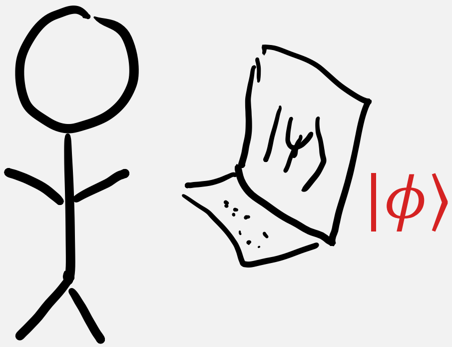
"I don't trust Merlin, but I can use $|\phi\rangle$ as input to my quantum computer to verify he is telling the truth."

Informal Definitions

- QMA (Quantum Merlin Arthur)

Arthur
"I have a question – is the answer yes or no?"

e.g. Does this local Hamiltonian have a low energy state?



QMA:
Class of problems where if answer is

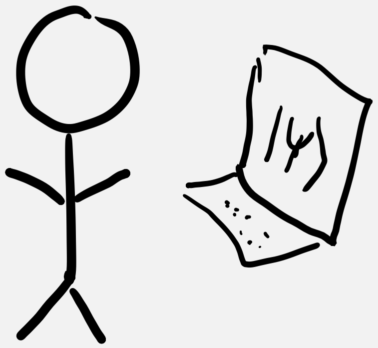
- YES, ∃ q. state that convinces Arthur with high probability
- NO, ∄ a q. state that convinces Arthur with high probability

Informal Definitions

- QCMA (Quantum Classical Merlin Arthur)

Arthur
“I have a question – is
the answer yes or no?”

e.g. Does this local Hamiltonian
have a low energy state?



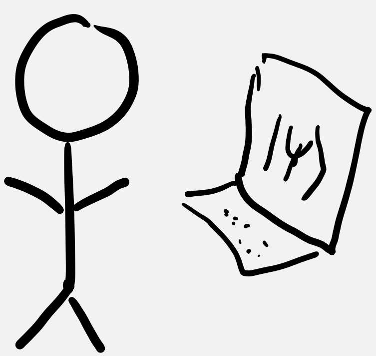
Informal Definitions

- QCMA (Quantum Classical Merlin Arthur)

Arthur
"I have a question – is the answer yes or no?"

e.g. Does this local Hamiltonian have a low energy state?

Merlin
"The answer is *yes*. Here is a **classical** state (proof) to convince you."



$s \in \{0,1\}^n$

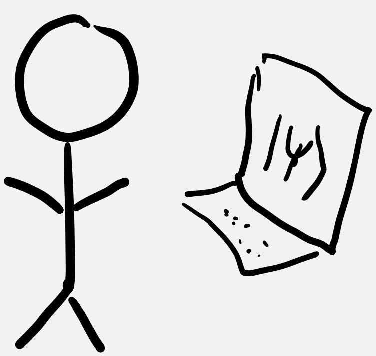
n~size of problem

Informal Definitions

- QCMA (Quantum Classical Merlin Arthur)

Arthur
"I have a question – is the answer yes or no?"

e.g. Does this local Hamiltonian have a low energy state?



s

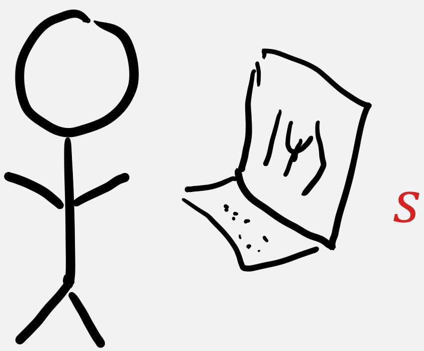
"I don't trust Merlin, but I can use s as input to my quantum computer to verify he is telling the truth."

Informal Definitions

- QCMA (Quantum Classical Merlin Arthur)

Arthur
"I have a question – is the answer yes or no?"

e.g. Does this local Hamiltonian have a low energy state?



QCMA:
Class of problems where if answer is
- YES, ∃ c. state Merlin can send that convinces Arthur with high probability
- NO, ∄ a c. state that convinces Arthur with high probability

Why Important

"Does this local Hamiltonian have a low energy state?":

In QMA [Kitaev '02]
The quantum proof is just the low energy state if it exists.

Why Important

"Does this local Hamiltonian have a low energy state?":

In QMA [Kitaev '02]
The quantum proof is just the low energy state if it exists.

Not known if in QCMA
Would imply there is a classical description of low energy states of local Hamiltonians.

Why Important

QMA vs QCMA

What is the relative computational power of quantum and classical states?

Our Goal

Show QCMA is less powerful than QMA.
(i.e. there are problems that you can verify with a quantum proof that you can't verify with a classical proof.)

Our Goal

Show QCMA is less powerful than QMA.
(i.e. there are problems that you can verify with a quantum proof that you can't verify with a classical proof.)

But proving this directly is HARD.

Our Goal

Show QCMA is less powerful than QMA.
(i.e. there are problems that you can verify with a quantum proof that you can't verify with a classical proof.)

But proving this directly is HARD.

Instead, will try to show $\mathrm{QCMA}^{\mathrm{O}}$ is less powerful than $\mathrm{QMA}^{\mathrm{O}}$.

- (With an oracle)
- Less impressive, but still interesting.

Oracle

In addition to the quantum computer, Arthur has a black box unitary operation O.

Oracle

In addition to the quantum computer, Arthur has a black box unitary operation O.

In-place Quantum Oracle:

Let $f: \{1,2, \ldots M\} \to \{1,2, \ldots, M\}$ be a bijective function.

Standard basis states (in-place oracle permutes states)

$$|x\rangle \to \boxed{O_f} \to |f(x)\rangle$$

Oracle

In addition to the quantum computer, Arthur has a black box unitary operation O.

In-place Quantum Oracle:

Let $f: \{1,2, \ldots M\} \rightarrow \{1,2, \ldots, M\}$ be a bijective function.

Standard basis states (in-place oracle permutes states)

$$|x\rangle \rightarrow \boxed{O_f} \rightarrow |f(x)\rangle$$

- Has classical counterpart (encodes classical function)

Previous result by Aaronson and Kuperberg ('07)` proved separation with an oracle without a classical analog.

Outline

1. QMA and QCMA (what? why?)
2. Our approach to differentiating them

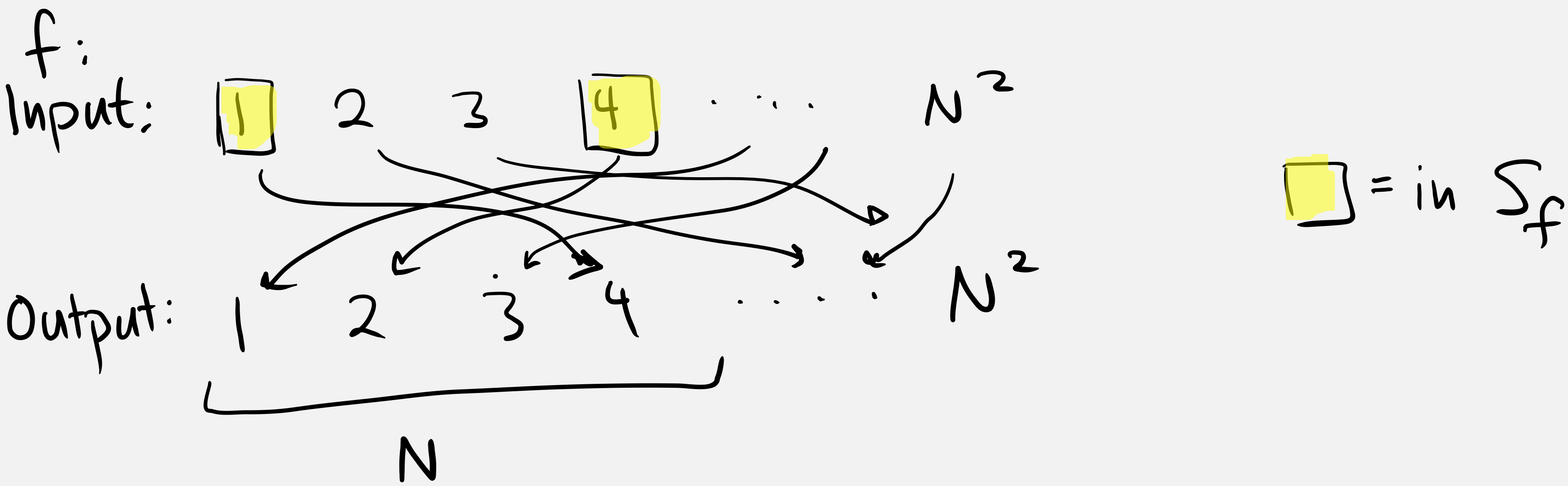
Our Yes-No Question

Intuition: Want a problem where quantum proof is a superposition of an exponentially large number of states.

Our Yes-No Question

Setup:

- Given oracle O_f with $f: [N^2] \to [N^2]$
- Let $S_f = \{i: f(i) \in [N]\} =$ "preimage subset"
- Is S_f mostly even? (Promised either mostly even or mostly odd)



Our Yes-No Question

Setup:

- Given oracle O_f with $f: [N^2] \to [N^2]$
- Let $S_f = \{i: f(i) \in [N]\} =$ "preimage subset"
- Is S_f mostly even? (Promised either mostly even or mostly odd)

This problem is in $\mathsf{QMA}^{\mathsf{O}}$ (with an in-place oracle O_f)

Our Yes-No Question

Setup:

- Given oracle O_f with $f\colon [N^2] \to [N^2]$
- Let $S_f = \{i \colon f(i) \in [N]\} =$ "preimage subset"
- Is S_f mostly even? (Promised either mostly even or mostly odd)

If "Yes"

- Merlin provides superposition of preimage subset states
- Arthur either
  - Measures in standard basis, gets even outcome with high probability.
  - Applies O_f and measures whether he got the superposition of the first N standard basis states. Succeeds with probability 1.

Our Yes-No Question

Setup:

- Given oracle O_f with $f: [N^2] \to [N^2]$
- Let $S_f = \{i: f(i) \in [N]\} =$ "preimage subset"
- Is S_f mostly even? (Promised either mostly even or mostly odd)

If "No":

- Merlin sends any state (on $n = \log{(N^2)}$ qubits)
- Arthur either
  - Measures in standard basis, gets even outcome with probability p_1.
  - Applies O_f and measures whether he got the superposition of the first N standard basis states. Succeeds with probability p_2.
- We show p_1 and p_2 can't both be large.

In-Place Oracle Problem

Approach to proving problem is not in $QCMA^O$

- A short classical proof can't contain enough information to convince Arthur about properties of a nearly structureless exponentially large subset.

In-Place Oracle Problem

Approach to proving problem is not in $QCMA^{O}$

- Use **Adversary Method** to show can't efficiently distinguish YES from NO instances..

In-Place Oracle Problem

Approach to proving problem is not in $QCMA^{O}$

- Use **Adversary Method** to show can't efficiently distinguish YES from NO instances.
- Merlin's proof complicates Adversary Method…

In-Place Oracle Problem

Approach to proving problem is not in $QCMA^O$

- Use **Adversary Method** to show can't efficiently distinguish YES from NO instances.
- Merlin's proof complicates Adversary Method…
- Use **Pigeon Hole Principle** to show one proof corresponds to a large number of permutations – by restricting to only those permutations we can ignore proof and use the Adversary Method.

In-Place Oracle Problem

Approach to proving problem is not in $\mathrm{QCMA}^{\mathrm{O}}$

- Use **Adversary Method** to show can't efficiently distinguish YES from NO instances.
- Merlin's proof complicates Adversary Method…
- Use **Pigeon Hole Principle** to show one proof corresponds to a large number of permutations – by restricting to only those permutations we can ignore proof and use the Adversary Method.
- Adapt Adversary Method to in-place and probabilistic oracles.

Other applications

We prove an oracle separation between QCMA and AM.

Our approach works in general for proving subset-based oracle problems, (including standard oracle problems), are not in QCMA.

Summary and Open Problems

- A quantum proof can be more powerful than a classical proof.

Summary and Open Problems

- A quantum proof can be more powerful than a classical proof.
  - Intuition: a quantum proof can contain information about an exponentially large set via superposition, while a classical prof can't.
  - Grilo, Kerenidis, Sikora '15: QMA proof can always be a subset state

Summary and Open Problems

- Remove probabilistic oracle? (Less Hard – artifact of proof techniques)
- Separation without an oracle? (Extremely Hard)
- QCMA<QMA using a standard oracle? (Hard)
- Find an oracle problem where standard oracle is exponentially better than in-place (opposite is known) (Less Hard)