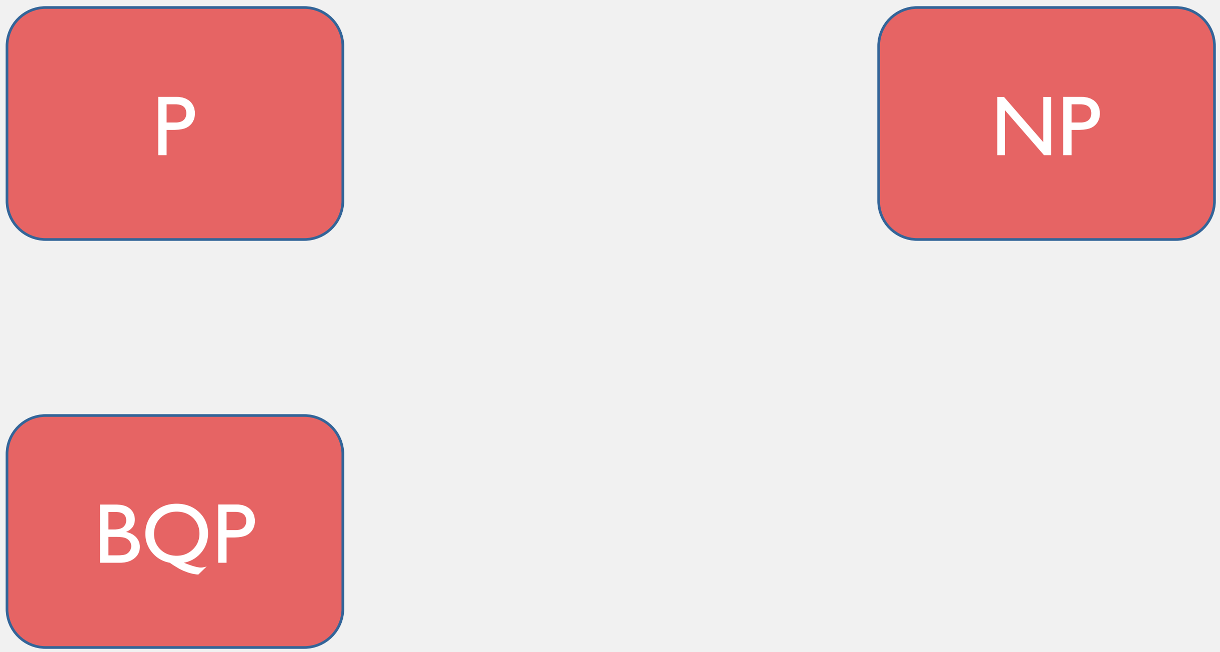
Quantum vs Classical Proofs

Shelby Kimmel (Middlebury College)
Bill Fefferman (UC Berkeley, NIST)

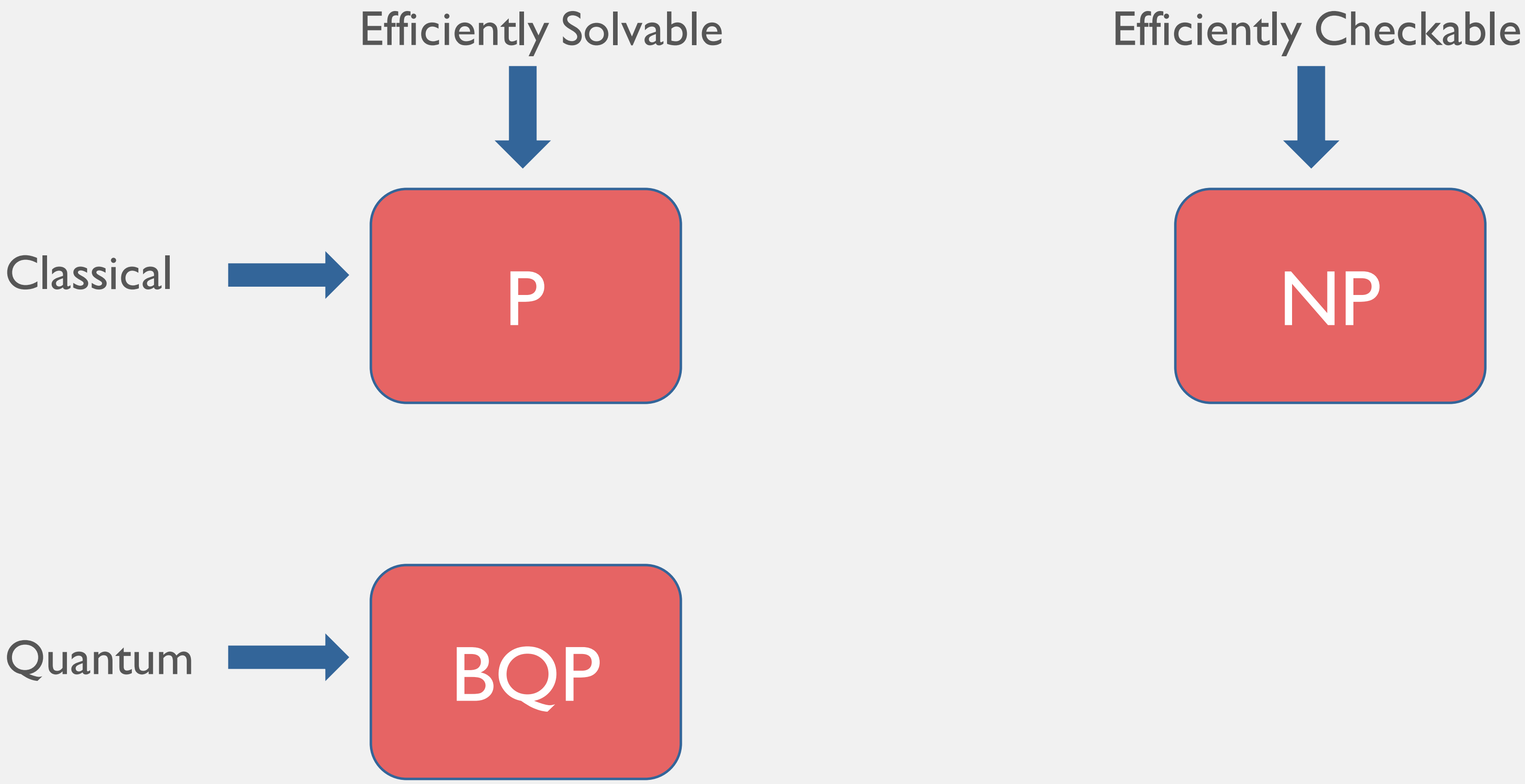
Arxiv/1510.06750

Middlebury

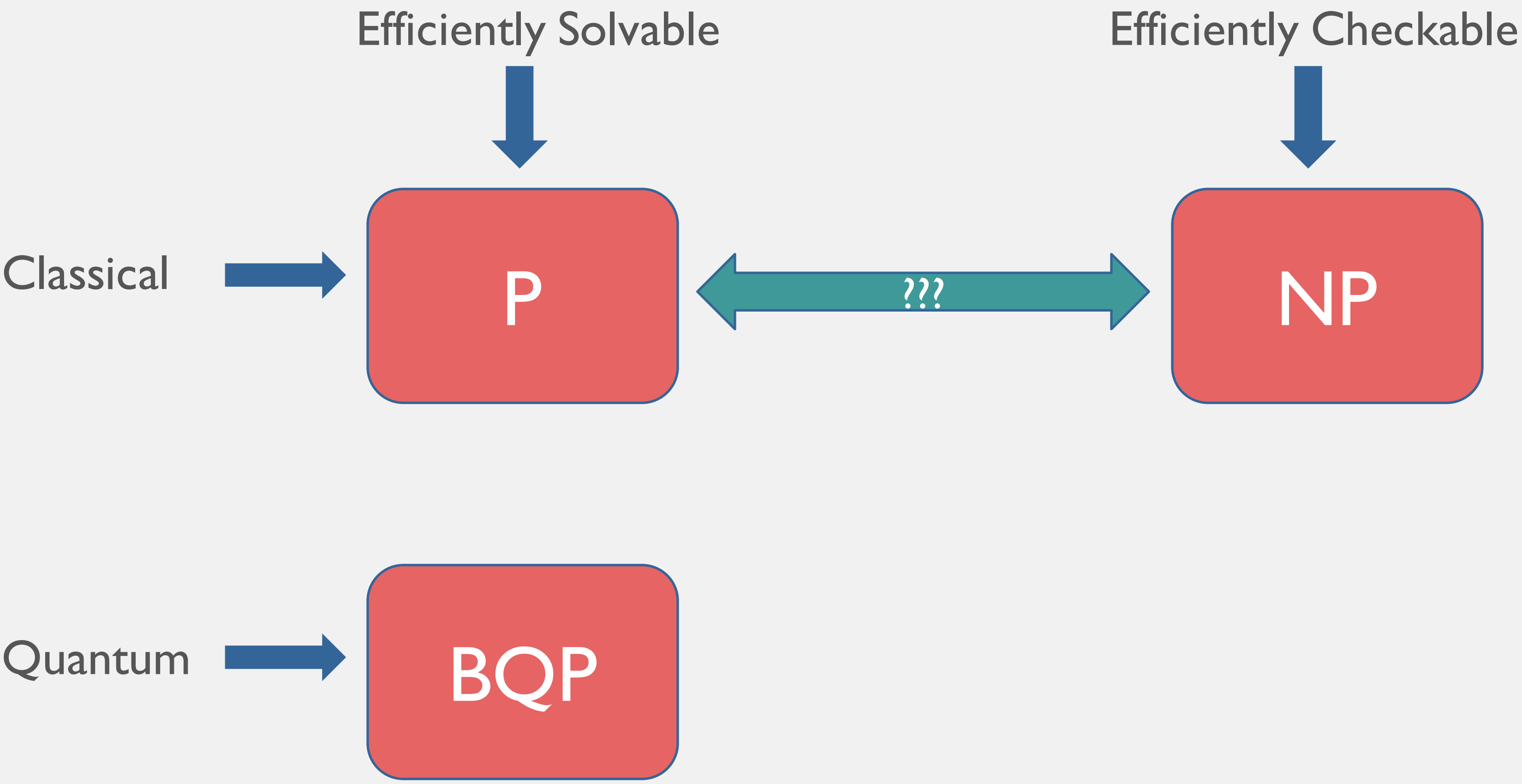
P vs NP vs BQP



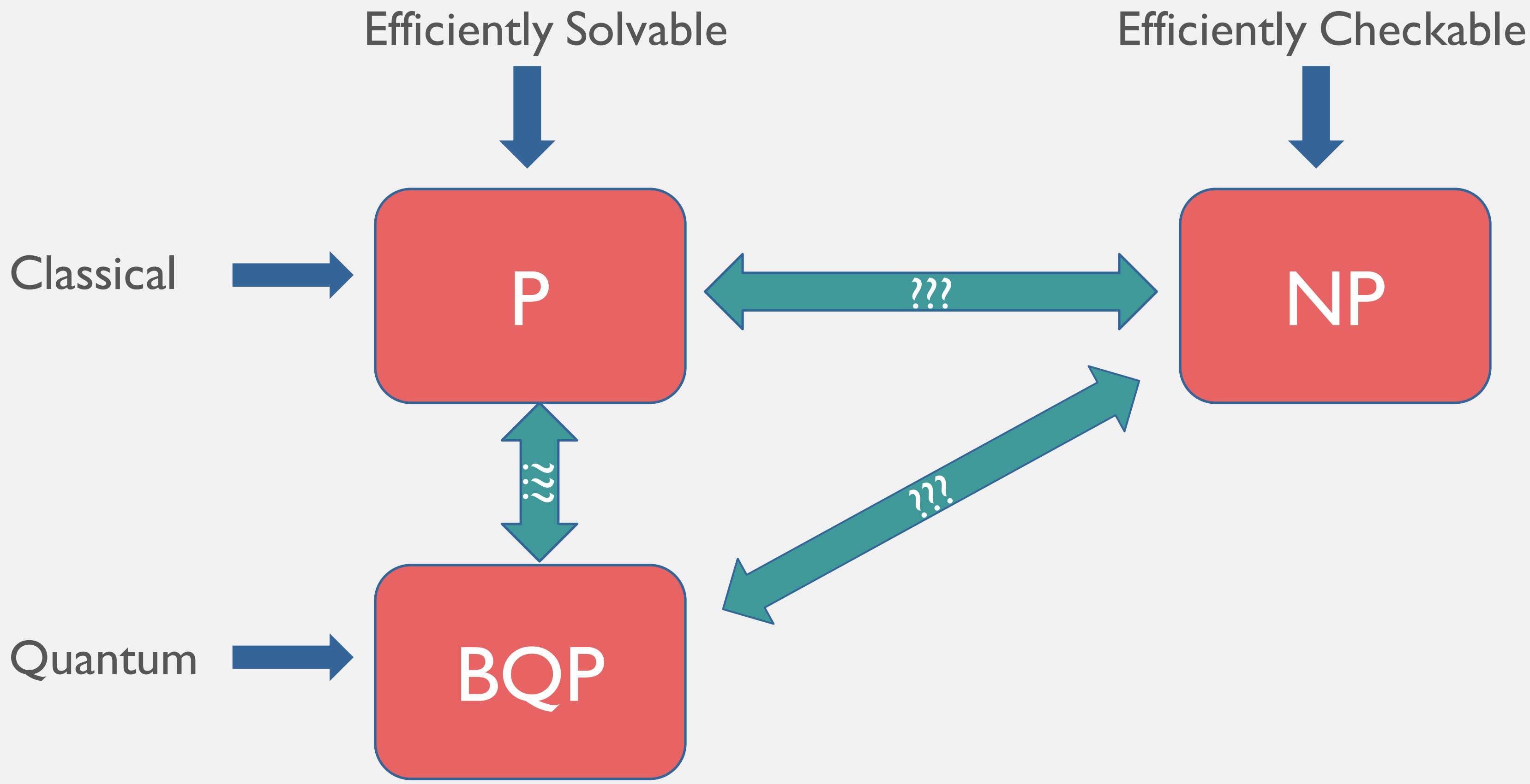
P vs NP vs BQP


Efficiently Solvable
Efficiently Checkable
Classical
P
NP
Quantum
BQP

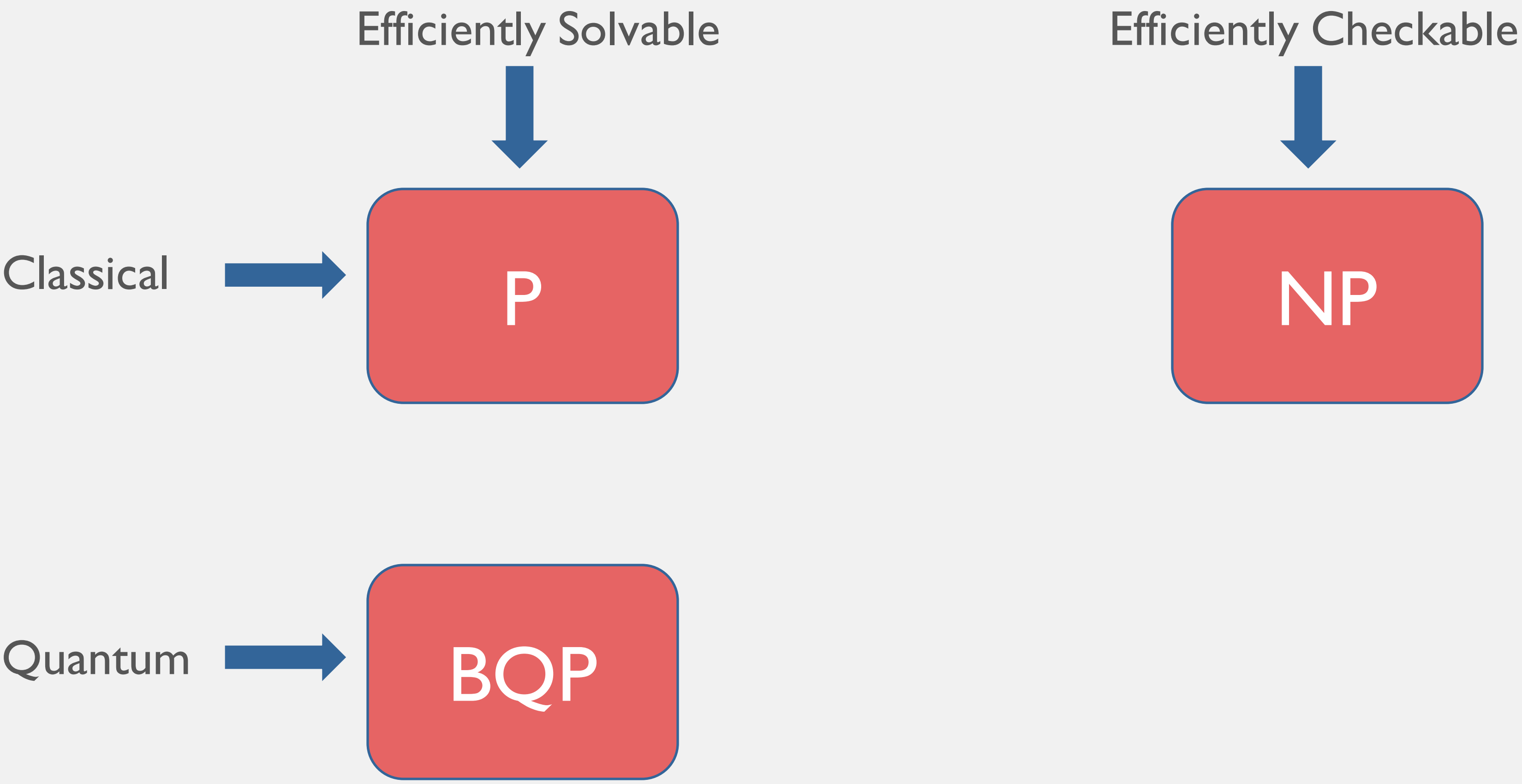
P vs NP vs BQP


Efficiently Solvable
Efficiently Checkable
Classical
P
???
NP
Quantum
BQP

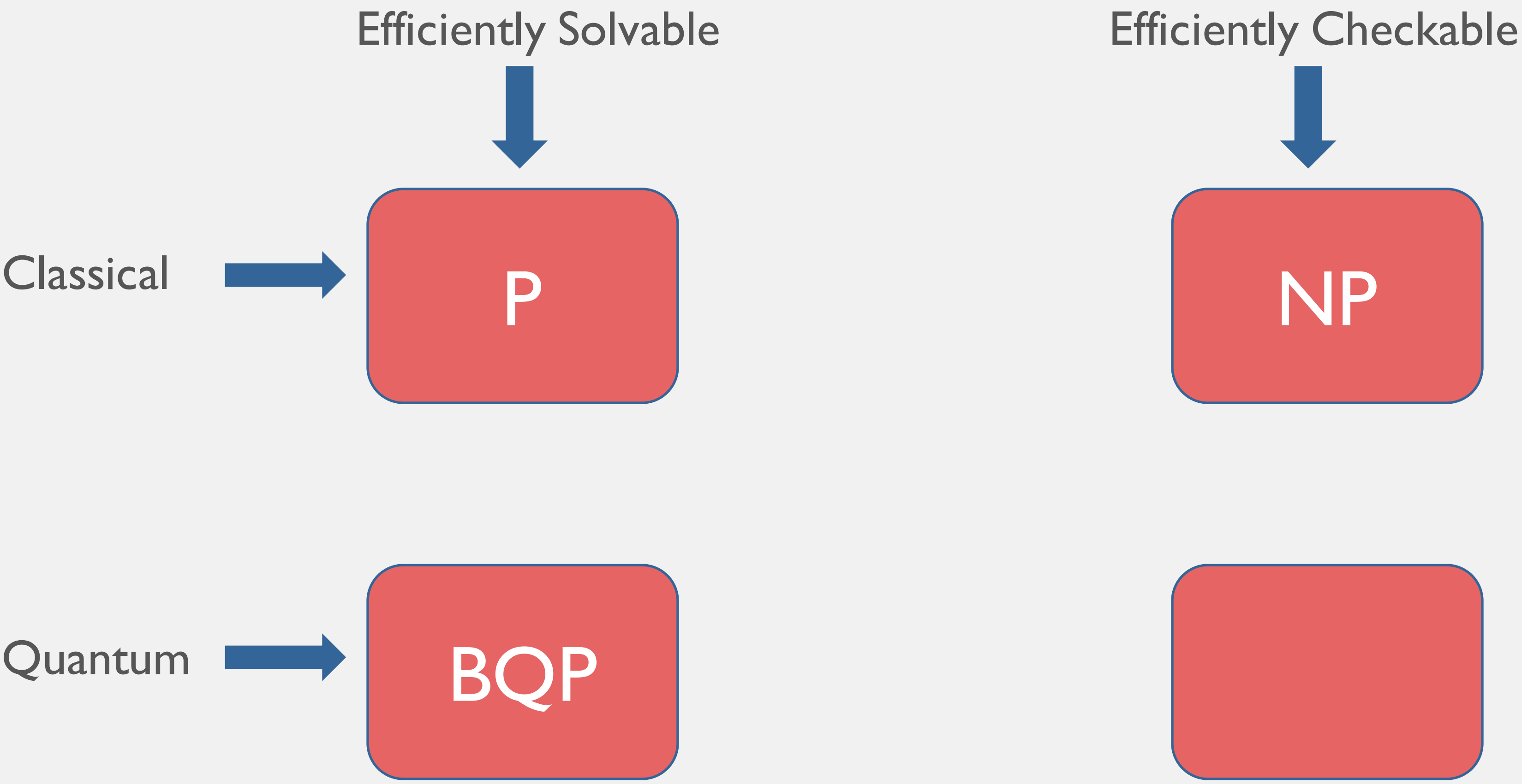
P vs NP vs BQP


Efficiently Solvable
Efficiently Checkable
Classical
Quantum
P
NP
BQP
???
???
???

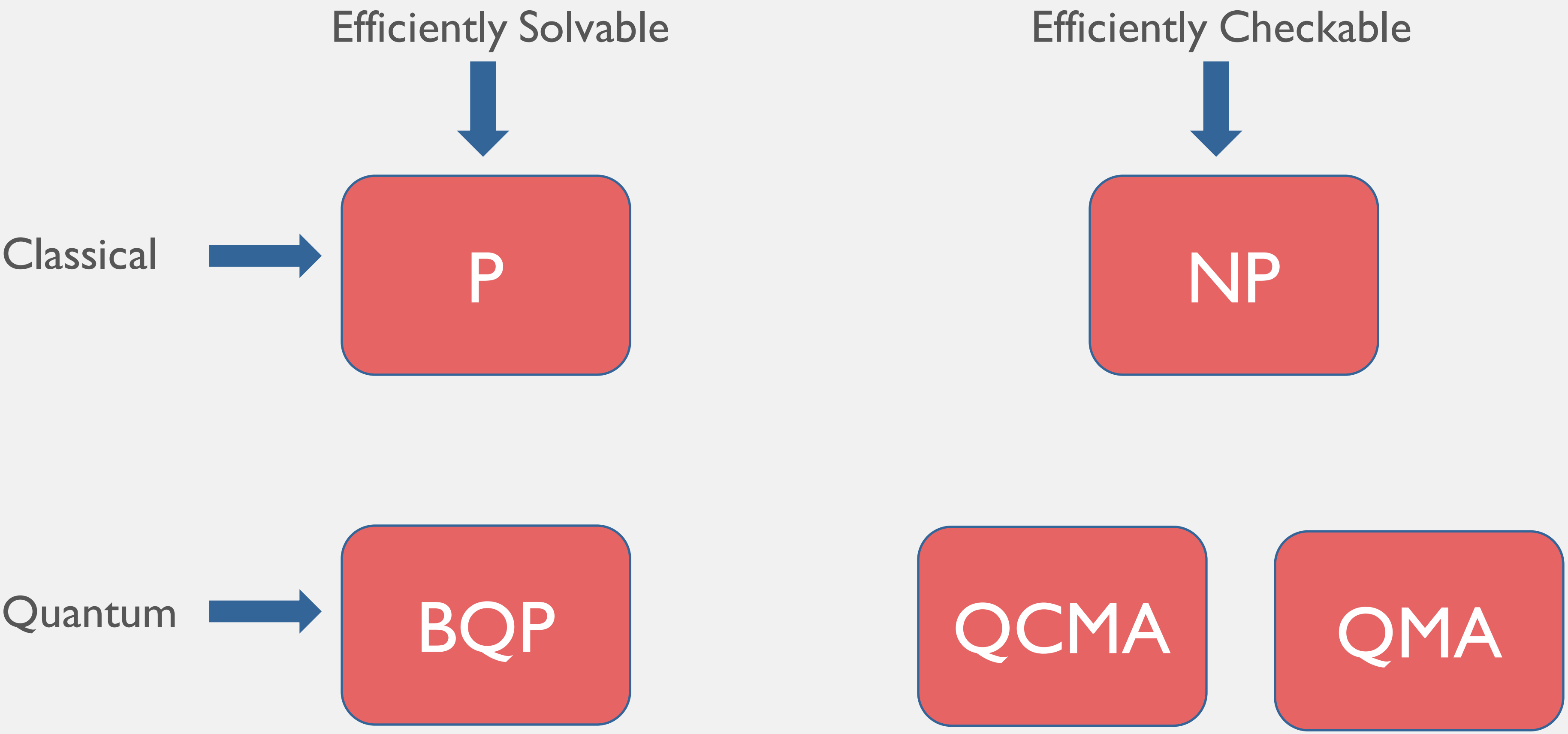
P vs NP vs BQP


Efficiently Solvable
Efficiently Checkable
Classical
P
NP
Quantum
BQP

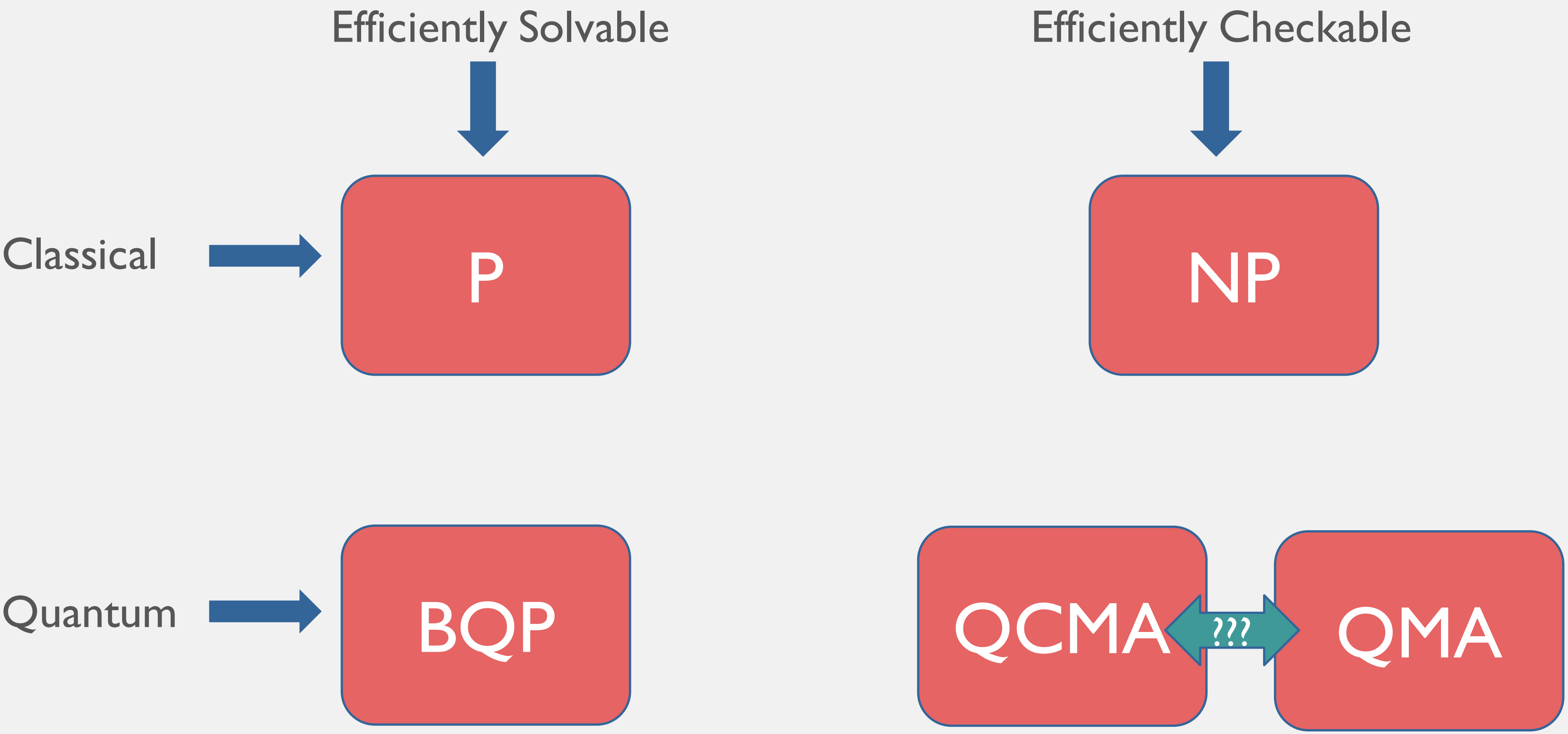
P vs NP vs BQP


Efficiently Solvable
Efficiently Checkable
Classical
Quantum
P
NP
BQP

P vs NP vs BQP


Efficiently Solvable
Efficiently Checkable
Classical
P
NP
Quantum
BQP
QCMA
QMA

P vs NP vs BQP



What computational power do you gain from a quantum state vs a classical state?

Outline

1. QMA and QCMA (what are they and why do we care?)
2. Oracle separations
3. Our approach

(Rough) Definitions

1. QMA (Quantum Merlin Arthur)

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

e.g. Does this local Hamiltonian (that I have a classical description of) have a low energy state?

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

$|\phi\rangle \in \mathbb{C}^n$

(Rough) Definitions

1. QMA (Quantum Merlin Arthur)

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

e.g. Does this local Hamiltonian (that I have a classical description of) have a low energy state?

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

$|\phi\rangle \in \mathbb{C}^n$

n is O(size of problem description)

(Rough) Definitions

1. QMA (Quantum Merlin Arthur)

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

e.g. Does this local Hamiltonian (that I have a classical description of) have a low energy state?

$|\phi\rangle$

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

(Rough) Definitions

1. QMA (Quantum Merlin Arthur)

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

e.g. Does this local Hamiltonian (that I have a classical description of) have a low energy state?

QMA:

Class of problems where if answer is
- YES, $\exists$ q. state Merlin can send that convinces Arthur with high probability
- NO, $\nexists$ a q. state that convinces Arthur with high probability

$|\phi\rangle$

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

(Rough) Definitions

1. QCMA (Quantum Classical Merlin Arthur)

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

e.g. Does this local Hamiltonian (that I have a classical description of) have a low energy state?

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

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

(Rough) Definitions

1. QCMA (Quantum Classical Merlin Arthur)

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

e.g. Does this local Hamiltonian (that I have a classical description of) 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 is O(size of problem description)

(Rough) Definitions

1. QCMA (Quantum Classical Merlin Arthur)

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

e.g. Does this local Hamiltonian (that I have a classical description of) have a low energy state?

s

"I don't trust Merlin, but I can use this bit string as input to my quantum computer and try to verify that he is telling the truth."

(Rough) Definitions

1. QCMA (Quantum Classical Merlin Arthur)

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

e.g. Does this local Hamiltonian (that I have a classical description of) 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

s

"I don't trust Merlin, but I can use this bit string as input to my quantum computer and try to verify that he is telling the truth."

Why Important

“Does this local Hamiltonian have a low energy state?”: in QMA

- This means there is a quantum state that allows you to verify that there is a low energy state. (The quantum proof is just the low energy state if it exists.)
- It might be hard to find that state.
- This question is interesting to physicists

Why Important

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

- This means there is a quantum state that allows you to verify that there is a low energy state. (The quantum proof is just the low energy state if it exists.)
- It might be hard to find that state.
- This question is interesting to physicists

"Does this local Hamiltonian have a low energy state?": not known if in QCMA

- If it was this would mean there is a classical description of low energy states of local Hamiltonians.
- This question is interesting to physicists

Why Important

QMA vs QCMA ~
What is the relative computational power of quantum and classical states?

This question is interesting to most of us.

Why Important

QMA vs QCMA $\sim$
What is the relative computational power of quantum and classical states?

This question is interesting to most of us.

Holevo's Theorem: n qubits can't communicate more than n bits of information

But in our scenario, only trying to communicate 1 bit, given a bunch of extra information.

Our Goal

We will try to 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

We will try to 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

We will try to 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 $QCMA^O$ is less powerful than QMA^O.

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

Outline

1. QMA and QCMA (what are they and why do we care?)
2. Oracle separations
3. Our approach

Oracle

Classical Oracle: $x \rightarrow \boxed{f} \rightarrow f(x)$

Standard Quantum Oracle: $|x\rangle|b\rangle \rightarrow \boxed{f} \rightarrow |x\rangle|b \oplus f(x)\rangle$

In-place Quantum Oracle: $|x\rangle \rightarrow \boxed{f} \rightarrow |f(x)\rangle$

Only possible if f is a permutation

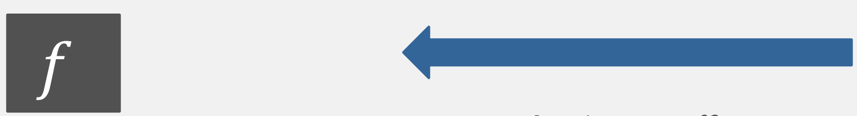
Generic Quantum Oracle: $|x\rangle \rightarrow \boxed{U} \rightarrow U|x\rangle$

(Rough) Definitions

1. QMA^{O} (Quantum Merlin Arthur)

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

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



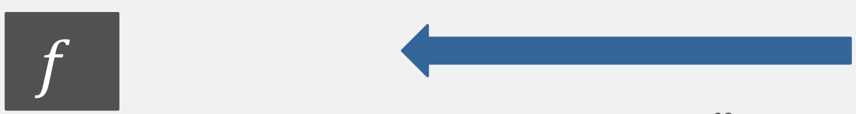
$|\phi\rangle \in \mathbb{C}^n$

(Rough) Definitions

1. QCMA^O (Quantum Merlin Arthur)

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

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



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

Hierarchy of Oracles

Standard Quantum Oracle: $|x\rangle|b\rangle \rightarrow$ f $\rightarrow |x\rangle|b \oplus f(x)\rangle$

Gold standard of oracles.

- 1-to-1 mapping to classical oracles (encodes classical function)
- Easy to reverse

Hierarchy of Oracles

In-place Quantum Oracle:

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

Pretty good oracle

- Has classical counterpart (encodes classical permutation)
- Not easily reversible

Hierarchy of Oracles

Generic Quantum Oracle:

$$|x\rangle \rightarrow \boxed{U} \rightarrow U|x\rangle$$

Not the best oracle

- No classical counterpart
- Not always easily reversible

Hierarchy of Oracles

Generic Quantum Oracle:

$$|x\rangle \rightarrow \boxed{U} \rightarrow U|x\rangle$$

Not the best oracle

- No classical counterpart
- Not always easily reversible

Aaronson and Kuperberg '07 proved $\mathrm{QCMA}^{\mathrm{O}} < \mathrm{QMA}^{\mathrm{O}}$ with this type of oracle (oracle based on Haar random state)

Hierarchy of Oracles

In-place Quantum Oracle:

$|x\rangle \rightarrow$ f $\rightarrow |f(x)\rangle$

Pretty good oracle

- Has classical counterpart (encodes classical function)
- Not easily reversible

We show a QMA-QCMA separation using an In-place Oracle*

*probabilistic

Hierarchy of Oracles

Standard Quantum Oracle:

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

Gold standard of oracles.

- Easy to reverse
- Has classical counterpart (encodes classical function)

Open question: is a QMA-QCMA separation possible with a standard quantum oracle?

Outline

1. QMA and QCMA (what are they and why do we care?)
2. Oracle Separations
3. Our approach

In-Place Oracle Problem

Setup:

- Let $f: [N^2] \rightarrow [N^2]$ be a permutation
- Let $S_f = \{i: f(i) \in [N]\}$ = "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

In-Place Oracle Problem

Setup:

- Let $f: [N^2] \to [N^2]$ be a permutation
- Let $S_f = \{i: f(i) \in [N]\} =$ "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

In-Place Oracle Problem

Setup:

- Let $f: [N^2] \rightarrow [N^2]$ be a permutation
- Let $S_f = \{i: f(i) \in [N]\} =$ "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

Problem would be easy if Arthur had oracle for f^{-1}

In-Place Oracle Problem

Setup:

- Let $f\colon [N^2] \to [N^2]$ be a permutation
- Let $S_f = \{i\colon f(i) \in [N]\} =$ "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

In-Place Oracle Problem

Setup:

- Let $f: [N^2] \to [N^2]$ be a permutation
- Let $S_f = \{i: f(i) \in [N]\}$ = "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

This problem is in $\mathrm{QMA}^{\mathrm{O}}$

In-Place Oracle Problem

Setup:

- Let $f: [N^2] \rightarrow [N^2]$ be a permutation
- Let $S_f = \{i: f(i) \in [N]\} =$ "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

If YES:

- Merlin sends $|\phi\rangle = \frac{1}{\sqrt{N}} \sum_{i \in S_f} |i\rangle$ (on $n = \log(N^2)$ qubits)
- With probability $1/2$, Arthur measures in standard basis, will get even outcome with probability $2/3$.
- With probability $1/2$, Arthur applies oracle to $|\phi\rangle$ and tries to project into $\frac{1}{\sqrt{N}} \sum_{i \in [N]} |i\rangle$, will succeed with probability 1.

In-Place Oracle Problem

Setup:

- Let $f: [N^2] \rightarrow [N^2]$ be a permutation
- Let $S_f = \{i: f(i) \in [N]\}$ = "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

If No:

- Merlin sends any state $|\phi\rangle$ (on $n = \log(N^2)$ qubits)
- With probability 1/2, Arthur measures in standard basis, will get even outcome with probability p_1.
- With probability 1/2, Arthur applies oracle to $|\phi\rangle$ and tries to project into $\frac{1}{\sqrt{N}} \sum_{i \in [N]} |i\rangle$, will succeed with probability p_2.
- We show p_1 and p_2 can't both be large.

In-Place Oracle Problem

Setup:

- Let $f: [N^2] \to [N^2]$ be a permutation
- Let $S_f = \{i: f(i) \in [N]\}$ = "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

This doesn't work with a standard quantum oracle because there is no way to catch Merlin if he tries to trick Arthur if the answer is no. There is no way to verify that Merlin sends a subset state.

In-Place Oracle Problem

Setup:

- Let $f: [N^2] \to [N^2]$ be a permutation
- Let $S_f = \{i: f(i) \in [N]\}$ = "preimage subset"
- We are promised that either more than 2/3 (YES) or less than 1/3 (NO) of the elements of S_f are even.
- Arthur is given an in-place oracle for f, wants to know which is the case.

This problem is not in QCMA^{O}

Intuition: Using n bits, Merlin needs to convince Arthur about properties of an exponentially large number of elements (N is exponentially large in n)

In-Place Oracle Problem

This problem is not in QCMA^{O}

- Fewer classical proofs s than possible functions f

In-Place Oracle Problem

This problem is not in $QCMA^O$

- Fewer classical proofs s than possible functions f
- Exists a proof that is optimal for lots of functions f (pigeon hole).

In-Place Oracle Problem

This problem is not in QCMA^O

- Fewer classical proofs s than possible functions f
- Exists a proof that is optimal for lots of functions f (pigeon hole).
- Restrict our attention to functions that correspond to this proof.

In-Place Oracle Problem

This problem is not in QCMA^{O}

- Fewer classical proofs s than possible functions f
- Exists a proof that is optimal for lots of functions f (pigeon hole).
- Restrict our attention to functions that correspond to this proof.
- Use adversary method: there is a subset of YESs that can't be distinguished from NOs without an exponentially large uses of the oracle (heart of the proof).

In-Place Oracle Problem

This problem is not in $QCMA^{O}$

- Fewer classical proofs s than possible functions f
- Exists a proof that is optimal for lots of functions f (pigeon hole).
- Restrict our attention to functions that correspond to this proof.
- Use adversary method: there is a subset of YESs that can't be distinguished from NOs without an exponentially large uses of the oracle (heart of the proof).
- In order to get the proof to work, oracle is probabilistic (changes with each use)

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

- 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.

- Remove probabilistic oracle? (Less Hard – artifact of proof techniques)
- 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)
- Separation without an oracle? (Extremely Hard)