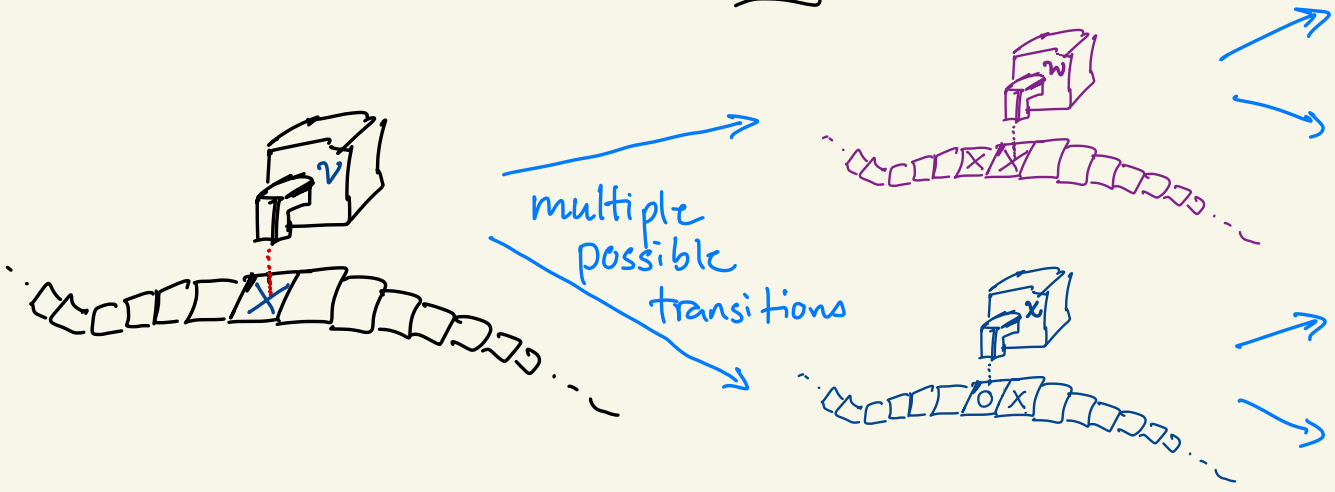
What is the correct notion of Quantum NP?

Or oracle separations between QMA and QCMA

Chinmay Nirkhe (UW & IBM)
based on joint work with Anand Natarajan (MIT)

NP has many defs. of equal comp. power

① Non-deterministic Turing Machine



accept if any path of T.M. accepts

② Prover + Deterministic Verifier Interaction.

Merlin ← an arbitrarily powerful computational machine that is untrustworthy

Is $x \in \mathcal{L}$?

proof π
(aka witness)

Deterministic Arthur ← a polynomial-time in $|x|$ det. Turing machine

↳ Arthur computes $V(x, \pi)$ and outputs 1/0.

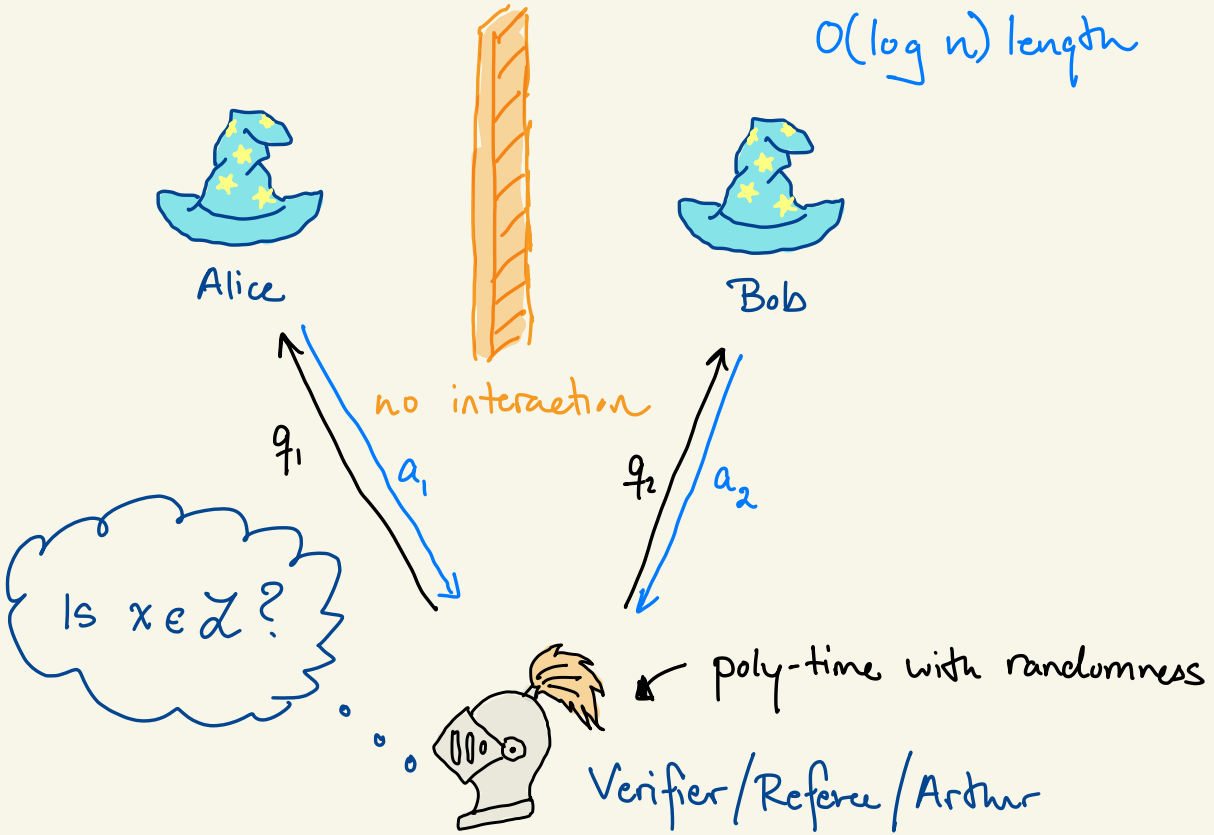
Requirements for the interaction

Completeness: If $x \in \mathcal{L}$, then $\exists$ a "honest" proof π, for which $V(x, \pi) = 1$.

Soundness: If $x \notin \mathcal{L}$, then $\forall$ proofs $\tilde{\pi}$, $V(x, \tilde{\pi}) = 0$ or equiv. Arthur detects the deceit with probability 1.

③ Multiprover Interactive Proofs with short messages

$O(\log n)$ length



Requirements for the interaction

Completeness: If $x \in \mathcal{L}$, then $\exists$ "honest" strategies for Alice and Bob s.t.

$$\Pr_{\substack{q_1, q_2, \\ A, B}} \left[V(x, q_1, q_2, a_1, a_2) = 1 \right] = 1 .$$

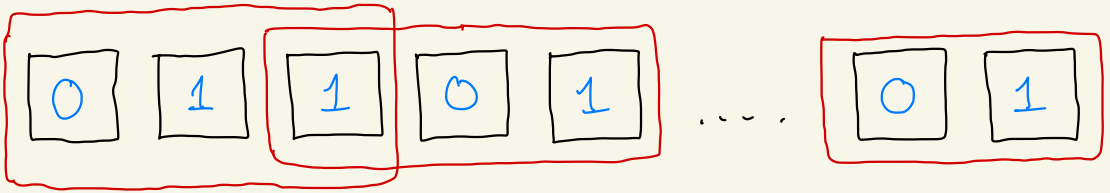
Soundness: If $x \notin \mathcal{L}$, then $\forall$ "dishonest" strategies for Alice and Bob,

$$\Pr_{\substack{q_1, q_2, \\ A, B}} \left[V(x, q_1, q_2, a_1, a_2) = 1 \right] \leq \frac{1}{3} .$$

(4) Characterization by a complete problem.

All the problems reducible to 3-SAT

or more generally, any Constraint satisfaction problem



C_i not necessarily geometrically local

local check $C_i = x_1 \oplus x_2 \oplus x_3 = 0$.

$C_i : \{0,1\}^3 \longrightarrow [0,1]$.

$C : \{0,1\}^n \longrightarrow [0,m]$ by $C(x) = \sum_{i=1}^{m} C_i(x)$

Decide if

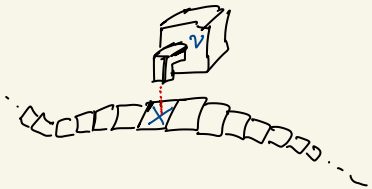
(1) $\exists\, x,\ C(x) = 0$.

(2) $\forall\, x,\ C(x) \geq 1$.

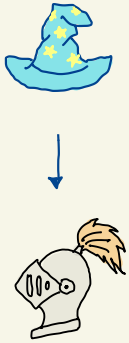
If we want to understand a quantum generalization of NP, which definition do we generalize? And how?

Punchline: Different generalizations yield different quantum complexity classes.

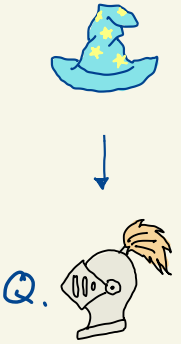
see Gharabian's survey on the 7 faces of Quantum NP.



Non-deterministic poly-time T.M. $\Rightarrow$ NQP, Q.T.M.s which accept with non-zero prob.



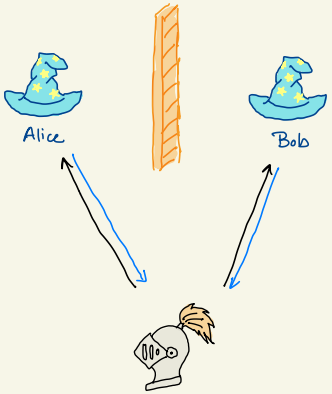
Prover + Det. Verifier $\Rightarrow$



QMA / QCMA

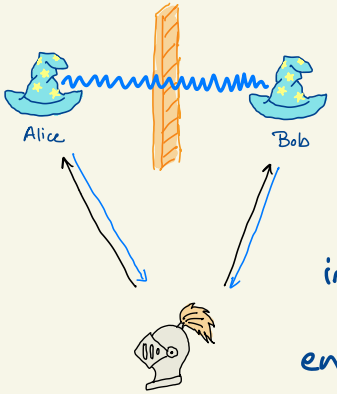
Quantum (Classical) Merlin Arthur, messages to a quantum poly-time Arthur

(Ji, Natarajan, Vidick, Wright, Yuen 2022)



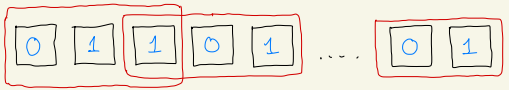
Multiprover Interactive Proofs with short messages

$\Rightarrow$



$MIP^* = RE$

short message interaction with entangled & non-communicating provers

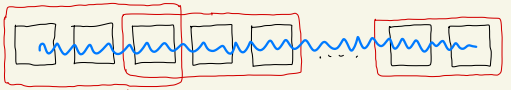


local check $C_i = x_1 \oplus x_2 \oplus x_3 = 0$.

$C_i : \{0,1\}^3 \longrightarrow [0,1]$.

Complete Problem in CSPs

$\Rightarrow$



local check $h_i = |000\rangle\langle 000| + |111\rangle\langle 111|$

$h_i : (\mathbb{C}^2)^{\otimes 3} \to \mathbb{R}$

QMA, Complete Problem in Local Hamiltonians

(aka quantum (or basis-free) analog of CSPs.

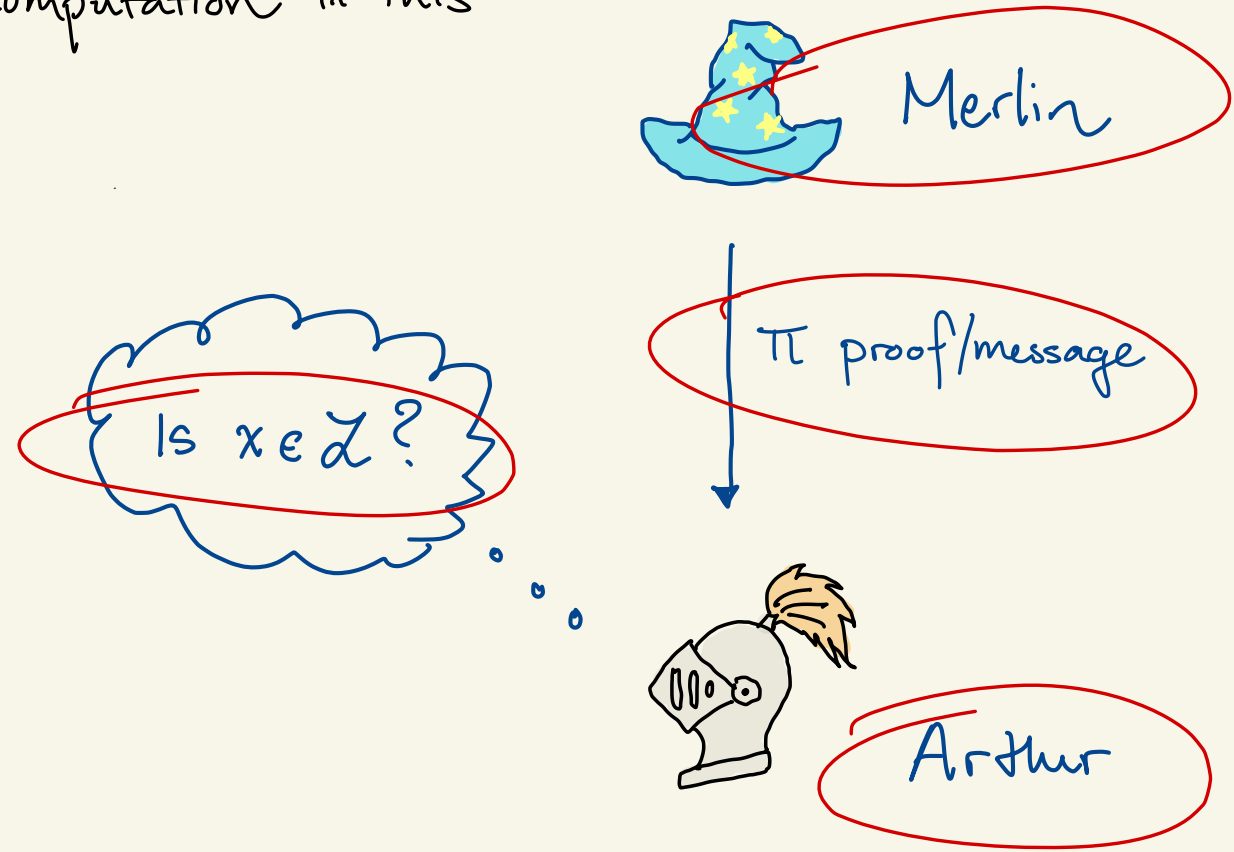
Are these different quantum analogs of NP, the same or different?

Which is the right definition?

Today, we will focus on the one prover interaction setting.

Goal: Why is this problem interesting and how can we hope to resolve it.

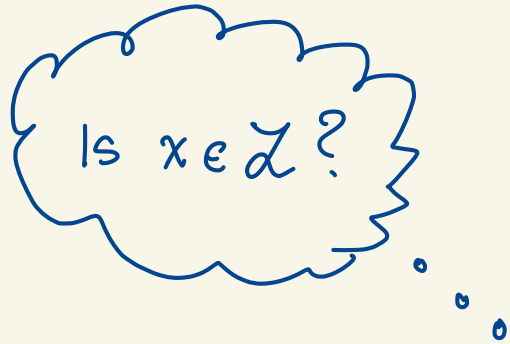
4 sites where we assumed classical information/computation in this picture.



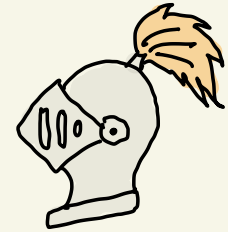
Making only Merlin quantum doesn't help unless the message is quantum

Quantum Merlin

Classical decision problem



Classical π proof/message



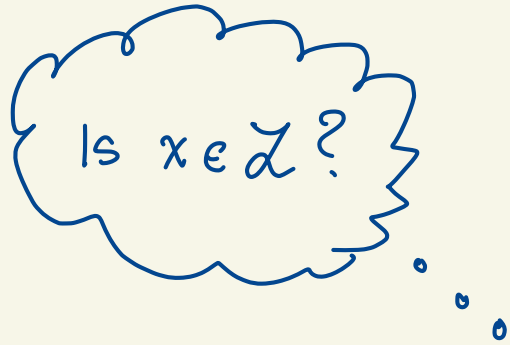
Classical Arthur

Unless Arthur is also quantum, sending him quantum messages adds no power

Quantum

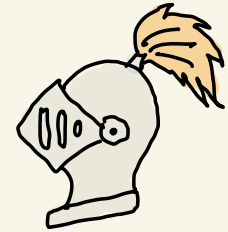
Merlin

Classical decision problem



Quantum

$|\pi\rangle$ proof/message



Classical

Arthur

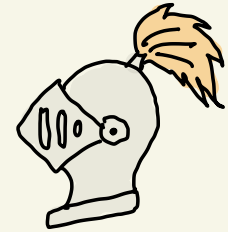
Quantum Merlin Arthur (QMA)

Quantum Merlin

Classical decision problem

Is $x \in \mathcal{L}$?

Quantum $|\pi\rangle$ proof/message



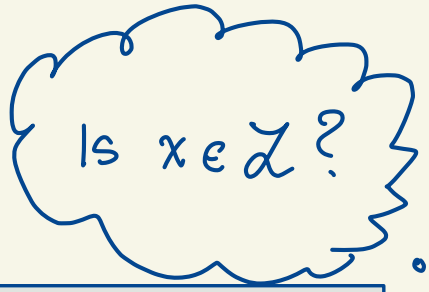
Quantum Arthur

min. amplification if we assume a quantum Merlin

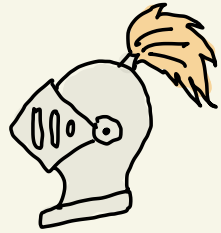
But if we only assume a quantum Arthur...

Classical Merlin

Classical decision problem



π Classical proof/message



Quantum Arthur

Quantum Merlin — Classical Arthur (QCMA)

There is one other source of classical information that we could generalize to quantum...

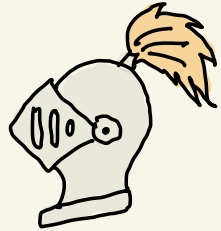
Merlin

Quantum problems

Does $|\psi\rangle$ have property P?

π proof/message

... but for another time



Quantum Arthur

$NP \subseteq MA \subseteq QCMA \subseteq QMA$

Merlin

Merlin

Merlin

Classical

π proof/message

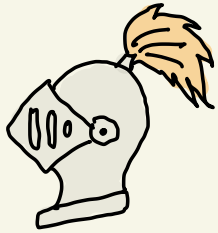
Classical

π proof/message

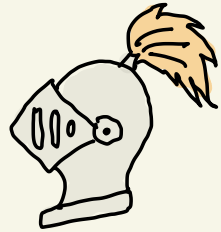
Quantum

$|\pi\rangle$ proof/message

Classical Arthur



Quantum Arthur



Quantum Arthur

Why care?

The Local Hamiltonian problem (quantum analog of Constraint Satisfaction Problems) is QMA-complete

- captures many natural problems from physics + chemistry
- solving QMA-complete problems is tantamount to being able to compute all "relevant" properties of local Hamiltonian groundstates
- if QCMA = QMA, then ∃ a classical description

of groundstates that sufficiently captures all the relevant properties.

- if QCMA ≠ QMA, then not all local Hamiltonian groundstates have short verifiable descriptions.

Corollary: If QCMA = QMA,
For the "relevant" quantum states, there exists

ex. QMA proof state

ex. local Hamiltonian groundstate

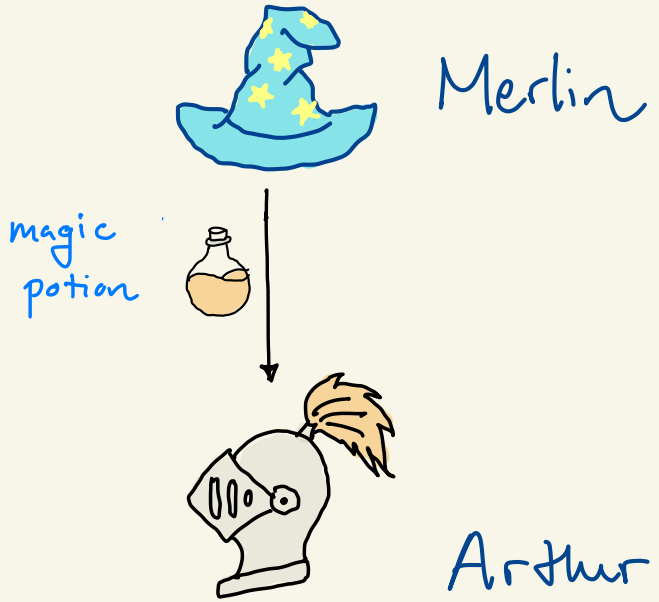
of groundstates that sufficiently captures all the relevant properties.

- if QCMA ≠ QMA, then not all local Hamiltonian groundstates have short verifiable descriptions.

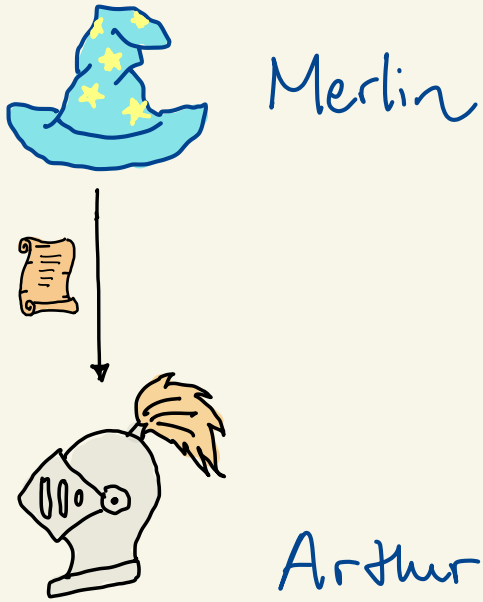
But my favorite perspective: just how magical is a quantum Merlin?

"morally" the QCMA pf can be interpreted as a classical description of the quantum state.

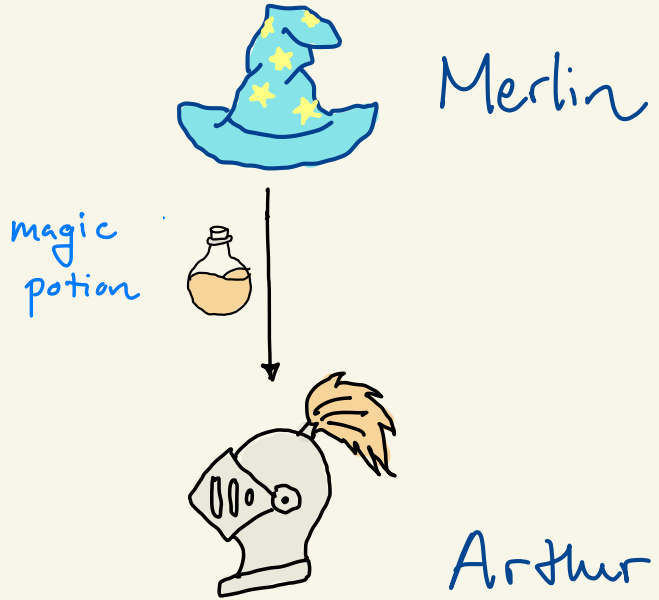
QMA



QCMA



QMA



If QCMA = QMA,

* Arthur uses  to create  and tests 

If QCMA ≠ QMA,

any  describing  must take exponential length.

i.e. Arthur can only recognize  , but he cannot write down an efficient recipe for creating  .

Constructible states:

Any state  for which there exists a poly(n) size 

i.e. outputs of poly(n) size quantum circuits

Fact There are roughly $2^{(2^n)}/\epsilon$ n-qubit quantum states.

Fact There are only $2^{\text{poly}(n)}$ many constructible states.

$\Rightarrow$ almost all states are not constructible.

QCMA v QMA asks whether all verifiable states are a subset of the set of constructible states.

i.e. if equal, even though quantum mechanics posits an exponential classical description complexity for most q. states, the subset that are verifiable and relevant have vastly simpler descriptions.

If QCMA $\neq$ QMA,

then there exist problems $(x \in \mathcal{L})$ with classical descriptions of length n, such that not all verifiable solutions have poly(n) length classical descriptions but have poly(n) qubit solutions

What's the evidence?

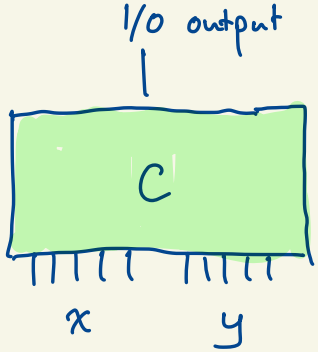
A similar paradigm appears when thinking about the complexity class NEXP.

NP	NEXP
non-det. poly time	non-det. exp time
3-color a graph	3-color a graph
G on poly(n) vertices	G on exp(n) vertices

There's a problem! How do we describe G

Notion of a succinct graph

$C : \{0,1\}^n \longrightarrow \{1,2,3\}$



$x, y \in \{0,1\}^n$

Input: circuit description $\langle C \rangle$

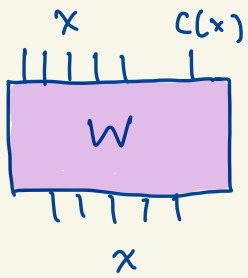
Let G be the graph defined on $V = \{0,1\}^n$ with $x \sim y \iff C(x,y) = 1$.

Output: If G is 3-colorable.

Succinct-3-Coloring is NEXP-complete

Does NEXP (equiv. Succinct-3-Coloring) have succinct solutions?

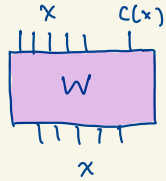
Succinct solutions



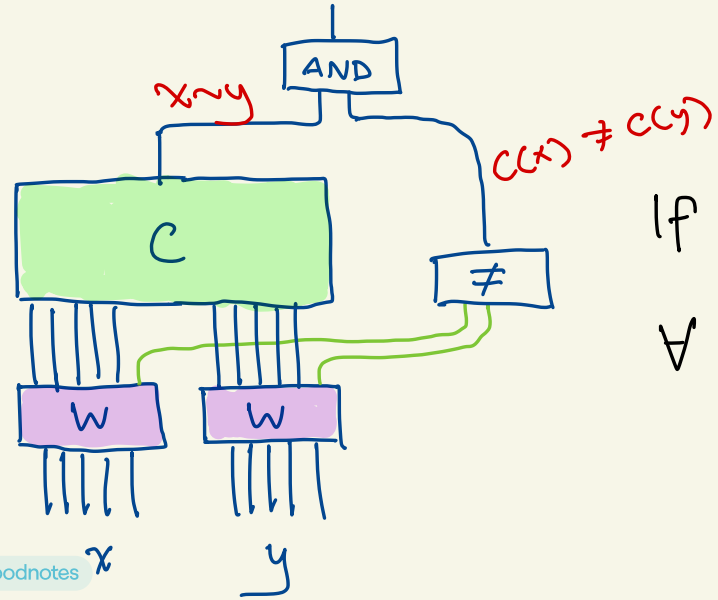
No, (Impagliazzo-Wigderson) assuming NEXP $\not\subseteq \Sigma_2 \subseteq$ PH.

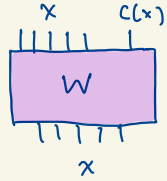
$\Rightarrow$ The solutions to NEXP-complete problems are vastly more complex to describe than the questions.

Pf (of Impagliazzo-Wigderson)

Assume a succinct solution 

always exists for 3-colorable graphs.

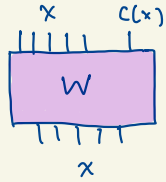


If 

is a solution, then

$\forall\, x, y,\ \mathrm{BIGCKT}(x, y) = 1.$

NEXP is reducible to

$\exists$ 

s.t. $\forall\, x, y$ $\text{BIGCKT}(x, y) = 1$

This puts the problem in $\Sigma_2 \subseteq \text{PH}$. ▨

Can we do something similar to prove that QMA doesn't have succinct solutions (i.e. = QCMA)?

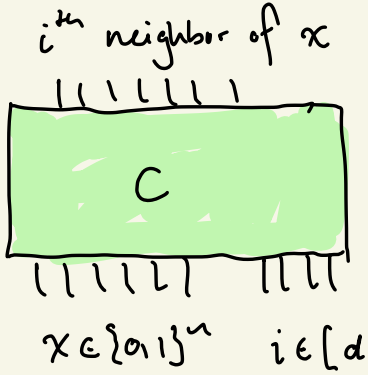
Important to note

$$P \subseteq QCMA \subseteq QMA \subseteq PSPACE.$$

So our "best" pf will need to make some complexity assumption.

Attempt (Natarajan–Nirkhe).

Let G be a d-regular graph on $\{0,1\}^n$ described succinctly by an adjacency list circuit.



Assume G is γ-expanding on each connected component.

2^{nd} eigenvalue is $\leq (1-\gamma)d$.

Then $\exists$ quantum algorithm which only accepts states

$$\propto \sum_{v \in \text{connected component } C} |v\rangle \qquad \text{for some } C.$$

and rejects all orthogonal states with probability $\geq \gamma$.

Nm—

Problem (Expansion distinguishing)

Given a graph G succinctly described in adjacency

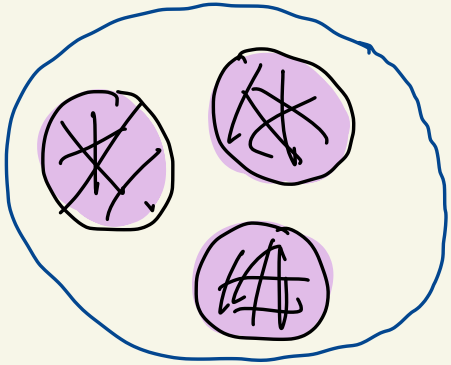
list, and some constant $\epsilon_0 > 0$ (think $\epsilon_0 = 0.01$),

decide if

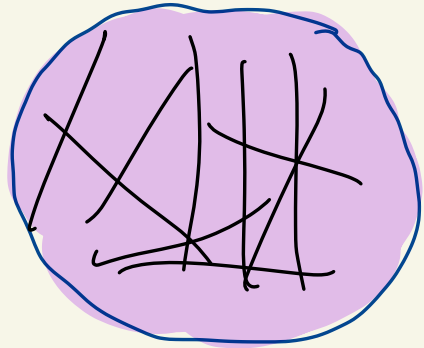
① YES : G has second eigenvalue $= d$

② NO : G has second eigenvalue $\leq d(1 - \epsilon_0)$.

YES :



NO :



multiple connected components

one expanding component

Fact Expander Distinguishing is $\in$ QMA.

Conjecture Expander Distinguishing is $\notin$ QCMA.

Intuition:

(a) The only way Q. Arthur accepts a proof is

if he constructs $\sum_{v \in \text{connected component}} |v\rangle$ on his q. computer

(b) There is no succinct description for the set of vertices in a connected component.

(c) No classical description can help Q. Arthur generate $\sum_{v \in \text{connected component}} |v\rangle$.

Proving this intuition is hard.

Oracle separations

Imagine that instead of a succinct graph, the QCMA Merlin & Arthur had access to an exponentially large graph.

Then can we prove the lower bound?

I.e., we believe that having access to the "source

code" for the succinct graph is no more useful than having black-box access to the graph itself.

For interactive proofs, this forces that Merlin cannot provide a pf based on the source code of the graph.

Oracle Expansion Distinguishing Problem

given an oracle describing a graph, decide if the graph is

① YES: multiple connected components

② NO: a good spectral expander

Thm (Natarajan - Nirkhe)

There is no QCMA algorithm to decide if a distribution of oracle graphs consists of

YES: only graphs with many connected components

NO: only expanding graphs

For more details, rest of talk is a chalk-talk.

(if time)