Quantum search-to-decision and the state synthesis problem

Chinmay Nirkhe
UC Berkeley

joint work with Sandy Irani, Anand Natarajan, Sujit Rao, & Henry Yuen

How does one <u>describe</u> a quantum state?

How does one <u>use</u> a description of a quantum state?

Do quantum problems of classical description length ℓ have classical solutions of length poly(ℓ)? (QCMA vs QMA)

- If not, what is the shortest length of a solution to the problem? What about complexity notions?

A motivation for complexity of sols. vs problems.

Thm (Impagliazzo - Wigderson) unless $NEXP \subseteq \Sigma_2 \subseteq PH$,

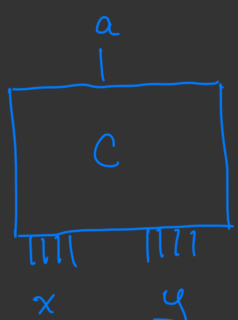
Succinct-3-coloring (NEXP-complete) does not have succinct solutions!

Succinct-3-coloring:

Input: $\langle C \rangle \leftarrow$ circuit description

G = graph implicitly defined by C.

edge $x \sim y \iff C(x, y) = 1$.

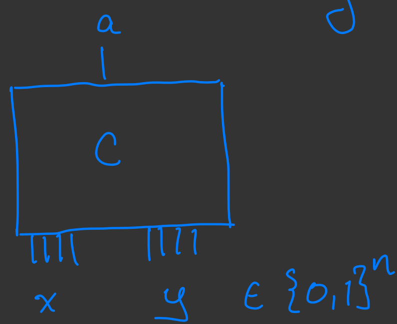


$\in \{0,1\}^n$

Goal: Decide if G is 3-colorable.

A motivation for complexity of sols. vs problems.

Succinct-3-coloring:



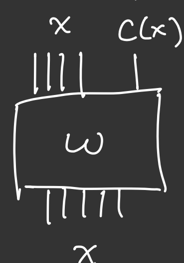
Input: $\langle C \rangle \leftarrow$ circuit description

G = graph implicitly defined by C.

edge $x \sim y \iff C(x,y) = 1$.

Goal: Decide if G is 3-colorable.

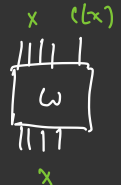
Say S3COL instance $\langle C \rangle$ has a succinct sol. if $\exists$ poly sized ckt



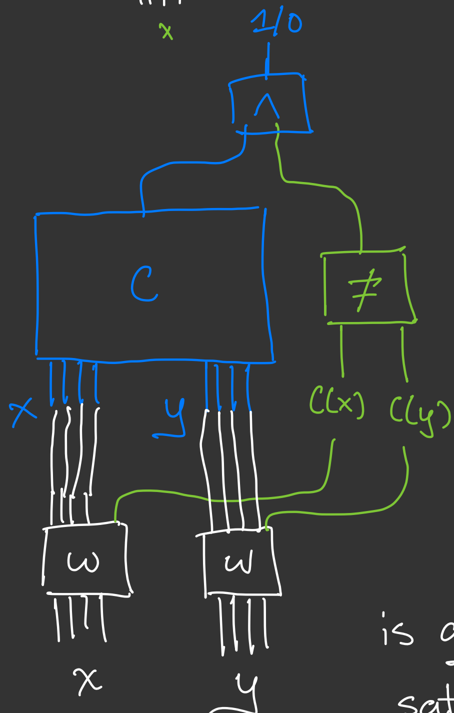
outputting coloring $c(x)$ from optimal coloring.

Thm S3COL doesn't have succinct sols.

Pf If $\exists$



then

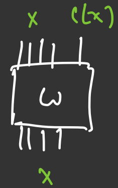


is always satisfiable.

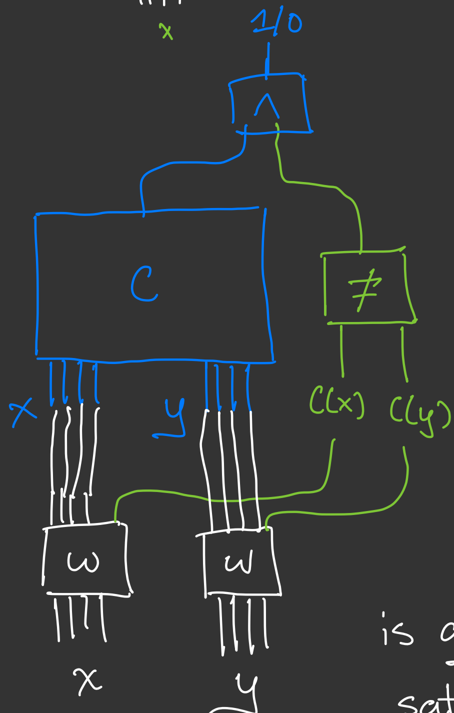
output 1 if

$x \sim y$ AND $c(x) \neq c(y)$.

Thm S3COL doesn't have succinct sols.

Pf If $\exists$ 

then



is always satisfiable.

Then $\langle C\rangle \in$ S3COL iff

$\exists \langle W\rangle$ s.t. BIG-CKT is always satisfiable.

i.e. $\exists\, W$ s.t. $\forall\, x, y$

$$B(x, y, W) = 1$$

$$\Rightarrow \text{NEXP} \subseteq \Sigma_2 \subseteq \text{PH}.$$

Why is this classical CS textbook pf important?

It provides a clear separation between the description complexity of sols. and questions.

Notice, that even with a succinct description of S3COL we would not expect to check the problem in sub-exponential time.

exponential time classes

$P \subseteq NP \subseteq \Sigma_2 \subseteq PH \subseteq \dots \subseteq NEXP$

Instead, description complexity yields a speedup among these large complexity classes that all take exponential time.

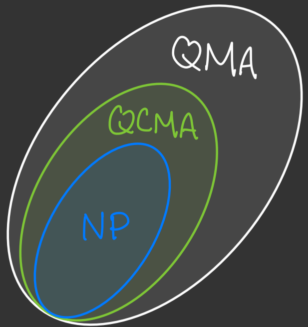
Why is this classical CS textbook pf important?

It provides a clear separation between the description complexity of sols. and questions.

Notice, that even with a succinct description of S3COL we would not expect to check the problem in sub-exponential time.

Today's talk: How should we define description complexity for quantum problems and what is known?

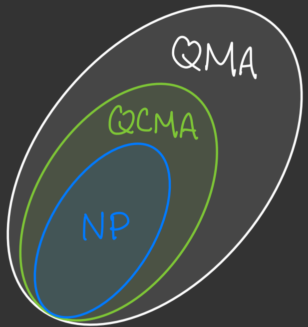
Non-deterministic quantum computation



$QMA \stackrel{?}{=} QCMA$: Do all "classically describeable" quantum questions have "classically describable" solutions?

Note: both cases still speculate the problem is exp-hard for BPP (or BQP). It's a matter of description.

Non-deterministic quantum computation



$QMA \stackrel{?}{=} QCMA$: Do all "classically describeable" quantum questions have "classically describable" solutions?

Note: both cases still speculate the problem is exp-hard for BPP (or BQP). It's a matter of description.

If $QCMA \neq QMA$, what complexity class captures the classical complexity of solutions to QMA problems?

Search-to-decisions :

How much harder is finding a solution than deciding if one exists?

For the class NP, it's equally hard...

$$\exists\, x_2 \dots x_n,\ \varphi(0, x_2, \dots, x_n) = 1$$

yes set $y_1 = 0$

no set $y_1 = 1$

$$\exists\, x_3 \dots x_n,\ \varphi(y_1, 0, x_3 \dots x_n) = 1$$

yes set $y_2 = 0$

no set $y_2 = 1$

$\vdots$

End of process, $y_1 \dots y_n$ forms a sol. to φ.

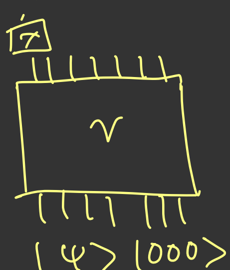
What about quantum search-to-decision?

First: What does search-to-decision mean in this context?

Issues:
1. QMA is a promise class.
2. The solution might depend on the verifier.

Search QMA def:

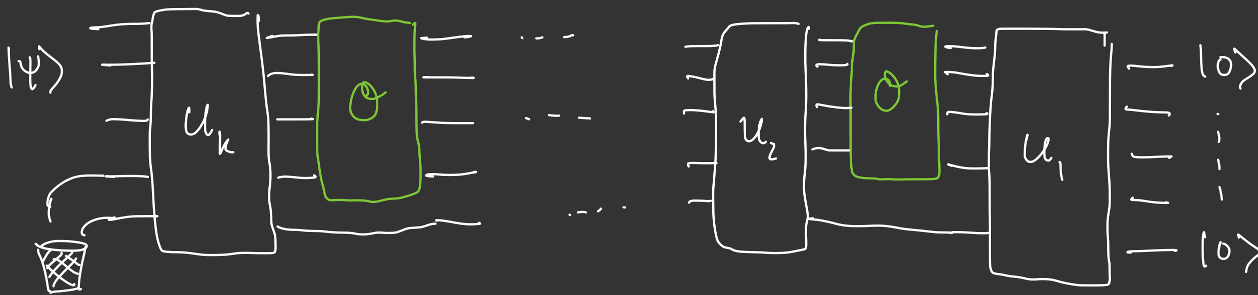
Given a canonical QMA problem described as a verifier V



Output a state $|\psi\rangle$ which that verifier will accept with prob. $\frac{2}{3}$.

QMA search-to-decision reductions

Input: Verifier ckt $\mathcal{V}$.



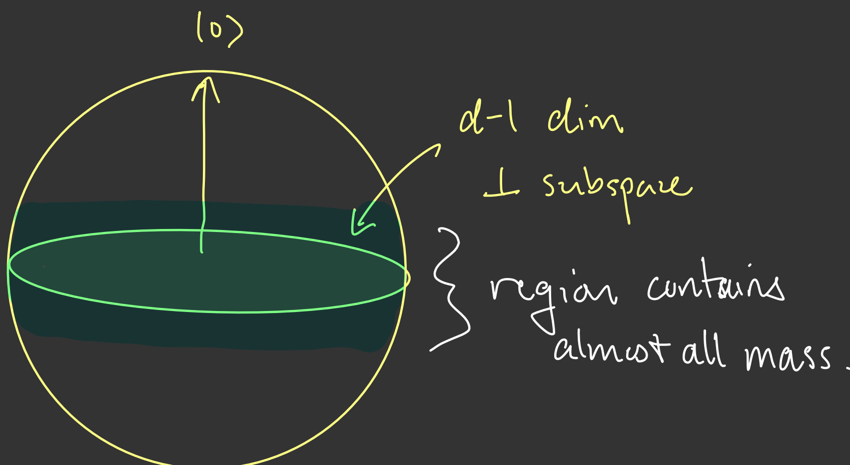
Circuit with oracle gates $\mathcal{O}$ accessed in superposition

$$\mathcal{O}(x) = \begin{cases} 1 & \text{if } x \text{ encodes a YES QMA question} \\ 0 & \text{if } x \text{ encodes a NO QMA question} \\ \text{either} & \text{if } x \text{ encodes an } \underline{\text{invalid}} \text{ QMA question} \end{cases}$$

Goal: Output $|\psi\rangle$ accepted w pr $\frac{2}{3}$ by $\mathcal{V}$.

Difficulties to overcome

There is no good way to binary search over the Hilbert space.



Trying to find $|\psi\rangle$ by a seq. of projectors is a no-go path.

"entanglement destroying"

(also why ground-space dim counting seems hard).

Thm (Aaronson/Folklore)

$\exists$ a $2n+1$ query algorithm for generating any state $|\psi\rangle$ up to $\exp(-n)$ accuracy.

(When applied to QMA sols., oracle complexity = PP.)

Our theorem Thm (INN+'21)

$\exists$ a 1-query PP algorithm for generating the sol. to QMA problems.

(We also have extensions to general states).

Crucial intuitions

① Building all states is unnecessarily powerful.

By counting, there are only $2^{\mathrm{poly}(n)}$ QMA problems $\ll$ $\exp(-n)$ net over $\mathcal{H}$.

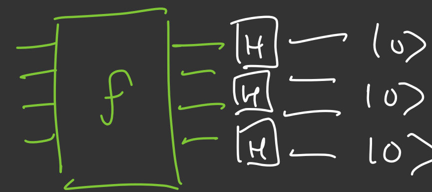
② Since QMA states are verifiable, ~~signs~~ real vs. imaginary-ness of amplitudes don't matter. $|\psi\rangle = \sum_x \alpha_x |x\rangle$, then $\exists$ $|\phi\rangle = \sum_x \beta_x |x\rangle$ $\beta_x \in \mathbb{R}$ s.t. $|\langle\phi|\psi\rangle| \geq$ constant.

③ If $|\psi\rangle$ is Haar-random, then the amplitudes concentrate around $\frac{1}{\sqrt{2^n}}$.

$$\mathop{\mathbb{E}}_{|\psi\rangle \sim \mathrm{Haar}} |\langle x|\psi\rangle|^2 = \frac{1}{2^n}, \quad \mathop{\mathbb{E}}_{|\psi\rangle \sim \mathrm{Haar}} |\langle x|\psi\rangle|^4 = \frac{2}{2^n(2^n+1)}.$$

Interlude: Phase states. $f:\{0,1\}^n \to \{0,1\}$

$$|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle =$$



For any vector $|v\rangle \in \mathbb{R}^{2^n}$, best phase state approx $|v\rangle$ is

with $f(x) = \mathrm{sgn}(\langle x|v\rangle)$.

$$\Rightarrow \langle \psi_f | v\rangle = \frac{\| |v\rangle \|_1}{\sqrt{2^n}}.$$

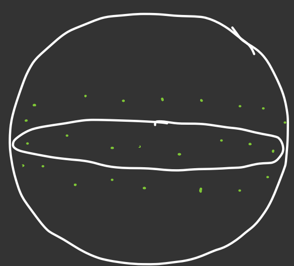
Lem $\Pr_{|v\rangle \sim \mathrm{Haar}}\left[\frac{\| |v\rangle\|_1}{\sqrt{2^n}} < \frac{\sqrt{\alpha}}{2} \right] < \alpha$.

Phase states (cont.)

Lem $$\Pr_{|v\rangle \sim \text{Haar}}\left[\frac{\| |v\rangle \|_1}{\sqrt{2^n}} < \frac{\sqrt{\alpha}}{2}\right] < \alpha.$$

$$\Pr_{f,g}\left[|\langle \psi_f | \psi_g \rangle| > \delta\right] \leq 2\exp\left(-\frac{\delta^2 \cdot 2^n}{3}\right)$$ Chernoff bound.

In short, phase states form an effective net for the Hilbert space under the Haar measure.



goal: show PP fn f s.t. $|\psi_f\rangle$ approximates QMA sol.

Small issues to handle

① Sol. $|\tau\rangle$ may not be approximable by phase states.

But for Clifford C, $C^\dagger H C$ will be whp.

Then can rotate phase state by $C^\dagger$ to recover.

② To define fn $f(x) = \mathrm{sgn}(\mathbb{R}(\langle x|\tau\rangle))$ we need $|\tau\rangle$. But,

$$|\tau\rangle \propto (\mathbb{1}-H)^{\mathrm{poly}(n)} \underbrace{D|0^n\rangle}_{\text{random clifford state}}$$

$f(x) =$

$$\mathrm{sgn}(\mathbb{R}(\langle x|C^\dagger (\mathbb{1}-H)^p D|0^n\rangle)).$$

Thm 1 query PP alg which outputs a state $|\psi\rangle$

s.t. $|\langle\psi|\tau\rangle|^2 \geq 2^{-10}$ whp.

- Can add phase estimation to either output $|\tau\rangle \pm \frac{1}{\text{poly}(n)}$
  w pr 2^{-10}.

- Algorithm is parallelizable with still one query
  to boost success prob. to $1 - \frac{1}{\text{poly}(n)}$.

Is this the best we can do?

Oracle no-go result for QMA-search to QMA-decision reduction.

Thm (INN+'21)

$QMA^{\mathcal{O}}$ search problem with no $QMA^{\mathcal{O}}$ decision oracle alg.

$\mathcal{O} = \mathbb{1} - 2|\psi_f\rangle\langle\psi_f|$ where $|\psi_f\rangle$ is a phase state

OR $\mathcal{O} = \mathbb{1}$. Problem: Decide which scenario.

Idea All sols. accepted w pr $\geq \frac{2}{3}$, have large support on $|\psi_f\rangle$.

Oracle no-go (cont.)

Pf sketch: ① Assume $\exists$ alg $A^{QMA^{\mathcal{O}}, \mathcal{O}}$ that produces $|\psi_f\rangle$.

② Show that when run on $\mathcal{O}' = \mathbb{1} - |\psi_g\rangle\langle\psi_g|$, alg's step-by-step behavior is similar (hybrid alg).

③ Argue whp should output nearly $\perp$ states and yet cannot by hybrid alg.

Consequences

QMA sols. can be described by phase states corresponding to PP fns ($2^{poly(n)}$ PP fns and $2^{poly(n)}$ QMA problems)

vs. 2^{2^n} phase states in general

$\nexists$ any hope for search-to-decision reductions for generic phase states (which are sols. to QMA^O problems)

Due to similarity of oracle separating QCMA/QMA, we suspect same oracles show S-to-D No-go's.

Final thoughts before I finish

① Devote more research to understanding descriptions of q. states. Not the same as decision problems!

② Simpler descriptions lead to decision problem speedups.

③ Big open questions are

(3a) QCMA $\stackrel{?}{=}$ QMA

(3b) Is description complexity robust to small perturbations? i.e. extensions of NLTS theorem.