# The Space “Just Above” BQP

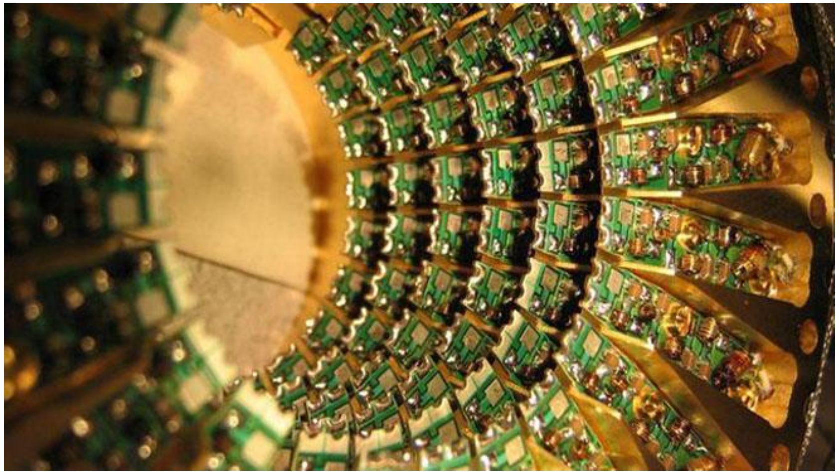
Adam Bouland

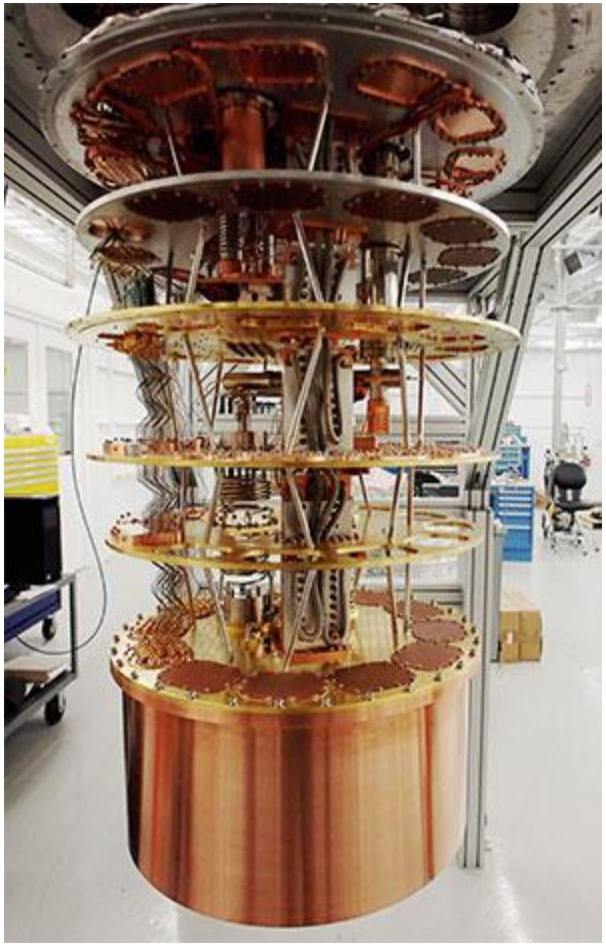
Based on joint work with Scott Aaronson,
Joseph Fitzsimons and Mitchell Lee

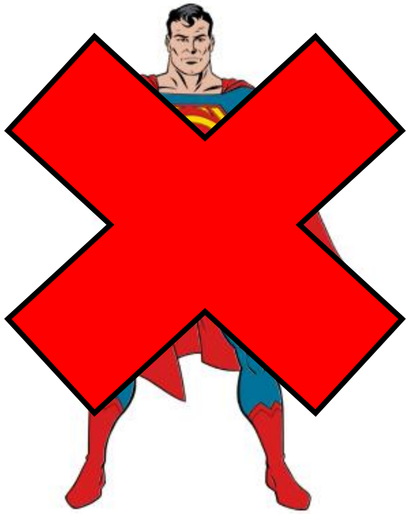
arXiv: 1412:6507
ITCS ‘16

CSAIL

# Quantum Computers







# Quantum Computers…

**CAN** efficiently

- Factor integers [Shor]

**CANNOT** efficiently

- Solve black-box NP-hard problems [BBBV]
  - Searching N item list takes θ(N^1/2) time
- Solve black-box SZK-hard problems [Aaronson]

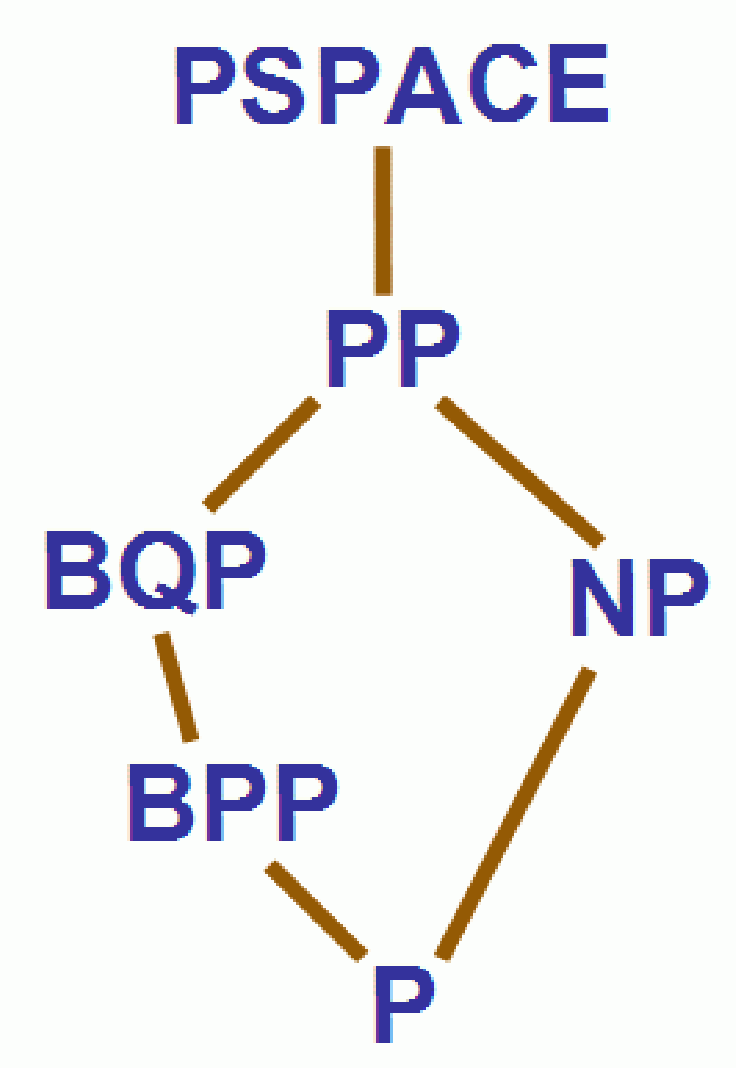



Image credit: Scott Aaronson

# Quantum Mechanics

1. State is vector $v \in \mathbb{C}^d \quad ||v||^2 = 1$
2. Unitary Evolution: $v \to Uv$
3. Measurement

$$x \text{ w.p. } |< e_x, v >|^2$$

$$v \to e_x$$

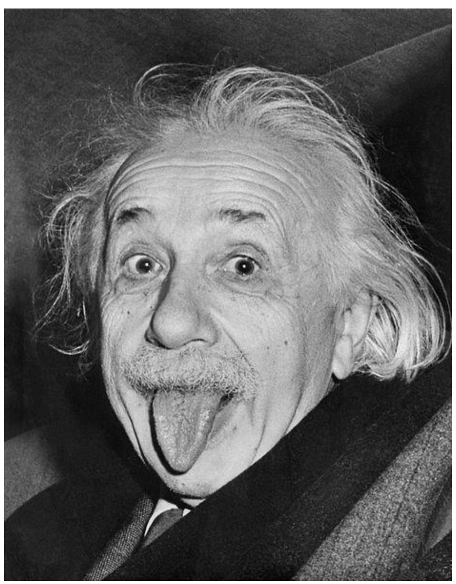
"Wavefunction Collapse"

# Quantum Mechanics

What happens to the power quantum computing if we perturb these axioms?

# Modifying QM

- Non-unitary evolution [Abrams-Lloyd],[Aaronson]
- Measurement based on p-norm for p!=2 [Aaronson]



Allow for superluminal signaling!

# Modifying QM

- Non-unitary evolution [Abrams-Lloyd],[Aaronson]
- Measurement based on p-norm for p!=2 [Aaronson]

Make QC too powerful!

# Modifying QM

- Non-unitary evolution [Abrams-Ll … onson]
- Measurement based on p-norm for p! … [Aaronson]

BQP->PP

Make QC too powerful!

# Modifying QM

# Modifying QM

Challenge:

Is there *any* modification of QM that boosts the power of quantum computing to something SMALLER than PP?

**Yes**

**(if you're careful)**

# Modifying QM

Challenge:

Is there *any* modification of QM that boosts the power of quantum computing to something SMALLER than ~~PP~~ NP?

**Yes**

**(if you're careful)**

# Non-Collapsing Measurements

$$v \in \mathbb{C}^d$$

Sample $x \text{ w.p. } | < e_x, v > |^2$

$$v \to v$$

“Wavefunction Collapse”

# Non-Collapsing Measurements

$v \in \mathbb{C}^d$

$x \text{ w.p. } |< e_x, v >|^2$

$x \text{ w.p. } |< e_x, v >|^2$

$v \quad v$

# Non-Collapsing Measurements

$$v \in \mathbb{C}^d \longrightarrow x v_x$$

Collapsing Measurement

**Can measure same collapsed state multiple times**

# Non-Collapsing Measurements

## CQP

"Collapse-free Quantum Polynomial time"

## naCQP

"non-adaptive CQP"

Quantum circuit must be non-adaptive to the non-collapsing measurement outcomes

# Non-Collapsing Measurements

How powerful are these classes?

A: naCQP is “just above” BQP

# Results

The class naCQP:

- Can solve SZK in poly-time
  - BQP cannot do this in black box manner
  - $\exists$ O such that naCQP^O $\neq$ BQP^O
- Can search in O(N^1/3) time
- Search requires Ω(N^1/4) time
  - $\exists$ O such that NP^O $\not\subset$ naCQP^O
- In BPP^PP

# Summary

| Property | BQP | naCQP |
|---|---|---|
| Contains SZK | Unknown | Yes |
| Contains $\mathsf{SZK}^O$ $\forall O$ | No | Yes |
| Upper Bound for Search | $O(N^{1/2})$ | $\tilde{O}(N^{1/3})$ |
| Lower Bound for Search | $\Omega(N^{1/2})$ | $\Omega(N^{1/4})$ |
| Upper Bound | AWPP | $\mathsf{BPP}^{\mathsf{PP}}$ |

# Summary

| Property | BQP | naCQP | CQP |
|---|---|---|---|
| Contains SZK | Unknown | Yes | Yes |
| Contains $\mathsf{SZK}^O\ \forall O$ | No | Yes | Yes |
| Upper Bound for Search | $O(N^{1/2})$ | $\tilde{O}(N^{1/3})$ | $\tilde{O}(N^{1/3})$ |
| Lower Bound for Search | $\Omega(N^{1/2})$ | $\Omega(N^{1/4})$ | $\Omega(1)$ |
| Upper Bound | AWPP | $\mathsf{BPP}^{\mathsf{PP}}$ | $\mathsf{BPP}^{\mathsf{PP}}$ |

# Relation to Prior work

Aaronson '05:

QC with Hidden Variable Theories

"DQP"

Imagine a hidden variable theory is true, and you "see" hidden variables of your system as it evolves

# Relation to Prior work

| Property | BQP | naCQP | CQP | DQP |
|---|---|---|---|---|
| Contains SZK | Unknown | Yes | Yes | Yes |
| Contains $\mathsf{SZK}^O\ \forall O$ | No | Yes | Yes | Yes |
| Upper Bound for Search | $O(N^{1/2})$ | $\tilde{O}(N^{1/3})$ | $\tilde{O}(N^{1/3})$ | $\tilde{O}(N^{1/3})$ |
| Lower Bound for Search | $\Omega(N^{1/2})$ | $\Omega(N^{1/4})$ | $\Omega(1)$ | Ω(N^1/3) |
| Upper Bound | AWPP | $\mathsf{BPP}^{\mathsf{PP}}$ | $\mathsf{BPP}^{\mathsf{PP}}$ | EXP |

# Don’t bet on this model just yet!

- FTL Signaling (if adaptive)
- No notion of query complexity
- Can clone if circuit **adaptive**
  - Perfect cloning-> #P [Bao B. Jordan ‘15]
  - Imperfect cloning -> ???

# Open Problems

| Property | BQP | naCQP | CQP |
|---|---|---|---|
| Contains SZK | Unknown | Yes | Yes |
| Contains $\mathsf{SZK}^O$ $\forall O$ | No | Yes | Yes |
| Upper Bound for Search | $O(N^{1/2})$ | $\tilde{O}(N^{1/3})$ | $\tilde{O}(N^{1/3})$ |
| Lower Bound for Search | $\Omega(N^{1/2})$ | $\Omega(N^{1/4})$ | $\Omega(1)$ |
| Upper Bound | AWPP | $\mathsf{BPP}^{\mathsf{PP}}$ | $\mathsf{BPP}^{\mathsf{PP}}$ |

# Questions

?