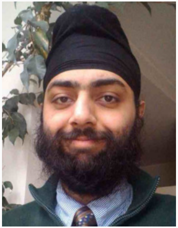
On the complexity of hybrid quantum computation

Andru Gheorghiu (Chalmers University of Technology)

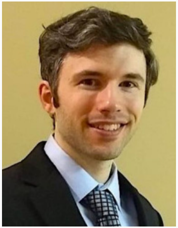


Atul Singh Arora

(Caltech)

Andrea Coladangelo

(University of Washington)



Matt Coudron

(University of Maryland, NIST)

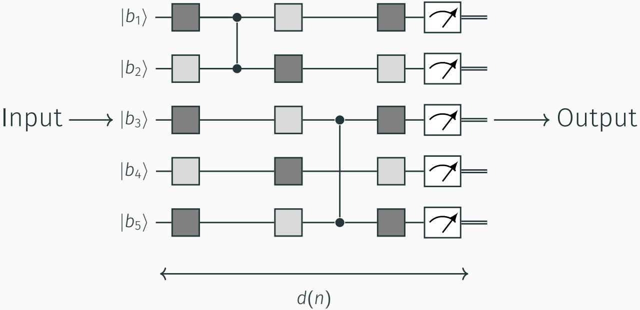
Uttam Singh

(Polish Academy of Sciences, IIT Hyderabad)

Hendrik Waldner

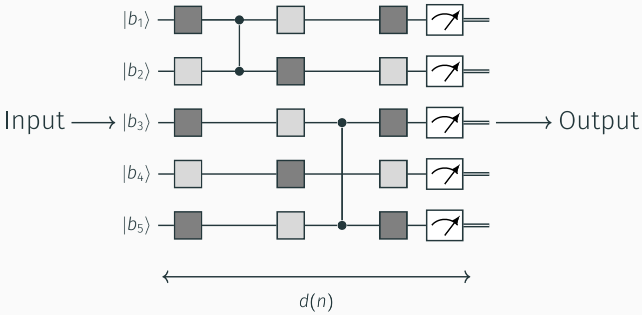
(Max Planck Institute, University of Maryland)

Hybrid quantum-classical computation



Quantum d depth.

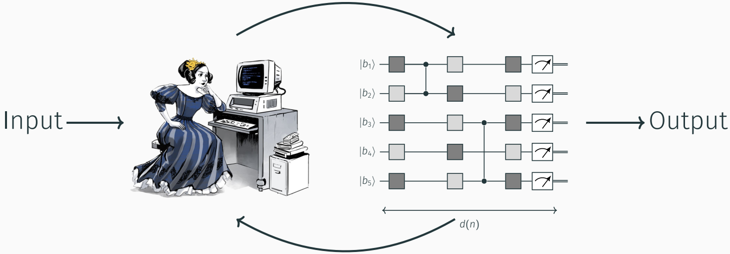
Hybrid quantum-classical computation



Quantum d depth.

Q_d,

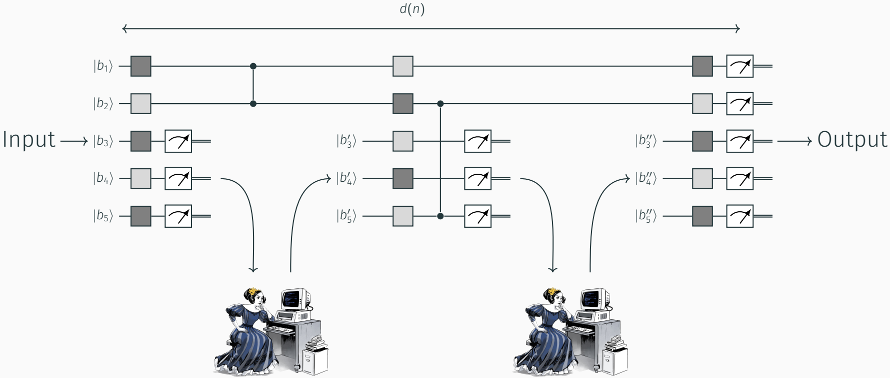
Hybrid quantum-classical computation



Classical invokes Quantum d depth.

Q_d, CQ_d,

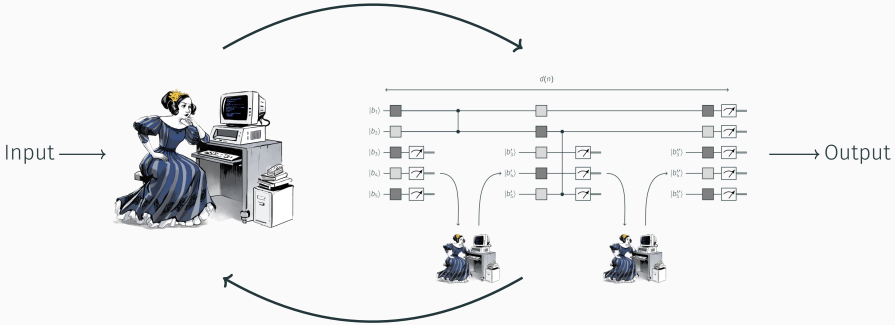
Hybrid quantum-classical computation



Quantum d depth invokes Classical.

Q_d, CQ_d, QC_d,

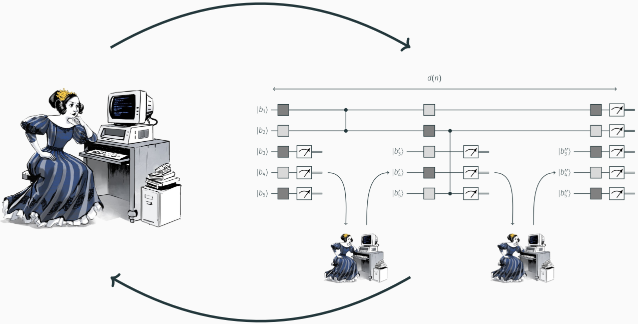
Hybrid quantum-classical computation



Classical invokes Quantum d depth that invokes Classical.

Q_d, CQ_d, QC_d, CQC_d.

Input $\longrightarrow$



$\longrightarrow$ Output

Classical invokes Quantum d depth that invokes Classical.

Q_d, CQ_d, QC_d, CQC_d.

QNC, $\mathsf{BPP}^{\mathsf{QNC}}$, $\mathsf{QNC}^{\mathsf{BPP}}$, $\mathsf{BPP}^{\mathsf{QNC}^{\mathsf{BPP}}}$

(when $d(n) = \log^{O(1)}(n) \equiv \mathrm{polylog}(n)$)

Hybrid quantum-classical computation

$$
\begin{tikzcd}
 & \mathsf{CQ}_d \arrow[dr, "\subseteq"] & & \\
\mathsf{Q}_d \arrow[ur, "\subseteq"] \arrow[dr, "\subseteq"'] & & \mathsf{CQC}_d \arrow[r, "\subseteq"] & \mathsf{BQP} \\
 & \mathsf{QC}_d \arrow[ur, "\subseteq"'] & &
\end{tikzcd}
$$

Why hybrid classes?

Why hybrid classes?

1. Easier to realize in practice.

Why hybrid classes?

1. Easier to realize in practice.
2. Parallel quantum computations.

Why hybrid classes?

1. Easier to realize in practice.
2. Parallel quantum computations.
3. Shallow quantum circuits are surprisingly versatile.

Why hybrid classes?

1. Easier to realize in practice.
2. Parallel quantum computations.
3. Shallow quantum circuits are surprisingly versatile.

$$\mathsf{Q}_{O(1)} \not\subseteq \mathsf{C}_{O(\log)}.^{1}$$

[1] [Bravyi, Gosset, König, 2017]

Why hybrid classes?

1. Easier to realize in practice.
2. Parallel quantum computations.
3. Shallow quantum circuits are surprisingly versatile.

$$\mathsf{Q}_{O(1)} \not\subseteq \mathsf{C}_{o(\log)}.^{1}$$

$$\mathsf{Q}_{O(1)} \not\subseteq \mathsf{BPP}, \text{ assuming non-collapse of } \mathsf{PH}.^{2}$$

[1] [Bravyi, Gosset, König, 2017]
[2] [Terhal, DiVicenzo, 2002], [Haferkamp et al., 2019]

Why hybrid classes?

1. Easier to realize in practice.
2. Parallel quantum computations.
3. Shallow quantum circuits are surprisingly versatile.

$$\mathsf{Q}_{O(1)} \not\subseteq \mathsf{C}_{o(\log)}.^{1}$$

$$\mathsf{Q}_{O(1)} \not\subseteq \mathsf{BPP}, \text{ assuming non-collapse of } \mathsf{PH}.^{2}$$

$$\text{Factoring, Discrete-log, Pell's equation} \in \mathsf{CQ}_{\log}, \mathsf{QC}_{O(1)}.^{3}$$

[1] [Bravyi, Gosset, König, 2017]
[2] [Terhal, DiVicenzo, 2002], [Haferkamp et al., 2019]
[3] [Cleve, Watrous, 2000], [Høyer, Špalek, 2005]

Why hybrid classes?

1. Easier to realize in practice.
2. Parallel quantum computations.
3. Shallow quantum circuits are surprisingly versatile.

$$\mathsf{Q}_{O(1)} \not\subseteq \mathsf{C}_{o(\log)}.^{1}$$

$\mathsf{Q}_{O(1)} \not\subseteq \mathsf{BPP}$, assuming non-collapse of PH.[2]

Factoring, Discrete-log, Pell's equation $\in \mathsf{CQ}_{\log}, \mathsf{QC}_{O(1)}$.[3]

Jozsa's conjecture[4] (reformulated)

$$\mathsf{CQC}_{\mathrm{polylog}} = \mathsf{BQP}.$$

[1] [Bravyi, Gosset, König, 2017]
[2] [Terhal, DiVicenzo, 2002], [Haferkamp et al., 2019]
[3] [Cleve, Watrous, 2000], [Høyer, Špalek, 2005]
[4] [Jozsa, 2005]

Limitations of hybrid models

Aaronson's challenge[5]

Does there exist an *oracle* relative to which Jozsa's conjecture is false? Can the oracle then be *instantiated?*

[5] "*Ten semi-grand challenges for quantum computing*" - S. Aaronson, 2005

Limitations of hybrid models

Aaronson's challenge[5]

Does there exist an *oracle* relative to which Jozsa's conjecture is false? Can the oracle then be *instantiated?*

Relativized/oracle/black-box models: given access to a function f.

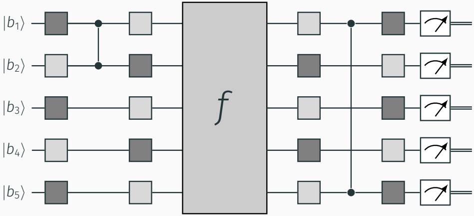
[5]"*Ten semi-grand challenges for quantum computing*" - S. Aaronson, 2005

Limitations of hybrid models

Aaronson's challenge[5]

Does there exist an *oracle* relative to which Jozsa's conjecture is false? Can the oracle then be *instantiated*?

Relativized/oracle/black-box models: given access to a function f.



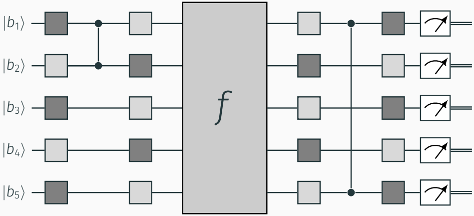
[5] "*Ten semi-grand challenges for quantum computing*" - S. Aaronson, 2005

Limitations of hybrid models

Aaronson's challenge[5]

Does there exist an *oracle* relative to which Jozsa's conjecture is false? Can the oracle then be *instantiated*?

Relativized/oracle/black-box models: given access to a function f.



$$\mathsf{Q}_d^f, \mathsf{CQ}_d^f, \mathsf{QC}_d^f, \mathsf{CQC}_d^f, \mathsf{BPP}^f, \mathsf{BQP}^f.$$

[5] "*Ten semi-grand challenges for quantum computing*" - S. Aaronson, 2005

Limitations of hybrid models

Relativized quantum depth separation[6]

There exists a function, f, such that $\mathsf{CQ}^f_{\mathrm{polylog}} \cup \mathsf{QC}^f_{\mathrm{polylog}} \subsetneq \mathsf{BQP}^f$.

[6] [Chia, Chung, Lai, 2020], [Coudron, Menda, 2020]

Limitations of hybrid models

Relativized quantum depth separation[6]

There exists a function, f, such that $\mathsf{CQ}^f_{\mathrm{polylog}} \cup \mathsf{QC}^f_{\mathrm{polylog}} \subsetneq \mathsf{BQP}^f$.

f has a special property that can only be found by querying it *quantumly, sequentially* $\Omega(n)$ times.

[6] [Chia, Chung, Lai, 2020], [Coudron, Menda, 2020]

Limitations of hybrid models

Relativized quantum depth separation[6]

There exists a function, f, such that $\mathsf{CQ}^f_{\mathrm{polylog}} \cup \mathsf{QC}^f_{\mathrm{polylog}} \subsetneq \mathsf{BQP}^f$.

f has a special property that can only be found by querying it *quantumly, sequentially* $\Omega(n)$ times.

Relativized separation of hybrids[7]

There exist functions, f_1, f_2, such that

- $\mathsf{QC}^{f_1}_{\mathrm{polylog}} \not\subseteq \mathsf{CQ}^{f_1}_{O(1)}$
- $\mathsf{CQ}^{f_2}_{\mathrm{polylog}} \not\subseteq \mathsf{QC}^{f_2}_{O(1)}$

[6] [Chia, Chung, Lai, 2020], [Coudron, Menda, 2020]
[7] [Arora, **G**, Singh, 2021]

Limitations of hybrid models

Relativized quantum depth separation[6]

There exists a function, f, such that $\mathsf{CQ}^f_{\text{polylog}} \cup \mathsf{QC}^f_{\text{polylog}} \subsetneq \mathsf{BQP}^f$.

f has a special property that can only be found by querying it *quantumly, sequentially* $\Omega(n)$ times.

Relativized separation of hybrids[7]

There exist functions, f_1, f_2, such that

- $\mathsf{QC}^{f_1}_{\text{polylog}} \not\subseteq \mathsf{CQ}^{f_1}_{O(1)}$
- $\mathsf{CQ}^{f_2}_{\text{polylog}} \not\subseteq \mathsf{QC}^{f_2}_{O(1)}$

- Functions have very special structure (structured oracles).

[6] [Chia, Chung, Lai, 2020], [Coudron, Menda, 2020]
[7] [Arora, **G**, Singh, 2021]

Limitations of hybrid models

Relativized quantum depth separation[6]

There exists a function, f, such that $\mathsf{CQ}^f_{\mathrm{polylog}} \cup \mathsf{QC}^f_{\mathrm{polylog}} \subsetneq \mathsf{BQP}^f$.

f has a special property that can only be found by querying it *quantumly, sequentially* $\Omega(n)$ times.

Relativized separation of hybrids[7]

There exist functions, f_1, f_2, such that

- $\mathsf{QC}^{f_1}_{\mathrm{polylog}} \not\subseteq \mathsf{CQ}^{f_1}_{O(1)}$
- $\mathsf{CQ}^{f_2}_{\mathrm{polylog}} \not\subseteq \mathsf{QC}^{f_2}_{O(1)}$

- Functions have very special structure (structured oracles).
- No known instantiations.

[6] [Chia, Chung, Lai, 2020], [Coudron, Menda, 2020]
[7] [Arora, **G**, Singh, 2021]

Limitations of hybrid models

Relativized quantum depth separation[6]

There exists a function, f, such that $\mathsf{CQ}^f_{\mathrm{polylog}} \cup \mathsf{QC}^f_{\mathrm{polylog}} \subsetneq \mathsf{BQP}^f$.

f has a special property that can only be found by querying it *quantumly, sequentially* $\Omega(n)$ times.

Relativized separation of hybrids[7]

There exist functions, f_1, f_2, such that

- $\mathsf{QC}^{f_1}_{\mathrm{polylog}} \not\subseteq \mathsf{CQ}^{f_1}_{O(1)}$
- $\mathsf{CQ}^{f_2}_{\mathrm{polylog}} \not\subseteq \mathsf{QC}^{f_2}_{O(1)}$

- Functions have very special structure (structured oracles).
- No known instantiations.
- Any instantiation should have at most $O(\mathrm{polylog}(n))$ depth.

[6] [Chia, Chung, Lai, 2020], [Coudron, Menda, 2020]
[7] [Arora, **G**, Singh, 2021]

The (quantum) random oracle model (QROM)

Random oracle = uniformly random (boolean) function.

The (quantum) random oracle model (QROM)

Random oracle = uniformly random (boolean) function.

Random oracle *model* = given access to a random oracle.

The (quantum) random oracle model (QROM)

Random oracle = uniformly random (boolean) function.

Random oracle *model* = given access to a random oracle.

$$
\begin{tikzcd}
 & & \text{RO} \arrow[dl] \arrow[dr] & \\
 & \text{OWF} \arrow[dl] \arrow[dr] & & \text{P} \neq \text{NP} \\
\text{Symmetric-key crypto} & & \text{Commitments} &
\end{tikzcd}
$$

The (quantum) random oracle model (QROM)

Random oracle = uniformly random (boolean) function.

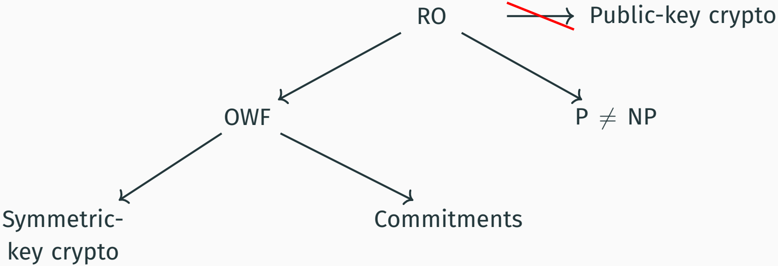
Random oracle *model* = given access to a random oracle.

$$\begin{tikzcd}
 & & \text{RO} \arrow[dl] \arrow[dr] \arrow[r, "/" marking] & \text{Public-key crypto} \\
 & \text{OWF} \arrow[dl] \arrow[dr] & & \text{P} \neq \text{NP} \\
\text{Symmetric-key crypto} & & \text{Commitments} &
\end{tikzcd}$$

The (quantum) random oracle model (QROM)

Random oracle = uniformly random (boolean) function.

Random oracle *model* = given access to a random oracle.



Inherently structureless.

The (quantum) random oracle model (QROM)

Random oracle = uniformly random (boolean) function.

Random oracle *model* = given access to a random oracle.

$$\begin{tikzcd}
 & & \text{RO} \arrow[dl] \arrow[dr] \arrow[r, "/" marking] & \text{Public-key crypto} \\
 & \text{OWF} \arrow[dl] \arrow[dr] & & \text{P} \neq \text{NP} \\
\text{Symmetric-key crypto} & & \text{Commitments} &
\end{tikzcd}$$

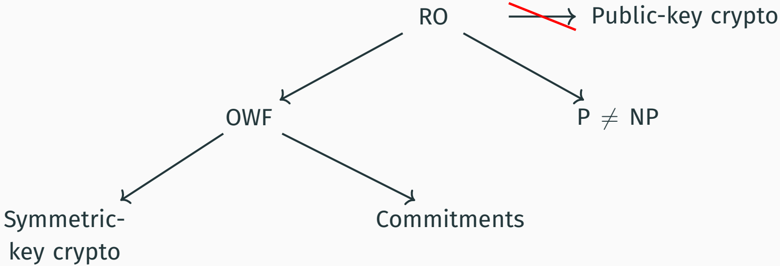
Inherently structureless.

Heuristic: can instantiate RO with a hash function (like SHA256).

The (quantum) random oracle model (QROM)

Random oracle = uniformly random (boolean) function.

Random oracle *model* = given access to a random oracle.



Inherently structureless.

Heuristic: can instantiate RO with a hash function (like SHA256).
(which can be implemented in log depth)

Our results

Unstructured quantum depth separation

Relative to a random f and for any $d(n) < \mathrm{poly}(n)$, we have that:

Our results

Unstructured quantum depth separation

Relative to a random f and for any $d(n) < \mathrm{poly}(n)$, we have that:

1. $\mathsf{Q}_d^f \subsetneq \mathsf{CQ}_d^f \subsetneq \mathsf{CQC}_d^f$ and $\mathsf{Q}_d^f \subsetneq \mathsf{QC}_d^f \subsetneq \mathsf{CQC}_d^f$.

Our results

Unstructured quantum depth separation

Relative to a random f and for any $d(n) < \mathrm{poly}(n)$, we have that:

1. $\mathsf{Q}_d^f \subsetneq \mathsf{CQ}_d^f \subsetneq \mathsf{CQC}_d^f$ and $\mathsf{Q}_d^f \subsetneq \mathsf{QC}_d^f \subsetneq \mathsf{CQC}_d^f$.
2. $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Our results

Unstructured quantum depth separation

Relative to a random f and for any $d(n) < \mathrm{poly}(n)$, we have that:

1. $\mathsf{Q}_d^f \subsetneq \mathsf{CQ}_d^f \subsetneq \mathsf{CQC}_d^f$ and $\mathsf{Q}_d^f \subsetneq \mathsf{QC}_d^f \subsetneq \mathsf{CQC}_d^f$.
2. $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$
3. $\mathsf{QC}_{O(1)}^f \not\subseteq \mathsf{CQ}_d^f$ and $\mathsf{CQ}_{O(1)}^f \not\subseteq \mathsf{QC}_d^f$.

Our results

Unstructured quantum depth separation

Relative to a random f and for any $d(n) < \mathrm{poly}(n)$, we have that:

1. $\mathsf{Q}_d^f \subsetneq \mathsf{CQ}_d^f \subsetneq \mathsf{CQC}_d^f$ and $\mathsf{Q}_d^f \subsetneq \mathsf{QC}_d^f \subsetneq \mathsf{CQC}_d^f$.
2. $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$
3. $\mathsf{QC}_{O(1)}^f \not\subseteq \mathsf{CQ}_d^f$ and $\mathsf{CQ}_{O(1)}^f \not\subseteq \mathsf{QC}_d^f$.

$$
\begin{tikzcd}
 & \mathsf{CQ}_d^f \arrow[dr, "\subsetneq"] & & \\
\mathsf{Q}_d^f \arrow[ur, "\subsetneq"] \arrow[dr, "\subsetneq"'] & & \mathsf{CQC}_d^f \arrow[r, "\subsetneq"] & \mathsf{BQP}^f \\
 & \mathsf{QC}_d^f \arrow[ur, "\subsetneq"'] & &
\end{tikzcd}
$$

Unstructured quantum depth separation

Relative to a random f and for any $d(n) < \mathrm{poly}(n)$, we have that:

1. $\mathsf{Q}_d^f \subsetneq \mathsf{CQ}_d^f \subsetneq \mathsf{CQC}_d^f$ and $\mathsf{Q}_d^f \subsetneq \mathsf{QC}_d^f \subsetneq \mathsf{CQC}_d^f$.
2. $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$
3. $\mathsf{QC}_{O(1)}^f \not\subseteq \mathsf{CQ}_d^f$ and $\mathsf{CQ}_{O(1)}^f \not\subseteq \mathsf{QC}_d^f$.

$$
\begin{tikzcd}
 & \mathsf{CQ}_d^f \arrow[dr, "\subsetneq"] \arrow[dd, phantom, "\not\subseteq \quad \not\supseteq"] & & \\
\mathsf{Q}_d^f \arrow[ur, "\subsetneq"] \arrow[dr, "\subsetneq"'] & & \mathsf{CQC}_d^f \arrow[r, "\subsetneq"] & \mathsf{BQP}^f \\
 & \mathsf{QC}_d^f \arrow[ur, "\subsetneq"'] & &
\end{tikzcd}
$$

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. **Fourier Sampling**[8]

Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} f(x) \right|^2$$

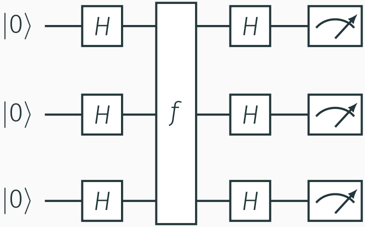
[8] [Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. **Fourier Sampling**[8]
Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} f(x) \right|^2$$



8[Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. **Fourier Sampling**[8]

Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} f(x) \right|^2$$

Consider $d+1$ random oracles f_0, f_1, ... f_d.

(for instance by splitting f into $d+1$ functions)

[8] [Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. **Fourier Sampling**[8]
Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} f(x) \right|^2$$

Consider $d+1$ random oracles $f_0, f_1, \ldots f_d$.
(for instance by splitting f into $d+1$ functions)

Redefine the problem with respect to $\tilde{f} = f_d \circ f_{d-1} \circ \ldots \circ f_0$.

[8] [Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. d-**Fourier Sampling**[8]
Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} \tilde{f}(x) \right|^2$$

Consider $d+1$ random oracles $f_0, f_1, \ldots f_d$.
(for instance by splitting f into $d+1$ functions)

Redefine the problem with respect to $\tilde{f} = f_d \circ f_{d-1} \circ \ldots \circ f_0$.

[8] [Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. d-**Fourier Sampling**[8]
Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} \tilde{f}(x) \right|^2$$

Consider $d+1$ random oracles $f_0, f_1, \ldots f_d$.
(for instance by splitting f into $d+1$ functions)

Redefine the problem with respect to $\tilde{f} = f_d \circ f_{d-1} \circ \ldots \circ f_0$.

Observation: New problem is still in BQP^f.

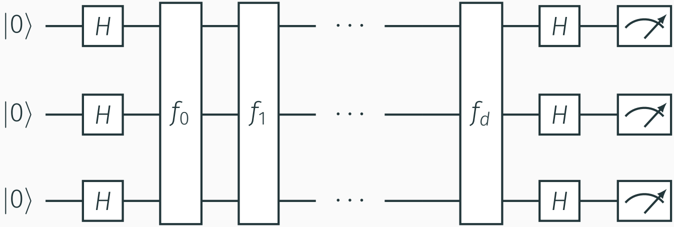
[8] [Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. d-**Fourier Sampling**[8]
Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} \tilde{f}(x) \right|^2$$



[8] [Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. d-**Fourier Sampling**[8]

Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} \tilde{f}(x) \right|^2$$

Consider $d+1$ random oracles $f_0, f_1, \ldots f_d$.

(for instance by splitting f into $d+1$ functions)

Redefine the problem with respect to $\tilde{f} = f_d \circ f_{d-1} \circ \ldots \circ f_0$.

Observation: New problem is still in BQP^f.

[8] [Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

Take *any problem* that separates BPP^f and BQP^f.

E.g. d-**Fourier Sampling**[8]
Output $y \in \{0,1\}^n$ with probability

$$\Pr(y) = \left| \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} \tilde{f}(x) \right|^2$$

Consider $d+1$ random oracles $f_0, f_1, \dots f_d$.
(for instance by splitting f into $d+1$ functions)

Redefine the problem with respect to $\tilde{f} = f_d \circ f_{d-1} \circ \dots \circ f_0$.

Observation: New problem is still in BQP^f.

Claim: New problem is not in CQC_d^f.

[8] [Aaronson, 2009]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

1. We know that the problem $\notin \mathsf{BPP}^f$.

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

1. We know that the problem $\notin \mathsf{BPP}^f$.
2. Hybrid argument + one-way to hiding lemma $\rightarrow$ problem $\notin \mathsf{Q}_d^f$.

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

1. We know that the problem $\notin \mathsf{BPP}^f$.
2. Hybrid argument + one-way to hiding lemma $\rightarrow$ problem $\notin \mathsf{Q}_d^f$.
3. Carefully combining 1 and 2 $\rightarrow$ problem $\notin \mathsf{QC}_d^f$.

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

1. We know that the problem $\notin \mathsf{BPP}^f$.
2. Hybrid argument + one-way to hiding lemma $\rightarrow$ problem $\notin \mathsf{Q}_d^f$.
3. Carefully combining 1 and 2 $\rightarrow$ problem $\notin \mathsf{QC}_d^f$.
4. Sampling argument together with 1 and 2 $\rightarrow$ problem $\notin \mathsf{CQ}_d^f$.

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

1. We know that the problem $\notin \mathsf{BPP}^f$.
2. Hybrid argument + one-way to hiding lemma $\rightarrow$ problem $\notin \mathsf{Q}_d^f$.
3. Carefully combining 1 and 2 $\rightarrow$ problem $\notin \mathsf{QC}_d^f$.
4. Sampling argument together with 1 and 2 $\rightarrow$ problem $\notin \mathsf{CQ}_d^f$.
5. Carefully combining 3 and 4 $\rightarrow$ problem $\notin \mathsf{CQC}_d^f$.

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

1. We know that the problem $\notin \mathsf{BPP}^f$.
2. Hybrid argument + one-way to hiding lemma $\rightarrow$ problem $\notin \mathsf{Q}_d^f$.
3. Carefully combining 1 and 2 $\rightarrow$ problem $\notin \mathsf{QC}_d^f$.
4. Sampling argument together with 1 and 2 $\rightarrow$ problem $\notin \mathsf{CQ}_d^f$.
5. Carefully combining 3 and 4 $\rightarrow$ problem $\notin \mathsf{CQC}_d^f$.

Can use the recent problem of Yamakawa and Zhandry.[9]

[9] [Yamakawa, Zhandry, 2022]

Intuition for $\mathsf{CQC}_d^f \subsetneq \mathsf{BQP}^f$

1. We know that the problem $\notin \mathsf{BPP}^f$.
2. Hybrid argument + one-way to hiding lemma $\rightarrow$ problem $\notin \mathsf{Q}_d^f$.
3. Carefully combining 1 and 2 $\rightarrow$ problem $\notin \mathsf{QC}_d^f$.
4. Sampling argument together with 1 and 2 $\rightarrow$ problem $\notin \mathsf{CQ}_d^f$.
5. Carefully combining 3 and 4 $\rightarrow$ problem $\notin \mathsf{CQC}_d^f$.

Can use the recent problem of Yamakawa and Zhandry.[9]

That problem is also in NP^f (efficiently verifiable).

[9] [Yamakawa, Zhandry, 2022]

Proofs of quantum depth

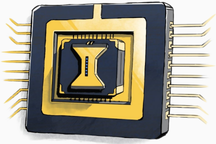
We obtain a *proof of d quantum depth protocol*.[10]

[10] [Chia, Hung, 2022]

Proofs of quantum depth

We obtain a *proof of d quantum depth protocol.*[10]

Verifier

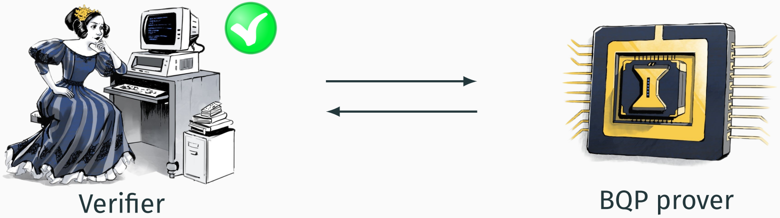


Prover

[10] [Chia, Hung, 2022]

Proofs of quantum depth

We obtain a *proof of d quantum depth protocol*.[10]



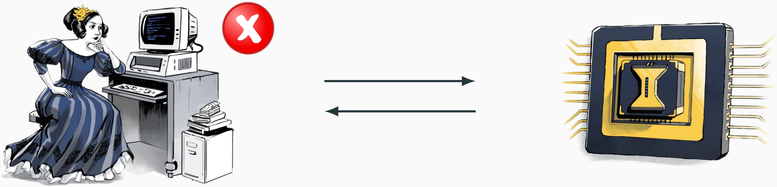
Completeness

There is a **BQP** prover that makes the verifier accept whp.

[10] [Chia, Hung, 2022]

Proofs of quantum depth

We obtain a *proof of d quantum depth protocol*.[10]



Verifier

CQC_d prover

Completeness

There is a **BQP** prover that makes the verifier accept whp.

Soundness

No $\mathbf{CQC}_d$ prover can make the verifier accept whp (in the QROM).

[10] [Chia, Hung, 2022]

Conclusions and open problems

- Unstructured separations of hybrid models.

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.
- Intermediate measurements provide a computational advantage.

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.
- Intermediate measurements provide a computational advantage.
- Sampling and search problems not decision problems (Aaronson-Ambainis conjecture).

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.
- Intermediate measurements provide a computational advantage.
- Sampling and search problems not decision problems (Aaronson-Ambainis conjecture).
- Proof of quantum depth.

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.
- Intermediate measurements provide a computational advantage.
- Sampling and search problems not decision problems (Aaronson-Ambainis conjecture).
- Proof of quantum depth.

- Can separations be based on standard crypto assumptions?

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.
- Intermediate measurements provide a computational advantage.
- Sampling and search problems not decision problems (Aaronson-Ambainis conjecture).
- Proof of quantum depth.

- Can separations be based on standard crypto assumptions?
- Are there natural separating problems? (fast-forwarding Hamiltonians)

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.
- Intermediate measurements provide a computational advantage.
- Sampling and search problems not decision problems (Aaronson-Ambainis conjecture).
- Proof of quantum depth.

- Can separations be based on standard crypto assumptions?
- Are there natural separating problems? (fast-forwarding Hamiltonians)
- What about $\mathsf{CQCQCQ}\ldots\mathsf{C}_d$?

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.
- Intermediate measurements provide a computational advantage.
- Sampling and search problems not decision problems (Aaronson-Ambainis conjecture).
- Proof of quantum depth.

- Can separations be based on standard crypto assumptions?
- Are there natural separating problems? (fast-forwarding Hamiltonians)
- What about $\mathsf{CQCQCQ}\ldots\mathsf{C}_d$?
- Fine-grained proofs of quantum depth.

Conclusions and open problems

- Unstructured separations of hybrid models.
- Refuting Jozsa's conjecture in the random oracle model.
- Intermediate measurements provide a computational advantage.
- Sampling and search problems not decision problems (Aaronson-Ambainis conjecture).
- Proof of quantum depth.

- Can separations be based on standard crypto assumptions?
- Are there natural separating problems? (fast-forwarding Hamiltonians)
- What about $\mathsf{CQCQCQ}\ldots\mathsf{C}_d$?
- Fine-grained proofs of quantum depth.

Thanks!