Topics: Restricted models of QC
      Near-term quantum algorithms
      Quantum computational supremacy

Plan:  1. Facts from complexity theory
       2. Hardness of exactly simulating quantum computation
       3. Approximate simulation
       4. Near-term quantum algorithms

1. Complexity facts

The polynomial hierarchy

\[ \text{PH} = \bigcup_{k=0,1,\ldots} \Sigma_k \]

where

\[ \Sigma_0 = \text{P} \]
\[ \Sigma_1 = \text{NP} \]
\[ \Sigma_2 = \text{NP}^\text{NP} \]
\[ \vdots \]
\[ \Sigma_k = \text{NP}^{\Sigma_{k-1}} \]
\[ \vdots \]

If \( \Sigma_i = \Sigma_{i+1} \) for some \( i \) then \( \text{PH} = \Sigma_i \)

This "polynomial hierarchy collapse" is thought to be extremely unlikely.
postselected circuits:

\[ C_n \]

A decision problem \( L \in \text{postBQP} \) if there is a uniformly generated polynomial-size postselected circuit family \( C_n \) s.t.

\[
\begin{align*}
    x \in L & \implies \Pr[z = 1 \mid y = 0] \geq \frac{2}{3} \\
    x \notin L & \implies \Pr[z = 1 \mid y = 0] \leq \frac{1}{3}.
\end{align*}
\]

Can likewise define \( \text{postBPP} \) by replacing the BQP circuit with a BPP circuit.

Can also define \( \text{postA} \) for a restricted family of BQP circuits \( A \).

Fact: Quantum postselection > classical postselection

\[
\text{postBPP} \quad \subseteq \quad \sum_3 \text{postBQP} \leq \text{PH} \quad \Rightarrow \quad \text{IF postBPP contains postBQP then PH collapses!}
\]

[Han, Hemaspaandra, Thierauf 1997]

[Aaronson 2005]
2. **Classical Hardness of exact simulation**

**Claim:** Suppose $A$ is a restricted circuit family s.t.

$$\text{post } A = \text{post } BQP$$

Suppose there exists an efficient classical algorithm that, given a circuit in $A$, samples from the distribution

$$p(z,y,r) \quad \text{(see (8))}$$

obtained at the output. Then $PH$ collapses.

**Pf:** Take the classical $BPP$ circuit that samples

$$p(z,y,r)$$

and then postselect on $y$. This $post$ $BPP$ circuit exactly simulates the $postselected$ quantum circuit.

$$\text{post } BQP = \text{post } A \leq \text{post } BPP \implies PH \subseteq \Sigma_3$$

The point is that restricted circuit families $A$ such that $\text{post } A = \text{post } BQP$ are hard to (exactly) simulate classically, even if they may be less powerful than general poly-size circuits.

**Examples:**

- $A = \text{depth 3 circuits}$ [Terhal-Divincenzo 2002]
- $A = IQP$ circuits [Bremner-Jozsa-Shepherd 2010]
- $A = QAQA$ circuits [Farhi-Harrow 2016]
Depth-3 circuits

Now let us see an example. We are going to show that postselected depth-3 quantum circuits can simulate postselected quantum circuits of polynomial size. The following is due to Terhal and Divincenzo but we present a simplified argument from [Fenner Green Homer Zhang 2003]:

Firstly, note that the following postselected circuit teleports a single qubit state:

\[ \text{POSTSELECT} \]

\[ \begin{array}{c}
1 \bar{y} \\
1 \bar{y} \\
1 \bar{y} \\
\end{array} \]

An n-qubit state can be teleported using \( n \) parallel copies of the above:

\[ \begin{array}{c}
1 \bar{y} \\
1 \bar{y} \\
1 \bar{y} \\
\end{array} \]
Now suppose we have a quantum circuit which applies 1- or 2-qubit gates $U_1, \ldots, U_m$ to some input basis state $|1\rangle$ followed by measurement/postselection.

$1\rangle \rightarrow U_1 \rightarrow U_2 \rightarrow \ldots \rightarrow U_m \rightarrow \alpha$

We can insert postselected teleportation after the 1st gate to get an equivalent circuit:

$1\rangle \rightarrow U_1 \rightarrow B^{\text{ent}} \rightarrow \alpha$

$10^n \rightarrow B^{\text{ent}} \rightarrow 10^n$

$10^n \rightarrow U_2 \rightarrow U_3 \rightarrow \ldots \rightarrow \alpha$

Now insert postselected teleportation after 2nd, 3rd, \ldots, m-1st gates:

$1\rangle \rightarrow U_1 \rightarrow B^{\text{ent}} \rightarrow \alpha$

$10^n \rightarrow B^{\text{ent}} \rightarrow 10^n$

$10^n \rightarrow B^{\text{ent}} \rightarrow U_2 \rightarrow B^{\text{ent}} \rightarrow \alpha$

$10^n \rightarrow B^{\text{ent}} \rightarrow U_3 \rightarrow B^{\text{ent}} \rightarrow \alpha$

$\ldots$

$10^n \rightarrow B^{\text{ent}} \rightarrow U_m \rightarrow \alpha$

This is a postselected depth-3 circuit that simulates $U_m U_{m-1} \ldots U_1 |1\rangle$. 

The above arguments thus show that no classical efficient algorithm can sample exactly from the output of depth-3 quantum circuits unless 

FA collapses.

(Moreover, depth-2 circuits can be efficiently simulated, see [Terhal D'Vincenzo 2002].)

**IQP circuits**

A second example is the "Instantaneous Quantum Polynomial time" circuit family [Bremner Jozsa Shepherd 2010].

![Diagram](image)

Where

\[
D = \left( \prod_{j < k} e^{i\pi \frac{\omega_{jk}}{8} Z_j Z_k} \right) \left( \prod_{k=1}^{n} e^{i\pi \frac{v_k}{8} Z_k^2} \right)
\]

for some \( \omega_{jk}, v_k \in \{0, 1, 2, \ldots, 7\} \).
See [BJS 2010] for a proof that post-IQP = post-BQP.

\(3\) Approximate Simulation

So far, PH collapses if there exists an efficient exact classical sampler for:

- BQP circuits
- depth-3 circuits
- IQP circuits
- also Boson Sampling [Aaronson Arkhipov 2010]

**Problem:** Not even a quantum computer can exactly sample from \( \rho(x) = |x| U |10\rangle^2 \) (due to noise).

A more realistic task is to sample from \( \hat{\rho} \) s.t.

\[
\sum_x |p(x) - \hat{p}(x)| \leq \epsilon = \frac{1}{\text{poly}(n)}.
\]

Is this task classically hard?

It has been proven only assuming additional conjectures (in addition to PH not collapsing)

for

- Boson Sampling [Aaronson Arkhipov 2010]
- IQP circuits [Bremner Montanaro Shepherd 2015]
- Random quantum circuits [Boixo et al. 2017]
- Random circuits [Aaronson Chen 2016]
- Random Pauli bases [Boosand Fefferman Nirkhe Yazirani 2018]

This classical hardness has been the basis of proposed demonstrations of quantum computational supremacy.
Near term quantum algorithms (??)

Want:
- low circuit depth
- limited connectivity of gates
- robustness to error
- solve useful problem better than classical

Mostly heuristics proposed so far. Many are "hybrid" algorithms that use both quantum and classical computers.

Example 1: Variational quantum eigensolver [Peruzzo et al 2013]

Here the goal is to prepare a low energy state of a Hamiltonian $H$. e.g. for quantum chemistry $H$ describes a molecule.

The quantum hardware has some input output behaviour

$$\begin{array}{c}
\begin{array}{c}
8_1, \ldots, 8_m \quad \text{QC} \quad 14(8_1, \ldots, 8_m) \end{array} \\
\text{classical parameters} \\
\text{(e.g. choices of gates)}
\end{array}$$

The variational quantum eigensolver aims to variationally minimize the energy

$$\langle 14(8_1, \ldots, 8_m) | H | 14(8_1, \ldots, 8_m) \rangle$$

over the set of states produced by the machine.
The \( \text{QAE}- \) algorithm is very simple and consists of:

i) choose initial \( \theta_1, \ldots, \theta_m \)

ii) use QC to prepare \( |\psi(\theta_1, \ldots, \theta_m)\rangle \) and compute its energy \( E_0 \)

iii) use a classical algorithm to choose a new set of parameters \( \theta'_1, \ldots, \theta'_m \) with the aim of reducing energy and start again from ii) with this new choice

\[
\theta_1, \ldots, \theta_m \quad \xrightarrow{\text{QC}} \quad |\psi(\theta_1, \ldots, \theta_m)\rangle \\
\quad \xrightarrow{\text{Measure}} \quad |\psi_1, \psi_2, \ldots\rangle \\

\]

**Example 2: Quantum Approximate Optimization Algorithm**

[Farhi Goldstone Gutfreund 2014]

Again this is a meta-algorithm. Here our goal will be to maximize a given cost function

\[
C : \{0,1\}^n \rightarrow \{0,1,2,\ldots \}
\]

We assume:

1. \( C \) is \( k \)-local \( \iff \) \( C(z) = \sum_{\alpha=1}^{m} C_\alpha(z) \)

\( k = O(1) \)

\( \text{depends on } \leq k \)
and

2) bounded-degree: Each bit $i = 1, \ldots, n$ is involved in $D = O(1)$ clauses $C_x$.

Goal: Compute a bit string $x_0 \in \{0, 1\}^n$ with a large approximation ratio

$$\frac{C(x_0)}{\max_x C(x)}$$

The setup is that we fix a parameter $p = O(1)$ and choose angles

$\alpha_1, \ldots, \alpha_p \in [0, 2\pi]$  
$\beta_1, \ldots, \beta_p \in [0, 2\pi]$

and consider a variational family of states

$$|\psi(x', \beta')\rangle = e^{-i\beta B} e^{-i\beta C} \ldots e^{-i\beta B} e^{-i\beta C} |1^n\rangle$$

where

$$\hat{B} = \sum_{j=1}^{n} X_j$$

$$\hat{C} = \sum_{x \in \{0, 1\}^n} C(x) |1^n\rangle \langle x_0|$$
It is easy to see that $|\psi(x, \beta^n)\rangle$ is prepared by a constant-depth quantum circuit. Since $\hat{C}$ is a k-local operator, this implies we can efficiently classically compute

$$F(x, \beta) = \langle \phi(x, \beta^n) | \hat{C} | \psi(x, \beta^n) \rangle$$

for any parameter choices $x, \beta$. In fact, for $p = O(1)$ one can classically efficiently compute $\hat{a}_0, \hat{b}_0$ such that

$$F(\hat{a}_0, \hat{b}_0)$$

achieves its maximum (it suffices to compute $F(x, \beta)$ on a uniformly spaced grid of parameter values - see [FGG-2014]).

The QAOA algorithm is then:

1. Use classical computer to find $\hat{a}_0, \hat{b}_0$ s.t. $F(\hat{a}_0, \hat{b}_0)$ is maximal.

2. Use quantum computer to prepare

$$|\psi(\hat{a}_0, \hat{b}_0)\rangle$$

3. Measure to get $x \in \{0,1\}^n$.

Steps 2,3 are repeated $L$ times to get

$$2^{n-1} \cdot 2^L \in \{0,1\}^n.$$
Choosing $L = \text{poly}(m)$ ensures w.h.p. that

$$\max \left\{ \sum_{i=1}^{L} C(z_i) \right\} \geq F(\alpha_0, \beta_0)$$

It is an open question whether there exists an optimization problem for which the above beats the best approx. ratio achieved by poly-time classical algorithms.