Gates, Universality, Solovay-Kitaev Theorem
BQP (bounded-error quantum polynomial-time) ≠ its relationship to classical computational models

Recall: Hadamard $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $11 \mapsto \frac{1}{\sqrt{2}} (10 - 11)$

Local unitary transformations ("gates")
- act as identity except on a constant number of qubits
  eg. $I \otimes (\mathbb{C}^{2})_{i}^{\otimes} = \sum_{x} \sum_{x'} \mathbb{C}^{2} \begin{pmatrix} 1 \\ x \end{pmatrix} \begin{pmatrix} 1 \\ x' \end{pmatrix}$
  $U \begin{pmatrix} x \\ x' \end{pmatrix} = \begin{pmatrix} 1 \\ x' \end{pmatrix}$

eg. $\begin{pmatrix} 1 \\ x \end{pmatrix} \begin{pmatrix} 1 \\ x' \end{pmatrix} \begin{pmatrix} 1 \\ x'' \end{pmatrix} \begin{pmatrix} 1 \\ x''' \end{pmatrix} \cdots \begin{pmatrix} 1 \\ x_{n} \end{pmatrix} \mapsto \sum_{x} \sum_{x'} \mathbb{C}^{2} \begin{pmatrix} 1 \\ x \end{pmatrix} \begin{pmatrix} 1 \\ x' \end{pmatrix} \begin{pmatrix} 1 \\ x'' \end{pmatrix} \begin{pmatrix} 1 \\ x''' \end{pmatrix} \cdots \begin{pmatrix} 1 \\ x_{n} \end{pmatrix}$

$= \text{CNOT}_{x} \otimes H_{y} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

want $U = U_{n}U_{n-1} \cdots U_{1}$, with the $U_{i}$'s all local
and from a simple set

Example * CNOT + all one-qubit gates form a universal family
* $\{\text{CNOT}, H, \{1 \otimes \text{Pauli} \} \}$

Def: A set of gates forms a universal family if for every $n$, every $U \in U(2^{n})$, and every $\varepsilon > 0$, a sequence of gates approximates $U$ to within error $\varepsilon$: $\| U - U_{n} \cdots U_{1} \| < \varepsilon$. "dense"

(technically, this is "strict universality"; a weaker notion allows for adding ancilla qubits, simulation [quant-ph/0110031])

Solovay-Kitaev Theorem: Let $G \subset SU(d)$ be a finite set of gates closed under inverses.
Assume $G$ is dense in $SU(d)$. Then for any $U \in SU(d)$, $\varepsilon > 0$,
there are $g_{1}, g_{2}, \ldots, g_{l} \in G$ with
$\| U - g_{1} \cdots g_{l} \| < \varepsilon$ and $l = O\left( \log^{5.5+\frac{5}{\varepsilon}} \right)$.

* "Dense $\Rightarrow$ Efficiently dense"
* $\Rightarrow$ all universal families are basically equivalent. Why?
Lemma: \[ \| U - V \| \leq \sum_{i=1}^{m} \| U_i - V_i \| \]

Proof: Recall \[ \| M \| = \max_{\| \phi \| = 1} \| M \phi \| \]

"hybrid expansion" \[ U - V = U_m U_{m-1} \cdots U_1 - V_m V_{m-1} \cdots V_1 + V_m U_{m-1} \cdots U_1 - V_m V_{m-1} U_{m-2} \cdots U_1 + \cdots + V_m \cdots V_2 U_1 - V_m V_{m-1} \cdots V_1 \]

\[ \| U - V \| \leq \sum_{j=1}^{m} \| V_m \cdots V_{j+1} U_j \cdots U_1 - V_m \cdots V_j U_{j-1} \cdots U_1 \| \]

\[ \| V_m \cdots V_{j+1} (U_j - V_j) U_{j-1} \cdots U_1 \| = \| U_j - V_j \| \]

Consequences:
- All universal families are equivalently efficient
- Quantum computers are not merely an analog computational model
- Eg., Shamir, "Factoring numbers in \((\log n)^{O(1)}\) arithmetic steps" assuming infinite-precision arithmetic
- Work isn't just in storing amplitudes to infinite precision
- Classical computers can simulate quantum computers with exponential overhead

\[
\begin{align*}
\text{EXP} & \xrightarrow{\text{BQP}} \text{PP} \\
\text{PP} & \xrightarrow{\text{PSPACE}} \text{PSPACE} \\
\text{NP} & \xrightarrow{\text{BQP}} \text{PSPACE} \\
\text{P} & \xrightarrow{\text{BPP}} \text{PSPACE}
\end{align*}
\]
Complexity results

1. $P =$ polynomial-time-decidable languages/problems
e.g., can decide whether $N$ is prime or not in $\text{poly}(\log N)$ time

   \[ C_n \rightarrow 0/1 \]
   \[ |C_n| = \mathcal{O}(\text{poly}(n)) \]
   uniformity: "$C_n$" computable in $\text{poly}(n)$ time

2. $\text{BPP} =$ bounded-error probabilistic polynomial time

   \[ x \in \text{PRIMES} \Rightarrow \Pr [C_n(r, x) \neq 1] < \frac{1}{3} \]
   \[ x \notin \text{PRIMES} \Rightarrow \Pr [C_n(r, x) \neq 0] > \frac{2}{3} \]

   "Boosting": Can reduce error to $\frac{1}{2^k}$ by running $\mathcal{O}(k)$ copies with independent $r$, taking majority.

3. $\text{BQP} =$ bounded-error quantum polynomial time

   \[ x : \frac{\text{answer bit}}{107} \rightarrow C_n \rightarrow 107 \]
   poly-uniform, poly-size circuits, with $\leq \frac{1}{3}$ error probability

Note: Boosting still works, by copying the input string $x$ with copies
Claim: \( P \subseteq BQP \) (in particular, majority can be implemented with a quantum circuit)

\[ 1x > \underbrace{U}_{\text{permutation, cannot erase}} \overbrace{1y >} \]

Fredkin gate

\[
\begin{array}{ccc}
a & \rightarrow & a \\
b & \rightarrow & b \\
c & \rightarrow & c
\end{array}
\]

Toffoli gate

\[
\begin{array}{ccc}
a & \rightarrow & a \\
b & \rightarrow & b \\
c & \rightarrow & c + ab \pmod{2}
\end{array}
\]

- can implement AND and NOT gates, universal for classical computation

Claim: \( BPP \subseteq \overline{BQP} \)

Proof:

- If \( C_n \) had non-permutation gates, e.g., \( H \), then should first "measure" the randomness with CNOTs

\[ 10 > \underbrace{10}_{\text{garbage}} \]

principle of deferred measurement: can delay measurement even forever