9/23/10 QIC 710 Lecture 4

Gates, Universality, Solovay-Kitaev Theorem

BQP (bounded-error quantum polynomial-time) & its relationship to classical computational models

Recall: Hadamard $-\boxed{H}-$ $|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, $|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$

CNOT: $a \to a$, $b \to a \oplus b$

Local unitary transformations ("gates")

— act as identity except on a constant number of qubits

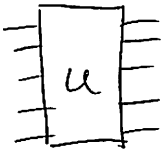
eg. $\mathbb{1} \otimes U_{i,i+1}$

$\sum_x \alpha_x |x\rangle$ — $U_{i,i+1}$ — $\sum_x \beta_x |x\rangle$

$2^n \times 2^n$ sparse

$$\sum_x \alpha_x |x_1 \cdots x_i x_{i+1} \cdots x_n\rangle \longmapsto \sum_x \alpha_x |x_1 \cdots x_{i-1}\rangle \otimes (U|x_i x_{i+1}\rangle) \otimes |x_{i+2} \cdots x_n\rangle$$

eg. $= CNOT_{1,2} \otimes H_3 = \begin{pmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1&1\\ 1&-1 \end{pmatrix} = \begin{pmatrix} H&0&0&0\\ 0&H&0&0\\ 0&0&0&H\\ 0&0&H&0 \end{pmatrix}$



want $U = U_k U_{k-1} \cdots U_1$, with the U_i's all local and from a simple set

Example * CNOT + all one-qubit gates form a universal family

* $\{CNOT, H, \begin{pmatrix} 1&0\\ 0&e^{i\pi/4} \end{pmatrix}\}$ " " "

Def: A set of gates forms a universal family if for every n, every $U \in \mathcal{U}(2^n)$, and every $\varepsilon > 0$, a sequence of gates approximates U to within error ε: $\|U - U_k \cdots U_2 U_1\| < \varepsilon$. "dense"

(technically, this is "strict universality"; a weaker notion allows for adding ancilla qubits, simulation [quant-ph/0201041])

Solovay-Kitaev Theorem: Let $G \subset SU(d)$ be a finite set of gates closed under inverses. [good reference: quant-ph/0111031]

Assume G is dense in $SU(d)$. Then for any $U \in SU(d)$, $\varepsilon > 0$, $\delta > 0$, there are $g_1, g_2, \ldots, g_\ell \in G$ with

$$\|U - g_\ell \cdots g_2 g_1\| < \varepsilon \quad \text{and} \quad \ell = O\left(\log^{3+\delta} \tfrac{1}{\varepsilon}\right).$$

* "Dense $\Rightarrow$ Efficiently dense"

* $\Rightarrow$ all universal families are basically equivalent. Why?

$U_1, U_2, \ldots, U_m$ ideal gates $\quad U = U_m \cdots U_1$

$V_1, V_2, \ldots, V_m$ actual gates $\quad V = V_m \cdots V_1$

Lemma: $\|U - V\| \leq \sum_{i=1}^{m} \|U_i - V_i\|$ "Errors add"

Proof: Recall $\|M\| = \max_{|\phi\rangle} \frac{\|M|\phi\rangle\|}{\||\phi\rangle\|}$.

"hybrid expansion"

$$U - V = U_m U_{m-1} \cdots U_1 = U_m U_{m-1} \cdots U_1 - V_m U_{m-1} \cdots U_1$$
$$- V_m V_{m-1} \cdots V_1 \quad + V_m U_{m-1} \cdots U_1 - V_m V_{m-1} U_{m-2} \cdots U_1$$
$$+ V_m V_{m-1} U_{m-2} \cdots U_1 - \cdots$$
$$+ V_m \cdots V_2 U_1 - V_m V_{m-1} \cdots V_1$$

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

$$\|V_m \cdots V_{j+1}(U_j - V_j) U_{j-1} \cdots U_1\| = \|U_j - V_j\| \checkmark \quad \square$$

Consequences:

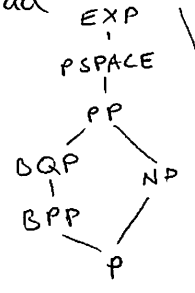
* All universal families are equivalently efficient

  i.e. a circuit of T gates from G_1 can be implemented w/in ε by $T \cdot (\log \frac{1}{\varepsilon})^{O(1)}$ gates from G_2

* Quantum computers are not merely an analog computational model Eg., Shamir, "Factoring numbers in $O(\log n)$ arithmetic steps" 1979
  assuming infinite-precision arithmetic
  —work isn't just in storing amplitudes to infinite precision

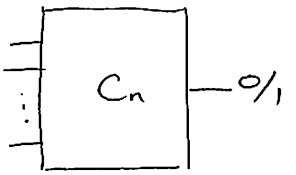
* Classical computers can simulate quantum computers with exponential overhead

In fact, BQP ⊆ PP



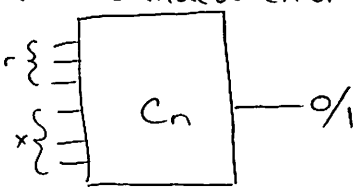
Complexity results

1. P = polynomial-time-decidable languages / problems
   eg. can decide whether N is prime or not in poly(log N) steps



$|C_n| = O(\text{poly}(n))$
uniformity: "C_n" computable in poly(n) time

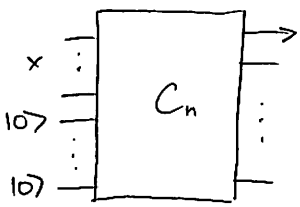
2. BPP = bounded-error probabilistic polynomial time



$x \in \text{PRIMES} \Rightarrow \mathbb{P}_R[C_n(R,x) = 1] \geq \frac{2}{3}$
$x \notin \text{PRIMES} \Rightarrow \mathbb{P}_R[C_n(R,x) = 0] \geq \frac{2}{3}$.

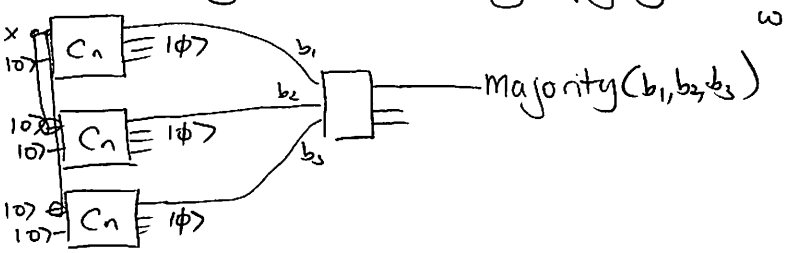
"Boosting": Can reduce error to $\frac{1}{2^k}$ by running $O(k)$ copies with independent r, taking majority.

3. BQP = bounded-error quantum polynomial time



classically
poly-uniform, poly-size circuits,
with $\leq \frac{1}{3}$ error probability

Note: Boosting still works, by copying the input string x. with CNOTs

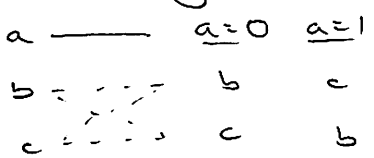


Claim: $P \subseteq BQP$ (in particular, majority can be implemented with a quantum circuit)

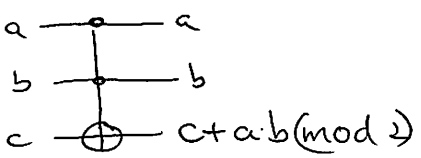
- permutation, cannot erase

reversible computing

Fredkin gate



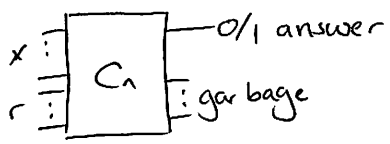
Toffoli gate



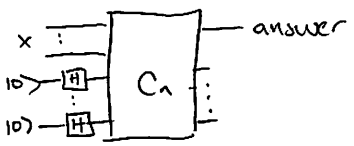
- can implement AND and NOT gates, universal for classical computation □

Claim: $BPP \subseteq BQP$.

Proof:

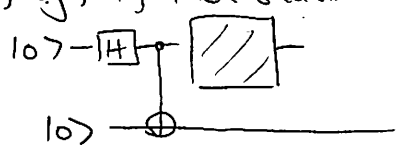


reversible BPP circuit



BQP circuit ✓ □

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



principle of deferred measurement: can delay measurement even forever)