CS121 Lecture 25: Quantum Computing Nov 26

Quantum Computing Summary

- Quantum mechanics in computing
- Adds computational power?
- Define BQP (problems solvable in quantum poly time)
- $P \subseteq BQP \subseteq EXP$
  - * both believed to be strict
- relation btwn NP and BQP unknown
  - * believed that $NP \nsubseteq BQP$
    if $3SAT \in BQP$ then $NP \subseteq BQP$

Physics 500BC – 1920s: Clockwork Universe

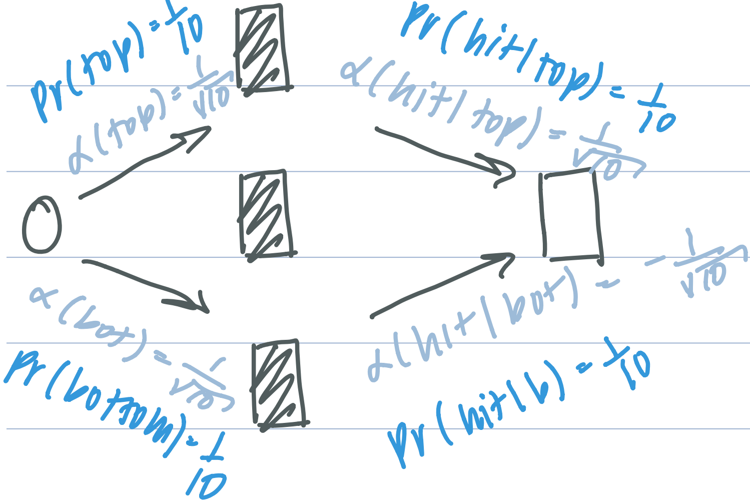
← quantum computing is not clock work

- physical theory has basic objects ("particles") and forces btwn them
- Given state of all particles at time t, can compute state at time $t+1$
- EX: Newtonian mechanics, Maxwell's Eqns, Special and General relativity

Quantum Weirdness

- every event has an amplitude: $[-1, 1]$
- probability of event is square of amplitude

- Event happens w/ α^2 and doesn't w/ $1-\alpha^2$



$$Pr(hit) = \left(\frac{1}{\sqrt{10}} \cdot \frac{1}{\sqrt{10}} - \frac{1}{\sqrt{10}} \cdot \frac{1}{\sqrt{10}}\right)^2$$
$$= 0$$

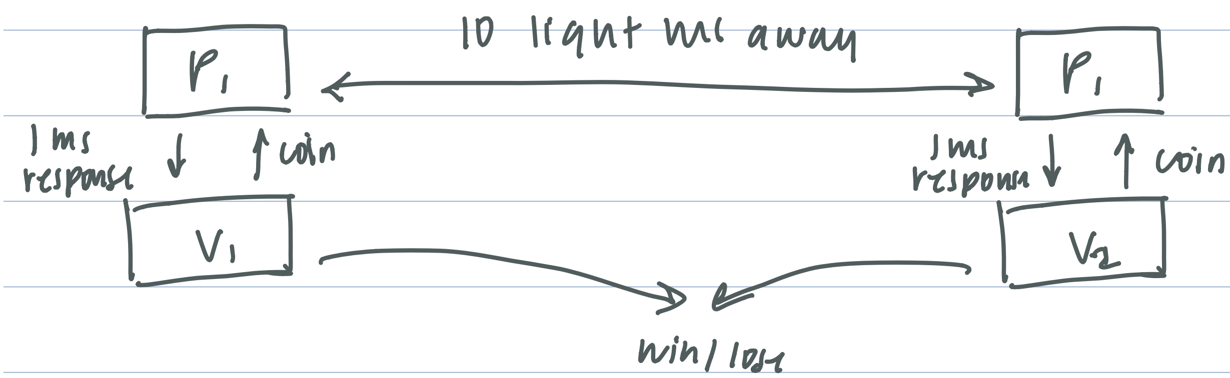
Bell's Inequality

killed the clockwork theory

Thm: $\exists$ game played btwn 2 provers and verifier s.t. if P1 and P2 only share classical bits and can't communicate, $Pr[win] \le 3/4$

prove the existance of non-local long-distance entanglement

$\exists$ P1 and P2 sharing quantum state not communicating s.t. $Pr[win] \ge 0.85$ ← can't be explained by classical clockwork theories



Quantum View of the World

n obj, on or off → $x \in \{0,1\}^n$ w/ prob $\alpha(x)^2$

- state of the world: 2^n-dim vector $\vec{v} = (\alpha(0^n), \alpha(0^{n-1}1) \ldots)$
  - $\vec{v}$ satisfies $v_1^2 + v_2^2 + \cdots + v_{2^n}^2 = 1$
  - operations preserve this property and are linear

unitary matrices

Quantum Operations

- The state of one qubit is unit vector $v \in \mathbb{R}^2$
- One qubit gate is a unitary matrix mapping $\mathbb{R}^2$ to $\mathbb{R}^2$

Interpretation problem

↳ how to interpret the models

Quantum Operations

- state is unit vector $v \in \mathbb{R}^2$
- one qubit gate is unitary matrix mapping $\mathbb{R}^2$ to $\mathbb{R}^2$

ex: $X = \begin{array}{c|cc} & 1 & 0 \\ \hline 1 & 0 & 1 \\ 0 & 1 & 0 \end{array}$ $\quad X\begin{pmatrix} v_0 \\ v_1 \end{pmatrix} = \begin{pmatrix} v_1 \\ v_0 \end{pmatrix}$

$X|b\rangle = |NOT(b)\rangle$

Quantum Circuit

- Circuit takes n qubits to n qubits
- implements unitary matrix $\mathbb{R}^{2^n} \to \mathbb{R}^{2^m}$

Computes

- Quantum circ C w/ $n+m$ inputs/outputs computes a function if for every $x \in \{0,1\}^n$, we measure first coordinate of state $v = U_C|x0^m\rangle$, get $f(x)$ w.p. $\geq 2/3$ ← reminiscent of BPP

BQP/poly

- contains F s.t. for every $n \in \mathbb{N}$, F_n has poly-size quantum circuit

f computed by s gate NAND circuit $\rightarrow$ f computed by s-gate quantum circuit

$P_{/poly} \subseteq BQP_{/poly}$

BQP

- contains F s.t. $\exists$ poly-time TM that for all n outputs quantum circuit computing F_n

$P \subseteq BQP$ $\quad$ $BPP \subseteq BQP$ $\quad$ $BQP \subseteq EXP$

exponentially-long state vector

$BQP \subseteq PSPACE$

Feinman path diagrams

Possible

$P = BQP = BPP \subseteq P_{/poly}$

$BPP \subseteq PSPACE = BQP$ $\leftarrow$ not likely

Shor's Algo

Input: Boolean circuit C computing $f: \{0, 1, \ldots N\} \rightarrow \{0, \ldots N-1\}$

$N = 2^n$

Output: p s.t. $\forall_{x \in [N]}\ f(x) = f(x + p \bmod N)$

- Algo for factoring using period finding
- Quantum algo for period finding using Quantum Fourier Transform

period of f = LCM of period of waves

Fourier Transform

Input: $f : \{0, 1, \ldots N-1\} \to \mathbb{R}$

Output: coeffs $\hat{f}$ expressing $f(x) = \sum \hat{f}(j) \chi_j(x)$

$\chi(j)$ = j^{th}-wave function

$f \mapsto \hat{f}$ is linear, can be computed by $N \times N$ matrix in $O(N^2)$