Extended Church-Turing Thesis

- The belief that TMs formalize our intuitive notion of an efficient algorithm is:
  - Quantum computation challenges this belief

A different model

- Infinite tape of a Turing Machine is an idealized model of computer
- Real computer is a Finite Automaton (!)
  - n bits of memory
  - 2^n states
Model of randomized computation

Possible states at time $t$: \[ \sum p_i = 1 \quad p_i \in \mathbb{R}^+ \]

State at time $t$ \[
\begin{pmatrix}
0 & \frac{1}{4} & 0 & \frac{1}{2} \\
\frac{1}{2} & 0 & \frac{1}{4} & 0 \\
0 & \frac{1}{2} & 0 & \frac{1}{4} \\
0 & 0 & 0 & 0
\end{pmatrix}
= \begin{pmatrix}
\frac{3}{4} \\
\frac{1}{2} \\
\frac{1}{4} \\
0
\end{pmatrix}
\]

State at time $t+1$

"Stochastic matrix" sum in each column $= 1$

Model of quantum computation

Possible states at time $t$: \[ \sum |c_i|^2 = 1 \quad c_i \in \mathbb{C} \]

State at time $t$ \[
\begin{pmatrix}
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}
\end{pmatrix}
= \begin{pmatrix}
0 \\
1
\end{pmatrix}
\]

State at time $t+1$

"Unitary matrix" preserves $L_2$ norm

One quantum register

- Register with $n$ qubits; shorthand for basic states

\[ |0 \rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad |1 \rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \]

Shorthand for general state

\[ |\psi \rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{2^n-1} \end{pmatrix} = \sum c_i |i \rangle \]

Two quantum registers

- Registers with $n, m$ qubits: shorthand for $2^{nm}$ basic states:

\[ |00 \rangle = |0 \rangle \otimes |0 \rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01 \rangle = |0 \rangle \otimes |1 \rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \]

\[ |10 \rangle = |1 \rangle \otimes |0 \rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11 \rangle = |1 \rangle \otimes |1 \rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \]
Two quantum registers

shorthand for general unentangled state

\[ |a\rangle = \sum_{i,j} a_{i,j} |i\rangle |j\rangle \]

example:

\[ \frac{1}{\sqrt{2}} (|0\rangle |0\rangle + |1\rangle |1\rangle) \]

Partial measurement

- general state:
  \[ |a\rangle = \sum_{i,j} a_{i,j} |i\rangle |j\rangle = \sum_{i} \left( \sum_{j} a_{i,j} |i\rangle \right) \otimes |j\rangle \]
  - if measure just 2nd register, see state \(|j\rangle\) in 2nd register with probability \(\sum_{i} |a_{i,j}|^2\)
  - state collapses to:
  \[ \alpha \left( \sum_{i} a_{i,j} |i\rangle \right) \otimes |j\rangle \]

EPR “paradox”

\[ \frac{1}{\sqrt{2}} (|0\rangle |0\rangle + |1\rangle |1\rangle) \]

- register 1 in LA, register 2 sent to NYC
- measure register 2
  - probability \%: see \(|0\rangle\) state collapses to \(|0\rangle |0\rangle\)
  - probability \%: see \(|1\rangle\) state collapses to \(|1\rangle |1\rangle\)
  - measure register 1
  - guaranteed to be same as observed in NYC
  - instantaneous “communication”

Quantum complexity

- classical computation of function \(f\)
  \[ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \]

- some functions are easy, some hard
- need to measure “complexity” of \(M_f\)

Quantum complexity

- analogous notion of “local operation” for quantum systems
- in each step
  - split qubits into register of 1 or 2, and rest
  - operate only on small register
- “efficient” in both settings: # local operations polynomial in # bits \(n\)
Efficiently quantum computable functions

- For every $f : \{0,1\}^n \to \{0,1\}^m$ that is efficiently computable classically
- the unitary transform $U_f$:
  $$U_f(i|j) = |i\rangle|f(i) + j\rangle$$
- note, when 2nd register = $|0\rangle$:
  $$U_f(i|0) = |i\rangle|f(i)\rangle$$

Shor’s factoring algorithm

- well-known: factoring equivalent to order finding
  - input: $y, N$
  - output: smallest $r > 0$ such that $y^r = 1 \mod N$ 

Factoring: step 1

- given $y, N$; $f(i) = y^i \mod N$; have $\sum_i |i\rangle|f(i)\rangle$
  - in each vector, period = $r$, the order of $y \mod N$
  - offset depends on 2nd register

Factoring: step 2

- measure register 2
- state collapses to:
  $$|f(x)\rangle = \sum_{|r|} |r + x| f(x)$$
  Key: period = $r$ (the number we are seeking)
Factoring: step 3

- Apply FT to register 1
- Measure register 1
- Obtain $b$
- Determine $r$ from $b$
  (classically, basic number theory)

Quantum computation

- If can build quantum computers, they will be capable of factoring in polynomial time
  - Big "if"
- Do not believe factoring possible in polynomial time classically
  - But factoring in $P$ if $P = NP$
- Serious challenge to extended Church-Turing Thesis

The very last slide

- Course review slides on website
- Fill out TQFR surveys!
- Course to consider
  - CS139 (advanced algorithms)
  - CS150 (probability and computation)
  - CS151 (complexity theory)
  - CS153 (current topics in theoretical CS)
- Good luck
  - On final
  - In CS, at Caltech, beyond…
- Thank you!