Outline

• Challenges to Extended Church-Turing
  – randomized computation
  – quantum computation

For use later...

• Fourier transform:

  \[
  \begin{array}{cc}
  \text{time domain} & \text{frequency domain} \\
  \hline
  \text{time domain} & \text{frequency domain} \\
  \hline
  r & \text{can recover } r \text{ from position}
  \end{array}
  \]

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 deterministic computation

\[
\begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\end{pmatrix}
\]

state at time t

state at time t+1

2^n possible basic states

one 1 per column

Model of randomized computation

\[
\begin{pmatrix}
p_0 \\
p_1 \\
p_2 \\
p_3 \\
\vdots \\
p_{2^n-1}
\end{pmatrix}
\]

possible states at time t: \(\sum p_i = 1\) \(p_i \in \mathbb{R}^+\)

\[
\begin{pmatrix}
0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\end{pmatrix}
\]

state at time t

state at time t+1

"stochastic matrix" sum in each column = 1

\[
\begin{pmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
\end{pmatrix}
\]

\[
\begin{pmatrix}
0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
\end{pmatrix}
\]
Model of randomized computation

- at end of computation, see specific state
- demand correct result with high probability
- think of as "measuring" system:

\[
\begin{pmatrix}
0 \\
1 \\
1 \\
1
\end{pmatrix} \Rightarrow \begin{pmatrix}
0 \\
0 \\
0 \\
0
\end{pmatrix}
\]

see i\textsuperscript{th} basic state with probability \( p_i \).

Model of quantum computation

- at end of computation, see specific state
- think of as "measuring" system:

\[
\begin{pmatrix}
c_0 \\
c_1 \\
c_2 \\
c_3
\end{pmatrix} \Rightarrow \begin{pmatrix}
0 \\
0 \\
0 \\
0
\end{pmatrix}
\]

see i\textsuperscript{th} basic state with probability \( |c_i|^2 \).

One quantum register

- register with \( n \) qubits; shorthand for basic states

\[
\begin{pmatrix}
0 \\
1 \\
2^{n-1}
\end{pmatrix}
\]

- shorthand for general state

\[
|\psi\rangle = \sum a_i |i\rangle
\]

Two quantum registers

- registers with \( n, m \) qubits: shorthand for \( 2^n \times 2^m \) basic states:

\[
\begin{pmatrix}
0 \\
1
\end{pmatrix} \otimes \begin{pmatrix}
0 \\
1
\end{pmatrix} = \begin{pmatrix}
0 \\
0
\end{pmatrix}
\]

\[
\begin{pmatrix}
1 \\
0
\end{pmatrix} \otimes \begin{pmatrix}
0 \\
1
\end{pmatrix} = \begin{pmatrix}
1 \\
0
\end{pmatrix}
\]

Two quantum registers

- shorthand for general unentangled state

\[
|\psi\rangle = \sum a_{ij} |i\rangle |j\rangle
\]

- shorthand for any other state (entangled state)

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

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”

- register 1 in LA, register 2 sent to NYC
- measure register 2
  - probability $\frac{1}{2}$: see $|0\rangle$ state collapses to $|0\rangle |0\rangle$
  - probability $\frac{1}{2}$: 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 $f$
- some functions are easy, some hard
- need to measure “complexity” of $M_f$

Efficiently quantum computable functions

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

- Fourier Transform
  - $N=2^n$, $\omega$ such that $\omega^N = 1$; unitary matrix $FT = \left( \begin{array}{ccc}
\omega^0 & \omega^1 & \cdots & \omega^{N-1} \\
\omega^1 & \omega^2 & \cdots & \omega^{2(N-1)} \\
\vdots & \vdots & \ddots & \vdots \\
\omega^{N-1} & \omega^{(N-1)^2} & \cdots & \omega^{(N-1)^{N-1}}
\end{array} \right)$
  - usual FT dimension $n$; this is dimension $N$
  - note: $FT\cdot |0\rangle = \text{all ones vector}$

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

input: $y, N$

- start state: $|0\rangle|0\rangle$
- apply FT on register 1: $(\sum_i |i\rangle) \otimes |0\rangle$
- apply $U_f$ for function $f(i) = y^i \mod N$

"quantum parallelization"

Factoring: step 2

- measure register 2
- state collapses to:

```
1 0 1 0 1 0 0 0
0 0 1 0 1 0 0 0
```

Key: period = $r$
(the number we are seeking)

Factoring: step 3

- Apply FT to register 1
- large in positions $b$ such that $r\cdot b$ close to $N$

- 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!