CS21
Decidability and Tractability

Lecture 27

March 12, 2014

Outline

- "Challenges to the (extended) Church-Turing Thesis"
  - randomized computation
  - quantum computation

Extended Church-Turing Thesis

- the belief that TMs formalize our intuitive notion of an efficient algorithm is:

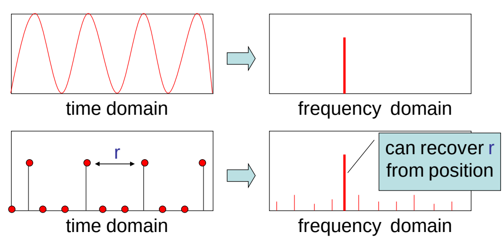
<u>The "extended" Church-Turing Thesis</u>

everything we can compute in time $t(n)$ on a physical computer can be computed on a Turing Machine in time $t(n)^{O(1)}$ (polynomial slowdown)

- quantum computation challenges this belief

For use later…

- Fourier transform:



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

$$\begin{pmatrix}1\\0\\0\\0\\\vdots\\0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\\\vdots\\0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\\\vdots\\0\end{pmatrix}\cdots\begin{pmatrix}0\\0\\0\\0\\\vdots\\1\end{pmatrix}$$

2^n possible basic states

state at time t+1

state at time t

one 1 per column

$$\begin{pmatrix}0&0&0&0\\1&0&0&0\\0&0&1&0\\0&1&0&1\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

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:
$\sum p_i = 1 \quad p_i \in \mathbb{R}^+$

state at time t

state at time t+1

"stochastic matrix"
sum in each column = 1

$$\begin{pmatrix} 0 & \frac{1}{4} & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{4} & 0 & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & 1 & \frac{1}{4} \\ 0 & \frac{1}{4} & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{3}{8} \\ \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{8} \end{pmatrix}$$

Model of randomized computation

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

$$\begin{pmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \\ \vdots \\ p_{2^n-1} \end{pmatrix} \Rightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

see i^{th} basic state with probability p_i

Model of quantum computation

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{2^n-1} \end{pmatrix}$$

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

state at time t

state at time t+1

"unitary matrix"
preserves L_2 norm

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Model of quantum computation

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

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{2^n-1} \end{pmatrix} \Rightarrow \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

see i^{th} basic state with probability $|c_i|^2$

One quantum register

- register with n qubits; shorthand for basic states

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots |2^n-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

shorthand for general state

$$|c\rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_{2^n-1} \end{pmatrix} = \sum c_i |i\rangle$$

Two quantum registers

- registers with n, m qubits: shorthand for 2^{n+m} basic states:

$$|0\rangle|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |0\rangle|1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|1\rangle|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |1\rangle|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Two quantum registers

shorthand for general unentangled state

$$|c\rangle|d\rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{2^n-1} \end{pmatrix} \otimes \begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ \vdots \\ d_{2^m-1} \end{pmatrix} = \sum_{i,j} c_i d_j |i\rangle|j\rangle$$

- shorthand for any other state (entangled 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:

  $$|a\rangle = \sum_{i,j} a_{i,j}|i\rangle|j\rangle = \sum_j (\sum_i a_{i,j}|i\rangle) \otimes |j\rangle$$

- if measure just the 2nd register, see state $|j\rangle$ in 2nd register with probability $\sum_i |a_{i,j}|^2$

normalization constant

- 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 ½: see $|0\rangle$, state collapses to $|0\rangle|0\rangle$
  - probability ½: 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

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

x^{th} position

$f(x)^{th}$ position

M_f = transition matrix for f

- some functions are easy, some hard
- need to measure "complexity" of M_f

Quantum complexity

- one measure: complexity of f =

  length of shortest sequence of local operations computing f

- example local operation:

position x = 0010

logical OR

position x' = 1010

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

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 $f:\{0,1\}^n \rightarrow \{0,1\}^m$ 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
  - $N=2^n$; ω such that $\omega^N = 1$; unitary matrix FT =

$$\begin{pmatrix} (\omega^0)^0 & (\omega^0)^1 & (\omega^0)^2 & \cdots & (\omega^0)^{N-1} \\ (\omega^1)^0 & (\omega^1)^1 & (\omega^1)^2 & \cdots & (\omega^1)^{N-1} \\ (\omega^2)^0 & (\omega^2)^1 & (\omega^2)^2 & \cdots & (\omega^2)^{N-1} \\ \vdots & & & & \\ (\omega^{N-1})^0 & (\omega^{N-1})^1 & (\omega^{N-1})^2 & \cdots & (\omega^{N-1})^{N-1} \end{pmatrix}$$

  - usual FT dimension n; this is dimension N
  - note: FT $\cdot$ $|0\rangle$ = all ones vector

Shor's factoring algorithm

- well-known: factoring equivalent to order finding
  - input: y, N
  - output : smallest r>0 such that

$y^r = 1 \bmod N$

Factoring: step 1

input: y, N

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

$$U_f\left(\left(\sum_i |i\rangle\right) \otimes |0\rangle\right) = \sum_i |i\rangle|f(i)\rangle$$

"quantum parallelization"

Factoring: step 1

- given y, N; $f(i) = y^i \bmod N$; have $\sum_i |i\rangle|f(i)\rangle$

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} |1\rangle + \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \\ 1 \\ \vdots \\ 0 \\ \vdots \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} |2\rangle + \cdots +$$

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:

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} |f(s)\rangle = \sum_{j=0}^{\lfloor 2^n/r \rfloor} |jr+s\rangle|f(s)\rangle$$

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

Factoring: step 3

- Apply FT to register 1

$$FT \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \text{small} \\ \text{large} \\ \vdots \\ \text{small} \\ \text{small} \\ \text{small} \\ \vdots \\ \text{small} \\ \vdots \\ \text{large} \\ \text{small} \\ \vdots \\ \text{small} \end{pmatrix}$$

large in positions b such that r·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

- Fill out TQFR surveys!
- Course to consider
  - CS138 (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!