BU CS 332 – Theory of Computation

https://forms.gle/XhdePDBNMYMw3xyCA

Lecture 19:

- Asymptotic Notation
- Time/Space Complexity
- Complexity Class P

Reading:

Sipser Ch 7.1, 7.2, 8.0

Mark Bun

November 17, 2022

Where we are in CS 332

Automata	Computability	Complexity

Previous unit: Computability theory
What kinds of problems can / can’t computers solve?

Final unit: Complexity theory
What kinds of problems can / can’t computers solve under constraints on their computational resources?

Time and space complexity

Today: Start answering the basic questions

1. How do we measure complexity? (as in CS 330)

2. Asymptotic notation (as in CS 330)

3. How robust is the TM model when we care about measuring complexity?

4. How do we mathematically capture our intuitive notion of “efficient algorithms”?

Time and space complexity

Time complexity of a TM = Running time of an algorithm

= Max number of steps as a <u>function</u> of input length n

↑

read / write / move

Space complexity of a TM = Memory usage of algorithm

= Max number of <u>tape cells</u> as a <u>function</u> of input length n

Example

In how much time/space can a basic single-tape TM decide $A = \{0^m1^m \mid m \geq 0\}$?

<u>Ex:</u> $w = 000111$

O(n) 1. Single left-right scan

2. First run: $\cancel{0}00\cancel{1}11 \leftarrow O(n)$

Second run: $\cancel{0}\cancel{0}0\cancel{1}\cancel{1}1 \leftarrow O(n)$

O(n) tries

Third run: $\cancel{0}\cancel{0}\cancel{0}\cancel{1}\cancel{1}\cancel{1} \leftarrow O(n)$

3. Accept

Let's analyze one particular TM M:

M = "On input w:

1. Scan input and reject if not of the form 0^*1^*
2. While input contains both 0's and 1's:

   Cross off one 0 and one 1

3. Accept if no 0's and no 1's left. Otherwise, reject."

Example

M = "On input w:

1. Scan input and reject if not of the form 0^*1^*
2. While input contains both 0's and 1's: ← $O(n)$

   Cross off one 0 and one 1 ← $O(n)$

3. Accept if no 0's and no 1's left. Otherwise, reject."

What is the time complexity of M?

~~a) $O(1)$ [constant time]~~

b) $O(n)$ [linear time]

$\boxed{\text{c)}}$ $O(n^2)$ [quadratic time]

d) $O(n^3)$ [cubic time]

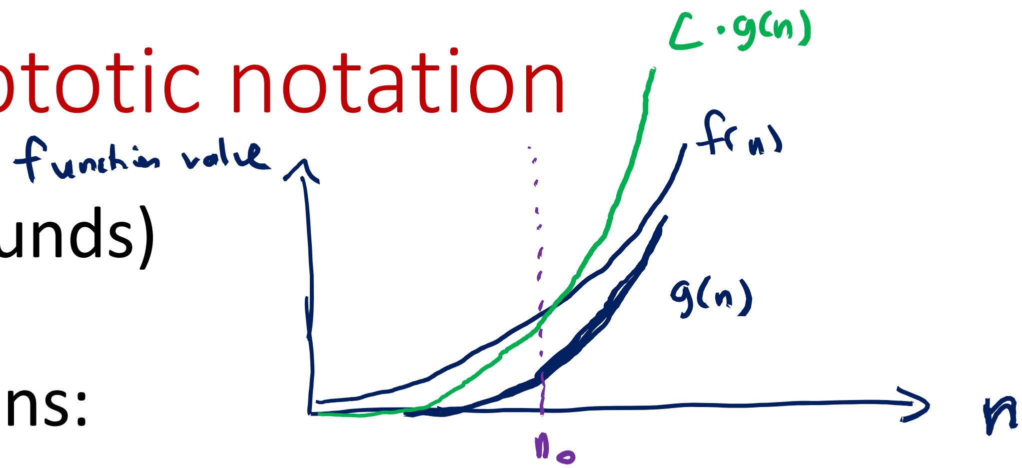
$$\underbrace{O(n)}_{\text{step 1}} + \underbrace{O(n)}_{\text{\# times through step 2 outer loop}} \cdot \overbrace{O(n)}^{\text{step 2 inner loop}} + \underbrace{O(n)}_{\text{step 3}}$$

$$= O(n^2)$$

What is the space complexity of M?

$O(n)$

Review of asymptotic notation



O-notation (upper bounds)

$f(n) = O(g(n))$ means:

There exist constants $c > 0, n_0 > 0$ such that

$f(n) \le cg(n)$ for every $n \ge n_0$

Example: $2n^2 + 12 = O(n^3)$ $(c = 3, n_0 = 4)$

IF $n \ge n_0 = 4$: $2n^2 + 12 \le 2n^2 + n^2$ $[n \ge 4 \Rightarrow n^2 \ge 16 \ge 12]$

$= 3n^2$

$[n \ge 1]$ $\le 3n^3 = cn^3$.

Properties of asymptotic notation:

Transitive:

$f(n) = O(g(n))$ and $g(n) = O(h(n))$ means $f(n) = O(h(n))$

Ex: $n = O(n^2)$ $\quad n^2 = O(n^3)$ $\Rightarrow$ $n = O(n^3)$

Not reflexive:

$f(n) = O(g(n))$ does not mean $g(n) = O(f(n))$

Example: $f(n) = 2n^2,\ g(n) = n^3$

$2n^2 = O(n^3)$ but n^3 is not $O(2n^2)$

Alternative (better) notation: $f(n) \in \underbrace{O(g(n))}$ $= \{h(n) \mid \exists\, c, n_0\ \forall n \geq n_0\ g(n) \leq c\,h(n)\}$

Examples

$f(n) = \Omega(g(n))$ if $g(n) = O(f(n))$
$f(n) = \Theta(g(n))$ if $f(n) = O(g(n))$
and $f(n) = \Omega(g(n))$

- $10^6 n^3 + 2n^2 - n + 10 = O(n^3)$

$= O(n^4)$, $= O(n^{27})$, $= O(2^n)$ [Also true, but less interesting]

- $\sqrt{n} + \log n = O(n)$

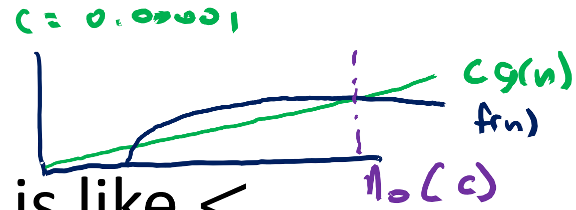
$= O(\sqrt{n})$

[all logs grow slower than all polynomials]

- $n(\log n + \sqrt{n}) = O(n^2)$

$n \log n + n\sqrt{n} = O(n\sqrt{n}) = O(n^{3/2})$

Little-oh



If O-notation is like $\leq$, then o-notation is like $<$

$f(n) = o(g(n))$ means:

Big-O | Little-o
$\exists c \; \exists n_0 \ldots$ | $\forall c \; \exists n_0$

For every constant $c > 0$, there exists $n_0 > 0$ such that

$f(n) \leq cg(n)$ for every $n \geq n_0$

$\iff \forall c \; \exists n_0$ s.t. $\frac{f(n)}{g(n)} \leq c \;\; \forall n \geq n_0 \iff \lim_{n \to \infty} \frac{f(n)}{g(n)} = 0$

Example: $2n^2 + 12 = o(n^3) \qquad (n_0 = \max\{4/c, 3\})$

~~Proof.~~ Let $c > 0$ be arbitrary

Set $n_0 = \max\{4/c, 3\}$

$2n^2 + 12 \leq 2n^2 + 2n^2 \quad [n \geq 3]$

$\leq 4n^2$

$\leq (cn)\, n^2 \quad [n \geq 4/c]$

$= cn^3$

Proof 2

$\lim_{n \to \infty} \frac{2n^2 + 12}{n^3} = \lim_{n \to \infty} \frac{2}{n} + \frac{12}{n^3}$

$= 0.$

True facts about asymptotic expressions

Which of the following statements is true about the function $f(n) = 2^n$?

a) $f(n) = O(3^n)$ ✓ $2^n \leq 3^n \ \forall n$

b) $f(n) = o(3^n)$ ✓ $\lim_{n \to \infty} \frac{2^n}{3^n} = \lim_{n \to \infty} \left(\frac{2}{3}\right)^n = 0$

c) $f(n) = O(n^2)$ ✗

All exponentials b^n grow faster than all polynomials n^c

d) $n^2 = O(f(n))$ ✓

Asymptotic notation within expressions

Asymptotic notation within an expression is shorthand for "there exists a function satisfying the statement"

Examples:

- $n^{O(1)}$ means: $n^{f(n)}$ where $f(n) = O(1)$

  $\Leftrightarrow n^c$ "for some constant c"

- $n^2 + O(n)$ means: $n^2 + f(n)$ for some $f(n) = O(n)$

- $(1 + o(1))n$ means: $(1 + f(n)) \cdot n$ for some $f(n) = o(n)$

  $\Leftrightarrow n + n \cdot o(1)$

FAABs: Frequently asked asymptotic bounds

- **Polynomials.** $a_0 + a_1 n + \ldots + a_d n^d$ is $O(n^d)$ if $a_d > 0$
- **Logarithms.** $\log_a n = O(\log_b n)$ for all constants $a, b > 0$

  $\log_a n = \frac{\log_b n}{\log_b a} = O(\log_b n)$

  For every $c > 0$, $\log n = o(n^c)$

  $\log n = o(n^{0.0000001})$

- **Exponentials.** For all $b > 1$ and all $d > 0$, $n^d = o(b^n)$

  $n^{99999} = o((1.00001)^n)$

- **Factorial.** $n! = n(n-1)\cdots 1$

  By Stirling's formula,

  $n^n = (2^{\log n})^n = 2^{n \cdot \log n}$

$$n! = (\sqrt{2\pi n})\left(\frac{n}{e}\right)^n (1 + o(1)) = 2^{O(n \log n)}$$

Time and Space Complexity

Running time analysis

Time complexity of a TM (algorithm) = maximum number of steps it takes on a worst-case input

input length $|w|$ # of steps TM takes

Formally: Let $f : \mathbb{N} \rightarrow \mathbb{N}$. A TM M runs in time $f(n)$ if on every input $w \in \Sigma^n$, M halts on w within at most $f(n)$ steps

- Focus on worst-case running time: Upper bound of $f(n)$ must hold for all inputs of length n
- Exact running time $f(n)$ does not translate well between computational models / real computers. Instead focus on asymptotic complexity.

Time complexity classes

Let $f : \mathbb{N} \rightarrow \mathbb{N}$

$\mathrm{TIME}(f(n))$ is a set ("class") of languages:

"complexity class"

= set of problems solvable in time $O(f(n))$

A language $A \in \mathrm{TIME}(f(n))$ if there exists a basic single-tape (deterministic) TM M that

1) Decides A, and

2) Runs in time $O(f(n))$

$\mathrm{TIME}(n^2) =$

$\{A \mid A$ can be decided in quadratic time$\}$

$\{0^m 1^m \mid m \geq 0\} \in \mathrm{TIME}(n^2)$

Time class containment

If $f(n) = O(g(n))$, then which of the following statements is always true?

Ex: $n^2 = O(n^3)$ $\quad$ $TIME(n^2) \subseteq TIME(n^3)$

a) $\mathrm{TIME}\big(f(n)\big) \subseteq \mathrm{TIME}\big(g(n)\big)$

b) $\mathrm{TIME}\big(g(n)\big) \subseteq \mathrm{TIME}\big(f(n)\big)$

c) $\mathrm{TIME}\big(f(n)\big) = \mathrm{TIME}\big(g(n)\big)$

d) None of the above

$A \in TIME(f(n))$

$\Rightarrow \exists$ TM M deciding A in $O(f(n))$ time

$\Rightarrow M$ decides A in $O(g(n))$

$\Rightarrow A \in TIME(g(n))$

Example

$A = \{0^m 1^m \mid m \geq 0\}$

M = "On input w:

1. Scan input and reject if not of the form 0^*1^*
2. While input contains both 0's and 1's:

   Cross off one 0 and one 1

3. Accept if no 0's and no 1's left. Otherwise, reject."

- M runs in time $O(n^2)$ $\Rightarrow A \in TIME(n^2)$
- Is there a faster algorithm?

Example

$A = \{0^m1^m \mid m \geq 0\}$

M' = "On input w:

1. Scan input and reject if not of the form 0^*1^* $O(n)$
2. While input contains both 0's and 1's: $\leftarrow O(\log n)$
   - Reject if the total number of 0's and 1's remaining is odd
   - Cross off every other 0 and every other 1

   $\Big\}\ O(n)$
3. Accept if no 0's and no 1's left. Otherwise, reject."

Runtime: $O(n) + O(\log n) \cdot O(n) + O(1) = O(n \log n)$

- Running time of M':

$A \in TIME(n \log n)$

- Is there a faster algorithm?

Example

Running time of M': $O(n \log n)$

Theorem (Sipser, Problem 7.49): If L can be decided in $o(n \log n)$ time on a 1-tape TM, then L is regular

Cor: There is no TM M running in $o(n \log n)$ deciding $\{0^m 1^m \mid m \geq 0\}$

Does it matter that we're using the 1-tape model for this result?

It matters: 2-tape TMs can decide A faster

M'' = "On input w:

1. Scan input and reject if not of the form 0^*1^*
2. Copy 0's to tape 2
3. Scan tape 1. For each 1 read, cross off a 0 on tape 2
4. If 0's on tape 2 finish at same time as 1's on tape 1, accept. Otherwise, reject."

Analysis: A is decided in time $O(n)$ on a 2-tape TM

Moral of the story (part 1): Unlike decidability, time complexity depends on the TM model

How *much* does the model matter?

Theorem: Let $t(n) \geq n$ be a function. Every multi-tape TM running in time $t(n)$ has an equivalent single-tape TM running in time $O(t(n)^2)$

Proof idea:

We already saw how to simulate a multi-tape TM with a single-tape TM

Need a runtime analysis of this construction

Moral of the story (part 2): Time complexity doesn't depend too much on the TM model (as long as it's deterministic, sequential)

Extended Church-Turing Thesis

Every "reasonable" model of computation can be simulated by a basic, single-tape TM with only a **polynomial** slowdown.

E.g., doubly infinite TMs, multi-tape TMs, RAM TMs

Does not include nondeterministic TMs (not reasonable)

Possible counterexamples? Randomized computation, parallel computation, DNA computing, quantum computation

Complexity class P

Definition: P is the class of languages decidable in polynomial time on a basic single-tape (deterministic) TM

$$P = \bigcup_{k=1}^{\infty} \mathrm{TIME}(n^k) = \mathrm{TIME}(n) \cup \mathrm{TIME}(n^2) \cup \mathrm{TIME}(n^3) \cup \ldots$$

$$= \{ A \mid \exists \text{ polynomial } p(n) \text{ s.t. } A \in \mathrm{TIME}(p(n)) \}$$

- Class doesn't change if we substitute in another reasonable deterministic model (Extended Church-Turing)
- Cobham-Edmonds Thesis: Roughly captures class of problems that are feasible to solve on computers

A note about encodings

We'll still use the notation $\langle \quad \rangle$ for "any reasonable" encoding of the input to a TM…but now we have to be more careful about what we mean by "reasonable"

How long is the encoding of a V-vertex, E-edge graph…

… as an adjacency matrix?

… as an adjacency list?

How long is the encoding of a natural number k

… in binary?

… in decimal?

… in unary?

Describing and analyzing polynomial-time algorithms

- Due to Extended Church-Turing Thesis, we can still use high-level descriptions on multi-tape machines
- Polynomial-time is robust under composition: $\mathrm{poly}(n)$ executions of $\mathrm{poly}(n)$-time subroutines run on $\mathrm{poly}(n)$-size inputs gives an algorithm running in $\mathrm{poly}(n)$ time.

  $\Rightarrow$ Can freely use algorithms we've seen before as subroutines if we've analyzed their runtime

- Need to be careful about size of inputs! (Assume inputs represented in binary unless otherwise stated.)

Space complexity

Space complexity of a TM (algorithm) = maximum number of tape cells it uses on a worst-case input

Formally: Let $f : \mathbb{N} \to \mathbb{N}$. A TM M runs in space $f(n)$ if on every input $w \in \Sigma^n$, M halts on w using at most $f(n)$ cells

A language $A \in \text{SPACE}(f(n))$ if there exists a basic single-tape (deterministic) TM M that

1) Decides A, and
2) Runs in time $O(f(n))$

Back to our examples

$A = \{0^m 1^m \mid m \geq 0\}$

Theorem: Let $s(n) \geq n$ be a function. Every multi-tape TM running in space $s(n)$ has an equivalent single-tape TM running in space $O(s(n))$