CISC 4090
Theory of Computation

Professor Daniel Leeds
dleeds@fordham.edu
JMH 332

1

Theory of computation

Computability:

What computations can be performed by machine X?

Complexity:

How long does it take to complete computation Y?

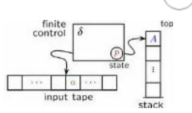
NP completeness

2

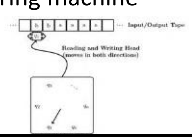
Machines studied

Finite state automaton

Push-down automaton



Turing machine



Computational analyses using **proofs**!

3

Requirements

- Attendance and participation
- Lectures
- Homeworks – roughly 5 across semester
- Quizzes – each 15 minutes, 4 across semester
- Exams – 1 midterm, 1 final

- Academic integrity – may discuss course material with your classmates, but you MUST come up with all your graded answers yourself

4

This is a challenging course!

Read and re-read course materials
- Text and lecture notes
- Practice problems

Ask questions
- In class
- In office hours JMH 332
- Of fellow students (without plagiarizing!)

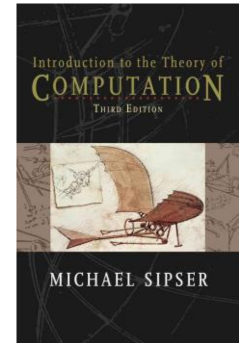
Start assignments early
- Homeworks may take 3-10 hours
- Start homework, take break, come back

5

Course textbook

Introduction to Theory of Computation
Third Edition

Michael Sipser



6

Course website

http://storm.cis.fordham.edu/leeds/cisc4090

Go online for
- Announcements
- Lecture slides
- Course materials/handouts
- Assignments

7

Instructor

Prof. Daniel Leeds
dleeds@fordham.edu
Office hours: Usually Mon 3-4pm, Thurs 1-2pm
Office: JMH 332

8

Mathematical background

Review of CISC 1400/2100

- Sets
- Logic
- Functions
- Graphs
- Proofs

Sets

- A set is an un-ordered group of objects

e.g.: {apple, banana} or {{A,B},{1,2,3,4}, {+,-,*}}

- Key concepts/operations:
  - Subsets: $A \subset B$, $A \subseteq B$
  - Cardinality: |A|
  - Intersection $A \cap B$, Union $A \cup B$, Complement A'
  - Venn Diagrams
  - Power set: P(A)

    If |A|=4, what is |P(A)| ?

Ordered-pairs, or *k*-tuples

- Ordered group of objects:

  e.g., (1, 3, 5) or (81, 3, 1, 12, 5)

- Cartesian product: AxB -> yields set of tuples
- Given j sets A_1, A_2, … A_j , A_1 x A_2 x … x A_j = $\{(a_1, a_2, \cdots, a_j) | a_i \in A_i\}$
- $\mathbb{Z}^2$ represents $\mathbb{Z}$ x $\mathbb{Z}$ which is $\{(a, b) | a \in \mathbb{Z}$ and $b \in \mathbb{Z}\}$

Logic

Operations
- AND $T \wedge T \equiv T$, all else is F
- OR $F \vee F \equiv F$, all else T
- NOT $T' \equiv \neg T \equiv F$
- IMPLIES $T \rightarrow F \equiv F$, all else T

13

Functions

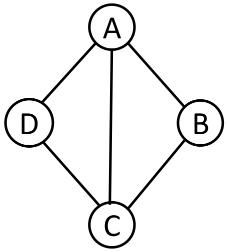
A function maps inputs to a single output
- f(a)=b func: Domain -> Co-domain

Examples: *Assume N -> N*
- $g(x) = x^2$
- h(y) = y+5
- m(x,y) = x-y

14

Graphs

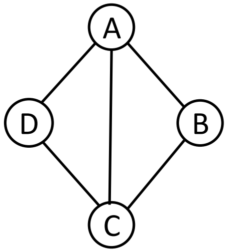
A graph is a set of **vertices** and **edges**
- G=(V,E)
- V={A, B, C, D}
- E={(A,B), (A,C), (C,D), (A,D), (B,C)}



15

Graph terminology

- ***Degree*** of vertex: number of touching edges
- ***Path***: sequence of nodes connected by edges
- ***Simple path***: path with no repeat nodes
- ***Cycle***: Path starting and ending in same node



16

Proofs

A proof is a clear logical argument

Types of proof
- Counterexample
- Contradiction
- Induction
- Construction – main technique we'll use this semester

18

Example 1

Claim: All positive integers are divisible by 3

Proof by **counterexample**:
- Let x=2
- x is a positive integer
- x is **not** divisible by 3

We have disproved our claim!

20

Example 2

Claim: There are no positive integer solutions to the equation x^2-y^2=1

21

Example 2

Claim: There are no positive integer solutions to the equation x^2-y^2=1

Proof by contradiction:
- Assume there IS an integer solution
- $x^2-y^2 = (x-y)\ (x+y) = 1$
- Either (a) x-y=1 and x+y=1 OR (b) x-y=-1 and x-y=-1
- (a) x=1, y=0 – non-positive! (b) x=-1 and y=0 – non-positive!

22

Example 3

Claim: For $x \geq 1$, $2+2^2+2^3+\ldots+2^x=2^{x+1}-2$

First review what is proof by induction:
Base case that is true
Inductive step: If true for k, prove for k+1

Proof by induction

- Base case: x=1 $2 = 2^{1+1}-2 = 4-2 = 2$
- Assume true for x=k, prove for x=k+1
- $2^{(k+1)+1}-2 = 2^{k+2}-2 = 2x2^{(k+1)}-2$

$= 2x(2 + 2+2^2+\ldots+2^k)-2$

$= 4 + 2^2 +2^3+\ldots+2^{k+1}-2$

$= 2 + 2^2 +2^3+\ldots+2^{k+1}$

Ask students for base case
Ask students for any part of inductive step

24

Example 4

Claim: For every even number n>2, there is a 3-regular graph with n nodes (Theorem 0.22, p21)

Graph is *k-regular* if every node has degree k

Proof by construction:

- Try constructing for n=4, n=6, n=8
- Describe a general pattern
  - Place nodes in a circle, connect each node to its neighbor (now all nodes have 2 degrees), connect each node to farthest node diagonally across (now each node gets 1 additional degree; since even # of nodes, all nodes paired up)

Here, all you need for your proof is a careful instruction how to make such a graph for any n>2

26

Strings and languages

Key topic in our class

- **Alphabet**
- **String**
- **Language**

Alphabet is non-empty finite set of symbols, e.g.,

- $\Sigma_1 = \{0,1\}$
- $\Sigma_2 = \{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z\}$

String is finite sequence of symbols from selected alphabet, e.g.,

- 0100 is string from Σ_1 and cat is string from Σ_2

27

Strings and languages

Key topic in our class

Length of string w, |w| is number of symbols

Empty string ε has length 0

Strings can be **concatenated**

- wz is the string w concatenated with string z
- string w can be concatenated with itself *k* time w^k

Language is set of strings

28