Chapter 0
Introduction

Overview

- we will cover three main areas
  - automata theory
    - mathematical models of computation
  - computability theory
    - which problems can be solved by computers?
  - complexity theory
    - what makes some problems computationally hard or easy?

Automata Theory

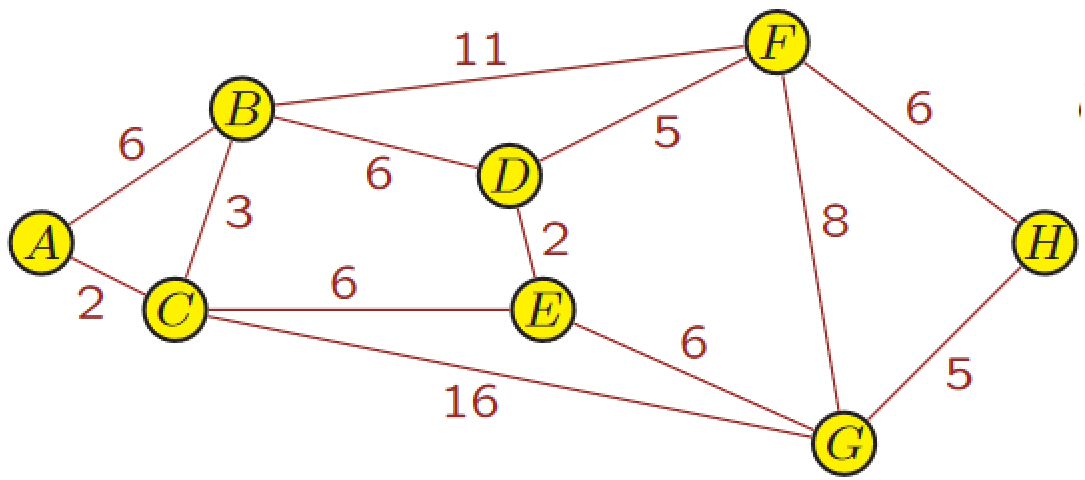
- finite automata and regular expressions
  - string matching (grep in Unix)
  - circuit design
  - communication protocols
- context-free grammars and pushdown automata
  - compilers
  - programming languages
- Turing machines
  - computers
  - algorithms
- why study different models of computation?

Computability Theory

- there are algorithms to solve many problems
- but there are some problems for which there is no algorithm: undecidable problems
  - does a program run forever?
  - is a program correct?
  - are two programs equivalent?

Complexity Theory

- for a solvable problem, is there an efficient algorithm to solve it?
- some problems can be solved efficiently:
  - is there a path from A to H with total cost at most 20?



edge labels are costs

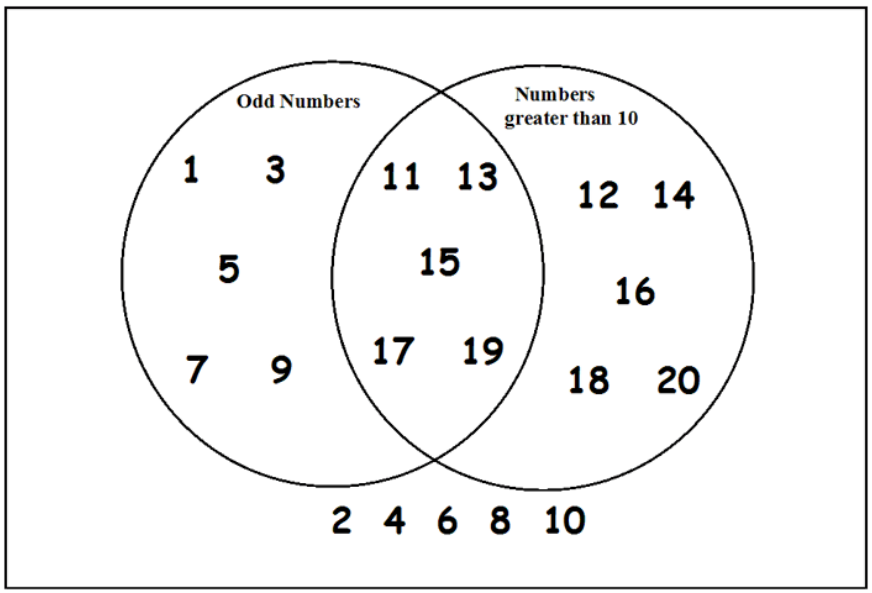
- some problems have no known efficient algorithm:
  - is there a path from A to H with total cost at least 50?

Sets

- set
  - an unordered collection of objects or elements
  - example: {0, 2, 5}
  - element of: $x \in S$
  - set notation: $\{x \mid x \in R, x > 0\}$
    - R - set of real numbers
    - | - such that
    - , - and

Sets

- the universal set U is the set containing everything currently under consideration
- the empty set is the set with no elements: Ø or { }
- Venn diagram



Sets

- elements
  - the set $\{0, 2, 5\}$ has elements 0, 2, and 5
  - order and duplicates don't matter
    - $\{2, 0, 0, 5, 5, 5\} = \{0, 2, 5\}$
  - $\{0\}$ and 0 are different

- cardinality: $|\{1, 2, 3\}| = 3$, $|\emptyset| = 0$
- set builder notation
  - $S = \{x \mid x \text{ is a positive integer less than } 100\}$
- subsets
  - $A \subseteq B$
  - proper subset: $A \subset B$

Sets

- operations
  - union: $A \cup B$
  - intersection: $A \cap B$
  - complement: A' or $\overline{A}$
  - cartesian product: $A \times B$
    - also called cross product
    - elements are ordered pairs
    - in general, k-tuples (or finite sequences)
  - power set: $P(A)$

Sets

- operation examples
  - $A = \{1,2\}$, $B=\{2,3\}$, $U = \{x \in N \mid x < 6\}$
  - $A \cup B = \{1,2,3\}$
  - $A \cap B = \{2\}$
  - $\overline{A} = \{3,4,5\}$
  - $A \times B = \{(1,2), (1,3), (2,2), (2,3)\}$
  - $P(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

Some Important Sets

- N = natural numbers = {1, 2, 3, …}
- W = whole numbers = {0, 1, 2, 3, …}
- Z = integers = {…, -3, -2, -1, 0, 1, 2, 3, …}
- Z^+ = positive integers = {1, 2, 3,…}
- R = set of real numbers
- R^+ = set of positive real numbers
- C = set of complex numbers
- Q = set of rational numbers

Functions

- function
  - operator, operation, or mapping that maps each element in a domain D to a single element in range R
    - $f : D \to R$
    - $f(a) = b$

- sometimes we define a function using a table.
  - $f : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$ as

n	f(n)
0	1
1	2
2	3
3	4
4	0

  - where $f(n) = (n + 1) \bmod 5$

Functions

- example: let A = {ROCK, PAPER, SCISSORS} and
  B = {TRUE, FALSE}

- consider the function beats : $A \times A \to B$
  defined by the table

beats	ROCK	PAPER	SCISSORS
ROCK	FALSE	FALSE	TRUE
PAPER	TRUE	FALSE	FALSE
SCISSOR	FALSE	TRUE	FALSE

- for example,
  beats (ROCK, SCISSORS) = TRUE
  beats (ROCK, PAPER) = FALSE

Functions

- a function f with k arguments is a k-ary function
  - k is called the arity of f

- a unary function has arity $k = 1$
  - $f(x) = 3x + 4$ or $f(w) = |w|$

- a binary function has arity $k = 2$
  - beats is a binary function

Functions

- a predicate or property is a function whose range is {TRUE, FALSE}
  - beats is a predicate
- a predicate whose domain is a set $A \times \cdots \times A$ of k-tuples is called a relation or a k-ary relation
  - a 2-ary relation is a binary relation
  - beats is a binary relation
- if R is a binary relation, aRb means aRb = TRUE
  - for the binary relation "<", $2 < 5$ = TRUE
- sometimes more convenient to describe predicates with sets instead of functions
  - beats can be written as {(ROCK, SCISSORS), (PAPER, ROCK), (SCISSORS, PAPER)}
  - which is the set $\{(x, y) \mid (x, y) \in D$ and xRy (i.e., x beats y)$\}$

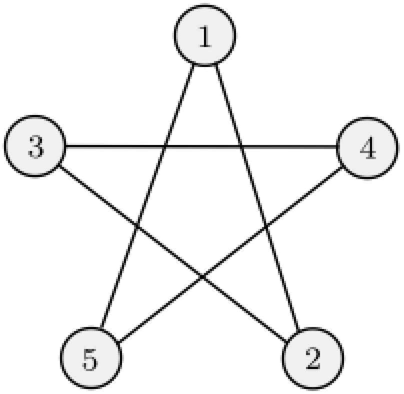
Functions

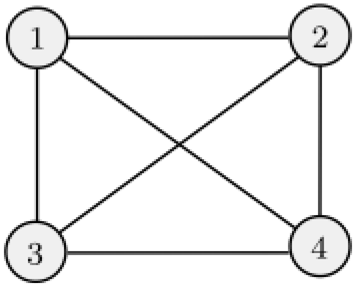
- equivalence relations are binary relations that are
  - reflexive: if for every x, xRx
  - symmetric: if for every x and y, xRy if and only if yRx
  - transitive: if for every x, y, and z, xRy and yRz → xRz

- example: (=, Z) is an equivalence relation
  - reflexive: every integer is = to itself
  - symmetric: if x = y, then y = x
  - transitive: if x = y and y = z, then x = z

Graphs

- undirected graph
  - nodes or vertices
  - edges
- degree
  - left: each node has degree 2
  - right: each node has degree 3
  - self loops

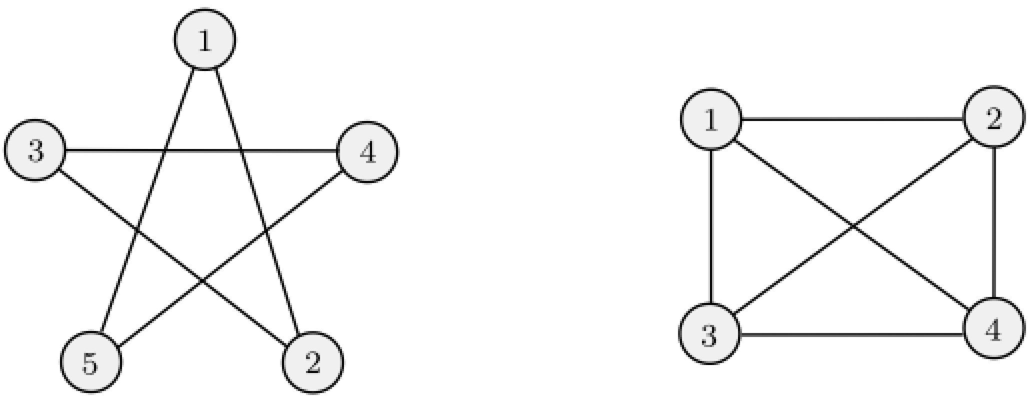




Graphs

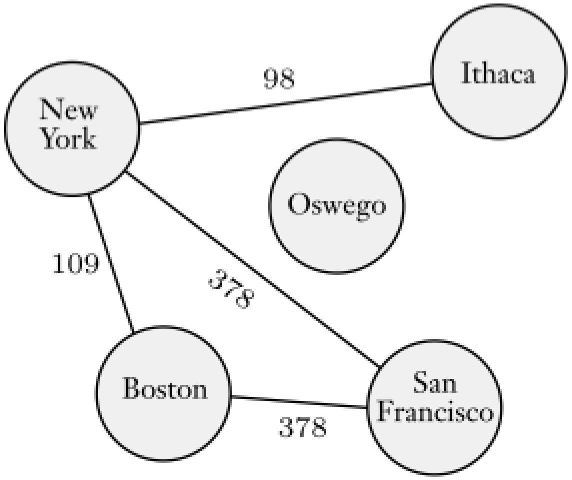
- edges represented by (unordered) pairs
  - (1, 2) or (2, 1)

- formal definition
  - G = (V, E)
  - left: ({1, 2, 3, 4, 5}, {(1, 2), (2, 3), (3, 4), (4, 5), (5, 1)})



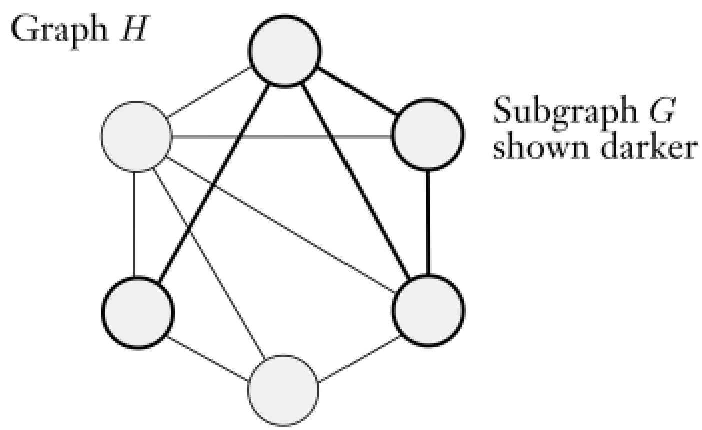
Graphs

- often used to represent data
  - labeled graph



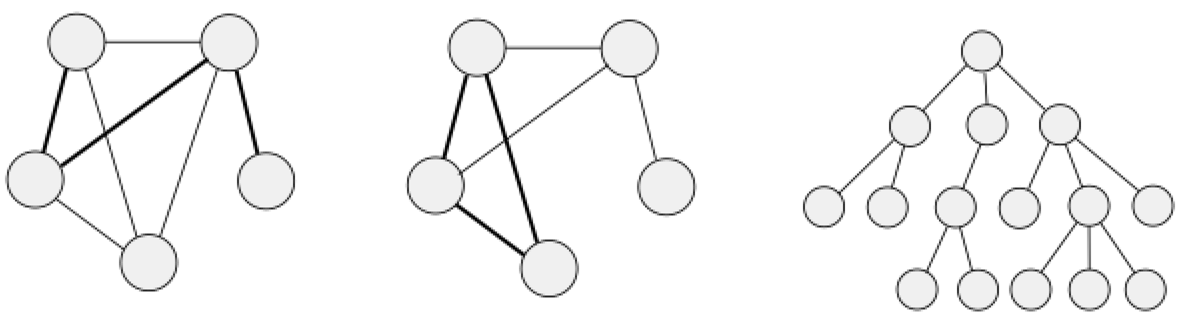
Graphs

- subgraph



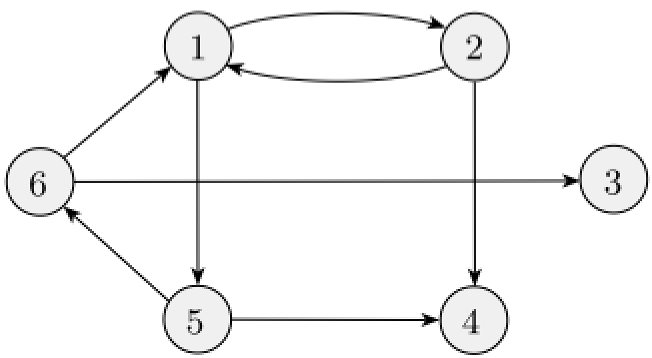
Graphs

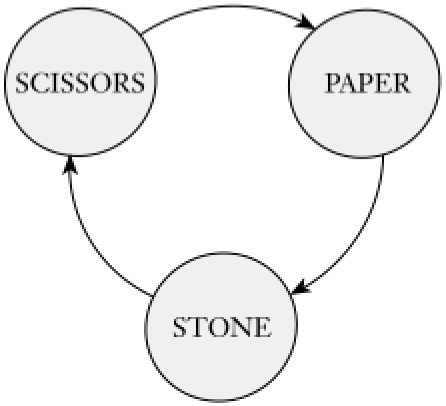
- path
  - simple path – no repeated nodes
  - connected
  - cycle
- tree
  - leaves
  - root



Graphs

- directed graph
  - in-degree
  - out-degree
  - represented by ordered pairs
    - (1, 2), (1, 5), (2, 1), (2, 4), (5, 4), (5, 6), (6, 1), (6, 3)
  - strongly connected
  - weakly connected





Strings and Languages

- alphabet – non-empty
  - symbols: individual elements
  - examples

$$\Sigma_1 = \{0,1\}$$

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

$$\Gamma = \{0, 1, x, y, z\}$$

Strings and Languages

- strings
  - finite sequence of symbols
  - 01001 is a string over Σ_1
  - length: $|w|$
    - empty string has length 0
  - substring
    - cad is a substring of abracadabra
  - concatenation – xy
    - x^k means

$$\overbrace{xx\cdots x}^{k}.$$

Strings and Languages

- order
  - lexicographic - dictionary
  - shortlex or string order
    - shorter strings first

$$(\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots).$$

  - prefix
    - proper prefix
  - language: a set of strings

Boolean Logic

- Boolean logic: TRUE and FALSE
- Boolean values: 1 and 0

- Boolean operations
  - conjunction (and) $\land$
  - disjunction (or) $\lor$
  - negation (not) $\neg$
  - exclusive or (xor) $\oplus$
  - biconditional (equality) $\leftrightarrow$
  - implication $\rightarrow$

Boolean Logic

- Boolean operations

$$\begin{array}{lll} 0 \wedge 0 = 0 & 0 \vee 0 = 0 & \neg 0 = 1 \\ 0 \wedge 1 = 0 & 0 \vee 1 = 1 & \neg 1 = 0 \\ 1 \wedge 0 = 0 & 1 \vee 0 = 1 & \\ 1 \wedge 1 = 1 & 1 \vee 1 = 1 & \end{array}$$

$$\begin{array}{lll} 0 \oplus 0 = 0 & 0 \leftrightarrow 0 = 1 & 0 \rightarrow 0 = 1 \\ 0 \oplus 1 = 1 & 0 \leftrightarrow 1 = 0 & 0 \rightarrow 1 = 1 \\ 1 \oplus 0 = 1 & 1 \leftrightarrow 0 = 0 & 1 \rightarrow 0 = 0 \\ 1 \oplus 1 = 0 & 1 \leftrightarrow 1 = 1 & 1 \rightarrow 1 = 1 \end{array}$$

Definitions, Theorems, and Proofs

- definition: describes objects and notations precisely
- mathematical statements: unambiguous statements about an object and its properties
- proof: logical argument to show a statement is true
- theorem: mathematical statement proven true
  - lemma: helping statement in proof
  - corollaries: related statements that are true

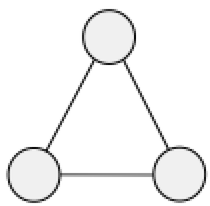
Strategies for Producing Proofs

- no simple set of rules to produce the right proof

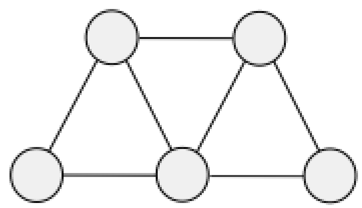
- general strategies
  - carefully read the statement to prove
  - rewrite statement in your own words
  - break down statement into parts
    - e.g., P iff Q, set A = set B
  - experiment with examples and counterexamples
    - see next slide for example
  - instead of proving the whole problem, try to prove a special case
    - if trying to prove property for $k > 0$, just try $k = 1$

Strategies for Producing Proofs

- experiment with examples and counterexamples
  - e.g., Prove that for every graph G, the sum of the degrees of all of the nodes is an even number
    - examples

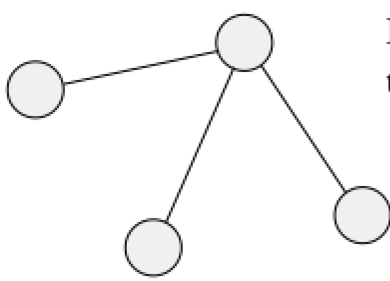


$$\text{sum} = 2+2+2 = 6$$



$$\text{sum} = 2+3+4+3+2 = 14$$

    - try to find counterexample



Every time an edge is added, the sum increases by 2.

Strategies for Producing Proofs

- writing a proof
  - be patient
  - come back to it
  - be neat
  - be concise

- example: Prove for every graph G, the sum of the degrees of all the nodes is an even number.
  - every edge is connected to two nodes
  - therefore, each edge adds 2 to the sum of degrees
  - if G contains e edges, then the sum of degrees = 2e, which is even

Types of Proofs

- types of proofs
  - Proof by Construction
  - Proof by Counterexample
  - Proof by Contradiction
  - Proof by Induction

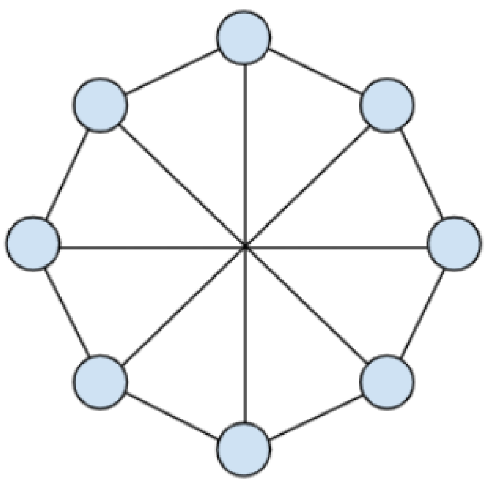
- note that a proof may contain more than one type of argument

Types of Proofs

- Proof by Construction
  - if claiming an object exists, demonstrate how to construct the object
  - e.g., For each even number n greater than 2, there exists a 3-regular graph with n nodes
    - regular graph: each vertex has the same number of neighbors
    - construct $G = (V, E)$ with n nodes

      $V = \{0, 1, \ldots, n - 1\}$

      $E = \{(i, i + 1) \mid \text{for } 0 \le i \le n - 2\} \cup$
      $\{(n - 1, 0)\} \cup$
      $\{(i, i + n/2) \mid \text{for } 0 \le i \le n/2 - 1\}$



Types of Proofs

- Proof by Counterexample
  - e.g., Prove or Disprove: All prime numbers are odd.
    - 2 is prime and even
    - therefore, the statement is not true

Types of Proofs

- Proof by Contradiction
  - assume theorem is false and show this assumption leads to a contradiction
  - e.g., Show that √2 is irrational
    - Suppose √2 is rational. Then there exists integers a and b with √2 = a/b, where b ≠ 0 and a and b have no common factors. So

$$2 = \frac{a^2}{b^2} \qquad\qquad 2b^2 = a^2$$

    - Therefore a^2 must be even. If a^2 is even, then a must be even. Since a is even, a = 2c for some integer c. Thus,

$$2b^2 = 4c^2 \qquad\qquad b^2 = 2c^2$$

    - Therefore b^2 is even, and b must be even as well. But then 2 must divide both a and b. This contradicts our assumption that a and b have no common factors. We have proved by contradiction that our initial assumption must be false and therefore √2 is irrational.

Types of Proofs

- Proof by Induction
  - advanced method to show all elements of an infinite set have a specified property
  - structure: 3 parts for proving $P(n)$ for all $n \geq b$
    - Basis Step: show base case (smallest value) is true; left-hand and right-hand sides computed independently
    - Inductive Hypothesis: assume $P(k)$ is true for some k
    - Inductive Step: Show $P(k+1)$ is true
      - explicitly write out Show statement
      - start with left-hand side
      - use Inductive Hypothesis (and show where!)
      - you're done when you've reached the RHS of Show

Types of Proofs

- Proof by Induction

  Example: Show that: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

  Solution:

  BASIS: n=1

  lhs: $\sum_{i=1}^{1} i = 1$ rhs: $\frac{1(1+1)}{2} = 1$ ✓

  INDUCTIVE HYPOTHESIS: Assume $\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ true for some k

  INDUCTIVE STEP: Show: $\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$$

$$= \frac{k(k+1)}{2} + (k+1) \quad \text{by I.H.}$$

$$= \frac{k(k+1) + 2(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2} \quad ✓$$