Review Materials

Mostly from Dr. Hughes Slides and Sipser Chapter 0.

Chapter 0 - Outline

- 0.2 Mathematical Notions and Terminology
  - Sets
  - Sequences and tuples
  - Functions and relations
  - Ordinals, cardinals and infinities, Cardinality
  - Graphs
  - Strings and languages
  - Operations on Strings
  - Properties of Languages
- 0.3 Definitions, Theorems, and Proofs
- 0.4 Types of Proof
    - Proof by construction
    - Proof by contradiction
    - Proof by induction
  - Set/Language Recognizer and Generators

Chapter 0

Sets

- **Sets** are unordered collections of distinct objects.
- **Sets** can be defined or specified in many ways:
  - By explicitly enumerating their members or elements

    e.g. S = { 1,2,3}

    Note: If S' = { 3,2,1}, then S and S' denote the same set (that is, $S' = S$)

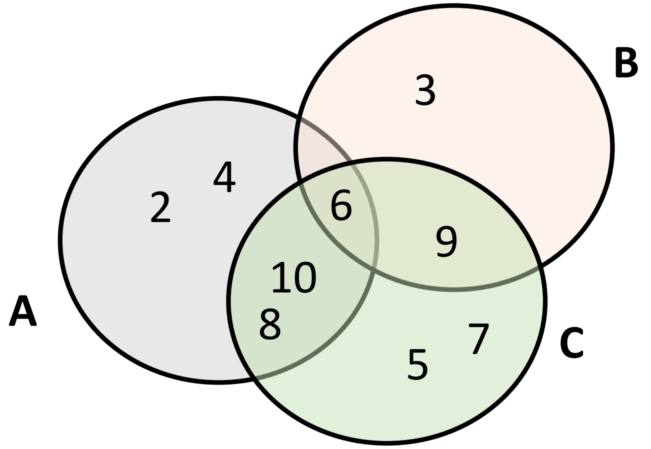
  - By specifying a condition for membership

    S = { x ∈ A | P(x) }, reads "S is the set of all x in A such that P(x) is true“

    P is called a "predicate" (a function from set A to {true, false})

    E.g. B = { x ∈ U | x is an even number }

- By Venn diagram



Chapter 0

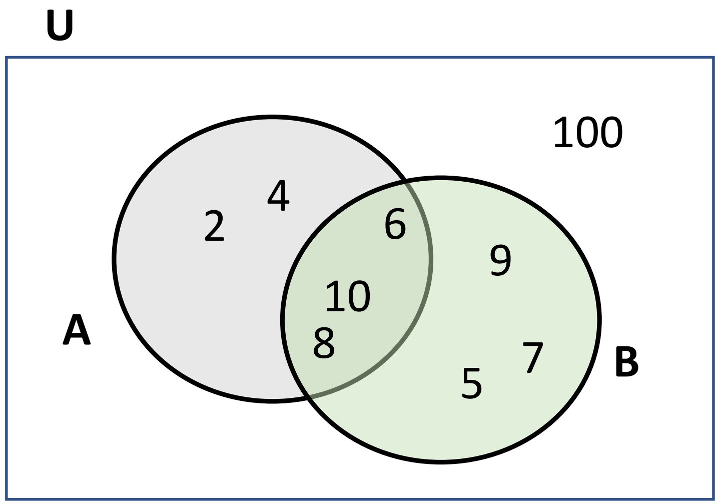
More on Sets

- The empty set is denoted, ∅, and is the set with no members; that is, ∅= { }.
- Multisets (mset) or Bags are unordered collections of objects where we keep track of repeated elements
  - Multiplicity of element: number of instances, given for each element
  - Example: S = { 1,2,3,1,2} → Multiplicity of 1 = 2

More on Sets

- **Membership:** If $S \neq \emptyset$, then there exists an x for which $x \in S$ is true; this predicate is read "x is an element of S" or "x is a member of S". The symbol " $\in$ " denotes the member relation. $x \notin S$ is true when x is not in S.

- Also, the predicate, $x \in \emptyset$ is always false! (why?)



$2 \in A$
$9 \notin B$

More on Sets

- Operations:
- Let **A** and **B** be sets contained in our universe **U**.
  - Set Union: the union of A and B, denoted $A \cup B$ is the set:

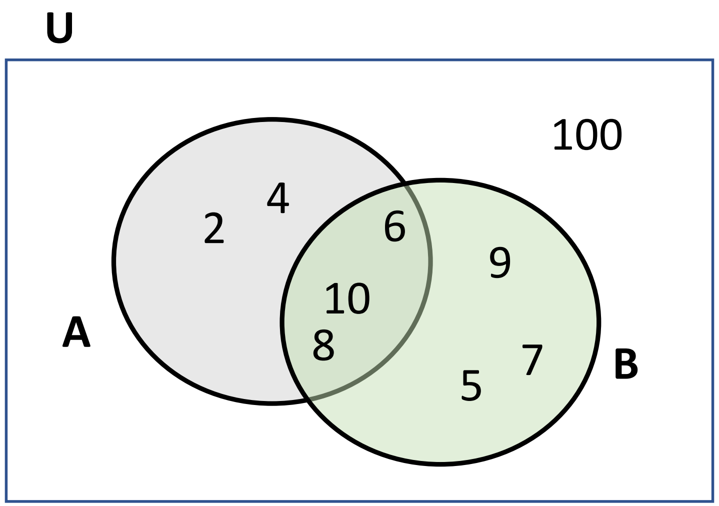
$$A \cup B = \{x : x \in A \text{ or } x \in B\}$$

  - Set intersection : the intersection of A and B, denoted $A \cap B$ is the set:

$$A \cap B = \{x : x \in A \text{ and } x \in B\}$$

  - complement $\sim A$ (usually A with a bar on it).

$$\sim A = \{x \in U : x \notin A\}$$



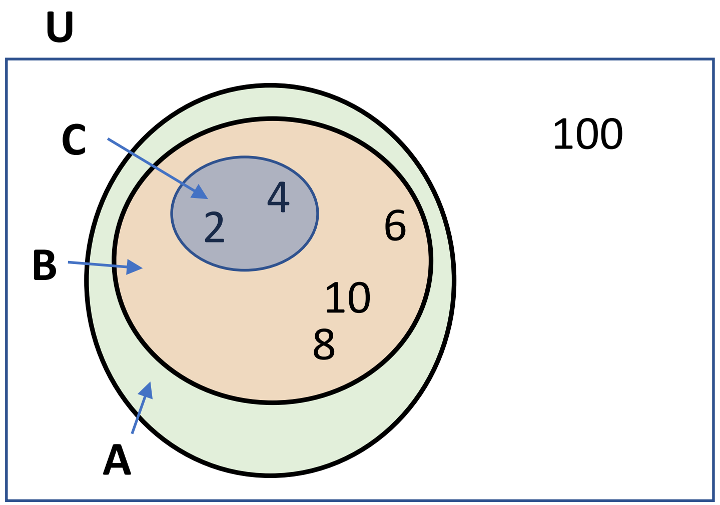
$$\left\{ \begin{array}{l} A \cup B = \{ 2,4,6,8,10,5,9,7\} \\ A \cap B = \{ 6,8,10\} \\ \sim A = \{ 100\} \end{array} \right.$$

More on Sets

- If A and B are sets, then we write "$A \subseteq B$" to mean that A is a subset of B.
  This means that for all $x \in A$, $x \in B$. Or, "$\forall x\, [x \in A \Rightarrow x \in B]$".

- The expression, "$A \subset B$" means that A is a proper subset of B.
  Mathematically, "$\forall x\, [x \in A \Rightarrow x \in B]$ and $\exists y\, [\, y \notin B$ and $y \in A]$.

- $(A = B) \Leftrightarrow (A \subseteq B) \wedge (B \supseteq A)$

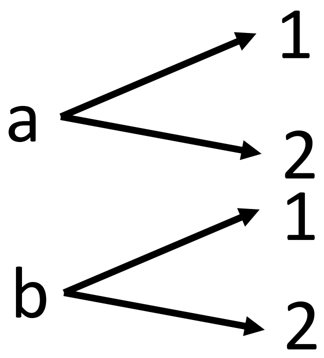


$$\left\{ \begin{array}{l} A \subseteq B \\ C \subset A \end{array} \right.$$

More on Sets

- The cross (Cartesian) product of two sets A and B is denoted, $A \times B$, and is the set defined as follows: $A \times B = \{ (a,b) \mid a \in A \text{ and } b \in B \}$.
- If $A \neq B$, then $A \times B \neq B \times A$.
- **Note:** (a,b) is a sequence not a set. (next slide)

$A \times B = \{(a,1),(a,2),(b,1),(b,2)\}$



A×B	1	2
a	(a,1)	(a,2)
b	(b,1)	(b,2)

Sequences

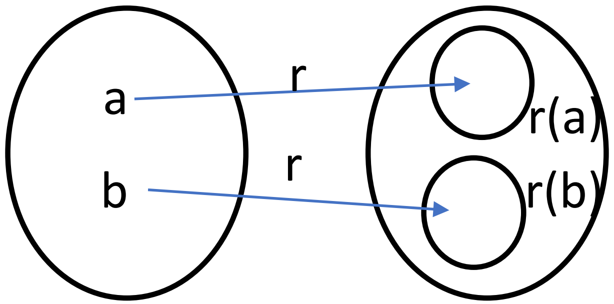
- While sets have no order and no repeated elements, sequences have order and can contain repeats at differing positions in the order.
  - The **set** {5,2,5} = {5,2} = {2,5}
  - The **sequence** (5,2,5) ≠ (2,5,5) ≠ (5,5,2) ≠ (5,2) ≠ (2,5)

- In sequence $(a_1, a_2, \ldots, \mathbf{a_k}, \ldots)$, $\mathbf{a_k}$ is called the k-th element of the sequence.

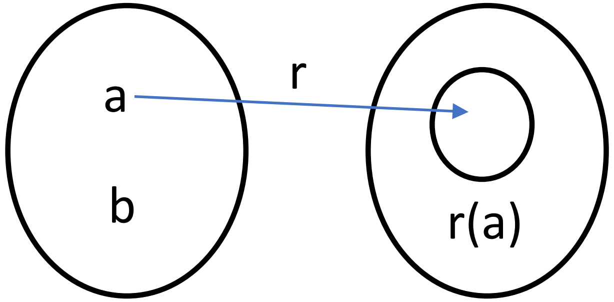
- Finite sequences are often called tuples. (3-tuple, 4-tuple, 0-tuple ?)
  - Those of length k are k-tuples.
  - A 2-tuple is also called a pair.

Relations

- A relation, r, is a mapping from some set A to some set B;
  - We write, r: A →B, and we mean that **r** assigns to **every** member of A a subset of B;
  - that is, for every a ∈ A, r(a) ⊆ B and r(a) ≠ Ø.
  - A relation, r, can also be **defined in terms of the cross product** of A and B:
    - r ⊆ A × B such that for every a ∈ A there is at least one b ∈ B such that (a, b) ∈ r.
- We say that a relation, r, from A to B is a partial relation if and only if for some a ∈ A, r(a) = Ø = { }.



relation

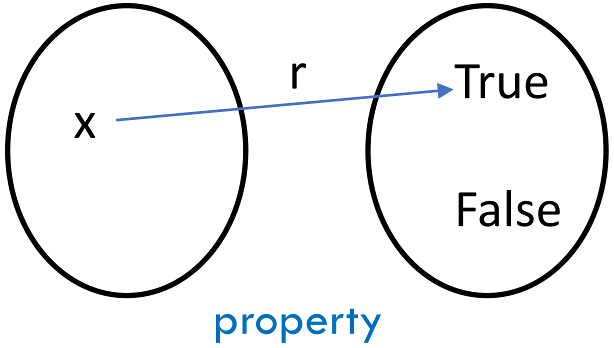


partial relation

More on Relations

- A predicate or property is a function with **range** {TRUE, FALSE}.

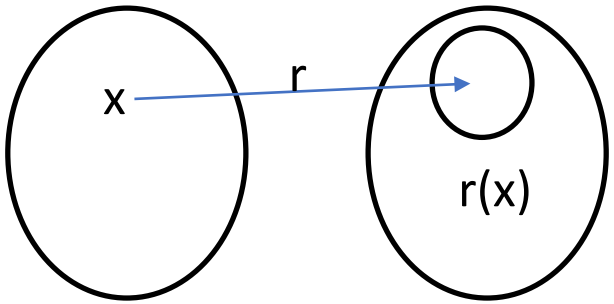
- A property with a domain of n-tuples A^n is an n-ary relation
- Binary relations are common, and like binary functions, we use **infix notations** for them
- Let R be a binary relation on A^2. R is:
  - Reflexive if "x ∈ A, xRx
  - Symmetric if x R y → y R x
  - Transitive if (x R y, y R z) → x R z
  - An equivalence relation if it is reflexive, symmetric and transitive



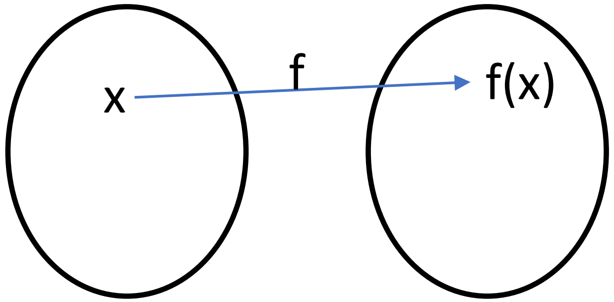
Functions

- Functions are special types of relations. Let X and Y be sets. A function is a map $f: X \to Y$ such that for every $x \in X$, there is a unique $y \in Y$ where $f(x) = y$; that is, $|f(x)| = 1$.

- If f is a partial function from A to B, then f may not be defined for every $x \in A$. In this case we write $|f(x)| \leq 1$, for every a in A; note that $|f(x)| = 0$ if and only if $f(x) = \emptyset$, and we say the function is undefined at a.



relation



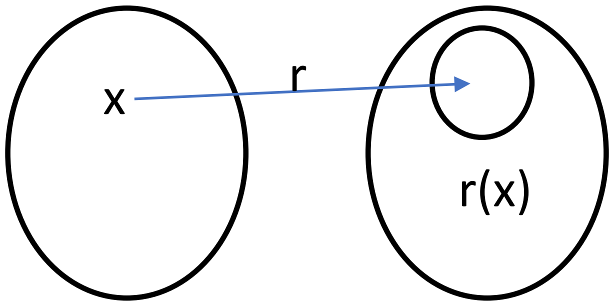
Function

Chapter 0

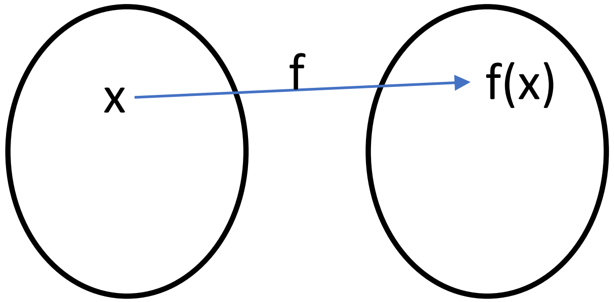
More on functions

- Domain is the complete **set of possible values** of on which f is defined.

- We say that X is the domain and Y is the codomain. The range or image is the set $f(X) = \{f(x) : x \in X\}$.



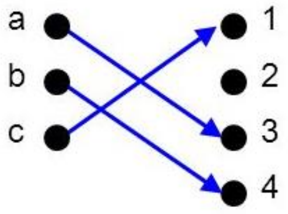
relation



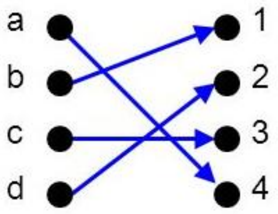
Function

More on Functions

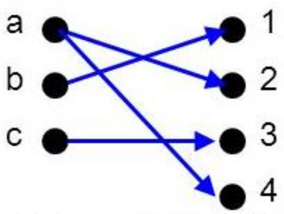
- A function, f, is said to be one-to-one (1-1) if and only if $x \neq y$ implies $f(x) \neq f(y)$.
  - A (total) function that is one-to-one is sometimes called an injection.
- A function, $f: A \rightarrow B$, is said to be onto if and only if for every $y \in B$ there is an $x \in A$ such that $y = f(x)$.
  - Total functions that are onto are called surjections.
- Ones that are 1-1 and onto are called bijections.



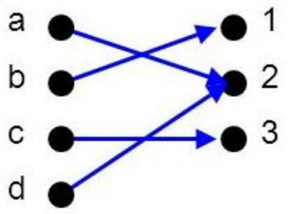
1-to-1, not onto



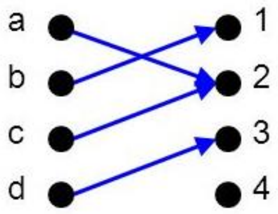
Both 1-to-1 and onto



Not a valid function



Onto, not 1-to-1



Neither 1-to-1 nor onto

Ordinal and Cardinal Numbers

- **Definition**: Ordinal numbers are **symbols** used to designate relative position in an ordered collection.
  - The ordinals correspond to the natural numbers: 0, 1, 2, ...
  - The set of all natural (ordinal) numbers is denoted, $\mathbb{N}$.
  - (Note: Here we include 0 as a natural number.)

- **Definition**. Let S be any set. We associate with S, the unique symbol $|S|$ called its cardinality. Symbols of this kind are called cardinal numbers and denote the size of the set with which they are associated.
  - $|\emptyset| = 0$.
  - If S = {0, 1, 2, 3, ..., n-1}, for some natural number n>0, then $|S|=n$.
  - The **cardinality** of any **finite set** (including the empty set) is simply the ordinal number that specifies the number of elements in that set.

More on Cardinality

- **Definition**: If A and B are two sets, then $|A| \leq |B|$ if and only if there exists an **injection**, f, from A to B; f is a 1-1 function from A into B.
- **Definition**: If A and B are two sets, then $|A| = |B|$ if and only if $|A| \leq |B|$ and $|B| \leq |A|$.
  - We may also say that $|A| = |B|$ if and only if there is a **bijection**, f, from A to B; f is a 1-1 function from A onto B.
- **Definition**: If A and B are two sets, then $|A| < |B|$ if and only if $|A| \leq |B|$ and $|A| \neq |B|$.
- **Definition**: A set S is said to be finite if and only if $|S| \in \mathbb{N}$; otherwise, S is said to be infinite.
- **Definition**: A set S is said to be countable if and only if S is finite or $|S| = |\mathbb{N}|$; otherwise S is said to be uncountable.

Infinities

Examples of infinite sets:

- N (the set of Natural numbers),
- Z (the set of Integers),
- Z+ (the set of Positive Integers),
- Q (the set of Rational numbers) and
- R (the set of Real numbers).

- But, are all these infinite sets the same size??

- Answer: $|N| = |Z+| = |Z| = |Q| < |R|$.

Power Set

- **Definition**: Let S be a set, then the power set of S, denoted P(S) or 2^S, is defined by $P(S) = \{ A \mid A \subseteq S \}$.

- Examples.
  - $P(\emptyset) = \{\emptyset\}$,
  - $P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$
  - $P(N) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \ldots, \{0,1\}, \{0,2\}, \{0,3\}, \ldots, \{0,1,2\}, \ldots\ldots \{ N\} \}$

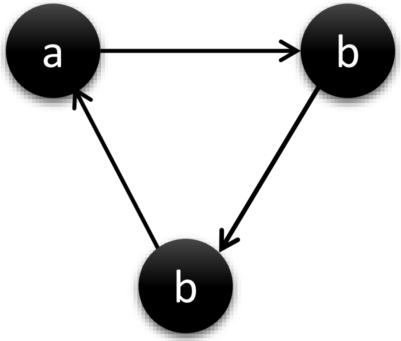
Undirected Graphs

An undirected Graph G is defined by a pair (V, E)

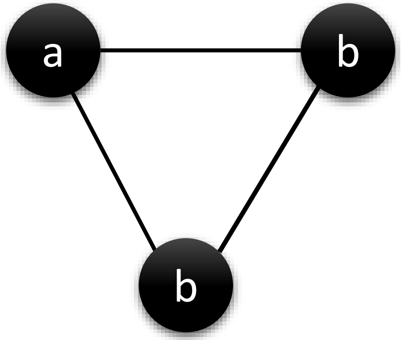
- V: Finite Set of Nodes/Vertices
- E: { <a,b> | a,b ∈ V are called Edges/Arcs}
  - $E \subseteq V \times V$ such that <a,b>∈E implies <b,a> ∈ E

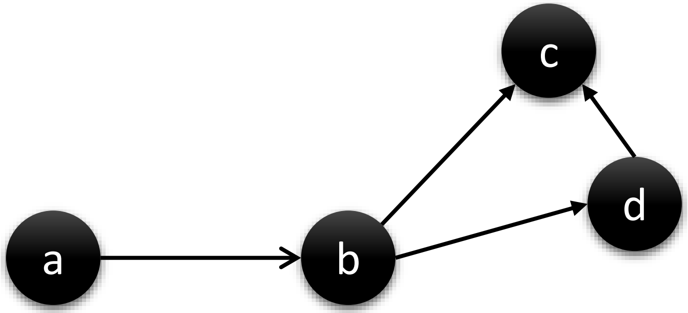
- Degree of node is number of edges at that node (number of nodes it relates to)
- Graphs can be labeled or unlabeled.
  - Labels can go on nodes, edges or both.

Directed Graphs



Undirected Graphs



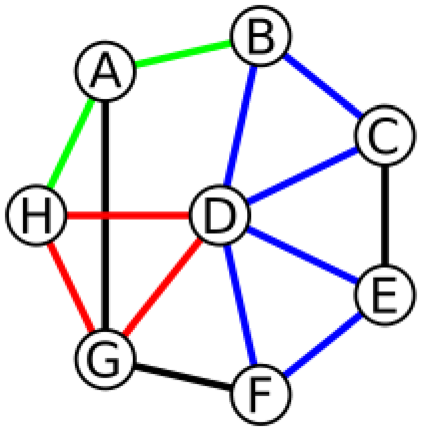


Degree of b = 3

More on Graphs

A subgraph H of a graph G is a **subset of the nodes** of G with all edges retained from G that involve node pairs in H.

- A path is a sequence of nodes connected by edges.
- A graph is connected if every two nodes are connected by a path.
- A cycle is a path that starts and ends in the same node.
- A simple cycle is a cycle such that all its vertices and edges are distinct.

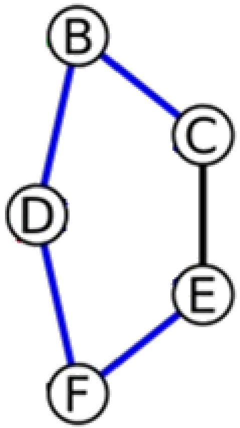


Nodes: A,B,C,….

Edges: AB, BD,GF,…

Path: HAB, DBC, CE,…

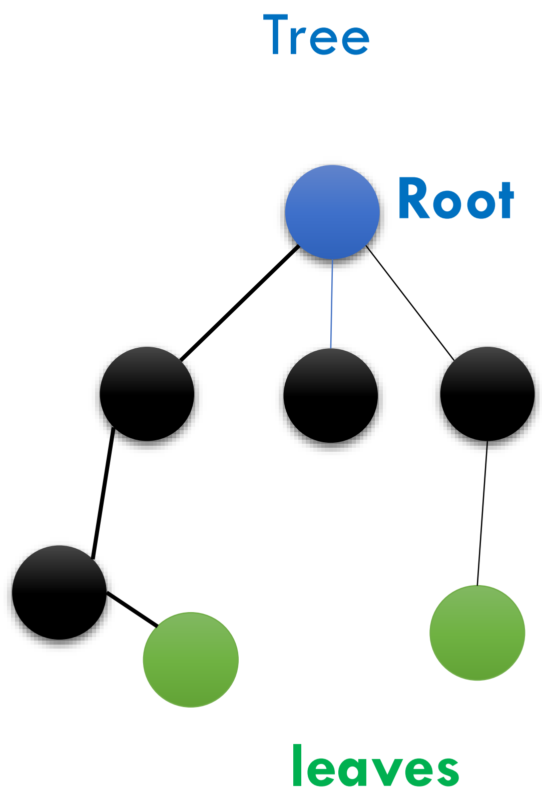
Cycle: BDCB, ABDHA,…



Subgraph: BDFECB

More on Graphs

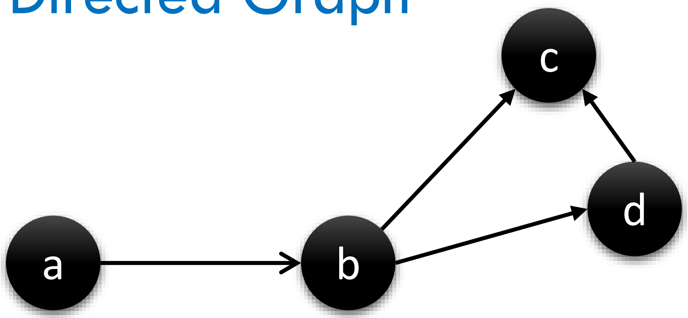
- A tree is a **graph** that is **connected** and has **no simple cycles**.
- A tree may contain a special node called the root.
- The nodes of degree 1 in a tree, excepting the root, are called leaves.
- The **set of leaves** of a tree are called the frontier.



In Directed Graph

- If the edges have direction then a graph is called directed
- in-degree (edges into node)
- out-degree (edges out of node).

Directed Graph



in-degree of b =1

Out-degree of b=2

Chapter 0

Alphabet
String
Language

Alphabets and Strings

- **DEFINITION 1.** An alphabet Σ is a finite, non-empty set of abstract symbols.
- The members of the alphabet are the symbols of the alphabet.

- **Example:**
  - $\Sigma = \{0,1\}$
  - $\Sigma = \{a, b, c, \ldots, z\}$
  - $\Sigma = \{1,2,3,\ldots,9\}$

Strings

- A string over an alphabet is a finite sequence of symbols from that alphabet, usually written next to one another and not separated by commas.

- Examples:
  - If Σ ={0,1} → 01001 is a string over Σ.
  - If Σ = {a,b,c,...,z} → racadabra is a string over Σ.

More on Strings

- **DEFINITION 2.** Σ^*, the set of all strings over the alphabet, Σ, is given inductively as follows.

  - **Basis**:
    - $\varepsilon \in \Sigma^*$ (the null string is denoted by **ε**, it is the string of length 0, that is $|\ \varepsilon\ | = 0$)
    - $\forall a \in \Sigma, a \in \Sigma^*$ (the members of Σ are strings of length 1, $|a| = 1$)

  - **Induction rule:**
    - If $x \in \Sigma^*$, and $a \in \Sigma$, then **a.x** $\in \Sigma^*$and **x.a** $\in \Sigma^*$.
    - Furthermore, $\varepsilon . x = x. \varepsilon = x$, and $|a . x| = |x. a| =1+|x|$
    - NOTE: a . x denotes "a concatenated to x " and is formed by appending the symbol a to the left end of x.
    - Similarly, x . a , denotes appending a to the right end of x.
    - In either case, if x is the null string (ε), then the resultant string is "a".

Operations on Strings

- Let s, t be arbitrary strings over Σ
  - $s = a_1a_2\ldots a_j$, $j \geq 0$, where each $a_i \in \Sigma$
  - $t = b_1b_2\ldots b_k$, $k \geq 0$, where each $b_i \in \Sigma$

- **length**: $|s| = j$; $|t| = k$
- **concatenate**: $= s.t = st = a_1a_2\ldots a_jb_1b_2\ldots b_k$; $|st| = j+k$
- **power**: $s^n = ss\ldots s$ (n times)
- **reverse**: $s^R = a_ja_{j-1}\ldots a_1$
- **substring**: for $s = a_1a_2\ldots a_j$, any $a_pa_{p+1}\ldots a_q$ where $1 \leq p \leq q \leq j$ or ε.

Languages

- **DEFINITION 3**. Let Σ be an alphabet. A language over Σ is a subset, **L**, of Σ^*.

- **Example:** Languages over the alphabet $\Sigma = \{a, b\}$.
  - $\varnothing$ (the empty set) is a language over Σ
  - Σ^*(the universal set) is a language over Σ
  - $\{a, bb, aba\}$ (a finite subset of Σ^*) is a language over Σ.
  - $\{ ab^n a^m \mid n = m^2, n, m > 0 \}$ (infinite subset) is a language over Σ.

- A language is a set of strings.

- Reversal: $L^R = \{w^R \mid w \in L\}$
- **Example:** $L = \{001,10,111\} \rightarrow L^R = \{100,01,111\}$

More on Languages

- **DEFINITION 4.** Let **L** and **M** be two languages over Σ. Then the concatenation of L with M, denoted L.M is the set, $L.M = \{ x.y \mid x \in L \text{ and } y \in M \}$

- The concatenation of arbitrary strings x and y is defined inductively as follows:
  - **Basis:**
    - When $|x| \leq 1$ or $|y| \leq 1$, then x.y is defined as in Definition 2.
  - **Inductive rule:**
    - when $|x| > 1$ and $|y| > 1$, then $x = x'.a$ for some $a \in \Sigma$ and $x \in \Sigma^*$, where $|x'| = |x|-1$. Then $x.y = x'.(a.y)$.

Recognizer and Generators (of a language)

- A recognizer for a specific language is a program or computational model that differentiates members from non-members of the given language
  - A portion of the job of a **compiler** is to check to see if an input is a legitimate member of some specific programming language

- An **automata** is a **recognizer** .

Recognizer and Generators (of a language)

- A generator for a specific language is a program that generates all and only members of the given language

- A **grammar** is a **generator**.

Chapter 0

Chapter 0

Proofs : Terminology

- Definitions: describe **the mathematical objects** and notions we use.
- Statement or assertion: expresses that some object has a certain property. The statement may or may not be true.
- Proof: is a convincing logical argument that a statement is true.
- Theorem: is a mathematical statement proved TRUE.
- Lemma: is a theorem that are not interesting on their own but are useful for proving other theorems
- Corollary: is a follow-on theorem that are easy to prove once you prove their parent theorems

Types of Proofs

- Direct Argument
  - Use assertions from theorem statement, known true properties and valid rules of inference
- Construction
  - Prove something exists by showing how to make it
- Contradiction
  - Prove something is true by showing it can’t be false

Chapter 0

More on types of Proofs

- Prove by induction
  - **Weak Induction**
  - **Strong Induction**

- Our **goal** is to prove that **P(k) is true** for each natural number k.
- Every proof by induction consists of two parts,
  - **the basis :** prove that **P(1) is true**.
  - **the induction step:** For each $i \geq 1$, assume that **P(i) is true** and use this assumption to show that **P(i + 1) is true**. (WI)

  - **P(i) is true** is called the **induction hypothesis.**

Sample Proof by Induction

Prove, if n is a positive whole number and $n \geq 4$, then $2^n \geq n^2$.

Hint: use induction with a base of n=4.

Proof by Induction:

- **Base Case:** $n = 4$: $2^4 \geq 4^2$ since $16 \geq 16$.
- **Induction Hypothesis:** Assume $2^k \geq k^2$, for some $k \geq 4$.
- **Induction Step:** Prove $2^{(k+1)} \geq (k+1)^2$
- First, we observe that $k^2 \geq 2k+1$ when $k \geq 3$. $(K>2 \rightarrow k.k>2.k \rightarrow k^2>2k \rightarrow k^2>2k+1)$
  - Consider $k=m+1$, where $k \geq 3$; and so $m \geq 2$
  - $k^2 = (m+1)^2 = \underline{m^2} + 2m+1 \geq \underline{4} + 2m+1 > 2m+3 = 2(m+1) + 1 = 2k+1$.
- Using this,
- $2^{(k+1)} = 2^k * 2 = 2^k + 2^k \geq k^2 + k^2 \geq k^2 + 2k + 1 = (k+1)^2$

QED

Sample Proof by Contradiction

- **Prove, if p and q are distinct prime numbers, then $\sqrt{\frac{p}{q}}$ is irrational.**
- Assume $\sqrt{\frac{p}{q}}$ is rational where p and q are distinct primes. Let $\frac{a}{b}$ be the reduced fraction (no common prime factors) that equals $\sqrt{\frac{p}{q}}$.
- $\sqrt{\frac{p}{q}} = \frac{a}{b}$: assumption (note a≠b, as p≠q)
- $\frac{p}{q} = \frac{a^2}{b^2}$: square both sides
- $p = a^2$ and $q = b^2$: since p and q have no common prime factors, and a and b have no common prime factors.
- But this is not possible because p and q are prime numbers and so cannot have multiple factors (e.g., a.a, in the case of p).
- This contradicts our original assumption that $\sqrt{\frac{p}{q}}$ is rational , so it must be irrational.
- QED