CSI 2350 Discrete Mathematics

Dr. Greg Speegle

Spring 2019
Section 1

Binary, Octal and Hex
Overview

- “Normal” numbers are base 10 (0,1,2,3,4,5,6,7,8,9)
- Base indicates the number of digits
- Any integer can be a base
  - Base 2 - (0,1)
  - Base 8 (octal) - (0,1,2,3,4,5,6,7)
  - Base 16 (hexadecimal or hex) - (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F)
Place Value

- Representing values greater than base requires place value
- Let $b$ represent the base
- Two digit number $xy = x \cdot b^1 + y \cdot b^0$
- Three digit number $xyz = x \cdot b^2 + y \cdot b^1 + z \cdot b^0$
- $k$ digit number
  $$x_{k-1}x_{k-2}x_{k-3} \ldots x_0 = x_{k-1} \cdot b^{k-1} + x_{k-2} \cdot b^{k-2} + \ldots + x_0 \cdot b^0$$
- Examples:
  - $22_{10} = 2 \cdot 10 + 2 \cdot 1 = 22$
  - $22_8 = 2 \cdot 8 + 2 \cdot 1 = 18_{10}$
  - $22_{16} = 2 \cdot 16 + 2 \cdot 1 = 34_{10}$
Conversion

- Converting to base 10 uses place value
- Converting from base 10 uses algorithm
  - `Convert(n, b)`
  - `answer = ""`
  - `while n > 0`
    - `prepend n % b to answer`
    - `n ← n / b`
  - `return answer`
- Note that `n % b` can be non-digit
- Examples on board
Conversion Powers of Base

- Special case conversion to/from base $b$ to base $b^k$
- Consider base 9 and base 3.
- Base 9 has 9 digits - 0,1,2,3,4,5,6,7,8.
- Two digits in base 3 has 9 values 00,01,02,10,11,12,20,21,22
- 1-1 correspondence of values
- Base 8 has 8 digits. Three digits in base 2 have 8 values.
- Convert each digit in base $b^k$ into $k$ digits in base $b$
- Convert $k$ digits in base $b$ (add leading zeros if needed) to one digit in base $b^k$
- Examples on board
Section 2

Propositional Logic
Propositional Logic

- A *proposition* is an expression which is true or false
- A statement is true if it is always true. Otherwise, it is false.
- Examples:
  - This class is CSI 2350. (true)
  - My name is Inigo Montoya. (false)
  - CSI 2350 is the best class at Baylor. (not a proposition)
- Use variables (often $p$ and $q$) to represent statements
- If $p$ is true, the negation ($\neg p$) is false.
- If $p$ is false, the negation ($\neg p$) is true.
Propositional Statements

- The *conjunction* ($\land$) of two statements is true, both statements are true.
- The *disjunction* ($\lor$) of two statements is true if either (or both) statements are true.
- Examples:
  - Let $p$ be “This class is CSI 2350”
  - Let $q$ be “My name is Inigo Montoya”
  - $p \land q = \text{false}$
  - $p \lor q = \text{true}$
Implication

- An *implication* \( p \rightarrow q \) represents the statement “if \( p \) is true then \( q \) is true”
- Note: It **DOES NOT** represent the statement “if \( p \) is false, then \( q \) is false”
- An implication is true UNLESS when \( p \) is true, \( q \) is false
- Examples:
  - Let \( p \) be the statement, “\( n \) is even”
  - Let \( q \) be the statement, “\( n \) is odd”
  - Let \( r \) be the statement, “\( 2n \) is even”
  - \( p \rightarrow r \) is true
  - \( q \rightarrow r \) is true
  - \( p \rightarrow q \) is false
  - \( q \rightarrow p \) is false
  - \( r \rightarrow p \) is false
- Equivalent to \( \neg p \lor q \)
Truth Tables

- Columns are propositions and propositional statements
- One row for every possible truth value of propositions

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \rightarrow q$</th>
<th>$q \rightarrow p$</th>
<th>$p \rightarrow q \land q \rightarrow p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

- $p \rightarrow q \land q \rightarrow p$ is called a biconditional and is represented as $p \leftrightarrow q$
- All values true, called tautology
- All values false, called contradiction
Knights and Knaves

- Logic puzzle that can be solved with truth tables
- In the land of knights and knaves, knights always tell the truth and knaves always lie.
- Example:
  - A says, "B is a knight." B says, "2=2=5".
  - B must be a knave
  - Therefore, A must also be a knave
  - See table below. Let $p$ be "A is a knight." Let $q$ be "B is a knight."

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$2 + 2 = 5$</th>
<th>(r) $q \leftrightarrow 2 + 2 = 5$</th>
<th>(s) $p \leftrightarrow q$</th>
<th>$r \land s$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>
Knights and Knaves Explained

- Translate “A says p” into prepositional statements
- If A is a knight, then p must be true
- If A is a knave, then p must be false
- $A \leftrightarrow p$ is equivalent
- Example:
  - A says, “We’re both knaves.” B says, “No, we’re not.”
  - A is a knave and B is a knight.

<table>
<thead>
<tr>
<th></th>
<th>(r)</th>
<th>(s)</th>
<th>(t)</th>
<th>(u)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$</td>
<td>$q$</td>
<td>$\neg p \land \neg q$</td>
<td>$p \leftrightarrow r$</td>
<td>$\neg (\neg p \land \neg q)$</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Section 3

Logical Equivalence and Sets
Truth Tables and DNF

- **Disjunctive normal form (DNF)** is $C_0 \lor C_1 \lor \ldots \lor C_{k-1}$ where each $C_i$ is of the form $p \land q \land \ldots \land r$
- Given a truth table, the DNF can be generated by creating conjunct for each true result
- “Consider 3 people where exactly one is a knave.”
- $P = (p \land q \land \neg r) \lor (p \land \neg q \land r) \lor (\neg p \land q \land r)$

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$r$</th>
<th>$P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Truth Tables and CNF

- **Conjunctive normal form (CNF)** is $D_0 \land D_1 \land \ldots \land D_{k-1}$ where each $D_i$ is of the form $p \lor q \lor \ldots \lor r$.
- No easy way to go directly from CNF to truth table or vice versa.
- $Q = (\neg p \lor \neg q \lor \neg r) \land (p \lor q) \land (p \lor r) \land (q \lor r)$

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$r$</th>
<th>$\neg p \lor \neg q \lor \neg r$</th>
<th>$p \lor q$</th>
<th>$p \lor r$</th>
<th>$q \lor r$</th>
<th>$Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Logical Equivalence

- Two propositions with the same truth table are equivalent: \( P \equiv Q \)
- \( P \leftrightarrow Q \) is a tautology
- Consider \( \neg(p \lor q) \equiv (\neg p \land \neg q) \) (DeMorgan’s Law)

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( p )</td>
<td>( q )</td>
<td>( p \lor q )</td>
<td>( \neg(p \lor q) )</td>
<td>( \neg p \land \neg q )</td>
<td>( P \leftrightarrow Q )</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td></td>
</tr>
</tbody>
</table>
Logical Equivalences

- $\neg(p \land q) \equiv (\neg p \lor \neg q)$ (DeMorgan’s Law)
- $\neg(\neg p) \equiv p$
- $p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$ (Distribution Law)
- $p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$ (Distribution Law)
- $p \lor (p \land q) \equiv p$ (Absorption Law)

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$r$</th>
<th>$p \lor (q \land r)$</th>
<th>$p \lor q$</th>
<th>$p \lor r$</th>
<th>$(p \lor q) \land (p \lor r)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>
Deriving Equivalences

- Apply equivalences to derive new ones
- Equivalence is transitive (everything in chain is equivalent)
- Equivalence is associative \((p \equiv q \leftrightarrow q \equiv p)\)
- Show \(p \rightarrow q \equiv \neg q \rightarrow \neg p\)
- \(p \rightarrow q \equiv \neg p \lor q\) Definition implication
- \(\neg p \lor q \equiv q \lor \neg p\) Association
- \(q \lor \neg p \equiv \neg (\neg q) \lor \neg p\) Double negation
- \(\neg (\neg q) \lor \neg p \equiv \neg q \rightarrow \neg p\) Definition implication
Satisfiability

- A predicate is *satisfiable* if there exists an assignment of truth values such that the predicate evaluates to true. Otherwise, it is unsatisfiable.

- $p \land \neg q$ is satisfiable when $p = T$ and $q = F$

- $p \rightarrow \neg p$ is satisfiable when $p = F$

- $p \land (p \rightarrow \neg p)$ is unsatisfiable.

- A predicate in DNF is easy to determine if satisfiable. Check each conjunct. If no negated and unnegated same variable, then satisfiable.

- A predicate in CNF has no known efficient algorithm to determine if satisfiable (check all truth table)

- Fundamental problem in computer science $P = NP$
Introduction to Sets

- Collection of unordered distinct elements
- $S = \{A, -3, \text{“orange”}\}$
- Size (or cardinality is number of elements $|S| = 3$
- $\mathbb{N}$ is the set of all natural numbers
- $\mathbb{Z}$ is the set of all integers
- $\mathbb{Z}^+$ is the set of all positive integers
- $\mathbb{Q}$ is the set of all rational numbers
- $\mathbb{R}$ is the set of all real numbers (others in text)
- Elements can be anything, even sets
- $S = \{\mathbb{N}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}\}$
- $|S| = 4$
- Empty set ($\emptyset$) contains no elements
Subsets

- $S \subset T$ iff all elements in $S$ are in $T$
- $S = T$ iff $S \subset T \land T \subset S$
- $\emptyset \subset S$ for any set $S$
- Proper and improper subsets
- Power set $2^S$ is the set of all subsets of $S$
- $2^\emptyset = \{\emptyset\}$. Therefore, $|2^\emptyset| = 1$
- Let $S = \{A, B\}$. $2^S = \{\emptyset, \{A\}, \{B\}, S\}$.
- $|2^S| = 2^{|S|}$.
Section 4

Sets and Quantification
Logical Predicates

- Statements can involve variables
- Let $P(x)$ be $x > 3$
- A *predicate* evaluates at statement with a particular value
- $P(4)$ is true. $P(2)$ is false.
- Quantifiers can be used to evaluate predicate over a set
- Universal quantification (for all – $\forall$) is true if true for all elements of set
- Existential quantification (there exists – $\exists$) is true if true for any element of set
- Let $S = \{2, 4, 6\}$.
- $\forall x \in S, P(x)$ is false.
- $\exists x \in S, P(x)$ is true
Quantifier Properties

- Two predicates are *equivalent* iff they hold the same truth value for any predicate and domain.
- \( \forall x(P(x) \land Q(x)) \equiv \forall x(P(x) \land \forall x(Q(x))) \)
- \( \neg \forall x P(x) \equiv \exists x(\neg P(x)) \)
- \( \neg \exists x P(x) \equiv \forall x(\neg P(x)) \)
- Order is important! Evaluate left to right.
- \( \forall \) tries to make statement false.
- \( \exists \) tries to make statement true.
- \( \forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}, x + y = 0 \) is true
- \( \exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x + y = 0 \) is false
- \( \exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}, xy = 0 \) is true
Sets and Quantifiers

- Set builder notation.
  - \( S = \{ x \in \mathbb{Z}^+ | P(x) \} \) is the set of all positive integers such that \( P(x) \) is true.
  - \( S = \{ x \in \mathbb{Z}^+ | x < 3 \} = \{1, 2\} \)
  - \( S = \{ x \in \mathbb{Z}^+ | x > 3 \} \). \( T = \{ x \in S | x < 6 \} \). \( T = \{4, 5\} \)
- \( S \subset T \) iff \( \forall x \in S, x \in T \)
- Union: \( S \cup T = \{ x | x \in S \lor x \in T \} \)
- Intersection: \( S \cap T = \{ x | x \in S \land x \in T \} \)
- Difference: \( S - T = \{ x | x \in S \land x \notin T \} \)
- Complement: \( \bar{S} = \{ x | x \notin S \} \)
- A universal set, \( U \) contains all possible values.
  - \( \bar{S} = U - S \)
  - \( S - T = S \cap \bar{T} = S \cap (U - T) = (S \cap U) - (S \cap T) = S - (S \cap T) \)
Proofs with Sets

- Prove $S - T = S \cap \overline{T}$
- Part 1. $S - T \subset S \cap \overline{T}$
  - Let $x \in S - T$ (if no $x$ exists, $S - T = \emptyset$ and done)
  - $x \in S \land x \notin T$ Definition of difference
  - $x \in \overline{T}$ Definition of complement.
  - $x \in S \cap \overline{T}$ Definition of intersection
- Part 2. $S \cap \overline{T} \subset S - T$
  - Let $x \in S \cap \overline{T}$ (if no $x$ exists, $S \cap \overline{T} = \emptyset$ and done)
  - $x \in S \land x \in \overline{T}$ Definition intersection
  - $x \notin T$ Definition of complement
  - $x \in S - T$ Definition of difference
- QED
Generalized Set Properties

- $A \cup B = B \cup A$ and $A \cap B = B \cap A$
- $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$
- Let $A_0, A_1, \ldots, A_{k-1}$ be sets.
  - $\bigcup_{i=0}^{k-1} = A_0 \cup A_1 \cup \ldots \cup A_{k-1}$
  - $\bigcap_{i=0}^{k-1} = A_0 \cap A_1 \cap \ldots \cap A_{k-1}$
Section 5

Proofs
Proof Techniques

- A proof is a convincing argument.
- Set of premises (things which are true at the start)
- Set of logical statements (which must be valid)
- Set of conclusions (which are now known to be true)
- Example:
  - Prove \( S - T = S - (S \cap T) \)
  - Premise: \( S \) and \( T \) are sets
  - Logical Statements: Set identities
  - Set of conclusions: \( x \in S - T \iff x \in S - (S \cap T) \)
Example Proof

- Proof $S - T = S - (S \cap T)$:
  - There are two items to show. (1) $x \in S - T \rightarrow x \in S - (S \cap T)$ and (2) $x \notin S - T \rightarrow x \notin S - (S \cap T)$
  - Case 1: $x \in S - T \rightarrow x \in S - (S \cap T)$
    - $x \in S - T \rightarrow x \in S \land x \notin T$
    - $\therefore x \notin S \cap T$
    - $\therefore x \in S - (S \cap T)$
  - Case 2: $x \notin S - T \rightarrow x \notin S - (S \cap T)$
    - $x \notin S - T \rightarrow x \notin S - (S \cap T) \equiv x \in S - (S \cap T) \rightarrow x \in S - T$ (why?)
    - $x \in S - (S \cap T) \rightarrow x \in S \land x \notin (S \cap T)$
    - $\therefore x \notin S \land (x \notin S \lor x \notin T)$
    - $\therefore (x \in S \land x \notin S) \lor (x \in S \land x \notin T)$
    - $\therefore x \in S \land x \notin T$
    - $\therefore x \in S - T$
Valid Logical Statements

- $p, p \rightarrow q, \therefore q$ - modus ponens
- $\neg q, p \rightarrow q, \therefore \neg p$ - modus tollens
- $p \rightarrow q, q \rightarrow r, \therefore p \rightarrow r$ - Hypothetical syllogism
- $p \lor q, \neg p, \therefore q$ - Disjunctive syllogism
- $\forall x P(x), \therefore P(c)$ - Universal instantiation
- $P(c)$ for an arbitrary $c, \therefore \forall x P(x)$ - Universal generalization
Proof by Contradiction

- Assume system is logically consistent
- Therefore, either $p$ or $\neg p$ can be true, but not both
- Start by assuming $\neg p$ is true
- Often $p$ is implication ($p \rightarrow q$)
- Negation of implication $\neg(\neg p \lor q) \equiv p \land \neg q$
- Apply logically sound statements
- Reach clearly false statement
- Therefore, $\neg p$ cannot be true, so $p$ must be true
Contradiction Proof Example

- Prove that if \( n \in \mathbb{Z} \land n^3 + 5 \) is odd, then \( n \) is even.
- \( n \in \mathbb{Z} \land (n^3 + 5) \mod 2 = 1 \rightarrow n \mod 2 = 0 \)
- Assume not. Therefore \((n^3 + 5) \mod 2 = 1 \land n \mod 2 = 1\)
- \( \therefore \exists k \in \mathbb{Z}, n = 2k + 1 \)
- \( \therefore n^3 + 5 = 8k^3 + 12k^2 + 6k + 1 + 5 \)
- \( 8k^3 \) is even, \( 12k^2 \) is even, \( 6k \) is even, and \( 6 \) is even.
- Since the sum of two even numbers is even, \( 8k^3 + 12k^2 \) and \( 6k + 6 \) are even.
- Similarly, \( (8k^3 + 12k^2) + (6k + 6) \) is even.
- Since an integer cannot be both even and odd, we have a contradiction!
Counter Example

- Best way to prove something false
- Theorem: \( \forall x \in \mathbb{Z}, x^2 > x \)
- Counter example: Let \( x = 0 \). \( x^2 = 0 = x \), so theorem is false.
- Theorem: \( \exists y, \forall x, xy = 1 \)
- Consider \( x \) and \( x + 1 \).
- \( xy = 1 \) and \( y(x + 1) = xy + y = 1 \)
- \( \therefore 1 + y = 1 \), so \( y = 0 \)
- \( 0x = 0 \neq 1 \)
Section 6

Sets, Tuples and Relations
A tuple is an ordered collection of elements. It may or may not contain duplicates. Similar to an array.

Each item in a tuple can be accessed by its location.

Standard notation not as common. We will use parenthesis to denote a tuple and brackets to note the index of an element.

Examples:

- $t_0 = (1, 2, 3, 1, 2, 3)$
- $t_1 = ("orange", \emptyset, 42)$
- $t_2 = (\{0, 1\}, (0, 0))$

- $t_0$ is a 6-tuple $t_0[0] = 1$
- $t_1$ is a 3-tuple (also called a triple) where $t_1[1] = \emptyset$.
- $t_2$ is a 2-tuple, usually called an ordered pair, where $t_2[1] = (0, 0)$ and $t_2[1][1] = 0$
Let \( S \) and \( T \) be sets. The *cross product* or *Cartesian product* \( S \times T \) is a set of ordered pairs where the first element is from \( S \) and the second element is from \( T \). All possible combinations are in the cross product.

Example

- Let \( S = \{ a, b, c \} \).
- Let \( T = \{ 1, 2 \} \).
- \( S \times T = \{ (a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2) \} \)

Note that \( (1, a) \notin S \times T \)

\[ |S \times T| = |S| \times |T| \]

Taking the cross product of \( k \) sets generates a \( k \)-tuple where the elements are from the corresponding sets.
Relations

- A *Relation* is a subset of the Cartesian product of an ordered collection of sets such that each tuple satisfies a predicate $P$.

Example:

- Let $S_0 = \{1, 2, 3\}$, $S_1 = \{"a", "b", "c"\}$, $S_2 = \{0, 3\}$.
- Let $R_0 = \{(a, b, c)| a \in S_0, b \in S_1, c \in S_2, b = "b" \land a \geq c\}$
- $R_0 = \{(1, "b", 0), (2, "b", 0), (3, "b", 0), (3, "b", 3)\}$
- Let $R_1 = \{(a, b, c)| a \in S_0, b \in S_1, c \in S_2, a = c\}$
- $R_1 = \{(3, "a", 3), (3, "b", 3), (3, "c", 3)\}$
- Since relations are sets, set operators can be applied. However, the result may not be a relation.

- $R_0 \cup S_0 = \{(1, "b", 0), (2, "b", 0), (3, "b", 0), 1, 2, 3\}$.
- Set operations on two relations over the same ordered collection of sets, is a relation.

- $R_0 \cap R_1 = \{(3, "b", 3)\}$
Properties of Relations

- Relations between a set and itself ($R \subseteq A \times A$) have special properties
- **Reflexive**: $\forall a \in A, R(a, a)$
  - $R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 \leq z_1\}$ is reflexive
  - Proof: $k \leq k$ is true for all integers.
  - $R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 < z_1\}$ is NOT reflexive
  - Counterexample: $3 \in \mathbb{Z}, (3, 3) \notin R$
- **Symmetric**: $\forall a, b \in A, R(a, b) \rightarrow R(b, a)$
  - $R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 \leq z_1\}$ is NOT symmetric
  - Counterexample: $3 < 7 \rightarrow (3, 7) \in R. 7 \not< 3, \therefore (7, 3) \notin R$
  - $R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 = z_1\}$ is symmetric (and reflexive)
  - Proof (symmetric): Follows from commutative property of equality
  - Proof (reflexive): Follows from reflexive property of equality
  - $R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 \text{ and } z_1 \text{ are relatively prime}\}$ is symmetric (and not reflexive)
  - Proof (symmetric): $\gcd(a, b) = \gcd(b, a)$
  - Counterexample (not reflexive): Consider 6. $\gcd(6, 6) > 1$
Properties of Relations

- **Antisymmetric (poorly named):**
  \[ \forall a, b \in A, R(a, b) \wedge R(b, a) \rightarrow a = b \]
  - \( R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 \leq z_1\} \) is antisymmetric
  - Proof: \( a \leq b \wedge b \leq a \rightarrow a = b \)
  - \( R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 = z_1\} \) is antisymmetric
  - Proof: Follows from commutative property of equality
  - \( R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 \text{ and } z_1 \text{ are relatively prime}\} \) is NOT antisymmetric
    - Counterexample: \( \gcd(5, 8) = 1, \gcd(8, 5) = 1, 5 \neq 8 \)

- **Transitive:** \( R(a, b) \wedge R(b, c) \rightarrow R(a, c) \)
  - \( R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 \leq z_1\} \) is transitive
  - Proof: \( a \leq b \wedge b \leq c \rightarrow a \leq c \)
  - \( R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 = z_1\} \) is transitive
  - Proof: Follows from the transitive property of equality
  - \( R = \{(z_0, z_1) | z_0, z_1 \in \mathbb{Z}, z_0 \text{ and } z_1 \text{ are relatively prime}\} \) is NOT transitive
    - Counterexample: \( \gcd(5, 8) = 1, \gcd(8, 15) = 1, \gcd(5, 15) = 5 \)
Compositions

- Let $S$, $T$ and $U$ be arbitrary sets.
- Let $R_0$ be a relation on $(S, T)$ and $R_1$ be a relation on $(T, U)$.
- The composition $R_C = R_1 \circ R_0$ is a relation on $(S, U)$ such that $\forall (s, u) \in R_C, \exists (s, t) \in R_0 \land (t, u) \in R_1$.
- Example:
  1. $R_0 = \{(1, 1), (1, -1), (4, 2), (4, -2)\}$
  2. $R_1 = \{(1, 0), (1, 2), (2, 1), (2, 3)\}$
  3. $R_1 \circ R_0 = \{(1, 0), (1, 2), (4, 1), (4, 3)\}$
- Not all elements in either relation must be used. Composition can be empty set.
- If relation is on single set, can take “powers” by composition.
- $R^1 = R.R^n = R^{n-1} \circ R$.
- Example: $A = \{1, 2, 3\}, R = \{(1, 2), (2, 3), (3, 1)\}$
- $R^2 = R \circ R = \{(1, 3), (2, 1), (3, 2)\}$
- $R^3 = R^2 \circ R = \{(1, 1), (2, 2), (3, 3)\}$
Section 7

Functions
A function is a relation over two sets such that the first element is unique.

\[ f : A \to B = \{(a, b) | \forall t, t' \in f, t[0] = t'[0] \to t = t'\} \]

\[ f(a) \in B. \cup_{a \in A} f(a) \subset B \text{ Also denoted } f(A) \subset B. \]

Examples: Let \( A, B = \mathbb{Z} \) and \( x \in \mathbb{Z} \)

- \( f(x) = x + 2 = \{(0, 2), (1, 3), (-1, 1) \ldots\} \)
- \( f(x) = x^2 = \{(0, 0), (1, 1), (-1, 1) \ldots\} \)
- \( f(x) = \sqrt{x} = \{(0, 0)(1, 1), (1, -1) \ldots\} \) NOT A FUNCTION!
Let $f : A \rightarrow B$, $f(a) = b$ and $g : A \rightarrow B$, $g(a) = b$

- $A$ is the **domain** of $f$
- $B$ is the **codomain** of $f$
- $\bigcup_{a \in A} f(a)$ is the **range** of $f$
- $b$ is the **image** of $a$
- $a$ is the **preimage** of $b$

Two functions $f = g$ if $f \subset g \land g \subset f$ and $f, g$ have same domain and codomain.

- Let $B = \mathbb{R}$. Then $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$
- Let $S \subset A$, $f(S) = \{x | \exists s \in S, (x = f(s))\}$
One-to-One and Onto

- A function is *one-to-one* or an *injection* iff 
  \[ f(a) = f(b) \rightarrow a = b. \]

- Note: \(|A| > |B|\) implies \( f \) is not 1-1

- Examples: \( f : A \rightarrow B, A = \{1, 2, 3\}, \)
  - \( B = \{1, 2, 3, 4\}, f(a) = a, f = \{(1, 1), (2, 2), (3, 3)\} \)
  - \( B = \{1, 2, 3, 4\} f(a) = \lceil a/2 \rceil, f = \{(1, 1), (2, 1), (3, 2)\} \) NOT 1-1

- A function is *onto* or an *surjection* iff \( \bigcup_{a \in A} f(a) = B \)

- Note \(|B| > |A|\) implies \( f \) is not onto

- Examples:
  - \( B = \{1, 2, 3\} f(a) = a \) onto and 1-1
  - \( B = \{1, 2, 3\} f(a) = \lceil a/2 \rceil, \) NOT onto

- A function is a *bijection* if it is 1-1 and onto
Function Inverse and Composition

- Given $f : A \rightarrow B, f^{-1} : B \rightarrow A = \{(b, a) | (a, b) \in f\}$
- $f$ must be a bijection for $f^{-1}$ to be a function
  - Not onto implies $f^{-1}$ is undefined for some elements in domain
  - Not 1-1 implies $\exists x f^{-1}(x)$ is not unique
- Composition of functions same as composition of relations
- $f : A \rightarrow B, g : B \rightarrow C. (g \circ f)(x) = g(f(a))$
- Examples:
  - $f^{-1}(f(x)) = x$
  - $f(x) = 2x + 1. g(x) = x^2. g(f(x)) = 4x^2 + 4x + 1. f(g(x)) = 2x^2 + 1$
  - $f(x) = 1. g(x) = x + 1. g(f(x)) = 2. f(g(x)) = 1.$
Section 8

Matrices
Matrix Overview

- Given two k-tuples, $A$ and $B$, provides a value for each element in $A \times B$
- Similar to relations with sets replaced by tuples and predicate replaced by value
- Each element in $A$ corresponds to row in $M$
- Each element in $B$ corresponds to column in $M$
- Example - Powers of numbers (Matrix $M$).
  $A = (1, 2, 3). B = (0, 1, 2, 3)$

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 \\ 1 & 3 & 9 & 27 \end{bmatrix}$$

- $m$ rows and $n$ cols is $m \times n$ matrix ($M$ is 3x4).
- $m=n$ is square matrix
- Element $M_{i,j}$ where $i$ is row number and $j$ is column number
Matrix Addition

- Requires $M, N$ be same size
- $M + N = L \rightarrow \forall i, j L_{i,j} = M_{i,j} + N_{i,j}$

\[
\begin{bmatrix}
1 & 1 & 1 & 1 \\
2 & 1 & 2 & 4 \\
3 & 1 & 3 & 9 \\
\end{bmatrix} + \begin{bmatrix}
1 & 2 & 3 & 4 \\
5 & 6 & 7 & 8 \\
9 & 10 & 11 & 12 \\
\end{bmatrix} = \begin{bmatrix}
2 & 3 & 4 & 5 \\
7 & 7 & 9 & 12 \\
12 & 11 & 14 & 21 \\
\end{bmatrix}
\]
Matrix Multiplication

- Columns in \( M \) must equal rows in \( N \)
- \( M \) is \( m \times k \), \( N \) is \( k \times n \), \( L \) is \( m \times N \)
- \( L_{i,j} = \sum_{h=1}^{k} M_{i,h} \times N_{h,j} \)

\[
\begin{bmatrix}
1 & 1 & 1 & 1 \\
2 & 1 & 2 & 4 \\
3 & 1 & 3 & 9 \\
\end{bmatrix}
\times
\begin{bmatrix}
1 & 2 \\
5 & 6 \\
9 & 10 \\
11 & 12 \\
\end{bmatrix}
= \begin{bmatrix}
26 & 30 \\
69 & 78 \\
134 & 150 \\
\end{bmatrix}
\]

- Example:
  \( L_{2,2} = \sum_{h=1}^{4} M_{2,h} \times N_{h,2} = 2 \times 2 + 1 \times 6 + 2 \times 10 + 4 \times 12 = 78 \)

- Example:
  \( L_{1,2} = \sum_{h=1}^{4} M_{1,h} \times N_{h,2} = 1 \times 2 + 1 \times 6 + 1 \times 10 + 1 \times 12 = 30 \)

- NOT commutative (e.g., \( M \times N \neq N \times M \), see above)
Identity Matrix and Transposition

- Identity matrix (usually $I$)
  - Square
  - Diagonal values are 1; all other values are 0
  - $M \times I = I \times M = M$

- Transpose of $M = M^t$
  - $M^t_{i,j} = M_{j,i}$
  - $M$ is symmetric if $M = M^t$ (note: must be square)

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 4 \\ 3 & 1 & 3 & 9 \end{bmatrix} \rightarrow M^t = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{bmatrix}$$
Matrix Powers

- Let $M$ be a square $n \times n$ matrix.
- $M^0 = I$
- $M^1 = IM = M$
- $M^k = M^{k-1}M$

\[
M = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \quad M^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad M^2 = \begin{bmatrix} 7 & 10 \\ 15 & 22 \end{bmatrix}, \quad M^3 = \begin{bmatrix} 37 & 54 \\ 81 & 118 \end{bmatrix}
\]
Boolean Matrices

- A matrix $M$ such that all values are T(1) or F(0)
- Let $M$ and $N$ be boolean matrices. $M \lor N = L$ (join)
  \[ L_{i,j} = M_{i,j} \lor N_{i,j} \]
- Let $M$ and $N$ be boolean matrices. $M \land N = L$ (meet)
  \[ L_{i,j} = M_{i,j} \land N_{i,j} \]
- Matrix multiplication of boolean matrices is disjunction of conjuncts of terms
- $M, N$ are boolean matrices. $M \otimes N = L$
- $L_{i,j} = \bigvee_{h=1}^{k} (M_{i,h} \land N_{h,j})$
- Example:

\[
M = \begin{bmatrix}
1 & 1 & 1 \\
0 & 1 & 0 \\
0 & 0 & 0
\end{bmatrix}, \quad N = \begin{bmatrix}
1 & 0 \\
0 & 1 \\
1 & 0
\end{bmatrix}, \quad L = \begin{bmatrix}
1 & 1 \\
0 & 1 \\
0 & 0
\end{bmatrix}
\]
Let $A$ be an arbitrary set of $k$ elements, and $R(A, A)$

Let $A'$ be a $k$-tuple of the elements in $A$ with an arbitrary order.

Let $M$ be a boolean matrix over $A' \times A'$, such that $(a_i, a_j) \in R \iff M[i][j] = 1$

Example:
- Let $A$ be a set of three volunteers
- $R(A, A) = \{(a, b)|a, b \in A, a \text{ “taller than” } b\}$
- Order elements in $A$ by first name (alphabetical)
- $M$ on board

Note: $M$ is square. Ordering is same for columns and rows.
Properties of Relations with Matrices

Given $R(A, A)$ and $M$ defined as before.

- If $M$ main diagonal is all 1’s, $R$ is reflexive.
- If $M = M^t$, $R$ is symmetric.
- If $M \land M^t$ is all zero except the main diagonal, $R$ is antisymmetric.
- If $\bigvee_{i=1}^k M^i = M$, $R$ is transitive.
Section 9

Summations and Induction
Summations

- Add the terms in a sequence
- Uses $\Sigma$
- Examples:
  - $\sum_{j=1}^{n} j = \frac{n(n+1)}{2}$
  - $\sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$
  - $\sum_{j=1}^{n} 2j + 3 = 2\sum_{j=1}^{n} j + \sum_{j=1}^{n} 3 = 2\frac{n(n+1)}{2} + 3n = n^2 + 4n$
  - $\sum_{j=0}^{n} ar^j = \frac{ar^{n+1} - a}{r - 1}[r \neq 1], (n+1)a[r = 1]$
  - Let $S = \{1, 2, 4, 8\}$ then $\sum_{x \in S} x = 1 + 2 + 4 + 8 = 15$
Double Summations

- Summation over two variables
- Inner and outer loop
- Examples:
  - $\sum_{i=1}^{4} \sum_{j=1}^{3} i \times j = 1 + 2 + 3 + 2 + 4 + 6 + 3 + 6 + 9 + 4 + 8 + 12 = 60$
  - $\sum_{i=1}^{4} \sum_{j=1}^{3} i \times j = \sum_{i=1}^{4} (i + 2i + 3i) = \sum_{i=1}^{4} 6i = 6 \times \sum_{i=1}^{4} i = 6 \times 10 = 60$
Induction

- Proof technique for showing infinite series is true
- Require incremental progress
- Basis – Initial step (usually very easy to show)
- Induction Hypothesis (IH) – Theorem is true for $k$ elements
- NOTE! Have not proved IH is true. Just assuming it is.
- Show Theorem is true for $k + 1$ elements
- Therefore, initially true. Basis is now IH for next step. Now have IH for following step, etc.
Induction Example

- Summations “easily” shown by induction (proof simple; algebra can be tricky)
- Prove $\sum_{i=1}^{n} i^3 = (n(n + 1)/2)^2$
- Basis: $P(1)$. $1^3 = 1 = (1(2)/2)^2$
- IH: $\sum_{i=1}^{k} i^3 = (k(k + 1)/2)^2$
- Let $n = k + 1$.
- $\sum_{i=1}^{k+1} i^3 = \sum_{i=1}^{k} i^3 + (k + 1)^3$
- By IH, $\sum_{i=1}^{k+1} i^3 = (k(k + 1)/2)^2 + (k + 1)^3$
- $= (((k^2 + k)/2)^2 + k^3 + 3k^2 + 3k + 1$
- $= (k^4 + 2k^3 + k^2)/4 + k^3 + 3k^2 + 3k + 1$
- $= (k^4 + 2k^3 + k^2 + 4k^3 + 12k^2 + 12k + 4)/4$
- $= (k^4 + 6k^3 + 13k^2 + 12k + 4)/4$
- Note that $((k + 1)(k + 2)/2)^2 = ((k^2 + 3k + 2)/2)^2 = (k^4 + 3k^3 + 2k^2 + 3k^3 + 9k^2 + 6k + 2k^2 + 6k + 4)/4$
- $= (k^4 + 6k^3 + 13k^2 + 12k + 4)/4$
- So $\sum_{i=1}^{k+1} i^3 = ((k + 1)(k + 2)/2)^2$
Induction Example

- Prove $x \geq 4 \rightarrow x \geq 2 \cdot \log(x)$
  - Lemma: $x \geq 3 \rightarrow x^2 \geq 2x + 1$
  - Basis $P(3)$. $3^2 \geq 2 \cdot 3 + 1$
  - IH: $x = k \rightarrow k^2 \geq 2k + 1$
  - Let $x = k + 1$. $x^2 = k^2 + 2k + 1$.
    - $> 2k + 1 + 2k + 1$
    - $> 2k + 3$
    - $> 2(k + 1) + 1$
  - Basis: $P(4)$. $4 \geq 2 \cdot \log(4) = 4$
  - IH: $x = k \rightarrow x \geq 2 \cdot \log(x)$
  - Let $x = k + 1$.
    - By IH, $x \geq 2 \cdot \log(k) + 1$
    - $x \geq \log(k^2) + \log(2)$
    - $x \geq \log(2 \cdot k^2)$
    - $x > \log(k^2 + 2 \cdot k + 1)$
    - $x > \log((k + 1)^2) = 2 \cdot \log(k + 1) = 2 \cdot \log(x)$
Odd Man Pie Fights (from text)
   - People stand in yard at distinct distances
   - Throw pie at nearest neighbor
   - Odd number of participants ensures at least 1 person is not hit

Technique - Induct over $n$ for $P(2n + 1)$

Basis: $n = 1, P(3)$. Let $(a, b)$ be closest pair. Then $a$ hits $b$ and $b$ hits $a$. $c$ hits whoever is closest to $c$, but nobody hits $c$
Odd Man Out Proof (cont’d)

- IH: Assume theorem is true for \( n = k, P(2 \ast k + 1) \).
- Let \( n = k + 1 \). Therefore, want to show \( P(2 \ast (k + 1) + 1) \) or \( P(2 \ast k + 3) \).
- Let \((a, b)\) be the closest pair (all distances unique implies least element exists).
- Therefore, \( a \) hits \( b \) and \( b \) hits \( a \).
- Case I:
  - Someone else throws a pie at \( a \) or \( b \)
  - Therefore, at least 3 pies thrown at \( a \) and \( b \), leaving at most \( 2k \) pies for \( 2k + 1 \) people.
- Case II:
  - Nobody throws a pie at \( a \) or \( b \)
  - Now \( 2 \ast (k + 1) \) people remain with pies.
  - By IH, at least one is not hit.
Induction Example

- Number of elements in $2^S$ (from text)
- Show $|2^S| = 2^{\left|S\right|}$
- Basis: $\emptyset$. The only subset of $\emptyset$ is itself. $|2^S| = 1 = 2^0$
- IH: $|S| = k \rightarrow |2^S| = 2^k$
- Let $|T| = k + 1$. $T = S \cup \{a\}$ such that $S = T - \{a\}$.
- Let $X \subseteq S$. Therefore, $X \subseteq T$ and $X \cup \{a\} \subseteq T$.
- By IH, there are $2^k$ such subsets of $S$, and $2 \times 2^k = 2^{k+1}$ subsets of $T$. 
Section 10

Recursion and Strong Induction
Strong (Complete) Induction

- IH is not just that \( P(k) \) is true, but
  \( P(1) \land P(2) \land P(3) \ldots \land P(k) \) is true
- Equivalent to Induction, but sometimes easier to use
- Example: Prove that every positive integer \( n \) can be written as a sum of distinct powers of 2
- Basis: \( n = 1. \ 2^0 = 1 = n \)
- IH: \( \forall n \leq k, n \) can be written as a sum of distinct powers of 2
- Let \( n = k + 1 \)
- Case I:
  - Let \( n \) be odd.
  - Since \( n \) is odd, \( k \) must be even.
  - By IH, let \( S \) be representation of the sum for \( k \)
  - Therefore, \( 2^0 \) cannot be in \( S \)
  - Therefore \( n = \text{(representation for } k) + 2^0 \).
Case II

- Let $n$ be even.
- Therefore, $n/2$ is an integer such that $n/2 \leq k$.
- By IH, let $S$ be representation of the sum for $n/2$
- Multiplying $S$ by 2 increases each exponent by 1. (DPMA)
- Therefore, $S$ with each exponent increased by 1 is $n$

Compare with normal induction

Case I is the same

Case II is more difficult
Proof?

- $n \in \mathbb{N} \rightarrow 5n = 0$ (include $0 \in \mathbb{N}$)
- Basis: $5 \cdot 0 = 0$
- IH For all $i < k$, $5 \cdot i = 0$
- Prove for $k + 1$
- $k + 1 = i + j$ where $i$ and $j$ are less than $k$
- $5 \cdot (k + 1) = 5(i + j) = 5i + 5j = 0 + 0 = 0$
- QED
- Any problems?
Function Recursion

- Compute values of a function based on previous values in the function
- Specify the value at 0 (or first $k$ values)
- Provide rule for $f(n)$ based on lower values of $n$
- Factorial: $f(0) = 1. \forall n, n > 0 \rightarrow f(n) = n \times f(n - 1)$.
- Fibonacci:
  $f(0) = 0, f(1) = 1. \forall n, n > 1 \rightarrow f(n) = f(n - 1) + f(n - 2)$
- Paradox:
  $f(0) = 0.5. \forall n, n > 1 \rightarrow f(n) = (1 - f(n - 1))/2 + f(n - 1)$
Set Recursion

- Compute elements in a set based on previous elements in the set
- Provide rule for initial elements. Provide rule for adding new elements.

Initial - $1 \in S$. Step - $s, t \in S \rightarrow s + t \in S$ Prove $S = \mathbb{Z}^+$ 
(Note! $s$ and $t$ do not have to be unique!):

- Clearly, $S \subseteq \mathbb{Z}^+$
- Basis: $1 \in S$ by definition of $S$
- IH: $k \in S$.
- Since $k$ and $1$ are in $S$, by rule, $k + 1 \in S$

Transitive Closure: Let $R(A, A)$ be a relation. The transitive closure of $R^*$ ($R$ plus all elements in $A \times A$ needed to make $R$ transitive) is:

- Initial $(a, b) \in R \rightarrow (a, b) \in R^*$
- Step - $(a, b), (b, c) \in R \rightarrow (a, c) \in R^*$
Recursive Algorithm

- Compute results using previously computed results
- Provide rule for terminal case. Provide rule for recursive call.
- Example: factorial
  - fact(n)
  - if $n \leq 0$ return 1
  - else return $n \cdot \text{fact}(n - 1)$
- Example: gcd
  - gcd(a,b)
  - if $a = 0$ return b
  - return gcd(b%a,a)
Recursive Algorithm Example

- Example: fibonacci (Problem?)
  - fib(a)
  - if a=0 return 0
  - if a=1 return 1
  - return fib(a-1)+fib(a-2)

- Example: Binary Search (Problem?)
  - Let $A = [a_1, a_2, \ldots, a_n]$
  - find($A, x, i, j$)
  - if $i \geq j$, then
    - if $a_i = x$ return $i$
    - else return 0
  - $m \leftarrow \lfloor (i + j)/2 \rfloor$
  - if $x > a_m$, then return find($A, x, m + 1, j$)
  - else return find($A, x, i, m$)
Section 11

The Big $\Omega\Theta$ Fraternity
Binary Search

- Input list of elements \([a_1, a_2, \ldots, a_n]\), search key \(x\)
- Output index of element matching \(x\), or 0 if not found
- Pseudocode
  - \(i \leftarrow 1\)
  - \(j \leftarrow n\)
  - while \((i < j)\)
    - \(m \leftarrow \lfloor (i + j)/2 \rfloor\)
    - if \(x > a_m\) then \(i \leftarrow m + 1\)
    - else \(j \leftarrow m\)
  - if \(x = a_i\) then return \(i\)
  - else return 0
Binary Search Runtime

- Assume $n = 2^k$ elements in list
- After iteration, remaining list half of previous list size
- After $k$ iterations, list is size 1
- $\log(n) = k$
- Worst case running time is $\log(n)$
Let $f$ and $g$ be functions. $f(x)$ is $O(g(x))$ if $\exists C, k$ such that $f(x) \leq C \ast g(x)$ for all $n > k$ Assume $x \geq 0$.

- Function $f$ grows slower than function $g$ for $n > k$

**NOTE:** Can say ”is” or $\in$ but $=$ is misleading (although used frequently)

**NOTE:** Existence proof. Find one $C$ and one $k$ (many may exist).

**Technique:** Start with known ($x > k$). Remember, we can select $k$

**Apply formulas to generate $C \ast g(x) \geq f(x)$**

**Examples:**

- $f(x) = 17x + 11 \in O(g(x) = x^2)$. Let $C = 2, k = 17$.
  - $x \geq 17 \rightarrow x^2 \geq 17x$
  - $\rightarrow x^2 + x^2 \geq 17x + 11$
  - $\rightarrow 2 \ast x^2 \geq 17x + 11$
Examples:

- $f(x) = x \log(x) \in O(g(x) = x^2)$. Let $C = 1, k = 1$
  - $x \geq 1 \rightarrow x \geq \log(x) \rightarrow x^2 \geq x \log(x)$
- $f(x) = x^2 + x + 1 \in O(g(x) = x^2)$. Let $C = 3, k = 1$
  - $x \geq 1 \rightarrow x^2 \geq x \rightarrow x^2 + x^2 \geq x^2 + x$
  - $\rightarrow x^2 + x^2 + x^2 \geq x^2 + x + 1 \rightarrow 3 \ast x^2 \geq x^2 + x + 1$

To show $f(x)$ is not $O(g(x))$ must show no such $C$ and $k$ can exist.

Example:

- $f(x) = x^2$ is not $O(g(x) = x)$.
  - Assume not. Therefore $\exists C, k$ such that $f(x) \leq C \ast g(x) \forall x > k$
  - Therefore, $x^2 \leq C \ast x \forall x \geq k$.
  - Therefore, $x \leq C \forall x \geq k$, which is a contradiction.
Let $f$ and $g$ be functions. $f(x)$ is $\Omega(g(x))$ if $\exists C, k$ such that $f(x) \geq C \cdot g(x)$ for all $n > k$ Assume $x \geq 0$.

Function $f$ grows faster than function $g$ for $n > k$

$f(x)$ in $\Omega(g(x)) \leftrightarrow g(x) \in O(f(x))$

Example:

- $f(x) = x^2$ is $\Omega(g(x) = x)$ because $g(x) = x$ is $O(f(x) = x^2)$
- $f(x) = x^4/2$ is $\Omega(g(x) = x^2)$. Show $g(x) = x^2$ is $O(f(x) = x^4/2)$

Let $C = 1, k = 2$

$x \geq 2 \rightarrow x^2 \geq 2x \rightarrow x^3 \geq 2x^2 \rightarrow x^4 \geq 2x^2 \rightarrow x^4/2 \geq x^2$
Let $f$ and $g$ be functions. If $f(x)$ is $\Omega(g(x))$ and $f(x)$ is $O(g(x))$, then $f(x)$ is $\Theta(g(x))$.

Equivalent: $f(x)$ is $O(g(x))$ and $g(x)$ is $O(f(x))$.

$f(x)$ is bounded above and below by $g(x)$.

Example:

- $f(x) = x^2 + x + 1$ is $\Theta(g(x) = x^2)$
- Show $f(x)$ is $O(g(x))$, previous slide.
- Show $g(x)$ is $O(f(x))$. Let $C = 1, k = 1$.

$x \geq 1 \rightarrow x^2 + x \geq x^2 \rightarrow x^2 + x + 1 \geq x^2$. 
Intractable Problems

- Show $f(x) = x^2$ is $O(g(x) = 2^x)$. Let $C = 1, k = 4$
- $x \geq 4 \rightarrow x \geq 2 \log(x) \rightarrow x \geq \log(x^2) \rightarrow \log(2^x) \geq \log(x^2) \rightarrow 2^x \geq x^2$
- Show $g(x) = 2^x$ is NOT $O(f(x) = x^2)$. Assume not.
- $\exists C, k$ such that $Cx^2 \geq 2^x, \forall x \geq k$
- Therefore, $\log(Cx^2) \geq \log(2^x), \forall x \geq k$
- Let $a = \log(C)$. Therefore, $a + 2 \log(x) \geq x, \forall x \geq k$
- Note that $\forall a \exists x$ s.t. $x > a + 2 \log(x)$. Consider $\max(x = 2^a, 16)$. Then $2^a > 3a$, which is true for $a \geq 4$.
- Therefore, problems requiring exponential time are “harder” than quadratic problems (or any polynomial)
- Such problems are called **intractable**
P=NP?

- P - class of problems solvable in polynomial time
- NP - class of problems best solutions require exponential time
- Unknown if NP problems can be solved in polynomial time
- One of grand challenges of mathematics for 21st century (Millennium Problems)
- Example: Satisfiability
  - Predicate $P$ in CNF $(p \lor q \lor r) \land (\neg p \lor s \lor \neg t)\ldots$
  - Can assign truth values to variables such that $P$ can be satisfied?
  - DNF is trivial $(p \land q \land r) \lor (\neg p \land s \land \neg t)\ldots$
Section 12

Basic Counting
Overview

- Needs to be added for Spring 2019
Section 13

Permutations and Combinations
Overview

- Permutations are the number of arrangements of a set of items of a specific size
- Combinations are the number of subsets of a specific size
- The Binomial Theorem is a general representation of binomial coefficients
- Playing cards
  - 4 suits - spades, hearts, diamonds, clubs
  - 13 values - A,K,Q,J,10,9,8,7,6,5,4,3,2
  - 52 total cards (+ jokers)
Permutations

- **Battle** - Card game where highest value wins (special rules for ties)
- **Demonstration (Hearts only)**
  - How many ways to arrange 6 cards? (Hint: Product rule.)
  - How many ways to arrange 3 of 6 cards?
  - How many ways to arrange k of 6 cards?
  - How many ways to arrange k of n cards?
Permutation Formulae

- All arrangements: \( n(n - 1)(n - 2) \ldots (1) = n! \)
- Arrangements of size \( r \): \( n(n - 1)(n - 2) \ldots n - (r - 1) \)
  - Last term is also \( n - r + 1 \)
  - \( (n - r)! = (n - r)(n - r - 1)(n - r - 2) \ldots (1) \)
  - \( \frac{n!}{(n-r)!} \) yields arrangements of size \( r \)
- Formula: \( P(n, r) = \frac{n!}{(n-r)!} \)
- Note: if \( n = r \) then \( P(n, n) \) or \( P(n) = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n! \)
Combinations

- Oh Heck - Card game with hands and “tricks”
- Demonstration (Hearts only)
  - Order of cards in hand does not matter
  - How many different hands of size 3 can be dealt?
  - Given my hand, how many different hands of size 3 can opponent have?
  - Given my hand, how many different hands of size 3 can opponent have with all cards lower than my highest?
Combination Formulae

- Number of permutations divided by the number that are the same (division rule)

\[ P(n, r) / P(r) = \frac{n!}{(n-r)!} = \frac{n!}{r!(n-r)!} \]

- Number of subsets of set \( S \) a given size
  - Size 0 is \( \emptyset \), only one \( \frac{n!}{0!(n-0)!} = 1 \)
  - Size \( n \) is \( S \), only one \( \frac{n!}{n!(n-n)!} = 1 \)
  - Size 1 subsets, each element is \( |S| \), \( \frac{n!}{1!(n-1)!} = n \)
  - Size \( n-1 \) subsets, \( S \) with each element removed, number is \( |S| \), \( \frac{n!}{(n-1)!(n-(n-1))!} = n \)

- Formula: \( C(n, r) \) or \( \binom{n}{r} = \frac{n!}{r!(n-r)!} \)

- Note: \( \binom{n}{n} = \frac{n!}{n!0!} = 1 \) and \( \binom{n}{0} = \frac{n!}{n!0!} = 1 \)
Binomial Theorem

\[(x + y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \ldots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n\]

- Can find coefficient for any term in binomial expansion
  - Given \((2x + 3y)^4\), what is the coefficient for the \(x^2y^2\) term?
  - \(\binom{4}{2}(2x)^2(3y)^2 = 6 \times 4 \times 9 = 216\)
  - Shows \(\sum_{k=0}^{n} \binom{n}{k} = 2^n\) (from text)
  - \(2^n = (1 + 1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^{n} \binom{n}{k}\)
Pascal’s Triangle

- Example on board
- Pascal’s Identity: \( \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \)
- Algebraic proof:
  \[
  \binom{n+1}{k} = \frac{(n+1)!}{k!(n+1-k)!} \\
  \binom{n}{k-1} = \frac{n!}{(k-1)!(n-(k-1))!} \\
  \frac{k*n!}{k!(n-k)!} \\
  \binom{n}{k} = \frac{n!}{k!(n-k)!} \\
  \frac{(n+1-k)n!}{k!(n-k)!(n+1-k)!} = \frac{(n+1-k)n!}{k!(n+1-k)!} \\
  \binom{n}{k-1} + \binom{n}{k} = \frac{k*n!}{k!(k-1)!(n+1-k)!} + \frac{(n+1-k)n!}{k!(n+1-k)!} \\
  \frac{k*n! + (n+1-k)n!}{k!(n+1-k)!} = \frac{n!(k+n-k+1)}{k!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!}
  \]
Section 14

Probability
Finite Probability

Let $S$ be a set of equally likely outcomes – sample space.

Let $E \subseteq S$ be a set of desired outcomes – event.

$p(E) = \frac{|E|}{|S|}$ – probability of $E$

Examples (sample space is deck of cards):

- Probability of drawing a heart $p(\text{heart}) = \frac{13}{52} = \frac{1}{4}$
- Probability of drawing a king $p(\text{king}) = \frac{4}{52} = \frac{1}{13}$
- Probability of drawing king of hearts $p(\text{Kheart}) = \frac{1}{52}$
- Probability of drawing two hearts in a row (replacing your card) $p(\text{2hearts}) = \frac{169}{2704}$
  - Why? Two draws makes total outcomes is $52 \times 52$.
  - 13 successes in each draw means 169 successful outcomes (product rule).

- Probability of drawing 5 hearts in a row (without replacement)
  \[ p(\text{flush}) = \frac{13 \times 12 \times 11 \times 10 \times 9}{52 \times 51 \times 50 \times 49 \times 48} \]
Complements and Unions

- The complement of \( E \) is \( \overline{E} \) is \( S - E \). \( p(\overline{E}) = 1 - p(E) \)
- Probability of not drawing a heart \( p(\overline{\text{heart}}) = 1 - 1/4 = 3/4 \)
- Sometimes much easier to calculate the complement
- The union of two events is \( E_1 \cup E_2 \).
  \[ p(E_1 \cup E_2) = p(E_1) + P(E_2) - P(E_1 \cap E_2) \]
- \( p(\text{kingorheart}) = p(\text{king}) + p(\text{heart}) - p(\text{Kheart}) = 1/13 + 1/4 - 1/52 = 16/52 \)
Let $S$ be a sample space

- Each element in $S$ is assigned a probability $(p(s))$.
- $0 \leq p(s) \leq 1$
- $\sum_{s \in S} p(s) = 1$

Function from $S$ to set of probabilities is called probability distribution function

- If all probabilities are the same, uniform distribution
  \[ |S| = n, \forall s \in S, p(s) = 1/n \]
- $p(E) = \sum_{s \in E} p(s)$
Conditional Probability

- Probability of event $E$ given that event $F$ has happened
  \[ p(E|F) \]
- \[ p(E|F) = \frac{p(E \cap F)}{p(F)} \]
- Example:
  - Given that 4 hearts in a row have been drawn, what is the probability that a 5th heart will be drawn?
  - \[ p(F) = p(4\text{hearts}) = \frac{13 \times 12 \times 11 \times 10}{52 \times 51 \times 50 \times 49} \]
  - In this case, \[ p(E \cap F) = p(E) = p(\text{flush}) = \frac{13 \times 12 \times 11 \times 10 \times 9}{52 \times 51 \times 50 \times 49 \times 48} \]
  - \[ p(E|F) = \frac{9}{48} \]
Independence

- Two events are independent if one happening has no effect on the other happening

- Examples:
  - I draw a 7 from a deck of cards and you draw a 10 from a different deck.
  - I wear a hat and President Livingstone wears a hat.
  - We have an exam in 2350 and Dr. Donahoo gives an exam in 4321.

- \( E \) and \( F \) are independent iff \( p(E) \times p(F) = p(E \cap F) \)

- Different decks:
  \( p(7) = \frac{1}{13}, p(10) = \frac{1}{13}, p(7 \wedge 10) = \frac{1}{169} \approx 0.0060 \)

- Same decks: \( p(7) = \frac{1}{13}, p(10) = \frac{1}{13}, p(7 \wedge 10) = \frac{1}{13} \times \frac{4}{51} = \frac{4}{663} \approx 0.0059 \)
Bernoulli Trials

- Probability of $k$ successes of $n$ independent trials with success $p$ and failure $q = 1 - p$ is $\binom{n}{k} p^k q^{n-k}$

- Examples (replacing cards back in deck)
  - Probability of drawing 4 hearts out of 5 cards
    - $n = 5, k = 4, p = .25, q = .75, p(4H) = \binom{5}{4} .25^4 .75 \approx .0146$
  - Probability of drawing at least 4 hearts out of 5 cards
    - $p(4H) + p(5H) = \binom{5}{4} .25^4 .75 + \binom{5}{5} .25^5 .75^0 = 0.015625$
  - Probability of drawing at least 2 hearts out of 5 cards
    - $1 - (p(0H) + p(1H)) = 1 - \binom{5}{0} .25^0 .75^5 + \binom{5}{1} .25^1 .75^4 \approx 0.367$
Random Variable

- Not random and not a variable
- Function from $S$ to $\mathbb{R}$ (assigns real number to each possible outcome)
- Example: (Replacing cards as before)
  - Draw 3 cards from a deck. The set of all possible outcomes is $S$.
  - Let $X(s)$ be the random variable of the number of times a heart is drawn, where $s \in S$
  - Quick demo
    - $\forall s \in S$, $0 \leq X(s) \leq 3$
  - Distribution of $X$ on $S$ is the set of pairs $(r, p(X = r))$ where $r \in X(s)$
  - From example:
    - $(0, 0.421875), (1, 0.421875), (2, 0.140625), (3, 0.015625)$
Section 15

Expected Value and Variance
Expected Value

- Given a random variable $X$, the *expected value* of $X$ is
- $E(X) = \sum_{s \in S} p(s)X(s)$
- Recall $X(s) = y$ means $y$ is the number of interesting occurrences in event $s$
- Examples:
  - Assume cards 2-10 of hearts. Let $X$ be the value of the card. Expected value of drawing a card:
    $1/9 \times 2 + 1/9 \times 3 + 1/9 \times 4 + 1/9 \times 5 + 1/9 \times 6 + 1/9 \times 7 + 1/9 \times 8 + 1/9 \times 9 + 1/9 \times 10 = 6$
  - Assume J,Q,K have value 10 and A has value 11. Expected value of a card:
    $E(X) = 1/13 \times (\sum_{k=2}^{9} k + 11) + 4/13 \times 10 = 95/13$
  - Assume 5 cards, consisting of 4 2s and 1 3.
    $E(X) = .8 \times 2 + .2 \times 3 = 2.2$
The expected number of success of $n$ Bernoulli trials with success $p$ is $n \times p$.

Proof: (from text)

Let $X(s)$ be the number of successes out of $n$ trials.

$p(X = k) = \binom{n}{k} p^k q^{n-k}$

$E(X) = \sum_{k=1}^{n} k \times \binom{n}{k} p^k q^{n-k} \quad \text{Note: } k = 0 \text{ adds } 0 \text{ to } E(X)$

$= \sum_{k=1}^{n} n \binom{n-1}{k-1} p^k q^{n-k}$

$= np \times \sum_{k=1}^{n} \binom{n-1}{k-1} p^{k-1} q^{n-k}$

$= np \times \sum_{j=0}^{n-1} \binom{n-1}{j} p^j q^{n-1-j} \quad \text{(by shifting index)}$

$= np \times (p + q)^n - 1 \quad \text{(by binomial theorem)}$

$= np \quad \text{(by } p + q = 1)$
Linearity

- Expected value of sum of random variables is sum of expected values
- \( E(X_1 + X_2 + \ldots + X_n) = E(X_1) + E(X_2) + \ldots + E(X_n) \)
- \( E(aX + b) = a \cdot E(X) + b \)
- Examples:
  - Sum of two cards (with replacement) is \( 14 \frac{8}{13} \)
  - Sum of two die rolls is \( 2 \cdot E(X) \) where \( E(X) = \frac{1}{6} \cdot \sum_{k=1}^{6} k = \frac{21}{6} \) or 7
Complex Example - Expected number of inversions in a polynomial

- A permutation $P$ of integers $1 \ldots n$ is an arrangement of the numbers
- An inversion is where $i < j$ but $j \prec i$ in $P$
- Example: $P = (1, 3, 5, 2, 4)$ the inversions are $(2, 3), (2, 5), (4, 5)$
- Let $l_{i,j}$ be the random variable on the set of all permutations of the first $n$ integers with $l_{i,j} = 1$ if $(i, j)$ is an inversion on the permutation
- For the example, $l_{2,3}(P) = 1, l_{1,4} = 0$
- Let $X$ be the random variable equal to the number of inversions, $X = \Sigma_{1 \leq i < j \leq n} l_{i,j}$
- For example, $X(P) = 3$
- $E(l_{i,j}) = 1 \times p(l_{i,j} = 1) + 0 \times p(l_{i,j} = 0) = 1/2$ (equally likely inversion as not)
- There are $\binom{n}{2}$ ways for 2 numbers to be arranged out of $n$
- $E(X) = \binom{n}{2} E(l_{i,j}) = \frac{n!}{(n-2)!2*2} = \frac{n*(n-1)}{4}$
Average Case Complexity

- $S$ is the possible inputs to the program
- $X : S \rightarrow \mathbb{R}$, such that $\forall s \in S, X(s)$ is the number of operations performed
- Let $p(s)$ be the probability of $s$ being the input to the program
- $\sum_{s \in S} p(s)X(s)$ is the expected (or average) number of operations
Average Complexity Linear Search (text)

- Let $p$ be the probability $x \in A$. Assume $x$ is equally likely to be in any other location
- Counting number of comparisons
- For each element, check to see if at end of array and compare value (2 comparisons per element)
- After loop, one comparison to see if past end of array
- Probability $x$ is at element $k$ is $p/n$
- Probability $x$ is not in list is $q = 1 - p$
- If $x \in A$, then $\Sigma_{k=1}^{n} \frac{p}{n} (2 \times k + 1) =$
  $$\frac{p}{n} \times \Sigma_{k=1}^{n} (2k + 1) = \frac{p}{n} \times (n + 2 \times \Sigma_{k=1}^{n} k)$$
  $$= \frac{p}{n} \times (n + 2 \times \frac{n(n+1)}{2}) = \frac{p}{n} \times (n + n(n+1)) = p \times (1 + n + 1) = p(n+2)$$
- If $x \not\in A$, then $(2n + 2)q$
- $E(X) = p(n + 2) + (2n + 2)q$
**Variance**

- Let $X$ by a random variable on $S$
- Variance on $X$ (denoted $V(X)$) indicates the spread of values in $X(S)$
- $V(X) = \sum_{s \in S} (X(s) - E(X))^2 p(s)$
- Standard deviation $\sigma(X) = \sqrt{V(X)}$
- Example:
  - Blackjack cards: $V(X) = \sum_{s \in S} (X(s) - 7 \cdot \frac{4}{13})^2 \cdot p(s) = $
  - $(-5 \cdot \frac{4}{13})^2 \cdot 1/13 + (-4 \cdot \frac{4}{13})^2 \cdot 1/13 + \ldots + (2 \cdot \frac{9}{13})^2 \cdot 4/13 + (3 \cdot \frac{9}{13})^2 \cdot 1/13$
  - $\approx 8.5$
  - $\sigma(X) \approx 2.9$
Variance Continued

- \( V(X) = E(X^2) - E(X)^2 \)
- **Example:**
  - Blackjack cards: \( E(X)^2 = (7 \frac{4}{13})^2 \approx 53.4 \)
  - \( E(X^2) = 1/13 \ast (\sum_{k=2}^{9} k^2 + 121) + 4/13 \ast 100 = \frac{784}{13} \approx 61.9 \)
  - \( \approx 8.5 \)
  - \( \sigma(X) \approx 2.9 \)
- Let \( E(X) = \mu \). Then \( V(X) = E((X - \mu)^2) \)
  - \( = 1/13 \ast (\sum_{k=2}^{9} (k - 7 \frac{4}{13})^2 + (11 - 7 \frac{4}{13})^2) + 4/13(10 - 7 \frac{4}{13})^2 = 8.5 \)
- Let \( X \) be a random variable such that \( X(t) = 1 \) if a Bernoulli trial is successful and \( X(t) = 0 \) otherwise.
- **Note:** Single trial, so \( n = 1 \) for Bernoulli distribution.
  - \( E(X) = p \ast 1 + q \ast 0 = p \). \( E(X^2) = p \ast 1^2 + q \ast 0^2 = p \).
  - \( E(X)^2 = p^2 \). \( V(X) = p - p^2 = p(1 - p) = pq. \)
Variance Equations

- Bienayme’s Formula
- If $X$ and $Y$ are independent random variables on $S$, then $V(X + Y) = V(X) + V(Y)$
- Chebyshev’s Inequality
- If $X$ is a random variable on $S$ with probability function $p$, then $p(|X(s) - E(X)| \geq r) \leq V(X)/(r^2)$
- Example:
  - Probability draw a card 3 or more from the mean of blackjack cards
  - $V(X)/r^2 \approx 8.5/9 \approx 0.94$
  - Actual is 2, 3, 4, $A = 4/13$
Section 16

Recurrence Relations
Definitions

- A recurrence relation is an equation that expresses $a_n$ in terms of one of more of the previous terms.
- A sequence is a solution to a recurrence relation if its terms satisfy the equations.
- Examples:
  - Recurrence Relation: $a_n = a_{n-1} + 3, a_0 = 2$. Solution: $[2, 5, 8, \ldots]$
  - Fibonacci: $a_n = a_{n-1} + a_{n-2}, a_0 = 1, a_1 = 1$. Solution: $[0, 1, 1, 2, 3, 5, \ldots]$
- A closed form solution is an equation for each term that does not reference other terms.
Linear Homogeneous Recurrence Relation

Definition

- A *linear homogeneous recurrence relation of degree k with constant coefficients* is a recurrence relation of the form:
  \[ a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} \]
  such that every \( c_i \in \mathbb{R} \) and \( c_k \neq 0 \).
- Linear because each right-hand side term is sum of previous terms
- Homogeneous because no terms occur that are not multiples of previous terms
- Constant coefficients means no \( c_i \) can reference \( n \) (but note that 0 is allowed for all but last coefficient)
- The degree is determined by the number of terms required
Linear Homogeneous Recurrence Relation

- **Examples**
  - \(a_n = \frac{3a_{n-1}}{2}\) is l.h.r.r. of degree 1
  - Fibonacci is l.h.r.r of degree 2
  - \(a_n = 2 \times a_{n-5}\) is l.h.r.r of degree 5 (4 terms with 0 as coefficient)
  - \(a_n = a_{n-1} + 3\) is not l.h.r.r because 3 is not multiple of previous term
  - \(a_n = 2^n a_{n-1}\) is not l.h.r.r because \(2^n\) is not constant coefficient
  - \(a_n = a_{n-1}^2\) is not l.h.r.r because squared term is not linear
Solving L.H.R.R. of degree 2

- Find closed form equation (of the form $a_n = r^n$).
- $r^n = c_1 r^{n-1} + c_2 r^{n-2} + \ldots + c_k r^{n-k}$
- $r^k = c_1 r^{k-1} + c_2 r^{k-2} + \ldots + c_k$ – divide both sides by $r^{n-k}$
- $r^k - c_1 r^{k-1} - c_2 r^{k-2} - \ldots - c_k = 0$ – is the characteristic equation
- Solutions to the characteristic equation are the characteristic roots
- Assuming degree=2 and distinct roots $r_0$ and $r_1$, $a_n = \alpha_1 r_0^n + \alpha_2 r_1^n$
- Use initial terms to solve for $\alpha_1$ and $\alpha_2$
Solving L.H.R.R.

- \( a_n = 5a_{n-1} - 6a_{n-2}, a_0 = 1, a_1 = 0 \)
- \( r^n = 5r^{n-1} - 6r^{n-2} \rightarrow r^2 = 5r - 6 \rightarrow r^2 - 5r + 6 = 0 \)
- Characteristic Roots are 3, 2
- \( a_n = \alpha_1 3^n + \alpha_2 2^n \)
- \( 1 = \alpha_1 + \alpha_2 \rightarrow 1 - \alpha_1 = \alpha_2 \)
- \( 0 = \alpha_1 \ast 3 + \alpha_2 \ast 2 \rightarrow 0 = \alpha_1 \ast 3 + (1 - \alpha_1) \ast 2 \rightarrow \alpha_1 = -2 \rightarrow \alpha_2 = 3. \)
- \( a_n = -2(3^n) + 3(2^n) \)
- Check: Sequence solution is \([1, 0, -6, -30, \ldots]\)
- \( a_3 = -2(3^3) + 3(2^3) = -54 + 24 = -30 \)
Fibonacci: $a_n = a_{n-1} + a_{n-2}, a_0 = 0, a_1 = 1$

$r^2 = 1r^1 + 1r^0$

$r^2 - r^1 - 1 = 0$

Quadratic Equation: $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$

$a = 1, b = -1, c = -1, \frac{1+\sqrt{1+4}}{2}, \frac{1-\sqrt{1+4}}{2}$

$a_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$

Use $a_0$ and $a_1$ to determine values for alpha
Solving L.H.R.R. continued

- $0 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^0 + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^0 = \alpha_1 + \alpha_2$
- Therefore, $-\alpha_1 = \alpha_2$
- $1 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^1 + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^1$
- Substituting: $1 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^1 - \alpha_1 \left(\frac{1-\sqrt{5}}{2}\right)^1$
- $1 = \alpha_1 \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = \alpha_1 \frac{1+\sqrt{5}-1+\sqrt{5}}{2} = \alpha_1 \sqrt{5}$
- $\alpha_1 = \frac{1}{\sqrt{5}}, \alpha_2 = -\frac{1}{\sqrt{5}}$
- $a_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n + -\frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n$
- Test cases:
  - $\text{fib(0)} = 0. \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^0 + -\frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^0 = \frac{1}{\sqrt{5}} - \frac{1}{\sqrt{5}} = 0$
  - $\text{fib(5)} = 5. \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^5 + -\frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^5 \approx 4.96 - -(0.04) = 5$
  - $\text{fib(18)} = 2584. \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^{18} + -\frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^{18} \approx 2584.00007 - (7 \times 10^{-5} = 2584)$
Let $r^2 - c_1 r^1 - c_2 r^0$ have only one real root $x$.

Closed form solution for $a_n = \alpha_1 x^n + \alpha_2 n \times x^n$

Example: $a_n = 4a_{n-1} - 4a_{n-2}$, $a_0 = 6$, $a_1 = 8$

$r^2 = 4r - 4 \rightarrow r^2 - 4r + 4 = 0$

$\frac{4 \pm \sqrt{16 - 4 \times 1 \times 4}}{2} = \frac{4}{2} = 2$

$a_n = \alpha_1 2^n + \alpha_2 n \times 2^n$

$a_0 = \alpha_1 2^0 + \alpha_2 0 \times 2^0 \rightarrow 6 = \alpha_1$

$a_1 = \alpha_1 2^1 + \alpha_2 1 \times 2^1 \rightarrow 8 = 6 \times 2 + \alpha_2 \times 2 \rightarrow -2 = \alpha_2$

$a_n = 6(2^n) - 2n(2^n)$

Check: $[6, 8, 8, 0, -32, \ldots]$

$a_4 = 6 \times 16 - 8 \times 16 = 96 - 128 = -32$
Section 17

Relations
Definitions of Relations

- A *relation* between sets $A$ and $B$ is a subset of $A \times B$
- Typically, a relation defines a connection between elements of the set
- Example 1: $A = \{ \text{students in class} \}, \ B = \{ \text{side of room} \}, \ R(a, b) \leftrightarrow a \text{ sits on } b \text{ side of the room. (on board)}$
- Example 2: $A = \{ \text{volunteers} \}, \ B = \{ \text{food} \}, \ R(a, b) \rightarrow a \text{ likes } b. \text{(on board)}$
- Functions are relations restricted such that elements from $A$ appear only once (Example 1)
- Graphs can show relations
- Relations can be on one set $A = \{ \text{food} \}, \ B = \{ \text{food} \}, \ R(a, b) \leftrightarrow a \text{ is the same color as } b \text{ (on board). Usually written as } R(a, a)$
Consider relations on $\mathbb{Z} \times \mathbb{Z}$

- **Reflexive**: $\forall a \in A, R(a, a)$
  - $R(z_0, z_1) \iff z_0 \leq z_1$ is reflexive
  - $R(z_0, z_1) \iff z_0 < z_1$ is NOT reflexive

- **Symmetric**: $\forall a \in A, \forall b \in B, R(a, b) \rightarrow R(b, a)$
  - $R(z_0, z_1) \iff z_0 \leq z_1$ is NOT symmetric
  - $R(z_0, z_1) \iff z_0 = z_1$ is symmetric (and reflexive)
  - $R(z_0, z_1) \iff z_0$ and $z_1$ are relatively prime is symmetric (and not reflexive)

- **Antisymmetric** (poorly named):
  $\forall a \in A, \forall b \in B, R(a, b) \land R(b, a) \rightarrow a = b$
  - $R(z_0, z_1) \iff z_0 \leq z_1$ is antisymmetric
  - $R(z_0, z_1) \iff z_0 = z_1$ is antisymmetric
  - $R(z_0, z_1) \iff z_0$ and $z_1$ are relatively prime is NOT antisymmetric
Properties of Relations

- **Transitive**: \( R(a, b) \land R(b, c) \rightarrow R(a, c) \)
  - \( R(z_0, z_1) \leftrightarrow z_0 \leq z_1 \) is transitive
  - \( R(z_0, z_1) \leftrightarrow z_0 = z_1 \) is transitive
  - \( R(z_0, z_1) \leftrightarrow z_0 \) and \( z_1 \) are relatively prime is NOT transitive
Sets and Relations

- Relations are sets of ordered pairs. Therefore, all set operations apply.

- \( R(z_0, z_1) \iff z_0 \leq z_1 - R(z_0, z_1) \iff z_0 < z_1 = R(z_0, z_1) \iff z_0 = z_1 \)

- Proof:
  - Let \( LEQ = R(z_0, z_1) \iff z_0 \leq z_1, LT = R(z_0, z_1) \iff z_0 < z_1 \) and \( EQ = R(z_0, z_1) \iff z_0 = z_1 \).
  - Let \((a, b) \in LEQ - LT\). Therefore, \((a, b) \in LEQ\) and \((a, b) \notin LT\).
  - Therefore, \( a \leq b \) and \( a \geq b \) (not less than).
  - Therefore, \( a = b \) and \( EQ(a, b) \). Reverse direction is similar.

- Let \( A = \{1, 2, 3\} \). Let \( R(a, a) = \{(1, 1), (2, 2), (1, 2)\}\) and \( S(a, a) = \{(1, 1), (2, 2), (2, 1)\}\).

  - \( R \cup S = \{(1, 1), (2, 2), (1, 2), (2, 1)\}\)
  - \( R \cap S = \{(1, 1), (2, 2)\}\)
  - \( R \oplus S = \{(1, 2), (2, 1)\}\)
N-ary Relations

- Text is awkward with notation
- Extend notion to n-wise cross product.
- Given sets $S_0, S_1, \ldots S_{n-1}$, $R \subseteq S_0 \times S_1 \times \ldots \times S_{n-1}$
- $r \in R$ is a n-tuple. Note that the ordering is important.
- Relational databases (Oracle, MySQL, SQLServer, etc.) use tables as relations with attributes representing sets
- Example: Students(Id, Name, Major, Favorite Number)
- Collection of attributes is the schema
- Note: Databases allow duplicate elements – database tables are bags of n-tuples
- Id is primary key uniquely identifies row in table
Basic Relational Algebra

- Let $R(A, B, C) = \{(1, 2, 3), (2, 3, 4)\}$ and $S(C, D, E) = \{(3, 4, 5), (3, 2, 1)\}$
- $\sigma_P R$ (selection) creates new table with same schema as $R$. A row is in $\sigma_P R$ if it is in $R$ and it satisfies predicate $P$
- $\sigma_{A=1} R = \{(1, 2, 3)\}$
- $\Pi_{A,B} R$ (projection) creates new table with columns $A$ and $B$. There is a 1-1 mapping from each row in $R$ to each row in $\Pi_{A,B} R$
- $\Pi_{B,C} R = \{(2, 3), (3, 4)\}$
- $R \bowtie S$ (natural join) creates new table with union of columns in $R$ and in $S$. A row is in $R \bowtie S$ if $\exists r \in R \land s \in S$ such that $r[R \cap S] = s[R \cap S]$.
- $R \bowtie S = \{ (1, 2, 3, 4, 5), (1, 2, 3, 2, 1) \}$
- Note: Results of relational algebra operators are relations. Operations can be composed.
- $\Pi_{A,E}(\sigma_{B=D}( R \bowtie S)) = \{ (1, 1) \}$
 Queries

- Example queries using relational algebra
- To be added Spring 2019
Section 18

Relations, Matrices and Digraphs
Matrices and Relations

- Matrix representation of $R(a, a)$ (can be any relation – see text)
- $M_R[i, j] = 1 \iff R(i, J)$. Otherwise, $M_R[i, j] = 0$.
- Matrix $M_R$ is the representation of $R = \{(1, 1), (1, 2), (2, 1), (3, 3)\}$
- Matrix $M_S$ is the representation of $S = \{(2, 2), (2, 3), (3, 2), (3, 3)\}$
- Matrix diagonal all 1's implies relation is reflexive
- $M = M^t$ implies relation is symmetric

\[
M_R = \begin{bmatrix}
1 & 1 & 0 \\
1 & 0 & 0 \\
0 & 0 & 1
\end{bmatrix}
\quad
M_S = \begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 1 \\
0 & 1 & 1
\end{bmatrix}
\]
Matrix Operations and Relational Operations

- $A \lor B$ is the *join* of matrices $A$ and $B$ – logical OR of corresponding elements
- $A \land B$ is the *meet* of matrices $A$ and $B$ – logical AND of corresponding elements
- $A \circ B$ is the *Boolean product* of matrices $A$ and $B$ – $C = A \circ B \rightarrow c_{ij} = (a_{i1} \land b_{1j}) \lor (a_{i2} \land b_{2j}) \lor \ldots \lor (a_{in} \land b_{nj})$ – see below (note similarity to matrix multiplication)
- $M_R \lor M_S = R \cup S$
- $M_S \land M_S = R \cap S$
- Boolean product is composition of relations
- $M_R \circ M_R = M_R \rightarrow R$ is transitive (but not “iff”)

\[
\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \circ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}
\]
Let $R$ be a relation on set $A$

$G_R = (A, E)$ where $E \subseteq A \times A$ such that $(a_i, a_j) \in E \iff R(a_i, a_j)$

Example on board for $R = \{(1, 1), (1, 2), (2, 3), (3, 1)\}$

Boolean product of $M_R \odot M_R$ contains edges two steps away

\[
\begin{bmatrix}
1 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{bmatrix}
\odot
\begin{bmatrix}
1 & 1 & 0 \\
0 & 0 & 1 \\
1 & 0 & 0
\end{bmatrix}
= \begin{bmatrix}
1 & 1 & 1 \\
1 & 0 & 0 \\
1 & 1 & 0
\end{bmatrix}
\]
Paths and Boolean Products

- $M^n_R[i, j] = 1$ (Boolean product of $M_R$ with itself $n$ times) iff $G_R$ contains a path of length $n$ from $a_i$ to $a_j$

- Proof (by induction):
  - WLOG, let $|A| = p$
  - Basis: By definition, $G_R$ contains an edge from $a_i$ to $a_j$ exactly when $M_R[i, j] = 1$
  - Inductive Hypothesis: If $M^k_R[i, j] = 1$, there exists a path of length $k$ from $a_i$ to $a_j$ in $G_R$.
  - Consider $M^{k+1}_R = M^k_R \odot M_R$. $M^{k+1}_R[i, j] = 1$ iff $\exists m, 1 \leq m \leq p$ such that $M^k_R[i, m] = 1$ and $M_R[m, j] = 1$.
  - By the IH, $M^k_R[i, m] = 1$ means there is a path of length $k$ from $a_i$ to $a_m$. Call this path $P$.
  - $M_R[m, j] = 1$ means there is an edge from $a_m$ to $a_j$.
  - The path $P'$ which follows $P$ for $k$ steps, then takes the edge from $a_m$ to $a_j$ is a path from $a_i$ to $a_j$ and is of length $k + 1$

- The completion of the proof (showing if there is a path of length $k$ in $G_R$ then $M^k_R[i, j] = 1$) is in the homework.
Let $|A| = n$.

\[ \bigvee_{k=1}^{n} M_{R}^{k} \text{ is the transitive closure of } R\]

Also called the connectivity relation $R^*$.

Given a graph $G = (A, E)$, we can define $R(a_i, a_j) \iff (a_i, a_j) \in E$ (e.g., derive relation from graph).

Note: If there is a path from $a_i$ to $a_j$ in $G$, then the shortest path cannot be longer than $|A|$.

Transitive closure is the set of all paths in $G$.
Equivalence Relations

- An equivalence relation is a relation that is reflexive, symmetric and transitive.
- If $R(A, A)$ is an equivalence relation, then $R(a_i, a_j)$ means $a_i \sim a_j$ (a_i and a_j are equivalent).
- Let $R(A, A)$ be an equivalence relation. The equivalence class of $a_i \in A$, $[a]_R = \{a_j | R(a_i, a_j)\}$.
- Note: $a_i \in [a_i]_R$, since $R$ is reflexive.
- Note: $\bigcup_{a \in A}[a]_R = A$
- Note: $a_j \notin [a_i]_R \rightarrow [a_j]_R \cap [a_i]_R = \emptyset$
- Note: $a_j \in [a_i]_R \rightarrow [a_j]_R = [a_i]_R$
- The equivalence classes of $R$ form a partition of $A$. 
Partial Orders

- $R(A, A)$ is a *partial order* on $A$ iff it is reflexive, antisymmetric and transitive.
- $(A, R)$ is a partially ordered set or a *poset*.
- Consider $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (1, 3), (2, 4)\}$ ($M_R$ is below).
- Arbitrary relation symbol is ≤, so $(A, \leq)$ is a poset with arbitrary relation.

$$M_R = \begin{bmatrix}
1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 \\
\end{bmatrix}$$
Poset Properties

- Not all elements are related – 2 and 3 from previous
- if $a \leq b$ holds a and b are comparable.
- if all elements in A are comparable, $(S, \preceq)$ is a total ordering.
- $\forall a_i \in A, a_j \npreceq a_i \rightarrow a_j$ is a maximal element (3 and 4 are maximal in example)
- $\forall a_i \in A, a_i \npreceq a_j \rightarrow a_j$ is a minimal element (1 is minimal in example)
- every poset has at least one minimal and one maximal element (can have more)
Section 19

Graphs
Terminology

- A graph $G = (V, E)$ where $V$ is a set of vertices (or nodes) and $E \subseteq V \times V$ is a set of edges.
- A graph can be directed
  - first vertex in an edge is the source
  - second vertex is the destination
  - connectivity is from source to destination
  - edges represented as arrows pointing at the destination
  - example on board
- A graph can be undirected
  - both vertices are incident on edge
  - connectivity is bidirectional
  - edges represented as lines between vertices
  - example on board
- A graph is simple if $E$ is a set and there are no self-loops.
Neighborhoods

- Vertex $v_i$ is adjacent to $v$ if there is an edge from $v$ to $v_i$
- Vertex $v_i$ is a *neighbor* of $v$ if it is adjacent to $v$
- Set of neighbors of $v$ are the *neighborhood* of $v$, denoted $N(v)$
- Directed graph definition: $N(v) = \{ v_i \in V | (v, v_i) \in E \}$
- Undirected graph definition: 
  $N(v) = \{ v_i \in V | (v, v_i) \in E \lor (v_i, v) \in E \}$
- Neighborhood can apply to $A \subset V. N(A) = \bigcup_{v \in A} N(v)$. 
- Example on board
Degree of a node

- The degree \( \text{deg}(v) \) of a node in an undirected graph is the number of times an edge connects to the node.

- \( \text{deg}(v) = |\{(v, v_i)|(v, v_i) \in E\}| + |\{(v_i, v)|(v_i, v) \in E\}| \)

- Example on board

- **Handshake Theorem**: Let \( G = (V, E) \) be an undirected graph. \( 2|E| = \sum_{v \in V} \text{deg}(v) \).

- **Proof by induction**
  - **Basis**: Let \( E = \emptyset \). Therefore, \( \forall v \in V, \text{deg}(v) = 0 \), so \( \sum_{v \in V} \text{deg}(v) = 0 = 2 \times |E| \)
  - **Inductive Hypothesis**: Let \( G = (V, E) \) be a graph with \( k \) edges. Therefore, \( 2|E| = \sum_{v \in V} \text{deg}(v) \).
  - Let \( G' = (V', E') \) such that \( V' = V \) and \( E' = E \cup (v_i, v_j) \).
  - **Case 1**: \( (v_i, v_j) \in E \). Therefore, \( E = E' \) and by the inductive hypothesis, the theorem holds.
  - **Case 2**: \( (v_i, v_j) \notin E \). Therefore, \( |E'| = |E| + 1 \).
  - Note that, \( \text{deg}(v_i) \) and \( \text{deg}(v_j) \) both increase by one. Therefore, \( \sum_{v \in V'} \text{deg}(v) = \sum_{v \in V} \text{deg}(v) + 2 \).
  - Therefore, \( 2|E'| = 2|E| + 2 = \sum_{v \in V} \text{deg}(v) + 2 = \sum_{v \in V'} \text{deg}(v) \).
The \textit{indegree} \((\text{deg}^-(v))\) of a node \(v\) in a directed graph is the number of edges with \(v\) as the destination.

The \textit{outdegree} \((\text{deg}^+(v))\) of a node \(v\) in a directed graph is the number of edges with \(v\) as the source.

Example on board:

\[
\sum_{v \in V} \text{deg}^-(v) = \sum_{v \in V} \text{deg}^+(v) = |E|
\]
Special Graphs

Let $G = (V, E)$ be a simple graph. $G$ is a complete graph iff $\forall v_i, v_j \in V, v_j \in N(v_i)$.

Example on board.

Let $G = (V_1 \cup V_2, E)$ be a simple graph. $G$ is a bipartite graph iff $\forall (v_i, v_j) \in E, v_i \in V_1 \rightarrow v_j \in V_2 \land v_i \in V_2 \rightarrow v_j \in V_1$.

Example on board.

Let $G = (V_1 \cup V_2, E)$ be a simple graph. $G$ is a complete bipartite graph iff it is bipartite and every node in $V_1$ is connected to every node in $V_2$. 

Matchings

- A **matching** of a bipartite graph $G = (V_1 \cup V_2, E)$ is a subgraph $G' = (V_1 \cup V_2, E' \subseteq E)$ such that $\forall v \in V_1 \cup V_2, \deg(v) \leq 1$.

- A **maximum matching** is a matching with the largest number of edges.

- A **complete matching** is a matching from $V_1$ to $V_2$ such that all nodes in $V_1$ are incident on an edge ($|E'| = |V_1|$)

- **Hall’s Marriage Theorem**: A bipartite graph $G = (V_1 \cup V_2, E)$ has a complete matching iff $\forall A \in 2^{V_1}, |N(A)| \geq |A|$.
Section 20

Graphs, Paths and Circuits
Graph Isomorphism

- $G_1 = (V_1, E_1)$ is isomorphic to $G_2 = (V_2, E_2)$ iff there exists a bijective function $f : V_1 \to V_2$ such that $v_i \in N(v_j)$ in $G_1$ iff $f(v_i) \in N(f(v_j))$ in $G_2$.
- Example on board (isomorphic and not isomorphic)
- Properties which must hold under isomorphism
  - Number of vertices
  - Number of edges
  - Number of vertices with same degree
- $M_G$ is adjacency matrix of $G$
- Rearrange rows and columns of $M_{G_1}$ until $M_{G_1} = M_{G_2}$, then $G_1$ is isomorphic to $G_2$
- Example on board
Paths

- A *path* in a simple graph $G$ is a sequence $P = [x_0, x_1, \ldots, x_{n-1}]$ of vertices such that $x_{i+1} \in N(x_i)$.
- A *circuit* is a path such that $x_0 = x_{n-1}$.
- The length of $P$ is $n - 1$.
- Example on board (undirected and directed).
- A graph is *connected* if there is a path (in both directions) between every pair of distinct vertices.
- A *connected component* of $G$ is a subgraph $G'$ such that $G'$ is connected and there does not exists a connected subgraph $G''$ of $G$ such that $G'$ is a proper subgraph of $G''$.
- An *articulation point* is a vertex $v \in V$ such that the removal of $v$ would make $G$ no longer connected.
- A *bridge* is an edge $(v_i, v_j) \in E$ such that the removal of $(v_i, v_j)$ would make $G$ no longer connected.
- Example on board.
- Paths are preserved under isomorphism. Therefore, if $G_1$ has a circuit of length $k$ and $G_2$ does not, then $G_1$ and $G_2$ are not isomorphic.
Euler Circuits and Paths

- A multigraph $G$ contains multiple edges from two vertices (i.e., $E$ is not a set)
- A Euler circuit in $G$ is a simple circuit containing every edge in $G$
- A Euler path in $G$ is a simple path containing every edge in $G$
- Example on board
- Conditions for Euler circuits:
  - $G$ must be connected
  - Every vertex must have even degree
- Conditions for Euler path, but NOT Euler circuit
  - $G$ must be connected
  - Exactly two vertices with odd degree
- Excellent proofs in text
Hamilton Circuits and Paths

- A Hamilton circuit in $G$ is a simple circuit containing every vertex in $G$
- A Hamilton path in $G$ is a simple path containing every vertex in $G$
- Example on board
- No known simple criteria for Hamilton circuits or paths (necessary and sufficient)
- Sufficient criteria for circuit in simple, undirected graph $G = (V, E)$
  - $G$ is connected
  - $|V| \geq 3 \land \forall v \in V, \ deg(v) \geq n/2$ (Dirac’s Theorem)
  - $|V| \geq 3 \land \forall u, v \in V, u \notin N(v) \rightarrow \deg(u) + \deg(v) \geq n$ (Ore’s Theorem)
Section 21

Shortest Path and Trees
Shortest Path

- A weighted graph $G^+(V, E)$ where $E$ is a set of 3-tuples $(v_i, v_j, w)$ such that $w$ is the weight of the edge $(v_i, v_j)$
- Can be directed or undirected
- The matrix representation of $G^+$ uses weights as values (assuming simple graph with all weights positive)
- Example on board using matrix below
- The shortest path has the least sum of weights
- Example on board from 0 to 4

\[
M = \begin{bmatrix}
0 & 10 & 0 & 20 & 0 \\
12 & 12 & 12 & 12 & 12 \\
0 & 0 & 0 & 0 & 0 \\
20 & 12 & 0 & 0 & 10 \\
0 & 12 & 5 & 10 & 0 \\
\end{bmatrix}
\]
Dijkstra’s Algorithm

- Inputs: $G^+, v_i, v_j \in V$
- Output: Shortest path from $v_i$ to $v_j$ in $G^+$
- Keep list of shortest known paths from $v_i$ to all $v \in V$
- Initialize list so that all nodes have unknown path ($P$) with infinite length ($L$)
- Set $P(v_i)$ to $[v_i]$ and $L(v_i) = 0$
- While $v_j$ is unmarked
  - Let $v$ be the vertex with the shortest path so far (choose randomly for ties)
  - Mark $v$
  - For all unmarked $v_k \in N(v)$
    - Let $w$ be from the edge $(v, v_k, w)$
    - If $L(v) + w < L(v_k)$, then set $P(v_k) = P(v).v$ and $L(v_k) = L(v) + w$
- Example on board
A directed acyclic graph (DAG) is a directed graph $G = (V, E)$ such that in the transitive closure of $G$ $G^*_R = (V, E^*)$, $\forall v \in V, v \notin N(v)$.

Example on board
$G = (\{0, 1, 2, 3\}, \{(0, 1), (1, 2), (0, 2), (3, 0)\})$

The relation corresponding to a DAG $G$ is not reflexive but it is antisymmetric. It may or may not be transitive.
Trees

- A *tree* is an undirected graph with no simple cycles
- A *rooted tree* is a DAG such that:
  - The undirected form of the graph is a tree
  - A root is a node with no incoming edges
  - All edges are directed away from the root
- Any edge in tree can be selected as root (different roots yield different trees)
- A *leaf* is a node with no outgoing edges
- The *branching factor* of a tree is the maximum number of children for each node
- If \( m \) is the branching factor, than the tree is *\( m \)-ary*. If \( m = 2 \), the tree is binary
Tree Properties

- A tree with $n$ vertices has $n - 1$ edges.
- Inductive Proof (from text):
  - Basis: $n=1$. One node. No edges.
  - Inductive Hypothesis: Every tree with $k$ vertices has $k - 1$ edges
  - Let $T$ be a tree with $k + 1$ nodes. Let $v$ be a leaf in $T$.
  - Removing $v$ from $T$ generates a tree $T'$ with $k$ nodes ($T'$ has no simple circuits)
  - Therefore, $T'$ has $k - 1$ edges.
  - There can be only one edge from any node in $T'$ to $v$, otherwise a cycle would exist (can you prove why?)
- The **level** of a node is the length of the path from the root to the node
- The **height** of a tree is the maximum level of any node
- A tree of height $h$ is *balanced* if all leaves are at level $h$ or $h - 1$
- There are at most $m^h$ leaves in an $m$-ary tree of height $h$
Section 22

Tree Traversals and Heaps
Sparse Graphs

- Consider complete binary tree \( T \) of height \( k \)
- \( T \) has \( 2^k \) leaf nodes, \( 2^k - 1 \) non-leaf nodes and \( 2^{k+1} - 1 \) nodes total.
- Matrix representation \( 2^{k+1} - 1 \times 2^{k+1} - 1 \) with \( 2^{2k+2} - 2^{k+2} + 1 \) entries
- Each non-leaf node has 2 neighbors. All leaves have zero neighbors.
- Matrix has \( 2^{k+1} - 2 \) non-zero values and \( 2^{2k+2} - 3(2^{k+1}) + 3 \) zeros.
- Examples:
  - \( k = 3 \). Matrix has 225 entries. 14 are one. 211 are zero.
  - \( k = 10 \) Matrix has 4,190,290 entries. 4,188,163 are zero.
Alternative Representations

- **Adjacency List**
  - Array of values for each node (size $2^k$).
  - Root is index location 0
  - Each entry is array with list of neighbors – “in order” if applicable
  - Weights become array of ordered pairs (neighbor, weight)

- **Tree Data Structure**
  - **Node Object**
    - Value with node references (pointers) (size $2^k$)
    - References stored “in order” (if applicable)
    - Weights stored with references (ordered pair object)
    - Parent reference can be stored in object
  - Root object stored in known location (usually variable called “root”)
  - Leaf and non-leaf can be subclasses
Tree Traversals

- Recursive procedure for processing nodes
- Preorder traversal
  - Visit node first
  - Visit children in order
  - Return
- Add motivations
- Inorder traversal (more common in binary trees)
  - Visit first child
  - Visit node
  - Visit remaining children in order
  - Return
- Add motivations
- Postorder traversal
  - Visit children in order
  - Visit node
  - Return
- Add motivations
Depth First Search

- Values can be complex.
- Example: Game of tic-tac-toe (below)
- Spanning tree of graph (tree containing all nodes of graph)
- Algorithm
  - Visit children in order
  - Visit node
  - Return
- Example on board

```
  O
  X
  O X
  X
```
Breadth First Search

- Same applications
- Algorithm
  - Place root in queue
  - While queue not empty
    - Pop node N from queue
    - Visit N
    - Append children of N to queue
- Example on board

```
 O
 X  O  X
 X
```
Heap

- Tree structure (often binary)
- Parent always greater than or equal to children (max heap)
- Insertion:
  - Add new value to first available leaf
  - if child greater than parent, swap (continue until swap root)
- Example: 10,5,15,8,12,20,2
- Pop: (remove top element)
  - Move greater child into empty slot
  - continue until leaf moved
- Different insertion order can yield different heaps
- Example: 2,5,8,10,12,15,20