# Math 61: Introduction to Discrete Structures (23W)

Instructor: Kim-Tuan Do
Textbook: Richard Johnsonbaugh - Discrete Mathematics (8th Edition - 2017)
Topics: Sets, proofs, functions, relations & equivalence relations, counting (incl. permutations, combinations, Binomial Theorem), recurrence relations, graphs (incl. paths & cycles, isomorphisms), trees (incl. binary trees), number theory*

Table of Contents:

# Intro to Sets

1/9/23
Lecture 1

## Sets (§1.1)

A set is a fundamental mathematical concept, denoting a collection of objects (known as elements/members).

A set is denoted by the use of curly braces ({}), e.g. {1,2,3}

## Properties of Sets

(*) The order of elements in a set does not matter.
(*) A set is defined uniquely by the elements that it contains.
(*) Anything can be an element of a set, even other sets.
(*) Duplicate elements in a set are ignored.

A set can be described by: - listing all of its elements (e.g. {1,2,3})
- listing conditions for membership in the set, e.g. $\{x \mid x \text{ is an integer}\}$ is a set consisting of all items fulfilling the conditions (being an integer)

## Set Notation

$|X|$: cardinality of set X (number of distinct elements in [finite set] X)
$\alpha \in X$: $\alpha$ is an element of (belongs to) X; $\alpha \notin X$ is the converse
$X \subseteq Y$: X is a subset of Y (every element in X is also in Y)
(*) $X \subset Y$: X is a proper subset of Y ($X \subseteq Y$, but $X \neq Y$)
(*) $P(x)$: $P(x)$ (power set of X) is the set containing all subsets of X
$X = Y$: X and Y have the same elements; identical to ($X \subseteq Y$ && $Y \subseteq X$)

↳ Alt: "$\subset$" = "subset" "$\subsetneq$" = "proper subset"

Common Sets: $\emptyset = \{\}$ = empty set (set with no elements) → subset of all sets
$\mathbb{Z} = \{x \mid x \text{ is an integer}\}$ (set of all integers)
$\mathbb{Q} = \{x \mid x \text{ is a rational number}\}$ (set of all rational numbers) $= \{\frac{a}{b} \mid a, b \in \mathbb{Z}\}$
$\mathbb{R} = \{x \mid x \text{ is a real number}\}$ (set of all real numbers)

# Set Theory

1/10/23
Disc. 1

A set represents a collection of things (of any form)

The natural numbers (1, 2, 3, ...) can be redefined as the cardinality of various sets, e.g.: "2" := $|\{\text{thing 1}, \text{thing 2}\}|$
(:= "is defined as")

↳ Addition can also be redefined as the cardinality of the set obtained from the union of non-overlapping sets, e.g. "1+2" := $|\{\text{thing 1}\} \cup \{\text{thing 2}, \text{thing 3}\}|$
$= |\{\text{thing 1}, \text{thing 2}, \text{thing 3}\}| =$ "3"

Multiplication can be defined via associations through the <u>Cartesian product of sets</u> $(X \times Y)$, e.g.: given $X = \{a, b\}$, $Y = \{c, d\}$,
$X \times Y = \{(a, c), (a, d), (b, c), (b, d)\}$

↳ Integer multiplication: Given $m = |A|$ and $n = |B|$, $m \cdot n = |A \times B|$

Subtraction can be defined as the inverse of addition (and division as inv. of multiplication)
↳ Negative numbers can be defined with subtraction

# Set Operations & Intro to Proofs

1/11/23
Lecture 2

## Set Operations

Union $(X \cup Y)$: $\{a \mid a \in X \text{ or } a \in Y\}$
Intersection $(X \cap Y)$: $\{a \mid a \in X \text{ and } a \in Y\}$
* If $X \cap Y = \emptyset$, $X$ and $Y$ are disjoint (no overlap)
Difference $(X - Y)$: $\{a \mid a \in X \text{ and } a \notin Y\}$

* "U" denotes the universal set
  - Exact contents depend on context (e.g. if $X$ = all evens, $U$ = all integers)
* $U - X$ = complement of $X = \overline{X}$
  └ Also written $U \setminus X$

## Notation

- Given collection of sets $\{A_i\}$ $(\{A_i\}_{i=1}^n)$, $\bigcup A_i$ denotes the union of all sets $A_i$
  - $\bigcup A_i = \bigcup_{i=1} A_i = \{x \mid x \in A_i \text{ for some } i\} = (A_1 \cup A_2 \cup \dots \cup A_n)$
  - Similarly, $\bigcap A_i$ = intersection of all sets $A_i$
- Given set $X$ and $S = \{A_i \mid A_i \subseteq X\}$, $S$ is a partition of $X$ if $\bigcup A_i = X$, $A_i \cap A_j = \emptyset \ \forall i, j$
- Cartesian product of sets $X$ and $Y$ = $X \times Y = \{(a, b) \mid a \in X, b \in Y\}$
  - e.g. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}$ └ produces ordered pairs.

## Proofs (§2)

A proof is an argument establishing the truth of a mathematical statement.

A mathematical statement is usually composed of a hypothesis (P) leading to a conclusion (Q).

* A proof is usually ended with the symbols "$\square$" and "Q.E.D."

* Can also be written as $P \to Q$

## Types of Proof (Proving $P \to Q$) - §2.2, 2.4

1. Direct proof: Show directly that "P is true" implies "Q is true"
2. Proof by contradiction: To show $P \to Q$, assume P is true and Q is false, then prove that these assumptions lead to a contradiction (impossible statement)

# Methods of Proof

1/13/23
Lecture 3

## Types of Proof (cont.)

3) Proof by contrapositive: to show $P \to Q$, show the equivalent statement $!Q \to !P$

e.g. to show "$x$ = irrational" ($P$) $\to$ "$\sqrt{x}$ is irrational" ($Q$):

$\sqrt{x}$ = rational ($!Q$) $\to \sqrt{x} = \frac{a}{b}, a,b \in \mathbb{Z} \to x = \frac{a^2}{b^2} \to x$ = rational ($!P$)

4) Proof by cases: to show $P \to Q$, break $P$ down into smaller cases $P_1 \dots P_n$ and show $P_i \to Q \; \forall i$

e.g. to show $n(n+1)$ is even for all $n \in \mathbb{Z}$:

case 1: $n$ is even $\to n(n+1) = (2k)(2k+1), k \in \mathbb{Z} = 2(2k^2+k)$ = even

case 2: $n$ is odd $\to n(n+1) = (2k-1)(2k), k \in \mathbb{Z} = 2(2k^2-k)$ = even

5) Proving "if and only if" ("iff") statements: $P$ iff $Q = \{P \to Q, Q \to P\} = \{$only if, if$\}$

e.g. to show $n$ = even ($P$) iff $n^2$ = even ($Q$), $n \in \mathbb{Z}$:

$P \to Q$: $n = 2k \to n^2 = 4k^2 = 2(2k^2)$

$Q \to P$: $n = 2k+1$ ($!P$) $\to n^2 = 4k^2+4k+1$ ($!Q$), therefore $Q \to P$

7) Proof by induction: To prove $P(n)$ is true for all $n \geq n_0$, prove that $P(n_0)$ is true and that if $P(n)$ is true for some $n$, then $P(n+1)$ is also true

e.g. Given $P(n)$ = "sum of the first $n$ positive odd integers is equal to $n^2$":

Base case ($n=1$): $1 = 1^2$ (true)

Inductive step ($P(n) \to P(n+1)$): Assume $P(n)$ ($\sum_{j=1}^{n} 2j-1 = n^2$).

case $n+1 \to \sum_{j=1}^{n+1} 2j-1 = n^2 + 2n + 1 = (n+1)^2$ ($P(n)$ implies $P(n+1)$)

e.g. To show $4^n - 1 = 3m$, $m \in \mathbb{Z} \; \forall n \in \mathbb{Z}^+$: ($4^n - 1$ is a multiple of 3 for all $n \in \mathbb{Z}^+$)

Base case ($P(0)$, $n=0$): $4^0 - 1 = 3 = 3(1)$ = multiple of three

Inductive step: Assume $4^n - 1 = 3m$ for some $n$, $m$

$\to 4^{n+1} - 1 = 4(3m+1) - 1 = 12m + 3 = 3(4m+1)$ = multiple of 3

(*) Induction can also be proven for $n \geq n_0$ by proving the $n_0$ and $(n-1)$ cases instead of $n_0$ and $(n+1)$

# Functions

1/18/23
Lecture 4

| Functions (§3.1) | Notation |
| --- | --- |
| A function from set $X$ to set $Y$ ($f: X \to Y$) is an assignment of an element $y \in Y$ to an element $x \in X$ (i.e. $f(x) = y$). | $f: X$ (domain [of $f$]) $\to Y$ (codomain [of $f$])<br>Range [of $f$] - set of all possible values of $f(x)$, i.e $\{y \in Y \mid y = f(x) \text{ for some } x \in X\}$ |

(*) Given function $f: X \to Y$, $f$ represents a subset of Cartesian product $X \times Y$
- i.e $f = \{(x, f(x)) \mid x \in X, f(x) \in Y\} = \{(x,y) \mid x \in X, y \in Y, y = f(x)\} \subseteq \{(x,y) \mid x \in X, y \in Y\} = X \times Y$

## Definitions

- $f$ is injective/one-to-one if $(f(x_1) = f(x_2)) \to (x_1 = x_2)$
- $f$ is surjective/onto if $\forall y \in Y \; \exists x \in X$ s.t. $f(x) = y$
  - Equivalent statement: "codomain = range"
- $f$ is bijective if $f$ is both injective and surjective
  - If $f$ is bijective, $\exists f^{-1}: Y \to X$ s.t. given $y = f(x)$, $f^{-1}(y) = x \; \forall x, y$
  - If $f$ is bijective, it can be concluded that $|X| = |Y|$
- Given function $f: X \to Y$ and function $g: Y \to Z$, we define the composition of functions $f$ and $g$ $g \circ f: X \to Z$, such that $f(x) = y$, $g(y) = z$ implies $g(f(x)) = g \circ f(x) = z$

## Common Functions

Floor: for $x \in \mathbb{R}$, floor of $x = \lfloor x \rfloor$ = largest integer $n \in \mathbb{Z}$ s.t. $n \leq x$

Ceiling: for $x \in \mathbb{R}$, ceiling of $x = \lceil x \rceil$ = smallest integer $n \in \mathbb{Z}$ s.t. $n \geq x$

# Sequences & Strings

1/20/23
Lecture 5

## Sequences (§3.2)

A sequence is a function with domain $I \subseteq \mathbb{Z}$, such that sequence $s: I \to X$ for some $X$.

Given sequence $s$, the value $s(n)$, $n \in I$ can also be written $s_n$, where $n$ represents an index of the sequence.

(*) $I$ is typically either $\in \mathbb{Z}_{>0}$ or $\in \mathbb{Z}_{\geq 0}$

(*) Def: A finite sequence refers to a sequence $s: I \to Y$, where $I$ is a finite set ($|I| \neq \infty$)

(*) Def: A closed formula for a sequence $s$ is an expression of $s_n$ as a function of $n$.

- A subsequence of a sequence $s$ is a sequence formed by deleting terms of $s$
  - $\text{subseq.}(s): I_2 \to X$, $I_2 \subset I$
  - A subsequence can be described via indices of $s$: $\text{subseq}(s) = \{s_{n_k}\}_{k=1}$, where the term $s_{n_k}$ represents the $k^{th}$ index (of $s$) included in the subsequence ($s_{n_k} \in I \ \forall k$)

## Operations

Given terms $\{s_i\}_{i=n}^{m} = \{s_n, \dots, s_m\}$, we define:

1) Addition (Summation): $\sum_{i=n}^{m} s_i = s_n + s_{n+1} + \dots + s_m$

2) Multiplication: $\prod_{i=n}^{m} s_i = s_n \cdot s_{n+1} \cdots s_m$

## Definitions

- Increasing sequence: $s_{n+1} \geq s_n \ \forall n \in I$
  - Strictly increasing: $s_{n+1} > s_n$
- Decreasing sequence: $s_{n+1} \leq s_n \ \forall n \in I$
  - Strictly decreasing: $s_{n+1} < s_n$

## Strings

A string is any finite sequence of characters (of any type); a substring is a subsequence of a string, composed of only consecutive elements of the string.

## Definitions

(*) All characters $\in X \to$ string is over $X$

(*) $|\alpha|$ = length of $\alpha$

(*) If $|\alpha| = 0$, then $\alpha$ is null

(*) $\alpha + \beta$ = concatenation $\alpha\beta$ (of $\alpha$ and $\beta$)

# Relations

1/23/23
Lecture 6

## Relations (§3.3,4,5)

Given sets $X$ and $Y$, we define a relation $R$ from $X$ to $Y$ as a subset of the Cartesian product $X \times Y$ ($R \subseteq X \times Y$).

If $(x \in X, y \in Y) \in R$, we write $x$ is related to $y$ ($x R y$, $x \sim y$).

Examples

1) $X = \mathbb{R}$, $R \subseteq (X \times X)$, $a \sim b \rightarrow a = b$
   $\rightarrow R = \{(a,b) \mid a,b \in X, a = b\}$
2) $X = \mathbb{R}$, $R \subseteq (X \times X)$, $a \sim b \rightarrow a < b$
   $\rightarrow R = \{(a,b) \mid a,b \in X, a < b\}$

(*) The expression defining a relation can take (virtually any form

Definitions

Given set $X$, relation $R$ on $X$ ($R \subseteq X \times X$):

1) $R$ is reflexive if $x \sim x \ \forall x \in X$
2) $R$ is symmetric if $a \sim b \rightarrow b \sim a \ \forall a,b \in X$
3) $R$ is transitive if $a \sim b, b \sim c \rightarrow a \sim c \ \forall a,b \in X$

## Equivalence Relations

An equivalence relation on $X$ is any relation $R$ [on set $X$] that is reflexive, symmetric, and transitive

(*) Has similar properties to the operator "="

## Equivalence Classes

Given equivalence relation $R$ on $X$, we can define equivalence class $[a]$ of $X$ ($a \in X$):

$$[a] = \{b \mid b \in X, aRb\}$$

(*) All elements in $X$ are elements of exactly 1 equivalence class of $X$

# Functions Review

1/24/23
Disc 3

## Definitions

**Surjective** - every element in the codomain is mapped to by <u>at least</u> one element in the domain (codomain = range)

Implies: $|\text{codomain}| \leq |\text{domain}|$

**Injective** - every element in the codomain is mapped to by <u>at most</u> one element in the domain

Implies: $|\text{domain}| \leq |\text{codomain}|$

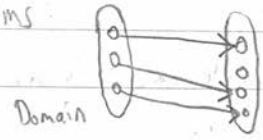
**Bijective** - every element in the codomain is mapped to <u>exactly</u> one element in the domain

Implies: $|\text{domain}| = |\text{codomain}|$

- If a function $f: A \to B$ is bijective, there must also exist a function $f^{-1}: B \to A$ s.t. $f^{-1}(f(a)) = a$, $f(f^{-1}(b)) = b$ [f is invertible]

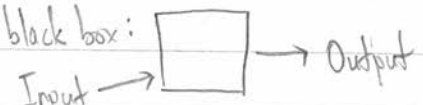
## Describing Functions

1) Arrow diagrams




(Suitable for small sets)

2) Functions as a black box:




3) Functions as labels: Each element in the domain maps to exactly one element of the codomain; that element in the codomain can thus be thought of as a label for the element in the domain
e.g. $f(\text{"apple"}) = \text{"red"}$, $f(\text{"banana"}) = \text{"yellow"}$

4) Bijective functions as translation: $f(\text{"Uno"}) = \text{"One"}$, $f^{-1}(\text{"One"}) = \text{"Uno"}$

# Properties of Equivalence Relations

1/25/23
Lecture 7

## Equivalence Classes

Given set $X$, equivalence relation $R$ on $X$, the set of equivalence classes $\{[a] \mid a \in X\}$ form a partition of $X$ (i.e. every element $b \in X$ is contained in exactly 1 equivalence class)

- Conversely, a partition of $X$ can be used to form a unique equivalence relation, i.e. given set $X$, $A_1, \dots A_n$ (partition of $X$), $R_{\{A_1,\dots,A_n\}} = a \sim b$ iff $\exists i$ s.t. $a, b \in A_i$,
  - Prof: $a \sim a \; \forall a \in X \to a \in [a]$ (each element belongs to at least 1 equivalence class)
    $a \sim b \to a, b \in [a] \to a \sim b, b \sim c \; (b \in [c]) \to a \sim c \to c \in [a] \to [a] = [c]$
    (each element belongs to at most 1 equivalence class)

## Modular Arithmetic

Notation: Given $a, b, c \in \mathbb{Z}$, if $a = b \cdot c \to$ "$b$ divides $a$", "$b \mid a$", "$a$ divisible by $b$"

→ Given $n \in \mathbb{Z}, n > 0, a, b \in \mathbb{Z}$, $n \mid a - b \to$ "$n$ is congruent to $b$ modulo $n$" ($n$ divides $a - b$)

→ "$a \equiv b \pmod{n}$" represents an equivalence relation with $n-1$ equivalence classes

## Matrices of Relations

Given set $X = \{x_1, \dots, x_n\}$ ($|X| = n$), relation $R$ on $X$, we can depict $R$ as an $n \times n$ matrix,

i.e.: $M_R = \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} \overset{\begin{matrix} x_1 & \cdots & x_n \end{matrix}}{\begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}} = \{M_{ij}\} \begin{cases} M_{ij} = 1 \text{ if } x_i \sim x_j \\ M_{ij} = 0 \text{ if } x_i \not\sim x_j \end{cases}$

### Properties

1) $R$ is reflexive → : matrix diagonal will be all 1s ($M_{ii} = 1 \; \forall i$)
2) $R$ is symmetric → : $M$ will be symmetric over its diagonal ($A_{ij} = A_{ji} \; \forall i, j$, $M = M^T$)
3) $R$ is transitive → : "$(A^2)_{ij} \neq 0 \to A_{ij} \neq 0$" ($\leftrightarrow$ transitive)

(*) Properties only hold if row order [of elements] = column order

# Intro to Counting

1/27/23
Lecture 8

## Counting (§6)

### · Counting

**Counting** is the process of determining the number of elements contained within a set (i.e. the size of the set), such that a bijection can be established between a set of size $n$ and the set of positive integers $\{1, 2, \dots, n\}$

Ex: Given set $Y$ ($|Y| = n$), a bijection $f: X \to Y$ can be made between $Y$ and the set $X \subseteq \mathbb{R}$ ($|X| = n$), such that every $i \in X$ is mapped to an element $x_i \in Y$ (i.e. $f(i) = x_i$)

### Principles of Counting

- **Multiplication Principle** - If an event/activity can be broken into $t \in \mathbb{R}$ independent steps, with $n_i$ ways to do a given step $i$, the total number of different possible events/activities is $n_1 \cdot n_2 \cdot \dots \cdot n_t$

  Ex: Creating a sequence of 4 English letters = 4 steps of picking 1 character each
  → total # of possible strings = 26 (step 1) · 26 (step 2) · 26 (step 3) · 26 (step 4)
  → total # (without repetition) = 26 (step 1) · 25 (step 2) · 24 (step 3) · 23 (step 4)

- **Addition Principle** - Given sets $X_1, \dots, X_t$ ($|X_i| = n_i$) if $X_i \cap X_j = \emptyset \ \forall i \neq j$ ($X_i$ and $X_j$ pairwise disjoint), the number of possible elements that can be chosen from either $X_1$ or $X_2$ or ... or $X_t = n_1 + n_2 + \dots + n_t$ (Alt: The union $X_1 \cup \dots \cup X_t$ contains $\sum_{j=1}^{t} n_j$ elements)

- **Inclusion/Exclusion Principle** (for $t = 2$) - Given finite sets $X$ and $Y$, $|X \cup Y| = |X| + |Y| - |X \cap Y|$
  (*) Used in place of the Addition Principle for non-disjoint sets
  (*) $t = 3$: Given sets $X, Y, Z$, $|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$

# Permutations and Combinations

1/30/23
Lecture 9

## Permutations

**Definition:** A permutation of $n$ distinct elements $x_1, \ldots, x_n$ is an ordering of the elements $x_1, \ldots, x_n$.

- Given $n$ elements, there are $n!$ possible permutations of those $n$ elements.

Ex: $\{A, B, C\} \rightarrow ABC, ACB, BAC, BCA, CAB, CBA$ (6 total $= 3!$)
(starting elements; all permutations of the 3 elements)

**Definition:** An $r$-permutation of $n$ elements $x_1, \ldots, x_n$ is an ordering of an $r$-element subset of the set of $n$ elements $X = \{x_1, \ldots, x_n\}$ (i.e. an $r$-permutation is an ordering of any $r$ elements selected from the original $n$ elements).

- Notation: The number of $r$-permutations of a set of $n$ distinct elements is denoted $P(n,r)$ $\left(P(n,r) = \frac{n!}{(n-r)!}\right)$

Ex: $P(3,2)$ for set $\{A,B,C\} = |\{AB, BA, AC, CA, BC, CB\}|$ $(= 6)$

## Combinations

**Definition:** An $r$-combination ([r-]arrangement) of a set $X$ containing $n$ distinct elements is an unordered selection of $r$ elements of $X$ (i.e. is an $r$-element subset of $X$ (i.e. $= \text{set } Y, Y \subseteq X, |Y| = r$)).

- Notation: The number of $r$-combinations of a set of $n$ elements is denoted $C(n,r)$ or $\binom{n}{r}$ ("$n$ choose $r$") $\left(C(n,r) = \frac{n!}{(n-r)! \cdot r!}\right)$

Ex: $C(n,r) = \binom{n}{r}$ for set $\{A,B,C\} = |\{\{A,B\}, \{A,C\}, \{B,C\}\}|$ $(= 3)$

# Equivalence Relations Review

1/31/23
Disc 4

## Equivalence Relations

- For every set $X$, there exists a bijection between the set of equivalence relations on $X$ and the set of partitions of $X$ (i.e. each equivalence relation is associated with a distinct partition, and vice versa)
  - The number of equivalence relations on $X$ (in terms of pairings of elements of $X$) is thus equal to the number of possible partitions of $X$

- An equivalence relation encodes some quality of "sameness" (equality), shared between all elements of an equivalence class
  - Relations (more generally) represent forms of "relationships" between elements

## Proving Statements

- In mathematics, a statement (e.g. "relation $R$ on $X$ is transitive") is held as true unless there exists a counterexample
  - A statement that is held to be true solely due to a lack of any examples to either prove or disprove it (e.g. "$x \sim y$ if $x = y+1$ is reflexive on the empty set" [because there are no elements in $\emptyset$ to disprove this]) are described as being "vacuously true"

- When proving transitivity for a relation (i.e. "$a \sim b, b \sim c \rightarrow a \sim c$"), the elements $a, b, c$ do not need to be distinct

# Counting (cont.)

2/7/23
Lecture 10

## Generalized Permutations & Combinations (§6.3)

**THM Counting** Given a sequence $S$ of $n$ items containing $n_1$ identical objects of type 1, $n_2$ of type 2, ..., $n_t$ of type $t$ → the number of orderings of $S$ is:

$$\#\text{ of orderings of } S = \frac{n!}{n_1!\, n_2! \cdots n_t!}$$

(*) "Stars and Bars"

Problem: How many solutions are there for the equation $x+y+z=9$? $(x,y,z \in \mathbb{Z}^+)$

Solution: We think of a solution to $x+y+z=9$ as a string of nine 1s and 2 slashes (where each slash demarcates a variable)

i.e.: $\underbrace{1\,1\,\ldots\,1}_{x} / \underbrace{1\,1\,\ldots\,1}_{y} / \underbrace{1\,1\,\ldots\,1}_{z}$ ; the values of $x, y, z$ being determined by the placement of the slashes

→ The number of solutions = the number of distinct possible strings = $\binom{11}{2}$

(*) Case: A restriction (e.g. $x \geq 2$) can be factored into the equation, i.e.: $(x-2)+y+z=7$

↓

**THM Counting** Given set $X$ ($|X| = t$), the number of possible unordered selections of $k$ elements from $X$ (allowing repetition) is:

$$\#\text{ of possible } k\text{-element selections: } \binom{k+t-1}{t-1} = ((k+t-1, t-1))$$

└ (*) This can be seen as an extension of "stars and bars", where each the value of the variables $x, y, z, \ldots$ represent the indices of the selection, i.e. $1\,1\,1\,/\,1\,/\,1\,1 \rightarrow \{x_3, x_4\}$

# Binomial Coefficients

2/6/23
Lecture 11

## Binomial Coefficients (§6.7)

**The Binomial Theorem**

Given two numbers $a, b \in \mathbb{R}$ and $n \in \mathbb{Z}^+$, then:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k},$$ where the numbers $\binom{n}{k}$ are referred to as binomial coefficients.

↳ Justification: The term $a^k b^{n-k}$ is obtained by picking $k$ a's out of $n$ choices $(a+b)$, hence the coefficient $\binom{n}{k}$.

(*) Note: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ (can be proven)

### Pascal's Triangle

$n=0$ 1
$n=1$ 1 1 ] $(a+b)$
$n=2$ 1 2 1 ] $(a+b)^2$
$n=3$ 1 3 3 1 ] $(a+b)^3$
$n=4$ 1 4 6 4 1 ] $(a+b)^4$

Pascal's Triangle is a triangle of numbers, where the $n^{th}$ row contains the coefficients for the expression $(a+b)^n$.

Each number in the triangle is a sum of the two numbers directly above it.

↳ **Theorem:** $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k+1}$

### Polynomial Coefficients

**The Trinomial Theorem**

Given $a, b, c \in \mathbb{R}$, $n \in \mathbb{Z}^+$:

$$(a+b+c)^n = \sum_{\substack{i,j,k \\ (i+j+k=0)}}^{n} \frac{n!}{i!\,j!\,k!} a^i b^j c^k$$

(*) Can be generalized for higher-dimensional polynomials

# The Pigeonhole Principle + Intro to Recurrence Relations

2/8/23
Lecture 12

## The Pigeonhole Principle (§6.8)

If ≥n+1 pigeons fly into n pigeonholes, at least one pigeonhole contains at least two pigeons.

↓

### The Pigeonhole Principle (v2)

Given a function $f: X \to Y$, if $|X| = n$ and $|Y| = m$, there are at least $\lceil \frac{n}{m} \rceil$ elements of X that map to the same element of Y.

i.e. $a_1, a_2, \ldots, a_k \left[k = \lceil \frac{n}{m} \rceil\right] \to f(a_1) = f(a_2) = \ldots = f(a_k)$

### Recurrence Relations (§7.1, 7.2)

Definition: A recurrence relation for sequence $\{a_k\}_{k=0}$ is a relation that defines the value of each element $a_i$ based on the values of the preceding elements.

i.e. $a_i = f(a_1, a_2, \ldots, a_{i-1})$

Notation: Typically, a certain number of elements at the beginning of the sequence are given explicit values in order to "start up" the sequence. Those elements are referred to as initial conditions.

# Solving Recurrence Relations

2/10/23
Lecture 13

## Solving Recurrence Relations (§6.2)

1) Iteration - continuously expressing a term $a_n$ in terms of its predecessors, until it can eventually be expressed in terms of the initial condition (e.g. $a_1$)

Ex: $a_n = 2a_{n-1} = 2(2a_{n-2}) = 2^3 a_{n-3} = \dots$

$\longrightarrow = 2^{n-1} a_1$ (for initial condition $a_1$)

2) Substitution - substituting a certain sequence for another may make a given expression easier to compute

Ex: $q_n = 2q_{n-1} + 1 \rightarrow$ We define $a_n = q_n + 1$

$= 2q_{n-1} + 1 + 1 = 2q_{n-1} + 2$

$= 2(q_{n-1} + 1) = 2a_{n-1} \rightarrow a_n = 2a_{n-1}$

$\longrightarrow q_n = a_n - 1 = \boxed{2^{n-1}(a_1) - 1}$

(*) 3) Linear homogenous recurrence relations with constant coefficients, of order $k$ (i.e. sequences $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}$, $c_k \neq 0$, $c_1, \dots, c_k \in \mathbb{R}$) can be solved algebraically, e.g.:

Ex: R: $a_n = c_1 a_{n-1} + c_2 a_{n-2}$, $n \geq 2$, w/ initial conditions $a_0, a_1$ (order = 2)

$\longrightarrow$ Assume that for the equation $x^2 - c_1 x + c_2 = 0$, $\exists$ two distinct solns. $r_1 \neq r_2$

$\longrightarrow \exists$ two constants $\alpha, \beta$ such that $\boxed{a_n = \alpha r_1^n + \beta r_2^n \ \forall\, n \geq 0}$

($\alpha$ and $\beta$ being computable from the initial conditions)

# Solving Recurrence Relations (cont.)

2/13/23
Lecture 14
+ Lecture 15
2/15/23

## General Solns. for Linear Homogenous Recurrence Relations (w/ Constant Coefficients):

Given $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k}$

→ Characteristic polynomial = $x^k - x^{k-1}c_1 - x^{k-2}c_2 - \dots - xc_{k-1} - c_k$

→ Use roots to compute soln.

Ex: $a_n = c_1 a_{n-1} + c_2 a_{n-2} + c_3 a_{n-3}$ (order 3) → $x^3 - c_1 x^2 - c_2 x - c_3 [= 0]$ → 3 roots $r_1, r_2, r_3$

→ 3 cases: 1) Distinct roots $r_1, r_2, r_3$ → $a_n = \alpha r_1^n + \beta r_2^n + \gamma r_3^n$

2) 2 distinct roots $r_1, r_2 = r_3$ → $a_n = \alpha r_1^n + \beta r_2^n + \gamma n r_3^n$ [one repeated root]

3) 1 distinct root $r_1 = r_2 = r_3 [= r]$ → $a_n = \alpha r^n + \beta n r^n + \gamma n^2 r^n$ [two repeated roots]

(*) Inclusion of addl. terms ($n, n^2, \dots$) expands space of solutions [satisfying the relation]

## (*) Notes on Solutions

- Solutions can take many forms (e.g. periodic)

- Complex roots may appear during the polynomial-solving process - are solved just like real roots
  (-) $i$ can be "eliminated" by being reexpressed (e.g. define $\delta = i\alpha + i\beta$, then find a real # value for $\delta$ → $i$ disappears)

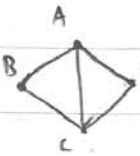
| Euler's Formula |
| --- |
| $e^{ix} = \cos(x) + i\sin(x)$ |

# Intro to Graphs

2/17/23
Lecture 16

## Graphs

A graph $G(V, E)$ is defined as a set of <u>vertices</u> $V(G)$ and associated <u>edges</u> between vertices $E(G)$ ($E(G) \subseteq \{(a,b) \mid a,b \in V(G)\}$).

Ex: 

$= G \begin{cases} V(G) = \{A, B, C, D\} \text{ (points [vertices])} \\ E(G) = \{(A,B), (A,C), (B,C), (C,D), (D,A)\} \text{ (lines [edges])} \end{cases}$

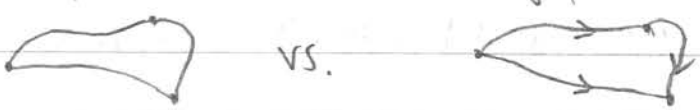
## Definitions

- Edge $e = (u, v) \rightarrow e$ is <u>incident</u> to vertices $u$ and $v$
- $u, v \in V(G), \exists e = (u,v) \in E(G)$ [$u$ and $v$ connected by an edge] $\rightarrow u$ and $v$ are <u>adjacent</u>
  $\rightarrow$ a vertex $v_0$ not adjacent to any other vertices is called <u>isolated</u>

## Types of Graphs

- Graph (<u>undirected graph</u>): graph where edge $(a,b) = (b,a)$ [edges unordered], vs:
- Digraph (<u>directed graph</u>): graph where edge $(a,b) \neq (b,a)$ [pairs of vertices ordered]

<u>Graph</u> vs. <u>Digraph</u>



- <u>Simple graph</u>: graph with no <u>loops</u> (edges $(a,a) \in E(G)$) and no parallel edges (i.e. any two vertices connected by <u>at most</u> one edge)


- <u>Complete graph with N vertices</u> ($K_n$): A graph with $n$ vertices ($|V(K_n)| = n$), such that all points are adjacent to all other points ($(a,b) \in E(K_n) \; \forall \; a,b \in V(K_n)$)

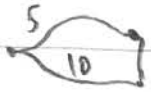
$K_1$: • $K_2$: — $K_3$: △ $K_4$: ⊠ etc... $\boxed{(\star |E(K_n)| = \binom{n}{2})}$

# Intro to Graphs (cont.)

2/17/23
Lecture 16 (cont.)

## Types of Graphs (cont.)

- **Weighted graph**: a graph where each edge has an associated number (weight/label)
  - An **unweighted graph** assigns weight 1 to every edge by default

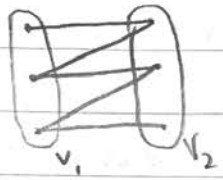


(Weighted graph)

- **Bipartite graph**: a graph where $\exists$ a partition of $V$, $V(G) = V_1 \cup V_2$ such that every edge in $E(G)$ is incident to one vertex in $V_1$ and one vertex in $V_2$

$(* \ (a,b) \in E(G) \rightarrow a \in V_1, b \in V_2)$

Ex:




(*) The graph shown below is not bipartite.


Proof: Assume the graph is bipartite $\rightarrow V(G) = V_1 \cup V_2$.
$\rightarrow$ each vertex 2, 3, 4 belongs to either $V_1$ or $V_2$
$\rightarrow$ at least two of $\{2,3,4\}$ will be in the same set (per Pigeonhole)
$\rightarrow \exists$ an edge between two points in the same set $\rightarrow$ **not bipartite!**

- **Complete bipartite graph on m & n vertices** ($K_{m,n}$): a bipartite graph, such that:
  (*) $V(K_{m,n}) = V_1 \cup V_2$, $|V_1| = m$, $|V_2| = n$
  (*) $E(K_{m,n}) = \{(a,b) \mid a \in V_1, b \in V_2\}$ (all points in $V_1$ connected to all points in $V_2$)

Ex:

$(K_{2,2})$ $(K_{3,2})$ $(K_{3,3})$

# Paths and Cycles

2/22/23
Lecture 17

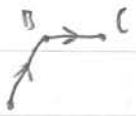
## Paths

A path from vertex $v$ to vertex $w$ on graph $G$ is defined as a sequence of vertices $(v_0, v_1, \dots, v_n)$ [length $= n$], where $v_0 = v$, $v_n = w$, and $\forall$ pairs of vertices $v_i$ and $v_{i+1} \rightarrow (v_i, v_{i+1}) \in E(G)$ ($v_i, v_{i+1}$ adjacent)

(*) On a weighted graph, the length of a path is defined as the sum of the weights of the edges traversed

(*) Alt. Notation: · Paths as a sequence of edges $((v_0, v_1), (v_1, v_2), \dots, (v_{n-1}, v_n))$

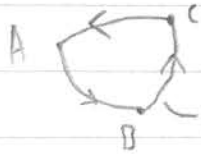
· Paths as a sequence of vertices + edges $(v_0, e_1, v_1, \dots, e_n, v_n)$




## Definitions

- A connected graph is a graph where $\exists$ a path between any two vertices $v, w \in V(G)$
- Given a graph $G(V, E)$, we define a subgraph $G'(V', E')$ of $G$ to be any graph such that 1. $V' \subseteq V$, 2. $E' \subseteq E$, 3. $\forall (v, w) \in E' \rightarrow v, w \in V'$ [no dangling edges]
  - Given a vertex $v \in V(G)$, the component of $G$ containing $V$ is the subgraph $G'$ of $G$ containing all vertices & edges of $G$ expressible as an element of at least 1 path beginning at $v$
- A simple path is a path that contains no repeated vertices
- A cycle is a path [of nonzero length] from $v$ to $v$, with no repeated edges
  - A simple cycle is a cycle containing no repeated vertices (except for the beginning/end)
  - An Eulerian cycle (Euler cycle/circuit/walk) is a cycle that visits every edge and vertex
    - A graph $G$ contains an Eulerian cycle iff $G$ is connected and contains only vertices of even degrees
- The degree $\delta(v)$ of a vertex $v$ is the number of edges incident to $v$

(*) For digraphs, we distinguish between the in-degree and out-degree




Cycle (A, B, C, A)

# Paths and Cycles (cont.)

2/24/23

Lecture 18

## Paths and Cycles (cont.)

- Given a graph $G(V, E)$ with vertices $V(G) = \{v_1, \ldots, v_n\}$, the sum of the degrees of $V(G)$ is even, i.e. $\sum_{i=1}^{n} \delta(v_i) = 2|E(G)|$
  - (*) Corollary: the number of vertices with odd weights is even
- An Eulerian path in graph $G$ is defined as a path from $v$ to $w$ ($v \neq w$), containing all edges and vertices of $G$
  - An Eulerian path exists if $G$ is connected and $v$ to $w$ are the only vertices $\in V(G)$ of odd degree
- Reminder: A simple cycle is a cycle $v \to v$ with no repeated vertices, except for $v$ itself
  - If there exists a cycle in a graph $G$, there also exists a simple cycle in $G$

## Hamiltonian Cycles (§8.3)

- A Hamiltonian cycle in a graph $G$ is a cycle that contains the initial vertex exactly twice, and all other vertices exactly one time
- Travelling Salesman Problem - finding the shortest Hamiltonian cycle in a graph (usually weighted)
  - (*) Length in terms of the sum of weights of the edges traversed
  - (*) If any given vertex can be proven to be visited more than once, a Hamiltonian cycle does not exist
  - (*) If $\delta(v_i) + \delta(v_j) \geq |V(G)|$ for any non-adjacent vertices $v_i, v_j$ in $V(G)$, then graph $G$ contains a Hamiltonian cycle (if, not iff)

# Dijkstra's & Intro to Isomorphisms

2/27/23
Lecture 19

## Dijkstra's Shortest-Path Algorithm (§18.4)

Given a weighted graph $G$, Dijkstra's algorithm returns the shortest path from $a \in V(G) \to z \in V(G)$.

Notation: Given edge $(i,j) \in E(G)$, $w(i,j)$ denotes the weight of $(i,j)$

Mechanism: Algorithm gives each vertex $i \in V$ a label $L(i)$, representing length of shortest path $a \to i$.

Algorithm: 1. $L(x) = \infty \; \forall \, x \in V, x \neq a$ ; $L(a) = 0$

2. Define $T$ = set of all vertices [w/ undetermined $L$]

while $(z \in T)$: a. choose $v \in T$ w/ smallest $L(v)$

b. $T = T - v$

c. for each $x$ adjacent to $v$, $L(x) = \min(L(x), L(v) + w(v,x))$

Logic: If a path $(v_1, v_2, \ldots, v_n)$ is the shortest path $v_1 \to v_n$, $(v_1, v_2, \ldots, v_{n-1})$ must have been the shortest path $v_1 \to v_{n-1}$.

Variations: $A^*$ (Dijkstra's with an added heuristic for guiding queries toward destination)

Negative-weight Dijkstra's (Dijkstra's only works for non-negative weights by default)

(*) Shortest-path algorithms are not restricted to abstract graphs (e.g. can be used for speedrunning)

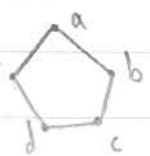
## Isomorphisms of Graphs (§8.6)

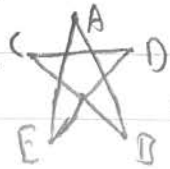
Definition: Two graphs $G_1, G_2$ are <u>isomorphic</u> if every vertex/edge $\in G_1$ can be mapped to a corresponding vertex/edge in $G_2$, i.e. $\exists$ bijective functions $f: V(G_1) \to V(G_2)$ and $g: E(G_1) \to E(G_2)$, such that $g((v,w)) = (f(v), f(w))$.

Notation: $G_1$ and $G_2$ isomorphic $\to G_1 \simeq G_2$

$\to$ The pair of functions $(f, g)$ is an <u>isomorphism</u> of $G_1$ onto $G_2$.

(*) Definition: Cyclic graph $C_n$ is the graph of $n$ vertices, where $E(C_n) = \{(v_i, v_{i+1}) \mid 0 \leq i \leq n-1\} + (v_n, v_0)$

$C_5 =$ 

$\simeq$ 


$\begin{cases} f(a) = A, f(b) = B, \ldots \\ g((a,b)) = (A,B), g((b,c)) = (B,C), \ldots \end{cases}$

# Planar Graphs

3/1/23
Lecture 20

## Invariants

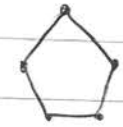
Definition: An <u>invariant</u> is any property that is preserved under isomorphisms (i.e. $G_1 \cong G_2 \rightarrow G_1, G_2$ share invariants).

(*)Contrapositive: If two graphs $G_1, G_2$ do not share invariants, $G_1 \ncong G_2$

Example Invariants: 1) # of vertices/edges in a graph
2) Connectedness
3) Degree sequence (* same deg seq. does not imply isomorphism)
4) Having simple cycles of length k

## Planar Graphs (§8.7)

Definition: A graph G is considered <u>planar</u> if it can be drawn on a plane without any of its edges intersecting.

Ex:  (not planar),  (planar - $C_5$). (*) $K_{3,3}$, $K_5$ non-planar across isomorphisms

When drawing connected planar graphs in the plane, the edges of the graph divide the plane into regions, known as <u>faces</u>. Each face is defined by the cycle of edges forming its boundary.

### (*)Theorem (Euler)

Given a connected planar graph G, with v vertices, e edges, and f faces:

# vertices - # edges + # faces = $\boxed{v - e + f = 2}$

(*) Proving non-planarity: Assume planarity, then prove-by-contradiction w/ the above theorem

# Planar Graphs (cont.)

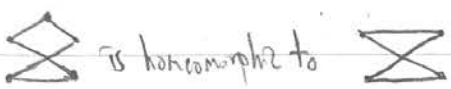
3/6/23
Lecture 21

## Planar Graphs

Definition: Given a vertex $v$ with $\delta(v) = 2$ incident to edges $(v_1, v)$ and $(v, v_2)$, we say edges $(v_1, v)$ and $(v, v_2)$ are in series. A series reduction deletes $v$ and replaces edges $(v_1, v), (v, v_2)$ with a single edge $(v_1, v_2)$.

Ex: 


Definition: Graphs $G_1, G_2$ are homeomorphic if $G_1, G_2$ can be reduced (by series reductions) to isomorphic graphs.

Ex:  is homeomorphic to 

**Kuratowski's Theorem** A graph $G$ is planar iff $G$ does not contain a subgraph homeomorphic to $K_{3,3}$ or $K_5$.

## (*) Applications of Planar Graphs (Platonic Solids)

Definition: A polyhedron is a solid where all faces are polygons, and all edges contained in exactly two faces.

→ The formula "$v - e + f = 2$" holds for polyhedrons. (Test: "project" into 2D, e.g.  →  )

Definition: A regular polyhedron is a polyhedron where all faces are regular polygons with $n$ sides and all vertices are of the same degree $(r)$.

→ $rV = 2E = nF$, $V + F - E = 2$ → $\frac{2E}{r} - E + \frac{2E}{n} = 2$, $E, n, r \in \mathbb{Z}^+$ (A Diophantine eq.)

→ $\frac{1}{r} + \frac{1}{n} = \frac{1}{2} + \frac{1}{E}$ → both $r, n$ cannot be $\geq 4$ → $\min(r, n) \leq 3$, but $\begin{cases} r \geq 3 \text{ (no "2-gon")} \\ n \geq 3 \text{ (solid)} \end{cases}$

→ either $r$ or $n = 3$, $\frac{1}{r} + \frac{1}{n} = \frac{1}{2} + \frac{1}{E}$ → The only possible combos $(r, n)$ are for a tetrahedron, icosahedron, cube, octahedron, dodecahedron (5 Platonic solids)

# Intro to Trees

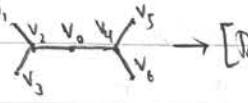
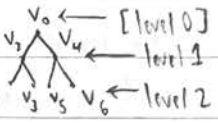
3/8/23
Lecture 22

## Trees (§9.1)

A tree $T$ is a [simple] graph where, for any vertices $v, w \in V(T)$, there exists exactly one unique simple path in $T$ from $v$ to $w$.

### Definitions

- A rooted tree is a tree where one vertex has been defined as the "root" of the tree

Ex: [Tree] $T$:  → [Rooted tree] $T_{v_0}$ 


(*) Any node in a tree can be the root

- The level of a vertex $w$ in a rooted tree is defined as the length of the unique path from the root of the tree to $w$
  - The height of the tree is the largest level number in the tree

## Properties of Trees (§9.2)

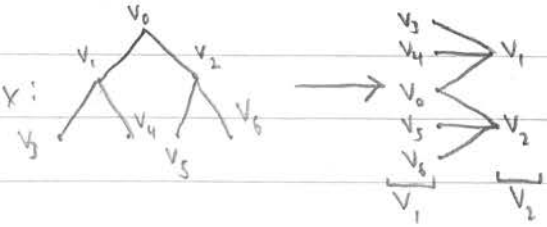
Definition: A graph $G$ is acyclic if it does not contain any cycles.

(*) Given a graph $G$ with $n$ vertices, the following statements are equivalent:

i. $G$ is a tree
ii. $G$ is a connected, acyclic graph
iii. $G$ is a connected graph with $(n-1)$ edges
iv. $G$ is an acyclic graph with $(n-1)$ edges

[All trees are connected, acyclic graphs with $(n-1)$ edges]

(*) All [rooted] trees are valid bipartite graphs $V(T) = V_1 \cup V_2$, where $V_1$ contains all nodes of even level and $V_2$ all nodes of odd level

Ex: 


(*) All trees are also planar

# Intro to Trees (cont.)

3/8/23
Lecture 22 (cont.)

**Tree Terminology**

Given a rooted tree $T$ rooted at $v_0$, let $x, y, z \in V(T)$ [be vertices of $T$] and let $(v_0, v_1, \dots, v_k)$ be a simple path $v_0$ to $v_k$ in $T$.

i. $v_{n-1}$ is the <u>parent</u> of $v_n$; conversely, $v_n$ is the <u>child</u> of $v_{n-1}$

(*) A vertex may also be described as having <u>children</u> in the plural case.

ii. $v_0, v_1, \dots, v_{k-1}$ are the <u>ancestors</u> of $v_k$.

→ iii. If a vertex $x$ is an ancestor of $y$, it can also be said that $y$ is a <u>descendant</u> of $x$.

iv. If two vertices $x$ and $y$ are both children of a third vertex $z$, $x$ and $y$ are called <u>siblings</u>.

**Definitions (cont.)**

- A vertex with no children is called a <u>leaf</u> or <u>terminal vertex</u>.
  (*) All leaves are of degree 1; the only vertices in a tree of degree 1 are the leaves, and potentially the root [which is not called a leaf].
- Any vertex that is not a leaf is called a <u>branch</u> or <u>internal vertex</u>.
- The <u>subtree</u> of $T$ rooted at $x$ (for some tree $T$ with vertex $x$) is the graph $T_x(V', E')$: $V' = \{x\} \cup \{\text{descendants of } x\}$,
  $E' = \{\text{all edges } e \text{ contained in a path from } x \text{ to some vertex } v \in V'\}$

# (*) Properties of Trees (Proof)

3/10/23

Lecture 23

Reminder: Given graph $G$ with $n$ vertices, TFAE: (1) $G$ is a tree

(2) $G$ is a connected, acyclic graph

(3) $G$ is a connected graph with $(n-1)$ edges

(4) $G$ is an acyclic graph with $(n-1)$ edges

Proof: (1) → (2): By definition of a tree

(2) → (3): (*) Lemma: Graph $G$ w/ $|V(G)| \geq 2$ contains at least two vertices of degree 1 (Endpoints of longest path in $G$)

↳ Proof by Induction: $T$ $(|V(T)| = 1) \rightarrow |E(T)| = 0$

$(n) \rightarrow (n+1)$: $T$ has $(n+1)$ vertices → define subgraph $T'$ (removing one leaf)

→ $|V(T)| = n$, $|E(T)| = n-1$ (per assumption) $= |E(T')| - 1 \rightarrow |E(T)| = n$ . □

(3) → (4): Proof by Contradiction: Assume $G$ is cyclic → removing one edge of the cycle still gives a connected graph w/ $(n-2)$ edges, $n$ vertices → impossible (contradiction). □

(4) → (1): (a) $T$ connected: Assume $T$ consists of $k$ connected components $T_1, \ldots, T_k$,

where $v_i = |V(T_i)|$, $n = v_1 + v_2 + \ldots + v_k$

All $T_i$ connected, acyclic (per assumption) → $|E(T_i)| = n_i - 1$ . □

→ $|E(T)| = (n_1 - 1) + \ldots + (n_k - 1) = n - k = n - 1$ (per (4)) → $k = 1$ [$T$ connected]

(b) ∃ a unique path between any two vertices:

i. $T$ is connected → # paths $(v \rightarrow w) \geq 1$

ii. $T$ acyclic → # paths $(v \rightarrow w) < 2$

→ # paths = 1 . □

↓

(1) → (2) → (3) → (4) → (1)

↓

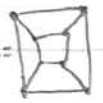
(1) ↔ (2) ↔ (3) ↔ (4) [are equivalent]

# Spanning Trees

3/10/23
Lecture 23 (cont.)

## Spanning Trees (§9.3)

Definition: A subgraph $T$ of a graph $G$ is called a spanning tree of $G$ if $T$ is a tree visiting all vertices of $G$ (i.e. $V(T) = V(G)$)

Ex: $G =$  $\rightarrow T =$  , e.g.

(*) A graph $G$ contains a spanning tree iff $G$ is connected

### (*) Methods for Finding Spanning Trees

#### 1) Breadth-First Search (BFS)

Given a connected graph $G$ with vertices ordered $v_1, \ldots, v_n$:

→ Starting from $v_1$, add all children of $v_1$ to a queue (sorted by order) + add all edges to the children, to $E'$ [add children to $V'$]

→ while $(V' \neq V(G))$:

for each vertex in the queue, add all of its children to $V'$ iff they have not already been, and add all edges to added children to $E'$

once the queue has been cleared, add all newly-added children to the queue

#### 2) Depth-First Search (DFS)

Given a connected graph $G$ with vertices ordered $v_1, \ldots, v_n$:

→ (Starting at $v_1$): while there is at least one edge incident to the current vertex that would not create a cycle if added, add the edge to the vertex of least ordered value (first in ordering) and move to that edge

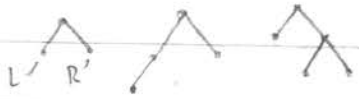
→ If there are no such edges, backtrack until there are; if the backtracking returns to $v_1$, and no such edges are present at $v_1$, terminate

# Binary Trees

3/15/26
Lecture 24

## Binary Trees (§9.5)

Definition: A binary tree is a rooted tree where each vertex has 0, 1, or 2 children. For internal vertices, we distinguish between a left and right child.

Ex: 


(*) Def: A full binary tree is a binary tree where each vertex has 0 or 2 children.

↳ 

**THM** Let $T$ be a full binary tree with $i$ internal vertices. $T$ has $i+1$ terminal vertices.

↳ (*) Corollary: $|V(T)| = 2i + 1$

↳ (*) Proof: $V(T) = \{\text{root}\} \cup \{v \in V \mid v \text{ is a child of another vertex}\}$

$\rightarrow |V(T)| = 1 + 2i$

**THM** Let $T$ be a binary tree of height $h$. The number of terminal vertices $t \leq 2^h$.

↳ (*) Can be proven by induction

(*) Applications of Binary Trees

- Binary search trees are binary tree-based structures that can be traversed and modified easily [in a computer science context].
- Binary trees can be used to model/describe the process of deciphering Morse code.

# (*) Intro to Number Theory

3/15/23
Lecture 24 (cont.)

## Number Theory (§5)

Def: The study of numbers (integers/whole numbers; elements $\in \mathbb{Z}$).

Branches:

1) Analytic Number Theory - real/complex analysis (the study of real/complex numbers, functions, series, etc.)
2) Elementary Number Theory - study of elementary numbers
3) Algebraic Number Theory - study of algebra & algebraic structures

## (*) Example Theorems

- Goldbach conjecture - every even integer $\geq 4$ can be expressed as the sum of two primes
  (* Verified up to $10^{14}$)
- Fermat's Last Theorem - $\nexists$ integers $x, y, z \neq 0$ s.t. $x^n + y^n = z^n$ (for any $n \geq 3$)
  (* Proven by Andrew Wiles in 1994; first stated in 1637)
- Helfgott's Theorem - every odd integer $\geq 7$ can be expressed as the sum of 3 primes

## Intro to Number Theory (§5.1)

Def: An integer ($\geq 2$) is said to be prime iff its only [integer] divisors are 1 and itself; otherwise, it is said to be composite.

> **Fundamental Theorem of Arithmetic** ☆
>
> Every integer $\geq 2$ can be expressed as a product of prime numbers.
> ⟶ The prime factorization of an integer is unique.

Def: Given two integers a and b, the greatest common denominator (gcd) of a and b is the largest integer n ($\leq a, b$) s.t. $n \mid a$ and $n \mid b$.

# (*) Intro to Number Theory (cont.)

3/17/23

ecture 25

## Euclid's Algorithm

To find $\gcd(a,b)$ $[a,b \in \mathbb{Z}^+;\ a<b]$: → find $r$ s.t. $b = qa + r$, $0 \le r \le a$ $[q \in \mathbb{Z}^+]$

→ case $r=0$: → $\gcd(a,b) = a$

case $r \neq 0$: → $\gcd(a,b) = \gcd(r,a)$ [repeat]

Lemma: Given $a,b \in \mathbb{Z}$ ($a$ and $b$ not both 0), $\exists\ u,v \in \mathbb{Z}$ s.t. $\gcd(a,b) = ua + vb$

Lemma: Given prime $p \in \mathbb{Z}$ s.t. $p \mid ab$ $(a,b \in \mathbb{Z})$, $p$ divides at least one of $a,b$

→ if $a$ and $b$ are coprime, $\gcd(a,b) = 1 = ua + vb = ua \pmod b$

Fermat's Little Theorem: $a \in \mathbb{Z}_{\ge 1} \rightarrow a^p \equiv a \pmod p$ [* ($a,p$ coprime) → $a^{p-1} \equiv 1 \pmod p$]

Proof: Define equiv. classes of $(x \equiv y \pmod p)$: $S = \{[0], [1], \dots, [p-1]\}$

→ all elements of $a \cdot S$ are distinct → $a \cdot S = S$

→ $\prod_{i \in S}[i] = \prod_{i \in S}[i] \rightarrow (p-1)! = a^{p-1}(p-1)! \rightarrow 1 = a^{p-1}$

(*) Corollary: Given $N = pq$ ($p \neq q$; $p,q$ prime) and $x \in \mathbb{Z}$ ($x, N$ coprime):

→ $x^{(p-1)(q-1)} \equiv 1 \pmod N$

## (*) RSA Public Key Cryptosystem (Rivest-Shamir-Adleman)

To send a message $m$ such that anyone can see it, but only the intended recipient can decipher it:

1) Recipient puts out a public key $(N, e)$ and stores a private key $d$

2) Sender puts out $c = m^e \pmod N$ $[m < N]$, recipient receives $c$

3) $N = pq$ [$p,q$ prime], $e \cdot d = 1 \bmod ((p-1)(q-1))$ [$p,q$ large]

→ $c^d = m^{ed} \equiv m^{k \cdot (p-1)(q-1)+1} \rightarrow$ [eliminate extra terms] → $m$

↳ Others cannot see the message because they do not know $d$, cannot decrypt $c$

(*) RSA outdated due to cost of storing large primes ($\sim 2^{4000}$ bits/key)