

# CS1231: Reference

## Proof Language

- $\exists!$ : Exists a unique...
- $\equiv$ : Logical Equivalence: identical truth table (Definition 2.1.6)

## Order of Operations

- $\neg$ , followed by  $\wedge \vee$ , followed by  $\rightarrow \leftrightarrow$

## Proving Methods

- **Construction**: just sub in all  $x \in D$
- **Counterexample**: show one condition that leads to contradiction
- **Contraposition**:  
To prove  $P \rightarrow Q$ , prove  $\neg Q \rightarrow \neg P$
- **Contradiction**: To prove  $A$ , prove  $\neg A$  is not true (Clearly this is absurd)

## Thm 2.1.1 Logical Equivalences

(Aaron, pp 21 - 22)

- **Commutative Law**:  $p \wedge q \equiv q \wedge p$
- **Associative Law**:  
 $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$  (same with  $\vee$ )
- **Distributive Law**:  
 $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$   
(swap  $\vee$  &  $\wedge$ )
- **Identity Law**:  $p \wedge \mathbf{t} \equiv p$  or  $p \vee \mathbf{c} \equiv p$
- **Negation Law**:  $p \vee \neg p \equiv \mathbf{t}$  or  $p \wedge \neg p \equiv \mathbf{c}$
- **Double Negation Law**:  $\neg(\neg p) \equiv p$
- **Idempotent Law**:  $p \wedge p \equiv p$  (same for  $\vee$ )
- **Universal Bound Law**:  
 $p \vee \mathbf{t} \equiv \mathbf{t}$  or  $p \wedge \mathbf{c} \equiv \mathbf{c}$

- **De Morgan's laws**:

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$

## Conditional Statements

- $p \rightarrow q \equiv \neg p \vee q$
- **Contrapositive** (Def 2.2.2):  
 $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- **Converse** (2.2.3):  $q \rightarrow p$
- **Inverse** (2.2.4):  $\neg p \rightarrow \neg q$
- $p \rightarrow q \not\equiv (q \rightarrow p \equiv \neg p \rightarrow \neg q)$
- **Only If** (2.2.5):  $p$  only if  $q \equiv p \rightarrow q$
- **Biconditional** (2.2.6):  
 $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
- **Necessary & Sufficient Cond** (2.2.7):  
 $r$  necessary  $s \equiv r \rightarrow s$   
 $r$  sufficient  $s \equiv \neg r \rightarrow \neg s$

## Valid Arguments

- **Argument** (2.3.1): If all premise true, conclusion must be true
- **Syllogism**: Two premises and one conclusion
- **Modus Ponens**:  $p \rightarrow q, p, \therefore q$
- **Modus Tollens**:  $p \rightarrow q, \neg q, \therefore \neg p$

## Rules of Inference

- **Generalization**:  $p, \therefore p \vee q$
- **Specialization**:  $p \wedge q, \therefore p$
- **Elimination**:  $p \vee q, \neg p, \therefore q$
- **Transitivity**:  $p \rightarrow q, q \rightarrow r, \therefore p \rightarrow r$
- **Proof by Division into Cases**:  
 $p \vee q, p \rightarrow r, q \rightarrow r, \therefore r$

## Rules of Inference (Wei Quan)

- **Conjunction Intro** –  $A, B, \therefore A \wedge B$
- **Conjunction Elim** –  $A \wedge B, \therefore A, B$
- **Disjunction Intro** –  $A, \therefore A \vee B, B \vee A$
- **Disjunction Elim** :  
 $A \vee B, A \rightarrow C, B \rightarrow C, \therefore C$
- **Contradiction Intro** –  $A, \neg A, \therefore \text{Cont.}$
- **Contradiction Elim**:  
 $A \rightarrow \text{Contradiction}, \therefore \neg A$
- **Double Negation Elim** –  $\neg \neg A, \therefore A$

## Fallacies

- **Converse Error**:  $p \rightarrow q, q, \therefore p$
- **Inverse Error**:  $p \rightarrow q, \neg p, \therefore \neg q$
- **Sound & Unsound Argument**: Sound iff valid and premises are true

## Predicates & Quantified Stmt

- **Predicate** (3.1.1): A **predicate** sentence contains a finite number of variables and becomes a stmt when specific values are subst in the vars. The **domain** of a predicate var is the set of all values that may be subst in place of the var.
- **Truth Set** (3.1.2): If  $P(x)$  is a predicate and  $D_x \equiv D$ , the truth set is the set of all elements of  $D$  that make  $P(x)$  true when they are subst for  $x$ . The truth set of  $P(x)$  is  $\{x \in D | P(x)\}$ .
- **Universal Stmt** (3.1.3):  $\forall x \in D, Q(x)$ 
  - Equivalent to  $Q(x_1) \wedge Q(x_2) \wedge \dots \wedge Q(x_n)$
  - Stmt is true iff  $Q(x)$  true  $\forall x \in D$

- Stmt is false iff  $Q(x)$  false for at least one  $x \in D$
- **Existential Stmt** (3.1.4):  
 $\exists x \in D$ , such that  $Q(x)$ 
  - Equivalent to  $Q(x_1) \vee Q(x_2) \vee \dots \vee Q(x_n)$
  - Stmt is true iff  $Q(x)$  true for at least one  $x \in D$
  - Stmt is false iff  $Q(x)$  false  $\forall x \in D$
- **Implicit Quantification**:  $\implies \iff$ 
  - $P(x) \implies Q(x)$ :  
truth set  $P(x) \subset$  truth set  $Q(x)$
  - $P(x) \iff Q(x)$ :  
truth set  $P(x) \equiv$  truth set  $Q(x)$

## Negation of Quantified Stmt

- **Negation of Universal Stmt** (Thm 3.2.1)  
 $\sim (\forall x \in D, P(x)) \equiv \exists x \in D, \text{ s.t. } \sim P(x)$
- **Negation of Existential Stmt** (Thm 3.2.1)  
 $\sim (\exists x \in D, \text{ s.t. } P(x)) \equiv \forall x \in D, \sim P(x)$

## Universal Conditional Stmt

- $\forall x \in D, P(x) \implies Q(x)$
- **Vacuously True**: iff  $P(x)$  false  $\forall x \in D$
- **Contrapositive**:  
 $\forall x \in D, \sim Q(x) \implies \sim P(x)$
- **Converse**:  $\forall x \in D, Q(x) \implies P(x)$
- **Inverse**:  $\forall x \in D, \sim P(x) \implies \sim Q(x)$
- Refer to 2.2.5 and 2.2.7 for only if, necessary & sufficient conditions
- **Universal Modus Ponens & Tollens**:  
 $\forall x \in D, P(x) \implies Q(x), P(a)$  for  $a \in D$   
 $\therefore Q(a)$   
( $\sim Q(a), \therefore \sim P(a)$  for tollens)

# CS1231: Number Theory

## Def/Thm in Lecture Slides

- **Even & Odd** (Def 1.6.1, Proofs Handout, TS):

$$n \text{ is even} \iff \exists k \in \mathbb{Z} \text{ such that } n = 2k$$

$$n \text{ is odd} \iff \exists k \in \mathbb{Z} \text{ such that } n = 2k + 1$$

- **Divisibility** (Def 1.3.1, PH):

$$d \mid n \iff \exists k \in \mathbb{Z}, \text{ s.t. } n = dk$$

- **Thm 4.1.1** (pg 4, Number Theory Week 4, TS) :  
 $\forall a, b, c \in \mathbb{Z}$ , if  $a \mid b$  &  $a \mid c$ , then  $\forall x, y \in \mathbb{Z}, a \mid (bx + cy)$

- **Prop 4.2.2** (p9, NTW4, TS):

For any two primes  $p$  and  $p'$ , if  $p \mid p'$  then  $p = p'$

- **Thm 4.2.3** (pg 16, NTW4):

If  $p$  is prime and  $x_1, x_2, \dots, x_n$  are any integers s.t.:

$$p \mid x_1 x_2 \dots x_n,$$

then  $p \mid x_i$  for some  $x_i (1 \leq i \leq n)$

- **Lower Bound** (Def 4.3.1, NTP2, p3):

$b \in \mathbb{Z}$  is lower bound for set  $X \subseteq \mathbb{Z}$  if  $b \leq x, \forall x \in X$

- **Well Ordering Principle** (Thm 4.3.2, NTP2, p5):

If non-empty set  $S \subseteq \mathbb{Z}$  has lower/upper bound, then  $S$  has a least/greatest element

- **Uniqueness of least element** (Prop 4.3.3, NTP2, p8):

If set  $S \subseteq \mathbb{Z}$  has least/greatest element, then least/greatest elem is unique

- **Quotient-Remainder Thm** (Thm 4.4.1):

Given any  $a \in \mathbb{Z}$  & any  $b \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z}$  s.t.:

$$a = bq + r \text{ \& } 0 \leq r < b$$

- **G.C.D.** (Def 4.5.1, NTP2, p21):

Let  $a, b \in \mathbb{Z}$ , not both zero, g.c.d. of  $a, b$ ,  $\gcd(a, b)$ , is  $d \in \mathbb{Z}$  satisfying:

$$d \mid a \text{ \& } d \mid b \quad (1)$$

$$\forall c \in \mathbb{Z}, \text{ if } c \mid a \text{ \& } c \mid b \text{ then } c \leq d \quad (2)$$

- Existence of gcd (Prop 4.5.2):  
 For any  $a, b \in \mathbb{Z}$ , not both zero, their gcd exists and unique

- Bézout's Identity (Thm 4.5.3):

Let  $a, b \in \mathbb{Z}$ , not both zero, &  $d = \gcd(a, b)$ .

Then,  $\exists x, y \in \mathbb{Z}$  s.t.:

$$ax + by = d$$

- Relatively Prime/Coprime (Def 4.5.4):

$a, b \in \mathbb{Z}$  are coprime  $\iff \gcd(a, b) = 1$

- Prop 4.5.5:

$a, b \in \mathbb{Z}$ , not both zero, if  $c$  is common divisor of  $a$  &  $b$ , then  $c \mid \gcd(a, b)$

- NTP2, p38:  $\forall a, b \in \mathbb{Z}^+, a \mid b \iff \gcd(a, b) = a$

- L.C.M. (Def 4.6.1, NTP2, p41):

$a, b \in \mathbb{Z} \setminus \{0\}$ , their l.c.m, denoted  $\text{lcm}(a, b)$ , is  $m \in \mathbb{Z}^+$  s.t.

$$a \mid m \text{ \& } b \mid m \quad (3)$$

$$\forall c \in \mathbb{Z}^+, \text{ if } a \mid c \text{ \& } b \mid c, \text{ then } m \leq c \quad (4)$$

- NTP2, p43:  $\forall a, b \in \mathbb{Z}^+, \gcd(a, b) \mid \text{lcm}(a, b)$

## Theorems By Epp

- Thm 4.3.1:  $\forall a, b \in \mathbb{Z}^+, \text{ if } a \mid b \text{ then } a \leq b$

- Thm 4.3.3:  $\forall a, b, c \in \mathbb{Z}, \text{ if } a \mid b \text{ and } b \mid c \text{ then } a \mid c$

- Thm 4.3.5: Given any integer  $n > 1$ ,  $\exists k \in \mathbb{Z}^+$ , distinct primes  $p_1, p_2, \dots, p_k$  & positive integers  $e_1, e_2, \dots, e_k$ , s.t.

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$$

and any other exp for  $n$  as a product of prime numbers is identical to this (except ordering)

- Thm 4.7.1:  $\sqrt{2}$  is irrational

- Prop 4.7.3:

For any  $a \in \mathbb{Z}$  and any prime  $p$ , if  $p \mid a$  then  $p \nmid (a + 1)$

- Thm 4.7.4: The set of primes is infinite

## Appendix A (Epp)

- T1 (Cancellation Law for Add):  $a + b = a + c \implies b = c$

- T2 (Possibility of Subtraction): Given  $a, b$ ,  $\exists! x$  such that  $a + x = b$ . This  $x$  is denoted by  $b - a$ .

- T3:  $b - a = b + (-a)$  T4:  $-(-a) = a$

- T5:  $a(b - c) = ab - ac$  T6:  $0 \cdot a = a \cdot 0 = 0$

- T7 (Cancellation Law for Multiplication):

$$ab = ac, a \neq 0 \implies b = c$$

- T8 (Possibility of Division):

Given  $a, b$  with  $a \neq 0$ ,  $\exists! x$  such that  $ax = b$ . This  $x$  is denoted  $b/a$  and is called the **quotient** of  $b$  and  $a$

- T9:  $a \neq 0 \implies b/a = b \cdot a^{-1}$

- T10:  $a \neq 0 \implies (a^{-1})^{-1} = a$

- T11 (Zero Product Property):  $ab = 0 \implies a \vee b = 0$

- T12 (Rule for Multiplication with Negative Signs):

$$(-a)b = a(-b) = -(ab), (-a)(-b) = ab$$

$$\& -\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$$

- T13 (Equivalent Fractions Property):  $\frac{a}{b} = \frac{ac}{bc}; b, c \neq 0$

- T14 (Rule for Addition of Fractions):  $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}; b, d \neq 0$

- T15 (Rule for Multiplication of Fractions):

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, b \neq 0, d \neq 0$$

- T16 (Rule for Division of Fractions):

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}, b \neq 0, c \neq 0, d \neq 0$$

- T17 (Trichotomy Law):  $a < b, b < a$  or  $a = b, \forall a, b \in \mathbb{R}$

- T18 (Transitive Law):  $a < b, b < c \implies a < c$

- T19:  $a < b \implies a + c < b + c$

# CS1231: Number Theories

## Basics

- **Even & Odd** (Def 1.6.1, Proofs Handout, TS):

$$n \text{ is even} \iff \exists k \in \mathbb{Z} \text{ such that } n = 2k$$

$$n \text{ is odd} \iff \exists k \in \mathbb{Z} \text{ such that } n = 2k + 1$$

- **The sum of two even  $\mathbb{Z}$  is even** (Thm 4.1.1, Epp)

- **Rational Number**

$$r \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z}, r = \frac{a}{b} \text{ \& } b \neq 0$$

- **Every  $\mathbb{Z}$  is a rational number** (Thm 4.2.1, Epp)

- **The sum of any two rational numbers is rational** (Thm 4.2.2, Epp)

- **The double of a rational number is rational** (Col 4.2.3, Epp)

## Divisibility

- **Divisibility** (Def 1.3.1, PH):

$$d \mid n \iff \exists k \in \mathbb{Z}, \text{ s.t. } n = dk$$

- **Thm 4.1.1** (pg 4, Number Theory Week 4, TS) :  
 $\forall a, b, c \in \mathbb{Z}, \text{ if } a \mid b \text{ \& } a \mid c, \text{ then } \forall x, y \in \mathbb{Z}, a \mid (bx + cy)$

- **Thm 4.3.1** (Epp):  $\forall a, b \in \mathbb{Z}^+, \text{ if } a \mid b \text{ then } a \leq b$

- **Thm 4.3.2** (Epp):  $d \mid 1, d \text{ is only } 1, -1$

- **Thm 4.3.3** (Epp):  $\forall a, b, c \in \mathbb{Z}, \text{ if } a \mid b \text{ \& } b \mid c \text{ then } a \mid c$

- **Thm 4.3.4** (Epp): Any integer  $n > 1$  is divisible by a prime number

## Prime Numbers

- **Definition of Prime**

$$n \in \mathbb{Z} \text{ \& } n > 1 \text{ then,}$$

$$n \text{ is prime} \iff \forall r, s \in \mathbb{Z}^+, n = rs \rightarrow ((r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$$

$$n \text{ is composite} \iff \exists r, s \in \mathbb{Z}^+ \text{ s.t. } (n = rs) \wedge (1 < r < n \wedge 1 < s < n)$$

- **Proposition 4.2.2** (NTW4)

For any two primes  $p$  &  $p'$ , if  $p \mid p'$  then  $p = p'$

- **Proposition 4.7.3** (Epp)

For any  $a \in \mathbb{Z}$  and any prime  $p$ , if  $p \mid a$  then  $p \nmid (a + 1)$

- **The set of primes is infinite** (Thm 4.7.4, Epp)

- **Theorem 4.2.3** (pg 16, NTW4):

If  $p$  is prime and  $x_1, x_2, \dots, x_n$  are any integers s.t.:

$$p \mid x_1 x_2 \dots x_n,$$

then  $p \mid x_i$  for some  $x_i (1 \leq i \leq n)$

- **Unique Prime Factorization** (Thm 4.3.5, Epp):

Given any integer  $n > 1$ ,  $\exists k \in \mathbb{Z}^+$ , distinct primes  $p_1, p_2, \dots, p_k$  & positive integers  $e_1, e_2, \dots, e_k$ , s.t.

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_k^{e_k}$$

and any other exp for  $n$  as a product of prime numbers is identical to this (except ordering)

## Well Ordering Principle

- **Lower Bound** (Def 4.3.1, NTP2):

An integer  $b$  is said to be a **lower bound** for a set  $X \subseteq \mathbb{Z}$  if  $b \leq x$  for all  $x \in X$

- **Well Ordering Principle** (Thm 4.3.2, NTP2):

If a non-empty set  $S \subseteq \mathbb{Z}$  has a lower/upper bound, then  $S$  has a least/greatest element

- **Uniqueness of least element** (Prop 4.3.3, NTP2):

If a set  $S$  of integers has a least/greatest element, then the least/greatest element is unique

## Quotient-Remainder Theorem

- **Quotient-Remainder Theorem** (Thm 4.4.1, NTP2):

Given any  $a \in \mathbb{Z}$  and any  $b \in \mathbb{Z}^+$ , there exist unique integers  $q, r$  such that:

$$a = bq + r \text{ and } 0 \leq r < b$$

## GCD/LCM

- **Greatest Common Divisor** (Def 4.5.1, NTP2):

Let  $a, b$  be integers, not both zero. The **greatest common divisor** of  $a$  and  $b$ , denoted  $\gcd(a, b)$ , is the integer  $d$  satisfying:

$$(i) \ d \mid a \text{ and } d \mid b$$

$$(ii) \ \forall c \in \mathbb{Z}, \text{ if } c \mid a \text{ and } c \mid b, \text{ then } c \leq d$$

- **Existence of gcd** (Prop 4.5.2, NTP2):

For any integers  $a, b$ , not both zero, their gcd exists and is unique

- **Bézout's Identity** (Thm 4.5.3, NTP2):

Let  $a, b \in \mathbb{Z}$ , not both zero, and let  $d = \gcd(a, b)$ . Then, there exists  $x, y \in \mathbb{Z}$  such that:  $ax + by = d$

- **Relatively Prime/Coprime** (Def 4.5.4, NTP2):

Integers  $a, b$  are **(relatively prime)/coprime** iff  $\gcd(a, b) = 1$

- **Proposition 4.5.5** (NTP2):

For any  $a, b \in \mathbb{Z}$ , not both zero, if  $c$  is a common divisor of  $a$  and  $b$  then  $c \mid \gcd(a, b)$

- **Some Theorem** (NTP2):

$$\forall a, b \in \mathbb{Z}^+, a \mid b \iff \gcd(a, b) = a$$

- **Theorem in Assignment 1:**

$\forall a, b \in \mathbb{Z}$ , not both zero &  $d = \gcd(a, b)$ , then  $\frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$  with no common divisor that is greater than 1

- **Least Common Multiple** (Def 4.6.1, NTP2):

For any non-zero integers  $a, b$ , their **least common multiple**, denoted  $\text{lcm}(a, b)$ , is the positive integer  $m$  such that:

$$(i) \ a \mid m \text{ and } b \mid m$$

$$(ii) \ \forall c \in \mathbb{Z}^+, \text{ if } a \mid c \text{ and } b \mid c, \text{ then } m \leq c$$

- **Some other Theorem** (NTP2, last page):

$$\forall a, b \in \mathbb{Z}^+, \gcd(a, b) \mid \text{lcm}(a, b)$$

## Modulo Arithmetic

- **Congruence Modulo** (4.7.1, NTP3):

Let  $m, n \in \mathbb{Z}$  &  $d \in \mathbb{Z}^+$ .  $m$  is congruent to  $n$  modulo  $d$ :

$$m \equiv n \pmod{d} \iff d \mid (m - n)$$

- **Modular Equivalences** (8.4.1, Epp):

For  $a, b, n \in \mathbb{Z}, n > 1$ . Then the following are *equivalent*:

1.  $n \mid (a - b)$
2.  $a \equiv b \pmod{n}$
3.  $a = b + kn, k \in \mathbb{Z}$
4.  $a, b$  have same (non-negative) remainder when divided by  $n$
5.  $a \bmod n = b \bmod n$

- **Modulo Arithmetic** (8.4.3, Epp):

Let  $a, b, c, d, n \in \mathbb{Z}, n > 1$  and suppose:

$$a \equiv c \pmod{n} \text{ \& } b \equiv d \pmod{n}$$

Then

1.  $(a \pm b) \equiv (c \pm d) \pmod{n}$
2.  $ab \equiv cd \pmod{n}$
3.  $a^m \equiv c^m \pmod{n}, \forall m \in \mathbb{Z}^+$

- **Corollary 8.4.4** (Epp):

For  $a, b, c \in \mathbb{Z}, n > 1$ . Then,

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n}$$

If  $m \in \mathbb{Z}^+$ , then,

$$a^m \equiv [(a \bmod n)^m] \pmod{n}$$

- **Multiplicative inverse modulo  $n$**  (4.7.2, NTP3):

For  $a, n \in \mathbb{Z}, n > 1$ , if  $s \in \mathbb{Z}, as \equiv 1 \pmod{n}$ , then  $s$  is the **multiplicative inverse of  $a$  modulo  $n$** . We write inverse as  $a^{-1}$ .

Since commutative law applies in modulo,  $a^{-1}a \equiv 1 \pmod{n}$ .

- **Existence of multiplicative inverse** (4.7.3, NTP3):

For any  $a \in \mathbb{Z}$ , its multiplicative inverse mod  $n$  (where  $n > 1$ ),  $a^{-1}$ , exists iff,  $a, n$  are coprime

- **Corollary 4.7.4** ( $n$  is prime):

If  $n = p$  is prime, then all  $a \in \mathbb{Z}, 0 < a < p$  have multiplicative inverses mod  $p$

- **Cancellation Law** (8.4.9, Epp):

$\forall a, b, c, n \in \mathbb{Z}, n > 1$  and  $a, n$  coprime, if  $ab \equiv ac \pmod{n}$ , then  $b \equiv c \pmod{n}$

# CS1231: Sequences & Recursion

## Definitions

- **Sequences**

Denote a seq. of numbers by:  $a_0, a_1, a_2, \dots$   $a_n = f(n)$ , for some fn  $f$  and  $n \in \mathbb{N}$ . The indexing variable is  $n$ .

- **Recursion Relations**

Seq. relating  $a_n$  to its predecessors:  $a_{n-1}, a_{n-2}, \dots$

## Summation & Product

- **Summation:**

$$\sum_{i=m}^n a_i = a_m + a_{m+1} + \dots + a_{n-1} + a_n = S_n, \forall n \in \mathbb{N}$$

$$\sum_{i=m}^n a_i = \begin{cases} 0, & n < m \\ (\sum_{i=m}^{n-1} a_i) + a_n & \text{otherwise} \end{cases}$$

- **Product:**

$$\prod_{i=m}^n a_i = a_m \times a_{m+1} \times \dots \times a_{n-1} \times a_n = P_n, \forall n \in \mathbb{N}$$

$$\prod_{i=m}^n a_i = \begin{cases} 1, & n < m \\ (\prod_{i=m}^{n-1} a_i) \cdot a_n & \text{otherwise} \end{cases}$$

- **Theorem 5.1.1** (Epp):

If  $a_m, a_{m+1}, \dots$  and  $b_m, b_{m+1}, \dots$  are sequences of real numbers and for any  $c \in \mathbb{R}$ , then the following equations hold for any integer  $n \geq m$ :

$$1. \sum_{k=m}^n a_k + \sum_{k=m}^n b_k = \sum_{k=m}^n (a_k + b_k)$$

$$2. c \cdot \sum_{k=m}^n a_k = \sum_{k=m}^n c \cdot a_k \text{ (generalized distributive law)}$$

$$3. \left( \prod_{k=m}^n a_k \right) \cdot \left( \prod_{k=m}^n b_k \right) = \prod_{k=m}^n (a_k \cdot b_k)$$

## Common Sequences

- **Arithmetic Sequence** ( $a_n = a_{n-1} + d$ )

$$\forall n \in \mathbb{N}, a_n = \begin{cases} a, & \text{if } n = 0, \\ a_{n-1} + d, & \text{otherwise.} \end{cases}$$

*Explicit Formula:*

$$a_n = a + nd, \forall n \in \mathbb{N} \ \& \ a, r \in \mathbb{R}$$

*Closed Form:*

$$S_n = \frac{n}{2}[2a + (n-1)d], \forall n \in \mathbb{N} \ \& \ a, r \in \mathbb{R}$$

- **Geometric Sequence** ( $a_n = ra_{n-1}$ )

$$\forall n \in \mathbb{N}, a_n = \begin{cases} a, & \text{if } n = 0, \\ ra_{n-1}, & \text{otherwise.} \end{cases}$$

*Explicit Formula:*

$$a_n = ar^n, \forall n \in \mathbb{N} \ \& \ a, r \in \mathbb{R}$$

*Closed Form:*

$$S_n = \frac{a(r^n - 1)}{r - 1}, \forall n \in \mathbb{N}, a, r \in \mathbb{R}$$

- **Square Numbers** (sum of first  $n$  odd numbers)

*Explicit Formula:*  $\forall n \in \mathbb{N}, \square_n = n^2$

- **Triangle Numbers** (sum of first  $n+1$  integers)

*Explicit Formula:*  $\forall n \in \mathbb{N}, \triangle_n = \frac{n(n+1)}{2}$

*Interesting:*

$$\forall n \in \mathbb{Z}^+, \triangle_n + \triangle_{n-1} = \square_n = (\triangle_n - \triangle_{n-1})^2$$

- **Fibonacci Numbers**

$$\forall n \in \mathbb{N}, F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$$

*Explicit Formula:*

$$\forall n \in \mathbb{N}, F_n = \frac{\phi^n - (-\phi)^{-n}}{\sqrt{5}}$$

where  $\phi = (1 + \sqrt{5})/2$

## Solving Recurrences

- **Second-order Linear Homogeneous Recurrence Relation with Constant Coefficients** (Def 5.4.1, Slides)

**This** is a recurrence relation in the form:

$$a_k = Aa_{k-1} + Ba_{k-2}, \forall k \in \mathbb{Z}_{\geq k_0}$$

where  $A, B \in \mathbb{R}$  constants,  $B \neq 0$  and  $k_0 \in \mathbb{Z}$  constant

- **Distinct-Roots Theorem** (Thm 5.8.3, Epp):

Suppose a sequence  $a_0, a_1, a_2, \dots$  satisfies a recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for  $A, B \in \mathbb{R}$  constants, with  $B \neq 0$  and  $k \in \mathbb{Z}_{\geq 2}$ . If **characteristic equation**

$$t^2 - At - B = 0$$

has two distinct roots  $r$  &  $s$  then  $a_0, a_1, a_2, \dots$  is given by **explicit formula**

$$a_n = Cr^n + Ds^n, \forall n \in \mathbb{N}$$

where  $C, D \in \mathbb{R}$  as determined by initial conditions  $a_0, a_1$

- **Single-Roots Theorem** (Thm 5.8.5, Epp):

Suppose a sequence  $a_0, a_1, a_2, \dots$  satisfies a recurrence relation

$$a_k = Aa_{k-1} + Ba_{k-2}$$

for  $A, B \in \mathbb{R}$  constants, with  $B \neq 0$  and  $k \in \mathbb{Z}_{\geq 2}$ . If **characteristic equation**

$$t^2 - At - B = 0$$

has a single real root  $r$  then  $a_0, a_1, a_2, \dots$  is given by **explicit formula**

$$a_n = Cr^n + Dnr^n, \forall n \in \mathbb{N}$$

where  $C, D \in \mathbb{R}$  as determined by the value  $a_0$  and any other known value of the sequence

# CS1231: Sets

## Basics

- **Subset** (Def 6.1.1, Slides):  
 $S$  is **subset** of  $T$  ( $S$  is contained in  $T$ ,  $T$  contains  $S$ ) if all elements of  $S$  are elements of  $T$ . We write it as  $S \subseteq T$

- **Empty set** (Def 6.3.1, Slides):  
 Empty set has no element, denoted by  $\emptyset$  or  $\{\}$

- **Empty set is a subset of all sets** (6.2.4, Epp):  
 $\forall X \forall Z ((\forall Y \sim (Y \in X)) \rightarrow (X \subseteq Z))$

- **Set Equality** (Def 6.3.2, Slides):  
 Two sets are equal iff they have same elements in them

$$\forall X \forall Y ((\forall Z (Z \in X \leftrightarrow Z \in Y)) \leftrightarrow X = Y)$$

**N.B.** duplicates and order does not matter!

- **Prop 6.3.3:**  
 For any sets  $X, Y$ ;  $X \subseteq Y$  &  $Y \subseteq X$  iff,  $X = Y$ :

$$\forall X \forall Y ((X \subseteq Y \wedge Y \subseteq X) \leftrightarrow X = Y)$$

- **Empty Set is Unique** (Col 6.2.5, Epp):  
 $\forall X_1 \forall X_2, ((\forall Y (\sim (Y \in X_1)) \wedge (\forall Y \sim (Y \in X_2)) \rightarrow X_1 = X_2)$

- **Power Set** (Def 6.3.4, Slides):  
 Given set  $S$ , the **power set** of  $S$ , denoted  $\mathcal{P}(S)$  or  $2^S$ , is the set whose elements are all the subsets of  $S$ , nothing less and nothing more.  
 That is, given set  $S$ , if  $T = \mathcal{P}(S)$ , then

$$\forall X ((X \in T) \leftrightarrow (X \subseteq S))$$

- **No. of elements in Power Set** (Thm 6.3.1, Epp)  
 For all integers  $n \geq 0$ , if a set  $X$  has  $n$  elements, then  $\mathcal{P}(X)$  has  $2^n$  elements.

## Operation on Sets

- **Union** (Def 6.4.1):  
 Let  $S$  be a set of sets, then we say that  $T$  is the **union** of the sets in  $S$ :

$$T = \bigcup S = \bigcup_{X \in S} X$$

iff each element of  $T$  belongs to some set  $S$ , nothing less and nothing more. That is, given  $S, T$  is such that:

$$\forall Y ((Y \in T) \leftrightarrow \exists Z ((Z \in S) \wedge (Y \in Z)))$$

- **Proposition 6.4.2** (Slides):

- $\bigcup \emptyset = \bigcup_{A \in \emptyset} A = \emptyset$
- $\bigcup \{A\} = A$
- $A \cup B = B \cup A$  (commutative)
- $A \cup (B \cup C) = (A \cup B) \cup C$  (associative)
- $A \cup A = A$
- $A \subseteq B \leftrightarrow A \cup B = B$

- **Intersection** (Def 6.4.3, Slides):  
 Let  $S$  be a **non-empty set** of sets. The **intersection** of the sets in  $S$  is the set  $T$  whose elements belong to all the sets in  $S$ , nothing less and more:

$$\forall Y ((Y \in T) \leftrightarrow \forall Z ((Z \in S) \rightarrow (Y \in Z)))$$

We write it as:

$$T = \bigcap S = \bigcap_{X \in S} X$$

- **Proposition 6.4.4** (Slides):

- $A \cap \emptyset = \emptyset$
- $A \cap B = B \cap A$
- $A \cap (B \cap C) = (A \cap B) \cap C$  (associative)
- $A \subseteq B \leftrightarrow A \cap B = A$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

- **Disjoint** (Def 6.4.5, Slides):  
 $S, T$ , being two sets, are disjoint iff  $S \cap T = \emptyset$

- **Mutually disjoint** (Def 6.4.6, Slides):  
 Let  $V$  be set of sets. The sets  $T \in V$  are **mutually disjoint** iff every two distinct sets are disjoint.

$$\forall X, Y \in V (X \neq Y \rightarrow X \cap Y = \emptyset)$$

(e.g.  $V = \{\{1, 2\}, \{3\}, \{\{1\}, \{2\}\}\}$ )

- **Partition** (Def 6.4.7, Slides):  
 Let  $S$  be set and let  $V$  be a set of non-empty subsets of  $S$ .  $V$  is a **partition** of  $S$  iff

1. The sets in  $V$  are mutually disjoint
2. The union of the sets in  $V$  equals  $S$ .

- **Non-symmetric difference** (Def 6.4.8, Slides):  
 Let  $S, T$  be two sets. The **difference** (or relative complement) of  $S$  and  $T$ , denoted  $S - T$  is the set whose elements belong to  $S$  and do not belong to  $T$

$$\forall X (X \in S - T \iff (X \in S \wedge \sim (X \in T)))$$

- **Symmetric Difference** [XORing] (Def 6.4.9, Slides):  
 Let  $S, T$  be two sets. The **symmetric difference** of  $S$  and  $T$ , denoted  $S \oplus T$  is the set whose elements belong to  $S$  or  $T$  but not both

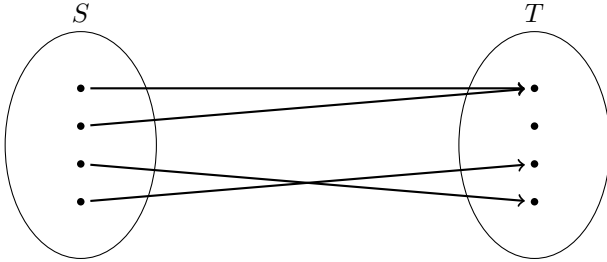
$$\forall X (X \in S \oplus T \leftrightarrow (X \in S \oplus X \in T))$$

- **Set Complement** (Def 6.4.10, Slides):  
 Let  $\mathcal{U}$  be the Universal set, let  $A \subseteq \mathcal{U}$ . Then, the complement of  $A$ , denoted  $A^c$ , is  $\mathcal{U} - A$ s

# CS1231: Functions

## Basics

- **Function** (Def 7.1.1, Slides):



Let  $f$  be a relation such that  $f \subseteq S \times T$ . Then  $f$  is **function** from  $S$  to  $T$  ( $f : S \rightarrow T$ )

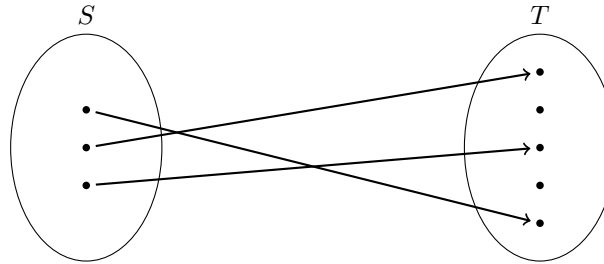
$$\forall x \in S, \exists! y \in T (x f y)$$

## Basic Function Definitions

- **Pre-image** (Def 7.1.2):  
Let  $f : S \rightarrow T$  be a function. Let  $x \in S$  and  $y \in T$  such that  $f(x) = y$ . Then,  $x$  is the **pre-image** of  $y$
- **Inverse image** (Def 7.1.3):  
Let  $f : S \rightarrow T$  be a function. Let  $y \in T$ . The **inverse image** of  $y$  is the set of all its pre-images:  $\{x \in S \mid f(x) = y\}$
- **Inverse image** (Def 7.1.4):  
Let  $f : S \rightarrow T$  be a function. Let  $U \subseteq T$ . The **inverse image** of  $U$  is the set that contains all the pre-images of all elements in  $U$ :  $\{x \in S \mid \exists y \in U, f(x) = y\}$
- **Restriction** (Def 7.1.5):  
Let  $f : S \rightarrow T$  be a function. Let  $U \subseteq S$ . The **restriction** of  $f$  to  $U$  is the set:  $\{(x, y) \in U \times T \mid f(x) = y\}$

## Properties of Functions

- **Injective/One-to-One** (Def 7.2.1, Slides):

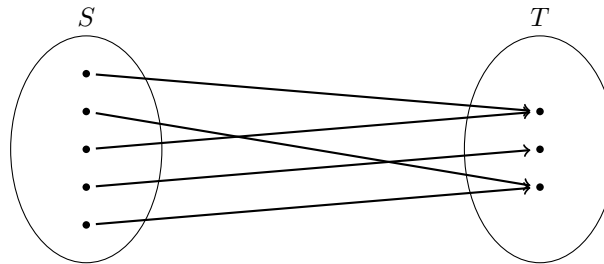


Let  $f : S \rightarrow T$  be a function.  $f$  is **injective** iff

$$\forall y \in T, \forall x_1, x_2 \in S ((f(x_1) = y \wedge f(x_2) = y) \rightarrow x_1 = x_2)$$

We can also say:  $f$  is an **injection** or **one-to-one** (i.e. every dot in  $T$  has **AT MOST** one incoming arrow)

- **Surjective/Onto** (Def 7.2.2, Slides):

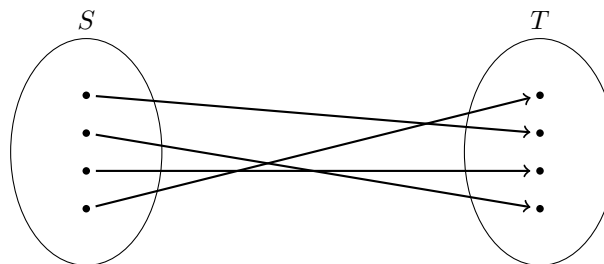


Let  $f : S \rightarrow T$  be a function.  $f$  is **surjective** iff

$$\forall y \in T, \exists x \in S (f(x) = y)$$

We can also say:  $f$  is a **surjection** or **onto** (i.e. every dot in  $T$  has **AT LEAST** one incoming arrow)

- **Bijective** (Def 7.2.3, Slides):



Let  $f : S \rightarrow T$  be a function.  $f$  is **bijective** iff  $f$  is both **injective** and **surjective**. We can also say:  $f$  is a **bijection**.

- **Inverse** (Prop 7.2.4, Slides):

Let  $f : S \rightarrow T$  be a function and  $f^{-1}$  be the inverse relation of  $f$  from  $T$  to  $S$ . Then,  $f$  is bijective iff  $f^{-1}$  is a function.

- **Composition** (Prop 7.3.1, Slides):

Let  $f : S \rightarrow T$  and  $g : T \rightarrow U$  be functions. The composition of  $f$  and  $g$ ,  $g \circ f$ , is a function from  $S$  to  $U$ .

- **Identity Function** (Def 7.3.2, Slides):

Given a set  $A$ , define function  $\mathcal{I}_A$  from  $A$  to  $A$  by:

$$\forall x \in A (\mathcal{I}_A(x) = x)$$

$\mathcal{I}_A$  is the **identity function** on  $A$

- **Composition of Inverse** (Prop 7.3.3, Slides):

Let  $f : A \rightarrow A$  be injective function on  $A$ . Thus,  $f^{-1} \circ f = \mathcal{I}_A$

## Generalization

- **(n-ary) operation** (Def 7.3.4, Slides):

An **(n-ary) operation** on a set  $A$  is a function  $f : \prod_{i=1}^n A \rightarrow A$ .  $n$  is called the **arity** or **degree** of the operation.

- **Unary operation** (Def 7.3.5, Slides):

A **unary operation** on a set  $A$  is a function  $f : A \rightarrow A$

- **Binary operation** (Def 7.3.6):

A **binary operation** on a set  $A$  is a function  $f : A \times A \rightarrow A$

# CS1231: Relations

## Basic Definitions

- **Ordered Pair** (Def 8.1.1):  
Let  $S$  be a non-empty set and let  $x, y \in S$ . The **ordered pair**, denoted  $(x, y)$ , is a mathematical object in which the first element is  $x$  and second element is  $y$ .

$$(x, y) = (a, b) \iff x = a, y = b$$

- **Ordered n-tuple** (Def 8.1.2)
- **Cartesian product** (Def 8.1.3):  
Let  $S, T$  be two sets. The **Cartesian product** (cross product) of  $S$  &  $T$ , denoted  $S \times T$ , is the set such that:

$$\forall X \forall Y ((X, Y) \in S \times T \leftrightarrow (X \in S) \wedge (Y \in T))$$

**N.B.** Cartesian product is **NOT** commutative nor associative and size of  $S \times T$  = size of  $S$   $\times$  size of  $T$

- **Generalized Cartesian Product** (Def 8.1.4):  
If  $V$  is a set of sets, the Generalized Cartesian product of its elements is:

$$\prod_{S \in V} S$$

- **Binary relations** (Def 8.2.1):  
Let  $S, T$  be two sets. A **binary relation** from  $S$  to  $T$ , denoted  $\mathcal{R}$ , is a subset of the Cartesian product  $S \times T$

**N.B.**  $s \mathcal{R} t$  is  $(s, t) \in \mathcal{R}$  and  $s \not\mathcal{R} t$  is  $(s, t) \notin \mathcal{R}$

## Properties of Binary Relations

Let  $\mathcal{R} \subseteq S \times T$  be a binary relation from  $S$  to  $T$

- **Domain** (Def 8.2.2):  
The **domain** of  $\mathcal{R}$  is the set

$$\text{Dom}(\mathcal{R}) = \{s \in S \mid \exists t \in T (s \mathcal{R} t)\}$$

- **Image** (Def 8.2.3):  
The **image** of  $\mathcal{R}$  is the set

$$\text{Im}(\mathcal{R}) = \{t \in T \mid \exists s \in S (s \mathcal{R} t)\}$$

- **Co-domain** (Def 8.2.4):  
The **co-domain** (range) of  $\mathcal{R}$  is the set

$$\text{coDom}(\mathcal{R}) = T$$

- **Inverse** (Def 8.2.6):  
Let  $S, T$  be sets and  $\mathcal{R} \subseteq S \times T$  be a binary relation. The **inverse** of the relation  $\mathcal{R}$ , denoted  $\mathcal{R}^{-1}$ , is the relation from  $T$  to  $S$  such that:

$$\forall s \in S, \forall t \in T (t \mathcal{R}^{-1} s \leftrightarrow s \mathcal{R} t)$$

- **n-ary relation** (Def 8.2.7):  
Let  $S_i$ , for  $i = 1$  to  $n$ , be  $n$  sets. An **n-ary relation** on the sets  $S_i$ , denoted  $\mathcal{R}$ , is a subset of the Cartesian product  $\prod_{i=1}^n S_i$ . We call  $n$  the **arity** or **degree** of the relation.

- **Composition** (Def 8.2.8):  
Let  $S, T, U$  be sets. Let  $\mathcal{R} \subseteq S \times T$  be a relation. Let  $\mathcal{R}' \subseteq T \times U$  be a relation. The composition of  $\mathcal{R}$  with  $\mathcal{R}'$ , denoted  $\mathcal{R} \circ \mathcal{R}'$ , is the relation from  $S$  to  $U$  such that:

$$\forall X \in S, \forall z \in U (x \mathcal{R}' \circ \mathcal{R} z \leftrightarrow (\exists y \in T (x \mathcal{R} y \wedge y \mathcal{R}' z)))$$

- **Associativity of Composition** (Prop 8.2.9):  
Let  $S, T, U, V$  be sets. Let  $\mathcal{R} \subseteq S \times T$ ,  $\mathcal{R}' \subseteq T \times U$ ,  $\mathcal{R}'' \subseteq U \times V$  be relations. Therefore,

$$\mathcal{R}'' \circ (\mathcal{R}' \circ \mathcal{R}) = (\mathcal{R}'' \circ \mathcal{R}') \circ \mathcal{R} = \mathcal{R}'' \circ \mathcal{R}' \circ \mathcal{R}$$

- **Proposition 8.2.10:**  
Let  $S, T, U$  be sets. Let  $\mathcal{R} \subseteq S \times T$  and  $\mathcal{R}' \subseteq T \times U$  be relations.

$$(\mathcal{R}' \circ \mathcal{R})^{-1} = \underbrace{\mathcal{R}^{-1} \circ \mathcal{R}'^{-1}}_{\text{reversed order}}$$

## Properties of Relations on a Set

Let  $A$  be a set and  $\mathcal{R} \subseteq A \times A$  be a relation. We say that  $\mathcal{R}$  is a **relation on  $A$** .

- **Reflexive** (Def 8.3.1)  
 $\mathcal{R}$  is **reflexive**  $\iff \forall x \in A, (x \mathcal{R} x)$

- **Symmetric** (Def 8.3.2)  
 $\mathcal{R}$  is **symmetric**  $\iff \forall x, y \in A, (x \mathcal{R} y \rightarrow y \mathcal{R} x)$

- **Anti-Symmetric** (Def 8.6.1)  
 $\mathcal{R}$  is **anti-symmetric**  $\iff \forall x, y \in A, ((x \mathcal{R} y \wedge y \mathcal{R} x) \rightarrow x = y)$

- **Asymmetric** (Tutorial 7)  
 $\mathcal{R}$  is **asymmetric**  $\iff \forall x, y \in A, (x \mathcal{R} y \rightarrow y \not\mathcal{R} x)$

- **Transitive** (Def 8.3.3)  
 $\mathcal{R}$  is **transitive**  $\iff \forall x, y, z \in A, ((x \mathcal{R} y \wedge y \mathcal{R} z) \rightarrow x \mathcal{R} z)$

- **Equivalence Relations** (Def 8.3.4):  
Let  $\mathcal{R}$  be a relation on set  $A$ .  
 $\mathcal{R}$  is called an **equivalence relation** iff  $\mathcal{R}$  is reflexive, symmetric and transitive.

- **Equivalence Class** (Def 8.3.5):  
Let  $x \in A$  and  $\mathcal{R}$  be an equivalence relation on  $A$ . The **equivalence class** of  $x$ , denoted  $[x]$  is the set of all elements  $y \in A$  that are in relation with  $x$ .

$$[x] = \{y \in A \mid x \mathcal{R} y\}$$

- **Partition induced by an equivalence relation** (Thm 8.3.4, Epp):  
Let  $\mathcal{R}$  be an equivalence relation on a set  $A$ . Then, the set of distinct equivalence classes form a partition of  $A$ .

- Lemma 8.3.2, Epp:  
Let  $\mathcal{R}$  be an equivalence relation on a set  $A$  and let  $a, b$  be two elements in  $A$ . If  $a \mathcal{R} b$  then  $[a] = [b]$

- Lemma 8.3.3, Epp:  
If  $\mathcal{R}$  is an equivalence relation on a set  $A$  and  $a, b$  are elements in  $A$ , then, either  $[a] \cap [b] = \emptyset$  or  $[a] = [b]$ .

- **Equivalence relation induced by a partition** (Thm 8.3.1, Epp):  
Given a partition  $S_1, S_2, \dots$  of a set  $A$ , there exists an equivalence relation  $\mathcal{R}$  on  $A$  whose equivalence classes make up precisely that partition.



## Additional Definitions

- **Transitive closure** (Def 8.5.1)

Let  $A$  be a set,  $\mathcal{R}$  be a relation on  $A$ . The **transitive closure** of  $\mathcal{R}$ , denoted  $\mathcal{R}^t$  is a relation that satisfies these three properties:

1.  $\mathcal{R}^t$  is transitive
2.  $\mathcal{R} \subseteq \mathcal{R}^t$
3. If  $\mathcal{S}$  is any other transitive relation such that  $\mathcal{R} \subseteq \mathcal{S}$ , then  $\mathcal{R}^t \subseteq \mathcal{S}$

- **Repeated compositions**

Let  $\mathcal{R}$  be a relation on a set  $A$ . We adopt the following notation for the composition of  $\mathcal{R}$  with itself:

1. We define  $\mathcal{R}^1 \triangleq \mathcal{R}$
2. We define  $\mathcal{R}^2 \triangleq \mathcal{R} \circ \mathcal{R}$
3. We define  $\mathcal{R}^n \triangleq \underbrace{\mathcal{R} \circ \dots \circ \mathcal{R}}_n = \bigodot_{i=1 \text{ to } n} \mathcal{R}$

- **Proposition 8.5.2**

Let  $\mathcal{R}$  be a relation on set  $A$ . Then

$$\mathcal{R}^t = \bigcup_{i=1}^{\infty} \mathcal{R}^i$$

## Partial & Total Orders

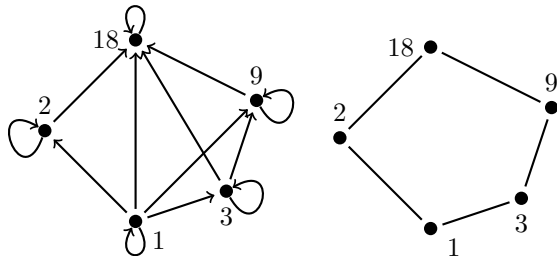
- **Partial Order** (Def 8.6.2)

$\mathcal{R}$  is said to be a **partial order** iff it is reflexive, anti-symmetric and transitive

**N.B.** Partial order is denoted by  $\preceq$  (note the curl)

- **Hasse Diagrams**

To convert from left diagram to right diagram:



**N.B.** Only works for partially ordered sets!

## Converting to Hasse:

1. Draw the directed graph so that all arrows point upwards
2. Eliminate all self-loops
3. Eliminate all arrows implied by the transitive property
4. Remove the direction of the arrows

- **Comparable** (Def 8.6.3)

Let  $\preceq$  be a partial order on a set  $A$ . Elements  $a, b \in A$  are **comparable** iff either  $a \preceq b$  or  $b \preceq a$ . Otherwise,  $a, b$  are **noncomparable**.

- **Total Order** (Def 8.6.4)

Let  $\preceq$  be a partial order on a set  $A$ .  $\preceq$  is a **total order** iff

$$\forall x, y \in A (x \preceq y \vee y \preceq x)$$

i.e.  $\preceq$  is a total order if  $\preceq$  is a partial order and all  $x, y$  are comparable

- **Maximal** (Def 8.6.5)

An element  $x$  is a **maximal element** iff

$$\forall y \in A, (x \preceq y \rightarrow x = y)$$

- **Maximum** (Def 8.6.6)

An element, usually noted  $\top$ , is the **maximum element** iff

$$\forall x \in A, (x \preceq \top)$$

- **Minimal** (Def 8.6.7)

An element  $x$  is a **minimal element** iff

$$\forall y \in A, (y \preceq x \rightarrow x = y)$$

- **Minimum** (Def 8.6.8)

An element, usually noted  $\perp$ , is the **minimum element** iff

$$\forall x \in A, (\perp \preceq x)$$

- **Well Ordering of Total Orders** (Def 8.6.9)

Let  $\preceq$  be a total order on a set  $A$ .  $A$  is **well ordered** iff every non-empty subset of  $A$  contains a minimum element

$$\forall S \in \mathcal{P}(A) (S \neq \emptyset \rightarrow (\exists x \in S, \forall y \in S, (x \preceq y)))$$

# CS1231: Counting & Probability

## Basic Definition

- **Sample Space & Event**

A **sample space** is the set of all possible outcomes of a random process or experiment. An **event** is a subset of a sample space.

- **Equally Likely Probability Formula**

If  $S$  is a finite sample space in which all outcomes are **equally likely** &  $E$  is an event in  $S$ , then the **probability** of  $E$ , denoted  $P(E)$  is

$$P(E) = \frac{\text{No. of outcomes in } E}{\text{Total no. of outcomes in } S} = \frac{N(E)}{N(S)}$$

- **Probability of the Complement of an Event**

If  $S$  is a finite sample space and  $A$  is an event in  $S$ , then  $P(A^c) = 1 - P(A)$

- **Number of Elements in a List** (Thm 9.1.1)

If  $m, n \in \mathbb{Z}$  and  $m \leq n$ , then there are  $(n - m) + 1$  integers from  $m$  to  $n$  inclusive

- **Multiplication Rule** (Thm 9.2.1)

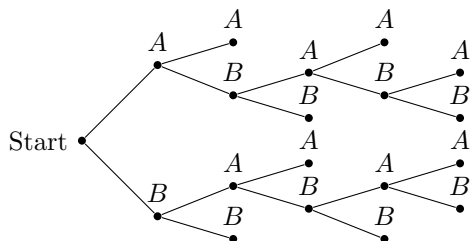
If an operation consists of  $k$  steps and the first step can be preformed in  $n_1$  ways the second step can be performed in  $n_2$  ways (regardless of how first step was performed)

$\vdots$

the  $k$ th step can be performed in  $n_k$  ways (regardless of how preceding steps was performed)

Then, the entire operation can be performed in  $n_1 \times n_2 \times \dots \times n_k$  ways

## Possibility Tree



- **Possible Ways in Tree**

**Possible ways** are represented by the distinct paths from "root" (start) to "leaf" (terminal point) in the tree

## Permutation

- **Definition**

A **permutation** of a set of objects is an ordering of the objects in a row.

- **No of Permutations** (Thm 9.2.2)

The **number of permutations** of a set with  $n$  ( $n \geq 1$ ) elements is  $n!$

- **r-permutation**

An **r-permutation** of a set of  $n$  elements is an ordered selection of  $r$  elements taken from the set. The number of  $r$ -permutations of a set of  $n$  elements is denoted  $P(n, r)$

- **r-permutations from a set of n elements** (Thm 9.2.3)

If  $n, r \in \mathbb{Z}$  and  $1 \leq r \leq n$ , then the **number of r-permutations of a set of n elements** is given by the formula

$$P(n, r) = n(n - 1) \dots (n - r + 1)$$

or, equivalently

$$P(n, r) = \frac{n!}{(n - r)!}$$

## Counting Elements of Sets

- **Addition Rule** (Thm 9.3.1)

Suppose a finite set  $A$  equals the union of  $k$  distinct mutually disjoint subsets  $A_1, A_2, \dots, A_k$ . Then,  $N(A) = N(A_1) + N(A_2) + \dots + N(A_k)$

- **Difference Rule** (Thm 9.3.2)

If  $A$  is a finite set and  $B$  is a subset of  $A$ , then  $N(A - B) = N(A) - N(B)$

- **Inclusion-Exclusion rule for 2 or 3 sets** (Thm 9.3.3)

If  $A, B, C$  are any finite sets, then

$$N(A \cup B) = N(A) + N(B) - N(A \cap B)$$

and

$$N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$$

## Pigeonhole Principle

- **Pigeonhole Principle**

A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least 2 elements in the domain that have the same image in the co-domain

- **Pigeonhole Principle** (Thm 9.4.1)

For any function  $f$  from a finite set  $X$  with  $n$  elements to a finite set  $Y$  with  $m$  elements, if  $n > m$ , then  $f$  is not one-to-one.

- **One-to-one and Onto for Finite Sets**

Let  $X, Y$  be finite sets with the same number of elements and suppose  $f$  is a function from  $X$  to  $Y$ . Then  $f$  is one-to-one iff  $f$  is onto.

- **Generalised Pigeonhole Principle**

For any function  $f$  from a finite set  $X$  with  $n$  elements to a finite set  $Y$  with  $m$  elements and for any  $k \in \mathbb{Z}^+$ , if  $k < n/m$ , then there is some  $y$  in  $Y$  such that  $y$  is the image of at least  $k + 1$  distinct elements of  $X$ .

- **Contrapositive Form of GPP**

For any function  $f$  from a finite set  $X$  with  $n$  elements to a finite set  $Y$  with  $m$  elements and for any  $k \in \mathbb{Z}^+$ , if for each  $y \in Y$ ,  $f^{-1}(y)$  has at most  $k$  elements, then  $X$  has at most  $km$  elements, i.e.,  $n \leq km$

## Combinations

- **r-combination**

Let  $n, r$  be non-negative integers with  $r \leq n$ . An **r-combination** of a set of  $n$  elements is a subset of  $r$  of the  $n$  elements.  $\binom{n}{r}$ , denotes the no. of subsets of size  $r$ , that can be chosen from a set of  $n$  elements.

- **Formula for  $\binom{n}{r}$**  (Thm 9.5.1)

The no. of subsets of size  $r$  (r-combinations) that can be chosen from a set of  $n$  elements,  $\binom{n}{r}$ , is given by the formula

$$\binom{n}{r} = \frac{P(n, r)}{r!}$$

or, equivalently

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

where  $n, r$  are non-negative integers with  $r \leq n$ .

- **Permutations with sets of indistinguishable objects** (Thm 9.5.2)

Suppose a collection consists of  $n$  objects of which

$n_1$  of type 1 & are indistinguishable from each other

$n_2$  of type 2 & are indistinguishable from each other

$\vdots$

$n_k$  of type  $k$  & are indistinguishable from each other

and suppose that  $n_1 + n_2 + \dots + n_k = n$ . Then, the **no. of distinguishable permutations** of the  $n$  objects is

$$\binom{n}{n_1} \binom{n-n_1}{n_2} \dots \binom{n-n_1-n_2-\dots-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!\dots n_k!}$$

- **No. of Partitions of a Set into r subsets**

(Stirling numbers of the Second Kind)

$S_{n,r}$  = no. of ways a set of size  $n$  can be partitioned into  $r$  subsets

- **r-combination with repetition**

An **r-combination with repetition allowed**, or **multiset of size r**, chosen from a set  $X$  of  $n$  elements is an

unordered selection of elements taken from  $X$  with repetition allowed. If  $X = \{x_1, x_2, \dots, x_n\}$ , we write an  $r$ -combination with repetition allowed as  $[x_{i_1}, x_{i_2}, \dots, x_{i_r}]$  where each  $x_{i_j}$  is in  $X$  and some of the  $x_{i_j}$  may equal each other

- **No. of r-combinations with repetition** (Thm 9.6.1)  
The **no. of r-combination with repetition allowed** (multisets of size  $r$ ) that can be selected from a set of  $n$  elements is

$$\binom{r+n-1}{r}$$

This equals the number of ways  $r$  objects can be selected from  $n$  categories of objects with repetitions allowed

- **Pascal's Formula** (Thm 9.7.1)  
Suppose  $n, r \in \mathbb{Z}^+$  &  $r \leq n$ . Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

- **Binomial Theorem** (Thm 9.7.2)

Given any  $a, b \in \mathbb{R}$  and any non-negative integer  $n$ ,

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k = a^n + \binom{n}{1} a^{n-1} b^1 + \dots + \binom{n}{n-1} a^1 b^{n-1} + b^n$$

## Probability

- **Probability Axioms**

Let  $S$  be a sample space. A **probability function**  $P$  from the set of all events in  $S$  to the set of real numbers satisfies the following axioms: For all events  $A$  and  $B$  in  $S$ ,

1.  $0 \leq P(A) \leq 1$
2.  $P(\emptyset) = 0$  and  $P(S) = 1$
3. If  $A$  and  $B$  are disjoint ( $A \cap B = \emptyset$ ), then  $P(A \cup B) = P(A) + P(B)$

- **Probability of a General Union of Two Events**

If  $A$  and  $B$  are any events in a sample space  $S$ , then  $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

- **Expected Value**

Suppose the possible outcomes of an experiment, or random process, are real numbers  $a_1, a_2, \dots, a_n$  which occur with probabilities  $p_1, p_2, \dots, p_n$ . The **expected value** of the process is

$$\sum_{k=1}^n a_k p_k = a_1 p_1 + a_2 p_2 + \dots + a_n p_n$$

- **Conditional Probability**

Let  $A$  and  $B$  be events in a sample space  $S$ . If  $P(A) \neq 0$ , then the **conditional probability of B given A**, denoted  $P(B | A)$  is

$$P(B | A) = \frac{P(A \cap B)}{P(A)}$$

- **Bayes' Theorem** (Thm 9.9.1)

Suppose that a sample space  $S$  is a union of mutually disjoint events  $B_1, B_2, \dots, B_n$ .

Suppose  $A$  is an event in  $S$ , and suppose  $A$  and all the  $B_i$  have non-zero probabilities.

If  $k \in \mathbb{Z}$  with  $1 \leq k \leq n$ , then

$$P(B_k | A) = \frac{P(A | B_k) \cdot P(B_k)}{P(A | B_1) \cdot P(B_1) + \dots + P(A | B_n) \cdot P(B_n)}$$

- **Independent Events**

If  $A, B$  are events in a sample space  $S$ , then  $A$  and  $B$  are **independent** iff  $P(A \cap B) = P(A) \cdot P(B)$

- **Pairwise/Mutually Independent**

Let  $A, B, C$  be events in a sample space  $S$ .  $A, B, C$  are **pairwise independent**, iff, they satisfy conditions 1 - 3 below. They are **mutually independent**, if, they satisfy all four conditions below.

1.  $P(A \cap B) = P(A) \cdot P(B)$
2.  $P(A \cap C) = P(A) \cdot P(C)$
3.  $P(B \cap C) = P(B) \cdot P(C)$
4.  $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

- **Generalised Mutually Independent Definition**

Events  $A_1, A_2, \dots, A_n$  in a sample space  $S$  are **mutually dependent** iff the probability of the intersection of any subset of the events is the product of the probabilities of the events in the subset

# CS1231: Graphs

## Basic Definitions

- **Graph**

A **graph**  $G$  consists of 2 finite sets: a nonempty set  $V(G)$  of **vertices** and a set  $E(G)$  of **edges**, where each edge is associated with a set consisting of either one or two vertices called its **endpoints**.

A edge is said to **connect** its endpoints; two vertices that are connected by an edge are called **adjacent vertices**; and a vertex that is an endpoint of a loop is said to be **adjacent to itself**.

An edge is said to be **incident on** each of its endpoints, and two edges incident on the same endpoint are called **adjacent edges**.

We write  $e = \{v, w\}$  for an edge  $e$  incident on vertices  $v$  and  $w$ .

- **Directed Graph**

A **directed graph**, or **digraph**,  $G$ , consists of 2 finite sets: a nonempty set  $V(G)$  of **vertices** and a set  $D(G)$  of **directed edges**, where each edge is associated with an ordered pair of vertices called its endpoints.

If edge  $e$  is associated with the pair  $(v, w)$  of vertices, then  $e$  is said to be the **(directed) edge** from  $v$  to  $w$ . We write  $e = (v, w)$ .

- **Simple Graph**

A **simple graph** is a undirected graph that does **not** have any loops or parallel edges.

- **Complement of Simple Graph** (Tutorial 10)

If  $G$  is a simple graph, the complement of  $G$ , denoted  $G'$ , is obtained as follows: The vertex set of  $G'$  is identical to the vertex set of  $G$ . However, two distinct vertices  $v$  and  $w$  of  $G'$  are connected by an edge iff  $v$  &  $w$  are not connected by an edge in  $G$ .

- **Complete Graph**

A **complete graph** on  $n$  vertices,  $n > 0$ , denoted  $K_n$ , is a simple graph with  $n$  vertices and exactly one edge connecting each pair of distinct vertices.

- **Subgraph of a Graph**

A graph  $H$  is said to be a **subgraph** of graph  $G$ , iff, every vertex in  $H$  is also a vertex in  $G$ , every edge in  $H$  is also an edge in  $G$ , and every edge in  $H$  has the same endpoints as it has in  $G$ .

- **Complete Bipartite Graphs**

A **complete bipartite graph** on  $(m, n)$  vertices, where  $m, n > 0$ , denoted  $K_{m,n}$ , is a simple graph with distinct vertices  $v_1, v_2, \dots, v_m$  and  $w_1, w_2, \dots, w_n$  that satisfies the following properties:

For all  $i, k = 1, 2, \dots, m$  and for all  $j, l = 1, 2, \dots, n$ ,

1. There is an edge from each vertex  $v_i$  to each vertex  $w_j$
2. There is no edge from any vertex  $v_i$  to any other vertex  $v_k$
3. There is no edge from any vertex  $w_j$  to any other vertex  $w_l$

- **Degree of a Vertex and Total Degree of a Graph**

Let  $G$  be a graph and  $v$  a vertex of  $G$ . The **degree** of  $v$ , denoted  $\deg(v)$ , equals the number of edges that are **incident on**  $v$ , with an edge that is a loop counted twice.

The **total degree of**  $G$  is the sum of the degrees of all the vertices of  $G$ .

- **Handshake Theorem** (Thm 10.1.1)

If  $G$  is any graph, then the sum of the degrees of all the vertices of  $G$  equals twice the number of edges of  $G$ . Specifically, if the vertices of  $G$  are  $v_1, v_2, \dots, v_n$ , where  $n \geq 0$ , then

$$\begin{aligned} \text{Total degree of } G &= \deg(v_1) + \deg(v_2) + \dots + \deg(v_n) \\ &= 2 \cdot (\text{the no. of edges of } G) \end{aligned}$$

- **Corollary 10.1.2**

The total degree of a graph is **even**

- **Proposition 10.1.3**

In any graph there are an even number of vertices of odd degree

## Trails, Paths and Circuits

Let  $G$  be a graph and let  $v, w$  be vertices of  $G$ .

- **Walk**

A **walk from**  $v$  **to**  $w$  is a finite alternating sequence of adjacent vertices and edges of  $G$ . Thus, a walk has the form

$$v_0 e_1 v_1 e_2 \dots v_{n-1} e_n v_n$$

where the  $v$ 's represent vertices, the  $e$ 's represent edges,  $v_0 = v, v_n = w$  and for all  $i \in \{1, 2, \dots, n\}$ ,  $v_{i-1}$  and  $v_i$  are the endpoints of  $e_i$

- **Trivial Walk**

A **trivial walk** from  $v$  to  $v$  consists of the single vertex  $v$

- **Trail**

A **trail from**  $v$  **to**  $w$  is a walk from  $v$  to  $w$  that does not contain a repeated edge

- **Path**

A **path from**  $v$  **to**  $w$  is a trail that does not contain a repeated vertex

- **Closed Walk**

A **closed walk** is a walk that starts and ends at the same vertex

- **Circuit/Cycle**

A **circuit/cycle** is a **closed walk** that contains at least one edge and does not contain a repeated edge

- **Simple Circuit/Cycle**

A **simple circuit/cycle** is a circuit that does not have any other repeated vertex except first and last

- **Triangle**

A simple circuit of **length three** is called a triangle

- **Connectedness**

Vertices  $v$  and  $w$  in graph  $G$  are **connected** iff there is a walk from  $v$  to  $w$

- **Connected Graph**

The graph  $G$  is **connected**, iff, given any two vertices  $v$  and  $w$  in graph  $G$ , there is a walk from  $v$  to  $w$

- **Lemma on Connectedness**

Let  $G$  be a graph

1. If  $G$  is connected, then any two distinct vertices in  $G$  can be connected by a path
2. If vertices  $v$  and  $w$  are part of a circuit in  $G$  and one edge is removed from the circuit, then there still exists a trail from  $v$  to  $w$  in  $G$
3. If  $G$  is connected and  $G$  contains a circuit, then an edge of the circuit can be removed without disconnecting  $G$

- **Connected Component**

A graph  $H$  is a **connected component** of a graph  $G$  iff,

1. The graph  $H$  is a subgraph of  $G$
2. The graph  $H$  is connected
3. No connected subgraph of  $G$  has  $H$  as a subgraph and contains vertices or edges that are not in  $H$

## Euler Circuits

- **Euler Circuit**

Let  $G$  be a graph. An **Euler circuit** for  $G$  is a circuit that contains every vertex and every edge of  $G$ .

That is, an **Euler circuit** for  $G$  is a sequence of adjacent vertices and edges in  $G$  that has at least one edge, starts and ends at the same vertex, uses every vertex of  $G$  at least once, and uses every edge of  $G$  exactly once.

- **Theorem 10.2.2**

If a graph is an Euler circuit, then every vertex of the graph has positive even degree

- **Contrapositive of 10.2.2**

If some vertex of a graph has odd degree, then the graph does not have an Euler circuit

- **Theorem 10.2.3**

If a graph  $G$  is **connected** and the degree of every vertex of  $G$  is a **positive even integer**, then  $G$  has an Euler circuit

- **Theorem 10.2.4: USE THIS FOR EULER**

A graph  $G$  has an Euler circuit  $\iff G$  is connected and every vertex of  $G$  has positive even degree

- **Euler Trail**

Let  $G$  be a graph, and let  $v$  and  $w$  be two distinct vertices of  $G$ . An **Euler trail/path from  $v$  to  $w$**  is a sequence of adjacent edges and vertices that starts at  $v$ , ends at  $w$ , passes through every vertex of  $G$  at least once, and traverses every edge of  $G$  exactly once.

- **Corollary 10.2.5**

Let  $G$  be a graph and let  $v$  and  $w$  be two distinct vertices of  $G$ . There is an Euler trail from  $v$  to  $w$   $\iff G$  is connected,  $v$  and  $w$  have odd degree, and all other vertices of  $G$  have positive even degree.

## Hamiltonian Circuits

- **Hamiltonian Circuit**

Given a graph  $G$ , a **Hamiltonian circuit** for  $G$  is a simple circuit that includes every vertex of  $G$ .

That is, a Hamiltonian circuit for  $G$  is a sequence of adjacent vertices and distinct edges in which every vertex of  $G$  appears exactly once, **except for the first and last**, which are the same.

**N.B.** Hamiltonian circuit does not have to use all edges, but since it is a circuit, it cannot use the same edge more than once.

- **Proposition 10.2.6**

If a graph  $G$  has a Hamiltonian circuit, then  $G$  has a subgraph  $H$  with the following properties:

1.  $H$  contains every vertex of  $G$
2.  $H$  is connected
3.  $H$  has the same number of edges as vertices
4. Every vertex of  $H$  has degree 2

## Matrix Representation of Graphs

- **Matrix**

An  $m \times n$  **matrix**  $A$  over a set  $S$  is a rectangular array of elements of  $S$  arranged into  $m$  rows and  $n$  columns

- **Adjacency Matrix of a Directed Graph**

Let  $G$  be a directed graph with ordered vertices  $v_1, v_2, \dots, v_n$ . The **adjacency matrix of  $G$**  is the  $n \times n$  matrix  $\mathbf{A} = (a_{ij})$  over the set of non-negative integers such that

$$a_{ij} = \text{the number of arrows from } v_i \text{ to } v_j$$

for all  $i, j = 1, 2, \dots, n$ .

- **Adjacency Matrix of an Undirected Graph**

let  $G$  be an undirected graph with ordered vertices  $v_1, v_2, \dots, v_n$ . The **adjacency matrix of  $G$**  is the  $n \times n$  matrix  $\mathbf{A} = (a_{ij})$  over the set of non-negative integers such that

$$a_{ij} = \text{the number of edges connecting } v_i \text{ and } v_j$$

for all  $i, j = 1, 2, \dots, n$ .

- **Symmetric Matrix**

An  $n \times n$  square matrix  $\mathbf{A} = (a_{ij})$  is called **symmetric**  $\iff$  for all  $i, j = 1, 2, \dots, n$

$$a_{ij} = a_{ji}$$

(i.e. mirror image along main diagonal)

- **Theorem 10.3.1**

Let  $G$  be a graph with connected components  $G_1, G_2, \dots, G_k$ . If there are  $n_i$  vertices in each connected component  $G_i$  and these vertices are numbered consecutively, then the adjacency matrix of  $G$  has the form:

$$\begin{bmatrix} A_1 & O & O & & O & O \\ O & A_2 & O & \dots & O & O \\ O & O & A_3 & & O & O \\ & \vdots & & & \vdots & \vdots \\ O & O & O & \dots & O & A_k \end{bmatrix}$$

where each  $A_i$  is  $n_i \times n_i$  adjacency matrix of  $G_i$  for all  $i = 1, 2, \dots, k$ , and the  $O$ 's represent matrices whose entries are all 0s

- **Scalar Product**

Suppose that all entries in matrices  $\mathbf{A}$  and  $\mathbf{B}$  are real numbers. If the number of elements,  $n$ , in the  $i$ th row of  $\mathbf{A}$  equals the number of elements in the  $j$ th column of  $\mathbf{B}$ , then the **scalar product** or **dot product** of the  $i$ th row of  $\mathbf{A}$  and the  $j$ th column of  $\mathbf{B}$  is the real number obtained as follows

$$\begin{bmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{bmatrix} \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{bmatrix} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}$$

- **Matrix Multiplication**

Let  $\mathbf{A} = (a_{ij})$  be an  $m \times k$  matrix and  $\mathbf{B} = (b_{ij})$  an  $k \times n$  matrix with real entries. The (matrix) product of  $\mathbf{A}$  times  $\mathbf{B}$ , denoted  $\mathbf{AB}$ , is the matrix  $(c_{ij})$  defined as follows:

$$\begin{bmatrix} c_{11} & c_{12} & \dots & c_{1j} & \vdots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2j} & \vdots & c_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{i1} & c_{i2} & \dots & c_{ij} & \vdots & c_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{k1} & c_{k2} & \dots & c_{kj} & \vdots & c_{kn} \end{bmatrix}$$

where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{ik}b_{kj} = \sum_{r=1}^k a_{ir}b_{rj}$$

for all  $i = 1, 2, \dots, m$  and  $j = 1, 2, \dots, n$ .

- **Identity Matrix**

For each  $n \in \mathbb{Z}^+$ , the  $n \times n$  **identity matrix**, denoted  $\mathbf{I}_n = (\delta_{ij})$  or just  $\mathbf{I}$ , if the size of matrix is obvious from context, is the  $n \times n$  matrix in which all the entries in the main diagonal are 1's and all other entries are 0's. In other words,

$$\delta_{ij} = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{if } i \neq j \end{cases}$$

for all  $i, j = 1, 2, \dots, n$ .

- **Identity Matrix II**

For any  $n \times n$  matrix  $\mathbf{A}$ , the **powers of  $\mathbf{A}$**  are defined as follows:

$$\mathbf{A}^0 = \mathbf{I} \text{ where } \mathbf{I} \text{ is the } n \times n \text{ identity matrix}$$

$$\mathbf{A}^n = \mathbf{A}\mathbf{A}^{n-1} \text{ for all integers } n \geq 1$$

- **No. of walks in Adjacency Matrix** (Thm 10.3.2)

If  $G$  is a graph with vertices  $v_1, v_2, \dots, v_m$  and  $\mathbf{A}$  is the adjacency matrix of  $G$ , then for each  $n \in \mathbb{Z}^+$  and for all integers  $i, j = 1, 2, \dots, m$ , the  $ij$ -th entry of  $\mathbf{A}^n$  = the number of walks of length  $n$  from  $v_i$  to  $v_j$ .

## Isomorphisms of Graphs

- **Isomorphic Graph**

Let  $G$  and  $G'$  be graphs with vertex sets  $V(G)$  and  $V(G')$  and edge sets  $E(G)$  and  $E(G')$  respectively.  $G$  is **isomorphic to  $G'$**   $\iff$  there exist one-to-one correspondences  $g : V(G) \rightarrow V(G')$  and  $h : E(G) \rightarrow E(G')$  that preserve the edge-endpoint functions of  $G$  and  $G'$  in the sense that for all  $v \in V(G)$  and  $e \in E(G)$ ,

$$v \text{ is an endpoint of } e \iff g(v) \text{ is an endpoint of } h(e).$$

- **Graph Isomorphism is an Equivalence Relation** (Thm 10.4.1)

Let  $S$  be a set of graphs and let  $R$  be the relation of graph isomorphism on  $S$ . Then,  $R$  is an equivalence relation on  $S$ .

- **Self-Complementary Graph** (Tutorial 10)

A **self-complementary graph** is isomorphic with its complement

- **Invariant-ness**

A property  $P$  is called an **invariant** for graph isomorphism  $\iff$  given any graphs  $G$  and  $G'$ , if  $G$  has property  $P$  and  $G'$  is isomorphic to  $G$ , then  $G'$  has property  $P$ .

- **Invariants for Graph Isomorphism** (Thm 10.4.2)

Each of the following properties is an invariant for graph isomorphism, where  $n, m, k$  are all non-negative integers

1. has  $n$  vertices
2. has  $m$  edges
3. has a vertex of degree  $k$

4. has  $m$  vertices of degree  $k$
5. has a circuit of length  $k$
6. has a simple circuit of length  $k$
7. has  $m$  simple circuits of length  $k$
8. is connected
9. has an Euler circuit
10. has a Hamiltonian circuit

- **Graph Isomorphism for Simple Graphs**

If  $G$  and  $G'$  are simple graphs, then  $G$  is **isomorphic to  $G'$**   $\iff$  there exists a one-to-one correspondence  $g$  from vertex set  $V(G')$  of  $G'$  that preserves the edge-endpoint functions of  $G$  and  $G'$  in the sense that for all vertices  $u$  and  $v$  of  $G$ ,

$$\{u, v\} \text{ is an edge in } G \iff \{g(u), g(v)\} \text{ is an edge in } G'$$

# CS1231: Trees

## Basic Definition

- **Circuit-Free**  
A **graph** is said to be **circuit-free**  $\iff$  it has no circuits
- **Tree**  
A graph is said to be a **tree**  $\iff$  it is circuit-free and connected
- **Trivial Tree**  
A **trivial tree** is a graph that consists of a single vertex
- **Forest**  
A graph is called a **forest**  $\iff$  it is circuit-free and not connected
- **Minimum vertex of non-trivial tree** (Lem 10.5.1)  
Any non-trivial tree has at least one vertex of degree 1
- **Terminal vertex (leaf) & internal vertex**  
Let  $T$  be a tree. If  $T$  has only one or two vertices, then each is called a **terminal vertex** (or **leaf**). If  $T$  has at least three vertices, then a vertex of degree 1 in  $T$  is called a **terminal vertex** (or **leaf**), and a vertex of degree greater than 1 in  $T$  is called an **internal vertex**.
- **Theorem 10.5.2**  
Any tree with  $n$  vertices ( $n > 0$ ) has  $n - 1$  edges
- **Lemma 10.5.3**  
If  $G$  is any connected graph,  $C$  is any circuit in  $G$ , and one of the edges of  $C$  is removed from  $G$ , then the graph that remains is still connected
- **Determining a Tree** (Thm 10.5.4)  
If  $G$  is a connected graph with  $n$  vertices and  $n - 1$  edges, then  $G$  is a tree

## Rooted Trees

- **Rooted Tree**  
A **rooted tree** is a tree in which there is one vertex that is distinguished from the others and is called the **root**

- **Level**  
The **level** of a vertex is the number of edges along the unique path between it and the root
- **Height**  
The **height** of a rooted tree is the maximum level of any vertex of the tree
- **Children**  
Given the root or any internal vertex  $v$  of a rooted tree, the **children** of  $v$  are all those vertices that are adjacent to  $v$  and are one level farther away from the root than  $v$
- **Parent**  
If  $w$  is a child of  $v$ , then  $v$  is called the **parent** of  $w$ , and two distinct vertices that are both children of the same parent are called **siblings**
- **Ancestor/Descendant**  
Given two distinct vertices  $v$  and  $w$ , if  $v$  lies on the unique path between  $w$  and the root, then  $v$  is an **ancestor** of  $w$ , and  $w$  is a **descendant** of  $v$

## Binary Trees

- **Binary Tree**  
A **binary tree** is a rooted tree in which every parent has **at most two children**. Each child is designated either a **left child** or a **right child** (but not both), and every parent has at most one left and one right child.
- **Full Binary Tree**  
A **full binary tree** is a binary tree in which each parent has **exactly two children**
- **Left/Right Subtree**  
Given any parent  $v$  in a binary tree  $T$ , if  $v$  has a left child, then the **left subtree** of  $v$  is the binary tree whose root is the left child of  $v$ , whose vertices consist of the left child of  $v$  and all its descendants, and whose edges consist of all those edges of  $T$  that connect the vertices of the left subtree  
The **right subtree** of  $v$  is defined analogously

- **Full Binary Tree Theorem** (Thm 10.6.1)  
If  $T$  is a full binary tree with  $k$  internal vertices, then  $T$  has a total of  $2k + 1$  vertices and has  $k + 1$  terminal vertices (leaves)
- **Maximum no. of terminal vertices** (Thm 10.6.2)  
For non-negative integers  $h$ , if  $T$  is any binary tree with height  $h$  and  $t$  terminal vertices (leaves), then

$$t \leq 2^h$$

Equivalently:  $\log_2 t \leq h$

## Binary Tree Traversal

- **Breath-First Search**  
In BFS, start at the root and visit the adjacent vertices, then move on to the next level
- **Depth-First Search**  
There are three kinds of DFS, **pre-order**, **in-order** and **post-order**.

### Pre-Order

- *Print the data of the root (or current vertex)*
- Traverse the **left** subtree by recursively calling the pre-order  $f(x)$
- Traverse the **right** subtree by recursively calling the pre-order  $f(x)$

### In-Order

- Traverse the **left** subtree by recursively calling the pre-order  $f(x)$
- *Print the data of the root (or current vertex)*
- Traverse the **right** subtree by recursively calling the pre-order  $f(x)$

### Post-Order

- Traverse the **left** subtree by recursively calling the pre-order  $f(x)$
- Traverse the **right** subtree by recursively calling the pre-order  $f(x)$
- *Print the data of the root (or current vertex)*

## Spanning Trees & Shortest Paths

### • Spanning Tree

A **spanning tree** for a graph  $G$  is a subgraph of  $G$  that contains every vertex of  $G$  and is a tree

### • Proposition 10.7.1

1. Every connected graph has a spanning tree
2. Any two spanning trees for a graph have the same no. of edges

### • Weighted Graph

A **weighted graph** is a graph for which each edge has an associated positive real number **weight**. The sum of the weights of all edges is the **total weight** of the graph

### • Minimum Spanning Tree

A **minimum spanning tree** for a connected weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph

### • $w(e)$ & $w(G)$

If  $G$  is a weighted graph and  $e$  is an edge of  $G$ , then  $w(e)$  denotes the weight of  $e$  and  $w(G)$  denotes the total weight of  $G$

### • Kruskal's Algorithm (Alg 10.7.1)

**Input:**  $G$  [a connected weighted graph with  $n$  vertices]  
**Algorithm:**

1. Init  $T$  to have all the vertices of  $G$  and no edges
2. Let  $E$  be the set of all edges of  $G$ , and let  $m = 0$
3. While  $(m < n - 1)$ 
  - (a) Find an edge  $e$  in  $E$  of least weight
  - (b) Delete  $e$  from  $E$
  - (c) If addition of  $e$  to the edge set of  $T$  does not produce a circuit, then add  $e$  to the edge set of  $T$  and set  $m = m + 1$
4. End While

**Output:**  $T$  [ $T$  is the MST for  $G$ ]

### • Prim's Algorithm (Alg 10.7.2)

**Input:**  $G$  [a connected weighted graph with  $n$  vertices]

**Algorithm:**

1. Pick a vertex  $v$  of  $G$  and let  $T$  be the graph with this vertex only
2. Let  $V$  be the set of all vertices of  $G$  except  $v$ .
3. For  $i = 1$  to  $n - 1$ 
  - (a) Find an edge  $e$  of  $G$  such that (1)  $e$  connects  $T$  to one of the vertices in  $V$ , and (2)  $e$  has the least weight of all edges connecting  $T$  to a vertex in  $V$ . Let  $w$  be the endpoint of  $e$  that is in  $V$
  - (b) Add  $e$  and  $w$  to the edge and vertex sets of  $T$ , delete  $w$  from  $V$ .

**Output:**  $T$  [ $T$  is the MST for  $G$ ]

### • Dijkstra's Algorithm (Alg 10.7.3)

**Input:**  $G$  [a connected weighted graph with positive weight for every edge],  $\infty$  [a no. greater than the sum of the weights of all the edges in  $G$ ],  $w(u, v)$  [the weight of edge  $\{u, v\}$ ],  $a$  [the source vertex],  $z$  [the dest vertex]

**Algorithm:**

1. init  $T$  to be the graph with vertex  $a$  and no edges. Let  $V(T)$  be the set of vertices of  $T$ , and let  $E(T)$  be the set of edges of  $T$
2. Let  $L(a) = 0$ , and for all vertices in  $G$  except  $a$ , let  $L(u) = \infty$  [The number  $L(x)$  is called the label of  $x$ ]
3. Init  $v$  to equal  $a$  and  $F$  to be  $\{a\}$ . [The symbol  $v$  is used to denote the vertex most recently added to  $T$ ]
4. Let  $Adj(x)$  denote the set of vertices adjacent to vertex  $x$
5. while  $(z \notin V(T))$ 
  - (a)  $F \leftarrow (F - \{v\}) \cup \{\text{vertices} \in Adj(v) \text{ and } \notin V(T)\}$  [Set  $F$  is set of fringe vertices]
  - (b) For each vertex  $u \in Adj(v)$  and  $\notin V(T)$ ,
    - If  $L(v) + w(v, u) < L(u)$  then
    - $L(u) \leftarrow L(v) + w(v, u)$

–  $D(u) \leftarrow v$

- (c) Find a vertex  $x$  in  $F$  with the smallest label. Add vertex  $x$  to  $V(T)$ , and add edge  $\{D(x), x\}$  to  $E(T)$ .  $v \leftarrow x$

**Output:**  $L(z)$  [this is the length of the shortest path from  $a$  to  $z$ ]