CS1231 Finals Cheatsheet v1.0 (2019-02-10)
by Julius Putra Tanu Setiaji, page 1 of 7

1 Proofs

Sets of Numbers

- $\mathbb{R}$ Real numbers
- $\mathbb{Z}$ Integers
- $\mathbb{Q}$ Rational numbers

Notation

- $\exists$ there exists
- $\exists!$ there exists a unique
- $\forall$ for all
- $\in$ member of (a set)
- $\ni$ such that

Proving Methods

- **By construction** = Finding the value with the correct properties
- **If-then** = (if P then Q)
  P is the origin, Q is the destination. Work forward from P and backwards from Q but <u>**NEVER**</u> assume Q is true.
- $\forall x P(x)$ Take x to be a particular, arbitrarily chosen value. Prove $P(x)$ is true. Conclude since $P(x)$ is true for this particular x, it must be true for all x
- **By contrapositive** :
  (if P then Q) Prove if $\sim Q$ then $\sim P$
- **By contradiction** :
  Assume $\sim S$ is true. Use known facts and theorems to arrive at a contradiction. Since $\sim S$ is false, S must be true.
- **By induction** : Template

1. For all $n \in \mathbb{N}$, let $P(n) = (3 \mid (4^n - 1))$
2. <u>Base case:</u> $n = 0$

   2.1. Clearly, $(4^0 - 1) = 0 = 3 \cdot 0$

   2.2. Thus, $P(0)$ is true.
3. <u>Inductive step:</u> For any $k \in \mathbb{N}$

   3.1. Assume $P(k)$ is true, i.e. $3 \mid (4^k - 1)$

   3.2. (<u>Strong induction:</u>
   Assume $P(i)$ is true for $1 < i \leq k$)

   3.3. Consider the $k+1$ case:

   3.4. $4^{k+1} - 1 = 4 \cdot 4^k - 1 = 4(4^k - 1) + 3$, by Basic Algebra

   3.5. By the inductive hypothesis, $3 \mid (4^k - 1)$

   3.6. Clearly, $3 \mid 3$

   3.7. So by Thm 4.1.1, $3 \mid (4(4^k - 1) + 3)$

   3.8. Thus, $P(k+1)$ is true
4. So by Mathematical Induction, the statement is true.

- **Disproving by counterexample** :
  show one condition that leads to contradiction

2 Compound Statements

Notation and Order of Operations

1	$\sim$	not (negation)
2	$\wedge$	and (conjunction)
2	$\vee$	or (disjunction)
3	$\to$	if-then (implies)
3	$\leftrightarrow$	iff
	$\equiv$	logically equivalent

Thm 2.1.1 Logical Equivalences

- **Commutative laws** :
  $p \wedge q \equiv q \wedge p \quad p \vee q \equiv q \vee p$
- **Associative laws** :
  $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r) \quad (p \vee q) \vee r \equiv p \vee (q \vee r)$
- **Distributive laws** :
  $p \wedge (q \vee r) \equiv (p \wedge q) \vee (q \wedge r)$
  $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
- **Identity laws** :
  $p \wedge \mathbf{t} \equiv p \quad p \vee \mathbf{c} \equiv p$
- **Negation laws** :
  $p \vee \sim p \equiv \mathbf{t} \quad p \wedge \sim p \equiv \mathbf{c}$
- **Double negative laws** : $\sim(\sim p) \equiv p$
- **Idempotent laws** :
  $p \wedge p \equiv p \quad p \vee p \equiv p$
- **Universal bound laws** :
  $p \vee \mathbf{t} \equiv \mathbf{t} \quad p \wedge \mathbf{c} \equiv \mathbf{c}$
- **De Morgan's laws** :
  $\sim(p \wedge q) \equiv \sim p \vee \sim q \quad \sim(p \vee q) \equiv \sim p \wedge \sim q$
- **Absorption laws** :
  $p \vee (p \wedge q) \equiv p \quad p \wedge (p \vee q) \equiv p$
- **Negation of t and c** :
  $\sim \mathbf{t} \equiv \mathbf{c} \quad \sim \mathbf{c} \equiv \mathbf{f}$

Conditional statements

- **Truth table** (when p is F, $p \to q$ is vacously true)

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

- **Implication law** : $p \to q \equiv \sim p \vee q$
- **Negation** : $\sim(p \to q) \equiv p \wedge \sim q$ (De Morgan's laws)
- **Contrapositive** (Def 2.2.2): $p \to q \equiv \sim q \to \sim p$
- **Converse** (Def 2.2.3): $q \to p$
- **Inverse** (Def 2.2.4): $\sim p \to \sim q$
- **Only if** (Def 2.2.5): p only if $q \equiv \sim q \to \sim p \equiv p \to q$
- **Biconditional** (Def 2.2.6): $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$
- **Necessary and Sufficient conditions** (Def 2.2.7)
  r sufficient for $s \equiv r \to s$
  r necessary for $s \equiv \sim r \to \sim s \equiv s \to r$

Valid Arguments

- **Argument** (Def 2.3.1): If all premises are true, conclusion must be true
- **Syllogism** : 2 premises and 1 conclusion
- **Modus Ponens** : $(p \to q), (p), \therefore q$
- **Modus Tollens** : $(p \to q), (\sim q), \therefore \sim p$

Rules of Inference

- **Generalization** : $p, \therefore p \vee q \quad q, \therefore p \vee q$
- **Specialization** : $p \wedge q, \therefore p \quad p \wedge q, \therefore q$
- **Elimination** :
  $(p \vee q), (\sim q), \therefore p$
  $(p \vee q), (\sim p), \therefore q$
- **Transitivity** : $(p \to q), (q \to r), \therefore p \to r$
- **Proof by Division into Cases** :
  $(p \vee q), (p \to r), (q \to r)$

Other rules of inference

- **Conjunction Intro** : $A, B, \therefore A \wedge B$
- **Conjunction Elim** : $A \wedge B, \therefore A, B$
- **Disjunction Intro** : $A, \therefore A \vee B, B \vee A$
- **Disjuction Elim** : $A \vee B, A \to C, B \to C, \therefore C$
- **Contradiction Intro** : $A, \sim A, \therefore$ contradiction
- **Contradiction Elim** : $A \to$ contradiction, $\therefore \sim A$

Fallacies

- **Converse Error** : $(p \to q), (q), \therefore p$
- **Inverse Error** : $(p \to q), (\sim p), \therefore \sim q$
- **Sound & unsound argument** :
  sound iff valid and premises are true.

3 Quantified Statements

- **Predicate** ($P(x)$) (Def 3.1.1):
  A sentence that contains contains a finite number of vars and becomes a statement when specific values are subbed for the vars. The **domain** of a pred var is the set of all values that may be subbed in place of the variable.
- **Truth set** (Def 3.1.2):
  If $P(x)$ is a pred and x has domain D, the truth set is the set of all elements of D that make $P(x)$ true when they are subbed for x. The truth set of $P(x)$ is denoted $\{x \in D \mid P(x)\}$.
- **Universal quantifier** (Def 3.1.3): $\forall x \in D(Q(x))$
  - equiv to $Q(x_1) \wedge Q(x_2) \wedge \ldots \wedge Q(x_n)$
  - true iff $Q(x)$ is true $\forall x \in D$
  - false iff $Q(x)$ is false for at least one $x \in D$
- **Existential quantifier** (Def 3.1.4): $\exists x \in D(Q(x))$
  - equiv to $Q(x_1) \vee Q(x_2) \vee \ldots \vee Q(x_n)$
  - true iff $Q(x)$ true for at least one $x \in D$
  - false iff $Q(x)$ false $\forall x \in D$
- **Implicit quantification** : $\Rightarrow \Leftrightarrow$
  - $P(x) \Rightarrow Q(x) \equiv \forall x \in D(P(x) \to Q(x))$
    truth set of $P(x) \subset$ truth set of $Q(x)$
  - $P(x) \Leftrightarrow Q(x) \equiv \forall x \in D(P(x) \leftrightarrow Q(x))$
    truth set of $P(x) \equiv$ truth set of $Q(x)$

Negation of Quantified Statement

- **Negation of $\forall$** (Thm 3.2.1)
  $\sim(\forall x \in D(P(x)) \equiv \exists x \in D(\sim P(x))$
- **Negation of $\exists$** (Thm 3.2.2)
  $\sim(\exists x \in D(P(x))) \equiv \forall x \in D(\sim P(x))$

Universal Conditional Statement

$\forall x \in D(P(x) \to Q(x))$

- **Vacously true** iff $P(x)$ is false $\forall x \in D$
- **Contrapositive** (Def 3.2.1):
  $\forall x \in D(\sim Q(x) \to P(x))$
- **Converse** (Def 3.2.1): $\forall x \in D, Q(x) \to P(x)$
- **Inverse** (Def 3.2.1): $\forall x \in D, \sim P(x) \to Q(x)$
- **Necessary and sufficient condition** (Def 3.2.2)
  $\forall x, r(x)$ sufficient for $s(x) \equiv \forall x, r(x) \to s(x)$
  $\forall x, r(x)$ necessary for $s(x) \equiv \forall x, \sim r(x) \to \sim s(x)$
- **Only if** (Def 3.2.2):
  $\forall x, r(x)$ only if $s(x) \equiv$
  $\forall x, \sim s(x) \to \sim r(x) \equiv \forall x, r(x) \to s(x)$
- **Negation of $\forall$ conditional**

$$\sim(\forall x(P(x) \to Q(x)) \equiv \exists x(\sim(P(x) \to Q(x)) \qquad (1)$$

$$\sim(P(x) \to Q(x)) \equiv P(x) \wedge \sim Q(x) \qquad (2)$$

Sub (2) into (1)

$$\sim(\forall x(P(x) \to Q(x)) \equiv \exists x(P(x) \wedge \sim Q(x))$$

Arguments with Quantified Statements

- **Universal Instantiation** :
  $(E \in D), (\forall x \in D(P(x))), \therefore P(E)$
- **Universal Introduction** :
  (For any $x \in D$: $P(x)$), $\therefore \forall x \in D(P(x))$
- **Existential Instantiation** :
  $(\exists x \in D(P(x)))), \therefore P(a)$ for some a
- **Existential Introduction** :
  $(E \in D), (P(E)), \therefore x \in D(P(x))$
- **Universal Modus Ponens** :
  $(\forall x(P(x) \to Q(x))$,
  ($P(a)$ for a particular a), $\therefore Q(a)$
- **Universal Modus Tollens** :
  $(\forall x(P(x) \to Q(x))$,
  ($\sim Q(a)$ for a particular a), $\therefore \sim P(a)$
- **Universal Transitivity** :
  $(\forall x(P(x) \to Q(x))), (\forall x(Q(x) \to R(x)))$,
  $\therefore \forall x(P(x) \to R(x))$

Fallacies

- **Converse Error** : $(\forall x(P(x) \to Q(x)))$, $(Q(a)$ for a particular $a)$, $\therefore P(x)$
- **Inverse Error** : $(\forall x(P(x) \to Q(x))$, $(\sim P(a)$ for a particular $a)$, $\therefore \sim Q(x)$

4 Number Theory

Basics

- **Even and Odd** (Def 1.6.1):
$$n \text{ is even} \Leftrightarrow \exists k \in \mathbb{Z}(n = 2k)$$
$$n \text{ is odd} \Leftrightarrow \exists k \in \mathbb{Z}(n = 2k+1)$$
- **The sum of two even $\mathbb{Z}$ is even** (Thm 4.1.1)
- **Rational Number**
$r \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z}, r = \frac{a}{b}$ and $b \neq 0$
- **Every $\mathbb{Z}$ is a rational number** (Thm 4.2.1)
- **The sum of any two $\mathbb{Q}$ is $\mathbb{Q}$** (Thm 4.2.2)
- **The double of a $\mathbb{Q}$ is $\mathbb{Q}$** (Col 4.2.3)

Divisibility

- **Divisibility** (Def 1.3.1): $n, d \in \mathbb{Z}$
$$d \mid n \Leftrightarrow \exists k \in \mathbb{Z}(n = dk)$$
- **Linear Combination** (Thm 4.1.1):
$\forall a, b, c \in \mathbb{Z}(a \mid b \wedge a \mid c \to \forall x, y \in \mathbb{Z}(a \mid (bx + cy)))$
- **Thm 4.3.1** : $\forall a, b \in \mathbb{Z}^+$, if $a \mid b$ then $a \leq b$
- **Thm 4.3.2** : The only divisors of 1 are $1, -1$
- **Transitivity of Divisibility** (Thm 4.3.3):
$\forall a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$
- **Thm 4.3.4** : Any integer $n > 1$ is divisible by a prime number.

Prime Numbers

- **Prime and Composite numbers** (Def 4.1.1)
$$n \text{ is prime} \Leftrightarrow \forall r, s, \in \mathbb{Z}^+(n = rs \to ((r = 1 \text{ and } s = n) \vee (r = n \text{ and } s = 1)))$$
$$n \text{ is composite} \Leftrightarrow \forall r, s, \in \mathbb{Z}^+(n = rs \text{ and } 1 < r < n \text{ and } 1 < s < n)$$
- **Prop 4.2.2** :
For any two primes p and p', if $p \mid p'$ then $p = p'$
- **Thm 4.2.3** :
If p is a prime and $x_1, x_2, ..., x_n \in \mathbb{Z}$ such that $p \mid x_1 x_2 ... x_n$, then $p \mid x_1$ for some x_i $(1 \leq i \leq n)$
- **Unique Prime Factorization / The Fundamental Thm of Arithmetic** (Thm 4.3.5):
Given $n \in \mathbb{Z}, n > 1$, there exists $k \in \mathbb{Z}^+$, distinct prime numbers $p_1, p_2, ..., p_k$, and positive integers $e_1, e_2, ..., e_k$ such that
$$n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$$
and any other expression for n as a product of prime numbers is identical to this except for ordering
- **Prop 4.7.3** :
For any $a \in \mathbb{Z}$ and any prime p, if $p \mid a$ then $p \nmid (a+1)$
- **Infinitude of Primes** (Thm 4.7.4):
The set of primes is infinite.

Well Ordering Principle

- **Lower bound** (Def 4.3.1):
$b \in \mathbb{Z}$ is a lower bound for set $X \subseteq \mathbb{Z}$ if $b \leq x \forall x \in X$
- **Well ordering principle** (Thm 4.3.2):
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):
If a set $S \subseteq \mathbb{Z}$ has a least/greatest element, then the least/greatest element is unique

Quotient-Remainder Thorem, GCD, LCM

- **Quotient-Remainder Thm** (Thm 4.4.1):
Given any $a \in \mathbb{Z}$ and any $b \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z}$ s.t.: $a = bq + r$ and $0 \leq r < b$
- **Greatest Common Divisor** (Def 4.5.1):
Let $a, b \in \mathbb{Z}$, not both zero. $gcd(a, b)$ is $d \in \mathbb{Z}$ s.t.:
$$d \mid a \text{ and } d \mid b \tag{1}$$
$$\forall c \in \mathbb{Z}, \text{ if } c \mid a \text{ and } c \mid b \text{ then } c \leq d \tag{2}$$
- **Existence of gcd** (Prop 4.5.2):
For any $a, b \in \mathbb{Z}$, not both zero, their gcd exists and is unique.
- **Bézout's Identity** (Thm 4.5.3):
Let $a, b \in \mathbb{Z}$, not both zero, and let $d = gcd(a, b)$. Then $\exists x, y \in \mathbb{Z}(ax + by = d)$
- Non-uniqueness of Bézout's Identity:
There are multiple solns to the eqn $ax + by = d$
$(x + \frac{kb}{d}, y - \frac{ka}{d}), k \in \mathbb{Z}$
- **Coprime/Relatively prime** (Def 4.5.4):
$a, b \in \mathbb{Z}$ are coprime $\Leftrightarrow gcd(a, b) = 1$
- **Prop 4.5.5** :
$a, b \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then $c \mid gcd(a, b)$
- **Least Common Multiple** (Def 4.6.1):
Let $a, b \in \mathbb{Z} \setminus \{0\}$, $lcm(a, b)$ is $d \in \mathbb{Z}^+$ s.t.:
$$a \mid m \text{ and } b \mid m \tag{3}$$
$$\forall c \in \mathbb{Z}^+, \text{ if } a \mid c \text{ and } b \mid c \text{ then } m \leq c \tag{4}$$
- **Existence of LCM** :
$lcm(a, b)$ exists because the Well Ordering Principle guarantees the existence of the least element on the set of common multiples of a, b
- $gcd(a, b) \cdot lcm(a, b) = ab$
Proof:
  1. By the Unique Prime Factorization Thm,
  $a = q_1^{r_1} \cdot q_2^{r_2} \cdot ... \cdot q_n^{r_n}$, $b = q_1^{s_1} \cdot q_2^{s_2} \cdot ... \cdot q_n^{s_n}$
  $\forall i \in \mathbb{Z}$ s.t. $i \leq i \leq n$, q_i is a prime number and $r_i \in \mathbb{Z}, r_i \geq 0$
  2. $gcd(a, b) = q_1^{min(r_1, s_1)} \cdot q_2^{min(r_2, s_2)} \cdot ... \cdot q_n^{min(r_n, s_n)}$
  3. $lcm(a, b) = q_1^{max(r_1, s_1)} \cdot q_2^{max(r_2, s_2)} \cdot ... \cdot q_n^{min(r_n, s_n)}$
  4. Thus, $gcd(a, b) \cdot lcm(a, b)$
  $= q_1^{min(r_1, s_1) + max(r_1, s_1)} \cdot q_2^{min(r_2, s_2) + max(r_2, s_2)} \cdot ... \cdot q_n^{min(r_n, s_n) + max(r_n, s_n)}$
  $= q_1^{r_1 + s_1} \cdot q_2^{r_2 + s_2} \cdot ... \cdot q_n^{r_n + s_n}$
  $= a \cdot b$

Modulo Arithmetic

- **Congruence modulo** (Def 4.7.1)
Let $m, n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, m is congruent to n modulo d:
$$m \equiv n \pmod d \iff d \mid (m - n)$$
- **Modular Equivalences** (Thm 8.4.1)
Let $a, b, n \in \mathbb{Z}, n > 1$. The following are all equiv:
  1. $n \mid (a - b)$
  2. $a \equiv b$
  3. $a = b + kn, k \in \mathbb{Z}$
  4. a, b have the same (non-negative) remainder when divided by n
  5. $a \pmod n = b \pmod n$
- **Modulo Arithmetic** (Thm 8.4.3)
Let $a, b, c, d, n \in \mathbb{Z}, n > 1$, and suppose
$$a \equiv c \pmod n \text{ and } b \equiv d \pmod n$$
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**
Let $a, b, n \in \mathbb{Z}, n > 1$. Then,
$$ab \equiv [(a \mod n)(b \mod n)] \pmod n$$
or equivalently,
$$ab \mod n = [(a \mod n)(b \mod n)] \mod n$$
If $m \in \mathbb{Z}^+$, then
$$a^m \equiv [(a \mod n)^m] \pmod n$$
or equivalently,
$$a^m \mod n = (a \mod n)^m \mod n$$
- **Multiplicative inverse modulo** n (Def 4.7.2):
For $a, n \in \mathbb{Z}, n > 1$, if $s \in \mathbb{Z}$ such that $as \equiv 1 \pmod n$, then s is the **multiplicative inverse of** a **modulo** n, denoted as a^{-1}.
Because the commutative law still applies in modulo arithmetic, $a^{-1}a \equiv 1 \pmod n$
- **Existence of multiplicative inverse** (Thm 4.7.3)
For $a \in \mathbb{Z}$, its multiplicative inverse modulo n (where $n > 1$), a^{-1} exists iff a and n are coprime.
- **Special case:** n **is prime** (Corollary 4.7.4):
If $n = p$ is prime, then all $a \in \mathbb{Z}, 0 < a < p$ have multiplicative inverses modulo p
- **Cancellation Law** (8.4.9):
$\forall a, b, c, n \in \mathbb{Z}, n > 1$, and a, n are coprime, if $ab \equiv ac \pmod n$, then $b \equiv c \pmod n$
- **Method to find inverse**
e.g. Find $3^{-1} \pmod{40}$.
  1. Prove $gcd(3, 40) = 1$ using Euclid's method
  2. Use extended Euclidean method to find Bézout's Identity
  3. $1 = -2(40) + 27(3) \Leftrightarrow 2(40) = 27(13) - 1$
  4. By Thm 8.4.1, $3(27) \equiv 1 \pmod{40}$
  5. Thus, $3^{-1} \equiv 27 \pmod{40}$

5 Sequences & Recursion

Formulae

- **Explicit Formula** : $a_n = f(n)$
- **Recurrence relation** : e.g. $a_0 = 0, a_n = a_{n-1} + 2$

Summation & Product

- **Summing a sequence yields another sequence**
$\sum_{i=m}^{n} a_i = S_n, \forall n \in \mathbb{N}$, e.g. Triangle no $\sum_{i=0}^{n} i = \Delta_n$
- **Multiplying a sequence yields another sequence**
$\prod_{i=m}^{n} a_i = P_n, \forall n \in \mathbb{N}$, e.g. factorial $\prod_{i=1}^{n} i = n!$
- **Recursive definition** :
$$\sum_{i=m}^{n} a_i = \begin{cases} 0, & \text{if } n < m, \\ (\sum_{i=m}^{n-1} a_i) + a_n, & \text{otherwise.} \end{cases}$$
$$\prod_{i=m}^{n} a_i = \begin{cases} 1, & \text{if } n < m, \\ (\prod_{i=m}^{n-1} a_i) \cdot a_n, & \text{otherwise.} \end{cases}$$

Thm 5.1.1

If $a_m, a_{m+1}, a_{m+2}, ...$ and b_m, b_{m+1}, b_{m+2} are sequences of real numbers and c is any real number, then 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. (generalised distributive law)
$c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$
3. $\left(\prod_{k=m}^{a_k}\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \prod_{k=m}^{n} (a_k \cdot b_k)$

Common Sequences

- **Arithmetic Sequence** :
  $\forall n \in \mathbb{N}, a_n = \begin{cases} a, & \text{if } n = 0, \\ a_{n-1} + d, & \text{otherwise.} \end{cases}$
  where a, d are real constants.
  Explicit formula: $a_n = a + nd, \forall n \in \mathbb{N}$
  $\sum_{i=0}^{n-1} a_i = \frac{n}{2}[2a + (n-1)d], \forall n \in \mathbb{N}$, and $a, d \in \mathbb{R}$
- **Geometric Sequence** :
  $\forall n \in \mathbb{N}, a_n = \begin{cases} a, & \text{if } n = 0, \\ r \cdot a_{n-1}, & \text{otherwise.} \end{cases}$
  where a, r are real constants.
  Explicit formula: $a_n = ar^n, \forall n \in \mathbb{N}$
  $S_n = \sum_{i=0}^{n-1} a_i = \frac{a(r^n - 1)}{r-1}, \forall n \in \mathbb{N}$, and $a, r \in \mathbb{R}, r \neq 1$
  For the special case $|r| < 1, s_\infty = \frac{a}{1-r}$
- **Square numbers** : sum of the first n odd numbers
- **Triangle numbers** : sum of the first $n+1$ integers
- **Fibonacci numbers** :
  $\forall n \in \mathbb{N}, F_0 = 1, F_1 = 1, F_n = F_{n-1} + F_{n-2}$
  Explicit formula: $\forall n \in \mathbb{N}, F_n = \frac{\phi^n - (-\phi)^{-n}}{\sqrt{5}}$
  where $\phi = \frac{1+\sqrt{5}}{2}$ (the golden ratio)
- **Binomial numbers** :
  Recurrence:
  $\forall n, r \in \mathbb{N}, \binom{n}{r} = \begin{cases} 1, & \text{if } r = 0 \wedge n \geq 0, \\ \binom{n-1}{r} + \binom{n-1}{r-1}, & \text{if } 0 < r \leq n, \\ 0, & \text{otherwise.} \end{cases}$
  Second line implies that adding 2 consecutive terms in one row gives one term in the next row.
  Explicit formula: $\forall n, r \in \mathbb{N}$ s.t. $r \leq n, \binom{n}{r} = \frac{n!}{r!(n-r)!}$
  Other interesting identities:
  - $\binom{n}{r} = \binom{n}{n-r}$ and $\sum_{r=0}^{n} \binom{n}{r} = 2^n$
  - Thus, $\sum_{r=0}^{n} \binom{n}{r} = 2 \times \sum_{r=0}^{n-1} \binom{n-1}{r}$
    Sum of no in 1 row is twice that of the previous row

Solving recurrences

- **Second-order Linear Homogeneous Recurrence Relation with Constant Coefficients** (Def 5.4.1)
  A recurrence relation of the form
  $a_k = Aa_{k-1} + Ba_{k-2}, \forall k \in \mathbb{Z}_{\geq k_0}$ where $A, B \in \mathbb{R}$, $B \neq 0$ and $k_0 \in \mathbb{Z}$
- **Distinct-Roots Thm** (Thm 5.8.3):
  For a sequence $a_0, a_1, a_2, \ldots$ if characteristic eqn $t^2 - At - B = 0$ has 2 distinct roots r, s then explicit formula is $a_n = Cr^n + Ds^n, \forall n \in \mathbb{N}$ where $C, D \in \mathbb{R}$ determined by initial conditions a_0, a_1.
- **Single-Roots Thm** (Thm 5.8.5):
  For a sequence $a_0, a_1, a_2, \ldots$ if characteristic eqn $t^2 - At - B = 0$ has a single real root r, then explicit formula is $a_n = Cr^n + Dnr^n, \forall n \in \mathbb{N}$ where $C, D \in \mathbb{R}$ is determined by a_0 or else

6 Sets

Characteristics

- Sets can be defined **in extension** by explicitly listing its member, e.g. $1, 2, 3$ or **in intention** by specifying its members' property, e.g. $X | X \in \mathbb{N} \wedge 1 < X \wedge X < 5$
- Membership: $1 \in \{1, \{1, 2\}\}$
- Non-membership $3 \notin \{1, 2\}$
- No duplicate $\{1, 1, 2, 2, 2\} = \{1, 2\}$
- Order does not matter: $\{1, 2\} = \{2, 1\}$

Subset and Proper Subset Subset

- **Subset** (Def 6.1.1):
  S is a subset of T (or S is contained in T, or T contains S, or $T$is a superset of S) if all the elements of S are elements of T.
  Notation: $S \subseteq T$, e.g. $\{1, 2\} \subseteq \{1, 2, 3\}$, $\{3, 4\} \not\subseteq \{1, 2, 3\}$, A set is a subset of itself $\{1, 2, 3\} \subseteq \{1, 2, 3\}$
- **Proper Subset** :
  S is a proper subset of $T \iff S \subseteq T \wedge \exists x \in T(x \notin S)$
  Notation: $S \subsetneq T$, e.g. $\{1, 2\} \subsetneq \{1, 2, 3\}$

Set Operations

- **Intersection** : $A \cap B$
- **Union** : $A \cup B$
- **Difference** : $B \setminus A$ or $B - A$

Basic Set Theory

- **Empty Set** (Def 6.3.1):
  An empty set has no element. (Notation: $\varnothing$ or $\{\}$)
  $\forall Y \sim (Y \in \varnothing)$
- **An empty set is a subset of all sets** (Thm 6.2.4):
  $\forall X \forall Z((\forall Y \sim (Y \in X)) \to (X \subseteq Z))$
- **Set equality** (Def 6.3.2):
  Two sets are equal iff they have the same elements.
  $\forall X \forall Y((\forall Z(Z \in X \leftrightarrow Z \in Y)) \leftrightarrow X = Y)$
  e.g. $\{1, 2, 3\} = \{2, 1, 3, 2\}$, $\{\} \neq \{\{\}\}$
- **Prop 6.3.3** :
  $\forall X \forall Y((X \subseteq Y \wedge Y \subseteq X) \leftrightarrow X = Y)$
- **The Empty Set is unique** (Cor 6.2.5):
  $\forall X_1 \forall X_2((((\forall Y \sim (Y \in X_1)) \wedge (\forall Y \sim (Y \in X_2)))) \to X_1 = X_2)$
- **Power Set** (Def 6.3.4):
  The set whose elements are all the subsets of S
  Given a set $S, T = \wp(S) \to \forall X((X \in T) \to (X \subseteq S))$
  Notation: $\wp(S)$ or 2^S
  e.g. $\wp(\{x, y\}) = \{\varnothing, \{x\}, \{y\}, \{x, y\}\}, \wp(\varnothing) = \{\varnothing\}$
  If S has n elements, then 2^S has 2^n elements.

Procedural Versions on Set Definitions

Let X and Y be subsets of a universal set U and suppose x and y are elements of U.

1. $x \in X \cup Y \iff x \in X \vee x \in Y$
2. $x \in X \cap Y \iff x \in X \wedge x \in Y$
3. $x \in X - Y \iff x \in X \wedge x \notin Y$
4. $x \in X^C \iff x \notin X$
5. $(x, y) \in X \times Y \iff x \in X \wedge y \in Y$

Operations on Sets

Let A and B be subsets of a universal set U.

- **Union** (Def 6.4.1):
  The set of all elements that are in at least one of A or B.
  Let S be a set of sets, T is the union of the sets in S.
  $\forall Y((Y \in T) \leftrightarrow \exists((Z \in S) \wedge (Y \in Z))$
  Notation: $T = \bigcup S = \bigcup_{X \in S} X$. For 2 sets, $T = A \cup B$
- **Prop 6.4.2**
  Let A, B, C be sets. Then:
  - $\bigcup \varnothing = \bigcup_{A \in \varnothing} A = \varnothing$
  - $\bigcup A = A$
  - $A \cup \varnothing = A$
  - $A \cup B = B \cup A$
  - $A \cup (B \cup C) = (A \cup B) \cup C$
  - $A \cup A = A$
  - $A \subseteq B \leftrightarrow A \cup B = B$
- **Intersection** (Def 6.4.3):
  The set of all elements that are common to both A and B.
  Let S be a non-empty set of sets, T is the union of the sets in S.
  $\forall Y((Y \in T) \leftrightarrow \forall Z((Z \in S) \to (Y \in Z))$
  Notation: $T = \bigcap S = \bigcap_{X \in S} X$. For 2 sets, $T = A \cap B$
- **Prop 6.4.4**
  Let A, B, C be sets. Then:
  - $A \cap \varnothing = \varnothing$
  - $A \cap B = B \cap A$
  - $A \cap (B \cap C) = (A \cap B) \cap C$
  - $A \cap B \leftrightarrow A \cap B = A$

  Distributivity laws:
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- **Disjoint** (Prop 6.4.5):
  Let S and T be two sets. S and T are disjoint $\leftrightarrow S \cap T = \varnothing$ (they have no element in common)
- **Mutually Disjoint** (Def 6.4.6):
  Let V be a set of sets. The sets $T \in V$ are mutually disjoint iff every two distinct sets are disjoint.
  $\forall X, Y \in V(X \neq Y \to X \cap Y = \varnothing)$
  e.g. the sets in $V = \{\{1, 2\}, \{3\}, \{\{1\}, \{2\}\}\}$ are mutually disjoint
- **Partition** (Def 6.4.7):
  Let S be a set, V be a set of non-empty subsets of S. Then V is called a partition of S iff:
  1. The sets in V are mutually disjoint
  2. The union of sets in V equals S ($\bigcup_{X \in V} X = S$)
- **Non-symmetric difference** (Def 6.4.8):
  The set of all elements that are in B and not A.
  Let S and T be two sets.
  $\forall X(X \in (S - T) \leftrightarrow (X \in S \wedge \sim (X \in T)))$
  Notation: $S - T$
- **Symmetric difference** (Def 6.4.9):
  Let S and T be two sets.
  $\forall X(X \in (S \ominus T) \leftrightarrow (X \in S \oplus X \in T))$ PS: $\oplus$ = XOR
  Notation: $S \ominus T$
- **Set complement** (Def 6.4.10):
  The set of all elements in U that are not in A.
  Let $\mathcal{U}$ be the Universal set (or the Universe of Discourse). Let A be a subset of $\mathcal{U}$. Then, the complement (or absolute complement) of A is $\mathcal{U} - A$
  Notation: A^C
- **Thm 6.2.1** :
  - **Inclusion of Intersection** :
    $\forall$ sets $A, B(A \cap B \subseteq A$ and $A \cap B \subseteq B)$
  - **Inclusion in Union** :
    $\forall$ sets $A, B(A \subseteq A \cup B$ and $B \subseteq A \cup B)$
  - **Transitive property of subsets** :
    $A \subseteq B \wedge B \subseteq C \to A \subseteq C$
- **Set Identities** (Thm 6.2.2):
  - **Commutative Laws** : $\forall$ sets A, B
    $A \cup B = B \cup A$ and $A \cap B = B \cap A$
  - **Associative Laws** : $\forall$ sets A, B, C
    $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$
  - **Distributive Laws** : $\forall$ sets A, B, C
    $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and
    $A \cap (B \cup C) = (C \cap B) \cup (A \cap C)$
  - **Identity Laws** : $\forall$ sets $A, A \cup \varnothing = A$ and $A \cap U = A$
  - **Complement Laws** : $A \cup A^C = U$ and $A \cap A^C = \varnothing$
  - **Double Complement Law** : $\forall$ sets $A, (A^C)^C = A$
  - **Idempotent Laws** : $\forall$ sets A,
    $A \cup A = A$ and $A \cap A = A$
  - **Universal Bound Laws** : $\forall$ sets A,
    $A \cup U = U$ and $A \cap \varnothing = \varnothing$
  - **De Morgan's Laws** : $\forall$ sets A, B
    $(A \cup B)^C = A^C \cap B^C$ and $(A \cap B)^C = A^C \cup B^C$
  - **Absorption Laws** : $\forall$ sets A, B
    $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$
  - **Complements of U and $\varnothing$** :
    $U^C = \varnothing$ and $\varnothing^C = U$
  - **Set Difference Law** : $\forall$ sets A, B
    $A - B = A \cap B^C$
- **Intersection & Union with a Subset** (Thm 6.2.3)
  $\forall$ sets $A, B(A \subseteq B \to A \cap B = A \wedge A \cup B = B)$

7 Relations

Definitions

- **Ordered Pair** (Def 8.1.1):
  Let S be a non-empty set, and let x, y be two elements in S. The ordered pair is a mathematical object in which the first element of the pair is x and the second element is y.
  Notation: (x, y)
- **Equality of ordered pair** :
  Two ordered pairs (x, y) and (a, b) are equal if $x = a$ and $y = b$.
  e.g. $(3,4) \neq (4,3)$
- **Ordered n-tuple** (Def 8.1.2):
  Let n be a positive integer and let $x_1, x_2, \ldots, x_n$ be (not necessarily distinct) elements. The ordered n-tuple consists of $x_1, x_2, \ldots, x_n$ together with the ordering: first x_1, then x_2, and so forth up to x_n. An ordered 2-tuple is called an **ordered pair**, and an ordered 3-tuple is called an **ordered triple**.
  Notation: $(x_1, x_2, \ldots, x_n)$
  $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \Leftrightarrow x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$
  e.g. $(1,4,3) \neq (1,3,4).((1,2),3) \neq (1,2,3)$
- **Cartesian Product** (Def 8.1.3):
  Let S and T be two sets. The Cartesian product (or cross product) is the set such that $\forall X \forall Y((X,Y) \in S \times T \leftrightarrow (X \in S) \wedge (Y \in T))$
  Notation: $S \times T$
  Cartesian product is neither commutative nor associative.
- **Generalised Cartesian Product** (Def 8.1.4):
  $A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$.
  If V is a set of sets, then the Generalized Cartesian product of its elements will be written as: $\prod_{S \in V} S$

Relations

- **Binary relation** (Def 8.2.1):
  Let S and T be 2 sets. A binary relation from S to T is a subset of $S \times T$
  Notation: $\mathcal{R}$
  $s \mathcal{R} t \iff (s,t) \in \mathcal{R}$
  $x \not\mathcal{R} y \iff (x,y) \notin \mathcal{R}$

  Let $R \subseteq S \times T$ be a binary relation from S to T
- **Domain** (Def 8.2.2):
  The set $Dom(\mathcal{R}) = \{s \in S \mid \exists t \in T(s \mathcal{R} T)\}$
- **Image (or Range)** (Def 8.2.3):
  The set $Im(\mathcal{R}) = \{t \in T \mid \exists s \in S(s \mathcal{R} t)\}$
- **Co-domain** (Def 8.2.4):
  The set $coDom(\mathcal{R}) = T$
- **Prop 8.2.5** :
  Let $\mathcal{R}$ be a binary relation. $Im(\mathcal{R}) \subseteq coDom(\mathcal{R})$
- **Inverse** (Def 8.2.6):
  Let S, T be sets, $R \subseteq S \times T$ be a binary relation.
  The inverse of relation $\mathcal{R}$ is the relation from T to S such that $\forall s \in S, \forall t \in T(t\, \mathcal{R}^{-1}\, s \leftrightarrow s \mathcal{R} t)$
  Notation: $\mathcal{R}^{-1}$
- **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 is a subset of the Cartesian product $\prod_{i=1}^{n} S_i$. n is the **arity** or **degree** of the relation
  Notation: $\mathcal{R}$
- **Composition** (Def 8.2.8):
  Let S, T, U be sets, $\mathcal{R} \subseteq S \times T$ be a relation, $\mathcal{R}' \subseteq T \times U$ be a relation. The composition of $\mathcal{R}$ with $\mathcal{R}'$ is the relation from S to U s.t.
  $\forall x \in S, \forall z \in U(x\, \mathcal{R}' \circ \mathcal{R}\, z \leftrightarrow (\exists y \in T(x \mathcal{R} y \wedge y \mathcal{R}' z)))$
  In another word, $x \in S$ and $z \in U$ are related iff there is a "path" from x to z via some intermediary element $y \in T$
  Notation: $\mathcal{R}' \circ \mathcal{R}$
- **Composition is Associative** (Prop 8.2.9):
  Let S, T, U, V be sets, $\mathcal{R} \subseteq S \times T$ be a relation, $\mathcal{R}' \subseteq T \times U$ be a relation, $\mathcal{R}'' \subseteq U \times V$ be a relation.
  $\mathcal{R}'' \circ (\mathcal{R}' \circ \mathcal{R}) = (\mathcal{R}'' \circ \mathcal{R}') \circ \mathcal{R} = \mathcal{R}'' \circ \mathcal{R}' \circ \mathcal{R}$
- **Prop 8.2.10** :
  Let S, T, U be sets, $\mathcal{R} \subseteq S \times T$ be a relation, $\mathcal{R}' \subseteq T \times U$ be a relation.
  $(\mathcal{R}' \circ \mathcal{R})^{-1} = \underbrace{\mathcal{R}^{-1} \circ \mathcal{R}'^{-1}}_{\text{reversed}}$

Properties of Relations on a Set

- **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 $\iff \forall x, y \in A(x \mathcal{R} y \rightarrow y \mathcal{R} x)$
- **Transitive** (Def 8.3.3)
  $\mathcal{R}$ is transitive $\iff \forall x, y, z \in A((x \mathcal{R} y \wedge y \mathcal{R} z) \rightarrow x \mathcal{R} z)$
- In terms of drawing:
  - **Reflexive** : all dots must have a self-loop
  - **Symmetric** : every outgoing arrow to a dot must have an incoming arrow from that same dot.
  - **Transitive** : if an arrow goes from one dot to a second dot, and another arrow goes from the second to a third, then there must be an arrow going from the first to the third dot.

Equivalence Relations

- **Equivalence relation** (Def 8.3.4):
  Let $\mathcal{R}$ be a relation on set A. $\mathcal{R}$ is called an equivalence relation iff $\mathcal{R}$ is relfexive, symmetric and transitive.
- **Equivalence class** (Def 8.3.5):
  Let $x \in A$. The equivalence class of x is the set of all elements $y \in A$ that are in relation with x.
  $[x] = \{y \in A \mid x \mathcal{R} y\}$
  Notation: $[x]$
- **Partition induced by an equivalence relation** (Thm 8.3.4):
  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** :
  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** :
  If $\mathcal{R}$ is an equivalence relation on a set A, and a, b are elements in A, then either $[a] \cap [b] = \varnothing$ or $[a] = [b]$.
- **Equivalence relation induced by a partition** :
  Given a partition $S_1, S_2, \ldots$ of a set A, there exists an equivalence relation $\mathcal{R}$ on A whose equivalence classes make up precisely that partition.

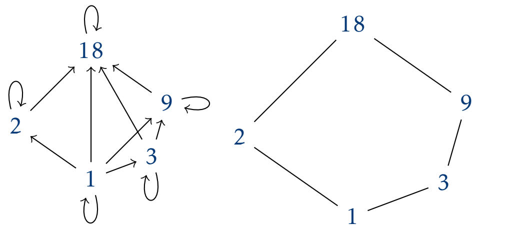
Additional Definitions

- **Transitive closure** (Def 8.5.1):
  Let A be a set. Let $\mathcal{R}$ be a relation on A. The transitive closure of R is a relation that satisfies these three properties:
  1. R^t is transitive.
  2. $R \subseteq R^t$
  3. If S is any other transitive relation such that $R \subseteq S$, then $R^t \subseteq S$.

  Notation: $\mathcal{R}^t$
- Thus we can say that the transitive closure is the smallest superset that is transitive.
- Similar definitions can be made for **reflexive closure** and **symmetric closure** of a relation.
- **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.
  - We define $\mathcal{R}^1 \triangleq \mathcal{R}$
  - We define $\mathcal{R}^2 \triangleq \mathcal{R} \circ \mathcal{R}$
  - We define $\mathcal{R}^n \triangleq \mathcal{R} \circ \ldots \circ \mathcal{R} \triangleq \bigodot_{i=1 \text{ to } n} \mathcal{R}$
- **Prop 8.5.2** :
  Let $\mathcal{R}$ be a relation on set A. Then,
  $\mathcal{R}^t = \bigcup_{i=1}^{\infty} \mathcal{R}^i$

Partial and Total Order

- **Anti-symmetric** (Def 8.6.1):
  $\mathcal{R}$ is anti-symmetric iff
  $\forall x \in A, \forall y \in A((x \mathcal{R} y \wedge x \mathcal{R} x) \rightarrow x = y)$
- **Partial Order** (Def 8.6.2):
  $\mathcal{R}$ is said to be a partial order if it is reflexive, anti-symmetric, and transitive.
  Notation: $\preceq$ (like $\leq$ but curly)
  A set A is called a **partially ordered set** (or **poset**) w.r.t. a relation $\preceq \iff \preceq$ is a partial order relation on A
- **Hasse Diagram** :

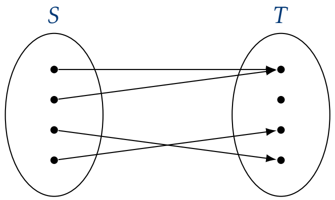


- How to convert to Hasse:
  1. Draw the directed graph so that all arrows point upwards.
  2. Eliminate all self-loops.
  3. Eliminate all arrows implied by the transitive property.
  4. Remove the direction of the arrows
- **Comparable** (Def 8.6.3):
  Let $\preceq$ be a partial order on set A. Elements $a, b \in A$ are **comparable** iff either $a \preceq b$ or $b \preceq a$. Otherwise, a, b are **non-comparable**. PS: comparable - there is a line in Hasse diagram connectint a and b
- **Total order (or linear order)** (Def 8.6.4):
  Let $\preceq$ be a partial order on set A. $\preceq$ is a total order iff $\forall x, y \in A(x \preceq y \vee y \preceq x)$
  In other words, $\preceq$ is total order if $\preceq$ is a partial order and all x, y are comparable.
  e.g. $(\mathbb{Z}, \leq)$ is a total order.
- **Maximal** (Def 8.6.5): can be more than one
  An element x is a maximal element iff
  $\forall y \in A(x \preceq y \rightarrow x = y)$
- **Maximum** (Def 8.6.6): only one (unique)
  An element is the maximum element iff
  $\forall x \in A(x \preceq \top)$
  Notation: $\top$
- **Minimal** (Def 8.6.7): can be more than one
  An element x is a minimal element iff
  $\forall y \in A(y \preceq x \rightarrow x = y)$
- **Minimum** (Def 8.6.8): only one (unique)
  An element is the minimum element iff
  $\forall x \in A(\bot \preceq x)$
  Notation: $\bot$
- **Well-ordering of Total Orders** (Def 8.6.9):
  Let $\preceq$ be a total order on set A. A is well-ordered iff every non-empty subset of A contains a minimum element, formally:
  $\forall S \in \wp(A)(S \neq \varnothing \rightarrow (\exists x \in S \forall y \in S(x \preceq y)))$
  e.g. $(\mathbb{N}, \leq)$ is well-ordered, $(\mathbb{Z}, \leq)$ is not well-ordered.

8 Functions

Definitions

- **Functions** (Def 7.1.1):



Let f be a relation s.t. $f \subseteq S \times T$. Then f is a function from S to T iff $\forall x \in S, \exists! y \in T(x\ f\ y)$
Notation: $f : S \to T$
Every dot in S must have **exactly one** outgoing arrow

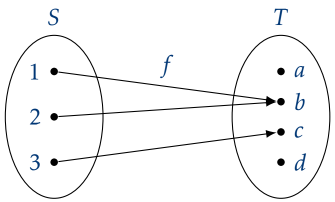
- **Pre-image** (Def 7.1.2):
Let $f : S \to T$ be a function, $x \in S$ and $y \in T$ s.t. $f(x) = y$. Then x is the pre-image of y.

- **Inverse image** (Def 7.1.3):
Let $f : S \to T$ be a function, $y \in T$. 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 $f : S \to T$ be a function, $U \subseteq T$. The inverse image of U is the set that contains all the pre-images of all elements of U: $\{x \in S \mid \exists y \in U, f(x) = y\}$

- **Restriction** (Def 7.1.5):
Let $f : S \to T$ be a function, $U \subseteq S$. The restriction of f to U is the set $\{(x, y) \in U \times T \mid f(x) = y\}$

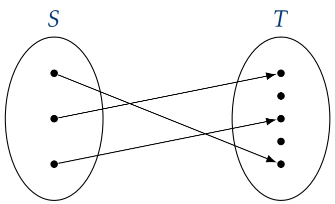
- Example:



  - pre-image of c is 3
  - inverse image of b is $\{1, 2\}$
  - inverse image of $\{a, d\}$ is $\emptyset$
  - inverse image of T is $\{1, 2, 3\}$
  - restriction of f to $\{2, 3\}$ is $\{\{2, b\}, \{3, c\}\}$

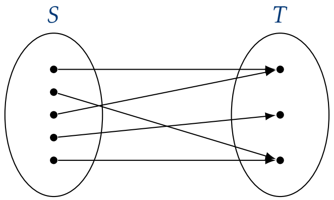
Properties

- **Injective/One-to-one** (Def 7.2.1):



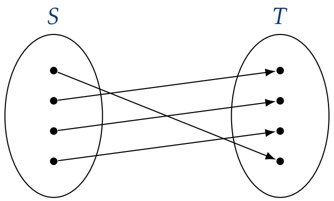
Let $f : S \to T$ be a function. f is injective iff $\forall y \in T, \forall x_1, x_2 \in S((f(x_1) = y \wedge f(x_2) = y) \to x_1 = x_2)$
Every dot in T has **AT MOST** one incoming arrow.

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



Let $f : S \to T$ be a function. f is surjective iff $\forall y \in T, \forall x \in S(f(x) = y)$
Every dot in T has **AT LEAST** one incoming arrow.

- **Bijective** (Def 7.2.3):



Let $f : S \to T$ be a function. f is bijective iff f is injective and f is surjective
Every dot in T has **EXACTLY** one incoming arrow.

- **Inverse** (Prop 7.2.4):
Let $f : S \to T$ be a function, 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):
Let $f : S \to T$ be a function, $g : T \to U$ be a function. The composition of f and g is a function from S to U
Notation: $g \circ f$

- **Identity function** (Def 7.3.2):
Given a set A, define function $\mathcal{I}_A$ from A to A by: $\forall x \in A(\mathcal{I}_A(x) = x)$
This is the **identity function** on A

- **Composition of inverse** (Prop 7.3.3):
Let $f : A \to A$ be an injective function on A. Then $f^{-1} \circ f = \mathcal{I}_A$

Generalisation

- **(n-ary) operation** (Def 7.3.4):
An **(n-ary) operation** on a set A is a function $f : \prod_1^n A \to A$.
n is called the **arity** or **degree** of the operation.

- **Unary operation** (Def 7.3.5):
A **unary operation** on a set A is a function $f : A \to A$.

- **Binary operation** (Def 7.3.6):
A **binary operation** on a set A is a function $f : A \times A \to A$

9 Counting & Probability

Definitions

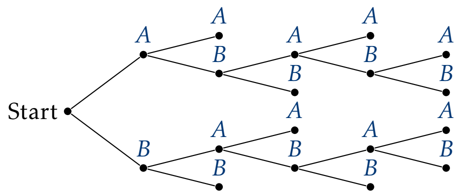
- **Sample space** :
the set of all possible outcomes of a random process or experiment.

- **Event** : a subset of a sample space.

- **Equally Likely Probability Formula** :
If S is a finite sample space in which all outcomes are equally likely and E is an event in S, then the **probability** of E, denoted $P(E)$, is:
$P(E) = \frac{\text{No. of outcomes in } E}{\text{Total no. of outcomes in } S} = \frac{N(E)}{N(S)}$

- **The 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.

Possibility Tree



- **Possible Ways in Tree** : represented by the distinct paths from "root" (the start) to "leaf" (a terminal point) in the tree.

The Multiplication Rule (Thm 9.2.1)

If an operation consists of k steps and
the 1st step can be performed in n_1 ways,
the 2nd step can be performed in n_2 ways,
(regardless of how the first step was performed),
$\vdots$
the k^{th} step can be performed in n_k ways
(regardless of how the preceding steps were performed),
Then the entire operation can be performed in $n_1 \times n_2 \times n_3 \times \ldots \times n_k$ ways.

Permutations

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

- **Formula** (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.
Notation: $P(n, r)$

- **r-Permutation formula** :
If $n, r \in \mathbb{Z}$ and $1 \leq r \leq n$, then the no. of r-permutations of a set of n elements is given by the formula $P(n, r) = n(n-1)(n-2)\ldots(n-r+1)$ or equivalently $P(n, r) = \frac{n!}{(n-r)!}$

Counting Elements of Disjoint Sets

- **The Addition Rule** (Thm 9.3.1):
Suppose a finite set A equals the union of k distinct mutually disjoint subsets $A_1, A_2, \ldots, A_k$. Then $N(A) = N(A_1) + N(A_2) + \ldots + N(A_k)$

- **The Difference Rule** (Thm 9.3.2):
If A is a finite set and $B \subseteq A$, then $N(A - B) = N(A) - N(B)$.

- **Formula for the Probability of the Complement of an Event**:
If S is a finite sample space and A is an event in S, then $P(A^C) = 1 - P(A)$

- **The 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.

- **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 positive integer k, if $k < n/m$, then there is some $y \in Y$ s.t. y is the image of at least $k + 1$ distinct elements of X.
e.g. Since $3 < 85/26$, the generalized pigeonhole

principle states that some initial must be the image of at least four (3 + 1) people.

- **Generalised Pigeonhole Principle** (Contrapositive form):
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; in other words, $n \leq km$.

- **The 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** (Thm 9.4.2):
Let X and 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.

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. Notation: $\binom{n}{r}, C(n,r), {}_nC_r, C_{n,r}, {}^nC_r$

- **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 of n objects of which
n_1 are of type 1 & indistinguishable fr each other
n_2 are of type 2 & indistinguishable fr each other
$\vdots$
n_k are of type k & indistinguishable fr each other
and suppose $n_1 + n_2 + ... + n_k = n$. Then the no. of distinguishable permutations of the n objects is
$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}...\binom{n-n_1-n_2-...-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!...n_k!}$

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

- **Number of r-combinations with repetition** (Thm 9.6.1):
The **no of r-combinations 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.

- **Summary** :

	Order Matters	Order doesn't matter
Repetition allowed	n^k	$\binom{k+n-1}{k}$
Repetition NOT allowed	$P(n,k)$	$\binom{n}{k}$

Pascal's Formula & the Binomial Thm

- **Pascal's Formula** (Thm 9.7.1):
Let $n, r \in \mathbb{Z}^+, r \leq n$, Then $\binom{n+1}{r} = \binom{n}{r-1}\binom{n}{r}$

- **Binomial Thm** (Thm 9.7.2):
Given any real numbers a, b and any non-negative integer n, then $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$
$= a^n + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + ... + \binom{n}{n-1}a^1 b^{n-1} + b^n$

Probability Axioms & Expected Values

- **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:
$\forall$ events A, 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 the Complement of an Event** :
If A is any event in a sample space S, then $P(A^C) = 1 - P(A)$

- **Probability of a General Union of 2 Events** :
If A, 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 $a_1, a_2, ..., a_n$ which occurs with probabilities $p_1, p_2, ..., p_n$. The **expected value** of the process is
$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + ... + a_n p_n$

Conditional Probability, Bayes' Formula, Independent Events

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

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)} \iff P(A \cap B) = P(B \mid A) \cdot P(A)$$

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

Notation: $P(B \mid A)$

- **Bayes' Thm** (Thm 9.9.1):
Suppose that a sample space S is a union of mutually disjoint events $B_1, B_2, B_3, ..., B_n$.
Suppose A is an event n S, and suppose $P(A) \neq 0$ and $P(B_i) \neq 0, \forall i \in \mathbb{Z}, 1 \leq i \leq n$.
If $k \in \mathbb{Z}, 1 \leq k \leq n$, then
$P(B_k \mid A) = \frac{P(A|B_k \cdot P(B_k))}{P(A|B_k) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + ... + P(A|B_n) \cdot P(B_n)}$

- **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 Independent & 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** iff they satisfy all 4 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. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

- **Mutually Independent** (for $n \geq 2$ events):
Events $A_1, A_2, ..., A_n$ in a sample space S are **mutually independent** iff the probability of the intersection of any subset of the events is the product of the probabilities of the events in the subset.
$P(A_1 \cap A_2 \cap ... \cap A_n) = P(A_1) \cdot P(A_2) \cdot ... \cdot P(A_n)$

10 Graphs

Definitions and Basic Properties

- **Graph** :
A **graph** G consists of 2 finite sets: a non-empty 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**.
An edge is said to **connect** its endpoints; 2 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**.
Notation: $e = \{v, w\}$ for an edge e incident on vertices v and w.

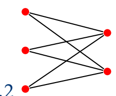
- **Directed Graph** :
A **directed graph** or **digraph** G consists of 2 finite sets: a non-empty set $V(G)$ of **vertices** and a set $D(G)$ of **directed edges**, where each edge is associated with an ordered pair of vertices called its **endpoints**.
If edge e is associated with the pair (v, w) of vertices, then e is said to be the **(directed) edge** from v to w.
Notation: $e = (v, w)$

- **Simple Graph** :
An undirected graph that does **not** have any **loops** or **parallel edges**.

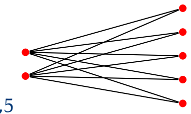
- **Complete Graph** :
A **complete graph** on n vertices, $n > 0$ is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices.
Notation: K_n

- **Complete Bipartite Graph** :
A **complete bipartite graph** on (m, n) vertices, where $m, n > 0$ is a simple graph with distinct vertices $v_1, v_2, ..., v_m$, and $w_1, w_2, ..., w_n$ that satisfies the following properties:
$\forall i, k = 1, 2, ..., m$ and $\forall j, l = 1, 2, ..., n$,
  1. There is an edge from each vertex v_i to each vertex w_j.
  2. There is no edge from each vertex v_i to any other vertex v_k.
  3. There is no edge from each vertex w_j to any other vertex w_l.

Notation: $K_{m,n}$



e.g. $K_{3,2}$



$K_{2,5}$

- **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.

- **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 equals the number of edges that are incident on v, with an edge that is a loop counted twice.
Notation: $deg(v)$.
The **total degree of a graph** is the sum of degrees of all the vertices of G.
PS: easy way to determine degree is draw a circle around a vertex and count the no of intersections

- **The Handshake Thm** (Thm 10.1.11):
If G is any graph, then the sum of the degrees of all the vertices of G equals twice the no of edges of G. Specifically, if the vertices of G are $v_1, v_2, ..., v_n$, where $n \geq 0$, then
The **total degree of** G= $deg(v_1) + deg(v_2) + ... + deg(v_n) = 2 \times$ (the no of edges of G)

- **Corollary 10.1.2** :
The total degree of a graph is even.

- **Prop 10.1.3** :
In any graph, there are an even no of vertices of odd degree.

Trails, Paths, and Circuits

Let G be a graph, 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 $v_0 e_1 v_1 e_2 ... v_{n-1} e_n v_n$, where the v's represent vertices, the e's represent edges, $v_0 = v, v_n = w$, and $\forall i \in \{1, 2, ..., n\}, v_{i-1}$ and v_i are endpoints of e_i.

- **Trivial Walk** from v to v consists of the single vertex v.

- **Trail** :
A **trail** from v to w is a walk 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 walk that starts and ends at the same vertex.
- **Circuit (Cycle)** :
A closed walk that contains at least one edge and does not contain a repeated edge.
- **Simple Circuit** :
A circuit that does not have any other repeated vertex except the first and last.
- **Summary** :

	Repeated edge	Repeated vertex	Starts and ends at same pt?	Must contain $\geq$ 1 edge
Walk	allowed	allowed	allowed	no
Trail	no	allowed	allowed	no
Path	no	no	no	no
Closed walk	allowed	allowed	yes	no
Circuit	no	allowed	yes	yes
Simple circuit	no	first and last only	yes	yes

- **Connectedness** :
Two vertices v and w of a graph G are **connected** iff there is a walk from v to w.
The graph G is connected iff given *any* 2 vertices v and w in G, there is a walk from v to w.
(G is connected $\Leftrightarrow \forall$ vertices $v, w \in V(G), \exists$ a walk from v to w)
- **Lemma on connectedness** (Lemma 10.2.1):
Let G be a graph.
  1. If G is connected, then any two distinct vertices of 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; and
  3. No connected subgraph of G has H has 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.
- **Eulerian Graph** :
A graph that contains an Euler circuit.
- **Thm 10.2.2** :
If a graph has an Euler circuit, then every vertex of the graph has positive even degree.
- **Contrapositive of Thm 10.2.2** :
If some vertex of a graph has odd degree, then the graph does not have an Euler circuit.
- **Thm 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.
- **Thm 10.2.4** :
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, v, w be 2 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.
- **Cor 10.2.5** :
Let G be a graph, v, w be 2 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.

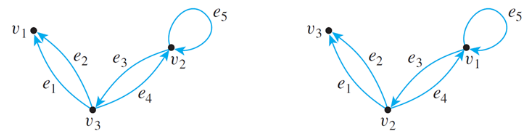
Hamiltonian Circuits

- **Hamiltonian Circuits** :
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 the last, which are the same.
- **Hamiltonian Graph** :
A graph that contains a Hamiltonian circuit.
- **Prop 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.

  PS: The contrapositive of Prop 10.2.6 says that if a graph G does **not** have a subgraph H with properties (1)-(4), then G does **not** have a Hamiltonian circuit.

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.
Notation: $A = (a_{ij})$
- **Adjacency Matrix of a Directed Graph** :
Let G be a directed graph with ordered vertices $v_1, v_2, ..., v_n$. The **adjacency matrix of** G is the $n \times n$ matrix $A = a_{ij})$ over the set of non-negative integers s.t.
a_{ij} = the number of arrows from v_i to v_j $\forall i, j = 1, 2, ..., n$.



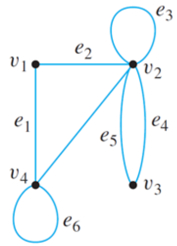
$$\begin{array}{c|ccc} & v_1 & v_2 & v_3 \\ \hline v_1 & 0 & 0 & 0 \\ v_2 & 0 & 1 & 1 \\ v_3 & 2 & 1 & 0 \end{array}$$

(a)

$$\begin{array}{c|ccc} & v_1 & v_2 & v_3 \\ \hline v_1 & 1 & 1 & 0 \\ v_2 & 1 & 0 & 2 \\ v_3 & 0 & 0 & 0 \end{array}$$

(b)

- **Adjacency Matrix of an Undirected Graph** :
Let G be an undirected graph with ordered vertices $v_1, v_2, ..., v_n$. The **adjacency matrix of** G is the $n \times n$ matrix $A = a_{ij})$ over the set of non-negative integers s.t.
a_{ij} = the number of edges connecting v_i and v_j $\forall i, j = 1, 2, ..., n$.



$$\mathbf{A} = \begin{array}{c|cccc} & v_1 & v_2 & v_3 & v_4 \\ \hline v_1 & 0 & 1 & 0 & 1 \\ v_2 & 1 & 1 & 2 & 1 \\ v_3 & 0 & 2 & 0 & 0 \\ v_4 & 1 & 1 & 0 & 1 \end{array}$$

PS: The matrix is **symmetric**
- **Symmetric Matrix** :
An $n \times n$ square matrix $A = (a_{ij})$ is called **symmetric** iff $a_{ij} = a_{ji}, \forall i, j = 1, 2, ..., n$
- **Thm 10.3.1** :
Let G be a graph with connected components $G_1, G_2, ..., G_k$. 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:

$$\begin{bmatrix} A_1 & 0 & 0 & & 0 & 0 \\ 0 & A_2 & 0 & \cdots & 0 & 0 \\ 0 & 0 & A_3 & & 0 & 0 \\ & \vdots & & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & A_k \end{bmatrix}$$

where each A_i is $n_i \times n_i$ adjacency matrix of G_i, $\forall i = 1, 2, ..., k$, and the 0s represent matrices whose entries are all 0's.
- **and so on...**