Revision notes - CS1231

Ma Hongqiang

August 11, 2017

Contents

1 Proof Techniques

1.1 Notations

$\exists$	:	There exists ...
$\exists!$	:	There exists a unique ...
$\forall$	:	For all ...
$\in$	:	Member of (a set)...
$\ni$	:	Such that

1.2 Methods of proof

- Proof by **Construction**

  Example: Prove the following: $\exists x \in \mathbb{Z} \ni x > 2 and x^2 - 5x + 6 > 0$

  1. Note that $1000 \in \mathbb{Z}$ and $1000 > 2$
  2. Also, $1000^2 - 5(1000) + 6 = 995006 > 0$

     QED

- Disproof by **Counterexample**

  Example: Disprove: $\forall x, y \in \mathbb{Z}^+, \sqrt{x+y} = \sqrt{x} + \sqrt{y}$

  1. Let $x = y = 2$. Clearly, they are nonnegative integers.
  2. Then $\sqrt{x+y} = \sqrt{2+2} = 2$,
  3. But, $\sqrt{x} + \sqrt{y} = 2\sqrt{2} = 2.828427\ldots$
  4. Thus, $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$, and the statement is false.

- Proof by **Contraposition**

- Proof by **Contradiction**

- Proof by **Mathematical Induction**

2 Logic of Compound Statements

2.1 Negation, Conjunction, Disjunction

Negation	$\sim p$
Conjunction	$p \wedge q$
Disjunction	$p \vee q$

2.2 Logical Equivalence

Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity laws	$p \wedge \texttt{true} \equiv p$	$p \vee \texttt{false} \equiv p$
Negation laws	$p \vee \sim p \equiv \texttt{true}$	$p \wedge \sim p \equiv \texttt{false}$
Double negative law	$\sim (\sim p) \equiv \texttt{true}$	
Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal bound laws	$p \vee \texttt{true} \equiv \texttt{true}$	$p \wedge \texttt{false} \equiv \texttt{false}$
De Morgan's laws	$\sim (p \wedge q) \equiv \sim p \vee \sim q$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation of true and false	$\sim \texttt{true} \equiv \texttt{false}$	$\sim \texttt{false} \equiv \texttt{true}$

2.3 If p,then q

Conditional	If p,then q	$p \rightarrow q$
	p only if$q$	
Contrapositive	If $\sim q$,then $\sim p$	$\sim q \rightarrow \sim p$
Converse	If q,then p	$q \rightarrow p$
Inverse	If $\sim p$,then $\sim q$	$\sim p \rightarrow \sim q$

2.3.1 Equivalence between conditionals

- $p \rightarrow q \equiv \sim q \rightarrow \sim p \equiv \sim p \vee q$
- $q \rightarrow p \equiv \sim p \rightarrow \sim q \equiv p \wedge \sim q$

2.3.2 Biconditional

Biconditional p if, and only if q, denoted as $p \leftrightarrow q$, is equivalent to $(p \rightarrow q) \wedge (q \rightarrow p)$. Biconditional $p \leftrightarrow q$ is true when $p \equiv q$ and false when $p \equiv \sim q$.

2.3.3 Necessary and Sufficient Conditions

If r and s are statements,

- "r is a sufficient condition for s" means $r \to s$.
- "r is a necessary condition for s" means $s \to r$.

2.4 Rules of Inference

1. Modus Ponens

   $p \to q$

   p

   - q

2. Modus Tollens

   $p \to q$

   $\sim q$

   - $\sim p$

3. Universal Modus Ponens

   $\forall x$, if $P(x)$ then $Q(x)$

   $P(a)$ for a particular a.

   - $Q(a)$

4. Universal Modus Tollens

   $\forall x$, if $P(x)$ then $Q(x)$

   $\sim Q(a)$ for a particular a.

   - $\sim Ps(a)$

5. Generalisation

   p

   - $p \vee q$

6. Conjunction

   p

   q

   - $p \wedge q$

7. Specialisation

$p \wedge q$

- p

8. Elimination

   $p \vee q$

   $\sim q$

   - p

9. Transitivity

   $p \to q$

   $q \to r$

   - $p \to r$

10. Division into cases

    $p \vee q$

    $p \to r$

    $q \to r$

    - r

11. Contradiction

    $\sim p \to$ `false`

    - p

3 Logic of Quantified Statements

Universal statement	$\forall x \in D, Q(x)$
Existential statement	$\exists x \in D$ such that $Q(x)$

3.1 Notation

- $P(x) \Rightarrow Q(x) \equiv \forall x, P(x) \rightarrow Q(x)$
- $P(x) \Leftrightarrow Q(x) \equiv \forall x, P(x) \leftrightarrow Q(x)$

3.2 Equivalent Form of Quantified Statement

The following are equivalent statements.

$$\forall x \in U, \text{if } P(x) \text{ then } Q(x) \equiv \forall x \in D = \{e \in U \mid P(e)\}, Q(x)$$

$$\exists x \text{ such that } P(x) \wedge Q(x) \equiv \exists x \in D = \{e \in U \mid P(e)\} \text{ such that } Q(x)$$

If $Q(x)$ is a predicate and the domain D of x is the set $x_1, x_2, \ldots, x_n$, then

$$\forall x \in D, Q(x) \equiv Q(x_1) \wedge Q(x_2) \wedge \ldots \wedge Q(x_n)$$

$$\exists x \in D \text{ such that } Q(x) \equiv Q(x_1) \vee Q(x_2) \vee \ldots \vee Q(x_n)$$

3.3 Negation

- $\sim (\forall x \in D, P(x)) \equiv \exists x \in D$ such that $\sim P(x)$
- $\sim (\exists x \in D$ such that $P(x)) \equiv \forall x \in D, \sim P(x)$
- $\sim (\forall x, P(x) \rightarrow Q(x)) \equiv \exists x \in D$ such that $P(x) \wedge \sim Q(x)$

3.4 Contrapositive, converse, inverse

Consider a universal statement of the form: $\forall x \in D, P(x) \rightarrow Q(x)$.

1. **Contrapositive**: $\forall x \in D, \sim Q(x) \rightarrow \sim P(x)$
2. **Converse**: $\forall x \in D, Q(x) \rightarrow P(x)$
3. **Inverse**: $\forall x \in D, \sim P(x) \rightarrow \sim Q(x)$

3.5 Formal Logical Notation

- $\forall x \in D, P(x)$ is written as $\forall x(x \in D \rightarrow P(x))$
- $\exists x \in D,$ such that $P(x)$ is written as $\exists x(x \in D \wedge P(x))$

4 Induction

4.1 Principle of Mathematical induction

Let $P(n)$ be a property that is defined for integers n, and let a be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true.
2. For all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true.

Then the statement

$$\text{for all integers } n \geq a, P(n)$$

is true.

4.2 Method of Proof by Mathematical Induction

Consider a statement of the form, "For all integers $n \geq a$, a property $P(n)$ is true."
To prove such a statement, perform the following two steps:
Step 1 (basis step): Show that $P(a)$ is true.
Step 2 (inductive step): Show that for all integers $k \geq a$, if $P(k)$ is true then $P(k+1)$ is true. To perform this step,

- suppose that $P(k)$ is true, where k is any particular but arbitrarily chosen integer with $k \geq a$.

  [This supposition is called the inductive hypothesis.]

  Then

- show that $P(k+1)$ is true.

4.3 Principle of String Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a), P(a+1), \ldots, P(b)$ are all true. (**basis step**)
2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. (**inductive step**)

Then the statement

$$\text{for all integers } n \geq a, P(n)$$

is true. (The supposition that $P(i)$ is true for all integers i from a through k is called the **inductive hypothesis**. Another way to state the inductive hypothesis is to say that $P(a), P(a+1), \ldots, P(k)$ are all true.)

5 Number Theory

5.1 Results from Chapter 1 Notes

Definition (Divisibility)**.**
If n and d are integers and $d \neq 0$ then n is **divisible** by d if, and only if, n equals d times some integer.
Instead of "n is divisible by d," we can say that

n is a multiple of d, or

d is a factor of n, or

d is a divisor of n, or

d divides n.

The notation $d \mid n$ is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = dk.$$

Theorem (4.3.1(Epp))**.**
For all integers a and b, if a and b are positive and a divides b, then $a \leq b$.

Theorem (4.1.1)**.**
$\forall a, b, c \in \mathbb{Z}$, if $a \mid b$ and $a \mid c$, then $\forall x, y \in \mathbb{Z}, a \mid (bx + cy)$

Theorem (4.3.3(Epp))**.**
For all integers a, b, and c, if a divides b and b divides c, then a divides c.

5.2 Prime Numbers

Definition (4.2.1 Prime Number)**.**
An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n.
An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

Proposition.
Every integer $n > 1$ is either prime or composite.

Proposition (4.2.2)**.**
For any two primes p and p', if $p \mid p'$ then $p = p'$.

Proposition (4.7.3(Epp))**.**
For any integer a and any prime number p, if $p \mid a$ then $p \nmid (a + 1)$.

Proposition (4.7.4)**.**
The set of prime numbers is infinite.

Theorem (4.2.3)**.**
If p is a prime and $x_1, x_2, \ldots, x_n$ are any integers such that $p \mid x_1 x_2 \cdots x_n$,

$$\text{then } p \mid x_i, \text{ for some } x_i (1 \leq i \leq n).$$

Theorem (4.3.5(Epp))**.**
Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

Algorithm (Sieve of Eratosthenes)**.**

1. Start by listing all integers greater than 1. Call this list C. Also, let L be an empty list.
2. Take the first number $p = 2$ in C, and add it to L. This is the first prime.
3. In C, cross out all multiples of p.
4. Let p be the next uncrossed number in C. This is the next prime. Add it to L, and repeat from Step 3.

5.3 Well Ordering Principle

Definition (4.3.1)**.**
An integer b is said to be a **lower bound** for a set $X \subseteq \mathbb{Z}$ if $b \leq x$ for all $x \in X$.

Theorem (4.3.2)**.**
If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then S has a least element.
If a non-empty set $S \subseteq \mathbb{Z}$ has an upper bound, then S has a greatest element.

Proposition (4.3.3)**.**
If a set S of integers has a least element, then the least element is unique.

Proposition (4.3.4)**.**
If a set S of integers has a greatest element, then the greatest element is unique.

Theorem (4.4.1)**.**
Given any integer a and any positive integer b, there exist unique integers q and r such that:

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

Theorem (Representation of Integers)**.**
Suppose n can be wriiten as $n = \Sigma_{i=0}^{m} r_i b^i$, then we may write n in base b as a sequence of the digits r_i, i.e

$$n = (r_m r_{m-1} \ldots r_1 r_0)_b$$

Definition (4.5.1)**.**
Let a and b be integers, not both zero. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the integer d satisfying:

- $d \mid a$ and $d \mid b$.
- $\forall c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$ then $c \leq d$.

Proposition (4.5.2)**.**
For any integers a, b, not both zero, their gcd exists and is unique.

Algorithm (Euclid's Algorithm for gcd)**.**

```
def gcd(I, CAN):
  # assumes I>0, CAN>=0
  # computes gcd using Euclid's algorithm
  while CAN > 0:
    DOIT = I % CAN
    (I, CAN) = (CAN, DOIT)
  return I
```

Theorem (4.5.3)**.**
Let a, b be integers, not both zero, and let $d = \gcd(a, b)$. Then there exist integers x, y such that:

$$ax + by = d.$$

Proposition (Non-uniqueness of Bezout's Identity)**.**
There are multiple solutions x, y to the equation $ax + by = d$.
Once a solution pair (x, y) is found, additional pairs may be generated by $(x + \frac{kb}{d}, y - \frac{ka}{d})$, where k is any integer.

Definition (4.5.4)**.**
Integers a and b are **relatively prime** (or **coprime**) iff $\gcd(a, b) = 1$.

Proposition (4.5.5)**.**
For any integers a, b, not both zero, if c is a common divisor of a and b, then $c \mid \gcd(a, b)$.

Proposition.
For all positive integers a, b, $a \mid b$ if, and only if, $\gcd(a, b) = a$.

Definition (4.6.1)**.**
For any non-zero integers a, b, their **least common multiple**, denoted $\operatorname{lcm}(a, b)$, is the positive integer m such that:

- $a \mid m$ and $b \mid m$,
- for all positive integers c, if $a \mid c$ and $b \mid c$, then $m \leq c$.

Proposition.
$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$

Proposition.
For all positive integers a and b, $\gcd(a, b) \mid \operatorname{lcm}(a, b)$.

5.4 Modulo Arithmetic

Definition (4.7.1)**.**

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

Theorem (8.4.1(Epp))**.**
Let a, b and n be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a-b)$

2. $a \equiv b \pmod{n}$

3. $a = b + kn$ for some integer k

4. a and b have the same (nonnegative) remainder when divided by n

5. $a \pmod{n} = b \pmod{n}$

Theorem (8.4.3(Epp))**.**
Let a, b, c, d and n be integers with $n > 1$, and suppose

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

Then

1. $(a+b) \equiv (c+d) \pmod{n}$

2. $(a-b) \equiv (c-d) \pmod{n}$

3. $ab \equiv cd \pmod{n}$

4. $a^m \equiv c^m \pmod{n}$ for all integers m.

Corollary (8.4.4(Epp))**.**
Let a, b and n be integers with $n > 1$. Then

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

or, equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

In particular, if m is a positive integer, then

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

Definition (4.7.2)**.**
For any integers a, n with $n > 1$, if an integer s is such that $as \equiv 1 \pmod{n}$, then s is called the **multiplicative inverse of a modulo n**. We may write the inverse as a^{-1}.
Because the commutative law still applies in modulo arithmetic, we also have $a^{-1}a \equiv 1 \pmod{n}$.

Theorem (4.7.3)**.**
For any integer a, its multiplicative inverse modulo n (where $n > 1$), a^{-1}, exists if, and only if, a and n are coprime.

Corollary (4.7.4)**.**
If $n = p$ is a prime number, then all integers a in the range $0 < a < p$ have multiplicative inverses modulo p.

Theorem (8.4.9(Epp))**.**
For all integers a, b, c and n with $n > 1$, if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

6 Sequence

6.1 Explicit Formula

In general, a sequence of numbers is denoted by:

$$a_0, a_1, a_2, a_3, \ldots$$

That is, $a_n = f(n)$, for some function $f()$ and $n \in \mathbb{N}$. The indexing variable is n.
For example, the Fibonacci sequence can be expressed as $f(n) = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$.

6.2 Recurrence Relation

Another way to express a sequence is to specify how a_n is related to its predecessors $a_{n-1}, a_{n-2}, \ldots$, called the **recurrence relation**, together with some **initial conditions**.
For example, the Fibonacci sequence can be expressed as $a_n = a_{n-1} + a_{n-2}$, with initial conditions $a_1 = 1, a_0 = 0$.

6.3 Summation and Product

Summation is as follows

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + \cdots + a_{n-1} + a_n = \begin{cases} 0 & \text{if } n < m \\ \sum_{i=m}^{n-1} a_i + a_n & \text{otherwise} \end{cases}$$

Multiplication is as follows

$$\prod_{i=m}^{n} a_i = a_m \times a_{m+1} \times \cdots \times a_{n-1} \times a_n = \begin{cases} 1 & \text{if } n < m \\ \sum_{i=m}^{n-1} a_i \times a_n & \text{otherwise} \end{cases}$$

Theorem (5.1.1(Epp))**.**
If $a_m, a_{m+1}, a_{m+2}, \ldots$ and $b_m, b_{m+1}, b_{m+2}, \ldots$ are sequences of real numbers and c is any real number, 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. $c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$
3. $(\prod_{k=m}^{n} a_k) \cdot (\prod_{k=m}^{n} b_k) = \prod_{k=m}^{n}(a_k \cdot b_k)$

6.4 Common Sequences

6.4.1 Arithmetic sequence

An arithmetic sequence is given by the recurrence:

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

where a, d are real constants.
The explicit formula is: $a_n = a + nd, \forall n \in \mathbb{N}$.
The sum of the first n terms is defined as $S_n = \sum_{i=0}^{n-1} a_i = \frac{n}{2}[2a + (n-1)d]$.

6.4.2 Geometric sequence

An geometric sequence is given by the recurrence:

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

where a, r are real constants.
The explicit formula is: $a_n = ar^n, \forall n \in \mathbb{N}$.
The sum of the first n terms is defined as $S_n = \prod_{i=0}^{n-1} a_i = \frac{a(r^n-1)}{r-1}$.
For the special case $|r| < 1$, the sum to infinity is $S_\infty = \frac{a}{1-r}$.

6.4.3 Square numbers

The square numbers is the sequence 0, 1, 4, 9, 16, 25,...
The explicit formula is $\forall n \in \mathbb{N}, \square_n = n^2$.
Also, $\square_n = 1 + 3 + \ldots + (2n-1)$.

6.4.4 Triangle numbers

The triangle numbers is the sequence 0,1,3,6,10,15,21,...
The explicit formula is $\forall n \in \mathbb{N}, \triangle_n = \frac{n(n+1)}{2}$.
Also, $\triangle_n = 0 + 1 + \ldots + n$.
Interestingly, $\forall n \in \mathbb{Z}^+, \triangle_n + \triangle_{n-1} = \square_n = (\triangle_n - \triangle_{n-1})^2$.

6.4.5 Fibonacci numbers

The Fibonacci sequence is usually defined recursively:

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

The explicit formula is:

$$\forall n \in \mathbb{N}, F_n = \frac{\phi^n - (-\phi)^{-n}}{\sqrt{5}} \quad \text{where } \phi = \frac{1+\sqrt{5}}{2}$$

6.4.6 Binomial numbers

The explicit formula is

$$\forall n, r \in \mathbb{N}\text{such that } r \leq n, \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

The recurrence relation and initial conditions are:

$$\forall n, r \in \mathbb{N}, \binom{n}{r} = \begin{cases} 1, & \text{if } r = 0 \text{ and } n \geq 0 \\ \binom{n-1}{r} + \binom{n-1}{r-1}, & \text{if } 0 < r \leq n \\ 0, & \text{otherwise} \end{cases}$$

Other identities include:

- $\binom{n}{r} = \binom{n}{n-r}$
- $\sum_{r=0}^{n} \binom{n}{r} = 2^n$
- $\sum_{r=0}^{n} \binom{n}{r} = 2 \times \sum_{r=0}^{n-1} \binom{n-1}{r}$

6.5 Solving Recurrences

To get an explicit closed form formula, methods include

1. Look it up.
2. Guess and check via ieration.
3. Use formula

Definition (Second-order Linear Homogeneous Recurrence Relation with Constant Coeffcients(5.4.1))**.**
A second-order linear homogeneous recurrence relation with constant coeffcients is 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 are real constants, $B \neq 0$ and k_0 is an integer constant.

Theorem (Distinct-Roots Theorem(5.8.3(Epp)))**.**
Suppose a sequence $a_0, a_1, a_2, a_3, \ldots$ satisfies a recurrence relation

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

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

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

has **two distinct roots** r and s, then $a_0, a_1, a_2, a_3, \ldots$ is given by the explicit formula

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

where C, D are real numbers determined by the initial conditions a_0, a_1.

Theorem (Single-Roots Theorem(5.8.5(Epp)))**.**
Suppose a sequence $a_0, a_1, a_2, \ldots$ satisfies a recurrence relation

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

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

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

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

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

where C, D are real numbers determined by the value a_0, and any other known value of the sequence.

7 Sets

Definition (Subset(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. We write $S \subseteq T$.

A set S is a **proper** subset, of T denoted $S \subsetneq T$ iff $S \subseteq T$ and there is at least one element in T that is not in S.

7.1 Basic Set Theory

Definition (Empty Set(6.3.1))**.**
An empty set has no element, and is denoted as $\varnothing$.
Mathematically, $\varnothing$ is such that:

$$\forall Y, \sim (Y \in \varnothing)$$

Theorem (6.2.4(Epp))**.**
An empty set is a subset of all sets.

$$\forall X, \forall Z((\forall Y, \sim (Y \in X)) \rightarrow (X \subseteq Z))$$

Definition (Set Equality(6.3.2))**.**
Two sets are equal if and only if they have the same elements.

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

Proposition (6.3.3)**.**
For any two sets X and Y, X is a subset of Y and Y is a subset of X if, and only if, $X = Y$.

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

Corollary (6.2.5(Epp))**.**
The empty set is unique.

$$\forall X_1, \forall X_2, ((\forall Y(\sim (Y \in X_1)) \wedge (\forall Y \sim (Y \in X_2))) \rightarrow X_1 = X_2)$$

Definition (6.3.4)**.**
Given any set S, the **power set** of S, denoted by $\mathcal{P}$, 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:

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

7.2 Operation on Sets

Definition (Union(6.4.1))**.**
Let S be a set of sets, then we say that T is the **union** of the sets in S, and write:

$$T = \cup S = \cup_{X \in S} X$$

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

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

For two sets A, B, we may simply write $T = A \cup B$.

Proposition (6.4.2)**.**
Let A, B, C be sets. Then,

- $\cup\varnothing = \cup_{A\in\varnothing} A = \varnothing$
- $\cup\{A\} = A$
- $A \cup \varnothing = A$
- $A \cup B = B \cup A$
- $A \cup (B \cup C) = (A \cup B) \cup C$
- $A \cup A = A$
- $A \subseteq B \leftrightarrow A \cup B = B$

Definition (Intersection(6.4.3))**.**
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 nothing more.
That is, given S, the set T is such that:

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

We write:

$$T = \cap S = \cap_{X\in S} X$$

For two sets A, B, we may simply write $T = A \cap B$.

Proposition (6.4.4)**.**
Let A, B, C be sets. Then,

- $A \cap \varnothing = \varnothing$
- $A \cap B = B \cap A$
- $A \cap (B \cap C) = (A \cap B) \cap C$
- $A \subseteq B \leftrightarrow A \cap B = A$

Distributivity laws:

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

Definition (Disjoint(6.4.5)).
Let S and T be two sets. S and T are **disjoint** iff$S \cap T = \varnothing$.

Definition (Mutually Disjoint(6.4.6)).
Let V be a set of sets. The sets $T \in V$ are **mutually disjoint** iff every two disinct sets are disjoint.

$$\forall X, Y \in V(X \neq Y \to X \cap Y = \varnothing)$$

Definition (Partition(6.4.7)).
Let S be a set, and let V be a set of non-empty subsets of S. Then V is called a **partition** of S iff

- The sets in V are mutually disjoint.
- The union of the sets in V equals S.

Definition (Non-symmetric difference(6.4.8)).
Let S and T be two sets. The **non-symmetric 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, nothing less and nothing more.

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

Definition (Symmetric difference(6.4.9)).
Let S and T be two sets. The **symmetric difference** of S and T, denoted $S \ominus T$ is the set whose elements belong to S or T but not both, nothing less and nothing more.

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

Definition (Set Complement(6.4.10)).
Let $\mathcal{U}$ be the Universal set (or the Unvierse of Discourse). And let A be a subset of $\mathcal{U}$. Then, the **complement** (or absolute complement) of A, denoted A^c, is $\mathcal{U} - A$.

Theorem (6.2.1(Epp)).

1 Inclusion of Intersection: For all sets A and B,

$A \cap B \subseteq A$ and $A \cap B \subseteq B$

2 Inclusion in Union: For all sets A and B,

$A \subseteq A \cup B$ and $B \subseteq A \cup B$

3 Transitive Property of Subsets: For all sets A, B, and C,

if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$

Theorem (6.2.2(Epp)).
Let all sets referred to below be subsets of a universal set U.

1. Commutative laws: For all sets A and B,

   $A \cup B = B \cup A$ and $A \cap B = B \cap A$

2. Associative Laws: For all sets A, B, and C,

   $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$

3. Distributive Laws: For all sets A, B, and C,

   $(A \cup B) \cap C = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

4. Identity Laws: For all sets A,

   $A \cup \varnothing = A$ and $A \cap U = A$

5. Complement Laws:

   $A \cup A^c = U$ and $A \cap A^c = \varnothing$

6. Double Complement Law: For all sets A,

   $(A^c)^c = A$

7. Idempotent Laws: For all sets A,

   $A \cup A = A$ and $A \cap A = A$

8. Universal Bound Laws: For all sets A,

   $A \cup U = U$ and $A \cap \varnothing = \varnothing$

9. De Morgan's Laws: For all sets A and B,

   $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$

10. Absorption Laws: For all sets A and B,

    $A \cup (A \cap B) = A$ and $A \cap (A \cup B) = A$

11. Complements of U and $\varnothing$:

    $U^c = \varnothing$ and $\varnothing^c = U$

12. Set Difference Law: For all sets A and B,

    $A - B = A \cap B^c$

Proposition (6.2.6(Epp))**.**
For all sets A, B, and C, if$A \subseteq B$ and $B \subseteq C^c$, then $A \cap C = \varnothing$.

Theorem (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.

8 Relation

Definition (Ordered Pair(8.1.1))**.**
Let S be a non-empty set, and let x, y be two elements in S.
The **ordered pair**, denoted (x, y), is a mathematical object in which the first element of the pair is x and the second element is y.
Two ordered pairs (x, y) and (a, b) are equal iff $x = a$ and $y = b$.

Definition (Ordered n-tuple(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**, $(x_1, x_2, \ldots, x_n)$, 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.

Definition (Cartesian Product(8.1.3))**.**
Let S and T be two sets. The **Cartesian product** of S and T, denoted $S \times T$ is the set such that:

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

Definition (Binary Relation)**.**
Let S and T be two sets. A **binary relation** from S to T, noted $\mathcal{R}$, is a subset of the Cartesian product $S \times T$.

The **domain** of $\mathcal{R}$ is the set $\mathcal{D}om(\mathcal{R}) = \{s \in S \mid \exists t \in T(s \mathrel{\mathcal{R}} t)\}$

The **image**(**range**) of $\mathcal{R}$ is the set $\mathcal{I}m(\mathcal{R}) = \{t \in T \mid \exists s \in S(s \mathrel{\mathcal{R}} t)\}$

The **co-domain** of $\mathcal{R}$ is the set $co\mathcal{D}om(\mathcal{R}) = T$

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

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

Definition (n-ary Relation(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** (**degree**) of the relation.

Definition (Composition of Relation(8.2.8))**.**
Let S, T and 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:

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

Proposition (Composition is Associative(8.2.9))**.**
Let S, T, U, V be sets. Let $\mathcal{R} \subseteq S \times T$ be a relation. Let $\mathcal{R}' \subseteq T \times U$ be a relation. Let $\mathcal{R}'' \subseteq U \times V$ be a relation.

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

Proposition (8.2.10)**.**
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.

$$(\mathcal{R}' \circ \mathcal{R})^{-1} = \mathcal{R}^{-1} \circ \mathcal{R}'^{-1}$$

8.1 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.

Definition (Reflexive, Symmetric, Transitive)**.**
$\mathcal{R}$ is said to be **reflexive** iff $\forall x \in A(x \mathrel{\mathcal{R}} x)$

$\mathcal{R}$ is said to be **symmetric** iff $\forall x, y \in A(x \mathrel{\mathcal{R}} y \rightarrow y \mathrel{\mathcal{R}} x)$.

$\mathcal{R}$ is said to be **transitive** iff $\forall x, y, z \in A((x \mathrel{\mathcal{R}} y \wedge y \mathrel{\mathcal{R}} z) \rightarrow x \mathrel{\mathcal{R}} z)$

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

Definition (Equivalence Class(8.3.5))**.**
Let $x \in A$. The **equivalence class** of x, denoted $[x]$, is the set of all elements $y \in A$ that are in relation with x.

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

Theorem (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 $a \mathrel{\mathcal{R}} b$ 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 $[a] \cap [b] = \varnothing$ or $[a] = [b]$.

Theorem (8.3.1(Epp))**.**
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.

Definition (Transitive Closure(8.5.1))**.**
Let A be a set. Let $\mathcal{R}$ 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 $\mathcal{R}^t \subseteq \mathcal{S}$.

Proposition (8.5.2)**.**
Let $\mathcal{R}$ be a relation on a set A. Then

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

where $\mathcal{R}^i$ is the i-th composition of $\mathcal{R}$ with itself.

8.2 Partial and Total Orders

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

Definition (Anti-symmetric(8.6.1))**.**
$\mathcal{R}$ is said to be **anti-symmetric** iff

$$\forall x \in A, \forall y \in A((x \mathcal{R} y \wedge y \mathcal{R} x) \to x = y)$$

Definition (Partial Order(8.6.2))**.**
$\mathcal{R}$ is said to be a **partial order** iff it is reflexive, anti-symmetric, and transitive.
Parital order is usually denoted by the symbol $\preccurlyeq$.

Definition (Comparable(8.6.3))**.**
Let $\preccurlyeq$ be a partial order on a set A. Element a, b of A are said to be **comparable** iff either $a \preccurlyeq b$ or $b \preccurlyeq a$. Otherwise, a and b are called **noncomparable**.

Definition (Total Order(8.6.4))**.**
Let $\preccurlyeq$ be a partial order on a set A. $\preccurlyeq$ is said to be a **total order** iff

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

In other words, $\preccurlyeq$ is a total order if $\preccurlyeq$ is a partial order and all x, y are comparable.

Definition (Maximal and Minimal)**.**
An element x is a **maximal element** iff $\forall y \in A(x \preccurlyeq y \to x = y)$.
An element x is a **minimal element** iff $\forall y \in A(y \preccurlyeq x \to x = y)$.

Definition (Maximum and Minimum)**.**
An element, usually noted $\top$, is the **maximum element** iff $\forall x \in A(x \preccurlyeq \top)$
An element, usually noted $\bot$, is the **minimum element** iff $\forall x \in A(\bot \preccurlyeq x)$.

9 Functions

Definition (Function(7.1.1))**.**
Let f be a relation such that $f \subseteq S \times T$. Then f is a **function** from S to T, denoted $f : S \to T$ iff

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

Or alternatively,

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

Definition (More definitions(7.1.2 - 7.1.5))**.**
Let $f : S \to T$ be a function. Let $x \in S$. Let $y \in T$ such that $f(x) = y$. Then x is called a **pre-image** of y.

Let $f : S \to T$ be a function. Let $y \in T$. The **inverse image** of y is the set of all its pre-images: $\{x \in S \mid f(x) = y\}$.

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

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

Definition (Injective(7.2.1))**.**
Let $f : S \to T$ be a function. f is **injective** iff

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

We say f is an injection or f is **one-to-one**.

Definition (Surjective(7.2.2))**.**
Let $f : S \to T$ be a function. f is **surjective** iff

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

We say f is a surjection or that f is **onto**.

Definition (Bijective(7.2.3))**.**
Let $f : S \to T$ be a function. f is **bijective** iff f is injective and f is surjective.

Proposition (Inverse(7.2.4))**.**
Let $f : S \to T$ be a function. Let f^{-1} be the inverse relation of f from T to S. The f is **bijective** iff f^{-1} is a function.

Proposition (Composition(7.3.1))**.**
Let $f : S \to T$ be a function. Let $g : T \to U$ be a function. The **composition** of f and g, $g \circ f$, is a function from S to U.

Definition (Identity Function(7.3.2))**.**
Given a set A, define a 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.

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

Definition (n-ary operation(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** (**degree**) of the operation.

10 Counting and Probability

10.1 Proability

Definition (Sample Space)**.**
A **sample space** is the set of all possible outcomes of a random process or experiment.

Definition (Event)**.**
An **event** is a subset of a sample space.

For a finite set A, $N(A)$ denotes the number of elements in A.

Theorem (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

$$P(E) = \frac{N(E)}{N(S)}$$

Theorem (9.1.1)**.**
If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

Theorem (Multiplication Rule(9.2.1))**.**
If an operation consists of k steps, and the first step can be performed in n_1 ways, $\cdots$, the k-th step can be performed in n_k ways. The entire operation can be performed in $n_1 \times n_2 \times \cdots \times n_k$ ways.

10.2 Permutation

Theorem (Permutation(9.2.2))**.**
The number of permutaions of a set with $n(n \geq 1)$ elements is $n!$.

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

Theorem (9.2.3)**.**
if n and r are integers and $1 \leq r \leq n$, then the number of r-permutation of a set of n elements is given by

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

Theorem (Addition Rule(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

$$N(A) = N(A_1) + N(A_2) + \cdots + N(A_k)$$

Theorem (Difference Rule(9.3.2))**.**
If A is a finite set and B is a subset of A, then

$$N(A - B) = n(A) - N(B)$$

Theorem (Probability of Complement)**.**
If S is a finite sample space and A is an event in S, then

$$P(A^c) = 1 - P(A)$$

Theorem (Inclusion/Exculsion Rule(9.3.3))**.**
If A, B and C are any finite sets, then

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

10.3 Pigeonhole Principle

Theorem (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 $k < \frac{n}{m}$, then there is some $y \in Y$ such that y is the image of at least $k + 1$ distinct elements of X.

Theorem (Generalised Pigeohole 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 positive integer k, if for each $y \in Y$, $f^{-1}(y)$ has at most k elements, then X has at most km elements; in other words, $n \leq km$.

Theorem (Pigeonhole Principle(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.

Theorem (One-to-one and Onto for Finite Sets(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 if, and only if, f is onto.

10.4 Combination

Definition (r-combination)**.**
Let n and 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, denoted by $\binom{n}{r}$.

Theorem (9.5.1)**.**
r-combinations from a set of n elements, $\binom{n}{r}$ is given by the formula

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

Theorem (Permutations with set of indistinguishable objects(9.5.2))**.**
Suppose a collection consists of n objects of which, n_1 are of type 1 and are indistinguishable from each other,$\cdots$, n_k are of the type k, and suppose that $n_1 + n_2 + \cdots + n_k = n$. Then the number of distinguishable permutations of the n objects is

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

Definition (r-combination with repetition allowed)**.**
An r**-combination with repetition allowed**, chosen from a set X of n elements is an unordered selection of elements taken from X with repetition allowed.

Theorem (9.6.1)**.**
The number of r-combination with repetition allowed that can be selected from a set of n elements is

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

10.5 Pascal's Formula and Binomial Theorem

Theorem (Pascal's Formula(9.7.1))**.**
Suppose n and r are positive integers with $r \leq n$. Then,

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

Theorem (Binomial Theorem(9.7.2))**.**
Given any real number a and b and any non-negative integer n,

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

To sum up,

	Order Matters	Order Does Not Matter
Repetition is Allowed	n^k	$\binom{n+k-1}{k}$
Repetition is Not Allowed	$P(n,k)$	$\binom{n}{k}$

10.6 More on Probability

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

Definition (Expected Value)**.**
Suppose the possible outcomes of an experiment, or random process, are real numbers $a_1, a_2, a_3, \cdots, a_n$ which occur with proabilities $p_1, p_2, p_3, \cdots, p_n$. The **expected value** of the process is

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

Definition (Conditional Proability)**.**
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 $P(B \mid A)$, is

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

Definition (Bayes' Theorem)**.**
Suppose that a sample space S is a union of mutually disjoint events $B_1, B_2, \cdots, B_n$.
Suppose A is an event in S, and suppose A and all the B_i have non-zero probabilities.
If k is an integer with $1 \leq k \leq n$, then

$$P(B_k \mid A) = \frac{P(A \mid B_k) \cdot P(B_k)}{P(A \mid B_1) \cdot P(B_1) + \cdots + P(A \mid B_n) \cdot P(B_n)}$$

Definition (Independent Events)**.**
If A and B are events in a sample space S, then A and B are **independent**, if and only if,

$$P(A \cap B) = P(A) \cdot P(B)$$

This gives, $P(A \cap B) = P(A) \cdot P(B)$ and $P(A) \neq 0 \Leftrightarrow P(B \mid A) = P(B)$.

Definition (Pairwise Independent and Mutually Independent)**.**
Let A, B and C be events in a sample space S. A, B and C are **pariwise independent**, if and only if, they satisfy conditions 1 - 3 below.
They are **mutually independent** if and only 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. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

More generally, events $A_1, A_2, \cdots, A_n$ in a sample space S are **mutually independent** if and only if, the probability of the intersection of any subset of the events is the product of the probabilities of the events in the subset.

11 Graphs

11.1 Graphs

Definition (Graph)**.**
A **graph** G consists of 2 finite sets: a nonempty set $V(G)$ of **vertices** and a set of $E(G)$ of **edges**, where eaech edge is associated with a set consisting of either one or two vertices called its **endpoints**.
An 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 iteslf**.
An edge is said to be **incident on** eacho f 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.

Definition (Directed Graph)**.**
A **directed graph** 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 $e = (v, w)$.

Definition (Simple Graph)**.**
A **simple graph** is an undirected graph that does not have any loops or parallel edges.

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

Definition (Complete Bipartite Graph)**.**
A **complete bipartite graph** on (m, n) vertices, where $m, n > 0$, denoted $K_{m,n}$, is a simple graph with distinct vertices $v_1, v_2, \ldots, v_m$, and $w_1, w_2, \ldots, l_n$ that satisfies the following properties:
For all $i, k = 1, 2, \ldots, m$ and for all $j, l = 1, 2, \ldots, n$,

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.

Definition (Subgraph)**.**
A graph H is said to be a **subgraph** of graph G, if and only if , 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.

Definition (Degree)**.**
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.

Theorem (The Handshake Theorem(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 $v_1, v_2, \ldots, v_n$, where $n \geq 0$, then

$$\text{The total degree of } G = \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n) = 2 \times \text{the number of edges of } G$$

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.

11.2 Trails, Path and Circuits

Definition (Walk)**.**
Let G be a graph, and let v and w be vertices of G.
A **walk** from v to w is a finite alternating sequence of adjacent vertices and edges of G. Thus a walk has the form

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

where the v's represent vertices, the e's represent edges, $v_0 = v$, $v_n = w$, and for all $\imath \in \{1, 2, \ldots, n\}$, v_{i-1} and v_i are the endpoints of e_i.
The trivial walk from v to v consists of the single vertex v.

Definition (Trail)**.**
A **trail** from v to w is a walk from v to w that does not contain a repeated edge.

Definition (Path)**.**
A **path** from v to w is a trial that does not contain a repeated vertex.

Definition (Closed Walk)**.**
A **closed walk** is a walk that starts and ends at the same vertex.

Definition (Circuit)**.**
A **circuit** is a closed walk that contains at least one edge and does not contain a repeated edge.

Definition (Simple Circuit)**.**
A **simple circuit** is a circuit that does not have any other repeated vertex except the first and last.

In summary,

	Repeated Edge?	Repeated Vertex?	Starts and Ends at Same Point	At Least One 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

Definition (Connectedness)**.**
Two vertices v and w of a graph G are **connected**, if and only if, tehre is a walk from v to w.
The graph G is **conntected**, if and only if, given any two vertices$v$ and w in G, there is a walk from v to w. Symbolically,

$$G \text{ is connected iff } \forall \text{ vertices } v, w \in V(G), \exists \text{a walk from } v \text{ to } w$$

Lemma (10.2.1)**.**
Let G be a graph.

- If G is connected, then any two distinct vertices of G can be connected by a path.
- 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.
- If G is connected and G contains a circuit, then an edge of the circuit can be removed without disconnecting G.

Definition (Connected Component)**.**
A graph H is a **connected component** of a graph G, if and only if,

- The graph H is a subgraph of G;
- The graph H is connected; and
- No connected subgraph of G has H as a subgraph and contains vertices or edges that are not in H.

Definition (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 has a Euler circuit, then every vetex of the graph has positive *even* degree.
Contrapositive: 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)**.**
A graph G has a Euler circuit, if and only if G is connected and every vertex of G has positive even degree.

Definition (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 if and only if

- G is connected;
- v and w has odd degree; and
- all other vertices of G have positive even degree

Definition (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 the last, which are the same.

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.

Hence, the contrapositive says, if a graph G does not have a subgraph H with properties 1 - 4, then G does not have a Hamiltonian circuit.

11.3 Matrix Representation of Graph

Definition (Adjacency Matrix of a Directed Graph)**.**
Let G be a directed graph with ordered vertices $v_1, v_2, \ldots, v_n$. 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 $i, j = 1, 2, \ldots, n$.

Definition (Adjacency Matrix of an undirected Graph)**.**
Let G be an undirected graph with ordered vertices $v_1, v_2, \ldots, v_n$. 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 $i, j = 1, 2, \ldots, n$.

Theorem (10.3.1)**.**
Let G be a graph with connected components $G_1, G_2, \ldots, G_k$, 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:

$$\begin{bmatrix} \boldsymbol{A_1} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \boldsymbol{A_2} & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \boldsymbol{A_k} \end{bmatrix}$$

where each $\boldsymbol{A_i}$ is $n_i \times n_i$ adjacency matrix of G_i, for all $i = 1, 2, \ldots, k$, and the $\mathbf{0}$'s represent matrices whose entries are all 0s.

Theorem (10.3.2)**.**
If G is a graph with vertices $v_1, v_2, \ldots, v_m$ and $\boldsymbol{A}$ is the adjacency matrix of G, then for each positive integer n and for all integers $i, j = 1, 2, \ldots, m$,
the (i, j)-th entry of $\boldsymbol{A}^n =$ the number of walks of length n from v_i to v_j.

11.4 Isomorphism

Definition (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' if and only if, there exists one-to-one correspondences $g : V(G) \to V(G')$ and $h : E(G) \to E(G')$ that preserve the edge-endpoint functions of G and G' in the sense that for all $v \in V(G)$ and $e \in E(G)$,

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

Theorem (10.4.1)**.**
Let S be a set of graphs and let $\mathcal{R}$ be the relation of graph isomorphism on S. Then $\mathcal{R}$ is an equivalence relation on S.

Definition (Invariant for Graph Isomorphism).
A property P is called an **invariant for graph isomorphism** if and only if, given any graphs G and G', if G has property P and g' is isomorphic to G, then G' has property P.

Theorem (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.

Definition (Graph Isomorphism for Simple Graphs).
If G and G' are simple graphs, then G is **isomorphic** to G' if and only if, there exists a one-to-one correspondence g from the vertex set $V(G)$ of G to the 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,

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

12 Trees

Definition (Tree)**.**
A graph is said to be **circuit-free** if and only if it has no circuits.
A graph is called a **tree** if and only if it is *circuit-free* and *connected.*
A trivial tree is a graph that consists of a single vertex.
A graph is called a **forest**, if and only if it is *circuit-free* and *not connected.*

Lemma (10.5.1)**.**
Any non-trivial tree has at least one vertex of degree 1.

Definition (Terminal Vertex and Internal Vertex)**.**
Let T be a tree. If T has only one or two vertices, then each is called a **terminal vertex**. If T has at least three vertices, then a vertex of degree 1 in T is called a **terminal vertex**, 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.

Theorem (10.5.4)**.**
If G is a connected graph wih n vertices and $n - 1$ edges, then G is a tree.

12.1 Rooted Trees

Definition (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**.
The **level** of a vertex is the number of edges along the unique path between it and the root.
The **height** of a rooted tree is the maximum level of any vertex of the tree.
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.
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**.
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.

12.2 Binary Trees

Definition (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**, and every parent has at most one left child and one right child.
A **full binary tree** is a binary tree in which each parent has exactly two children.

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.

Theorem (Full Binary Tree Theorem(10.6.1))**.**
If T is a full binary tree with k internal verticfes, then T has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices.

Theorem (10.6.2)**.**
For non-negative integers h, if T is any binary tree with height h and t terminal vertices, then

$$t \leq 2^h$$

12.2.1 Binary Tree Traversal

Tree traversal is the process of visiting each node in a tree data structure exactly once in a systematic manner.
There are two types of traversal: **breadth**-first search or **depth**-first search.
In breadth-first search, it starts at the root and visits its adjacent vertices, and then moves to the next level.
In depth-first search, there are three types of depth-first traversasl: Pre-order, In-order and Post-order.

- Pre-order
    - Print the data of the root.
    - Traverse the left subtree by recursively calling the pre-order function
    - Traverse the right subtree by recursively calling the pre-order function

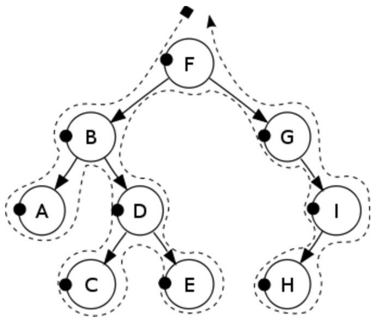

Figure 1: F,B,A,D,C,E,G,I,H

- In-order
    - Traverse the left subtree by recursively calling the in-order function

  - Print the date of the root
  - Traverse the right subtree by recursively calling the in-order function

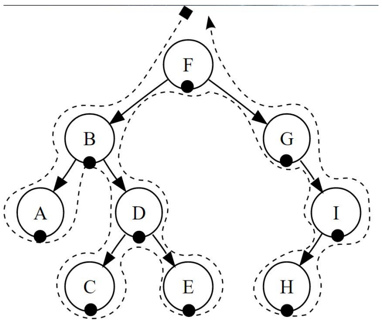

Figure 2: A,B,C,D,E,F,G,H,I

- Post-order
  - Traverse the left subtree by recursively calling the post-order function
  - Traverse the right subtree by recursively calling the post-order function
  - Print the data of the root

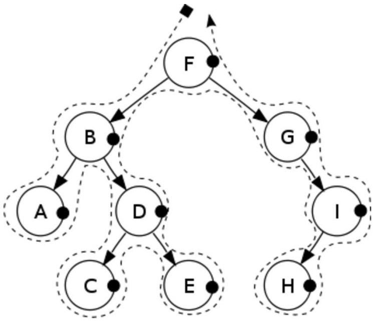

Figure 3: A,C,E,D,B,H,I,G,F

12.3 Spanning Trees and Shortest Path

Definition (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 number of edges.

Definition (Weighted graph and Minimum Spanning Tree)**.**
A **weighted graph** is a graph for which each edge has an associated positive real number **weight**. The sum of the weights of all the edges is the **total weight** of the graph.
A **mininum 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.
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.

Algorithm (Kruskal)**.**
Input: G [a connected weighted graph with n vertices]
Algorithm:

```
1. Initialise $T$ to have all the vertices of $G$ and no edges.
2. Let $E$ be the set of all the edges of $G$, and let $m = 0$.
3. While $(m < n - 1)$
    3a. Find an edge $e$ in $E$ of least weight.
    3b. Delete $e$ from $E$.
    3c. 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 $m = m + 1$.
   End while
```

Algorithm (Prim)**.**
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 $n - 1$
    3a. 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 eedges connecting $T$ to a vertex in $V$. Let $w$ be
        the endpoint of $e$ that is in $V$.
    3b. Add $e$ and $w$ to the edge and vertex sets of $T$, and delete $w$ from $V$.
```

Output: T [T is a mininum spanning tree for G.]

Algorithm (Dijkstra)**.**
Input: G [a connected simple graph with positive weight for every edge].∞ [a number 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 destination vertex].
Algorithm:

```
1 Initialise $T$ 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 Initialise $v$ to equal $a$ and $F$ to be $\{a\}$.
  [The symbol $v$ is used to denote the vertex most recently added to $T$.]
  Let Adj($x$) denote the set of vertices adjacent ot vertex $x$.

4 while($z \notin V(T)$)

    a. $F \leftarrow (F - \{v\}) \cup \{\text{vertices } \in \text{Adj}(v) \text{ and } \notin V(T)\}$
       [The set $F$ is the set of fringe vertices.]
    b. For each vertex $u \in \text{Adj}(v)$ 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 $z$]
```

13 Appendix 1: Definitions

This Appendix contains useful definitions from textbook.

Definition (Even and Odd Numbers)**.**
An integer n is **even** if, and only if, n equals twice some integer.
An integer n is odd, if, and only if, n equals twice some integer plus 1.

Definition (Prime Number)**.**
An integer n is **prime** if, and only if, $n > 1$ and for all positive integers r and s, if $n = rs$, then either r or s equals n.
An integer n is **composite** if, and only if, $n > 1$ and $n = rs$ for some integers r and s with $1 < r < n$ and $1 < s < n$.

Definition (Rational and Irrational Number)**.**
A real number r is rational if, and only if, it can be expressed as a quotient of twointegers with a nonzero denominator. A real number that is not rational is irrational.
More formally, if r is a real number, then

$$r \text{ is rational} \Leftrightarrow \exists \text{ integers } a \text{ and } b \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0$$

Definition (Root of Polynomial)**.**
A number c is called a root of a polynomial $p(x)$ if, and only if, $p(c) = 0$.

Definition (Divisibility)**.**
If n and d are integers and $d \neq 0$ then n is **divisible** by d if, and only if, n equals d times some integer.
Instead of "n is divisible by d," we can say that

n is a multiple of d, or

d is a factor of n, or

d is a divisor of n, or

d divides n.

The notation $d \mid n$ is read "d divides n." Symbolically, if n and d are integers and $d \neq 0$:

$$d \mid n \Leftrightarrow \exists \text{ an integer } k \text{ such that } n = dk.$$

Definition (Standard Factored Form)**.**
Given any integer $n > 1$, the **standard factored form** of n is an expression of the form

$$n = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k},$$

where k is a positive integer; $p_1, p_2, \ldots, p_k$ are prime numbers; $e_1, e_2, \ldots, e_k$ are positive integers; and $p_1 < p_2 < \ldots < p_k$.

Definition (Decimal Representation)**.**
Given any nonnegative integer n, the **decimal representation** of n is an expression of the form

$$d_k d_{k-1} \cdots d_2 d_1 d_0,$$

where k is a nonnegative integer; $d_0, d_1, d_2, \ldots, d_k$ (called the **decimal digits** of n) are integers from 0 to 9 inclusive; $d_k \neq 0$ unless $n = 0$ and $k = 0$; and

$$n = d_k 10^k + d_{k-1} 10^{k-1} + \cdots + d_2 10^2 + d_1 10 + d_0.$$

Definition (*div* and *mod*)**.**
If n and d are integers and $d > 0$, then

$$ndivd = q\text{and}nmodd = r \Leftrightarrow n = dq + r$$

where q and r are integers and $0 \leq r < d$.

Definition (Absolute Value)**.**
For any real number x, the **absolute value** of x, denoted $|x|$, is defined as follows:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Definition (Floor)**.**
If x is a real number and n is an integer, then

$$\lfloor x \rfloor = n \Leftrightarrow n \leq x < n + 1.$$

Definition (Ceiling)**.**
If x is a real number and n is an integer, then

$$\lceil x \rceil = n \Leftrightarrow n - 1 < x \leq n.$$

Definition (Greatest Common Divisor)**.**
Let a and b be integers that are not both zero. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is that integer d with the following properties:

1. d is a common divisor of both a and b. In other words,

   $$d \mid a \text{ and } d \mid b.$$

2. For all integers c, if c is a common divisor of both a and b, then c is less than or equal to d. In other words,

   $$\text{for all integers } c, \text{ if } c \mid a \text{ and } c \mid b, \text{ then } c \leq d.$$

Algorithm (4.8.2 Euclidean Algorithm)**.**
[*Given two integers A and B with $A > B \geq 0$, this algorithm computes* $\gcd(A, B)$*. It is based on two facts:*

1. $\gcd(a,b) = \gcd(b,r)$ *if* a, b, q *and* r *are integers with* $a = b \cdot q + r$ *and* $0 \leq r < b$.

2. $\gcd(a,0) = a$.]

```
Input: A, B [integers with $A > B \geq 0$] Algorithm Body:
    $a := A, b := B, r := B$
    [If $b \neq 0$, compute $a \mod b$, the remainder of the integer division of $a$ by $b$, and set $r$
    equal to this value. Then repeat the process using $b$ in place of $a$ and $r$ in place of $b$.]
    while ($b \neq 0$)
            $r := a \mod b$
    [The value of $a \mod b$ can be obtained by calling the division algorithm.]
            $a := b$
            $b := r$
    end while
    [After execution of the while loop, $\gcd(A,B) = a$.]
    gcd := $a$
Output: gcd [a positive integer]
```

Definition (Modulo)**.**

$$m \equiv n \pmod d \Leftrightarrow d \mid (m - n)$$

Definition (Linear Combination of Integer)**.**
An integer d is said to be a **linear combination of integers** a and b if, and only if, there exist integers s and t such that $as + bt = d$.

Definition (Coprime)**.**
Integers a and b are **relatively prime** if, and only if, $\gcd(a,b) = 1$. Integers $a_1, a_2, a_3, \ldots, a_n$ are **pairwise relatively prime** if, and only if, $\gcd(a_i, a_j) = 1$ for all integers i and j with $1 \leq i, j \leq n$, and $i \neq j$.

Definition (Inverse Relation)**.**
Let $\mathcal{R}$ be a relation from A to B. Define the inverse relation $\mathcal{R}^{-1}$ fom B to A as follows:

$$\mathcal{R}^{-1} = \{(y,x) \in B \times A \mid (x,y) \in \mathcal{R}\}$$

14 Appendix 2: Theorems

Theorem (4.1.1)**.**
The sum of any two even integers is even.

Theorem (4.2.1)**.**
Every integer is a rational number.

Theorem (4.2.2)**.**
The sum of any two rational numbers is rational.

Theorem (4.3.1)**.**
For all integers a and b, if a and b are positive and a divides b, then $a \leq b$.

Theorem (4.3.2)**.**
The only divisors of 1 are 1 and -1.

Theorem (4.3.3)**.**
For all integers a, b, and c, if a divides b and b divides c, then a divides c.

Theorem (4.3.4)**.**
Any integer $n > 1$ is divisible by a prime number.

Theorem (4.3.5)**.**
Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = {p_1}^{e_1}{p_2}^{e_2} \cdots {p_k}^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

Theorem (4.4.1)**.**
Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d$$

Theorem (4.4.2)**.**
Any two consecutive integers have opposite parity.

Theorem (4.4.3)**.**
The square of any odd integer has the form $8m + 1$ for some integer m.

Lemma (4.4.4)**.**
For all real numbers r, $-|r| \leq r \leq |r|$.

Lemma (4.4.5)**.**
For all real numbers r, $|-r| = |r|$.

Theorem (4.4.6)**.**
For all real numbers x and y, $|x + y| \leq |x| + |y|$.

Theorem (4.5.1)**.**
For all real numbers x and all integers m, $\lfloor x+m \rfloor = \lfloor x \rfloor + m$.

Theorem (4.5.2)**.**
For any integer n,

$$\lfloor \frac{x}{2} \rfloor = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Theorem (4.5.3)**.**
If n is any integer and d is a positive integer, and if $q = \lfloor n/d \rfloor$ and $r = n - d\lfloor n/d \rfloor$, then

$$n = dq + r \text{ and } 0 \leq r < d.$$

Theorem (4.6.1)**.**
There is no greatesst integer.

Theorem (4.6.2)**.**
There is no integer that is both even and odd.

Theorem (4.6.3)**.**
The sum of any rational number and any irrational number is irrational.

Proposition (4.6.4)**.**
For all integers n, if n^2 is even then n is even.

Theorem (4.7.1)**.**
$\sqrt{2}$ is irrational.

Proposition (4.7.3)**.**
For any integer a and any prime number p, if $p \mid a$ then $p \nmid (a+1)$.

Proposition (4.7.4)**.**
The set of prime numbers is infinite.

Lemma (4.8.1)**.**
If r is a positive integer, then $\gcd(r, 0) = r$.

Lemma (4.8.2)**.**
If a and b are any integers not both zero, and if q and r are any integers such that $a = bq+r$, then $\gcd(a, b) = \gcd(b, r)$.

Theorem (5.2.2)**.**
For all integers $n \geq 1$,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Theorem (5.2.3)**.**
For any real number r except 1, and any integer $n \geq 0$,

$$\Sigma_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

Proposition (5.3.1)**.**
For all integers $n \geq 0$, $2^{2n} - 1$ is divisible by 3.

Proposition (5.3.2)**.**
For all integers $n \geq 3$, $2n + 1 < 2^n$.

Theorem (5.4.1)**.**
Given any positive integer n, n has a unique representation in the form

$$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 2^2 + c_1 \cdot 2 + c_0,$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$.

Theorem (Well Ordering Principle for the Integers)**.**
Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element.

Theorem (8.4.1)**.**
Let a, b and n be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some integer k
4. a and b have the same (nonnegative) remainder when divided by n
5. $a \pmod{n} = b \pmod{n}$

Theorem (8.4.3)**.**
Let a, b, c, d and n be integers with $n > 1$, and suppose

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

Then

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$ for all integers m.

Corollary (8.4.4)**.**
Let a, b and n be integers with $n > 1$. Then

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

or, equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

In particular, if m is a positive integer, then

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

Theorem (8.4.5)**.**
For all integers a and b, not both zero, if $d = \gcd(a, b)$, then there exist integers s and t such that $as + bt = d$.

Corollary (8.4.6)**.**
If a and b are relatively prime integers, then there exist integers s and t such that $as + bt = 1$.

Corollary (8.4.7)**.**
For all integers a and n, if $\gcd(a, n) = 1$, then there exists an integer s such that $as \equiv 1 \pmod{n}$. The integer s is called the **inverse of a modulo n**.

Lemma (8.4.8)**.**
For all integers a, b and c, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

Theorem (8.4.9)**.**
For all integers a, b, c and n with $n > 1$, if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.

Theorem (8.4.10)**.**
If p is any prime number and a is any integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem (7.1.1)**.**
If $f : X \to Y$ and $g : X \to Y$ are functions, then $f = g$ if, and only if, $f(x) = g(x)$ for all $x \in X$.

Theorem (7.2.3)**.**
If X and Y are sets and $f : X \to Y$ is one-to-one and onto, then $f^{-1} : Y \to X$ is also **one-to-one** and **onto**.

Theorem (7.3.1)**.**
If f is a function from a set X to a set Y, and I_X is the identity function on X, and I_Y is the identity function on Y, then

$$f \circ I_X = f, I_Y \circ f = f$$

Theorem (7.3.3)**.**
If $f : X \to Y$ and $g : Y \to Z$ are both one-to-one functions, then $g \circ f$ is one-to-one.

Theorem (7.3.4)**.**
If $f : X \to Y$ and $g : Y \to Z$ are both onto functions, then $g \circ f$ is onto.

Theorem (9.2.2)**.**
For any integer n with $n \geq 1$, the number of permutations of a set with n elements is $n!$.

Free ebooks ==> www.ebook777.com

APPENDIX A

PROPERTIES OF THE REAL NUMBERS*

In this text we take the real numbers and their basic properties as our starting point. We give a core set of properties, called axioms, which the real numbers are assumed to satisfy, and we state some useful properties that can be deduced from these axioms.

We assume that there are two binary operations defined on the set of real numbers, called **addition** and **multiplication,** such that if a and b are any two real numbers, the **sum** of a and b, denoted $\boldsymbol{a+b}$**,** and the **product** of a and b, denoted $\boldsymbol{a \cdot b}$ or $\boldsymbol{ab}$**,** are also real numbers. These operations satisfy properties F1–F6, which are called the **field axioms.**

F1. *Commutative Laws* For all real numbers a and b,

$$a+b=b+a \quad \text{and} \quad ab=ba.$$

F2. *Associative Laws* For all real numbers a, b, and c,

$$(a+b)+c=a+(b+c) \quad \text{and} \quad (ab)c=a(bc).$$

F3. *Distributive Laws* For all real numbers a, b, and c,

$$a(b+c)=ab+ac \quad \text{and} \quad (b+c)a=ba+ca.$$

F4. *Existence of Identity Elements* There exist two distinct real numbers, denoted 0 and 1, such that for every real number a,

$$0+a=a+0=a \quad \text{and} \quad 1\cdot a=a\cdot 1=a.$$

F5. *Existence of Additive Inverses* For every real number a, there is a real number, denoted $-a$ and called the **additive inverse** of a, such that

$$a+(-a)=(-a)+a=0.$$

F6. *Existence of Reciprocals* For every real number $a \neq 0$, there is a real number, denoted $1/a$ or a^{-1}, called the **reciprocal** of a, such that

$$a\cdot\left(\frac{1}{a}\right)=\left(\frac{1}{a}\right)\cdot a=1.$$

All the usual algebraic properties of the real numbers that do not involve order can be derived from the field axioms. The most important are collected as theorems T1–T16 as follows. In all these theorems the symbols a, b, c, and d represent arbitrary real numbers.

*Adapted from Tom M. Apostol, *Calculus, Volume I* (New York: Blaisdell, 1961), pp. 13–19.

Copyright 2011 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

Free ebooks ==> www.ebook777.com

T1. *Cancellation Law for Addition* If $a + b = a + c$, then $b = c$. (In particular, this shows that the number 0 of Axiom F4 is unique.)

T2. *Possibility of Subtraction* Given a and b, there is exactly one x such that $a + x = b$. This x is denoted by $b - a$. In particular, $0 - a$ is the additive inverse of a, $-a$.

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* If $ab = ac$ and $a \neq 0$, then $b = c$. (In particular, this shows that the number 1 of Axiom F4 is unique.)

T8. *Possibility of Division* Given a and b with $a \neq 0$, there is exactly one x such that $ax = b$. This x is denoted by b/a and is called the **quotient** of b and a. In particular, $1/a$ is the reciprocal of a.

T9. If $a \neq 0$, then $b/a = b \cdot a^{-1}$.

T10. If $a \neq 0$, then $(a^{-1})^{-1} = a$.

T11. *Zero Product Property* If $ab = 0$, then $a = 0$ or $b = 0$.

T12. *Rule for Multiplication with Negative Signs*

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

and

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

T13. *Equivalent Fractions Property*

$$\frac{a}{b} = \frac{ac}{bc}, \quad \text{if } b \neq 0 \text{ and } c \neq 0.$$

T14. *Rule for Addition of Fractions*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \text{if } b \neq 0 \text{ and } d \neq 0.$$

T15. *Rule for Multiplication of Fractions*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \text{if } b \neq 0 \text{ and } d \neq 0.$$

T16. *Rule for Division of Fractions*

$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}, \quad \text{if } b \neq 0, c \neq 0, \text{ and } d \neq 0.$$

The real numbers also satisfy the following axioms, called the **order axioms.** It is assumed that among all real numbers there are certain ones, called the **positive real numbers,** that satisfy properties Ord1–Ord3.

Copyright 2011 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

www.ebook777.com

Free ebooks ==> www.ebook777.com

Ord1. For any real numbers a and b, if a and b are positive, so are $a + b$ and ab.

Ord2. For every real number $a \neq 0$, either a is positive or $-a$ is positive but not both.

Ord3. The number 0 is not positive.

The symbols $<$, $>$, $\leq$, and $\geq$, and negative numbers are defined in terms of positive numbers.

• Definition

Given real numbers a and b,

$a < b$ means $b + (-a)$ is positive.	$b > a$ means $a < b$.
$a \leq b$ means $a < b$ or $a = b$.	$b \geq a$ means $a \leq b$.
If $a < 0$, we say that a is **negative.**	If $a \geq 0$, we say that a is **nonnegative.**

From the order axioms Ord1–Ord3 and the above definition, all the usual rules for calculating with inequalities can be derived. The most important are collected as theorems T17–T27 as follows. In all these theorems the symbols a, b, c, and d represent arbitrary real numbers.

T17. *Trichotomy Law* For arbitrary real numbers a and b, exactly one of the three relations $a < b$, $b < a$, or $a = b$ holds.

T18. *Transitive Law* If $a < b$ and $b < c$, then $a < c$.

T19. If $a < b$, then $a + c < b + c$.

T20. If $a < b$ and $c > 0$, then $ac < bc$.

T21. If $a \neq 0$, then $a^2 > 0$.

T22. $1 > 0$.

T23. If $a < b$ and $c < 0$, then $ac > bc$.

T24. If $a < b$, then $-a > -b$. In particular, if $a < 0$, then $-a > 0$.

T25. If $ab > 0$, then both a and b are positive or both are negative.

T26. If $a < c$ and $b < d$, then $a + b < c + d$.

T27. If $0 < a < c$ and $0 < b < d$, then $0 < ab < cd$.

One final axiom distinguishes the set of real numbers from the set of rational numbers. It is called the **least upper bound axiom.**

LUB. Any nonempty set S of real numbers that is bounded above has a least upper bound. That is, if B is the set of all real numbers x such that $x \geq s$ for all s in S and if B has at least one element, then B has a smallest element. This element is called the **least upper bound** of S.

The least upper bound axiom holds for the set of real numbers but not for the set of rational numbers. For example, the set of all rational numbers that are less than $\sqrt{2}$ has upper bounds but not a least upper bound within the set of rational numbers.

Copyright 2011 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s).
Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.