CS1231 Cheatsheet

for finals, by ning

Appendix A of Epp is not covered. Theorems, corollaries, lemmas, etc. from the Epp textbook are prefixed with '*Epp*'; those without asterisks (*) are from the lecture notes, those with the asterisk are not (e.g. Epp theorems not covered by the lecture). In titles, 'T' is short for theorem, 'L' for lemma, 'C' for corollary.

Proofs

Basic Notation

$\mathbb{R}$	set of real numbers
$\mathbb{Z}$	set of integers (includes 0)
$\mathbb{Q}$	set of rationals
$\mathbb{N}$	set of natural numbers (usually includes 0)
$\exists$	there exists...
$\exists!$	there exists a unique...
$\forall$	for all...
$\in$	member of...
$\ni$	such that...

Proof Types

- **By Construction**: finding or giving a set of directions to reach the statement to be proven true. In proving equality, a useful note:

$$a \leq b \wedge a \geq b \rightarrow a = b$$

- **By Contraposition**: proving a statement through its logically equivalent contrapositive.
- **By Contradiction**: proving that the negation of the statement leads to a logical contradiction.
- **By Exhaustion**: considering each case.
- **By Mathematical Induction**: proving for a base case, then an induction step. In the inductive step, work from the $k+1$, not the k case.
- **By Strong Induction**: mathematical induction assuming $P(k), P(k-1), \cdots, P(a)$ are all true.

Order of Operations

First $\sim$ (also represented as $\neg$). No priority within $\wedge$ and $\vee$, so $p \wedge q \vee r$ is ambiguous and should be written as $(p \wedge q) \vee r$ or $p \wedge (q \vee r)$. The implication, $\rightarrow$ is performed last. Can be overwritten by parenthesis.

Universal & Existential Generalisation

'All boys wear glasses' is written as

$$\forall x(\text{Boy}(x) \rightarrow \text{Glasses}(x))$$

If conjunction was used, this statement would be falsified by the existence of a 'non-boy' in the domain of x.

'There is a boy who wears glasses' is written as

$$\exists x(\text{Boy}(x) \wedge \text{Glasses}(x))$$

If implication was used, this statement would true even if the domain of x is empty.

Valid Arguments as Tautologies

All valid arguments can be *restated* as tautologies.

Rules of Inference

Modus ponens

$$\begin{array}{l} p \rightarrow q \\ p \\ \therefore q \end{array}$$

Modus tollens

$$\begin{array}{l} p \rightarrow q \\ \neg q \\ \therefore \neg p \end{array}$$

Generalization

$$\begin{array}{l} p \\ \therefore p \vee q \end{array}$$

Specialization

$$\begin{array}{l} p \wedge q \\ \therefore p \end{array}$$

Elimination

$$\begin{array}{l} p \vee q \\ \neg q \\ \therefore p \end{array}$$

Transitivity

$$\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \therefore p \rightarrow r \end{array}$$

Proof by Division into Cases

$$\begin{array}{l} p \vee q \\ p \rightarrow r \\ q \rightarrow r \\ \therefore r \end{array}$$

Contradiction Rule

$$\begin{array}{l} \neg p \rightarrow \mathbf{c} \\ \therefore p \end{array}$$

Universal Rules of Inference

Only modus ponens, modus tollens, and transitivity have universal versions in the lecture notes.

Implicit Quantification

The notation $P(x) \implies Q(x)$ means that every element in the truth set of $P(x)$ is in the truth set of $Q(x)$, or equivalently, $\forall x, P(x) \rightarrow Q(x)$.

The notation $P(x) \iff Q(x)$ means that $P(x)$ and $Q(x)$ have identical truth sets, or equivalently, $\forall x, P(x) \leftrightarrow Q(x)$.

Implication Law

$$p \rightarrow q \equiv \neg p \vee q$$

Universal Instantiation

If some property is true of everything in a set, then it is true of any particular thing in the set.

Universal Generalization

If $P(c)$ must be true, and we have assumed nothing about c, then $\forall x, P(x)$ is true.

Regular Induction

Modify the domain of the quantifiers below according to P, if necessary:

$$P(0)$$
$$\forall k \in \mathbb{N}, P(k) \rightarrow P(k+1)$$
$$\forall k \in \mathbb{N}, P(n)$$

Epp T2.1.1 Logical Equivalences

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

$$p \wedge \mathbf{t} \equiv p$$
$$p \vee \mathbf{c} \equiv p$$

Negation Laws

$$p \vee \neg p \equiv \mathbf{t}$$
$$p \wedge \neg p \equiv \mathbf{c}$$

Double Negative Law

$$\neg(\neg p) \equiv p$$

Idempotent Laws

$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$

Universal Bound Laws

$$p \vee \mathbf{t} \equiv \mathbf{t}$$
$$p \wedge \mathbf{c} \equiv \mathbf{c}$$

De Morgan's Laws

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

Absorption Laws

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

Negations of $\mathbf{t}$ and $\mathbf{c}$

$$\neg \mathbf{t} \equiv \mathbf{c}$$
$$\neg \mathbf{c} \equiv \mathbf{t}$$

Definition 2.2.1 (Conditional)

If p and q are statement variables, the conditional of q by p is "if p then q" or "p implies q", denoted $p \rightarrow q$. It is false when p is true and q is false; otherwise it is true. We call p the *hypothesis* (or *antecedent*), and q the *conclusion* (or *consequent*).

A conditional statement that is true because its hypothesis is false is called *vacuously true* or *true by default*.

Definition 2.2.2 (Contrapositive)

The contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$.

Definition 2.2.3 (Converse)

The converse of $p \rightarrow q$ is $q \rightarrow p$.

Definition 2.2.4 (Inverse)

The inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$.

Definition 2.2.6 (Biconditional)

The biconditional of p and q is denoted $p \leftrightarrow q$ and is true if both p and q have the same truth values, and is false if p and q have opposite truth values.

Definition 2.2.7 (Necessary & Sufficient)

"r is sufficient for s" means $r \rightarrow s$, "r is necessary for s" means $\neg r \rightarrow \neg s$ or equivalently $s \rightarrow r$.

Definition 2.3.2 (Sound & Unsound Arguments)

An argument is called *sound*, iff it is valid and all its premises are true.

Definition 3.1.3 (Universal Statement)

A *universal statement* is of the form

$$\forall x \in D, Q(x)$$

It is defined to be true iff $Q(x)$ is true for every x in D. It is defined to be false iff $Q(x)$ is false for at least one x in D.

Definition 3.1.4 (Existential Statement)

A *existential statement* is of the form

$$\exists x \in D \text{ s.t. } Q(x)$$

It is defined to be true iff $Q(x)$ is true for at least one x in D. It is defined to be false iff $Q(x)$ is false for all x in D.

Theorem 3.2.1 (Negation of Universal State.)

The negation of a statement of the form

$$\forall x \in D, P(x)$$

is logically equivalent to a statement of the form

$$\exists x \in D \text{ s.t. } \neg P(x)$$

Theorem 3.2.2 (Negation of Existential State.)

The negation of a statement of the form

$$\exists x \in D \text{ s.t. } P(x)$$

is logically equivalent to a statement of the form

$$\forall x \in D, \neg P(x)$$

Number Theory

Properties (of Numbers)

Closure, i.e.

$$\forall x, y \in \mathbb{Z},\ x + y \in \mathbb{Z},\ \text{and } xy \in \mathbb{Z}$$

Commutativity, i.e.

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

Distributivity, i.e.

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

Trichotomy, i.e.

$$(a < b) \oplus (b < a) \oplus (a = b)$$

(Can be used without proof)

Definition 1.1.1 (Colorful)
An integer n is said to be colorful if there exists some integer k such that $n = 3k$.

Definition 1.3.1 (Divisibility)
If n and d are integers and $d \neq 0$,

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

Theorem 4.1.1 (Linear Combination)

$$\forall a, b, c \in \mathbb{Z},\ (a \mid b) \wedge (a \mid c) \to \forall x, y \in \mathbb{Z}, a \mid (bx + cy)$$

***Epp T4.3.1 (Pos. Divisors of Pos. Integers)**
For all positive integers a, b,

$$a \mid b \to a \leq b$$

Epp T4.3.3 (Transitivity of Divisibility)

$$\forall a, b, c \in \mathbb{Z},\ (a \mid b) \wedge (b \mid c) \to a \mid c$$

Theorem 4.4.1 (Quotient-Remainder Theorem)
Given any integer a and any positive integer b, there exist unique integers q and r such that

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

Representation of Integers
Given any positive integer n and base b, repeatedly apply the Quotient-Remainder Theorem to get,

$$\begin{aligned} n &= bq_0 + r_0 \\ q_0 &= bq_1 + r_1 \\ q_1 &= bq_2 + r_2 \\ &\cdots \\ q_{m-1} &= bq_m + r_m \end{aligned}$$

The process stops when $q_m = 0$. Eliminating the quotients q_i we get,

$$n = r_m b^m + r_{m-1} b^{m-1} + \cdots r_1 b + r_0$$

Which may be represented compactly in base b as a sequence of the digits r_i,

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

Definition 4.2.1 (Prime number)

$$\begin{aligned} n \text{ is prime} &\iff \forall r, s \in \mathbb{Z}^+ \\ &\quad n = rs \to \\ &\quad (r = 1 \wedge s = n) \vee (r = n \wedge s = 1) \\ n \text{ is composite} &\iff \exists r, s \in \mathbb{Z}^+ \text{ s.t.} \\ &\quad n = rs \wedge \\ &\quad (1 < r < n) \wedge (1 < s < n) \end{aligned}$$

List of Primes to 100
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Proposition 4.2.2
For any two primes p and p',

$$p \mid p' \to p = p'$$

Theorem 4.2.3
If p is a prime and $x_1, x_2, \cdots, x_n$ are any integers s.t. $p \mid x_1 x_2 \cdots x_n$, then $p \mid x_i$ for some $x_i, i \in \{1, 2, \cdots, n\}$.

Epp T4.3.5 (Unique Prime Factorisation)
Given any integer $n > 1$

$$\begin{gathered} \exists k \in \mathbb{Z}^+, \\ \exists p_1, p_2, \cdots, p_k \in \text{ primes}, \\ \exists e_1, e_2, \cdots, e_k \in \mathbb{Z}^+, \end{gathered}$$

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, except perhaps for the order in which the factors are written.

Epp Proposition 4.7.3
For any $a \in \mathbb{Z}$ and any prime p,

$$p \mid a \to p \nmid (a + 1)$$

Epp T4.7.4 (Infinitude of Primes)
The set of primes is infinite.

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

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

Does not require b to be in X.

Theorem 4.3.2 (Well Ordering Principle)
If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then S has a least element.

Note three conditions: $|S| > 0$, $S \subseteq \mathbb{Z}$, and S has lower bound.

Likewise, if ... upper bound ... has a greatest element.

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

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

Theorem 4.4.1 (Quotient-Remainder Theorem)
Given any integer a and any positive integer b, there exist unique integers q and r such that

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

Definition 4.5.1 (Greatest Common Divisor)
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

1. $d \mid a$ and $d \mid b$
2. $\forall c \in \mathbb{Z}\ ((c \mid a)\ \wedge (c \mid b) \to c \leq d)$

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

Theorem 4.5.3 (Bézout's Identity)
Let a, b be integers, not both zero, and let $d = \gcd(a, b)$. Then there exists integers x, y such that

$$ax + by = d$$

Or, the gcd of two integers is some linear combination of the said numbers, where x, y above have multiple solution pairs once a solution pair (x, y) is found. Also solutions, for any integer k,

$$(x + \frac{kb}{d}, y - \frac{ka}{d})$$

***Epp T8.4.8 (Euclid's Lemma)**
For all $a, b, c \in \mathbb{Z}$, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

***Epp L4.8.1 (gcd of an integer and 0)**
If r is a positive integer, then $\gcd(r, 0) = r$.

***Epp L4.8.2 (Basis of Euclid's Algorithm)**
If $a, b \in \mathbb{Z}^+$, and $q, r \in \mathbb{Z}$ s.t. $a = bq + r$, then

$$\gcd(a, b) = \gcd(b, r)$$

Algorithm 4.8.2 (Euclidean Algorithm)

```
def gcd(a, b):
  if a == 0:
    return b
  if b == 0:
    return a
  return gcd(a%b, b) if a >= b else gcd(a, b%a)
```

For example, to evaluate $\gcd(330, 156)$:

$$\begin{aligned} &\gcd(330, 156) && (= \gcd(330 \bmod 156, 156)) \\ =\ &\gcd(18, 156) && (= \gcd(18, 156 \bmod 18)) \\ =\ &\gcd(18, 12) && (= \gcd(18 \bmod 12, 12)) \\ =\ &\gcd(6, 12) && (= \gcd(6, 12 \bmod 6)) \\ =\ &\gcd(6, 0) \\ =\ &6 \end{aligned}$$

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

Definition 4.7.1 (Congruence modulo)
Let $m, z \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. We say that m is *congruent* to n *modulo* d and write

$$m \equiv n \pmod{d}$$

iff

$$d \mid (m - n)$$

More concisely,

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

Epp T8.4.1 (Modular Equivalences)
Let $a, b, n \in \mathbb{Z}$ and $n > 1$. The following statements are all equivalent,

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

Epp T8.4.3 (Modulo Arithmetic)
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. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$, for all $m \in \mathbb{Z}^+$

Epp C8.4.4
Let $a, b, c, d, n \in \mathbb{Z}$, $n > 1$, then

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

or equivalently,

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

In particular, if m is a positive integer, then

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

Definition 4.7.2 (Multiplicative inv. modulo n)
For any integers a, n with $n > 1$, if an integer s is such that $as \equiv 1 \pmod{n}$, then s is the *multiplicative inverse of a modulo n*. We may write s as a^{-1}.

Because the commutative law still applies in modulo arithmetic, we also have

$$a^{-1} a \equiv 1 \pmod{n}$$

Multiplicative inverses are not unique. If s is an inverse, then so is $(s + kn)$ for any integer k.

Theorem 4.6.3 (Existence of multiplicative inverse)
For any integer a, its multiplicative inverse modulo n where $n > 1$, a^{-1}, exists iff a and n are coprime.

Finding the Multiplicative Inverse
To find the multiplicative inverse $a^{-1} \bmod b$, note that since a, b are coprime, using Bézout's Identity, there exists $x, y \in \mathbb{Z}_{\neq 0}$ such that,

$$\begin{aligned} ax + by &= \gcd(a, b) \\ ax + by &= 1 \\ ax + by &\equiv 1 \pmod{b} \\ ax &\equiv 1 \pmod{b} \\ a^{-1} &\equiv x \pmod{b} \end{aligned}$$

To find x, employ the extended Euclidean algorithm: express b using the quotient-remainder theorem (T4.4.1) with a as the quotient. Then express the remainder r using the divisor as quotient. Repeat with the new remainder until a remainder of 1 is obtained. Finally, express 1 in terms of a and b using the equalities formulated during the algorithm. For example, to find the multiplicative inverse of 5 mod 18.

quotient-remainder theorem: $n = dq + r$

$$\begin{aligned} n &= d\ q + r && (1) \\ 18 &= (3)5 + 3 && (2) \\ 5 &= (1)3 + 2 && (3) \\ 3 &= (1)2 + 1 && (4) \end{aligned}$$

Now, express 1 in terms of 5 and 18.

$$\begin{aligned} 1 = &\ (1)\ 3 \ - \ (1)\ 2 \\ = &\ (1)\ 3 \ - \ (1)\ [(1)5 - (1)3] \\ = &\ (-1)\ 5 \ + \ (2)\ 3 \\ = &\ (-1)\ 5 \ + \ (2)\ [(1)18 - (3)5] \\ = &\ (2)\ 18 + (-7)\ 5 \end{aligned}$$

Take $\bmod 18$ on both sides,

$$\begin{aligned} 1 &\equiv (2)18 + (-7)5 \pmod{18} \\ (2)18 + (-7)5 &\equiv 1 \pmod{18} \\ (-7)5 &\equiv 1 \pmod{18} \\ (11)5 &\equiv 1 \pmod{18} \end{aligned}$$

So, $5^{-1} \bmod 18 = 11$.

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

Epp T8.4.9 (Cancellation Law for mod. arith.)
For all $a, b, c, n \in \mathbb{Z}$, $n > 1$, and a and n are coprime,

$$ab \equiv ac \pmod{n} \to b \equiv c \pmod{n}$$

***Epp T8.4.10 (Fermat's Little Theorem)**
For any prime p and any integer a, $a^p \equiv a \pmod{p}$.

Alternatively, if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

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

1. $a \mid m$ and $b \mid m$
2. $\forall c \in \mathbb{Z}^+((a \mid c) \wedge (b \mid c) \to c \leq m$

Sequences

Empty Sums & Products
By definition, when $n < m$,

$$\sum_{i=m}^{n} a_i = 0$$

$$\prod_{i=m}^{n} = 1$$

Epp T5.1.1
For real numbered sequences $a_m, a_{m+1}, a_{m+2}, \ldots$ and $b_m, b_{m+1}, b_{m+2} \ldots$, $c \in \mathbb{R}$, the following holds for any $n \geq m$

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

$$c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$$

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

Common Sequences

Arithmetic sequence:

$$S_n = \frac{n}{2}(2a + (n-1)d)$$

Geometric sequence:

$$S_n = \frac{a(r^n - 1)}{r - 1}$$

$$S_\infty = \frac{a}{1 - r}\ , \quad |r| < 1$$

Triangle numbers:

$$T_n = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Fibonacci numbers:

$$\forall n \in \mathbb{N},\ F_k = \begin{cases} 0 & \text{if } k = 0 \\ 1 & \text{if } k = 1 \\ F_{k-1} + F_{k-2} & \text{otherwise} \end{cases}$$

$$= \frac{\phi^k - (-\phi)^{-k}}{\sqrt{5}}$$

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

Definition 5.4.1
A second-order linear homogeneous recurrence relation with constant coefficients is a recurrence relation of the form:

$$F_k = aF_{k-1} + bF_{k-2}$$

Where $a, b \in \mathbb{R}$, $b \neq 0$; and $\forall k \in \mathbb{Z}_{k \geq k_0}$ for $k_0 \in \mathbb{Z}$.

- *Second-order* means recurrence relation goes up to but not exceeding F_{k-2}.
- *Linear* means the highest power of the $(F_{k-r})^m$ term is $m = 1$.
- *Homogeneous* means $C = 0$ in the more general case $F_k = aF_{k-1} + bF_{k-2} + C$.
- *Constant coefficients* means a, b does not depend on k.

Epp T5.8.3 (Distinct-Roots Theorem)
If a second-order linear homogeneous recurrence relation with constant coefficients has real roots r and s for its characteristic equation,

$$t^2 - at - b = 0$$

Then F_k can be written in closed form as

$$F_k = cr^k + ds^k$$

Where $c, d \in \mathbb{R}$ can be found by solving for known values of the sequence. Recall that the roots of a quadratic equation $ax^2 + bx + c$ are given by:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Epp T5.8.5 (Single-Roots Theorem)
If a second-order linear homogeneous recurrence relation with constant coefficients has one single real root r for its characteristic equation,

$$t^2 - at - b = 0$$

Then F_k can be written in closed form as

$$F_k = cr^k + dkr^k$$

Where $c, d \in \mathbb{R}$ can be found by solving for known values of the sequence.

Sets

Definition 6.1.1 (Subsets & Supersets)
S is a subset of T if all the elements of S are elements of T, denoted $S \subseteq T$. Formally,

$$S \subseteq T \longleftrightarrow \forall x \in S(x \in T)$$

Definition 6.2.1 (Empty Set)
An empty set has no element, and is denoted $\varnothing$ or $\{\}$. Formally, where $\mathcal{U}$ is the universal set:

$$\forall Y \in \mathcal{U}(Y \notin \varnothing)$$

Epp T6.24
An empty set is a subset of all sets.

$$\forall S,\ S \text{ is a set},\ \varnothing \subseteq S$$

Definition 6.2.2 (Set Equality)
Two sets are equal iff they have the same elements.

Proposition 6.2.3
For any two sets X, Y, X and Y are subsets of each other iff $X = Y$. Formally,

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

Epp C6.2.5 (Empty Set is Unique)
It's what it says.

Definition 6.2.4 (Power Set)
The power set of a set S denoted $\mathcal{P}(S)$, or 2^S; is the set whose elements are all possible subsets of S. Formally,

$$\mathcal{P}(S) = \{X \mid X \subseteq S\}$$

Theorem 6.3.1
If a set X has n elements, $n \geq 0$, then $\mathcal{P}(X)$ has 2^n elements.

Definition 6.3.1 (Union)
Let S be a set of sets. T is the union of sets in S, iff each element of T belongs to some set in S. Formally,

$$T = \bigcup S = \bigcup_{X \in S} X = \{y \in \mathcal{U} \mid \exists X \in S(y \in X)\}$$

Proposition 6.3.2
Some properties of union,

- $\bigcup \varnothing = \bigcup_{A \in \varnothing} A = \varnothing$
- $\bigcup \{A\} = A$
- $A \cup \varnothing = A$
- $A \cup B = B \cup A$
- $A \cup (B \cup C) = (A \cup B) \cup C$
- $A \cup A = A$
- $A \subseteq B \longleftrightarrow A \cup B = B$

Definition 6.3.3 (Intersection)
Let S be a non-empty set of sets. T is the intersection of sets in S, iff each element of T also belongs to all the sets in S. Formally,

$$\begin{aligned} T = \bigcap S &= \bigcap_{X \in S} X \\ &= \{y \in \mathcal{U} \mid \forall X((X \in S) \to (y \in X))\} \end{aligned}$$

Proposition 6.3.4
Let A, B, C be sets. Some properties of intersection,

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

Definition 6.3.5 (Disjoint)
Let S, T be sets. S and T are disjoint iff $S \cap T = \varnothing$.

Definition 6.3.6 (Mutually Disjoint)
Let V be a set of sets. The sets $T \in V$ are mutually disjoint iff every two distinct sets are disjoint. Formally,

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

Definition 6.3.7 (Partition)
Let S be a set, and V a set of non-empty subsets of S. Then V is a partition of S iff

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

Definition 6.3.8 (Non-symmetric Difference)
Let S, T be two sets. The (non-symmetric) difference of S and T denoted $S - T$ or $S \setminus T$ is the set whose elements belong to S and do not belong to T. Formally,

$$S - T = \{y \in \mathcal{U} \mid y \in S \wedge y \notin T\}$$

This is analogous to subtraction for numbers.

Definition 6.3.9 (Symmetric Difference)
Let S, 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. Formally,

$$S \ominus T = \{y \in \mathcal{U} \mid y \in S \oplus y \in T\}$$

This is analogous to the exclusive-or in predicate logic.

Definition 6.3.10 (Set Complement)
Let $A \subseteq \mathcal{U}$. Then, the complement of A denoted A^c is $\mathcal{U} - A$.

Relations

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

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

Definition 8.1.2 (Ordered n-tuple)

Generalise the ordered pair to n elements. The ordered n-tuple $(x_1, x_2, \cdots, x_n)$ consists of $x_1, x_2, \cdots, x_n$ elements together with ordering.

$$\begin{aligned} &(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n) \\ \iff &x_1 = y_1, x_2 = y_2, \cdots, x_n = y_n \end{aligned}$$

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

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

For example,

$$\begin{aligned} &\{1, 2, 3\} \times \{a, b\} \\ &= \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\} \end{aligned}$$

Definition 8.1.4 (Generalised Cartesian Prod.)

Generalise the cartesian product for n sets.

$$A_1 \times A_2 \times \cdots \times A_n$$
$$= \{(a_1, \cdots, a_n) \mid a_1 \in A_1, \cdots, a_n \in A_n\}$$

Let V be a set of sets with which to apply the cartesian product to. We can also write

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

Definition 8.2.1 (Relations)
Let S, T be two sets. A *binary relation* from S to T denoted $\mathcal{R}$ is a subset of the cartesian product $S \times T$. The notation $s \mathcal{R} t$ stands for $(s,t) \in \mathcal{R}$. $s \not\mathcal{R} t$ stands for $(s,t) \notin \mathcal{R}$.

Definitions 8.2.[2-4] (Dom, Im, coDom)
Let $\mathcal{R} \subseteq S \times T$ be a binary relation from S to T. Denote the domain (8.2.2) of $\mathcal{R}$ as $Dom(\mathcal{R})$; the image (or range, 8.2.3) as $Im(\mathcal{R})$; and the co-domain (8.2.4) as $coDom(\mathcal{R})$.

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

Proposition 8.2.5
Let $\mathcal{R}$ be a binary relation. $Im(\mathcal{R}) \subseteq coDom(\mathcal{R})$.

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

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

Definition 8.2.7 (n-ary relation)
Generalise the binary relation for n sets $S_1, S_2, \cdots, S_n$. An n-ary relation on the n sets is a subset of the cartesian product $\prod_i S_i$. n is the arity or degree of the relation.

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

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

In other words, $x \in S$ and $z \in U$ are related iff there is a 'path' from x to z via some intermediate $y \in T$.

Repeated Compositions

$$\mathcal{R}^n := \underbrace{R \circ \cdots \circ R}_{n} = \bigodot_{n} \mathcal{R}$$

Proposition 8.2.9 (Associativity of Composition)

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

Proposition 8.2.10 (Inverse of Composition)

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

Definitions 8.3.[1-3] (Properties of Relations)
Let A be a set, and $\mathcal{R} \in A \times A$ be a relation on A.

$\mathcal{R}$ is reflexive (8.3.1) iff $\forall x \in A(x \mathcal{R} x)$.

$\mathcal{R}$ is symmetric (8.3.2) iff $\forall x, y \in A(x \mathcal{R} y \rightarrow y \mathcal{R} x)$.

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

Definition 8.6.1 (Anti-symmetric)
Let A be a set, and $R \in A \times A$ be a relation on A. $\mathcal{R}$ is anti-symmetric iff

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

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

Definition 8.3.5 (Equivalence Class)
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. That is

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

Epp T8.3.4 (Partition by Equivalence Relation)
Let $\mathcal{R}$ be an equivalence relation on a set A. Then the set of distinct equivalence classes form a partition of A.

Epp L8.3.2
Let $\mathcal{R}$ be an equivalence relation on a set A, and let $a, b \in A$. If $a \mathcal{R} b$ then $[a] = [b]$.

Epp L8.3.3
Let $\mathcal{R}$ be an equivalence relation on a set A, and let $a, b \in A$. Either $[a] \cap [b] = \varnothing$ or $[a] = [b]$.

Epp T8.3.1 (Equivalence Relation by Partition)
Given a partition $S_1, S_2, cdots$ of a set A, there exists an equivalence relation $\mathcal{R}$ on A whose equivalence classes make up precisely that partition.

Definition 8.5.1 (Transitive Closure)
Let A be a set and $\mathcal{R}$ a relation on A. The transitive closure of $\mathcal{R}$ denoted $\mathcal{R}^t$ is a relation that satisfies the three properties:

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

Intuitively, the transitive the closure can be understood as the smallest superset that is transitive. Similar definitions exist for the reflexive closure and symmetric closure.

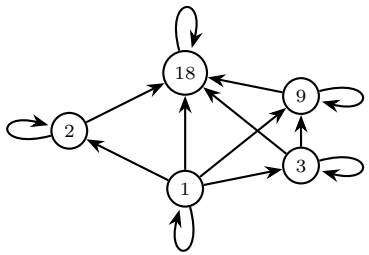
Proposition 8.5.2

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

Definition 8.6.2 (Partial Order)
$\mathcal{R}$ is a partial order iff it is reflexive, anti-symmetric, and transitive. A set A is called a partially ordered set with respect to a relation $\preceq$ iff $\preceq$ is a partial order relation on A.

Hasse Diagrams
The Hasse diagram is a simplified directed graph.

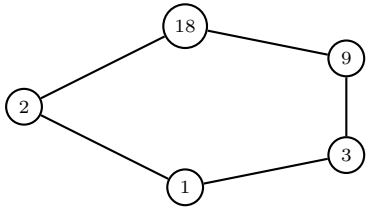
1. Draw the directed graph so that all arrows point upwards.
2. Eliminate all self-loops
3. Eliminate all arrows implied by transitivity.
4. Remove the direction of the arrows.



The above diagram represents the partial order for "divides" on the set $A = \{1, 2, 3, 9, 18\}$. That is

$$\forall a, b \in A(a \mid b \longleftrightarrow \exists k \in \mathbb{Z}(b = ka))$$

It can be represented by the following Hasse diagram.



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

Definition 8.6.4 (Total Order)
Let $\preceq$ be a partial order on set A. $\preceq$ is said to be a total order iff $\preceq$ is a partial order, and all $x, y \in A$ are comparable. Formally,

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

Definition 8.6.5 (Maximal)
Let $\preceq$ be a partial order on the set A. An element x is a maximal element iff

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

Definition 8.6.6 (Maximum)
Let $\preceq$ be a partial order on the set A. An element T is the maximum element iff

$$\forall x \in A(x \preceq T)$$

Definition 8.6.7 (Minimal)
Let $\preceq$ be a partial order on the set A. An element x is a minimal element iff

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

Definition 8.6.8 (Minimum)
Let $\preceq$ be a partial order on the set A. An element $\perp$ is the minimum element iff

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

Definition 8.6.9 (Well Ordered)
Let $\preceq$ be a partial order on the set A. A is well ordered iff every non-empty subset of A contains a minimum element. Formally,

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

Functions

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

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

Intuitively, this means that every element in S must have exactly one 'outgoing arrow'.

Definitions 7.1.[2-5]
Let $f : S \rightarrow T$ be a function, $x \in S$ and $y \in T$ such that $f(x) = y$; $U \subseteq S$, and $V \subseteq T$.

x is a pre-image (7.1.2) of y.

The inverse image of the element (7.1.3) y is the set of all its pre-images, i.e. $\{x \in S \mid f(x) = y\}$.

The inverse image of the set (7.1.4) V is the set that contains all the pre-images of all the elements of V, i.e. $\{x \in S \mid \exists y \in V(f(x) = y)\}$.

The restriction (7.1.5) of f to U is the set $\{(x, y) \in U \times T \mid f(x) = y\}$.

Definition 7.2.1 (Injective, or One-to-one)
Let $f : S \rightarrow T$ be a function. f is injective (or one-to-one) iff

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

Intuitively, this means that every element in T has have at most one 'incoming arrow'.

Definition 7.2.2 (Surjective, or Onto)
Let $f : S \rightarrow T$ be a function. f is surjective (or onto) iff

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

Intuitively, this means that every element in T has at least one 'incoming arrow'.

Definition 7.2.3 (Bijective)
A function is bijective (or is a bijection) iff it is injective and subjective. Intuitively, this means that every element in T has exactly one incoming arrow.

Definition 7.2.4 (Inverse)
Let $f : S \rightarrow T$ be a function and let f^{-1} be the inverse relation of f from T to S. Then f is bijective iff f^{-1} is a function.

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

Definition 7.3.2 (Identity)
The identity function on a set A, $\mathcal{I}_A$ is defined by,

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

Proposition 7.3.3

Let $f : A \to A$ be an injective function of A. Then $f^{-1} \circ f = \mathcal{I}_A$.

Combinatorics

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

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

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

An r-combination of as set of n elements is a subset of r of the n elements, denoted $\binom{n}{r}$.

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; denoted as $[x_{i_1}, x_{i_2}, \cdots, x_{i_r}]$ where each x_{i_j} is in X and some of the x_{i_j} may equal each other.

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 (Number of Elements)
If m and n are integers and $m \leq n$, then there are $n - m + 1$ integers from m to n inclusive.

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

Theorem 9.2.2 (Permutations)
The number of permutations of a set with n $(n \geq 1)$ elements is $n!$

Theorem 9.2.3 (r-permutations from n)
If $n, r \in \mathbb{Z}$ and $1 \leq r \leq n$, then the number of r-permutations of a set of n elements is given by,

$$\begin{aligned} P(n, r) &= n(n-1)(n-2)\cdots(n-r+1) \\ &= \frac{n!}{(n-r)!} \end{aligned}$$

Theorem 9.3.1 (Addition Rule)
Let A be a finite set equal to the union of k distinct mutually disjoint sets $A_1, A_2, \cdots, A_k$. Then,

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

Theorem 9.3.2 (Difference Rule)
Let A be a finite set and B a subset of A. Then,

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

Theorem 9.3.3 (Inclusion/Exclusion Principle)
If A, B, C are finite sets, then

$$\begin{aligned} N(A \cup B) =& N(A) + N(B) - N(A \cap B) \\ N(A \cup B \cup C) =& N(A) + N(B) + N(C) \\ & - N(A \cap B) - N(A \cap C) \\ & - N(B \cap C) + N(A \cap B \cap C) \end{aligned}$$

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 $y \in Y$ such that y is the image of at least $k + 1$ distinct elements of X.

Gen. Pigeonhole Principle, Contrapositive
For any function f form 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 9.5.1 (r-combinations from n)
If $n, r \in \mathbb{Z}^+$ and $r \leq n$, then the number of $r-$*combinations* that can be chosen from a set of n elements is given by,

$$\begin{aligned} \binom{n}{r} &= \frac{P(n, r)}{r!} \\ &= \frac{n!}{r!(n-r)!} \end{aligned}$$

Theorem 9.5.2 (Perm. w/ Indistinguishables)
For a set of n objects of which n_1 are indistinguishable from each other, as are n_2, and n_3, ..., and n_k, then the number of distinguishable permutations of the n objects is

$$\begin{aligned} &\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n-n_1-n_2-\cdots-n_k-1}{n_k} \\ =&\frac{n!}{n_1!n_2!\cdots n_k!} \end{aligned}$$

Theorem 9.6.1 (Multisets of r)
The number of r-combinations with repitition allowed 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.

Theorem 9.7.1 (Pascal's Formula)
Let $n, r \in \mathbb{Z}^+$, $r \leq n$. Then

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

Theorem 9.7.2 (Binomial Theorem)
Given $a, b \in \mathbb{R}$ and $n \in \mathbb{Z}^+$,

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

Probability

Axioms of Probability
Let S be a sample space, and P a probability function from the set of all events in S to the set of real numbers; $A, B \subseteq S$,

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

Theorem 9.3.3 (Inclusion/Exclusion Principle)
If A, B, and C are any finite sets, then

$$\begin{aligned} N(A \cup B) &= N(A) + N(B) - N(A \cap B) \\ N(A \cup B \cup C) &= N(A) + N(B) + N(C) \\ &\quad - N(A \cap B) - N(A \cap C) \\ &\quad - N(B \cap C) + N(A \cap B \cap C) \end{aligned}$$

Probability of the Complement

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

Probability of the Union

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

Expected Value
The expected value of a random experiment with discrete real numbered outcomes $a_1, a_2, \cdots, a_n$ with corresponding probabilities $p_1, p_2, \cdots, p_n$ is

$$\sum_n a_k p_k$$

Conditional Probability
Let $A, B \subseteq S$. If $P(A) \neq 0$, then the conditional probability of B given A, denoted $P(B|A)$ is

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

A useful form of this equality is

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

Bayes' Theorem
Suppose a sample space S has mutually disjoint events $B_1, B_2, \cdots, B_n$. Suppose A is an event in S, and all events have non-zero probabilities. If $k \in \mathbb{Z}^+$, $1 \leq k \leq n$, then

$$P(B_k|A) = \frac{P(A|B_k)P(B_k)}{\sum_{i=1}^{n} P(A|B_i)P(B_i)}$$

Independent Events
Let $A, B \subseteq S$, A, B be independent events iff

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

Pairwise/Mutually Independent
Let $A, B, C \subseteq S$. A, B, C are pairwise independent iff they satisfy conditions 1–3 below. They are mutally independent iff they satisify all 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. $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

In general, n events are mutually independent iff the probability of the intersection of any subset of events is the product of the corresponding probabilities of said events.

Graphs

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 connects its two endpoints. Two vertices connected by an edge are adjacent vertices. A vertex with a self-loop is adjacent to itself. An edge is incident on each of its endpoints, and two edges incident on the same endpoint are adjacent edges.

For an edge e incident on vertices v, w, we can write $e = \{v, w\}$.

Directed Graph
A directed graph (or digraph) 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.

For a directed edge e associated with the pair (v, w) of vertices, we can write $e = (v, w)$.

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

Complete Graph
A complete graph on n vertices, $n > 0$, denoted K_n, is a simple graph with n vertices and exactly one edge connecting each pair of distinct vertices. The number of edges is T_n, the n^{th} triangle number.

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

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

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

Subgraph
A graph H is a subgraph of a graph G iff every vertex in H is also a vertex in G, and 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
The degree of v, a vertex of graph G, denoted $deg(v)$, equals the number of edges that are incident on v, with self-loops counted twice. The total degree of G is

the sum of the degrees of all vertices of G.

Theorem 10.1.1 (Handshake Theorem)
The sum of the degrees of all the vertices of a graph G is twice the number of edges of G.

$$\text{Total Degree of } G = \sum_{v \in V(G)} deg(v)$$
$$= 2 \times N(\text{edges in G})$$

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.

	Repeated Edge?	Repeated Vertex?	Same Start/End?	Must Contain ≥ 1 Edge?
Walk	allowed	allowed	allowed	no
Trail	no	allowed	allowed	no
Path	no	no	no	no
Closed Walk	no	allowed	yes	no
Circuit	allowed	allowed	yes	yes
Simple Circuit	no	first, last only	yes	yes

Walk, Trails, Paths, etc.
Let G be a graph and $v, w \in V(G)$.

A walk from v to w is a finite alternating sequence of adjacent vertices and edges of G. It can be written in the form $v_0e_1v_1e_2 \cdots v_ne_nw$; or $v_0v_1 \cdots v_nw$; or $e_1e_2 \cdots e_n$.

A trivial walk from v to v consists of the single vertex v.

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

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

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

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

A simple circuit is a circuit that does not have any repeated vertex except the first and last.

Connectedness
Two vertices v, w of a graph G are connected iff there is a walk from v to w.

The graph G is connected iff $\forall v, w \in V(G)$ there is a walk from v to w. Then, G is either a tree or has a circuit.

Lemma 10.2.1
Let G be a graph.

- If G is connected, then any two distinct vertices of G can be conted by a path.
- If vertices v and w are part of a circuit in G and one edge is remd 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.

Connected Component
A graph H is a connected component of a graph G iff

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

Euler Circuit
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.

An Eulerian graph is a graph that contains an Euler circuit.

Theorem 10.2.2
If a graph has an Euler circuit, then every vertex 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 an Euler circuit iff G is connected and every vertex of G has positive even degree.

Euler Trail
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 v, w be 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 Circuit
A Hamiltonian circuit for a graph 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 very vertex of G appears exactly once, except for the first and last, which are the same.

A Hamiltonian graph (or Hamilton graph) is a graph that contains a Hamiltonian circuit. There is no analogous criterion to T10.2.4 to determining whether a given graph has a Hamiltonian circuit.

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.

Since the converse is not true, this proposition cannot be used to check if a graph has a Hamiltonian circuit. However, the contrapositive can be used to check if a graph does not have a Hamiltonian circuit.

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

Two matrices A and B are equal iff A and B are the same size, and all the corresponding entries of A and B are equal.

Adjacency Matrix of a Directed Graph
Let G be a directed graph with ordered vertices $v_1, v_2, \cdots, v_n$. The adjacency matrix of G is the $n \times n$ matrix $A = (a_{ij})$ over the set of non-negative integers such that for all $i, j = 1, 2, \cdots, n$,

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

Adjacency Matrix of an Undirected Graph
Let G be an undirected graph with ordered vertices $v_1, v_2, \cdots, v_n$. The adjacency matrix of G is the $n \times n$ matrix $A = (a_{ij})$ over the set of non-negative integers such that for all $i, j = 1, 2, \cdots, n$,

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

Symmetric Matrix
A $n \times n$ matrix is symmetric iff for all $i, j = 1, 2, \cdots, n$,

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

Theorem 10.3.1
Let G be a graph with connected components $G_1, G_2, \cdots, G_k$. 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

$$\begin{pmatrix} A_1 & O & \cdots & O & O \\ O & A_2 & \cdots & O & O \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & \cdots & A_{k-1} & O \\ O & O & \cdots & O & A_k \end{pmatrix}$$

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

Scalar Product

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

Matrix Multiplication
Let $A = (a_{ij})$, $B = (b_{ij})$, then the matrix product of $A \times B$, denoted AB, defined as (c_{ij}), is the matrix where

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj}$$

Intuitively, this means that the $(i, j)^{\text{th}}$ entry of AB can be found by the scalar product of the i^{th} row of A and the j^{th} column of B.

Identity Matrix
The $n \times n$ identity matrix I_n (or I) is the $n \times n$ matrix in which all the entries of the main diagonal are 1's, and all other entries are 0's.

n^{th} Power of a Matrix
For any $n \times n$ matrix A, the powers of A are defined as

$$A^k = \begin{cases} I & \text{if } k = 0 \\ AA^{k-1} & \text{for } k \in \mathbb{Z}^+, k \geq 1 \end{cases}$$

Theorem 10.3.2
Let G be the graph with vertices $v_1, v_2, \cdots, v_m$ and adjacency matrix A. Then, for each positive integer n and for all integers $i, j = 1, 2, \cdots, m$, the $(i, j)^{\text{th}}$ entry of A^n is the number of walks of length n from v_i to v_j.

Isomorphic Graph
Let G and G' be graphs with vertex sets $V(G), V(G')$ and edge sets $E(G), E(G')$ respectively. G is isomorphic to G' iff there exists a one-to-one correspondence (relabelling) $g : V(G) \to V(G')$ and $h : E(G) \to E(G')$ such that the edge-endpoint functions of G and G' are preserved. Formally, this means that

$$\forall v \in V(G), e \in E(G),$$
$$v \text{ is endpoint of } e \iff g(v) \text{ is endpoint of } h(e)$$

Theorem 10.4.1
Let S be a set of graphs and R be the relation of graph isomorphism on S. Then R is an equivalence relation

on S.

Theorem 10.4.2 (Invariant Properties)
Each of the following properties is an invariant for graph isomorphism, where n, m, and 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.

Planar Graph
A planar graph is a graph that can be drawn on a two-dimensional plane without edges crossing.

Euler's Formula
For a connected planar simple graph $G = (V, E)$ with $e = |E|$ and $v = |V|$, the number of faces $f = e - v + 2$.

Tree
A graph is circuit-free iff it has no circuits. A graph is a tree iff it is circuit-free and connected. A trivial tree is a graph that consists of a single vertex. A graph is a forest iff it is circuit-free and not connected.

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

Terminal & Internal Vertices
If a tree T has only one or two vertices, then each is a terminal vertex (or leaf). If T has at least three vertices, then a vertex of degree 1 in T is called a terminal vertex (or leaf), and a vertex of degree greater than 1 in T is called an internal vertex (or leaf).

Theorem 10.5.2
Any tree with $n > 0$ vertices has $n - 1$ edges.

Lemma 10.5.3
Let C be any circuit in a connected graph G. If one of the edges of C is removed from G, then the graph that remains is still connected.

Theorem 10.5.4
Let G be a connected graph with n vertices and $n - 1$ edges. G is a tree.

Rooted Tree
A rooted tree is a tree in which there is one vertex that is distinguished from the others as 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 the parent of w. Two distinct vertices that are both children of the same parent are called siblings.

Given two distinct vertices v, w; if v lies on a unique path between w and the root, then v is an ancestor of w, and w a descendant of v.

(Full) Binary Tree
A binary tree is a rooted tree in which every parent has at most two children. Each child is either a left child xor right child. 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.

The total number of vertices is the number of vertices that have a parent plus vertices that do not have a parent; or equivalently the number of internal vertices plus the terminal vertices.

Subtrees
The left subtree of a parent v in in binary tree T 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 consists of all those edges of T that connect the vertices of the left subtree. The right subtree is defined similarly.

***Epp T10.6.1 (Full Binary Tree Theorem)**
If T is a full binary tree with k internal vertices, then T has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices.

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

$$t \leq 2^h$$
$$\log_2 t \leq h$$

Binary Tree Traversal
Breadth-first search starts at the root and visits its adjacent vertices, then moves to the next level.

Depth-first search can be pre-order, in-order, or post-order. In pre-order, print, traverse left then right; in in-order, traverse left, print, then traverse right; in post-order, traverse left, right, then print.

The print operation can be represented by a 'dot' on a vertex in its tree diagram, and the order of prints can be determined by tracing the outline of the diagram anti-clockwise from the root. Draw the 'dot' on the left, bottom, and right of the vertex for pre-order, in-order, and post-order respectively.

Reconstructing BT from Traversal Order
Given a sequence of nodes traversed in depth-first pre-order, in-order, or post-order; it may be possible to reconstruct the binary tree. Note that in pre-order and post-order, the first node traversed is always the root node (of traversal). Then, the nodes to the left of the identified root node in the in-order sequence all belong to the left subtree, and likewise for the right subtree. Repeat these observations recursively for each subtree until the full binary tree is constructed.

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
Every connected graph has a spanning tree, and any two spanning trees for a graph have the same number of edges.

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

Minimum Spanning Tree
A minimum spanning tree for a connected weighted graph is a spanning tree that has the least possible total weight compared to all other spanning trees for the graph. 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 10.7.1 (Kruskal's Algorithm)
In this algorithm, the edges of a connected weighted graph are examined one by one in order of increasing weight. At each stage, the edge being examined is added to what will become the minimum spanning tree, provided that this addition does not create a circuit.

```
def kruskal(G):
    T = new Graph()
    edges = edges_of(G)
    for edge in edges:
        e = min(edge) # wrt weight
        if T + e has no circuit:
            T = T + e
    return T
```

Algorithm 10.7.2 (Prim's Algorithm)
In this algorithm, a minimum spanning tree T is build by expanding outward in connected links from some vertex. One edge and one vertex are added at each iteration. The edge added is the one of least weight that connects the vertices already in T with those not in T, and the vertex is the endpoint of this edge that is not already in T.

```
def prims(G):
    seed = random.choice(V(G))
    T = new Graph(seed)
    vertices = V(G) - seed
    while V(T) != V(G):
        # find min edge connecting T to G - T
        e = least_edge(T, vertices)
        T = T + e
        vertices = vertices - endpts(e)
    return T
```