CS1231 Cheat Sheet

[2018-08-28 Tue]

Contents

1 Proof Techniques

1.1 Proof by Construction

Strategy: Prove ∃ statements by finding an explicit solution. Alternatively, disprove ∀ statements by finding an explicit counterexample.

1.2 Proving If-Then Statements

Strategy: Assume P is true → chain of logical deductions → show that Q must be true. Thus P → Q.

1.3 Proving For-All Statements

Strategy: Take any particular arbitrarily chosen value (e.g. x). Show that if P(x) is true for this x, then it must be true that $\forall x P(x)$.

(Example: proof that ∀a,b,c ∈ ℤ, (a|b ∧ b|c) → a|c)

1. Take *any* three integers a, b, c.
2. Assume that a|b and b|c.
   2.1. ...
   2.x. *<Proof that a|c>*

1.4 Proof by Contraposition

Strategy: Instead of proving P → Q directly, you can prove ∼Q → ∼P.

Useful when dealing with if-then statements with an *absent* form, by turning it into one with a *present* form, so it's easier to manipulate.

(Example: instead of proving that x^2 is irrational → x is irrational, prove that x is rational → x^2 is rational)

1.5 Proof by Contradiction

Strategy: To prove that P is true, assume that ∼P is true. Then arrive at a contradiction using logical deductions. So the assumption must be false, i.e. P must be true.

(Example: proving that $\sqrt{2}$ is irrational: assume that $\sqrt{2}$ is rational, then arrive at a contradiction)

(Example: proving that 7 is not divisible by 3 by assuming that 3|7, then arrive at a contradiction)

2 Logic of Compound Statements

2.1 Logical Form and Logical Equivalence

Statement/proposition is a sentence that is true or false, but not both.

Negation of a statement variable p is denoted $\sim p$.

Conjunction of p and q is denoted $p \wedge q$.

Disjunction of p and q is denoted $p \vee q$.

Statement form is an expression made up of statement variables and logical connectives that becomes a statement when actual statements are substituted for the component statement variables.

Logical equivalence: two statement forms are logically equivalent if they have identical truth values for each possible substitution of statements for statement variables.

Tautology is a statement form that is always true regardless of truth values of statement variables.

Contradiction is a statement form that is always false regardless of truth values of statement variables.

Theorem 2.1.1 Logical Equivalences

Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv p \vee q$
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	$p \wedge true \equiv p$	$p \vee false \equiv p$
Negation laws	$p \vee \sim p \equiv true$	$p \wedge \sim p \equiv false$
Double negative law	$\sim (\sim p) \equiv p$	
Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal bound laws	$p \vee true \equiv true$	$p \wedge false \equiv false$
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	$\sim true \equiv false$	$\sim false \equiv true$

2.2 Conditional Statements

Conditional statements and their variants

- Conditional of q by p is "if p then q" or "p implies q" denoted $p \to q$. Hypothesis/antecedent $\to$ conclusion/consequent.

Conditional	$p \to q$	$\sim q \to \sim p$	Contrapositive
Converse	$q \to p$	$\sim p \to \sim q$	Inverse

Implication law: $p \to q \equiv \sim p \vee q$

Other forms

- Necessary: p is a necessary condition for $q \equiv q \to$ p
- Sufficient: p is a sufficient condition for $q \equiv p \to$ q
- Biconditional: p if and only if $q \equiv p \leftrightarrow q$
- Only if: p only if $q \equiv p \to q$

2.3 Order of Operations

1. $\sim$
2. $\wedge$, $\vee$ (coequal in order)
3. $\rightarrow$, $\leftrightarrow$ (coequal in order)

2.4 Valid and Invalid Arguments

Argument (form) is a sequence of statements (statement forms). The final statement is called the conclusion, all other statements are called premises.

Valid: An argument is valid if no matter what statements are substituted for the statement variables, if the premises are true, the conclusion is also true.

Sound: An argument is sound if and only if it is valid and all its premises are true.

Table 2.3.1 Rules of Inference

Modus Ponens	$p \rightarrow q$ p $\bullet\ q$	
Modus Tollens	$p \rightarrow q$ $\sim q$ $\bullet \sim p$	
Generalisation	p $\bullet\ p \vee q$	q $\bullet\ p \vee q$
Specialisation	$p \wedge q$ $\bullet\ p$	$p \wedge q$ $\bullet\ q$
Conjunction	p q $\bullet\ p \wedge q$	
Elimination	$p \vee q$ $\sim p$ $\bullet\ q$	$p \vee q$ $\sim q$ $\bullet\ p$
Transitivity	$p \rightarrow q$ $q \rightarrow r$ $\bullet\ p \rightarrow r$	
Proof by Division Into cases	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\bullet\ r$	
Contradiction Rule	$\sim p \rightarrow$ false $\bullet\ p$	

3 Logic of Quantified Statements

3.1 Predicates and Quantified Statements

Predicate: a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables.

Domain of a predicate variable: set of all values that may be substituted in place of the variable.

Truth set: If *P(x)* is a predicate and x has domain D, the truth set is the set of all elements in D that make *P(x)* true when they are substituted for x.

- Notation: Truth set of *P(x)* is denoted $\{x \in D | P(x)\}$

Universal statement: a statement of the form $\forall x \in D, Q(x)$

- Defined true iff *Q(x)* is true for every x in D
- Defined false iff *Q(x)* is false for at least one x in D
- Counterexample: a value for x for which *Q(x)* is false

Existential statement: a statement of the form $\exists x \in D$ such that $Q(x)$

- Defined true iff *Q(x)* is true for at least one x in D
- Defined false iff *Q(x)* is false for every x in D

Notation

- $P(x) \Rightarrow Q(x)$ is equivalent to $\forall x, P(x) \rightarrow Q(x)$
- $P(x) \Leftrightarrow Q(x)$ is equivalent to $\forall x, P(x) \leftrightarrow Q(x)$

Theorem 3.2.1 Negation of a Universal Statement

$\sim (\forall x \in D, P(x)) \equiv \exists x \in D, \sim P(x)$

Theorem 3.2.2 Negation of an Existential Statement

$\sim (\exists x \in D, P(x)) \equiv \forall x \in D, \sim P(x)$

Contrapositive, converse, inverse

Conditional	$\forall x \in D, P(x) \rightarrow Q(x)$	$\forall x \in D, \sim Q(x) \rightarrow \sim P(x)$	Contrapositive
Converse	$\forall x \in D, Q(x) \rightarrow P(x)$	$\forall x \in D, \sim P(x) \rightarrow \sim Q(x)$	Inverse

Necessary and sufficient conditions, only if

- $\forall x, r(x)$ is a sufficient condition for $s(x)$ means $\forall x, r(x) \rightarrow s(x)$
- $\forall x, r(x)$ is a necessary condition for $s(x)$ means $\forall x, s(x) \rightarrow r(x)$
- $\forall x, r(x)$ only if $s(x)$ means $\forall x, r(x) \rightarrow s(x)$

3.2 Statements with Multiple Quantifiers

Multiply quantified statements

Can combine $\exists / \forall$ together (if types are not mixed), and are interchangeable.

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

$\exists x, y \in D, P(x, y) \equiv \exists x \in D, \exists y \in D, P(x, y)$

Negations of multiply-quantified statements

$\sim (\forall x \in D, \exists y \in E, P(x,y)) \equiv \exists x \in D, \forall y \in E, \sim P(x,y)$

$\sim (\exists x \in D, \forall y \in E, P(x,y)) \equiv \forall x \in D, \exists y \in E, \sim P(x,y)$

Order of quantifiers

If the types ($\forall/\exists$) are the same, can interchange order of quantifiers.

If the types ($\forall/\exists$) are different, cannot interchange order of quantifiers.

$\forall x \in D, \exists y \in D, P(x,y) \not\equiv \exists y \in D, \forall x \in D, P(x,y)$

3.3 Arguments with Quantified Statements

Rule of universal instantiation: If some property is true for everything in a set, then it is true for any particular thing in the set.

Universal Modus Ponens	$\forall x, P(x) \to Q(x)$ $P(a)$ for a particular a $\bullet Q(a)$
Universal Modus Tollens	$\forall x, P(x) \to Q(x)$ $\sim Q(a)$ for a particular a $\bullet \sim P(a)$
Universal transitivity	$\forall x, P(x) \to Q(x)$ $\forall x, Q(x) \to R(x)$ $\bullet \forall x, P(x) \to R(x)$

Valid argument form: no matter what particular predicates are substituted for the predicate symbols in its premises, if the resulting premise statements are all true, then the conclusion is also true.

Converse error (quantified form)	$\forall x, P(x) \to Q(x)$ $Q(a)$ for a particular a $\bullet P(a)$
Inverse error (quantified form)	$\forall x, P(x) \to Q(x)$ $\sim P(a)$ for a particular a $\bullet \sim Q(a)$

4 Number Theory

4.1 Divisibility

Divisibility

$d|n \leftrightarrow \exists k \in \mathbb{Z}$ such that $n = dk$

Theorem 4.1.1 Linear Combination

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

Theorem 4.3.1 (Epp)

$\forall a, b, c \in \mathbb{Z}^+, a|b \rightarrow a \leq b$

Theorem 4.3.2 (Epp)

$\forall d \in \mathbb{Z}, d|1 \rightarrow d = \pm 1$

Theorem 4.3.3 (Epp) Transitivity of Divisibility

$\forall a, b, c \in \mathbb{Z}, a|b$ and $b|c \rightarrow a|c$

4.2 Primes

Prime and Composite

n is prime $\leftrightarrow \forall r, s \in \mathbb{Z}^+, n = rs \rightarrow (r = 1$ and $s = n)$ or $(r = n$ and $s = 1)$

n is composite $\leftrightarrow \exists r, s \in \mathbb{Z}^+, n = rs$ and $(1 < r < n)$ and $(1 < s < n)$

Every integer n>1 is either prime or composite.

Proposition 4.2.2

For any 2 primes p and p', $p \mid p' \rightarrow p = p'$

Proposition 4.7.3 (Epp)

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

Theorem 4.3.4 (Epp) Divisibility by a Prime

Any integer $n > 1$ is divisible by a prime number

Theorem 4.7.4 (Epp) Infinitude of Primes

The set of primes is infinite

Theorem 4.2.3

If p is prime and $x_1, x_2 ... x_n$ are any integers such that $p|x_1 x_2 ... x_n$, then $p|x_i$ for some $x_i (1 \leq i \leq n)$

Theorem 4.3.5 (Epp) Unique Prime Factorization

Given any integer $n > 1, \exists k \in \mathbb{Z}^+$ and $\exists$distinct prime numbers $p_1, p_2 ... p_k$ and $\exists e_1, e_2 ... e_k \in \mathbb{Z}^+$ such that $n = {p_1}^{e_1} {p_2}^{e_2} ... {p_k}^{e_k}$

4.3 Primality Testing

1) Trial Division

Test if n is divisible by all integers k between 2 and sqrt{n} (rounded up).

2) Sieve of Eratosthenes

Generate a list of primes using the sieve (crossing out all multiples of a number starting from 2, etc.). Check n against the list of primes.

3) Miller-Rabin probabilistic test

Tests for compositeness—if the tests come out positive, it is definitely composite, but if it's negative, it's *probably* not. Run the test over and over to reduce the probability of a pseudoprime.

4.4 Well-Ordering Principle

Lower bound

An integer b is a lower bound for a set $X \subseteq \mathbb{Z}$ if b≤x ∀x∈X.

Well-ordering principle I (Theorem 4.3.2)

S has a least element if a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound.

- S is non-empty
- $S \subseteq \mathbb{Z}$
- S has a lower bound

Proposition 4.3.3 Uniqueness of least element

If a set $S \subseteq \mathbb{Z}$ has a least element, then the least element is unique.

Well-ordering principle II (Theorem 4.3.2)

S has a greatest element if a non-empty set $S \subseteq \mathbb{Z}$ has an upper bound.

- S is non-empty
- $S \subseteq \mathbb{Z}$
- S has an upper bound

Proposition 4.3.4 Uniqueness of greatest element

If a set $S \subseteq \mathbb{Z}$ has a greatest element, then the greatest element is unique.

4.5 Quotient-Remainder Theorem

Quotient-remainder theorem

Given any integer a, and any positive integer b, $\exists! q, r \in \mathbb{Z}$ such that $a = bq + r$, where $0 \leq r < b$.

Representation of integers in base b

$$
\begin{aligned}
&n = bq_0 + r_0\\
&q_0 = bq_1 + r_1\\
&q_1 = bq_2 + r_2\\
&\ldots\\
&q_{m-1} = bq_m + r_m\\
&\text{(process stops when } q_m = 0)
\end{aligned}
$$

Read the remainders from bottom up to get $(r_m r_{m-1} \ldots r_1 r_0)_b$

Representation: $n = (r_m r_{m-1} \ldots r_1 r_0)_b = r_m b^m + r_{m-1} b^{m-1} + \ldots + r_1 b + r_0$

4.6 GCD

GCD(a,b) is the integer d satisfying: (where a and b are not both 0)

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

GCD(0,0) is undefined.

GCD can be found through prime factorization.

Existence of GCD (Prop 4.5.2)

For any $a, b \in \mathbb{Z}$, not both 0, their GCD exists and is unique

Euclid's algorithm

GCD(a,0) $= a$

GCD(a,b) = GCD(b,r) where r is the remainder of a/b (or a mod b)

Bezout's identity

There exists $x, y \in \mathbb{Z}$ such that $ax + by = d$, where $d =$ GCD(a,b) and a and b are not both 0.

i.e. GCD(a,b) can be expressed as a linear combination of a and b

Relatively prime

a, b are relatively prime (coprime) $\leftrightarrow$ GCD(a,b) = 1

Theorem 4.2.3

If p is prime and $x_1, x_2 \ldots x_n$ are integers such that $p|x_1 x_2 \ldots x_n$, then $p|x_i$ for some $1 \leq i \leq n$

Proposition 4.5.5

$\forall a, b \in \mathbb{Z}$, not both 0, if c is a common divisor of a and b, then $c|$GCD(a,b)

4.7 LCM

LCM(a,b) for any non-zero integers a,b, is the positive integer m such that:

- $a|m$ and $b|m$
- $\forall c \in \mathbb{Z}^+$, if $a|c$ and $b|c$, then $m \leq c$

GCD(a,b) $\cdot$ LCM(a,b) = ab

4.8 Modulo Arithmetic

Congruence modulo

m $\equiv$ n (mod d) $\leftrightarrow$ d | (m-n), where m,n$\in \mathbb{Z}$, d$\in \mathbb{Z}^+$

Theorem 8.4.1 (Epp): Modular equivalences

1. a $\equiv$ b (mod n)
2. n | (a-b)
3. a = b + kn, for some k$\in \mathbb{Z}$
4. a and b have same remainder when divided by n
5. a mod n = b mod n

Theorem 8.4.3 (Epp): Modulo arithmetic

Suppose a $\equiv$ c (mod n) and b $\equiv$ d (mod n), where a,b,c,d,n$\in \mathbb{Z}$ with n>1.

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

Corollary 8.4.4 (Epp): Further modulo arithmetic

1. ab $\equiv$ [(a mod n)(b mod n)] mod n
2. ab mod n = [(a mod n)(b mod n)] mod n
3. $a^m \equiv$ (a mod n)^m (mod n)

Inverses

Multiplicative inverse modulo n

If as $\equiv$ 1 (mod n), then s is the multiplicative inverse of a modulo n. $aa^{-1} \equiv$ 1 (mod n), and $a^{-1}a \equiv$ 1 (mod n)

Theorem 4.7.3 Existence of modulo inverse

For any integer a, a^{-1} exists iff a and n are coprime.

(Find a^{-1} (mod n) by running the Extended Euclidean Algorithm!)

Corollary 4.7.4 Special case: n is prime

All integers a in range 0<a<p have multiplicative inverses (mod p) if p is prime (because gcd(a,p) = 1 if 0<a<p)

Theorem 8.4.9 (Epp): Cancellation law for modulo arithmetic

If ab $\equiv$ ac (mod n) where a and n are coprime, then b $\equiv$ c (mod n), $\forall$a,b,c,n with n > 1

5 Induction

5.1 Regular Induction

Proof (by Mathematical Induction)

1. ∀n ∈ Domain, let P(n) = <statement>.
2. Base case: n = <base>
   2.x *<Show that P(base) is true>*
3. Inductive step: for any k ∈ Domain,
   3.1 Assume that P(k) is true, i.e. ... (Strong induction: Assume that P(i) is true for <base>≤i≤k)
   3.2 Consider the k+1 case:
   3.x *<Show that P(k+1) is true>*
4. So by Mathematical Induction, P(n) is true ∀n ∈ Domain. QED.

5.2 Strong Induction

Like regular induction (as above), but make a stronger assumption in the inductive step: instead of assuming that P(k) is true, assume that P(base) until P(k) is true.

6 Sequences and Recursion

6.1 Sequences

Explicit formula: $a_n = f(n)$ for some function f, where you can calculate the n^{th} term directly. (*Cannot guess f of an infinite sequence with finite number of terms!)

Recurrence relation: tells you how a_n is related to a_{n-1}, $a_{n-2} \ldots$, *initial conditions* e.g. $a_0 = 0$, $a_1 = 1$

6.2 Summation and Product

Summing a sequence yields another sequence.

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + ... + a_n = S_n, \forall n \in \mathbb{N} \text{ e.g. } \sum_{i=0}^{n} = \frac{n(n+1)}{2} = triangle(n)$$

Multiplying a sequence also yields another sequence.

$$\prod_{i=m}^{n} a_i = a_m \times a_{m+1} \times \cdots \times a_n = P_n, \forall n \in \mathbb{N} \text{ e.g. } \prod_{i=0}^{n} i = n!$$

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, the following holds for $n \geq m$:

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

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

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

Note: lower and upper limits must be the same!

Changing variables

$$\sum_{k=1}^{n+1} \frac{k}{n+k} \to \sum_{j=0}^{n} \frac{j+1}{n+j+1} \to \sum_{k=0}^{n} \frac{k+1}{n+k+1} \quad \text{(sub } k = j+1\text{)}$$

6.3 Common Sequences

Arithmetic sequence

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

Explicit formula: $a_n = a + (n-1)d$

Sequence of sum of first n terms: $S_n = \frac{n}{2}[2a + (n-1)d]$

Geometric sequence

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

Explicit formula: $a_n = ar^n$

Sequence of sum of first n terms: $S_n = \frac{a(r^n-1)}{r-1}$ and if |r|<1, $S_\infty = \frac{a}{1-r}$

Square numbers: $f(n) = n^2 =$ sum of first n odd numbers

Triangle numbers: $f(n) = \frac{n(n+1)}{2} =$ sum of first n+1 integers

Fibonacci numbers: $\begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ F_{n-1} + F_{n-2} & \text{otherwise} \end{cases}$

Binomial numbers: $\begin{cases} 1 & \text{if } r = 0 \text{ and } n \geq 0 \\ \binom{n-1}{r} + \binom{n-1}{r-1} & \text{if } 0 < r \leq n \\ 0 & \text{otherwise} \end{cases}$

Some identities:

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

6.4 Solving Recurrences

Guess and check

Calculate a few terms, guess the pattern, and check using induction.

Second-order linear homogeneous recurrence relation with constant coefficients

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

Theorem 5.8.3 (Epp) Distinct-Roots Theorem

For the above relation, if the characteristic equation $t^2 - At - B = 0$ has 2 distinct roots r and s, then explicit formula = $a_n = Cr^n + Ds^n$, where C and D are determined by initial conditions a_0 and a_1 (use substitution).

Theorem 5.8.5 (Epp) Single-Roots Theorem

(Same as above, but) if the characteristic equation $t^2 - At - B = 0$ has a SINGLE real root r, then explicit formula: $a_n = Cr^n + Dnr^n$, where C and D are determined by initial conditions a_0 and a_1 (use substitution).

7 Sets

7.1 Introduction

Subset: $S \subseteq T \leftrightarrow \forall x \in S, x \in T$

Proper subset: $S \subset T \leftrightarrow S \subseteq T \ \wedge \ \exists x \ (x \in T \wedge x \notin S)$

7.2 Basic Set Theory

Universal set: U contains all objects.

Empty set: ϕ or $\{\}$ has no elements.

Power set of S, $\mathcal{P}$(S): set whose elements are all possible subsets of S. Has $2^{|S|}$ elements.

Proposition 6.2.3 Proving set equality

$X \subseteq Y \wedge Y \subseteq X \ \leftrightarrow \ X = Y$

Corollary 6.2.5 (Epp) Empty set is unique

7.3 Operations on Sets

Union: $A \cup B = \{x \in U \mid x \in A \vee x \in B\}$

Intersection: $A \cap B = \{x \in U \mid x \in A \wedge x \in B\}$

Disjoint: S and T are disjoint $\leftrightarrow S \cap T = \phi$

Mutually disjoint: Let V be a set of sets. V is mutually disjoint $\leftrightarrow$ every 2 distinct sets in V is disjoint.

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

Partition: V (a set of non-empty subsets of S) is a partition of S if:

- Sets in V are mutually disjoint
- Union of sets in V = S
- (Each element in S belongs to 1 and only 1 set in V)

Non-symmetric difference: $S - T = \{ \ y \in U \mid y \in S \wedge y \notin T \ \}$

Symmetric difference: $S \ominus T = \{ \ y \in U \mid y \in S \oplus y \in T \ \}$

Complement: $A^c = U - A$ such that $x \in A \rightarrow x \notin A^c$

Theorem 6.2.1 (Epp) Subset relations

Inclusion of intersection	$A \cap B \subseteq A$	$A \cap B \subseteq B$
Inclusion in union	$A \subseteq A \cup B$	$B \subseteq A \cup B$
Transitive property of subsets	$A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$	

Theorem 6.2.2 (Epp) Set identities

Commutative laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative laws	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity laws	$A \cup \phi = A$	$A \cap U = A$
Complement laws	$A \cup A^c = U$	$A \cap A^c = \phi$
Double complement law	$(A^c)^c = A$	
Idempotent laws	$A \cup A = A$	$A \cap A = A$
Universal bound laws	$A \cup U = U$	$A \cap \phi = \phi$
De Morgan's laws	$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$
Absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complements	$U^c = \phi$	$\phi^c = U$
Set difference	$A - B = A \cap B^c$	

Theorem 6.2.3 (Epp) Intersection and Union with a subset

$A \subseteq B \rightarrow (A \cap B = A) \;\wedge\; (A \cup B = B)$

8 Relations

8.1 Introduction to Relations

Ordered pair (x,y): object with first element x, second element y

Cartesian product S×T: set of all ordered pairs (x,y) where x∈S, y∈T

8.2 Relations

Binary relation R from S to T: subset of S×T

- $s\ R\ t \equiv (s,t) \in R$
- $s \not R\ t \equiv (s,t) \notin R$

Domain of R, Dom(R): the set $\{\ s \in S \mid \exists t \in T\ (s\ R\ t)\ \}$

Image of R, Im(R): the set $\{\ t \in T \mid \exists s \in T\ (s\ R\ t)\ \}$ (also known as *range*)

Codomain of R, coDom(R): the set T

Proposition 8.2.5

$Im(R) \subseteq coDom(R)$ where R is a binary relation

Inverse of R, R^{-1}: the relation from T to S, where $\{\ (t,s) \in T \times S \mid (s,t) \in\ R\ \}$ i.e. $\forall s \in S, \forall t \in T, (s\ R\ t \leftrightarrow t\ R^{-1}\ s)$

Composition of R with R', $R' \circ R$: where $R \subseteq\ S \times T\ R' \subseteq\ T \times U$, is the relation from S to U such that $\forall s \in S, \forall u \in U(s\ R' \circ R\ u \leftrightarrow (\exists t \in T(s\ R\ t \wedge t\ R'\ u)))$

- i.e. s∈S and u∈U are related iff there is a 'path' from s to u, through some intermediate element t∈T

Proposition 8.2.9 Composition is associative

$R'' \circ R' \circ R = (R'' \circ R') \circ R = R'' \circ (R' \circ R)$

Proposition 8.2.10 Inverse of composite

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

8.3 Properties of Relations on a Set

Let A be a set, R be a relation on A.

Reflexive: R is reflexive $\leftrightarrow \forall x \in A\ (x\ R\ x)$

Symmetric: R is symmetric $\leftrightarrow \forall x, y \in A\ (x\ R\ y \rightarrow y\ R\ x)$

Transitive: R is transitive $\leftrightarrow \forall x, y, z \in A\ (x\ R\ y \wedge y\ R\ z \rightarrow x\ R\ z)$

8.4 Equivalence Relations

Equivalence relation: R is an equivalence relation $\leftrightarrow$ R is reflexive, symmetric, and transitive

Equivalence class of x, [x]: $[x] = \{\ y \in A \mid x\ R\ y\ \}$ where R is an equivalence relation on A (i.e. all related to x)

Theorem 8.3.4 (Epp) Partition induced by an equivalence relation

Let R be an equivalence relation on A. Then the set of distinct equivalence classes form a *partition* of A.

Theorem 8.3.1 (Epp) Equivalence relation induced by a partition

Let S_1, $S_2 \dots$ be a partition of A. Then there exists an *equivalence relation* R on A where equivalence classes make up that partition.

8.5 More Definitions

Transitive closure of R, R^t is a relation such that:

- R^t is transitive
- $R \subseteq R^t$
- If S is any other transitive relation such that $R \subseteq S$, then $R^t \subseteq S$ (i.e. R^t is the *smallest superset* that is transitive)

Reflexive closure and symmetric closure are defined similarly

Repeated compositions

$R^n \ = \ R \circ R \circ \dots R \ = \ \bigodot_{i=1}^{n} R$

Proposition 8.5.2 Finding the transitive closure

$R^t = \bigcup_{i=1}^{\infty} R^i$ i.e. $R^1 \cup R^2 \cup R^3 \cup \dots$

8.6 Partial and Total Orders

Partial order: $\preceq$ is a partial order $\leftrightarrow$ $\preceq$ is *reflexive*, *anti-symmetric*, and *transitive* (where $\preceq$ is a binary relation)

- Anti-symmetric: R is anti-symmetric $\leftrightarrow \forall x, y \in A \ (x \ R \ y \wedge y \ R \ x) \rightarrow x = y$

Total order: A partial order $\preceq$ is a total order $\leftrightarrow \forall x, y \in A \ (x \preceq y \vee y \preceq x)$ (i.e. it is a partial order where all x,y are comparable)

- Comparable: Elements a and b are comparable $\leftrightarrow a \preceq b \vee b \preceq a$ (w.r.t some partial order $\preceq$)
- E.g. $(\mathbb{Z}, \leq)$ is a total order

8.7 Max, Min, Well-ordered

For $\preceq$ as a partial order on A,

- Maximal: An element x is maximal $\leftrightarrow \forall y \in A \ (x \preceq y \rightarrow x = y)$
- Maximum: An element $\top$ is maximum $\leftrightarrow \forall x \in A \ (x \preceq \top)$
- Minimal: An element x is minimal $\leftrightarrow \forall y \in A \ (y \preceq x \rightarrow x = y)$
- Minimum: An element $\perp$ is minimum $\leftrightarrow \forall x \in A \ (\perp \preceq x)$

Well-ordered: A is well-ordered $\leftrightarrow \forall S \in \mathcal{P}(A) \ (S \neq \phi \rightarrow \exists x \in S \ \ \forall y \in S \ (x \preceq y))$ for some total order $\preceq$, i.e. every non-empty subset contains a minimum element

- E.g. $(\mathbb{Z}^+, \leq)$ is well-ordered, but $(\mathbb{Z}, \leq)$ is not

9 Functions

9.1 Functions

Function: f is a function from S to T, $f : S \to T \leftrightarrow$ f a relation where $\forall x \in S, \exists! y \in T\ (x\ f\ y)$

Pre-image: x is a pre-image of y $\leftrightarrow$ for some x∈S, ∃y∈T such that f(x)=y

Inverse image

- Inverse image of y = $\{\ x \in S \mid f(x) = y\ \}$ i.e. set of all its pre-images
- Inverse image of U = $\{\ x \in S \mid \exists y \in U, f(x) = y\ \}$ i.e. set of all pre-images of all elements of U

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

9.2 Function Properties

Let $f : S \to T$ be a function.

Injective: $f : S \to T$ is injective/one-one $\leftrightarrow \forall y \in T, \forall x_1, x_2 \in S\ (f(x_1) = y \wedge f(x_2) = y) \to x_1 = x_2$

Surjective: $f : S \to T$ is surjective/onto $\leftrightarrow \forall y \in T, \exists x \in S\ (f(x) = y)$

Bijective: $f : S \to T$ is bijective $\leftrightarrow$ f is both injective and surjective

Inverse: f is bijective $\leftrightarrow$ f^{-1} is a function

9.3 Composition

Let $f : S \to T$ and $g : T \to U$ be two functions.

Composition: $g \circ f : S \to U$ is a function where $(g \circ f)(x) = g(f(x))$

Identity function on A, I_A: $\forall x \in A\ (I_A(x) = x)$

Proposition 7.3.3 Composing with inverse gives identity

$f^{-1} \circ f = I_A$ where $f : A \to A$ is injective

$f \circ f^{-1} = I_A$ where $f : A \to A$ is bijective

10 Counting and Probability

Sample space: Set of all possible outcomes of a random process

Event: Subset of a sample space

N(A): Number of elements in event A

$P(E) = \frac{N(E)}{N(S)}$, where S is a finite sample space, all outcomes are equally likely, E is an event in S

Theorem 9.1.1 Number of elements in a list

There are $n - m + 1$ integers from m to n inclusive.

10.1 Possibility Trees and Multiplication Rule

Probability tree: Keeps track of all possibilities of situations that happen in order

Theorem 9.2.1 Multiplication Rule

An operation of k steps (where step 1 has n_1 ways, step 2 has n_2 ways) can be performed in $n_1 \times n_2 \times \cdots \times n_k$ ways. The steps must be independent.

Permutation: A permutation of a set of n objects is an **ordering** of the objects in a row. $\#Permutations = n!$

r-Permutation: A r-permutation of a set of n elements, P(n, r) is an ordered selection of r elements from that set.

Theorem 9.2.3 r-Permutations from a set of n elements

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

10.2 Counting Elements of Disjoint Sets

Theorem 9.3.1 Addition Rule

$N(A) = N(A_1) + N(A_2) + \cdots + N(A_k)$, where $A = A_1 \cup A_2 \cup \cdots \cup A_k$ (A is the union of mutually disjoint sets)

Theorem 9.3.2 Difference Rule

$N(A - B) = N(A) - N(B)$, where $B \subseteq A$

Probability of complement

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

Theorem 9.3.3 Inclusion/Exclusion Rule for 2 or 3 sets

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

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

10.3 Pigeonhole Principle

Pigeonhole principle: A function from a finite set to a smaller finite set cannot be one-to-one/injective.

Generalized pigeonhole principle

For any function $f : X \to Y$ (where X has n elements, Y has m elements), for any positive integer k such that $k < \frac{n}{m}$, there exists some $y \in Y$ such that y is the image of at least *k+1* distinct elements of X.

Generalized pigeonhole principle (contrapositive)

For any function $f : X \to Y$ (where X has n elements, Y has m elements), if for all $y \in Y$ $f^{-1}(y)$ has at most k elements, then X has at most km elements, i.e. $n < km$.

Theorem 9.4.2

For a function $f : X \to Y$ (where X and Y have the same number of elements), f is one-to-one $\leftrightarrow$ f is onto.

10.4 Combinations

Combination: A subset of a set.

r-Combination: A r-Combination of a set of n elements is a subset with r elements.

Theorem 9.5.1 r-Combinations from a set of n elements

$\binom{n}{r} = \frac{n!}{r!(n-r!)} = \frac{P(n,r)}{r!}$, so we can deduce $P(n,r) = r! \times C(n,r)$

Theorem 9.5.2 Permutations of sets with repeated/indistinguishable elements (think MISSISSIPPI)

$\#Permutations = \binom{n}{n_1} \times \binom{n-n_1}{n_2} \times \binom{n-n_1-n_2}{n_3} \times \cdots \times \binom{n-n_1-\cdots-n_{k_1}}{n_k} = \frac{n!}{n_1! \times n_2! \times \ldots \times n_k!}$

(where n_1 elems are indistinguishable from one another, n_2 elems are indistinguishable from one another, etc.)

10.5 r-Combinations with Repetition Allowed

Multiset: a multiset of size r is a r-combination with repetition allowed

Theorem 9.6.1 Number of r-combinations with repetition allowed

#Number of ways $= \binom{r+n-1}{r}$

10.6 Summary

Select r of n elements	Order matters	Order does NOT matter
Repetition allowed	r^k	$\binom{r+n-1}{r}$
Repetition NOT allowed	$P(n,r)$	$C(n,r)$

10.7 Pascal's Formula and Binomial Theorem

Pascal's formula: $\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}$

Theorem 9.7.2 Binomial Theorem

$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n$

10.8 Probability Axioms and Expected Value

Probability axioms: (let S be a sample space, P be a probability function)

- $0 \leq P(A) \leq 1$
- $P(\phi) = 0$ and $P(S) = 1$
- $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

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

Expected value of a process $= \sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 P_2 + \cdots + a_n p_n$ (where a_i is an outcome with probability p_i)

Linearity of expectation: holds true regardless of whether the events are independent!

$E(X+Y) = E(X) + E(Y)$

$E(\sum_{i=1}^{n} c_i X_i) = \sum_{i=1}^{n} (c_i \times E(X_i))$

10.9 Conditional Probability, Bayes' Theorem, Independent Events

Conditional probability: $P(B|A) = \frac{P(B \cap A)}{P(A)}$ i.e. $P(A \cap B) = P(B|A) \times P(A)$

Theorem 9.9.1 Bayes' Theorem

$P(B_k|A) = \frac{P(A|B_k) \times P(B_k)}{P(A|B_1) \times P(B_1) + P(A|B_2) \times P(B_2) + ... + P(A|B_n) \times P(B_n)}$

where sample space S is a union of mutually disjoint events B_1 to B_n

Independent events: A and B are independent $\leftrightarrow P(A \cap B) = P(A) \times P(B)$

Pairwise independent: A, B, C are pairwise independent $\leftrightarrow$ A and B, A and C, B and C are independent

Mutually independent: A, B, C are mutually independent $\leftrightarrow$ A, B, C are pairwise independent and $P(A \cap B \cap C) = P(A) \times P(B) \times P(C)$

11 Graphs and Trees

11.1 Graphs

Graph: $G = \{V, E\}$ where $E(G)$ contains $e = \{v, w\}$ for $v, w \in V(G)$

- Edges incident on v: edges with v as one of its endpoints
- Edges adjacent to e: edges with a common endpoint to e
- Vertices adjacent to v: vertices connected by a common edge

Directed graph: $G = \{V, D\}$ where $D(G)$ contains $e = (v, w)$

Simple graph: undirected graph with no loops or parallel edges

Complete graph on n vertices, $\mathrm{K_n}$: a simple graph with n vertices, exactly 1 edge connecting each distinct pair of vertices. $\#edges = \binom{n}{2}$

Complete bipartite graph on (m,n) vertices, $\mathrm{K_{m,n}}$: simple graph with distinct vertices $\mathrm{v_1}$ to $\mathrm{v_m}$, $\mathrm{w_1}$ to $\mathrm{w_m}$ where:

- Edge between each $\mathrm{v_i}$ to each $\mathrm{w_j}$, no edge between any $\mathrm{v_i}$ to $\mathrm{v_k}$ or any $\mathrm{w_i}$ to $\mathrm{w_l}$
- $\#edges = m \times n$

Degree of vertex v, deg(v): #edges incident on v, where loops (if any) are counted twice

Total degree of graph G: sum of degrees of all the vertices of G

Theorem 10.1.1 Handshake Theorem

Total degree of G = 2 × #edges in G

So total degree is even, and there is an even number of vertices with odd degrees.

11.2 Trails, Paths, and Circuits

Walk from v to w: Finite alternating sequence of adjacent vertices and edges of G

Trail from v to w: Walk from v to w with no repeated edges

Path from v to w: Trail from v to w with no repeated vertices

Closed walk: Walk that starts and ends at same vertex

Circuit/cycle: Closed walk that is non-trivial with no repeated edges

Simple circuit/cycle: Circuit with no repeated vertices (except first and last)

	Repeated edge?	Repeated vertex?	Starts and ends at same pt?	Must have at least 1 edge?
Walk	OK	OK	OK	X
Trail	X	OK	OK	X
Path	X	X	X	X
Closed walk	OK	OK	✓	X
Circuit	X	OK	✓	✓
Simple circuit	X	Only first and last	✓	✓

Connected vertices: v and w are connected ↔ there is a walk from v to w

Connected graph: for all vertices v and w, they are connected i.e. there is a walk from v to w

Lemma 10.2.1

- If G is connected, any v,w$\in$V(G) can be connected by a path
- If vertices v,w$\in$V(G) are part of a circuit, and you remove 1 edge in the circuit, there still exists a trail from v to w
- If G is connected and G contains a circuit, then can remove 1 edge in the circuit without disconnecting G

Connected component: graph H is a connected component of G $\leftrightarrow$ H is a connected subgraph, and it is the largest possible (no other connected subgraph is a superset of H, containing vertices/edges not in H)

Euler circuit: A circuit that contains every vertex and every edge (i.e. starts and ends at same vertex, uses every edge exactly once, every vertex at least once)

Eulerian graph: A graph with an Euler circuit

Theorem 10.2.4

A graph has an Euler circuit $\leftrightarrow$ the graph is connected and every vertex has a positive even degree

Euler trail: A trail from v to w that contains every vertex and every edge (i.e. Euler circuit but can start and end at different vertices)

Corollary 10.2.5

A graph has an Euler trail from v to w $\leftrightarrow$ the graph is connected, every vertex has a positive even degree except v and w (odd degree)

Hamiltonian circuit: A simple circuit that includes every vertex of G (i.e. starts and ends at same vertex, uses every vertex exactly once except first/last)

Hamiltonian graph: A graph with a Hamiltonian circuit

Proposition 10.2.6

If graph G has a Hamiltonian circuit, then G has a subgraph H where:

- H has every vertex of G, H is connected
- H has same number of edges as vertices
- Every vertex of H has degree 2

11.3 Matrix Representations of Graphs

Adjacency matrix: (a_{ij}) represents number of edges from v_i to v_j. Undirected adjacency matrices are always symmetric.

Theorem 10.3.1

A graph G with connected components G_1 to G_k can be represented as the follows, with A_i representing the adjacency matrix of G_i:

$$\begin{bmatrix} A_1 & 0 & \dots & 0 \\ 0 & A_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & A_k \end{bmatrix}$$

Theorem 10.3.2 Number of walks of length N

(i,j)-entry of A^n = #walks of length n from v_i to v_j

11.4 Planar Graphs

Isomorphism: G is isomorphic to G' $\leftrightarrow$ there exists one-to-one correspondences (mappings) from each vertex to another vertex, each edge to another edge

Theorem 10.4.1 Graph isomorphism as an equivalence relation

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

Planar graph: A graph that can be drawn on a 2D plane without crossing edges

Euler's formula: $f = e - v + 2$

11.5 Trees

Tree: a connected graph that is circuit-free

Forest: a graph that is circuit-free and NOT connected

Lemma 10.5.1

Any non-trivial tree has at least one vertex of degree 1. (actually, at least two vertices)

Leaf: A vertex in a tree with degree 1, i.e. terminal vertex

Internal vertex: A vertex in a tree (with $\geq$3 vertices) with degree $>$ 1

Theorem 10.5.2

Any tree with n vertices (n>0) has n-1 edges.

Theorem 10.5.4

If G is a connected graph with n vertices and n-1 edges, then G is a tree.

11.6 Rooted Trees

Rooted tree: a tree in which one vertex is designated as the root

- Level of the root = 0

Binary tree: a rooted tree in which every parent has no more than 2 children

Full binary tree: a rooted tree in which every parent has exactly 2 children

Theorem 10.6.1 Full Binary Tree Theorem

If T is a full binary tree with k internal vertices, then T has (2k+1) vertices and (k+1) terminal vertices.

Theorem 10.6.2 Height and Terminal Vertices of a Binary Tree

A binary tree T with height h and t terminal vertices => $t \leq 2^h$ and $log_2 t \leq h$

BFS: Traverse the tree level by level, starting from root and exploring adjacent vertices

DFS: Traverse the tree by exploring immediate neighbours recursively

11.7 Spanning Trees and Shortest Paths

Spanning tree for G (connected graph): a tree containing every vertex of G

Proposition 10.7.1

Every connected graph with n vertices has a spanning tree with $n-1$ edges.

Minimum spanning tree for G (connected weighted graph): a spanning tree with minimum total weight

Kruskal's algorithm: Greedy, repeatedly pick edge of minimum weight that doesn't create a circuit

Prim's algorithm: Greedy, start from a vertex v and explore outwards, adding the edge of minimum weight that connects a vertex in the current tree to another vertex NOT in the current tree

12 Epp

12.1 Inequalities

T17: *Trichotomy law* For arbitrary real numbers a and b, exactly 1 of the 3 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 $a + c < b + c$ (*addition*)

T20: If $a < b$ and $c > 0$, then $ac < bc$ (*multiplication with +ve*)

T21: If $a \neq 0$, then $a^2 > 0$ (*square > 0*)

T22: $1 > 0$.

T23: If $a < b$ and $c < 0$, then $ac > bc$ (*multiplication with -ve*)

T24: If $a < b$, then $-a > -b$. In particular, if $a < 0$, then $-a > 0$. (*taking negatives*)

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

T26: If $a < c$ and $b < d$, then $a+b < c+d$. (*adding inequalities*)

T27: If $0 < a < c$ and $0 < b < d$, then $0 < ab < cd$ (*multiplying inequalities*)