CS1231S Note

November 28, 2024

1 Speaking Mathematically

1.1 Defintions

Natural Numbers	$\mathbb{N} = \{ 0, 1, 2, 3, ... \}$
Integers	$\mathbb{Z} = \{ -100, 3, 21, 32, ... \}$
Rational Numbers	$\mathbb{Q} = \{ -23, 8.6, \frac{1}{2}, 3, ... \}$
Real Numbers	$\mathbb{R} = \{ -1, \pi, \sqrt{2}, 4.5, ... \}$

1.1.1 Real Numbers vs Rational?

Rational numbers ($\mathbb{Q}$) are numbers that can be represented as a ratio of two numbers, e.g. $\frac{4}{3}$. Real numbers ($\mathbb{R}$) is the set of rational & irrational numbers.

1.2 Properties of Integers[1]

- Closure $x + y \in \mathbb{Z}$
- Commutativity $x + y = y + x$, and, $xy = yx$
- Associativity $x + y + z = (x + y) + z = x + (y + z)$, and $xyz = (xy)z = x(yz)$
- Distributivity $x(y + z) = xy + xz$
- Trichotomy $x = y$, or, $x < y$, or $x > y$

1.3 Even and Odd Integers[2]

n is even $\Leftrightarrow \exists k$ s.t. $n = 2k$
n is odd $\Leftrightarrow \exists k$ s.t. $n = 2k + 1$

1.4 Proofs in Lecture 1

- Product of two consecutive odd numbers is always odd[3]

2 Propositional Logic

2.1 Definitions

2.1.1 Statements

A statement is a sentence that is true or false, but not both.

[1] 1.3.3 pg.26
[2] 1.3.4 pg.27
[3] 1.3.4 pg. 28

2.1.2 Negation

If p is a statement variable, the negation of p is "not p", denoted ~p

2.1.3 Conjunction

Conjunction of 2 statement variables p, q, said "p and q", is denoted $p \wedge q$

2.1.4 Disjunction

Disjunction of 2 statement variables p, q, said "p or q", is denoted $p \vee q$

2.1.5 Statement Form

A statement form is an expression made up of statement variables and logical connectives

2.1.6 Logical Equivalence

Two statements are logically equivalent iff they have identical truth values. Denoted $p \equiv q$

2.1.7 Tautology

A statement form that is always true

2.1.8 Contradiction

A statement form that is always false

2.1.9 Conditional (only if)

Given statement variables p and q, "if p then q", or "p implies q" is denoted $p \rightarrow q$. p is the antecedent, and q is the consequent.
In this example, p is a sufficient condition for q - the "existence" of p guarantees the "existence" of q
q is a neccessary condition for p - if q occurs, p *may* occur.

$$p \rightarrow q \equiv \ ^{\sim}p \vee q$$

2.1.10 Converse, Inverse, Contrapositive

Given a statement P→Q,
1. **Converse**: Q→ P
2. **Inverse**: ~P→ ~Q
Converse ≡ Inverse

3. **Contrapositive**: ~Q → ~P
Contrapositive ≡ Original Statement

2.1.11 Vacuous Truth

A conditional statement that is true by virtue of the fact that its hypothesis is false

2.1.12 Biconditional

Given stmt variables p and q, "p, if and only if, q" is denoted p↔q
p is a necessary and sufficient condition for q

2.2 Truth Table of Operators

P	Q	P∨Q	P∧Q	P→Q	P⇔Q
T	T	T	T	T	T
T	F	T	F	F	F
F	T	T	F	T	F
F	F	F	F	T	T

2.3 Order of operation of statements

First

Op1	Op2
$\sim$	
$\wedge$	$\vee$
$\rightarrow$	$\Longleftrightarrow$

Last

2.4 Arguments

Arguments are a sequence of statements. All statements except the final one are called **premises**

if p, then Q ← premise
p ← premise
therefore q ← conclusion

2.4.1 Modus Ponens

$p \rightarrow q$
p
•q

2.4.2 Modus Tollens

$p \rightarrow q$
$\sim q$
• $\sim p$

2.4.3 Generalization

p
•p ∨ q

q
•p ∨ q

2.4.4 Specialization

p∧q
•p

p∧q
•q

2.4.5 Transitivity

$p \to q$
$q \to r$
$\bullet p \to r$

2.4.6 Proof By Division into Cases

$p \vee q$
$p \to r$
$q \to r$
$\bullet r$

2.4.7 Contradiciton Rule

$\sim p \to \text{false}$
$\bullet p$

2.4.8 Fallacies

1. Converse Error
$p \to q$
q
$\bullet p$

2. Inverse Error
$p \to q$
$\sim p$
$\bullet \sim q$

3. False Premise
When the premise is not true, e.g. If you're Singaporean, then you're rich.

2.4.9 Checking the Validity of Arguments

To do this, construct a truth table and then check the critical rows. Critical rows are rows in which each premise evaluates to true. If the conclusions are also true in the critical rows, they are valid.
Now consider that a premise with contraditions will have no critical rows. This makes it vacuously valid.

3 Predicate Logic

3.1 Definitions

3.1.1 Predicate

A predicate is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The domain is the set of all values that may be subbed in place of the variables.

3.1.2 Truth Set

The set of all elements of domain D that make P(x) true, denoted $\{x \in D \mid P(x)\}$

3.1.3 Universal Statement

A universal statement of the form ∀x∈D, Q(x) is defined to be true iff Q(x) is true for all x in D. It is false if Q(x) is false for at least one of x in D.

3.1.4 Existential Statement

A existential statement of the form ∃x∈D, Q(x) is defined to be true iff Q(x) is true for at least one x in D. It is false iff Q(x) is false for all x in D

3.1.5 Existential Quantifier

The symbol ∃! denotes "There exists a unique".

3.1.6 Negation of Universal Statements

A universal statement ∀x∈D, Q(x) is negated like so: ∃x∈D, ~Q(x) *Theorum 3.2.1*

3.1.7 Negation of Existential Statements

An existential statement ∃x∈D, Q(x) is negated like so: ∀x∈D, ~Q(x) *Theorum 3.2.2*

3.1.8 Universal Instantation

If some property is true of everything in the set, then it is true of any particular thing in the set. Universal instantation is taking an instance of something in that set, and using the properties on the set to prove some particular thing.

3.1.9 Universal Generalization

Paraphrased from tutorial: It is using an extablished property for an arbitrarily chosen element in the domain, and generalizing it to the domain as a whole.

3.2 Lessons Learnt

3.2.1 Complicated Quantifiers

The order of quantifiers matter. ∀ x ∃ y means "For all x there exists a y" - the y is variable across x. ∃ x ∀ y means "There exists a x for all y" - the x is **fixed** for all values of y.

When there are multiple existential qualifiers, things can get confusing but try to "scope" it. e.g. $\forall x \exists y \forall z$ - Scope the first two terms. The y is variable across x. Then, the last two terms - a specific y must work for all z.

3.2.2 Always consider the counterexample when proving an implication

If you see an implication, immediately consider the counterexample where T → F

3.2.3 Consider all sides in counterexamples

Just don't be careless. e.g. $\forall x, y \in \mathbb{Q}, (x \neq y \rightarrow \exists m \in \mathbb{Q}((x < m) \wedge (m < y)))$. Considered that it's possible that in a real number line there's always a number between 2 other numbers - but is it always more than x and less than y? Nope!

3.2.4 Universal statements apply for all, unless Implication

Consider the distinction between $\forall x \in A\ (P(x) \wedge Q(x))$ and $\forall x \in A\ (P(x) \rightarrow Q(x))$. The first statement states that P(x) and Q(x) are true for all x. The second statement has an *if*. Simple but don't get careless.

4 Set Theory

4.1 Definitions

4.1.1 Sets

Sets are an unordered collection of objects. The objects are members of sets
Membership of sets is denoted x∈S
The cardinality of the set, denoted |S|, is the amount of elements in the set.

4.1.2 Set Notations

1. Set Roster Notation
Specifies all members of the set.
S = {1, 2, 3}

2. Set Builder Notation
Builds a set using a predicate.
S = {x∈U : P(x)}
e.g. S = {(x,y) $\in \mathbb{Z} \times \mathbb{Z}$: x=2z for some $Z \in \mathbb{Z}$ }
This builds a set for ordered pairs where x must be even and y is **unrestricted**

3. Set Replacement Notation
Similar to Set builder, but reversed
S = {t(x) : x∈U}

4. Interval Notation
Describes a set using mathematical equalities.
(a, b) = {x∈ $\mathbb{R}$: a < x < b}

4.1.3 Definition of Subset

A is a subset of B iff every element of A is also an element of B.

$$A \subseteq B \text{ iff } \forall x \in A \rightarrow x \in B$$

A note on subsets. Ensure the comparison of items are always in the same "scope". e.g. if A = {1, 2, 3} and B = { {1,2,3}, 4, 5, 6}, then A∈B, but A$\not\subseteq$B

4.1.4 Proper Subsets

A is a proper subset of B iff A is a subset of B **and** A≠B.
Denoted A$\subsetneq$B.

4.1.5 Set equality

If A$\subseteq$B and B$\subseteq$A, then A=B.

4.1.6 Set difference

The difference of B minus A, denoted B\A, is the set of all elements that are in B and not A.
Symbolically,

$$B\backslash A = \{x \in U : x \in B \wedge x \notin A\}$$

A note on set difference.
Again, always consider the scope. If A = {1,2,3,{4}} and B = {4}, then A\B = {1,2,3,{4}}
Another note. Any set differenced by the empty set is the set itself.

4.1.7 Union of Sets

A union of 2 sets is the set of all elements in either set.
Symbolically,

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

4.1.8 Intersection of Sets

An intersection of 2 sets is the set of all elements appearing in **BOTH** sets.
Symbolically:

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

4.1.9 Complement of Sets

The complement of a set A is all the elements in the domain that are not in A.
Symbolically,

$$\bar{A} = \{\ \mathrm{x} \in \mathrm{U} \mid \mathrm{x} \notin \mathrm{A}\}$$

4.1.10 Empty Sets

A set with no element is denoted $\varnothing$.
An empty set is a subset of every set. $\varnothing \subseteq \forall A$ *Theorum 6.2.4*

4.1.11 Ordered Pairs

An ordered pair is of the form (x,y)

Equality of ordered pairs
Two ordered pairs (a,b) and (c,d) are equal iff a=c $\wedge$ b=d. **Remember** to explicitly show and write this out in proofs.

4.1.12 Cartesian Products

The cartesian products of two sets A and B is the set of all ordered pairs (a,b) where a$\in$A and b$\in$B.
Symbolically,

$$A \times B = \{(a, b)\ :\ a \in A \wedge b \in B\}$$

Cardinality of cartesian product is $|\ A\ | \times |\ B\ |$

4.1.13 Mutually Disjoint Sets

Two sets are disjoint iff A∩B = ∅
Multiple Sets A1,A2,...An are **mutually disjoint** if no two sets Ai and Aj have any elements in common.

4.1.14 Partitions of Sets

A division of sets into mutually disjoint sets.

4.1.15 Power Sets

Given a set A, the **power set** of A is the set of all subsets of A.
Symbolically,

$$x \in \mathcal{P}(A) \iff x \subseteq A$$

Power sets of empty set
$\mathcal{P}(\varnothing) = \{ \varnothing \}$
The power set of an empty set is the set containing the empty set - the empty set is the subset of every set.
The $\mathcal{P}(\mathcal{P}(\varnothing)) = \{ \varnothing, \{ \varnothing \} \}$
Always consider how the set at hand can be rearranged into subsets. If things get confusing, verify with cardinality - $| \mathcal{P}(A) | = 2^{|A|}$

Cardinality of power set
The cardniality of any power set is given 2^n where n = $| A |$

4.2 Lessons Learnt

4.2.1 Union of Power Sets

$\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$. Think of the biggest set in $A \cup B$ - the set of the elements in *both* A and B is not included in the union of two power sets.

4.2.2 Intersection of Power Sets [4]

$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

4.2.3 Difference of empty set

Any set S\∅ = S. Empty set has no elements, so elements in S that are not in the empty set is S.

4.2.4 Empty set confusion

Sometimes, empty sets can get confusing. When dealing with intersections or unions, I prefer to "enumerate" the empty set. That is, instead of using ∅, use {}. As such, it can be seen that any set A ∩ {} = ∅

[4] Assignment 1 Qn 6c

4.2.5 Properties of Sets

For all sets A, B, and C,

Inclusion of Intersection *Theorum 6.2.1*
a) $A \cap B \subseteq A$
b) $A \cap B \subseteq B$

Inclusion in Union
a) $A \subseteq A \cup B$
b) $B \subseteq A \cup B$

Transitive property of subsets
$A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$

Using properties for proofs
Make sure that you're strictly following these properties in proofs. E.g. if $S \subseteq A \cap B$, you cannot simply state $S \subseteq A$. Use the properties like so:

$$A \cap B \subseteq A \text{ (Inclusion of Intersection)}$$
$$S \subseteq (A \cap B) \wedge (A \cap B) \subseteq A$$
$$S \subseteq A \text{ (Transitive property of subsets)}$$

5 Relations

5.1 Definitions

5.1.1 Relation

A relation from A to B is a subset of $A \times B$
Given an ordered pair (x,y) in $A \times B$, xRy iff (x,y) $\in$ R.

5.1.2 Domain, Co-domain, Range

Domain is the set $\{a \in A : \ aRb \ for \ some \ b \in B\}$

Co-domain is the set B.

Range is the set $\{b \in B : \ aRb \ for \ some \ a \ \in A\}$

5.1.3 Inverse Relations

If R is a relation from A to B, the inverse relation R^{-1} is from B to A as follows: $R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$

5.1.4 Composition of Relations

Let A, B, and C be sets. Let $R \subseteq A \times B$ be a relation, and $S \subseteq B \times C$ be a relation. The **composition of R with S**, denoted $S \circ R$ is the relation from A to C such that:

$\forall x \in A, \forall z \in C \ (xS \circ Rz \iff (\exists y \in B(xRy \wedge ySz)))$

In other words, there must be some "link" (y in the above) between the two Relations

To find $R \circ R \circ ... \circ R$, we can put R in a graph first. Count how many R's there are - this is the amount of compositions. Then, check the graph for walks of count(R) - put in adjacency matrix

Composition of Self-Relations

A relation can be composited by itself. (From tutorial) In a digraph, an easy way to compute $R \circ R$ is as follows. (i) Start with the first element a and trace all possible destinations after taking exactly n arrows, n being the amount of compositions + 1. So if $R \circ R$, n=2. (ii) In a separate graph, draw the arrows pointing from the start element to the end. (iii) Repeat for all other elements.

Associativity of Compositions

$T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R$

Do not confuse this for commutativity! Compositions are noncommutative.

Inverse of Compositions

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

5.1.5 Reflexivity

R is reflexive iff $\forall x \in A \ (xRx)$

Note that this is not an implication, and thus cannot be vacuously true. That is to say, every element in the domain of the relation (in this case, A) MUST have a self-relation to be considered reflexive.

5.1.6 Irreflexivity

R is irreflexive iff $\forall x \in A \ (x \not R x)$

5.1.7 Symmetry

R is symmetric iff $\forall x, y \in A \ (xRy \rightarrow yRx)$

Note that this ***is*** an implication, and thus *can* be vacuously true if there is no xRy.

5.1.8 Asymmetry[5]

It's worth noting that asymmetry $\neq$ ~symmetry.

$\forall a, b \in A (aRb \rightarrow b \not R a)$

5.1.9 Antisymmetry

$$\forall x, y \in A \ (xRy \wedge yRx \rightarrow x = y)$$

5.1.10 Transitivity

R is transitive iff $\forall x, y, z \in A \ (xRy \wedge yRz \rightarrow xRz)$

Same as above, this can be vacuously true.

Exhaustively checking transitivity

To exhaustively check transitivity of a relation with N amount of elements, you'd have to check every triplet that fulfils aRb, bRc, aRc. In a set with N elements, there are N^2 amount of possible pairs, because each element is related to N other elements, including itself. Now, for each pair (a,b), we need to check all (b,c) pairs. There are N (b,c) pairs, as b is related to n c's. So, Each pair in the set is compared with N other pairs, so $\mathbf{N^3}$ checks are needed.

[5] Tutorial 5 Qn. 8

5.1.11 Transitive Closure

The transitive closure of a relation R fulfills these 3 properties
1. R^t is transitive
2. $R \subseteq R^t$
3. If S is any other transitive relation that contains R, then $R^t \subseteq S$

That is to say, the transitive closure is the *smallest* set that makes the relation R transitive.

5.1.12 Parititions (again)

$\mathcal{C}$ is a partition of set A if the following hold:
1) $\mathcal{C}$ is a set for wihch all elements are non-empty subsets of A.
2) Every element of A is in exactly one element of $\mathcal{C}$
Elements of a partition are called components of the partition.
Symbolically,

$$\forall x \in A, \exists! S \in \mathcal{C} \ (x \in S)$$

5.1.13 Relation induced by partitions

Given a partition $\mathcal{C}$ on a set A, the relation R **induced by the partition** is defined on A as follows:

$$\forall x, y, \in A,$$
$$xRy \iff \exists \ a \ component \ S \ of \ \mathcal{C} \ s.t. \ x, y \in S$$

A relation induced in this manner is reflexive, symmetric, and transitive. *Theorum 8.3.1*

5.1.14 Equivalence Relations

An equivalence relation is a relation R that is **reflexive, symmetric, and transitive**. The symbol $\sim$ denotes an equivalence relation. Additionally, the relation should partition the domain into dijoint sets, so each element must reside in 1 and only 1 equivalence class.

5.1.15 Equivalence Classes

The equivalence class of a, denoted [a], is the set of all elements x $\in$ A s.t. a is related to x.
Symbolically, $[a] \equiv \{x \in A : \ a \sim x\}$

A note on listing equivalent classes
Note that the equivalence class of a relation refers to the *elements* of the set A. While the relation are ordered pairs (x,y), [x] = {x, y}. The equivalence class is not an ordered pair.

5.1.16 Partition Induced by an Equivalence Relation

If A is a set and R is an equivalence relation on A, then the distinct equivalence classes of R form a partition of A. *Theorum 8.3.4*
Essentially saying, the equivalence classes are nonoverlapping.

5.1.17 Dividing a set by an equivalence relation

$A/\sim$ is the set of all equivalence classes with respect to $\sim$
$A/\sim = \{[x]\sim: \ x \in A\}$
e.g. S = { 1, 2, 3, 4, 5, 6}. Then, we have some $\sim$ s.t. [1] = {1,2}, [3] = {3,4,5,6}.
Then, $A/\sim$ = { {1,2}, {3,4,5,6}}

5.1.18 Antisymmetry

R is antisymmetric iff

$$\forall x, y \in A \ (xRy \wedge yRx \rightarrow x = y)$$

It's negation, R is **not antisymmetric** iff

$$\exists x, y \in A(xRy \wedge yRx \wedge x \neq y)$$

Antisymmetry and not symmetric are different
Observe carefully. Antisymmetry and symmetry can happen at the same time: think xRx.

5.1.19 Partial Order Relations

R is a **partial order relation** iff
1. R is reflexive
2. R is antisymmetric
3. R is transitive

A partial order of two elements x and y is denoted $x \preccurlyeq y$, where x occures *before* y. I prefer to call it x "unlocks" y.

Can a relation be a partial order and equivalence relation at the same time?
This essentially asks if a relation can be reflexive, antisymmetric, symmetric, and transitive at the same time. The only case in which asymmetry and symmetry holds is if there are no distinct x and y s.t. xRy. So they're all self-relations.

5.1.20 Comparability

Elements in a partial order are comparable if either $a \preccurlyeq b$ or $b \preccurlyeq a$. Otherwise, they are noncomparable.

A **set** is comparable iff

$$\forall x, y \in A \ (xRy \vee yRx)$$

Note that this is not an implication - all elements **have** to be related in one way with another!
In a Hasse Diagram, an element is comparable with all elements in any chain containing that element.

5.1.21 Compatibility [6]

Two elements a and b are **compatible** iff there exist some c ∈ A s.t. $a \preccurlyeq c$ and $b \preccurlyeq c$

5.1.22 Maximal, Minimal, Largest, Smallest Elements

Maximal Elements
Symbolically, $\forall x \in A(c \preccurlyeq x \rightarrow c = x)$
Essentially, if c is "unlocks" an element x, it must be itself. Note the implication, which means noncomparable elements do not prevent a c from being a maximal element

Minimal Elements
$\forall x \in A(x \preccurlyeq c \rightarrow c = x)$
If any element "unlocks" c, it must be itself.

[6] Tutorial 5, Qn. 9

Largest Elements
$\forall x \in A\ (x \preccurlyeq c)$
All elements "unlock" c. There is no implication, so **all** elements in the domain must "unlock" c.

Smallest Elements
$\forall x \in A\ (c \preccurlyeq x)$
c "unlocks" all elements. As above, there is no implication.

5.1.23 Total Order Relations

Given a partial order R on set A, R is a total order iff
A total order fulfils the 3 properties of a partial order, as well as **comparability**.

So, R is :
1. Reflexive
2. Antisymmetric
3. Transitive
4. **Comparable**

Cardinality of Total Orders
When asking for the cardinality of a total order, you must consider the amount of pairs in the definition $\forall x, y \in A\ (xRy \vee yRx)$. Because each element must be related to another, and because the relations must be antisymmetric, we can count the cardinality going down through N + (N-1) + (N-2) ... This is an arithmetic sequence, and its formula is given $\frac{(N+1)(N)}{2}$

5.1.24 Linearization of Partial Orders

If $\preccurlyeq$ is a partial order on Set A, A linearization of $\preccurlyeq$ is a total order $\preccurlyeq^*$ s.t.
$\forall x, y \in A\ (x \preccurlyeq y \rightarrow x \preccurlyeq^* y)$
Looking at the definition before, a linearization of a partial order essentially makes a partial order comparable. So, a partial order given as such:
$a \preccurlyeq b$ and $a \preccurlyeq c$
becomes a (possible) total order by adding $b \preccurlyeq^* c$
The final total order is: $a \preccurlyeq^* b \preccurlyeq^* c$.

5.1.25 Well-ordered Set

Given $\preccurlyeq$ a total order on set A, it is **well-ordered** iff every non-empty subset of A contains a smallest element.
Symbolically, $\forall S \in \mathcal{P}(A), S\ \neq \varnothing \rightarrow (\exists x \in S\ \forall y \in S(x \preccurlyeq y))$

Checking of well-ordered sets
When checking well-ordered sets, ensure that the domain *has* a smallest element. $\mathbb{Z}, \leq$ is not well ordered because $\mathbb{Z}$ has no smallest element in the first place! Then, check that the relation is a total order in the first place, that it satisfies the **comparability** axiom.

Well-Ordering Principle Every nonempty subset of $Z_{\geq 0}$ has a smallest element

5.2 Lessons Learnt

5.2.1 Transitive Closure

When calculating transitive closures, don't forget to check if the extra elements introduce new requirements for transitivity. e.g.

S = { (a,b), (b,c), (c,d) }, then

S^+ = { (a,c), (b,d) }

But this is wrong! (a,c) introduces another requirement for transitivity, as (a,c) and (c,d) requires **(a,d)**

5.2.2 Counterexamples in relations

If a question asks you to evaluate the truthyness of properties on relations, think of counterexamples but don't be too myopic. E.g, a question tells you that R is reflexive. Then, you may say $A = \{a, b\}$ and R $= \{(a, a), (b, b)\}$ But wouldn't $R = \{(a, a), (b, b), (\mathbf{a}, \mathbf{b})\}$ be reflexive too? Think of the edge cases.

5.3 Symmetry and equalness of R[7]

R is symmetric if and only if R $= R^{-1}$

5.4 Reflexivity and subsetitity of R ∘ R [8]

If R is reflexive, then $R \subseteq R \circ R$
Proof:
First, (x,y) ∈ R for some x,y ∈ A. Since R is reflexive, (x,x) and (y,y) ∈ R, and composing these with each other we have (x,y) ∈ R ∘ R.

5.5 Transitivity and subsetitity of R [9]

If R is transitive, then $R \circ R \subseteq R$ Given any (x,z) $\in R \circ R$, there exists some $y \in A$ such that (x,y) and (y,z) $\in R$. As R is transitive, then $(x, z) \in R$

5.6 Equivalence relation and equalness of compositions

From the previous two theorums, any relation that is symmetric, reflexive, and transitive (*equivalence relations*), will mean that $R \subseteq R \circ R$, and $R \circ R \subseteq R$. So, $R = R \circ R$

6 Functions

6.1 Definitions

6.1.1 Functions

Some function f from set X to set Y, $f : X \to Y$ is a relation satisfying the following:

$$\forall x \in X, \exists! y \in Y \ (x, y) \in f$$

A function from X to Y is a mapping from each element of X to exactly one element of Y. Denoted:

$$\text{f(x)} = \text{y} \ (x, y) \in f$$

In this case,

1. x is the **argument** of f.
2. f(x) is the **image** of x under f.
3. if f(x) = y, then x is a **preimage** of y.

[7] Tutorial 4, Qn. 2
[8] Tutorial 4, Qn. 5
[9] Tutorial 4, Qn. 5

6.1.2 Function Equality

Two functions f:A→B and g:$C \to D$ are equal iff

1. A = C
2. B = D
3. f(x) = g(x) $\forall x \in A$

6.1.3 Setwise image

This is a function defined on a set as the input. If $\mathbf{A} \subseteq X$,

$$f(\mathbf{A}) = \{\text{f(x): x}\in\mathbf{A}\}$$

It is essentially the range of a subset of the domain X.

6.1.4 Setwise preimage

Another function defined on a set as the input. If $\mathbf{B} \subseteq Y$,

$$f^{-1}(\mathbf{B}) = \{x \in X\text{: f(x)} \in \mathbf{B}\}$$

It is essentially the values in x that get the output y in B.
It is NOT an inverse function

6.1.5 Domain, Co-domain, Range

Using the previously-defined function f, the **domain** of f is X, **co-domain** is Y.

The **range** of f is the setwise image of X under f:

$$\{\text{y}\in\text{Y} : \text{y=f(x)}\ x \in X\}$$

Note that the range *subseteq* Co-domain

6.1.6 Injections

f:X→Y is injective (one-to-one) iff

$$\forall x_1, x_2 \in X\ (\text{f}(x_1) = \text{f}(x_2) \Rightarrow x_1 = x_2)$$

That is, each $x \in X$ injects a unique $y \in Y$.
You don't get an injection at the same place twice. probably.

6.1.7 Surjection

A function f:X→Y is surjective (onto) iff

$$\forall y \in Y\ \exists x \in X\ (\text{y=f(x)})$$

All elements in Y are occupied by some f(x).
*Every dart has been thrown **onto** the dartboard. And somehow, each dart occupies each score zone.*

6.1.8 Bijections

A function is bijective if it is injective and surjective: *Theorum 7.2.3*

$$\forall y \in Y \ \exists! x \in X \ (\text{y=f(x)})$$

Order of bijections The **order** of a bijection is the smallest n $\in \mathbb{Z}^+$ st:

$$f \circ f \circ f \circ ... \circ f = id_A$$

Where n corresponds to the amount of f's in the compositions. To clarify, it's the amount of compositions to make to get back the original function.

6.1.9 Inverse Functions

The inverse function "undoes" the function. It only exists if a bijection on f exists:

$$\forall x \in X \ \forall y \in Y \ (\text{y = f(x)} \Leftrightarrow \text{x=}f^{-1}\text{(y)})$$

Uniqueness of Inverses If g_1 and g_2 are inverses of f, then $g_1 = g_2$

6.1.10 Composition of Functions

Let f:X→Y and g:$Y \to Z$ be functions, g composed of f is denoted $g \circ f$ and is defined:

$$(g \circ f)\text{(x)} = \text{g(f(x))} \ \forall x \in X$$

Note which function is "executed" first - f

Associativity of Function Composition

$$(h \circ g) \circ f = h \circ (g \circ f)$$

However, it is noncommutative

6.1.11 Composition with identity functions

If f:X→ Y, then $f \circ id_x = f$. This is because $f(id_x(x)) = f(x)$. *Theorum 7.3.1*

Then, $id_Y \circ f = f$. This is because $id_Y(f(x)) = f(x)$.

6.1.12 Composition with inverse

Similarly, $f^{-1} \circ f = f^{-1}(f(x)) = f^{-1}(y) = x \Rightarrow id_X$ *Theorum 7.3.2*

And, $f \circ f^{-1} = f(f^{-1}(y)) = f(x) = y \Rightarrow id_Y$

6.1.13 Composition of Injections

If f and g are both injective, then $g \circ f$ is injective.

BUT note that f can be non-injective and $g \circ f$ can still be injective.

6.1.14 Composition of Surjection

If f and g are both injective, then $g \circ f$ is surjective. Same notice as before, be careful about the other way.

6.1.15 Sequence

An infinite **sequence** $a_0, a_1, a_2, ...$ can be represented by a function a whose domain is $\mathbb{Z}_{\geq 0}$ that satisfies $a(n) = a_n$ for every $n \in \mathbb{Z}_{\geq 0}$

6.1.16 String

A finite length string is of the form:

$$a_0 a_1 a_2 \dots a_{l-1}$$

where A is a set and $a_n \in A$, and l is the **length** of the string.
The **empty string** ϵ is the string of length 0.

6.1.17 String Equality

Given two strings $s_1 = a_0 a_1 a_2 .... a_{l-1}$ and $s_2 = b_0 b_1 b_2 ... b_{l-1}$,

s1=s2 iff $a_i = b_i$ for all $i \in \{0, 1, 2, .., l-1\}$

6.2 Lessons Learnt

6.2.1 Declare strings properly

Type that whole shit out. $s1$ is a string such that $s1 = a_0 a_1 a_2 ... a_{l-1}$. Don't lose mark like in the Assignment

7 Mathematical Induction

7.1 Definitions

7.1.1 Infinite Sequence Expression

We can express an infinite sequence in other forms. E.g., $\frac{1}{2}$, $\frac{2}{3}$, $\frac{3}{4}$, $\frac{4}{5}$...

7.1.2 Explicit Formulas

Some formula such that a_k = sequence for all integers k$\geq$1

For the example above, the explicit formula is

$$a_k = \frac{k}{k+1}$$

Alternatively,

$$b_{k-1} = \frac{k-1}{k} \text{ for all integers k} \geq 2$$

7.1.3 Sequence Comprehension

Some set-builder ish notation that fully expresses the sequence:

$$\text{a} = [\tfrac{k}{k+1} : \text{k}\in[1..]]$$

Alternatively,

$$\text{b} = [\tfrac{k-1}{k} : \text{k}\in[2..]]$$

Summation Notation
$\sum_{k=m}^{n} a_k$ is the **sum** of all terms $a_m, a_{m+1}, a_{m+2}, ..., a_n$

k is the **index** of the summation, m the **lower limit**, and n the **upper limit**.

Note that some sums are telescoping, where terms in different indexes cancel each other out and you are left with a simple sum.

It's worth noting that a natural sum till an integer n is given:

$$\tfrac{n(n+1)}{2}$$

Rules for Summations

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

Recursive Definition $\sum_{k=m}^{n} a_k = (\sum_{k=m}^{n-1} a_k) + a_n$

7.1.4 Product Notation

Similar to sum, $\prod_{k=m}^{n} a_k$. You can probably guess what this is.
Rules for Products

1. $\prod_{k=m}^{n} a_k$ * $\prod_{k=m}^{n} b_k = \prod_{k=m}^{n}(a_k * b_k)$

Recursive definition $\prod k = m^n a_k = (\prod k = m^{n-1} a_k)$ * a_n

7.1.5 Common Sequences

Arithmetic Progression
A sequence is an arithmetic progression iff there is a constant d such that

$$a_k = a_{k-1} + d \text{ for all integers k} \geq 1$$

As such,

$$a_n = a_0 + dn \text{ for all integers n}\geq 0$$

The arithmetic progression is given by the summation:

$$\sum_{k=0}^{n-1} a_k = \tfrac{n}{2}(2a_0 + \text{(n-1)d})$$

Geometric Sequence
A geometric sequence is some sequence such that there is some constant r that:

$$a_k = ra_{k-1} \text{ for all integers k}\geq 1$$

As such,

$$a_n = a_0 r^n \text{ for all integers n}\geq 0$$

The geometric sequence is given by the summation:

$$\sum_{k=0}^{n-1} a_k = a_0(\tfrac{1-r^n}{1-r})$$

7.1.6 Weak Mathematical Induction (MI1)

Method of Proof by Mathematical Induction

1. BEFORE you get ahead of yourself, establish a proposition of the form P(n). You want to prove P(n) is true.
2. **Basis Step:** Prove that P(a) is true, where a is the **SMALLEST** member of the domain of the preposition
3. **Inductive Hypothesis:** Assume P(k) is true for some integer $k \geq \underline{a}$
4. **Inductive Step:** Show that P(k+1) is true. Use properties of P(k) to do this.
5. Conclude: Since P(k) implies P(k+1), and P(k=a) is true, P(n) is true.

7.1.7 Strong Mathematical Induction (MI2)

Method of Proof by Strong Mathematical Induction

1. BEFORE you get ahead of yourself, establish a proposition of the form P(n). You want to prove P(n) is true.
2. **Basis Step:** P(a), P(a+1),...,P(b) are all true
3. **Inductive Hypothesis:** P(i) is true for all integers i from a through k
4. **Inductive Step:** Prove that P(k+1) is true. Use properties from previous sequences, like P(k-3) even to show that it's true. Or use division to cases.
5. Conclude: Therefore, P(n) is true.

Example: Strong MI Question: Consider the Fibonacci function:

$$F(0) = 0, \quad F(1) = 1, \quad F(n+1) = F(n) + F(n-1) \quad \text{for } n \geq 1.$$

One interesting property of this function can be expressed as:

$$P(a,b) : F(a+b) = F(a+1) \cdot F(b) + F(a) \cdot F(b-1), \quad \forall a \geq 0, b \geq 1.$$

Use mathematical induction to prove the above property. Simplify expressions when using properties of addition, multiplication, or the Fibonacci recurrence relation.

Solution

Step 1: Basis Steps
We verify the property $P(a, b)$ for the smallest values of b, namely $b = 1$ and $b = 2$.

1. **Case $b = 1$:** The property becomes:

$$F(a + 1) = F(a + 1) \cdot F(1) + F(a) \cdot F(0).$$

   Substituting $F(1) = 1$ and $F(0) = 0$, we have:

$$F(a + 1) = F(a + 1) \cdot 1 + F(a) \cdot 0 = F(a + 1).$$

   This is true.

2. **Case $b = 2$:** The property becomes:

$$F(a + 2) = F(a + 1) \cdot F(2) + F(a) \cdot F(1).$$

   Substituting $F(2) = 1 + 0 = 1$ and $F(1) = 1$, we have:

$$F(a + 2) = F(a + 1) \cdot 1 + F(a) \cdot 1 = F(a + 1) + F(a).$$

   By the Fibonacci recurrence relation $F(a + 2) = F(a + 1) + F(a)$, this is true.

Thus, the basis steps are satisfied for $b = 1$ and $b = 2$.
Step 2: Inductive Step
We assume the property $P(a, b)$ holds for some $b \geq 1$, i.e.,

$$F(a + b) = F(a + 1) \cdot F(b) + F(a) \cdot F(b - 1),$$

and that $P(a, b - 1)$ also holds:

$$F(a + b - 1) = F(a + 1) \cdot F(b - 1) + F(a) \cdot F(b - 2).$$

We need to prove $P(a, b + 1)$, i.e.,

$$F(a + b + 1) = F(a + 1) \cdot F(b + 1) + F(a) \cdot F(b).$$

1. **Expand $F(a + b + 1)$:** Using the Fibonacci recurrence $F(n + 1) = F(n) + F(n - 1)$, we have:

$$F(a + b + 1) = F(a + b) + F(a + b - 1).$$

2. **Substitute the Inductive Hypotheses:** Using the inductive hypotheses for $F(a + b)$ and $F(a + b - 1)$, substitute:

$$F(a + b) = F(a + 1) \cdot F(b) + F(a) \cdot F(b - 1),$$
$$F(a + b - 1) = F(a + 1) \cdot F(b - 1) + F(a) \cdot F(b - 2).$$

3. **Combine Terms:** Substitute these into $F(a + b + 1)$:

$$F(a + b + 1) = \big(F(a + 1) \cdot F(b) + F(a) \cdot F(b - 1)\big) + \big(F(a + 1) \cdot F(b - 1) + F(a) \cdot F(b - 2)\big).$$

   Group terms involving $F(a + 1)$ and $F(a)$:

$$F(a + b + 1) = F(a + 1) \cdot \big(F(b) + F(b - 1)\big) + F(a) \cdot \big(F(b - 1) + F(b - 2)\big).$$

4. **Simplify Using the Fibonacci Recurrence:** Using $F(b+1) = F(b) + F(b-1)$ and $F(b) = F(b-1) + F(b-2)$, we simplify:

$$F(a+b+1) = F(a+1) \cdot F(b+1) + F(a) \cdot F(b).$$

Thus, $P(a, b+1)$ holds, completing the induction step.
Step 3: Conclusion
By the principle of mathematical induction, the property:

$$F(a+b) = F(a+1) \cdot F(b) + F(a) \cdot F(b-1)$$

holds for all $a \geq 0$ and $b \geq 1$.

7.1.8 Recursive Defintion of a set S

1. **base clause** Specify that certain elements, called founders, are in S:

   if c is a founder, c∈S

2. Specify certain functions, called constructors, under which the set S is closed:

   if f is a constructor and $x \in S$, f(x) ∈ S

3. Membership for S can always be demonstrated by finitely many successive applications of the clauses above.

Note that if new elements are introduced such that they are unique, the set will be **countably infinite**. It would be uncountably infinite if the base step had an uncountable base case (real numbers), or some uncountable generation in the step.

7.1.9 Structural Induction of S (not sure if tested!)

To prove that $\forall x \in S$ P(x) is true, where P(x) is a proposition, it suffices to:

1. **basis step** Show that P(c) is true for every founder c,
2. show that $\forall x \in S$ (P(x) ⇒ P(f(x))) is true for every constructor f.

7.2 Lessons Learnt

TODO

8 Cardinality

8.1 Definitions

8.1.1 Pigeonhole Principle

Let A and B be finite sets. If there is an injection f:A→B, then $| A | \leq | B |$

8.1.2 Dual Pigeonhole Principle

If there is a surjection f:A→B, then $| A | \geq | B |$

8.1.3 Finite Sets

Let $\mathbb{Z}_n$ = {1,2,3,...,n}
A set S is said to be **finite** if there exists a bijection from S to $\mathbb{Z}_n$ for some n$\in \mathbb{Z}^+$

Cardinality of Finite Sets

1. 0 if S = $\emptyset$
2. n if f:S$\rightarrow \mathbb{Z}_n$ is a bijection

$| A |=| B |$ iff there is a bijection f:A$\rightarrow$B *Theorum Cardinality of Finite Sets*
Subset of a finite set is finite *Theorum Cadinality.1: Subset of a Finite Set*

Properties of Cardinality *Theorum 7.4.1*

1. Reflexive: $| A |=| A |$
2. Symmetric: $| A |=| B | \rightarrow | B |=| A |$
3. Transitive: $(| A |=| B |) \wedge (| B |=| C |) \rightarrow | A |=| C |$

8.1.4 WTF

An infinite set can have the same cardinality as a proper subset of itself. That is,
$| 2\mathbb{Z} | = | \mathbb{Z} |$

8.1.5 Countably Infinite

IS defined as a set having the same cardinality as $\mathbb{Z}^+$

If a set is countably infinite, then $| S | = \aleph_0$
A set is said to be countable iff it is finite or countably finite. Otherwise, it is uncountable

Showing countable by establishing a bijection
Given the following sets:

$$A = \{(a_0, a_1, a_2, \dots) : \forall i \in \mathbb{N},\ a_i \in \{0, 1\}\},$$
$$B = \{(a_0, a_1, a_2, \dots) \in A : \exists k \in \mathbb{Z}^+,\ \forall n \geq k,\ a_n = 0\}.$$

Prove or disprove: B is countable.
(Hint: Recall that for each positive integer n, there exists a unique binary representation given by

$$n = \sum_{i=0}^{m} a_i \cdot 2^i,$$

for some non-negative integer m and $(m+1)$-tuple $(a_0, a_1, \dots, a_m) \in \{0, 1\}^{m+1}$ such that $a_m = 1$.)
We prove that B is countable by constructing a bijection f between the set $\mathbb{N}$ (natural numbers) and the set B.
Let:

$$f : \mathbb{N} \rightarrow B$$
$$f(n) = (a_0, a_1, a_2, \dots),$$

where:

$$a_i = \begin{cases} 1, & \text{if the } i\text{-th bit of the binary representation of } n \text{ is } 1, \\ 0, & \text{otherwise.} \end{cases}$$

The function $f(n)$ converts a natural number n into a binary sequence in B by interpreting its binary representation as a sequence. Since every $n \in \mathbb{N}$ has a unique binary representation, f is injective. Moreover, every sequence in B corresponds to a finite binary representation, so f is surjective as well.

Examples:

$$\begin{aligned} f(0) &= (0,0,0,0,\dots) && \text{(binary 0)},\\ f(1) &= (1,0,0,0,\dots) && \text{(binary 1)},\\ f(3) &= (1,1,0,0,\dots) && \text{(binary 11)},\\ f(5) &= (1,0,1,0,0,\dots) && \text{(binary 101)}. \end{aligned}$$

The function f is a bijection, and therefore B is countable.

8.1.6 Cartesian Products and infinity

If sets A and B are both countably infinite, then so is $A \times B$
Since $\mid A \mid = \mid B \mid = \aleph_0$, the cardinality of their cartesian product is $\aleph_0 * \aleph_0 = \aleph_0$

8.1.7 Countability via Sequences

An infinite set B is countable iff there is a sequence $b_0, b_1, b_2, ..., \in B$ in which every element of B appears exactly once.

8.1.8 Uncountability via Diagonalization

To prove uncountability, use the following proof:

Cantor's Diagonalization Proof

1. Suppose something is countable
2. Since it is not finite, it is countably infinite
3. As such, we can list element x_i of the sequence: $a_{11}a_{12}a_{13}...a_{1n}..$
4. List elements out from x_1 to x_n and beyond.
5. Since our supposition is that it is countable, this set of sequences should contain all possible variations.
6. Construct a new sequence by taking elements of the diagonal
7. Transform the element at the diagonal somehow that it is not equal to the diagonal of the index
8. If this is possible, then you have created a new sequence that is not in the list. Theoretically you could do this infinite times to keep producing new elements
9. But then, the supposition that it is countable is false! It is thus uncountable.

8.2 Lessons Learnt

8.2.1 Countability of Power set

Cantor's theorum (find) states that the power set of any countably infinite set is uncountable.

8.2.2 Countable union is countable

A countable union of countably infinite sets are countable.

Determining whether sets are uncountable or not
Say you have a polynomial with random rational coefficients.

A polynomial is a finite set of Xs, and rational numbers are countably infinite. So you can think of it as unioning two countable sets $\{x_1x_2...x_n\}$ and $\{q_1q_2...q_n\}$. As the union of countable sets is countable, this is **countable**

So, always think about the bounds (whether they're finite) and objects (whether they're countable) you're dealing with.

Countability cheat sheet

Set	Countability
$\mathbb{N}$ (Natural Numbers)	Countable
$\mathbb{Z}$ (Integers)	Countable
$\mathbb{Q}$ (Rational Numbers)	Countable
$\mathbb{R}$ (Real Numbers)	**Uncountable**
Σ^* (Strings over a finite alphabet)	Countable
$\{0,1\}^{\mathbb{N}}$ (Infinite binary sequences)	**Uncountable**
$P(Z)$ (Power set of countable)	**Uncountable**

8.3 Theorems

Any subset of any countable set is countable *Theorum 7.4.3*
Any set with an uncountable subset is uncountable *Theorum 7.4.4*
Every infinite set has a countably infinite subset *Theorum Proposition 9.3*
A and B are countably infinite sets. Then, $A \cup B$ is countable. *Theorum Lemma 9.4*

9 Counting and Probability

9.1 Definitions

9.1.1 Number of elements in a list

If m and n are integers and $m \leq n$, then there are *Theorum 9.1.1*

$$\text{n-m+1}$$

integers from m to n inclusive.

Counting advanced cool stuff How many 3 digit integers are divisible by 5?
100=5***20**, and 995=5***199**
Then, apply 199-20 + 1 = 180!

9.1.2 Multiplication/Product rule for probability trees

If an operation consists of k steps, and the first step can be performed n_1 ways while the second n_2, k^{th} n_k, then the entire operation can be performed in:

$$n_1 \times n_2 \times ... \times n_k \text{ ways.}$$

9.1.3 Permutations

A permutation is an ordering of distinguishable objects in a row. The amount of permutations is given n!

Permutations of a set of n elements over r "slots" is given: P(n, r) = $\frac{n!}{(n-r)!}$

Circular Permutations simply (n-1)!

Permutations with repeated items If the object is not a set, like a string, then permutations of object is given:

$$\frac{n!}{r_1!r_2!...r_k!}$$

Where r_x is the amount of repeats for that particular symbol.

9.1.4 Counting choices

If you have n objects, and each object can have m states, the combination is give:

$$m^n$$

So, if you have 4 objects and each object can have state A or state B, $4^2 = 16$

9.1.5 Counting elements of disjoint sets

Addition Rule
Pretty obvious but if A equals the union of k distinct mutually disjoint sets $A_1, A_2, ..., A_k$, then:

$$| A | = \sum_1^k | A_i |$$

Difference Rule
If A is a finite set and $B \subseteq A$, then:
$| A \backslash B | = | A | - | B |$

9.1.6 Probability of Complement of Event

The probability of the complement of an event is obtained by:

$$P(\bar{A}) = 1 - P(A)$$

9.1.7 Inclusion/Exclusion rule

If elements in A and B overlap, their union is given: *Theorum 9.3.3.*

$$| A \cup B | = | A | + | B | - | A \cap B |$$

For 3 sets,

$$| A \cup B \cup C | = | A | + | B | + | C | - | A \cap B | - | A \cap C | - | B \cap C | + | A \cap B \cap C |$$

9.1.8 Pigeonhole Principle (PHP)

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.

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

Using general PHP
If there is a group of 85 objects (set X, n=85), and 26 "slots" (set Y, m=26), $85/26 \approx 3.27$.
Since K = 3.27, Generalized PHP tells us that there is some Y such that it is the image of K+1 = 4 elements of X.

9.1.10 Generalized Pigeonhole Principle (Contrapositive Form)

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

Using Contrapositive form PHP For the preivous example, we suppose that all y is at most the image of 3 $x \in X$ By generalized PHP, the total number of people is then 26*3 = 78. But this contradicts the fact that there are 85 people in all, so one hole must have at least 4 objects.

Another example: Suppose that set X has 42 objects, and set Y has 12 holes. Each hole has a maximum capacity of 6. Show that at least 5 holes have 3 or more objects.

Use contradiction: Suppose that only 4 or fewer holes are occupied by 3 or more holes. Then, 8 or more holes are occupied by 2 or fewer objects (invert the previous sentence)
Then, maximum amount of objects that can occupy 4 holes is: 4*6 = 24
Maximum amount of objects that can occupy 2 holes is: 2*8 = 16
This means that the total amount of holes that can be occupied is 24+16 which is 40, which is a contradition. Therefore supposition is false and original statement is true.

9.1.11 Combinations

A combination is finding out how many subsets (order doesn't matter) of size r you can choose from a set S of size n. Denoted:

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

Multi-step Combinations
Sometimes you can't compute everything at once. If you need to choose from a overall group subdivided into subgroups, divide into steps and choose from the subgroups.

9.1.12 Combinations with repetition allowed - Multisets

The number of r-combination with repetition allowed that can be selected from n elements is:

$$^{r+n-1}C_r$$

That is, if you have n categories/multisets and r elements the formula applies.

Multiset Let's say you have a set X = $\{x_1, x_2, ...x_n\}$. Then, you generate an r-combination with repetition. You obtain $[x_{i1}, x_{i2}, ..., x_{ir}]$ (square bracket notation) where some values may equal to each other - their assignment is the same

9.1.13 Pascal's Formula

Let n and r be positive integers, with $r \leq n$. Then

$$^{n+1}C_r = {}^nC_{r-1} + {}^nC_r$$

9.1.14 Binomial Theorem

$$(a+b)^n = \sum_{k=0}^{n} {}^nC_k * a^{n-k}b^k = a^n + {}^n C_1 a^{n-1}b^1 + {}^n C_2 a^{n-2}b^2 + ... + {}^n C_{n-1} a^1 b^{n-1} + b^n$$

nCk is called the binomial coefficient.
For example, if you want to count how many possible ways to put 6 objects in 6 holes:

$$\sum_{k=0}^{6} {}^6C_k(1*1) = (2)^6$$

We take a and b to be equal to 1, hence we get the value.

9.1.15 Probability Axioms

S is a sample space, and **P** is a probability function from the set of all events in S to real numbers. Let A and B be events in S.

1. 0 ≤P(A)≤ 1
2. P($\emptyset$) = 0, and P(S) = 1
3. If A and B are disjoint, then P(A∪B) = P(A) + P(B)
   (a) Generally, P(A∪B) = P(A) + P(B) - P(A∩B)
4. P($\bar{A}$) = 1 - P(A)

9.1.16 Probability summary table

Operation	**General Case**	**Disjoint**	**Independent**
$P(A \cup B)$	$P(A) + P(B) - P(A \cap B)$	$P(A) + P(B)$	$P(A) + P(B) - P(A)P(B)$
$P(A \cap B)$	$P(A \cap B)$	0	$P(A)P(B)$
$P(A \mid B)$	$\frac{P(A \cap B)}{P(B)}$	0	$P(A)$
$P(A \cap \bar{B})$	$P(A) - P(A \cap B)$	$P(A)$	$P(A)(1 - P(B))$
$P(A)$	$1 - P(A)$	$1 - P(A)$	$1 - P(A)$
$P(A \setminus B)$	$P(A) - P(A \cap B)$	$P(A)$	$P(A)(1 - P(B))$
$P(A \oplus B)$	$P(A) + P(B) - 2P(A \cap B)$	$P(A) + P(B)$	$P(A)(1 - P(B)) + P(B)(1 - P(A))$
Total Probability	$P(A) = \sum_i P(A \cap B_i)$	$P(A) = \sum_i P(A \cap B_i)$	$P(A) = P(A)$
Bayes' Theorem	$P(A \mid B) = \frac{P(B \mid A)P(A)}{P(B)}$	$P(A \mid B) = 0$	$P(A \mid B) = P(A)$

9.1.17 Expected Values

To say that on average a person will lose money on the lottery is to say that the expected value of playing the lottery is negative.
If the outcomes of some experiment are random and have probabilities p_x associated to outcomes a_x, then:

$$\text{Expected Value} = \sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + ... + a_n p_n$$

9.1.18 Linearity of Expectation

The expected value of the sum of random variables is equal to the sum of their individual expected values, regardless of whether they are independent

$$\mathrm{E[X + Y]} = \mathrm{E[X]} + \mathrm{E[Y]}$$

9.1.19 Conditional Probability

Let A and B be events in a sample space S. The conditional probability of B **given** A is: *Theorum 9.9.1*

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

We can rearrange this in any way:

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

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

9.1.20 General Bayes Theorem

$\mathrm{P(A|B)} = \frac{P(B|A) * P(A)}{P(B)}$
It is equivalent to: $\frac{P(A \cap B)}{P(B)}$, which makes sense if ya think about it.

9.1.21 Bayes Theorem

Suppose that a sample space S is a union of mutually disjoint events $B_1, B_2, B_3, ..., B_n$
Suppose A is an event in S, and suppose A and all B_i have non-zero probabilities. Then:

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

This tells us the likelihood that B_k "came from" A.

9.1.22 Independent Events

If A and B are events in a sample space S, then A and B are **independent**, iff:

$$\mathrm{P(A \cap B)} = \mathrm{P(A)} \cdot \mathrm{P(B)}$$

9.1.23 Mutually Independent Events

If A, B and C are mutually independent events, then:

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

These events are mutually independent iff the probability of the intersection of any subset of events is the product of the probabilities of the events in the subset.

10 Graphs

10.1 Definitions

10.1.1 Undirected Graphs

An undirected graph is denoted by G = (V, E), where:

1. V = $\{v_1, v_2, ..., v_n\}$ is the **nonempty** set of vertices (nodes) in G
2. E = $\{e_1, e_2, ..., e_n\}$ is the set of the undirected edges in G.
3. An undirected edge e connecting v_i and v_j is denoted as e = $\{v_i, v_j\}$
   (a) An edge is said to be **indident on** each of its endpoints
   (b) Two edges incident on the same endpoint are called **adjacent edges**
   (c) Vertices that are connected by an edge are called **adjacent vertices**
   (d) A vertex at the endpoint of a loop is said to be **adjacent to itself**

10.1.2 Directed Graphs

A directed graph consist of the same 2 sets as a normal undirected graph. The only difference is that the edge sets are now tuples - (v_i,v_j) is a directed edge pointing from v_i **to** v_j

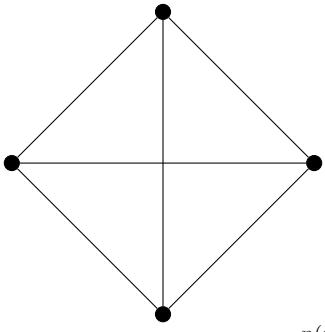
10.1.3 Simple Graphs

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

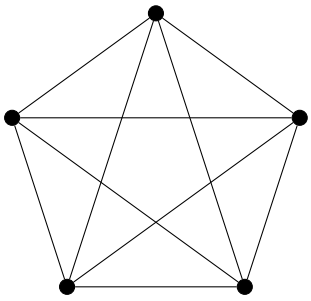
That is to say, there is at most one edge between each pair of distinct vertices.

10.1.4 Complete Graphs

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.



n=4

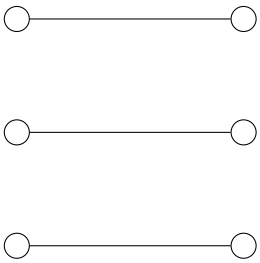


n=5

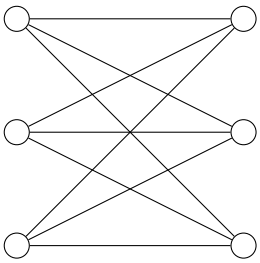
The amount of edges is given $\frac{n(n-1)}{2}$

10.1.5 Bipartite Graphs

A bipartite graph is a simple graph whose vertices can be divided into 2 disjoint sets U and v such that every edge connect a vertex in U to one in V. It is said to be **complete** if every vertex in U connects to every vertex in V.



Bipartite Graph



Complete Bipartite Graph
Denoted $K_{m,n}$ where m=$|U|$ and n = $|V|$

10.1.6 Subgraphs

G = (v_s,e_s), and H = (v, e)
G is said to be a **subgraph**of H iff $v_s \subseteq v$ and $e_s \subseteq e$

10.1.7 Degree of Vertex (Undirected)

The **degree** of a vertex v, deg(v), is the number of edges incident on v. Edge loops are counted twice.

10.1.8 Total Degree of an Undirected Graph

The **total degree** of an undirected graph is the sum of degrees of all its vertices.

10.1.9 The Handshake Theorem

G = (V, E)
deg(G) = $2 \times |E|$

Corollary 10.1.2 The total degree of the graph is even.

Proposition 10.1.3 There are always an even number of vertices that have odd degree.

10.1.10 Degree of Vertex (Directed)

Indegree
The indegree of a vertex v, $deg^-(v)$ is the number of directed edges **pointing towards** v.

Outdegree
The outdegree of v, $deg^+(v)$ is the number of edges pointing out **from** v.

Total Edges
$|E| = \sum deg^-(v) = \sum deg^+(v)$

10.1.11 Walks

A **walk** is a finite alternating sequence of adjacent vertices and edges of G.

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

Trivial Walks
A walk that is **trivial** is the walk from v to v consisting of only v.

v

10.1.12 Trails

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

10.1.13 Paths

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

10.1.14 Closed Walk

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

10.1.15 Circuit

A circuit is a closed walk of length ≥ 3 that does not contain a repeated edge.

10.1.16 Simple Circuit

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

10.1.17 Cyclic

An undirected graph is **cyclic** if it contains a loop.
If it doesn't, then it's **acyclic**

10.1.18 Connectedness

Two vertices v and w of a graph G are **connected** iff there is a walk from v to w.
The **graph** is connected iff given any two vertices v and w, there is a walk.

$$\forall v, w \in V, \exists \text{ a walk from v to w}$$

Number of edges and vertice in connected graph If G=(V,E) is a simple, undirected graph, that is connected, then $|E| \geq |V| - 1$ *Theorum Tutorial 11 Qn 4*

Minimum bound If G is a simple graph with n vertices and every vertex has degree at least floor($\frac{n}{2}$), G is connected

10.1.19 Circuit removal lemma

If vertices v and w are a part of a circuit in G and one edge is removed from the circuit, there exists still a trail from v to w in G.

10.1.20 Connectedness lemma

If G is connected, then any 2 distinct vertices of G can be connected by a path.

10.1.21 Circuit removal lemma 2

If G is connected and G contains a circuit, then an edge of the circuit can be removed and G will still be connected.

10.1.22 Connected Components

A graph H is a connected component of a graph G iff:

1. The graph H is a **subgraph** of G.
2. The graph H is connected
3. No other connected subgraph of G has H as a subgraph
4. (a) Essentially, H is the largest connected subgraph of G.

10.1.23 Euler Circuit

An euler circuit for G is a circuit that contains every vertex and traverses every edge of G exactly **once**
If a graph contains an Euler Circuit, it is an **Eulerian graph**

If a graph has an Euler circuit, then every vertex of the graph has a positive even degree. (note that its only one way) *Theorum 10.2.2*
Contrapositively, If some vertex of a graph has an odd degree, then the graph does not have an Euler circuit.

If G is connected and the degree of every vertex of G is a even integer, then G has an Euler circuit. *Theorum 10.2.3*

A graph G has an Euler circuit if and only if G is connected and every vertex of G has even degree. *Theorum 10.2.4*

10.1.24 Euler Trail

An Euler trail from v to w is a sequence of adjacent edges and verteices that starts at v, ends at w, passes thorugh every vertex of G at least once, and traverses every edge of G exactly once.
An Euler Circuit, but it doesn't start and end at the same place.

If G is connected, v and w have odd degree, and all other vertices of G have even degree, then there is a Euler trail from v to w. *Theorum Corollary 10.2.5*

10.1.25 Hamiltonian Circuit

A **Hamiltonian Circuit** for G is a simple circuit that includes every vertex of G.
If a graph has a Hamiltonian Circuit, then it is a Hamiltonian graph.

10.1.26 Checking for Hamiltonian Circuits

We can reliably show that a graph does not have a hamiltonian circuit:
If a graph G has a Hamilotnian 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.

10.1.27 Isomorphic Graphs

G = (V_G, E_G) and B = (V_B, E_B)
G is isomorphic to B, G ≅ B iff:

1. ∃ f: $V_G \to V_B$ s.t. bijective
2. ∃ h: $E_G \to E_B$ s.t. bijective

that preserve edge-endpoint functions of G.
That is to say, they are essentially the same graph but represented differently.

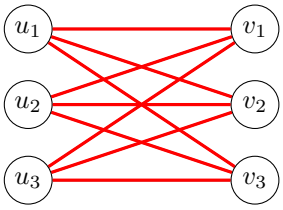
Equivalence Relation of Isomorphism
Graph isomorphism is an equivalence relation. Find out more what the fak this means.

10.1.28 Planar Graphs

A **planar graph** is a graph that can be drawn without edges crossing

10.1.29 Kuratowski's theorem

A finite graph is planar iff it does not contain a subgraph that is a subdivision of the complete graph K_5 or the complete bipartite graph $K_{3,3}$. *Theorum Kuratowski*



10.1.30 Euler's Formula

For a connected planar simple graph G = (V,E), the number of "faces" (regions) = |E| - |V| + 2 *Theorum Euler's Formula*

Euler's Formula for #edges in planar graph
Each face is bounded by at least 3 edges, and each edge shares exactly two faces in a planar graph:

$$3f \leq 2e \to f \leq \frac{2e}{3}$$

Now, from Euler's formula:

$$2 + e - v \leq \frac{2e}{3} \to e \leq 3v - 6$$

Thus, for a planar graph the number of edges must satisfy:

$$e \leq 3v - 6$$

For **bipartite planar graphs**, every face is bounded by at least 4 edges, which means:

$$e \leq 2v - 4$$

for planar bipartite graphs

Using #edges to determine planarity of Bipartite Graph
For a planar graph, we have that f + v - e = 2. For a *complete* $K_{m,n}$ graph, number of vertices is given v = m + n. The number of edges is given m*n.
Now if $K_{2,n}$ is planar, the maximum edges it can have must satisfy:

$$e \leq 2v - 4 \rightarrow 2n \leq 2(2+n) - 4 \rightarrow 2n \leq 2n$$

This holds true for any n, so $K_{2,n}$ is planar for any n.

Proof: Every planar graph has a vertex of degree 5 or less Our statement is that Planar $\rightarrow$ $deg(v) \leq 5$
We take the contrapositive, that $\forall v$ $deg(v) \geq 6 \rightarrow$ Non planar

1. Assume every vertex has a degree of at least 6. This means that there are at least 7 vertices in the graph.
2. By euler's formula, $e \leq 3v - 6$. This holds because v≥3
3. By handshake theorem, $\sum deg(v) = 2E$
4. By assumption, $\sum deg(v) \geq 6v$
5. 2E≥6v and thus $E \geq 3v$
6. However,by euler's formula, $e < 3v - 6$, which is less than $3n$.
7. As such, euler's formula cannot hold and this graph is nonplanar.
8. Therefore, the contrpositive is proven

For a graph with degree

10.1.31 Matrix Representation of Graphs

We can create an adjancency matrix of an undirected graph by +1'ing in the corresponding rows/cols if there exists edges between the graphs. This is **symmetric** for a undirected graph
Using this, we can see the number of walks that exist between two vectors.

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

Calculating walks Note that to calculate walks of length 4, you are taking A * A * A * A

11 Trees

11.1 Definitions

11.1.1 Tree

A simple graph is called **tree** if and only if it is circuit-free and connected.

Trivial
It is trivial if there is only vertex.

Forest
If it is not connected, then it is a forest.

Any non-trivial tree has at two vertices of degree 1 *Theorum Lemma 10.5.1*

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

If G is a connected graph with n vertices and n-1 edges, then G is a tree. *Theorum 10.5.4*

11.1.2 Terminal Vertex (leaf)

A vertex is a terminal vertex if its degree is **1**. It is the "end" of that branch of the tree.

11.1.3 Internal Vertex

A vertex is internal if its degree is ≥ 2.

11.1.4 Rooted Trees

A **rooted tree** is a tree in wihch there is one vertex that is distinguished from the others and is called the **root**.

Level
The level of a vertex is the number of edges along the unique path between it and the root

Height
The height of the rooted tree is the maximum level of any vertex.

Child
The children of a vertex v are all vertices **adjacent** to v and are 1 level down.

Parent
If w is a child of v, v is the parent of w.

Siblings
Distinct vertices with the same parent are siblings.

Ancestor, Descendent.
Given v & w, if v lies on the unique path between w and the root, v is the **ancestor** of w, and w a **descendent** of v.

11.2 Binary Trees

A **binary tree** is a rooted tree in which every parent has at most two children, left or right.

Full Binary Tree
A full binary tree is a binary tree in which each parent has exactly two children

A full binary tree with k internal vertices, has a total of 2k+1 vertices and has k+1 terminal vertices. *Theorum 10.6.1*

Left/Right subtree
Given any parent v, its left/right subtree is the binary tree whose root is the left/right child of v.
Its vertexes are the descendents of the child, along with the edges.

Height of Binary Trees
The height of a binary tree with t terminal vertices has a lower bound:

$$\log_2 t \leq \text{height}$$

11.2.1 Tree traversal (Depth-First Search)

There are 3 types of depth-first traversal:

1. Pre-Order

2. (a) Print data of vertex
   (b) Traverse left subtree by recursive call
   (c) Traverse right subtree by recursive call
3. In-order
4. (a) Traverse left subtree by recursive call
   (b) Print data of the vertex
   (c) Traverse right subtree by recursive call
5. Post-order
6. (a) Traverse left subtree by recursive call
   (b) Traverse right subtree by recursive call
   (c) Print data of vertex

11.2.2 Spanning Trees

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

1. Every connected graph has a spanning tree
2. Any 2 spanning tree for a graph have the same number of edges

11.2.3 Minimum Spanning Tree

An MST for a weighted graph is a spanning tree which has the least possible total weight compared to all other spanning trees for the graph.

Kruskal's Algorithm

1. Initialize T to have all vertices of G but no edges
2. For all edges in graph, sorted from least weight to most weight:
3. (a) Check if addition of edge into T introduces a circuit
   (b) If it does not, add edge to T.

Prim's Algorithm

1. Pick a vertex out of G and initialize T to include this vertex
2. For all edges incident to the graph T,
3. (a) Pick the least weight edge connecting T to a vertex out of T
   (b) Add the edge and vertex to T
   (c) Repeat

12 Other Theorems

12.1 Logical Equivalences[10]

Law	Conjunction (AND)	Disjunction (OR)
Commutative laws	$p \wedge q = q \wedge p$	$p \vee q = q \vee p$
Associative laws	$p \wedge q \wedge r \equiv (p \wedge q) \wedge r = p \wedge (q \wedge r)$	$p \vee q \vee r \equiv (p \vee q) \vee r = p \vee (q \vee r)$
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	$p \wedge \text{true} = p$	$p \vee \text{false} = p$
Negation laws	$p \wedge \sim p = \text{false}$	$p \vee \sim p = \text{true}$
Double negative law	$\sim (\sim p) = p$	
Idempotent laws	$p \wedge p = p$	$p \vee p = p$
Universal bound laws	$p \vee \text{true} = \text{true}$	$p \wedge \text{false} = \text{false}$
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	$\sim \text{true} \equiv \text{false}$	$\sim \text{false} \equiv \text{true}$

Advanced Logical Statements
Note that if there is a lot of fluff on screen, you can still apply basic laws.
e.g. $(p \wedge q \wedge s) \vee (!p \wedge q \wedge !r \wedge t) \vee q \vee (q \wedge r \wedge s \wedge !t)$
To do advanced logical statements, try to look for common elements, then apply basic rules.
If you localise the last term and let some random variable $z = r \wedge s \wedge \ ^{\sim}\text{t}$, then we can easily see the absorption law: $q \vee (q \wedge z)$. Be resourceful.
Additionally, think of counterexamples. Any situation in which it's possible for an implication to have a T $\rightarrow$ F value invalidates the logical statement.

12.2 Every integer is a rational number[11]

12.3 The sum of any two rational numbers is rational[12]

12.4 Positive Divisor of a Positive Integer[13]

For all positive integers a and b, if a | b, then a $\leq$ b

12.5 Divisors of 1[14]

The only divisors of 1 are 1 and -1.

12.6 Transitivity of Divisibility[15]

For all integers a,b, and c, if $a \mid b, b \mid c, \rightarrow a \mid c$

[10] 2.1.1 pg. 25
[11] 4.2.1 pg. 19
[12] 4.2.2 pg. 20
[13] 4.3.1 pg. 25
[14] 4.4.2 pg. 25
[15] 4.3.3 pg.27

12.7 There is no greatest integer[16]

12.8 Evenness of n^2 [17]

For all integers n, if n^2 is even, then n is even.

12.9 Oddness of n^2 [18]

If n is an integer, n^2 is odd $/iff$ n is odd.

12.10 Quotient-Remainder Theorum

Given any integer n and positive integer d, there exist unique integers q and r such that
$n = dq + r$ and $0 \leq r < d$

12.11 The product of any two odd integers is an odd integer [19]

13 Random Definitions

13.1 Congruence

Let $a, b \in \mathbb{Z}^+$. Then, a is **congruent** to b modulo n iff a-b = nk for some k $\in \mathbb{Z}$. In other words, n |(a-b).
Written as $a \equiv b(mod\ n)$
Congruence-mod n is an equivalence relation on $\mathbb{Z}$ for every n $\in \mathbb{Z}^+$

13.1.1 Congruence Modulo Quotient

Recall dividing by equivalence relation.
The quotient $\mathbb{Z}/\sim_{\mathbf{x}}$ where $\sim_{\mathbf{x}}$ is the congruence-modulo-**x** relation on Z, is denoted $Z_{\mathbf{x}}$
Essentially, it is all the partitions of congruence modulo on some integer x.

Addition and multiplication on the quotient [x] + [y] = [x+y] (the quotient of x + quotient of y is simply quotient of x+y; congruence modulo x+y)

[x] * [y] = [x*y]

13.2 Recurrence Relations

A **recurrence relation** of a sequence is aformula that relates each term to some predecessor(s). Fibonnaci Sequence is an example.

14 Methods of Proofing

14.1 Constructive Proof of Existential Statements

Given a statement

$$\exists x \in DQ(x)$$

We can prove it by using one of the constructive proofs of existence:

[16] 4.7.1 pg.29
[17] 4.6.4 pg.32
[18] Tutorial 1, Qn. 11
[19] Tutorial 1, Qn. 10

1. Find an x in D that makes Q(x) true
2. Give a set of directions for finding such an x

14.2 Vertex colouring

Is an assignment of colours to vertices that no two adjacent vertices have the same colour.

Four-colour conjecture You can accomplish a vertex colouring of any graph using 4 colours.

14.3 Disproving Universal statements by Counterexample

Given a universal conditional:

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

We can show that this statement is false by showing that its negation is true

$$\exists x \in D\ (P(x) \wedge\ \ ^{\sim}Q(x))$$

14.4 Proof by exhaustion

Given a universal conditional:

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

Showing that this statement is true for **all** of D shows that the statement is true.

14.5 Generalizing from the generic particular

Showing that every element of a set satisfies a certain property, suppose x is particular but arbitrarilychosen element of the set, and show that x satisfies the property.
e.g. If m and n are two particular but arbitrarily chosen integers, m = 2r and n = 2s. Using this, prove the wanted property.

14.6 Division into cases

If the proof has multiple cases, e.g. even and odd, we split the proof into cases and solve each one individually

14.6.1 Without Loss of Generality

WLOG are when the proof has multiple cases, but the proof of one case is exactly the same as the proof of the other case. As such, we can use WLOG to generalize the proof. [20]

14.7 Proof By Contradiction

1. Suppose that the statement to be proved, S, is false. So, $^{\sim}$S is true
2. Show that this supposition leads logically to a Contradiction
3. Conclude that the statement S is true.

There's no need to negate the premise!

Another example, suppose we know or have an intuition that a property is true. Let's say if $g \circ f$ is injective, then f is injective. If we want to proof that f is injective, we can assume that f is *not* injective. Then, do the proof as usual, and once there's a contradiction we know that the assumption is false.

[20] Assignment 1 Qn. 5

14.8 Proof by Contraposition

Recall that a contraposition is $\equiv$ the original statement. Proving a contraposition is true is equivalent to proving that the original statement is true.

1. Suppose the statement to be proved is $\forall x \in D \ (P(x) \rightarrow Q(x))$
2. Rewrite the statement into Contrapositive form:

$$\forall x \in D \ (\ {}^{\sim}Q(x) \rightarrow \ {}^{\sim}P(x))$$

3. Prove the contrapositive directly
4. Therefore, the original statement is true.