Discrete Maths Notes

September 28, 2023

Contents

1 Logic **3**

- 1.1 Propositional Logic . . . 3
  - 1.1.1 Basics . . . 3
  - 1.1.2 Terminology . . . 3
  - 1.1.3 Examples . . . 4
  - 1.1.4 Satifiability, Tautology, Contradiction . . . 4
- 1.2 Truth Tables . . . 5
  - 1.2.1 Basics . . . 5
  - 1.2.2 Connective Outputs . . . 5
  - 1.2.3 Examples . . . 6
  - 1.2.4 Taut/Sati/Contra Excersises . . . 6
- 1.3 Equivalence . . . 8
  - 1.3.1 Introduction to Equivalence . . . 8
  - 1.3.2 Equivalence Laws . . . 10
- 1.4 Arguments . . . 12
  - 1.4.1 Valid Arguments / Inference Rules . . . 13
  - 1.4.2 Proving a Valid Argument . . . 15
  - 1.4.3 The Deduction Method . . . 17
- 1.5 Predicate Logic . . . 18
  - 1.5.1 Predicate representation . . . 19
  - 1.5.2 Translating to Logical Expressions . . . 21
  - 1.5.3 Translation Examples . . . 24
  - 1.5.4 Negating Nested Quantifiers . . . 26
  - 1.5.5 Arguments In Predicate Logic . . . 27
  - 1.5.6 Chapter 1 Cheatsheet . . . 34

2 Proofs **36**

- 2.1 Proof Basics . . . 36
- 2.2 Proof Methods . . . 37
  - 2.2.1 Direct Proof . . . 37
  - 2.2.2 Proof by Contraposition . . . 38
  - 2.2.3 Proof by Contradiction . . . 39

2.2.4 Proof By Cases 41
2.3 Disproving a Statement & Proof Strategies 42
2.4 Proof by Induction 44
2.4.1 Examples 45
2.5 Strong Induction 46
2.5.1 Examples 46

1 Logic

1.1 Propositional Logic

1.1.1 Basics

A **proposition** is a statement that is either true or false.
Prepositions will be represented mathematically with capital letters A, B, C...
These prepositions are then are connected into more complex compound prepositions using *connectives*. Connectives are statements like "and, implies, if-then" and are represented mathematically with the symbols below.

It's not always easy to determine if they're true/false.

Connectives			
Symbol	Name	English Term(s)	Reading
$\wedge$	AND	And, But, Also	A and B
$\vee$	OR	-	A or B
$\implies$	IMPLICATION	If A, Then B If A, then B A implies B A, therefore B A only if B B follows from A A is a sufficient condition for B B is a necessary condition for A	A implies B
$\iff$	BICONDITIONAL	If & only if A is necessary and sufficient for B	A if and only if B
$\neg$	NEGATION	Not...	Not A

A Biconditional can also be thought of $(A \implies B) \wedge (B \implies A)$
Negation may sometimes be represented as $A\prime$ *or* $\overline{A}$

1.1.2 Terminology

$A \wedge B$ - conjunction of conjuncts A and B
$A \vee B$ - disjunction of disjuncts A and B
$A \implies B$ - A is the hypothesis$_{\text{/antecedent}}$ and B is the conclusion$_{\text{/consequence}}$

1.1.3 Examples

1 Compound Proposition

If all humans are mortal$_{\text{prp } A}$ and all Greeks are human$_{\text{prp } B}$
then all Greeks are mortal$_{\text{prp } C}$ can be represented as $A \wedge B \implies C$

2 Negation

Chocolate is sweet $\rightarrow$ Chocolate is not sweet

Peter is tall and thin $\rightarrow$ Peter is short or fat

Short and fat would be incorrect!

The river is shallow or polluted $\rightarrow$ The river is deep and polluted.

Not shallow or not polluted would be incorrect!

3 Implication: hypothesis and conclusion

If the rain continues then the river will flood

A sufficient condition for a network failure is that the central switch goes down

The avocados are ripe only if they are dark and soft

A good diet is a necessary condition for a healthy cat

1.1.4 Satifiability, Tautology, Contradiction

A proposition is satisfiable if it is true for *at least one* combination of boolean values.

You don't need a whole truth table for this, just look for one!

A Boolean Satisfiability Problem (SAT) is checking for satisfiability in a propositional logic formula.

A Tautology is a proposition that is always true
ex $A \vee \neg A$

A Contradiction is a proposition that is always false.
ex $A \wedge \neg A$

1.2 Truth Tables

1.2.1 Basics

Truth Tables are used for determining all the possible outputs of a complex compound propostion.

The Columns Are for the prepositions, intermediate compound prepositions and the whole compound preposition.

The intrmt' prepositions are optional steps to make solving easier, use as needed.

The Rows Are to contain the different sets of possible truth values for each proposition. You will have 2^p rows where p is the number of propositions (then +1 for the header).

The connectives in a compound propositional logic problem follow an order of precedence (the PEMDAS of logic) in the following order;
$\neg$, $\wedge$, $\vee$, $\implies$, $\iff$

1.2.2 Connective Outputs

Negation

A	$\neg A$
T	F
F	T

And

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

Or

A	B	$A \vee B$
T	T	T
T	F	T
F	T	T
F	F	F

Implication

A	B	$A \implies B$
T	T	T
T	F	F
F	T	T
F	F	T

An implication is true when the hypothesis is false or the conclusion is true.

Biconditional

A	B	$A \iff B$
T	T	T
T	F	F
F	T	F
F	F	T

A Biconditional is true when the two prepositions have the same value.

Out of all these outputs, the most unintuitive is the 3rd implication output ($F, T \implies T$). The easiest way to understand this output is with the proposition "If it is raining, then the ground is wet"; now say you step outside and it is not raining, but the ground is wet. The entire statement isn't false or incorrect, but the first part of it still has a false value.
The only way to make an implication false is when the hypothesis is true but the conclusion is false.

1.2.3 Examples

$A \implies B \iff B \implies A$

A	B	$A \implies B$	$B \implies A$	——
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

$A \wedge \neg B \implies \neg C$

A	B	C	$A \wedge \neg B$	——
T	T	T	F	T
T	T	F	F	T
T	F	T	T	F
T	F	F	T	T
F	T	T	F	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

ℹ *Remember, columns like $A \implies B$ are optional in-between steps to help solve each problem.*

1.2.4 Exercise: Finding Tautologies, Satisfiable & Contradicting Props'

Indicate whether each of the following is a tautology, satisfiable but not a tautology or a contradiction;

$A \implies B$

$A \implies A$

$A \implies \neg B \vee \neg C$

$A \vee B \implies B$

$(A \wedge B) \implies (A \vee B)$

$A \vee \neg A \implies B \wedge \neg B$

(Answers and explanations on the next page...)

Notice how none of these rely on drawing out a whole truth table! Focus on trying to find a way to get each proposition to output true and a way to get it to output false!

$A \implies B$
Satisfiable but not a tautology
Just knowing the properties of an implication you should know there's way to get true outputs and a false output.

$A \implies A$
Tautology
Only would be $T \implies T$ or $F \implies F$, both of which result in true.

$A \implies \neg B \vee \neg C$
Satisfiable but not a tautology
Instead of making a long unpleasant truth table, it's easiest to start by simply looking for one true and one false possible output.
We can make the left side true simply by making A false, since all that remains is an or statement we now have a true output.
We can just as easily find a false output for this proposition with $A = T$, $B = T(\neg B = F)$ to make the implication false, then we can just make $\neg C$ false to make the or output false.

$A \vee B \implies B$
Satisfiable but not a tautology
If we make B true then the biconditional will always be true regardless of A.
There is only one way to make an implication false, so if we can set up A and B to result in that false output, it won't be a tautology. If we make A true and B false it will make the implication false!

$(A \wedge B) \implies (A \vee B)$
Tautology
Remember the only way to make an implication false is if the hypothesis is true and the conclusion is false. There is absolutely no way to do this because of the and/or setup!

$A \vee \neg A \implies B \wedge \neg B$
Contradiction
The left side is always true and the right side is always false. So the result of the implication is always false!

1.3 Equivalence

1.3.1 Introduction to Equivalence

Two (compound) propositions P and Q are **logically equivalent** when their truth values always match (Meaning they'll have the same truth table!).
Equivalence is denoted by $P \equiv Q$.

Equivalence relates heavily to the concept of Tautologies;

P and Q are equivalent when $P \iff Q$ is a tautology.

A proposition P is a tautology iff (if and only if) it is equivalent to T (true), i.e $P \equiv T$

Examples

1

Given the implication $A \implies B$, are the following equivalent?

The contrapositive: $\neg B \implies \neg A$

The converse: $B \implies A$

A	B	$A \implies B$	$\neg B \implies \neg A$	$B \implies A$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	T	T

Looking at the table we can see that $A \implies B$ and $\neg B \implies \neg A$ are equivalent.

Now, what about $\neg A \vee B$?

A	B	$A \implies B$	$\neg A \vee B$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Yep! $\neg A \vee B \equiv A \implies B$.

This is actually one of the equivalence laws you'll see in the next section!

Understanding equivalent boolean expressions is very important in computer science (for code) and chip design (for logic gates). Consider the code below;

```
if(x > 0 || (x <= 0 && y > 100))
```

Lets see if we can change this expression to something equivalent but simplified.
Let A be `x > 0` and let B be `y > 100`
Now we can compare the truth values of $A \vee (\neg A \wedge B)$ and $A \vee B$.

A	B	$A \vee (\neg A \wedge B)$	$A \vee B$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

They're equivalent! We can reduce the if statement's expression to simply;

```
if(x > 0 || y > 100)
```

1.3.2 Equivalence Laws

For more complex propositions it is impractical to create a set of massive truth tables to check for equivalence. So instead we utilize equivalence laws to directly prove equivalence.

Nine Equivalence Laws;

Many of these are pretty self-explanatory

Double Negation Law: $\neg(\neg A) \equiv A$

Identity Laws: $A \wedge T \equiv A \qquad A \vee F \equiv A$

Domination Laws: $A \vee T \equiv T \qquad A \wedge F \equiv F$

Commutative Laws: $A \wedge B \equiv B \wedge A \qquad A \vee B \equiv B \vee A$

Associative Laws: $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C) \qquad (A \vee B) \vee C \equiv A \vee (B \vee C)$

Idempotent Laws: $A \wedge A \equiv A \qquad A \vee A \equiv A$

Distributive Laws: $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C) \qquad A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ Very similar to the algebriac distributive law

DeMorgan's Laws: $\neg(A \wedge B) \equiv \neg A \vee \neg B \qquad \neg(A \vee B) \equiv \neg A \wedge \neg B$

Implication Laws: $A \implies B \equiv \neg B \implies \neg A \equiv \neg A \vee B$

Examples

1 Prove $A \vee (\neg A \wedge B) \equiv A \vee B$

$$\begin{aligned} A \vee (\neg A \wedge B) &\equiv (A \vee \neg A) \wedge (A \vee B) && \text{(Distributive)} \\ &\equiv T \wedge (A \vee B) \\ &\equiv A \vee B && \text{(Identity)} \end{aligned}$$

In solving these, the goal should be to reduce the # of letters in the propositions. Focus on the side of an equivalence with more going on and try to reduce it down since the more complex proposition will have more oppurtunities to utilize the different equivalence laws.

2 Simplify $A \wedge \neg(A \wedge B)$

$$\begin{aligned} A \wedge \neg(A \wedge B) &\equiv A \wedge (\neg A \vee \neg B) && \text{(DeMorgan's)} \\ &\equiv (A \wedge \neg A) \vee (A \wedge \neg B) && \text{(Distributive)} \\ &\equiv F \vee (A \wedge \neg B) \\ &\equiv A \wedge \neg B && \text{(Identity)} \end{aligned}$$

You don't have to name the laws you're using in the homework, the simple $\equiv$ down the middle format for each step is fine.

3 Show that $(A \wedge B) \implies (A \vee B)$ is a tautology.

$$\begin{aligned} (A \wedge B) \implies (A \vee B) &\equiv \neg(A \wedge B) \vee (A \vee B) && \text{(Implication)} \\ &\equiv (\neg A \vee \neg B) \vee (A \vee B) && \text{(DeMorgan's)} \\ &\equiv \neg A \vee \neg B \vee A \vee B && \text{(Associative)} \\ &\equiv \neg A \vee A \vee \neg B \vee B && \text{(Commutative)} \\ &\equiv (\neg A \vee A) \vee (\neg B \vee B) && \text{(Associative)} \\ &\equiv T \vee T \\ &\equiv T && \text{(Idempotent)} \end{aligned}$$

1.4 Arguments

An **argument** is a sequence of propositions in which the conjunction of the initial propositions implies the final proposition
An argument can be represented as;
$P_1 \wedge P_2 \wedge P_3 ... \wedge P_n \implies Q$

Examples

If George Washington was the first president of the United States, then John Adams was the first vice president. George Washington was the first president of the United States. Therefore John Adams was the first vice president.

- Let A be “George Washington was the first president of the United States.”
- Let B be "John Adams was the first vice president.”
- $(A \implies B) \wedge A \implies B$

If Martina is the author of the book, then the book is fiction. But the book is nonfiction. Therefore Martina is not the author.

- Let A be “Martina is the author of the book.”
- Let B be “The book is fiction.”
- $(A \implies B) \wedge \neg B \implies \neg A$

The dog has a shiny coat and loves to bark. Consequently, the dog loves to bark.

- Let A be “The dog has a shiny coat.”
- Let B be “The dog loves to bark."
- $A \wedge B \implies B$

1.4.1 Valid Arguments / Inference Rules

An argument is **valid** if and only if **its conclusion is never false while its premises are true.**

We can't use a truth table to validate an argument since it only shows the truth values for the statement as a whole, instead we need to use new **Inference Rules**

Inference Rules

$$\begin{array}{l} P \\ P \implies Q \\ \hline \therefore Q \end{array} \qquad \begin{array}{l} P \implies Q \\ \neg Q \\ \hline \therefore \neg P \end{array}$$

Ex: If George Washington... Ex: If Martina...

$$\begin{array}{l} P \wedge Q \\ \hline \therefore P \end{array} \qquad \begin{array}{l} P \\ \hline \therefore P \vee Q \end{array}$$

$$\begin{array}{l} P \\ Q \\ \hline \therefore P \wedge Q \end{array}$$

Ex: Paul is a good swimmer. Paul is a good runner.

Therefore Paul is a good swimmer and a good runner

The items above the line can be combined/transformed into a new proof step defined below the line

Examples (finding conclusions)

1. If the car was involved in the hit-and-run, then the paint would be chipped. But the paint is not chipped.
   - "Car was involved in a hit-and-run" $\to P$
   - "Paint would be chipped" $\to Q$
   - "The paint is not chipped" $\to \neg Q$
   - Conclusion: The car was not involved in a hit-and-run. From the second rule!
2. If the bill was sent today, then you will be paid tomorrow. You will be paid tomorrow.
   - Nothing can be concluded from this. ☺
3. If the program is efficient$_P$, it executes quickly$_Q$. Either the program is efficient$_P$, or it has a bug$_R$. However, the program does not execute quickly$_{\neg Q}$.
   - "If the program is efficient" $\to P$
   - "it executes quickly" $\to Q$
   - "it has a bug" $\to R$
   - "the program does not execute quickly" $\to \neg Q$
   - We start by knowing $P \implies Q$ and $P \vee R$ and $\neg Q$...
   - $(P \implies Q)$ and $\neg Q$ can imply $\neg P$
   - We need to transform $P \vee R$ to use it: $P \vee R \equiv \neg(\neg P) \vee R \equiv \neg P \implies R$
   - $\neg P \implies R$ and $\neg P$ (the first implication we isolated) now implies R by the first inference rule.

1.4.2 Proving a Valid Argument

Assuming the premises are true, apply a sequence of premises and derivation rules, which include the equivalence laws and inference.

General Steps

1. Identify all the premises (might need some transformations).
2. Think backwards. Start from what you want and then seek supporting premises, current results, and necessary equivalence laws and inference rules, until you reach the given premises.

   ℹ Start with the RHS of the argument on the bottom of the list and work your way up
3. Write the proof sequence, where each step is either one premise or derived from previous step(s) using equivalence laws or inference rules.

Examples

1 Prove $(A \implies B) \wedge (\neg C \vee A) \wedge C \implies B$

> ℹ *This one is already in its standard form - so we just need to identify each part of the standard $P_1 \wedge P_2 \wedge P_3 ... \wedge P_n \implies Q$ form. At the end of this we want to prove that B is true.*

$(A \implies B)$	$\wedge$	$(\neg C \vee A)$	$\wedge$	C	$\implies B$
$\downarrow$	$\wedge$	Implication Law $C \implies A$	$\wedge$	C	$\downarrow$
$(A \implies B)$	$\wedge$	first inference rule law A			$\downarrow$
		also by first inf rule B			$\implies B$

> ℹ *This is not usually how you would format these proofs, this table was to give you an idea of the actual process. The actual proof would look like the following;*
>
> 1. $A \implies B$
> 2. $\neg C \vee A$
> 3. C
> 4. $C \implies A$ *(2, Implication)*
> 5. A *(3,4)*
> 6. B *(1,5)*
>
> *You need to put every step in a seperate (numbered) line, starting with each component of the argument and then the transformations you do with the reason given. You dont need to name the law used but you need to mention the steps you combined to acheive the next part.*

2 Prove $A \wedge (B \implies C) \wedge ((A \wedge B) \implies (D \vee \neg C)) \wedge B \implies D$

ℹ *For this one focus on step 3 ($D \vee \neg C$) as your point to figure out this argument since its the only portion that has D in it.*

1. A
2. $B \implies C$
3. $(A \wedge B) \implies (D \vee \neg C)$
4. B
5. $A \wedge B$ (1,4)
6. $D \vee \neg C$ (3,5)
7. $C \implies D$ (6, Commutative, Implication) - Communicative used to swap C, D
8. C (2,4)
9. D (7,8)

3 Prove $(A \implies B) \wedge (\neg C \vee A) \wedge C \implies A \wedge B$

ℹ *For this one notice that the right-hand side isn't a single letter anymore. We now need to focus on proving the whole $A \wedge B$ statement. So this problem is actually solved a bit backwards, start by writing the last steps ($A, B, A \wedge B$) and then go up and figure out how you can prove A.*

1.	$A \implies B$	
2.	$\neg C \vee A$	
3.	C	
4.	$C \implies A$	(2, Implication)
5.	A	(3,4)
6.	B	(1,5)
7.	$A \wedge B$	(5,6)

ℹ *If instead this problem was looking for $A \vee B$, you could just prove either A or B to make the entire statement valid.*

1.4.3 The Deduction Method

Now, what if the conclusion is in implication form?
There are two ways of solving for this form, the main one being **The Deduction Method...**

Suppose the argument has the form:

$$P_1 \wedge P_2 \wedge P_3 ... \wedge P_n \implies (R \implies S)$$

where the conclusion itself is an implication. <u>We can add R as an additional premise and then imply S</u>. In other words, we can have the argument:

$$P_1 \wedge P_2 \wedge P_3 ... \wedge P_n \wedge R \implies S$$

Examples

1 Prove $(A \implies B) \wedge (B \implies C) \implies (A \implies C)$

> ℹ *Start with C at the bottom. Now the only way to validate C is if B is true, so make B step 4 and find the proper relations to make B true.*

Deduction: $(A \implies B) \wedge (B \implies C) \wedge A \implies C$

1. $A \implies B$
2. $B \implies C$
3. A
4. B (1,3)
5. C (2,4)

2 Prove $\neg(A \wedge \neg B) \wedge (B \implies C) \implies (A \implies C)$
Deduction: $\neg(A \wedge \neg B) \wedge (B \implies C) \wedge A \implies C$

1. $\neg(A \wedge \neg B)$
2. $B \implies C$
3. A
4. $\neg A \vee B$ (1, DeMorgan's)
5. $A \implies B$ (4, Implication)
6. B (3,5)
7. C (2,6)

1.5 Predicate Logic

A **predicate** represents the properties of/relations among objects.
Examples:
n *is a perfect square*
x *is greater than* y

Often propositional logic is not enough!

There are several cases where propositional logic won't help us reach needed conclusions or information;

Suppose we know that "All CS students must take CSCI 358". We cannot conclude that "Alice must take CSCI 358 where Alice is a CS student" using our current propositional logic knowledge.

Statements that hold many objects must be enumerated;

- Example:
  - If Alice is a CS student, then Alice must take CSCI358.
  - If Bob is a CS student, then Bob must take CSCI358.
  - If Chris is a CS student, then Chris must take CSCI358.
  - ...
- Solution: make statements with variables
  - If x is a CS student, then x must take CSCI358.

Statements that define the property of a group of objects;

- Example:
  - All new cars must be registered.
  - Some of the new CS students graduate with honor.
- Solution: Make statements with quantifiers:
  - Universal Quantifier - the property is satisfied by all members of the group.
  - Existential Quantifier - at least one member of the group satisfies the property.

1.5.1 Predicate representation

Predicates are represented like functions in other branches of maths;
e.g $P(x)$ represents some predicate such as "x is a perfect square".

Once we plug in a value for x, the predicate becomes a proposition

Note that predicates can involve multiple variables, e.g Q(x,y) is "x is greater than y."

The two main quantifiers are represented with $\forall$ and $\exists$

- Universal Quantifier: $\forall$
  - Read as "for all," "for every," "for each," or "for any."
  - Ex: $\forall x, x > 0$ is read as "for any number x, x is greater than 0."
- Existential Quantifier: $\exists$
  - Read as "there exists one," "there is," "for at least one," or "for some."
  - Example: $\exists x, x > 0$ is read as "there exists a number x such that x is greater than zero."

When $\forall x P(x)$ or $\exists x P(x)$ is used, the domain must be specified.

Truth Values of Predicates

Predicate	True When...	False When...	Examples
$\forall x P(x)$	If P(x) is true for **every** x in the domain	If there is **any** x in the domain such that P(x) is false	$P(x)$ is $x+1>x$, $\forall P(x)$ is true for the domain consisting of all real numbers. $Q(x)$ is $x<2$. $\forall x Q(x)$ is false for the domain consisting of all real numbers because $Q(3)$ is false. $x=3$ is a counterexample of $\forall x Q(x)$
$\exists x P(x)$	There's is an x **anywhere** such that P(x) is true.	P(x) is false for **every** x	$P(x)$ is $x>3$. $\exists x P(x)$ is true for the domain consisting of all real numbers. Because when x=4, P(4) is true. $Q(x)$ is $X=x+1$. $existsxQ(x)$ is false for the domain consisting of all real numbers. Because $Q(x)$ is false for every real number x

The quantifiers $\forall$ and $\exists$ have higher precedence than all logical connectives from propositional logic.

For Example:

$$\forall x P(x) \wedge Q(x) \text{ means } (\forall x P(x)) \wedge Q(x) \text{ rather than } \forall x (P(x) \wedge Q(x))$$

Negating Quantified Expressions

$$\neg \forall x P(x) \equiv \exists x \neg P(x)$$

Example:

- Every CS Student Must take CSCI385.
- Negation: There is a CS student who doesn't have to take CSCI358

$$\neg \exists x P(x) \equiv \forall x \neg P(x)$$

Example:

- There is s student in this class who has taken CSCI 262.
- Negation: Every student in this class has **not** taken CS262

1.5.2 Translating to Logical Expressions

Converting statements to expressions

English to Logical Expressions

1 Every parrot is beautiful

Translation:

- Assume that the domain consists of all parrots.
  - Let $B(x)$ denote "x is beautiful"
  - Then $\forall x \ B(x)$
- Assume that the domain consists of all animals.
  - Let $P(x)$ denote "x is a parrot".
  - Let $B(x)$ denote "x is beautiful"
  - Then $\forall x \ (P(x) \implies B(x))$

$\forall x (P(x) \wedge B(x))$ would be incorrect

2 There exists a beautiful parrot

Translation:

- Assume that the domain consists of all parrots.
  - Let $B(x)$ denote "x is beautiful
  - Then $\exists x \ B(x)$
- Assume that the domain consists of all animals.
  - Let $P(x)$ denote "x is a parrot"
  - Let $B(x)$ denote "x is beautiful"
  - Then $\exists x \ (P(x) \wedge B(x))$

$\exists x \ (P(x) \implies B(x))$ is an incorrect solution. If x is not a parrot then P(x) is false, since P(x) is attached to the start of the implication it would make the entire expression true (when it should be false)

3 Let $P(x)$ denote "x speaks Russian"
and let $Q(x)$ denote "x knows the computer language C++"
Let the domain consist of all students at Mines.
Translate the following into logical expressions;

There is a student at Mines who speaks Russian and knows C++

- $\exists x \ (P(x) \wedge Q(x))$

There is a student at Mines who speaks Russian but doesn't know C++

- $\exists \ (P(x) \wedge \neg Q(x))$

Every student at Mines either speaks Russian or knows C++

- $\forall x \ (P(x) \vee Q(x))$

No student as Mines speaks Russian or knows C++

- $\forall x \ (\neg P(x) \wedge \neg Q(x))$
- or $\neg \exists x \ (P(x) \vee Q(x))$

Nested quantifiers

More than one quantifier may be needed to represent the meaning of a statemente in predicate logic.

1 Every real number has its corresponding negative

Assume that the domain consists of all real numbers

Let $P(x, y)$ denote "$x + y = 0$"

Then we can write $\forall x \ \exists y \ P(x, y)$

2 There is a person who loves everybody.

Assume that the domain consists of all people

Let $L(x, y)$ denote "x loves y".

Then we can write $\exists x \ \forall y \ L(x, y)$

Order of quantifiers

When quantifiers are of the **same** type, the order doesn't matter.

Example:

- Assume that the domain consists of all real numbers.
- Let $P(x, y)$ denote "$x + y = y + x$"
- $\forall x \; \forall y \; P(x, y)$ represents "For every real number x, for every real number y, x + y = y + x."
- $\forall y \; \forall x \; P(x, y)$ represents "For every real number y, for every real number x, x + y = y + x."
- $\forall x \; \forall y \; P(x, y)$ and $\forall y \; \forall x \; P(x, y)$ have the same meaning!

When quantifiers are of **different** types, the order does matter!

Example:

- Assume that the domain consists of all real numbers.
- Let $Q(x, y)$ denote "$x + y = 0$"
- $\forall x \; \exists y \; Q(x, y)$ represents "For every real number x, there is a real number y, such that x + y = 0."
- $\exists y \; forallx \; Q(x, y)$ represents "There is a real number y, such that for every real number x, x + y = 0."
- $\forall x \; \exists y \; Q(x, y)$ and $\exists y \; forallx \; Q(x, y)$ have different meanings!

Ex: Let $Q(x, y, z)$ be "$x + y = z$" and assume that the domain consists of all real numbers.

$$\forall x \; \forall y \; \exists z \; Q(x, y, z) \not\equiv \exists z \; \forall x \; \forall y \; Q(x, y, z)$$

1.5.3 Translation Examples

English to Logical Expression Examples

1 Given the two unique statements;

1. John loves only Mary (If John loves any person, then that person is Mary.)
2. Only John loves Mary (If any person loves Mary, then that person is John.)

Let $J(x)$ be "x is John". let M(x) be "x is Mary". Let L(x,y) be "x loves y". The domain consists of all people.

1. John loves only Mary.
   - For any person x, if x is John, then if it loves any person y, then y is Mary.
   - $\forall x\ (J(x) \implies \forall y(L(x, y) \implies M(y)))$
     Or $\forall x\ \forall y\ (J(x) \land L(x, y) \implies M(y))$
2. Only John loves Mary.
   - For any person x, if x is Mary, then if any person y loves x, then y is John.
   - $\forall x\ (M(x) \implies \forall(L(y, x) \implies J(y)))$
     Or $\forall x\ \forall y\ (M(x) \land L(y, x) \implies J(y))$

2 Given that; D(x) is "x is a dog". R(x) is "x is a rabbit". C(x,y) is "x chases y". The domain consists of all animals.
Translate the following;

1. All dogs chase rabbits.
   - For any animal, if it is a dog, then for any other animal, if that animal is a rabbit, then the dog chases it.
   - $\forall x\ (D(x) \implies \forall y(R(y) \implies C(x, y)))$
2. Some dogs chase all rabbits.
   - There is some animal that is a dog and, for any other thing, if that animal is a rabbit, then the dog chases it.
   - $\exists x\ \forall y(D(x) \land (R(y) \implies C(x, y)))$
3. Only dogs chase rabbits.
   - For any animals, if it is a rabbit then, if any animal chases it, that animal is a dog.
   - $\forall y\ (R(y) \implies \forall x(C(x, y) \implies D(x)))$
   - or: For any two animals, if one is a rabbit and the other chases it, then the other is a dog.
   - $\forall y\ \forall x\ (R(y) \land C(x, y) \implies D(x))$

Mathematical Statements to Logical Expression Examples

1 Translate "The sum of two positive integers is always positive."

Assume that the domain consists of all integers.

- For every two integers, if they are both positive, then the sum of them is positive.
- $\forall x\ \forall y\ (x > 0 \land y > 0 \implies (x + y > 0))$

Assume that the domain consists of all positive integers.

- For every two positive integers, the sum of them is positive.
- $\forall x\ \forall y\ (x + y > 0)$

2 Translate "The difference of two positive integers is not necessarily positive."

Assume that the domain consists of all integers.

- It is not the case that, for every two integers, if they are both positive, then the difference of them is positive.
- $\neg\forall x\ \forall y\ (x > 0 \land y > 0 \implies (x - y > 0))$
  Or: $\exists x\ \exists y((x > 0 \land y > 0) \land (x - y \leq 0))$

Logical Expressions to English Examples

1 Translate: $\forall x(C(x) \lor \exists y(C(y) \land F(x, y)))$, where $C(x)$ denotes "x has a computer," $F(x, y)$ denotes "x and y are friends," and the domain consists of all Mines students.

For every student x at Mines, x has a computer or there is a student y such that y has a computer and x and y are friends.

Simplifies to: Every student at Mines has a computer or a friend that has a computer.

2 Translate: $\exists x\ \forall y\ \forall z((F(x, y) \land F(x, z) \land (y \neq z)) \implies \neg F(y, z))$, where $F(x, y)$ denotes "x and y are friends," and the domain consists of all students at Mines.

$\exists x\ \forall y\ \forall z((F(x, y) \land F(x, z) \land (y \neq z)) \implies \neg F(y, z))$ means that if students x and y are friends, and students x and z are friends, and y and z are not the same student, then y and z are not friends.

There is a student x such that for every student y and every student z other than y, if x and y are friends, x and z are friends, then y and z are not friends.

There is a Mines student none of whose friends are friends.

1.5.4 Negating Nested Quantifiers

General Principle: Moving a $\neg$ across a quantifier changes the kind of quantifier.

What is the negation of $\forall x\ \exists y(xy = 1)$?

Let $P(x)$ denote $\exists y(xy = 1)$

Then we know how to negate $\forall x\ P(x)$

$\neg \forall x\ P(x) \equiv \exists x\ \neg P(x)$

In addition, $\neg P(x) \equiv \neg \exists y\ (xy = 1) \equiv \forall y\ (xy \neq 1)$

Therefore, the negation of $\forall x\ \exists y\ (xy = 1)$ is $\exists x\ \forall y(xy \neq 1)$

1.5.5 Arguments In Predicate Logic

Just like propositional logic, we need to utilize inference rules to prove these arguments.

Basic examples: (Assume the domain is all Mines CS students.)

1. All the CS students must take CSCI 358. Thus some CS students must take CSCI 358.
   - $\forall x\ P(x) \implies \exists x\ P(x)$ ✓
   - If every element has property P, then some element has property P
2. All the CS students must take CSCI 358. Thus Alice must take CSCI 358, where Alice is a CS student
   - $\forall x\ P(x) \implies P(a)$, where a is a constant ✓
   - If every element has property P, then a particular element has property P.
3. All the CS students must take CSCI 261 and CSCI 358. Thus all the CS students must take CSCI 261 and all the CS students must take CSCI 358.
   - $\forall x\ (P(x) \wedge Q(x)) \implies \forall x\ P(x) \wedge \forall x\ Q(x)$ ✓
   - If both P and Q are true for all the elements, then P is true for all elements and Q is true for all elements (duh)
4. Some CS students graduate with honors. Thus all the CS students graduate with honors.
   - $\exists x\ P(x) \implies \forall x\ P(x)$ ✖
   - If some element has property P, then all the elements have property P.

The $P(a)$ here represents a "constant" Alice whom is a particular element within the domain

This one also just doesn't make intuitive sense. Try rewriting arguments like this into English and see if they make sense!

All the equivalence laws and inference rules still hold!

- Double Negation Law: $\neg(\neg A) \equiv A$
- Identity Laws: $A \land T \equiv A$ $\quad A \lor F \equiv A$
- Domination Laws: $A \lor T \equiv T$ $\quad A \land F \equiv F$
- Commutative Laws: $A \land B \equiv B \land A$ $\quad A \lor B \equiv B \lor A$
- Associative Laws: $(A \land B) \land C \equiv A \land (B \land C)$ $\quad (A \lor B) \lor C \equiv A \lor (B \lor C)$
- Idempotent Laws: $A \land A \equiv A$ $\quad A \lor A \equiv A$
- Distributive Laws: $A \lor (B \land C) \equiv (A \lor B) \land (A \lor C)$
  $A \land (B \lor C) \equiv (A \land B) \lor (A \land C)$
- DeMorgan's Laws: $\neg (A \land B) \equiv \neg A \lor \neg B$
  $\neg (A \lor B) \equiv \neg A \land \neg B$
- Implication Laws: $A \rightarrow B \equiv \neg B \rightarrow \neg A \equiv \neg A \lor B$

- $P, P \rightarrow Q$ can imply Q
- $P \rightarrow Q, \neg Q$ can imply $\neg P$
- P, Q can imply $P \land Q$
- $P \land Q$ can imply P, Q
- P can imply $P \lor Q$

However, these rules are not enough, predicates will utilize four new inference rules;

Universal Instantiation

$\forall x\ P(x)$ can imply $P(c)$, where c is a particular element or any arbitrary element in the domain.

> If for any x in which $P(x)$ is true, then $P(c)$ must also be true. More intuitively thought as the fact that if all elements in the domain have property "P", then any element (particular or arbitrary within the domain) must also have this property.

Existential Instantiation

$\exists x\ P(x)$ can imply $P(a)$, where a is a particular element not previously used in a proof sequence

> $\exists x P(x)$ means there must be some element in the domain that has property "P". Even though we don't know *exactly* what that element is, we can use the letter "a" to represent this particular element.

Universal Generalization

$P(c)$ can imply $\forall x\ P(x)$, where c is an arbitrary element in the domain.

> If any/every arbitrary element in the domain has property P ($P(c)$ always true), we can obviously say $\forall x P(x)$

Existential Generalization

$P(a)$ can imply $\exists x\ P(x)$, where a is a particular element.

> If a particular element in the domain has property "P", we can obviously say $\exists x\ P(x)$

ℹ *The first two rules can be used to remove the quantifiers in front of the predicates. The last two rules can be used to add quantifiers to the front of predicates*

Let's look at all of these in more depth...

Universal Instantiation (UI)

$\forall x\ P(x)$ can imply $P(c)$, where c is a particular element or any arbitrary element in the domain.

Restrictions: If c is a variable, it cannot be already in $P(x)$

An **incorrect** use of UI would be saying $\forall x\ \exists y\ P(x, y)$ implies $\exists y\ P(y, y)$

For example, in the integer domain, if $P(x, y)$ means "$y > x$" then $\forall x\ \exists y\ P(x, y)$ is true, but $\exists y\ P(y, y)$ is false (y can't be greater than y ☺).

Example

Prove the following argument is valid: "All CS students must take CSCI358. Alice is a CS student. Therefore Alice must take CSCI 358." The domain consists of all Mines students.

Let $C(x)$ be "x is a CS student." s is a constant symbol. $D(x)$ is "x has to take CSCI358"

The argument would be: $\forall x(C(x) \implies D(x)) \wedge C(s) \implies D(s)$

1. $\forall x\ (C(x) \implies D(x))$
2. $C(s)$
3. $C(s) \implies D(s)$ (1,UI)
4. $D(s)$ (2,3)

Existential Instantiation (EI)

$\exists x\ P(x)$ can imply $P(a)$, where a is a particular element not previously used in a proof sequence

In English: If P is true for some element of the domain, we can give that element a specific notation.

Restrictions: a must not be used before!

Incorrect Uses of EI:

- $\exists\ P(x,a)$ CANNOT imply $P(a,a)$
  For example: in the integer domain, let P(x,y) denote $x > y$ and $a = 1$
- $\forall x\ \exists y\ Q(x,y)$ CANNOT imply $\forall x Q(x,a)$
  For example: in the integer domain, let $Q(x,y)$ denote that $x > y$.

Example: $\forall x\ (P(x) \implies Q(x)) \wedge \exists y\ P(y) \implies Q(a)$

1.	$\forall x\ (P(x) \implies Q(x))$	
2.	$\exists y\ P(y)$	
3.	$P(a)$	(2,EI)
4.	$P(a) \implies Q(a)$	(1,UI)
5	$Q(a)$	(3,4)

TODO: Update these incorrect use examples, what do these mean?

Universal Generalization (UG)

$P(c)$ can imply $\forall x\ P(x)$, where c is an arbitrary element in the domain.

In English: If $P(c)$ is true and c is arbitrary, then we can conclude $\forall x\ P(x)$

No weird restrictions or common misuses.

Example: $\forall x\ (P(x) \implies Q(x)) \land \forall x\ P(x) \implies \forall x\ Q(x)$

1.	$\forall x\ (P(x) \implies Q(x))$	
2.	$\forall x\ P(x)$	
3.	$P(c) \implies Q(c)$	(1,UI)
4.	$P(c)$	(2,UI)
5.	$Q(c)$	(3,4)
6.	$\forall x\ Q(x)$	(5,UG)

Existential Generalization (EG)

$P(a)$ can imply $\exists x\ P(x)$, where a is a particular element.

In English: Something has been named as having property P, so we can say that there exists something that has property P.

Restrictions: x must not appear in $P(a)$

Incorrect Uses of EG:

- $P(z, y)$ CANNOT imply $\exists y P(y, y)$
  For example: In the positive integer domain, let $P(x, y)$ mean that $y > x$, and a stands for 0, then $y > 0$ does not mean $y > y$

Example: $\forall x\ P(x) \implies \exists x\ P(x)$

1.	$\forall x\ P(x)$	
2.	$P(a)$	(1,UI)
3. $\exists x\ P(x)$	(2,EG)	

Proving a Valid Predicate Logic Argument (examples)

General Steps:

1. Strip off the quantifiers.
2. Work with the separate statements.
3. Insert quantifiers, as necessary.

---

1 $\forall x\ (P(x) \wedge Q(x)) \implies \forall x\ P(x) \wedge \forall x\ Q(x)$

1.	$\forall x\ (P(x) \wedge Q(x))$	
2.	$P(c) \wedge Q(c)$	(1,UI)
3.	$P(c)$	(2)
4.	$Q(c)$	(2)
5.	$\forall x\ P(x)$	(3,UG)
6.	$\forall x\ Q(x)$	(4,UG)
7.	$\forall x\ P(x) \wedge \forall x\ Q(x)$	(5,6)

You can use the same arbitrary element c for both P and Q

2 Prove the following argument is valid: "A student in this class has not attended any in-person classes. Everyone in this class passed the first exam. Therefore someone who passed the first exam has not attended any in-person classes."

Let C(x) be "x is in this class," B(x) be "x has attended in-person classes," and P(x) be "x passed the first exam." Let the domain consist of all Mines students.

$\exists x\ (C(x) \wedge \neg B(x)) \wedge \forall x\ (C(x) \implies P(x)) \implies \exists x\ (P(x) \wedge \neg B(x))$

Its easier to figure this one out in reverse, follow the proof from the bottom up as a process of what we need preceeded by what we use to get it!

1.	$\exists x\ (C(x) \wedge \neg B(x))$	
2.	$\forall x\ (C(x) \implies P(x))$	
3.	$C(a) \wedge \neg B(a)$	(1,EI)
4.	$C(a)$	(3)
5.	$C(a) \implies P(a)$	(2, UI)
6.	$P(a)$	(4,5)
7.	$\neg B(a)$	(3)
8.	$P(a) \wedge \neg B(a)$	(6,7)
9.	$\exists x(P(x) \wedge \neg B(x))$	(8,EG)

TODO: Add HW answers as examples later, HW had some weird situations that would be good to note.

1.5.6 Chapter 1 Cheatsheet

Connectives					
$\wedge$ AND	$\vee$ OR	$\implies$ IMPLIES	$\iff$ BICONDITIONAL	$\neg$ NEGATION	
A and B	A or B	If A then B	A if and only if B	Not A	
Both True	Either's True	$\star$	A = B	-	$\leftarrow$ true when

$\star$ - *An implication is only false when A is true and B is false.* *ref truth tables (1.2.2)*

Equivalence Laws	
Double Negation Laws	$\neg(\neg A) \equiv A$
Identity Laws	$A \wedge T \equiv A$ $A \vee F \equiv A$
Domination Laws	$A \vee T \equiv T$ $A \wedge F \equiv F$
Communicative Laws	$A \wedge B \equiv B \wedge A$ $A \vee B \equiv B \vee A$
Associative Laws	$(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ $(A \vee B) \vee C \equiv A \vee (B \vee C)$
Idempotent Laws	$A \wedge A \equiv A$ $A \vee A \equiv A$
Distributive Laws	$A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
DeMorgans Laws	$\neg(A \wedge B) \equiv \neg A \vee \neg B$ $\neg(A \vee B) \equiv \neg A \wedge \neg B$
Implication Laws	$A \implies B \equiv \neg B \implies \neg A$ $A \implies B \equiv \neg A \vee B$
Not a law, but helpful biconditional equivalence...	$A \iff B \equiv (A \implies B) \wedge (B \implies A)$

Inference Rules	
P $P \implies Q$ $\therefore Q$	Modus Ponens
$P \implies Q$ $\neg Q$ $\therefore \neg P$	Modus Tollens
$P \implies Q$ $Q \implies R$ $\therefore P \implies R$	Hypothetical Syllogism
$P \vee Q$ $\neg P$ $\therefore Q$	Disjunctive Syllogism
P Q $\therefore P \wedge Q$	Conjunction
$P \vee Q$ $\neg P \vee R$ $\therefore Q \vee R$	Resolution
P $\therefore P \vee Q$	Addition
$P \wedge Q$ $\therefore P$	Simplification you're basically "pulling" p out to its own line

Quantified Inference Rules

These names don't really matter for this class

TODO: Quantified Statement Inf Rules (ref saved screenshot) + other misc helpful stuff like negations of quantifiers. Just look up and copy-paste important details ☺

2 Proofs

2.1 Proof Basics

Some New Terminology

> A **theorem** is a proposition that can be shown to be true.

> A **lemma** is a preliminary proposition useful for proving later propositions.

> A **corollary** is a proposition that can be established directly from a theorem.

> A **conjecture** is a proposition that is being proposed to be a true statement.

> Propositions that are simply accepted as true are called **axioms.**

ex: For all real numbers x and y, x + y = y + x

ex: There is a straight-line segment between every pair of points.

> A **proof** is a valid argument that establishes the truth of a statement.
Can use axioms, premises (if any) and previously proved theorems.

Common Theorem Forms

T

ex: "$\sqrt{2}$ is not a rational number."

$\exists x T(x)$

ex: "There exists one integer n such that $n^2 + n + 41$ is composite"

* You would have to find an element a in the domain such that $T(a)$ is true and then apply Existential Generalization
* To disprove, prove that T(x) is false for all elements in the domain

$\forall x \ (P(x) \implies Q(x))$

ex: "For every integer n, if $3n + 2$ is odd, then n is odd."

* You would have to show that $P(c) \implies Q(c)$, where c is an arbitrary element of the domain, and then apply Universal Generalization
* Show that Q is true if P is true.
* To disprove, find a element e such that $P(e)$ is true, but $Q(e)$ is false.

$\forall x \ (P \iff Q)$

ℹ Proving $(P \iff Q)$ is equivalent to proving $(P \implies Q) \land (Q \implies P)$

2.2 Proof Methods

There are four main proof methods;

Direct Proof   Proof by Contraposition   Proof by Contradiction   Proof by Cases

---

2.2.1 Direct Proof

Directly show that if P is true, then Q must be true, using axioms, definitions, and previously proven theorems, together with inference rules.

Examples

1 Prove that "If n is odd, then n^2 is odd."

Proof:

Assume that n is odd, then $n = 2k + 1$, where k is some integer.

We have $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

n is odd when $n = 2(...) + 1$. We have to figure out how to transform n^2 into this form.

Therefore, n^2 is an odd integer.

2 Prove that "If m and n are both perfect squares, then mn is also a perfect square."

Proof:

Assume that m and n are both perfect squares, then $m = s^2$ and $n = t^2$, where s and t are some integers.

We have $mn = s^2t^2 = (st)^2$

Therefore, mn is a perfect square.

2.2.2 Proof by Contraposition

Instead of proving $P \implies Q$, prove $\neg Q \implies \neg P$.
We do this because we can then utilize the implication law:

$$P \implies Q \equiv \neg Q \implies \neg Q$$

Examples

1 Prove that "For any integer n, if n^2 is even, then n is even."
Proof:

Contraposition: "If n is odd, then n^2 is odd."

(Reference example 1 of the direct proof)

We have now proven this theorem.

2 Prove that "If $3n + 2$ is odd for an integer n, then n is odd."
Proof:

Contraposition: "If n is even, then 3n + 2 is even"

Assume that n is even, then $n = 2k$, where k is some integer.

We have $3n + 2 = 6k + 2 = 2(3k + 1)$

Therefore $3n + 2$ is even.

We have proved the theorem "If $3n + 2$ is odd then n is odd."

3 Prove that "If r is irrational, then $\sqrt{r}$ is also irrational"
Proof:

Contraposition: "if $\sqrt{r}$ is rational, then r is rational."

Assume that $\sqrt{r}$ is rational.

There exists integers p and q (no common factors), such that $\sqrt{r} = \frac{p}{q}$

Squaring both sides gives $r = \frac{p^2}{q^2}$

Since p^2 and q^2 are integers, r is also rational.

This proves the theorem.

2.2.3 Proof by Contradiction

Assume we want to prove S is true.
Now, suppose we can find a contradiction C such that $\neg S \implies C$ is true.
Since C is false, but $\neg S \implies C$ is true, then S must be true.

Examples

1 Prove that '$\sqrt{2}$ is not a rational number."

Proof:

Assume that $\sqrt{2}$ is a rational number.

Then $\sqrt{2} = \frac{p}{q}$ where p and q have no common factors and $2 = \frac{p^2}{q^2}$ or $2q^2 = p^2$

Since p^2 is even, p is even (See example 1 of Proof by Contraposition). This means that 2 is a factor of p: hence 4 is a factor of p^2, and the equation $2q^2 = p^2$ can be written as $2q^2 = 4x$ for some integer x.

We have q^2 is even and thus q is even (Same Proof by Contraposition Example)

Now 2 is a factor of q and a factor of p, which contradicts that statement that p and q have no common factors.

Hence, $\sqrt{2}$ is not rational.

Proof by Contradiction (cont.)

For prepositions of the implication form $(P \implies Q)$...
We instead prove $\neg(P \implies Q) \implies$ T or $(P \land \neg Q) \implies$ F
So, how do you find a contradiction?

- Imply Q. Then assert $Q \land \neg Q$ as a contradiction.
- Imply $\neg P$. Then assert $P \land \neg P$ as a contradiction.
- Imply $R \land \neg R$ during the proof for some proposition R.

Examples

1 Prove that "If $3n + 2$ is odd for an integer n, then n is odd."
Proof:

Assume to the contrary that $3n + 2$ is odd, and n is even.

Since n is even, $n = 2k$, where k is some integer.

We now have $3n + 2 = 6k + 2 = 2(3k + 1)$

Thus $3n + 2$ is even, which contradicts the assumption $3n + 2$ is odd.

Therefore, we have proved the theorem "If $3n + 2$ is odd, then n is odd.

2 Prove that "If a number added to itself gives itself, then the number is 0"
Proof:

Assume to the contrary that $x + x = x$ and $x \neq 0$

Then $2x = x$ and $x \neq 0$

Because $x \neq 0$, we can divide both sides of the equation by x and arrive at $2 = 1$, which is a contradiction.

Hence, $x + x = x \implies x = 0$

2.2.4 Proof By Cases

Assume that $P \equiv P_1 \lor P_2 \lor ... \lor P_n$.
Instead of proving $P \implies Q$, prove $(P_1 \implies Q) \land (P_2 \implies Q) \land ... \land (P_n \implies Q)$ We can do this because...

$$\begin{aligned} P_1 \lor P_2 \lor ... \lor P_n \implies Q &\equiv \neg(P_1 \lor P_2 \lor ... \lor P_n) \lor Q \\ &\equiv (\neg P_1 \land \neg P_2 \land ... \land \neg P_n) \lor Q \\ &\equiv (\neg P_1 \lor Q) \land (\neg P_2 \lor Q) \land ... \land (\neg P_n \lor Q) \\ &\equiv (P_1 \implies Q) \land (P_2 \implies Q) \land ... \land (P_n \implies Q) \end{aligned}$$

Examples

1 Prove that "If n is an even integer, $4 \leq n \leq 12$ then n is the sum of two prime numbers."
Proof:
We prove this for each value of n within the domain:

- $n = 4 = 2 + 2$
- $n = 6 = 3 + 3$
- $n = 8 = 3 + 5$
- $n = 10 = 5 + 5$
- $n = 12 = 5 + 7$

This completes the proof

2 Prove that "For any two numbers x and y, $\|x||y| = |xy|$."
Proof:
There are 4 cases:

1. $x \geq 0,\ y \geq 0$
   - $xy \geq 0$ and $|xy| = xy = |x||y|$
2. $x \geq 0,\ y < 0$
   - $xy \leq 0$ and $|xy| = -xy = x(-y) = |x||y|$
3. $x < 0,\ y \geq 0$
   - $xy \leq 0$ and $|xy| = -xy = (-x)y = |x||y|$
4. $x < 0,\ y < 0$
   - $xy > 0$ and $|xy| = (-x)(-y) = |x||y|$

Therefore, $|x||y| = |xy|$

2.3 Disproving a Statement & Proof Strategies

Disproving a Statement

Find a counterexample of the statement! For example, "Every positive integer is the sum of the squares of two positive integers"
Proof:
3 cannot be written as the sum of squares of two integers.

To show this, note that the only possible integers are 0 and 1. And it is not possible to write 3 by summing the squares of 0 and 1 (or just 1 twice).

What Makes a Good Proof?

- State your game plan.
- Keep a linear flow.*
- A proof is an essay, not a calculation!
- Avoid excessive symbolism.
- Revise and simplify.
- Introduce notation thoughtfully.
- Structure long proofs.
- Be wary of the "obvious"

One of the examples was showing 2k was even!

Proof Strategies

- Understand the definitions
- Analyze the meaning of the hypothesis and the conclusion
- Prove the statement using one of the proof methods.
- Use forward and backward reasoning.

Example: Incorrect Proofs

The examples below contain proofs with some sort of highlighted issue related to the strategies and pitfalls mentioned above.

1. "The sum of two even numbers is a multiple of 4."

- Proof:
  - Let x and y be even numbers.
  - Then x = 2k and y = 2k, where k is an integer.
  - So x + y = 2k + 2k = 4k, which is a multiple of 4.

x and y may not be equal.

2. "1/8 > 1/4."

- Proof:
  - 3 > 2
  - $3 \log_{10}(1/2) > 2 \log_{10}(1/2)$
  - $\log_{10}(1/2)^3 > \log_{10}(1/2)^2$
  - $(1/2)^3 > (1/2)^2$

The inequality symbol should be reversed when multiplying by a negative number.

3. "1¢ = \$1."

- Proof:
  - 1¢ = \$0.01 = (\$0.1)^2 = (10¢)^2 = \$1

\$ ≠ \$^{2}

2.4 Proof by Induction

If you can prove that you can get to $P(n+1)$ from $P(n)$ and also prove that just $P(1)$ is true you can prove $\forall n \ P(n)$ since you're starting at 1 being true and saying anything following it will also be true.

> ℹ *if* $P(1)$ *is true and* $\forall k \ (P(k) \implies P(k+1))$ *is true. Then we just follow* $P(1) \implies P(2)$, $P(2) \implies P(3)$ *and so on...*

<u>More specifically</u>;

Let P be a predicate on positive integers. If...

1. <u>Basis Step:</u> $P(1)$ is true.
2. <u>Inductive Step:</u> $\forall k \ (P(k) \implies P(k+1))$ is true.
   - You prove this by assuming P(k) is true for an arbitrary positive integer k and show that P(k+1) is true.

P(n) is true for all positive integers.

General Steps / Template

1. Translate into the form "For all $n \geq b, P(n)$" for a fixed integer b.
2. Write out the words "Basis step." Then show that $P(b)$ is true.
   - This is often just a basic sub-in and proving equality.
3. Write out the words "Inductive step."
   (a) State and clearly identify the inductive hypothesis, in the form "Assume that $P(k)$ is true for an arbitrary (fixed) integer $k \geq b$."
   (b) State what needs to be proved under the assumption that the inductive hypothesis is true, i.e., write out what $P(k+1)$ says.
   (c) Prove $P(k+1)$ to be true using the assumption P(k) is true.
4. Finally, state the conclusion.

2.4.1 Examples

Note: there's a ton of additional practice problems on the 9/19 slides if needed.

1 Prove: $1 + 2 + 3 + ... + n = \frac{n(n+1)}{2}$ for any positive integer n.

Let $f(n)$ denote "$1 + 2 + 3 + ... + n$

Basis Step $(n = 1)$: $1 = 1(1 + 1)/2$ ✓

Inductive Step:

- Assume that for any arbitrary positive integer k, $f(k) = \frac{k(k+1)}{2}$
- We need to show $f(k + 1) = \frac{(k+1)(k+2)}{2}$ $\leftarrow$ *here we're plugging in $k + 1$ in for k*
- $f(k+1) = 1+2+3+...+k+(k+1) = f(k)+k(k+1) = \frac{k(k+1)}{2}+(k+1) = \frac{(k+1)(k+2)}{2}$
- Thus, the statement is true for $k + 1$ as well.

2 Prove $n^2 > 3n$ for $n \geq 4$ for any positive integer n.

Basis step $(n = 4)$: we have $4^2 > 3 * 4$ ✓

Inductive Step:

- Assume that for any arbitrary positive integer $k \geq 4$, $k^2 > 3k$
- We need to show that $(k + 1)^2 > 3(k + 1)$
- $(k + 1)^2 = k^2 + 2k + 1$
  $> 3k + 2k + 1$ (by the inductive hypothesis)
  $\geq 3k + 8 + 1$ $(k \geq 4)$
  $> 3k + 3$
  $= 3(3 + 1)$ $\leftarrow$ remember this is what we were trying to reduce the RHS to prove $(k + 1)^2 > 3(k + 1)$

this completes the proof

3 Prove $7^n - 2^n$ is divisible by 5 for <u>any positive integer n</u>

Basis Step: $(n = 1)$: we have $7 - 2 = 5$, which is divisible by 5.

We need to show that $7^{k+1} - 2^{k+1}$ is divisible by 5

Induction Step:

- Assume that for any arbitrary positive integer k, $7^k - 2^k$ is divisible by 5.
- We need to show that $7^{k+1} - 2^{k+1}$ is divisible by 5.

$$\begin{aligned} 7^{k+1} - 2^{k+1} &= 7 * 7^k - 2 * 2^k \\ &= 7 * 7^k - 7 * 2^k + 5 * 2^k \\ &= 7 * (7^k - 2^k) + 5 * 2^k \end{aligned}$$

By the inductive hypothesis, $7 * (7^k - 2^k)$ is divisible by 5,
thus $7^{k+1} - 2^{k+1}$ is divisible by 5.

this completes the proof

2.5 Strong Induction

Let P be a predicate on positive integers. If...

1. $P(1)$ is true.

   ℹ This doesn't necessarily mean integer positive 1. This is wherever the set begins.

2. $\forall k(P(1) \wedge P(2) \wedge P(3) \wedge ... \wedge P(k) \implies P(k+1))$

Then $P(n)$ is true for all positive integers.

This method has more assumptions that can be utilized for the proof as it's assuming a bunch of elements *up to* $P(k)$ are true.

The template is nearly identical to our proof by induction.

Induction vs Strong Induction

- Induction applies when information about "one position back" is enough for the inductive sterp.
- Strong induction applies when you cannot directly prove that $P(k+1)$ is true just because you know $P(k)$ is true.

ℹ *Technically, you could use either type for a proof (as their technically equivalent). However, each is significantly easier for different types of proofs.*

2.5.1 Examples

ℹ Theres also extra excercises for this on the 9/26 slides.

1 Prove: every integer $n > 1$ is prime or a product of primes.

Basis step ($n = 2$): 2 is prime.

Inductive step.

> Assume that for any integer $k \geq 2$, the statement is true for any integer r, where $2 \leq r \leq k$

> We need to show that $k+1$ is prime or a product of primes.

ℹwe can split it into two the separate conditions using proof by cases.

- If $k+1$ is prime, we're done.
- If $k+1$ isn't prime, then $k+1 = ab$, where $1 < a < k+1$ and $1 < b < k+1$, or equivalently $2 \leq a \leq k$, $2 \leq b \leq k$. Based on this assumption, a and b are either prime or the product of primes. Thus, $k+1 = ab$ is a product of primes.

This completes the proof

2 Prove any amount of postage greater than or equal to 8 cents can be built using only 3-cent and 5-cent stamps.

Basis Step ($n = 8$): $8 = 3 + 5$

Inductive Step

- Assume that given any positive integer $k \geq 8$, the statement is true for any integer r, where $8 \leq r \leq k$.
- Show that $k+1$ can be built using only 3-cent and 5-cent stamps.
  - Case 1: $(k + 1 = 9)$: 9
  - Case 2: $(k + 1 = 10)$: $10 = 5 + 5$
  - Case 3 $(k+1 \geq 11)$: $k+1 = k-2+3$. Since $k-2 \geq 8$, $k-2$ can be written as the sum of 3's and 5's. Thus $k+1$ can be written as a sum of 3's and 5's.

This completes the proof.

Thats a lot of cases to go through in the induction steps! Let's do this example again but let's add more base cases in the basis step to avoid adding proof by cases within the inductive step.

2.1 Prove any amount of postage greater than or equal to 8 cents can be built using only 3-cent and 5-cent stamps.

Basis Step: $(n = 8, 9, 10)$: $8 = 3 + 5, 9 = 3 + 3 + 3, 10 = 5 + 5$

Inductive Step:

- Assume that given any positive integer $k \geq 10$, the statement is true for any integer r, where $8 \leq r \leq k$
- Show that $k+1$ can be built using only 3-cent and 5-cent stamps.
- $k+1 = k-2+3$. Since $k-2 \geq 8$, $k-2$ can be written as the sum of 3's and 5's.
- Thus, $k+1$ can be written as the sum of 3's and 5's.

this connects our inductive step to our basis step

This completes the proof.

TODO: add the tribonacci sequence exercise (its very different than the other examples covered)