Logic

Chapter 3

MATH 280 Discrete Mathematical Structures

Proposition

- A *proposition* is a sentence that is one of either *true* or *false*
  - A proposition is also known as a *statement*
- Possible propositions:
  - The wall is tan.
  - $5 < 10$
  - Tennessee is a state.
  - Animals live beneath the surface of Mars.
- Non-propositions:
  - The painting is beautiful.
  - When is Christmas?
  - He is tall. Who?
  - $x < 10$ $x = ?$
- We can use variables such as p, q, and r to represent propositions
  - p might represent "$5 < 10$"

Truth Tables

- We can construct compound propositions from simpler propositions using logical operators
- The common logical operators include to *and*, *or*, and *not*
- A *truth table* shows the possible range of true values for a compound proposition
  - 0 represents false
  - 1 represents true

p	q	$f(p,q)$
0	0	0
0	1	1
1	0	0
1	1	1

Conjunction

- Logical *and*

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

- The only way to obtain a 1 (true) is if both operands are true
- Mathematics: $a \wedge b$
  Digital logic: ab
  C++: `a && b`
  Python: `a and b`

Disjunction

- Logical *or*

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

- The only way to obtain a 0 (false) is if both operands are false
- Mathematics: $a \vee b$
  Digital logic: $a + b$
  C++: `a || b`
  Python: `a or b`

Negation

- Logical *not*

p	$\neg p$
0	1
1	0

- Negation is a unary operator and so requires only one operand
- Mathematics: $\neg a$ $\sim a$ a'
  Digital logic: $\overline{a}$
  C++: `!a`
  Python: `not a`

Conditional Operator

- Logical *if ... then*, or *implies*

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

- p is the antecedent, and q is consequent
- Example: If it is raining, the grass is wet
  - If it raining and the grass is wet, the statement is a true statement
  - If is raining but the grass is not wet, the statement is not true
  - If it is not raining and the grass is not wet, the statement cannot be false; it only makes a claim about when it is raining
  - The most interesting case: If it is not raining and the grass is wet, the statement cannot be false; it only makes a claim about when it is raining. If it is not raining, the grass could be wet for other reasons, such as a sprinkler system or dew.

Converse

- The converse of $p \to q$ is $q \to p$
- These two propositions are **not** logically equivalent
- Given the propositions r = "it is raining" and w = "the grass is wet", if the compound proposition $r \to w$ is true, we cannot conclude that its converse ($w \to r$) also is true.
  - The grass could be wet due to sprinklers
- A logical fallacy: *affirming the consequent*

Biconditional Operator

- if and only if (iff)

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

- Short for $(p \to q) \land (q \to p)$
- Represents logical equivalence

English Equivalents

$p \to q$	$p \leftrightarrow q$
if p, then q	p if and only if q
p implies q	p is necessary and sufficient for q
q follows from p	p is equivalent to q
q, if p	if p, then q, and if q, then p
p, only if q	if p, then q and conversely
p is sufficient for q	
q is necessary for p	

Compound Propositions

- If p and q are propositions (e.g., p = "The tree is tall", q = "The lake is deep")
  - $p \land q$ is a proposition "The tree is tall and the lake is deep."
  - $p \lor q$ is a proposition "The tree is tall or the lake is deep."
  - $\neg p$ is a proposition "The tree is not tall." (or "The tree is short.")
  - (p) is a proposition (use parentheses for grouping)
- This applies recursively: $(p \land q) \lor \neg p$ is a proposition
- Generally understood precedence rules: negation first, conjunction second, disjunction third
  - $p \land q \lor r$ is equivalent to $(p \land q) \lor r$
  - $\neg p \land q$ is equivalent to $(\neg p) \land q$
- What about $\to$ and $\leftrightarrow$?

Truth Table for Compound Proposition

- $\neg p \lor q$

p	q	$\neg p$		
0	0			
0	1			
1	0			
1	1			

Truth Table for Compound Proposition

- $\neg p \vee q$

p	q	$\neg p$		
0	0	1		
0	1	1		
1	0	0		
1	1	0		

Truth Table for Compound Proposition

- $\neg p \vee q$

p	q	$\neg p$	$\neg p \vee q$	
0	0	1		
0	1	1		
1	0	0		
1	1	0		

Truth Table for Compound Proposition

- $\neg p \vee q$

p	q	$\neg p$	$\neg p \vee q$	
0	0	1	1	
0	1	1	1	
1	0	0	0	
1	1	0	1	

Truth Table for Compound Proposition

- $\neg p \vee q$

p	q	$\neg p$	$\neg p \vee q$	$p \to q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

Truth Table for Compound Proposition

- $\neg p \vee q$

p	q	$\neg p$	$\neg p \vee q$	$p \to q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

The propositions $\neg p \vee q$ and $p \to q$ are equivalent

Truth Table for Compound Proposition

- Construct a truth table for $(p \wedge q) \vee (\neg q \wedge r)$

p	q	r	$p \wedge q$	$\neg q$	$\neg q \wedge r$	$(p \wedge q) \vee (\neg q \wedge r)$
0	0	0				
0	0	1				
0	1	0				
0	1	1				
1	0	0				
1	0	1				
1	1	0				
1	1	1				

Truth Table for Compound Proposition

- Construct a truth table for $(p \wedge q) \vee (\neg q \wedge r)$

p	q	r	$p \wedge q$	$\neg q$	$\neg q \wedge r$	$(p \wedge q) \vee (\neg q \wedge r)$
0	0	0	0			
0	0	1	0			
0	1	0	0			
0	1	1	0			
1	0	0	0			
1	0	1	0			
1	1	0	1			
1	1	1	1			

Truth Table for Compound Proposition

- Construct a truth table for $(p \wedge q) \vee (\neg q \wedge r)$

p	q	r	$p \wedge q$	$\neg q$	$\neg q \wedge r$	$(p \wedge q) \vee (\neg q \wedge r)$
0	0	0	0	1		
0	0	1	0	1		
0	1	0	0	0		
0	1	1	0	0		
1	0	0	0	1		
1	0	1	0	1		
1	1	0	1	0		
1	1	1	1	0		

Truth Table for Compound Proposition

- Construct a truth table for $(p \wedge q) \vee (\neg q \wedge r)$

p	q	r	$p \wedge q$	$\neg q$	$\neg q \wedge r$	$(p \wedge q) \vee (\neg q \wedge r)$
0	0	0	0	1	0	
0	0	1	0	1	1	
0	1	0	0	0	0	
0	1	1	0	0	0	
1	0	0	0	1	0	
1	0	1	0	1	1	
1	1	0	1	0	0	
1	1	1	1	0	0	

Truth Table for Compound Proposition

- Construct a truth table for $(p \wedge q) \vee (\neg q \wedge r)$

p	q	r	$p \wedge q$	$\neg q$	$\neg q \wedge r$	$(p \wedge q) \vee (\neg q \wedge r)$
0	0	0	0	1	0	0
0	0	1	0	1	1	1
0	1	0	0	0	0	0
0	1	1	0	0	0	0
1	0	0	0	1	0	0
1	0	1	0	1	1	1
1	1	0	1	0	0	1
1	1	1	1	0	0	1

Logial Equivalence

- Recall that $\neg p \vee q$ and $p \to q$ are equivalent propositions

p	q	$\neg p \vee q$	$p \to q$	$(\neg p \vee q) \leftrightarrow (p \to q)$
0	0	1	1	
0	1	1	1	
1	0	0	0	
1	1	1	1	

Logial Equivalence

- Recall that $\neg p \vee q$ and $p \to q$ are equivalent propositions

p	q	$\neg p \vee q$	$p \to q$	$(\neg p \vee q) \leftrightarrow (p \to q)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	1	1	1

Logial Equivalence

- Recall that $\neg p \vee q$ and $p \rightarrow q$ are equivalent propositions

p	q	$\neg p \vee q$	$p \rightarrow q$	$(\neg p \vee q) \leftrightarrow (p \rightarrow q)$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	1	1	1

- A proposition that always is true regardless of the truth values of its variables is called a *tautology*

  A column consisting of all 1s represents a tautology
- If $p \leftrightarrow q$ is a tautlogy, p and q are equivalent propositions
- $p \Leftrightarrow q$ indicates that p and q represent equivalent propositions (i.e., $p \leftrightarrow q$ is a tautology)

Negating a Conjunction

- $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$?
- p = "I am tall" q = "I am smart"
- $\neg(p \wedge q)$ represents "I am not both tall and smart"
- $\neg p \vee \neg q$ represents "I am not tall or I am not smart"
- The propositions will be true for some people and false for others, but both expressions will have the *same truth value* for the *same person*
- You can prove it with a truth table

Negating a Conjunction

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
0	0						
0	1						
1	0						
1	1						

Negating a Conjunction

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
0	0	0					
0	1	0					
1	0	0					
1	1	1					

Negating a Conjunction

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
0	0	0	1				
0	1	0	1				
1	0	0	1				
1	1	1	0				

Negating a Conjunction

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
0	0	0	1	1			
0	1	0	1	1			
1	0	0	1	0			
1	1	1	0	0			

Negating a Conjunction

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
0	0	0	1	1	1		
0	1	0	1	1	0		
1	0	0	1	0	1		
1	1	1	0	0	0		

Negating a Conjunction

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
0	0	0	1	1	1	1	
0	1	0	1	1	0	1	
1	0	0	1	0	1	1	
1	1	1	0	0	0	0	

Negating a Conjunction

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
0	0	0	1	1	1	1	1
0	1	0	1	1	0	1	1
1	0	0	1	0	1	1	1
1	1	1	0	0	0	0	1

Negating a Conjunction

p	q	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$	$\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$
0	0	0	1	1	1	1	1
0	1	0	1	1	0	1	1
1	0	0	1	0	1	1	1
1	1	1	0	0	0	0	1

- The tautology proves $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

Contradiction

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

p	q	$\neg p$	$\neg p \vee q$	$p \wedge (\neg p \vee q)$	$\neg q$	$p \wedge (\neg p \vee q) \wedge \neg q$
0	0					
0	1					
1	0					
1	1					

Contradiction

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

p	q	$\neg p$	$\neg p \vee q$	$p \wedge (\neg p \vee q)$	$\neg q$	$p \wedge (\neg p \vee q) \wedge \neg q$
0	0	1				
0	1	1				
1	0	0				
1	1	0				

Contradiction

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

p	q	$\neg p$	$\neg p \vee q$	$p \wedge (\neg p \vee q)$	$\neg q$	$p \wedge (\neg p \vee q) \wedge \neg q$
0	0	1	1			
0	1	1	1			
1	0	0	0			
1	1	0	1			

Contradiction

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

p	q	$\neg p$	$\neg p \vee q$	$p \wedge (\neg p \vee q)$	$\neg q$	$p \wedge (\neg p \vee q) \wedge \neg q$
0	0	1	1	0		
0	1	1	1	0		
1	0	0	0	0		
1	1	0	1	1		

Contradiction

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

p	q	$\neg p$	$\neg p \vee q$	$p \wedge (\neg p \vee q)$	$\neg q$	$p \wedge (\neg p \vee q) \wedge \neg q$
0	0	1	1	0	1	
0	1	1	1	0	0	
1	0	0	0	0	1	
1	1	0	1	1	0	

Contradiction

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

p	q	$\neg p$	$\neg p \vee q$	$p \wedge (\neg p \vee q)$	$\neg q$	$p \wedge (\neg p \vee q) \wedge \neg q$
0	0	1	1	0	1	0
0	1	1	1	0	0	0
1	0	0	0	0	1	0
1	1	0	1	1	0	0

- A column of all 0s represents a *contradiction*

Tautologies and Contradictions

- A proposition that is always true is a *tautology*
  - $p \vee \neg p$ is always true regardless of the truth value of p
  - We represent a tautology as 1
- A proposition that can never be true under any circumstances is a *contradiction*
  - $p \wedge \neg p$ is always false regardless of the truth value of p
  - We represent a contradiction as 0
- A proposition that can be either true of false is a *contingency*
  - $p \rightarrow q$ is false if p is true and q is false; otherwise, it is true

Truth Table Facts

- A truth table with two variables has how many rows? 4
- A truth table with three variables has how many rows? 8
- A truth table with four variables has how many rows? 16
- A truth table with n variables has how many rows? 2^n
- A truth table with 2 variables can have how many unique columns?

A Full Truth Table

p	q	0	$p \wedge q$	$\neg(p \to q)$	p	$\neg(q \to p)$	q	$p \oplus q$	$p \vee q$	$p \overline{\vee} q$	$p \leftrightarrow q$	$\neg q$	$q \to p$	$\neg p$	$p \to q$	$p \overline{\wedge} q$	1
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Fundamental Laws of Logic

Commutative	$p \wedge q \Leftrightarrow q \wedge p$ $p \vee q \Leftrightarrow q \vee p$
Associative	$p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$ $p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$
Distributive	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge 1 \Leftrightarrow p$ $p \vee 0 \Leftrightarrow p$
Negation	$p \wedge \neg p \Leftrightarrow 0$ $p \vee \neg p \Leftrightarrow 1$
Idempotence	$p \wedge p \Leftrightarrow p$ $p \vee p \Leftrightarrow p$
Null	$p \wedge 0 \Leftrightarrow 0$ $p \vee 1 \Leftrightarrow 1$
Absorption	$p \wedge (p \vee q) \Leftrightarrow p$ $p \vee (p \wedge q) \Leftrightarrow p$
DeMorgan's	$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$
Involution	$\neg(\neg p) \Leftrightarrow p$

Inference Rules

- If $r \to s$ is a tautology, we say $r \to s$ is an *inference rule*
- Your author uses the notation $r \Rightarrow s$ to denote an inference rule
- Note that unlike an equivalence ($a \Leftrightarrow b$), an inference rule ($a \Rightarrow b$) goes only one direction

Inference Rules

Detachment	$(p \to q) \wedge p \Rightarrow q$
Indirect reasoning	$(p \to q) \wedge \neg q \Rightarrow \neg p$
Disjunctive addition	$p \Rightarrow p \vee q$
Conjunction	$p, q \Rightarrow p \wedge q$
Conjunctive simplification	$p \wedge q \Rightarrow p$
Disjunctive simplification	$(p \vee q) \wedge \neg p \Rightarrow q$
Chain rule	$(p \to q) \wedge (q \to r) \Rightarrow p \to r$
Conditional equivalence	$p \to q \Leftrightarrow \neg p \vee q$
Biconditional equivalence	$p \leftrightarrow q \Leftrightarrow (p \to q) \wedge (q \to p)$
Contrapositive	$p \to q \Leftrightarrow \neg q \to \neg p$

Mathematical System

A *mathematical system* consists of

- a set or universe, U
- definitions—sentences that explain the meaning of concepts that relate to the universe
- axioms—assertions about the properties of the universe and rules for creating and justifying more assertions
- theorems—additional assertions derived from the axioms of the mathematical system

Propositional Calculus

- The logic we have covered so far is part of propositional calculus
- A theorem is a true proposition derived from the axioms of the system
- A theorem proved to be true is an extension of the axioms of the system
- Theorems are usually expressed as a finite number of premises (propositions) with a conclusion (a proposition)
  $p_1 \wedge p_2 \wedge p_3 \wedge \ldots \wedge p_n \Rightarrow C$

Proof

- Proof of a theorem: a finite sequence of logically valid steps that demonstrate that the premises of a theorem imply its conclusion
- The form of a proof can vary depending on its intended audience
- A proof in propositional calculus can be verified mechanically
- Truth tables are sufficient to prove theorems in propositional calculus, but they often are not convenient

Formal Proof

- A proof must end in a finite number of steps
- Each step must be either a premise or a proposition implied from previous steps using a valid equivalence or rule of inference; each step requires explicit justification
- For a direct proof, the last step must be the conclusion; for an indirect proof the last step must be a contradicion

Direct Proof

Theorem: $(p \to r) \wedge (q \to s) \wedge (p \vee q) \Rightarrow s \vee r$

	Statement	**Reason**
1.	$p \vee q$	premise
2.	$\neg(\neg p) \vee q$	1, involution
3.	$\neg p \to q$	2, conditional rule
4.	$q \to s$	premise
5.	$\neg p \to s$	3, 4, chain rule
6.	$\neg s \to \neg(\neg p)$	5, contrapositive
7.	$\neg s \to p$	6, involution
8.	$p \to r$	premise
9.	$\neg s \to r$	7, 8, chain rule
10.	$\neg(\neg s) \vee r$	9, conditional rule
11.	$s \vee r$	10, involution ■

Direct Proof (Extra detail)

Theorem: $(p \to r) \wedge (q \to s) \wedge (p \vee q) \Rightarrow s \vee r$

	Statement	**Reason**
1.	$p \vee q$	premise
2.	$\neg(\neg p) \vee q$	1, involution
3.	$\neg p \to q$	2, conditional rule
4.	$q \to s$	premise
5.	$(\neg p \to q) \wedge (q \to s)$	3, 4, conjunction
6.	$\neg p \to s$	5, chain rule
7.	$\neg s \to \neg(\neg p)$	6, contrapositive
8.	$\neg s \to p$	7, involution
9.	$p \to r$	premise
10.	$(\neg s \to p) \wedge (p \to r)$	8, 9, conjunction
11.	$\neg s \to r$	10, chain rule
12.	$\neg(\neg s) \vee r$	11, conditional rule
13.	$s \vee r$	12, involution ■

Direct Proof

Theorem: $(\neg p \vee q) \wedge (s \vee p) \wedge \neg q \Rightarrow s$

	Statement	**Reason**
1.	$\neg p \vee q$	premise
2.	$\neg q$	premise
3.	$\neg p$	1, 2, disjunctive simplification
4.	$s \vee p$	premise
5.	s	3, 4, disjunctive simplification ■

Worksheet Problem #1

Theorem: $(p \to q) \wedge (\neg p \to q) \Rightarrow q$

	Statement	**Reason**
1.	$p \to q$	premise
2.	$\neg p \to q$	premise
3.	$\neg q \to \neg p$	1, contraposition
4.	$\neg q \to q$	2, 3, chain rule
5.	$\neg(\neg q) \vee q$	4, conditional equivalence
6.	$q \vee q$	5, involution
7.	q	6, idempotence

Worksheet Problem #2

Theorem: $\neg(a \wedge b) \wedge \neg(\neg c \wedge a) \wedge \neg(c \wedge \neg b) \Rightarrow \neg a$

	Statement	**Reason**
1.	$\neg(a \wedge b)$	premise
2.	$\neg(\neg c \wedge a)$	premise
3.	$\neg(c \wedge \neg b)$	premise
4.	$\neg a \vee \neg b$	1, de Morgan's law
5.	$\neg b \vee \neg a$	4, commutative law
6.	$b \to \neg a$	5, conditional equivalence
7.	$\neg(\neg c) \vee \neg a$	2, de Morgan's law
8.	$\neg c \to \neg a$	7, conditional equivalence
9.	$\neg c \vee \neg(\neg b)$	3, de Morgan's law
10.	$\neg(\neg b) \vee \neg c$	9, commutative law
11.	$\neg b \to \neg c$	10, conditional equivalence
12.	$\neg b \to \neg a$	8, 11, chain rule
13.	$(b \to \neg a) \wedge (\neg b \to \neg a)$	6, 12, conjunction
14.	$\neg a$	13, Worksheet Problem #1

A Useful Equivalence

p	h	c	$p \to (h \to c) \leftrightarrow (p \wedge h) \to c$
0	0	0	
0	0	1	
0	1	0	
0	1	1	
1	0	0	
1	0	1	
1	1	0	
1	1	1	

A Useful Equivalence

p	h	c	$p \to (h \to c) \leftrightarrow (p \wedge h) \to c$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	1

Conditional Conclusions

- When the conclusion of a theorem is a conditional proposition, the premise of the condition can be added as a premise in the proof of the theorem
- $p \to (h \to c) \Leftrightarrow (p \wedge h) \to c$

Conditional Conclusions

$[p \to (q \to s)] \wedge (\neg r \vee p) \wedge q \Rightarrow r \to s$
$[p \to (q \to s)] \wedge (\neg r \vee p) \wedge q \wedge r \Rightarrow s$

	Statement	**Reason**
1.	$\neg r \vee p$	premise
2.	r	added premise
3.	p	1, 2, disjunctive simplification
4.	$p \to (q \to s)$	premise
5.	$q \to s$	3, 4, detachment
6.	q	premise
7.	s	5, 6, detachment ■

Validity of Verbal Arguments

- You can check the validity of a verbal argument (sales pitch, political speech, etc.) using the tools we have seen so far, as long as the argument uses simple declarative statements
- Consider the following announcement made by a government official:

  If the interest rates drop, the housing market will improve. Either the federal discount rate will drop or the housing market will not improve. Interest rates will drop; therefore, the federal discount rate will drop.
- Use the following variables to represent the individual propositions:
  - r: Interest rates will drop.
  - h: The housing market will improve.
  - f: The federal discount rate will drop.

  to produce $(r \to h) \wedge (f \vee \neg h) \wedge r \Rightarrow f$

Validity of Verbal Arguments

- Use the following variables to represent the individual propositions:
  - r: Interest rates will drop.
  - h: The housing market will improve.
  - f: The federal discount rate will drop.

  to produce $(r \to h) \land (f \lor \neg h) \land r \Rightarrow f$

	Statement	Reason
1.	$r \to h$	premise
2.	$f \lor \neg h$	premise
3.	r	premise
4.	$\neg h \lor f$	2, commutative
5.	$h \to f$	4, conditional equivalence
6.	$r \to f$	1, 5, chain rule
7.	f	3, 6, detachment

Proof by Contradiction

- As known as an *indirect proof*
- Stategy: Show that the premises coupled with the negation of the conclusion lead to a contradiction
- The contradiction can appear in various forms:
  - For proofs involving propositional calculus: a proposition of the form $p \land \neg p$
  - For proofs involving numbers: $0 = 1$ or $0 < 0$
  - For proofs involving sets: $x \in \varnothing$ or $x \in S \land x \in S^C$

Proof by Contradiction Justification

- Consider a theorem $P \Rightarrow C$, where P represents the premises $p_1 \land p_2 \land \ldots \land p_n$
- $(P \land \neg C \to 0) \to (P \to C)$

P	C	$\neg C$	$P \land \neg C$	0	$P \land \neg C \to 0$	$P \to C$	$(P \land \neg C \to 0) \to (P \to C)$
0	0	1	0	0	1	1	1
0	1	0	0	0	1	1	1
1	0	1	1	0	0	0	1
1	1	0	0	0	1	1	1

Proof by Contradiction

Theorem: $(p \to r) \land (q \to s) \land (p \lor q) \Rightarrow s \lor r$

	Statement	Reason
1.	$\neg(s \lor r)$	negated conclusion
2.	$\neg s \land \neg r$	1, DeMorgan's law
3.	$\neg s$	2, conjunctive simplification
4.	$q \to s$	premise
5.	$\neg q$	3, 4, indirect reasoning
6.	$\neg r$	2, conjunctive simplification
7.	$p \to r$	premise
8.	$\neg p$	6, 7, indirect reasoning
9.	$\neg p \land \neg q$	5, 8, conjunction
10.	$\neg(p \lor q)$	9, DeMorgan's law
11.	$p \lor q$	premise
12.	$\neg(p \lor q) \land (p \lor q)$	10, 11, conjunction
13.	0	12, negation $\to\leftarrow$ $\blacksquare$

Higher-level Proofs

- Most mathematicians write proofs at a higher level than the proofs we have seen so far
- The difference is like the difference between programming in a higher-level language vs. assembly language programming
- Most proofs consist largely of natural language text (like English) and do not explicitly mention the inference rules involved
- Prove that the sum of any two odd numbers is even

Background for Proof

Prove that the sum of any two odd numbers is even

- We need to establish some definitions and facts that go beyond those we have seen so far:
  - Only integers may be classified as even or odd
  - Any even number may be expressed as $2k$, for some integer k. Even numbers are multiples of two.
  - Any odd number many be expressed as $2k+1$, for some integer k. Odd numbers are not multiples of two.
  - The set of integers is closed under addition. This means if you add any two integers the result is guaranteed to be an integer.
  - The set of integers is closed under multiplication. This means if you multiply any two integers the result is guaranteed to be an integer.
  - The normal rules of algebra apply.

The Proof

Prove that the sum of any two odd numbers is even

Let m and n be any two odd integers. There exist $k, p \in \mathbb{Z}$ such that $m = 2k+1$, and $n = 2p+1$. (Why use two different variables, k and p?)

$$\begin{aligned} m+n &= (2k+1)+(2p+1) \\ &= 2k+2p+1+1 \\ &= 2k+2p+2 \\ &= 2(k+p+1) \end{aligned}$$

$k+p+1$ is an integer because the set of integers is closed under addition. Thus, the sum of any two odd numbers is an even number. ■

Proof by Contradiction

- Prove that $\sqrt{2}$ is irrational.
- Background: An irrational number is a number that may not be represented as the ratio of two integers
  - Examples include π, e, and $\sqrt{2}$

  The product of two even numbers is even, and the product of two odd numbers is odd.
- To prove by contradiction, we will assume the conclusion is false and produce a contradiction

Prove $\sqrt{2}$ is Irrational

Suppose $\sqrt{2}$ is rational. Let $\sqrt{2} = \frac{m}{n}$, where $m, n \in \mathbb{Z}$, and $n \neq 0$.

Further, let $\frac{m}{n}$ be a fraction reduced the lowest terms (this means m and n have no common factors except 1).
Square both sides of the equation to obtain

$$2 = \frac{m^2}{n^2}$$

Multiplying both sides by n^2 yields

$$2n^2 = m^2$$

Thus, m is an even number, because the product of two odd numbers is odd. Since m is even, we can express it as $m = 2k$, for some integer k.

Prove $\sqrt{2}$ is Irrational

Since $m = 2k$, for some integer k, we can rewrite

$$2n^2 = m^2$$

as

$$2n^2 = (2k)^2$$

or

$$2n^2 = 4k^2$$

Dividing both sides by 2 produces

$$n^2 = 2k^2$$

which means n is an even number. Since both m and n are even, they have a common factor of 2, and this contradicts the premise that $\frac{m}{n}$ is a fraction reduced to lowest terms. $\rightarrow\leftarrow$ ■

Proof by Contradiction (2)

- Prove the following theorem: If $x+x=x$, then $x=0$.
- To produce a contradiction, assume $x+x=x$ and $x \neq 0$.

$x+x=x$	Premise
$2x=x$	Combine like terms
$\frac{2x}{x}=\frac{x}{x}$	Divide both sides by a non-zero number
$\frac{2\cancel{x}}{\cancel{x}}=\frac{\cancel{x}1}{\cancel{x}}$	Cancel equal factors
$2=1$	$\rightarrow\leftarrow$ ■

Mathematical Induction

- Some have said this is only kind of proof that computer scientists can do
  - (This is an exageration)
- Mathematical induction is valuable for proving theorems about positive integers
  - Or just about anything that in some way ties into positive integers
  - Perhaps surprisingly, many things that computer scientists do relate somehow to the positive integers
- A proof using mathematical induction is a two step process:
  - basis
  - induction

Mathematical Induction

- A proof using mathematical induction is a two step process:
  - basis
  - induction
- To show that property $P(n)$ is true for all positive integers:
  - Show $P(1)$; that is, show the property is true for 1 (basis)
  - Show that for an arbitrary integer k, $P(k) \to P(k+1)$ (induction)
- The basis step is almost always trivial.
- The induction step usually is more interesting

Induction Example

Prove:

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

- **Basis** (Show $P(1)$)

$\sum_{i=1}^{1} i = 1 = \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1(1+1)}{2}$

- **Induction** (Show $P(k) \to P(k+1)$)

$$\begin{aligned}
\sum_{i=1}^{k+1} i &= \sum_{i=1}^{k} i + \sum_{i=k+1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) \\
&= \frac{k(k+1)}{2} + \frac{2k}{2} + \frac{2}{2} = \frac{k(k+1)+2k+2}{2} \\
&= \frac{k^2+k+2k+2}{2} = \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2} \\
&= \frac{(k+1)([k+1]+1)}{2} \quad \blacksquare
\end{aligned}$$

Non-inductive Proof

Prove:

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

Let $s = \sum_{i=1}^{n} i$

$$\begin{aligned}
s &= 1+2+3+\ldots+(n-2)+(n-1)+n \\
+\ s &= n+(n-1)+(n-2)+\ldots+3+2+1
\end{aligned}$$

$2s =$

$(n+1)+(n-1+2)+(n-2+3)+\ldots(n-2+3)+(n-1+2)+(n+1)$

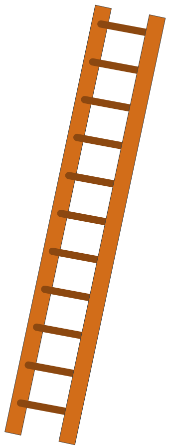
$2s = (n+1)+(n+1)+(n+1)+\ldots(n+1)+(n+1)+(n+1)$

How many terms? n

$2s = n(n+1)$

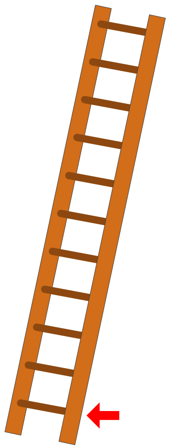
$s = \frac{n(n+1)}{2}$

Ladder Analogy



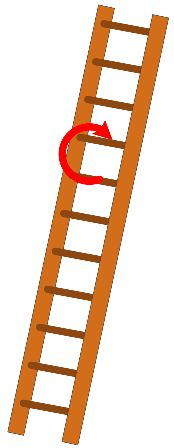
- The concept of mathematical induction is analogous to climbing a ladder

Ladder Analogy



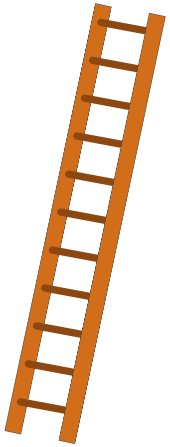
- The concept of mathematical induction is analogous to climbing a ladder
- Proving the basis step indicates that you can get on the first rung of the ladder

Ladder Analogy



- The concept of mathematical induction is analogous to climbing a ladder
- Proving the basis step indicates that you can get on the first rung of the ladder
- Proving the induction step indicates that if you are on *any* rung of the ladder, you can get to the next rung of the ladder

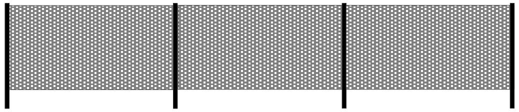
Ladder Analogy



- The concept of mathematical induction is analogous to climbing a ladder
- Proving the basis step indicates that you can get on the first rung of the ladder
- Proving the induction step indicates that if you are on *any* rung of the ladder, you can get to the next rung of the ladder
- Together the two parts show that you climb to any rung of the ladder as high as you wish

Fence Example

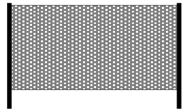
- A fence is built by connecting fence segments to fence posts



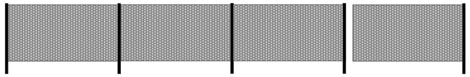
- The length of a fence is determined by the number of segments it contains
- Prove that any fence built with n segments will contain $n+1$ fenceposts.

Fence Example Proof—Basis

- **Basis**
  A fence containing one segment contains two posts

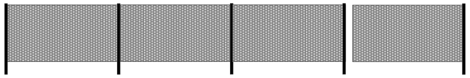


- Consider a fence that contains $k+1$ segments.



Fence Example Proof—Induction

- **Induction**
- Consider a fence that contains $k+1$ segments.



- Embedded within a $k+1$ long fence is a fence of length k.
- The fence of length $k+1$ adds one segment and one fencepost to the fence of length k so the number of fenceposts in a fence of length $k+1$ is the number of fenceposts in a fence of length k, plus one.
- By the inductive hposthesis, the number of fenceposts in the fence of length k is $k+1$, so the number of fenceposts in the fence of length $k+1$ is $(k+1)+1$. ■

Induction on Inequalities

When proving $x = y$ we use a chain of equalities begining at x and ending at y:

$$x = \quad \ldots \quad = y$$

Proving that $x < y$, $x \leq y$, $x > y$, or $x \geq y$ is a little different.

- For example, to show $x \leq y$, we use a chain of expressions as before, but we may use $=$ and $\leq$ to connect the expressions.
- For example, to show $x < y$, we use a chain of expressions as before, but we may use $=$, $\leq$, and $<$ to connect the expressions.

Review:

- $x \leq x + a$, if $a \geq 0$
- $x < x + a$, if $a > 0$
- $x \leq ax$, if $a \geq 1$
- $x < ax$, if $a > 1$

Induction Example

Prove:

$$5n^2 + n + 10 < n^3, \text{ for all } n \geq 6$$

- **Basis** (Show $P(6)$)
  $5 \cdot 6^2 + 6 + 10 = 5 \cdot 36 + 16 = 180 + 16 = 196 < 216 = 6^3$
- **Induction** (Show $P(k) \rightarrow P(k+1)$)

$$\begin{aligned}
5(k+1)^2 + (k+1) + 10 &= 5(k^2 + 2k + 1) + k + 1 + 10 \\
&= 5k^2 + 10k + 5 + k + 1 + 10 \\
&= 5k^2 + k + 10 + 10k + 5 + 1 \\
&= 5k^2 + k + 10 + 10k + 6 \\
&< k^3 + 10k + 6 \quad \text{(Inductive hypothesis)} \\
&\leq k^3 + 10k + k \quad (k \geq 6) \\
&= k^3 + 11k \\
&< k^3 + 18k
\end{aligned}$$

Induction Example (continued)

- **Induction** (Show $P(k) \to P(k+1)$)

$$\begin{aligned}
5(k+1)^2+(k+1)+10 &= 5(k^2+2k+1)+k+1+10 \\
&= 5k^2+10k+5)+k+1+10 \\
&= 5k^2+k+10+10k+5+1 \\
&= 5k^2+k+10+10k+6 \\
&< k^3+10k+6 \\
&\leq k^3+10k+k \\
&= k^3+11k \\
&< k^3+18k \\
&= k^3+3\cdot 6\cdot k \\
&\leq k^3+3\cdot k\cdot k \qquad (k \geq 6) \\
&= k^3+3k^2 \\
&< k^3+3k^2+3k+1 \\
&= (k+1)^3 \quad \blacksquare
\end{aligned}$$

Quantifiers

- Existential quantifier ($\exists$)
  - there exists
  - $(\exists x)[P(x)]$ means there is at least one element in the set for which property P is true
  - $(\exists k \in \mathbb{Z})(3k = 102)$ says that 102 is a multiple of three (true statement)
  - $(\exists k \in \mathbb{Z})(3k = 100)$ says that 100 is a multiple of three (false statement)
    - We can write $(\nexists k \in \mathbb{Z})(3k = 100)$
- When the set of interest, sometimes called *domain of discourse*, is understood, we can omit the set associated with the quantifier: $(\exists k)(3k = 102)$

Quantifiers

- Universal quantifier ($\forall$)
  - for all
  - $(\forall x)[P(x)]$ means that property P is true for every element in the set
  - $(\forall x \in \mathbb{R})(x^2 \geq 0)$
  - $(\forall n \in \mathbb{Z})(n+0 = n = 0+n)$
- When the domain of discourse is understood, we can omit the set associated with the quantifier: $(\forall x)(x^2 \geq 0)$

Quantifiers

- Let the universal set U be everything in the world
- Let $P(x)$ mean "x is a parrot"
- Let $G(x)$ mean "x is green"
- How do we express the following?
  "All parrots are green"
- $(\forall x \in U)[P(x) \wedge G(x)]$
  - "Everything in the world is a green parrot"
- $(\forall x \in U)[P(x) \to G(x)]$
  - "Anything that is a parrot must be green"
- Almost always, $\to$ and $\forall$ work together
  - Almost never, $\wedge$ and $\forall$ go together

Quantifiers

- Let the universal set U be everything in the world
- Let $P(x)$ mean "x is a parrot"
- Let $G(x)$ mean "x is green"
- How do we express the following?
  "There is a green parrot"
- $(\exists x \in U)[P(x) \to G(x)]$
  - This is equivalent to $(\exists x \in U)[\neg P(x) \vee G(x)]$
  - "Something exists in the world that is not a parrot or is green"
  - Because of the $\vee$ this is true as long as you can find something (x) in the world that is not a parrot!
- $(\exists x \in U)[P(x) \wedge G(x)]$
  - "Something exists in the world that is both a parrot and green"
- Almost always, $\wedge$ and $\exists$ work together
  - Almost never, $\to$ and $\exists$ go together

Negating Quantifiers

- $\neg\{(\forall x)[P(x)]\} \Leftrightarrow (\exists x)[\neg P(x)]$
- Let A be the set of all animals
  - $W(x)$ means x lives in water
  - $F(x)$ means x is a fish
  - Is the following statement true?
    $(\forall x \in A)[W(x) \to F(x)]$
  - **No**. Consider dolphins, and other sea mammals
  - The following **is** true:
    $\neg\{(\forall x \in A)[W(x) \to F(x)]\}$

$$\begin{aligned}
\neg\{(\forall x \in A)[W(x) \to F(x)]\} &\Leftrightarrow (\exists x \in A)\{\neg[W(x) \to F(x)]\} \\
&\Leftrightarrow (\exists x \in A)\{\neg[\neg W(x) \vee F(x)]\} \\
&\Leftrightarrow (\exists x \in A)\{[W(x) \wedge \neg F(x)]\}
\end{aligned}$$

Negating Quantifiers

- $\neg\{(\exists x)[P(x)]\} \Leftrightarrow (\forall x)[\neg P(x)]$
- Let H be the set of all humans alive today
  - $T(x)$ means x is taller than six feet
  - $C(x)$ means x is less than one year old
  - Is the following statement true? $(\exists x \in H)[T(x) \wedge C(x)]$
  - **No**.
  - The following **is** true: $\neg\{(\exists x \in H)[T(x) \wedge C(x)]\}$

$$\begin{aligned}\neg\{(\exists x \in H)[T(x) \wedge C(x)]\} &\Leftrightarrow (\forall x \in H)\{\neg[T(x) \wedge C(x)]\}\\ &\Leftrightarrow (\forall x \in H)[\neg T(x) \vee \neg C(x)]\\ &\Leftrightarrow (\forall x \in H)[T(x) \to \neg C(x)]\end{aligned}$$

Multiple Quantifiers

- Multiple variables require multiple qualifiers
  - $P(x,y)$ could mean $x^2 - y^2 = (x+y)(x-y)$
  - This is true for all real numbers x and y
  - $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})[x^2 - y^2 = (x+y)(x-y)]$
- You may arrange multiple universal quantifiers in any order without changing the logical meaning:
  - $(\forall x)(\forall y)[P(x,y)] \Leftrightarrow (\forall y)(\forall x)[P(x,y)]$
- $P(x,y)$ could mean $x+y=4$ and $x-y=2$
  - This is true for only two real numbers, $x=3$ and $y=1$
  - $(\exists x \in \mathbb{R})(\exists y \in \mathbb{R})[(x+y=4) \wedge (x-y=2)]$
- You may arrange multiple existential quantifiers in any order without changing the logical meaning:
  - $(\exists x)(\exists y)[P(x,y)] \Leftrightarrow (\exists y)(\exists x)[P(x,y)]$

Mixing Universal and Existential Quantifiers

- Order matters
- Consider the set P consisting of all the people in the world. Let likes(x,y) mean "x likes y." Interpret each of the following statements:
  - $(\forall x \in P)(\exists y \in P)[\text{likes}(x,y)]$
    - "Everyone likes somebody"
  - $(\exists y \in P)(\forall x \in P)[\text{likes}(x,y)]$
    - "There is somebody that everyone likes"
  - These are not the same
  - $(\exists x \in P)(\forall y \in P)[\text{likes}(x,y)]$
    - "There is somebody that likes everyone"
- $(\forall x \in \mathbb{Z})(\exists y \in \mathbb{Z})(x+y=0=y+x)$
  - For every integer (x) you can find an integer (y) such that the sum of the two is zero ($x+y=0$).
  - Every integer has an additive inverse: $x+(-x)=0=(-x)+x$
- $(\exists y \in \mathbb{Z})(\forall x \in \mathbb{Z})(x+y=0=y+x)$
  - There is an integer (y) that may be added to any integer (x) to produce zero.
  - There is no such integer that works for any integer

Proof Methods

- Theorems in mathematics are expressed in one of two ways:
  - If P, then C $\quad P \Rightarrow C$
  - P if and only if C $\quad P \Leftrightarrow C$
    - In order to prove $P \Leftrightarrow C$, we must prove $(P \Rightarrow C) \wedge (C \Rightarrow P)$
- Ways to prove $P \Rightarrow C$:
  - **Direct**: Assume P is true and deduce C
  - **Indirect (proof by contradiction)**: Assume P is true and C is false and derive a contradiction to a premise, theorem, or other basic concept

Exhaustive Proof

- If the theorem involves a small, finite number of cases, an exhaustive proof may be possible
  - Demonstrate the theorem's correctness in all possible cases
- Prove: $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})[(m < 4 \wedge n < 4) \to (m \cdot n < 10)]$
  - Build a multiplication table

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	4	6
3	0	3	6	9

- Most interesting theorems deal with properties of infinite sets like $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$

Examples and Counterexmples

- Unless an exhaustive enumeration of all the cases is possible, "proof by example" is **not** a proof!
  - Prove: The sum of two integers equals the product of those two integers
  - Example: $2+2=4=2\cdot 2$; therefore, the sum of two integers equals the product of those integers
  - Is this true in general?
    - No. $2+3=5\neq 6=2\cdot 3$
- We cannot use an example to *prove* a theorem, but we use an example to *disprove* a proposed theorem
- An example that disproves a proposed theorem is called a *counterexample*
- A counterexample is an easy way to disprove a theorem, but a counterexample may not always be easy to find

Examples and Counterexmples

- Examples provide evidence that a theorem may be true
- Examples may suggest a strategy for constructing a proof, but do not constitute a proof
- Prove or disprove that all numbers in the sequence $12, 121, 1211, 12111, 121111, 1211111, \ldots$ are composite
  - A composite number has factors (divisors) other than 1 and itself
  - Try some examples and perhaps find a quick counterexample:

1	12	$3 \cdot 4$
2	121	$11 \cdot 11$
3	1211	$7 \cdot 173$
4	12111	$3 \cdot 4{,}037$
5	121111	$281 \cdot 431$
6	1211111	$11 \cdot 110{,}101$
7	12111111	$3 \cdot 4{,}037{,}037$
8	121111111	$11 \cdot 11{,}010{,}101$
9	1211111111	$7 \cdot 173{,}015{,}873$
10	12111111111	$3 \cdot 4{,}037{,}037{,}037$

  - Looking good!

Examples and Counterexmples

- Prove or disprove that all numbers in the sequence $12, 121, 1211, 12111, \ldots$ are composite
  - Try some examples:

1	12	$3 \cdot 4$
2	121	$11 \cdot 11$
3	1211	$7 \cdot 173$
4	12111	$3 \cdot 4{,}037$
5	121111	$281 \cdot 431$
6	1211111	$11 \cdot 110{,}101$
7	12111111	$3 \cdot 4{,}037{,}037$
8	121111111	$11 \cdot 11{,}010{,}101$
9	1211111111	$7 \cdot 173{,}015{,}873$
10	12111111111	$3 \cdot 4{,}037{,}037{,}037$

  - Write a computer program to check
  - But ...

$$\underbrace{12111\ldots111}_{138\text{ digits}}$$

is a prime number (not composite)