MTH-2215
Applied Discrete Mathematics

Chapter 1, Section 1.1
Propositional Logic

These class notes are based on material from our textbook, **Discrete Mathematics and Its Applications**, 6th ed., by Kenneth H. Rosen, published by McGraw Hill, Boston, MA, 2006. They are intended for classroom use only and are **not** a substitute for reading the textbook.

Proposition

- A *proposition* is a declarative sentence that is either true or false, but not both.
- Other way: A proposition is a statement that is *true* or *false*.
- Examples:
  - The capital of New York is Albany.
  - The moon is made of green cheese.
  - Go to town. (not a proposition – why?)
  - What time is it? (not a proposition – why?)
  - $x + 1 = 2$ (not a proposition – why?)

Simple/Compound Propositions

- A simple proposition has a value of T/F
- A compound proposition is constructed from one or more simple propositions using logical operators
- The truth value of a compound proposition depends on the truth values of the constituent propositions

Negation (NOT)

- *NOT* can be represented by the ~ or ¬ symbols
- *NOT* is a logical operator:

  p: I am going to town.

  ~*p*: I am not going to town.

Truth table for ~ (NOT)

p	***~p***
T	F
F	T

Truth Tables

- A truth table lists ALL possible values of a (compound) proposition
  - one column for each propositional variable
  - one column for the compound proposition
  - 2^n rows for n propositional variables

Conjunction (AND)

- The conjunction *AND* is a logical operator

  p: I am going to town.
  q: It is raining.
  $p \wedge q$: I am going to town and it is raining.

- Both p and q must be true for the conjunction to be true.

Truth table for ^ (AND)

p	***q***	***p*** ^ ***q***
T	T	T
T	F	F
F	T	F
F	F	F

Disjunction (OR)

- Inclusive or - only one proposition needs to be true for the disjunction to be true.

  p: I am going to town.

  q: It is raining.

  $p \vee q$: I am going to town or it is raining.

Truth table for $\vee$ (OR)

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Exclusive OR

- Only one of p and q are true (not both).

  p: I am going to town.

  q: It is raining.

  $p \oplus q$: Either I am going to town or it is raining.

Truth table for $\oplus$ (Exclusive OR)

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Conditional statements

- A *conditional* statement is also called an *implication* or an *if .. then* statement.
- It has the form $p \rightarrow q$

  p: I am going to town.

  q: It is raining.

  $p \rightarrow q$: If I am going to town, then it is raining.
- The implication is false only when p is true and q is false!

Truth table for Conditional statements

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Implication - Equivalent Forms

- If *p*, then *q*
- *p* implies *q*
- If *p*, *q*
- *q* if *p*
- *q* whenever *p*
- *p* is a sufficient condition for *q*
- *q* is a necessary condition for *p*
- *p* only if *q*

Converse of an Implication

- Implication: $p \rightarrow q$
- Converse: $q \rightarrow p$
- Implication:
  - If I am going to town, it is raining.
- Converse:
  - If it is raining, then I am going to town.

Converse of an Implication

p	q	$q \rightarrow p$
T	T	T
T	F	T
F	T	F
F	F	T

(for p $\rightarrow$ q, this would be F)

(for p $\rightarrow$ q, this would be T)

Contrapositive of an Implication

- Implication: $p \rightarrow q$
- Contrapositive: $\neg q \rightarrow \neg p$
- Implication:
  - If I am going to town, it is raining.
- Contrapositive:
  - If it is not raining, then I am not going to town.
- The contrapositive has the same truth table as the original implication.

Inverse of an Implication

- Implication: $p \rightarrow q$
- Inverse: $\neg p \rightarrow \neg q$
- Implication:
  - If I am going to town, it is raining.
- Inverse:
  - If I am not going to town, then it is not raining.
- The inverse of an implication has the same truth table as the converse of that implication.

Biconditional

- “if and only if”, “iff”
- $p \leftrightarrow q$
- I am going to town if and only if it is raining.
- Both p and q must have the same truth value for the assertion to be true.

Truth Table for $\leftrightarrow$ (Biconditional)

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Truth Table Summary of Connectives

p	q	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

Compound Propositions

- To construct complex truth tables, add intermediate columns for smaller (compound) propositions
- One column for each propositional variable
- One column for each compound proposition
- For n propositional variables there will be 2^n rows
- Example:

$$(p \vee q) \rightarrow \neg r$$

Truth Tables for Compound Propositions

p	q	r	$p \vee q$	$\sim r$	$(p \vee q) \rightarrow \sim r$
T	T	T	T	F	F
T	T	F	T	T	T
T	F	T	T	F	F
T	F	F	T	T	T
F	T	T	T	F	F
F	T	F	T	T	T
F	F	T	F	F	T
F	F	F	F	T	T

Precedence of Logical Operators

- Parentheses gets the highest precedence
- Then:

Operator	Precedence
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Precedence of Logical Operators

- Examples:

  $p \wedge q \vee r$ means $(p \wedge q) \vee r$, not $p \wedge (q \vee r)$

  $p \vee q \rightarrow r$ means $(p \vee q) \rightarrow r$

Translating English Sentences

- To remove natural language ambiguity
- Helps in reasoning
- Examples:
  - You can access the Internet from campus only if you are a computer science major or you are not a freshman.
  - You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old.

Logic and Bit Operations

- Binary numbers use *bits*, or *bi*nary digi*t*s.
- Each bit can have one of two values:

  1 (which represents TRUE)

  0 (which represents FALSE)
- A variable whose value can be true or false is called a Boolean variable. A Boolean variable's value can be represented using a single bit.

Logic and Bit Operations

- Computer bit operations are exactly the same as the logic operations we have just studied. Here is the truth table for the bit operations OR, AND, and XOR:

x	y	$x \vee y$	$x \wedge y$	$x \oplus y$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

MTH 2215

Applied discrete mathematics

Chapter 1, Section 1.2
Propositional Equivalences

Basic Terminology

- A *tautology* is a proposition which is always true. Example:

$$p \vee \neg p$$

- A *contradiction* is a proposition that is always false. Example:

$$p \wedge \neg p$$

Basic Terminology

p	**¬p**	**p ∨ ¬p**	**p ∧ ¬p**
T	F	T	F
F	T	T	F

Basic Terminology

- A *contingency* is a proposition that is neither a tautology nor a contradiction. Example:

$$p \vee q \rightarrow \neg r$$

Logical Equivalences

- Two propositions p and q are logically equivalent if they have the same truth values in all possible cases.
- Two propositions p and q are logically equivalent if $p \leftrightarrow q$ is a tautology.
- Notation: $p \Leftrightarrow q$ or $p \equiv q$

Determining Logical Equivalence

- Consider the following two propositions:

  $\neg(p \vee q)$

  $\neg p \wedge \neg q$

- Are they equivalent? Yes. (They are part of DeMorgan's Law, which we will see later.)
- To show that $\neg(p \vee q)$ and $\neg p \wedge \neg q$ are logically equivalent, you can use a truth table:

Equivalence of $\neg(p \vee q)$ and $\neg p \wedge \neg q$

p	**q**	**p ∨ q**	**¬(p ∨ q)**	**¬p**	**¬q**	**¬p ∧ ¬q**
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

Show that: $\neg p \vee q \equiv p \rightarrow q$

p	**q**	**$\neg p$**	**$\neg p \vee q$**	**$p \rightarrow q$**
T	T	F	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

Determining Logical Equivalence

- This is not a very efficient method. Why?
- To be more efficient, we develop a series of equivalences, and use them to prove other equivalences.

Important Equivalences

$p \wedge \mathbf{T} \Leftrightarrow p$ $p \vee \mathbf{F} \Leftrightarrow p$	Identity
$p \vee \mathbf{T} \Leftrightarrow \mathbf{T}$ $p \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$	Domination
$p \vee p \Leftrightarrow p$ $p \wedge p \Leftrightarrow p$	Idempotent
$\neg(\neg p) \Leftrightarrow p$	Double Negation

Important Equivalences

$p \vee q \Leftrightarrow q \vee p$ $p \wedge q \Leftrightarrow q \wedge p$	Commutative
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	Associative
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributive
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	De Morgan's

Important Equivalences

$p \vee (p \wedge q) \Leftrightarrow p$ $p \wedge (p \vee q) \Leftrightarrow p$	Absorption
$p \vee \neg p \Leftrightarrow \mathbf{T}$ $p \wedge \neg p \Leftrightarrow \mathbf{F}$	Negation

Example

Show that $\neg(p \rightarrow q)$ and $p \wedge \neg q$ are logically equivalent:

$\neg(p \rightarrow q)$	$\equiv \neg(\neg p \vee q)$	Example 3
	$\equiv \neg(\neg p) \wedge \neg q$	2nd DeMorgan law
	$\equiv p \wedge \neg q$	double negation law

Q.E.D

Example

Show that $\neg(p \rightarrow q)$ and $p \wedge \neg q$ are logically equivalent:

$\neg(p \rightarrow q)$	$\neg(\neg p \vee q)$	Example 3
	$\neg(\neg p) \wedge \neg q$	2nd DeMorgan law
	$p \wedge \neg q$	double negation law

Q.E.D

Example

Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically equivalent:

$\neg(p \vee (\neg p \wedge q))$	$\neg p \wedge \neg(\neg \mathrm{p} \wedge \mathrm{q})$	2nd DeMorgan
	$\neg p \wedge [\neg(\neg \mathrm{p}) \vee \neg \mathrm{q})]$	1st DeMorgan
	$\neg p \wedge (\mathrm{p} \vee \neg \mathrm{q})$	double negation
	$(\neg p \wedge \mathrm{p}) \vee (\neg\ \mathrm{p} \wedge \neg \mathrm{q})$	2nd distributive
	$\mathrm{FALSE} \vee (\neg\ \mathrm{p} \wedge \neg \mathrm{q})$	negation
	$(\neg\ \mathrm{p} \wedge \neg \mathrm{q}) \vee \mathrm{FALSE}$	commutative
	$\neg p \wedge \neg q$	identity

Equivalences Involving Implications

$$p \rightarrow q \quad \Leftrightarrow \quad \neg p \vee q$$

$$p \rightarrow q \quad \Leftrightarrow \quad \neg q \rightarrow \neg p$$

$$p \vee q \quad \Leftrightarrow \quad \neg p \rightarrow q$$

$$p \wedge q \quad \Leftrightarrow \quad \neg(p \rightarrow \neg q)$$

$$\neg(p \rightarrow q) \quad \Leftrightarrow \quad p \wedge \neg q$$

More Equivalences Involving Implications

$$(p \rightarrow q) \wedge (p \rightarrow r) \quad \Leftrightarrow \quad p \rightarrow (q \wedge r)$$

$$(p \rightarrow r) \wedge (q \rightarrow r) \quad \Leftrightarrow \quad (p \vee q) \rightarrow r$$

$$(p \rightarrow q) \vee (p \rightarrow r) \quad \Leftrightarrow \quad p \rightarrow (q \vee r)$$

$$(p \rightarrow r) \vee (q \rightarrow r) \quad \Leftrightarrow \quad (p \wedge q) \rightarrow r$$

Equivalences Involving Biconditionals

$$p \leftrightarrow q \quad \Leftrightarrow \quad (p \rightarrow q) \wedge (q \rightarrow p)$$

$$p \leftrightarrow q \quad \Leftrightarrow \quad \neg p \leftrightarrow \neg q$$

$$p \leftrightarrow q \quad \Leftrightarrow \quad (p \wedge q) \vee (\neg p \wedge \neg q)$$

$$\neg(p \leftrightarrow q) \quad \Leftrightarrow \quad p \leftrightarrow \neg q$$

Example

- Show that $(p \wedge q) \rightarrow (p \vee q)$ is a tautology.

$(p \wedge q) \rightarrow (p \vee q)$	$\neg(p \wedge q) \vee (p \vee q)$	$p \rightarrow q \Leftrightarrow \neg p \vee q$
	$(\neg p \vee \neg q) \vee (p \vee q)$	1st DeMorgan law
	$\neg p \vee (\neg q \vee (p \vee q))$	Associative law
	$\neg p \vee ((p \vee q) \vee \neg q)$	Commutative law
	$(\neg p \vee p) \vee (q \vee \neg q)$	Associative law
	TRUE $\vee$ TRUE	Negation
	TRUE	Domination law

MTH 2215

Applied discrete mathematics

Chapter 1, Section 1.3
Predicates and Quantifiers

Predicates

- A predicate is a statement that contains variables.
- Examples:

  $P(x) : x > 3$

  $Q(x,y) : x = y + 3$

  $R(x,y,z) : x + y = z$

- The area of logic that deals with predicates and quantifiers is called *predicate calculus*.

Predicates

- A predicate becomes a proposition if the variables contained in it are either:
  - Assigned specific values
  - Quantified (*all*, *many*, *some*, *few*, *none*)

$P(x) : x > 3$

What are the truth values of $P(4)$ and $P(2)$?

$Q(x,y) : x = y + 3$

What are the truth values of $Q(1, 2)$ and $Q(3, 0)$?

Quantifiers

- Two types of quantifiers
  - Universal quantifier: $\forall$
  - Existential quantifier: $\exists$

- Universe of discourse - the particular *domain* of the variable in a propositional function

Universal Quantification

- $P(x)$ is true for all values of x in the universe of discourse.

  $\forall x\, P(x)$

  "for all x, $P(x)$"

  "for every x, $P(x)$"

- The variable x is bound by the *universal quantifier*, producing a proposition.

Examples

- U = {all real numbers}, $P(x)$: $x+1 > x$
  - What is the truth value of $\forall x\, P(x)$
- U = {all real numbers}, $Q(x)$: $x < 2$
  - What is the truth value of $\forall x\, Q(x)$
- U = {all students in MTH 2215}

  $R(x)$: x has an account on *Banner*
  - What does $\forall x\, R(x)$ mean?

For universal quantification

$$P(x) \Leftrightarrow P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$$

- If the elements in the universe of discourse can be listed, then $U = \{x_1, x_2, \ldots, x_n\}$

  $\forall x\, P(x) \Leftrightarrow P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$

- *Example*

  U = {positive integers not exceeding 3} and $P(x)$: $x^2 < 10$

  – What is the truth value of $\forall x\, P(x)$?

  P(1) $\wedge$ P(2) $\wedge$ P (3)

  T $\wedge$ T $\wedge$ T

  T

Existential Quantification

- $P(x)$ is true *for some* x in the universe of discourse

  $\exists x\, P(x)$

  "for some x, $P(x)$"

  "There exists an x such that $P(x)$"

  "There is at least one x such that $P(x)$"

- The variable x is bound by the *existential quantifier*, producing a proposition

Example

- U = {all real numbers}, $P(x)$: $x > 3$
  - What is the truth value of $\exists x\, P(x)$

- U = {all real numbers}, $Q(x)$: $x = x + 1$
  - What is the truth value of $\exists x\, Q(x)$

- U = {all students in MTH 2215},

  $R(x)$: x has an account on *Banner*
  - What does $\exists x\, R(x)$ mean?

For existential quantification

$$\exists x\, P(x) \Leftrightarrow P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$$

- If the elements in the universe of discourse can be listed, $U = \{x_1, x_2, \ldots, x_n\}$

  $$\exists x\, P(x) \Leftrightarrow P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$$

- *Example*

  U = {positive integers not exceeding 4} and $P(x)$: $x^2 < 10$

  – What is the truth value of $\exists x\, P(x)$?

  P(1) $\vee$ P(2) $\vee$ P(3) $\vee$ P(4)

  T $\vee$ T $\vee$ T $\vee$ F

  T

Binding Variables

- *Bound* variable: if a variable is quantified
- *Free* variable: Neither bound nor assigned a specific value
  - Example: $\forall x\, P(x), \exists x\, Q(x,y)$
- *Scope* of Quantifiers: Part of a logical expression to which a quantifier is applied
  - Example: $\exists x\, (P(x) \wedge Q(x)) \vee \forall x\, R(x)$

Negation of Quantifiers

- Distributing a negation operator across a quantifier changes a universal to an existential and vice versa.

$$\sim\forall x\, P(x) \Leftrightarrow \exists x\, \sim P(x)$$

$$\sim \exists x\, P(x) \Leftrightarrow \forall x\, \sim P(x)$$

Negation of Quantifiers

- Example:

  Assume the domain of x is: {students in MTH 2215}, and $P(x)$: x has taken a course in calculus. Then
  $\forall x\, P(x)$

  means "All students in MTH 2215 have taken a course in calculus."

  The *negation* of this statement would be, "Not every student in MTH 2215 has taken a course in calculus," or "There exists some student in MTH 2215 who has not taken a course in calculus." This would be:

  $\exists x \neg P(x)$

Translating from English

- There are many ways to translate a given sentence
- The goal is to produce a logical expression that is simple and can be easily used in subsequent reasoning
- Steps:
  - Clearly identify the appropriate quantifier(s)
  - Introduce variable(s) and predicate(s)
  - Translate using quantifiers, predicates, and logical operators

Example

"Every student in this class has studied calculus."

- Solution 1
  - Assume, U = {all students in MTH 2215}
  - Rewrite the sentence: "For every student in the class, that student has studied calculus."
  - Introduce a variable, x: "For every student x in the class, x has studied calculus."
  - Replace "x has studied calculus" with: $C(x)$
  - Since our domain is all students in MTH 2215, we can now represent our sentence with: $\forall x\, C(x)$

Example

- "Every student in this class has studied calculus."
- Solution 2
  - Assume, U = {all people}
  - Rewrite the sentence: "For every person x, if x is a student in the class, then x has studied calculus."
  - Replace "x is a student in the class" with: $S(x)$
  - Replace "x has studied calculus" with: $C(x)$
  - We can now represent our sentence with:

    $\forall x\, S(x) \rightarrow C(x)$

Example

- Some student in this class has visited Mexico
- Solution 1
  - Assume, U = {all students in MTH 2215}
  - $\exists x\ M(x)$
- Solution 2
  - Assume, U = {all people}
  - $\exists x\ S(x) \wedge M(x)$

More Examples

- $C(x)$: x is a CSE student
- $E(x)$: x is an ECE student
- $S(x)$: x is a smart student
- U = {all students in MTH 2215}

More Examples (Cont..)

- Everyone is a CSE student.

  $\forall x\, C(x)$

- Nobody is an ECE student.

  $\forall x \sim E(x)$ or $\sim\exists x\, E(x)$

- All CSE students are smart students.

  $\forall x\, [C(x) \rightarrow S(x)]$

- Some CSE students are smart students.

  $\exists x\, [C(x) \wedge S(x)]$

Use implication or conjunction?

- Universal quantifiers usually take implications
- All CSE students are smart students.

$\forall x\,[C(x) \rightarrow S(x)]$ Correct

$\forall x\,[C(x) \wedge S(x)]$ Incorrect

Use implication or conjunction?

- Existential quantifiers usually take conjunctions
- Some CSE students are smart students.

$\exists x\,[C(x) \wedge S(x)]$ Correct

$\exists x\,[C(x) \rightarrow S(x)]$ Incorrect

More Examples

- No CSE student is an ECE student.
  - If x is a CSE student, then that student is not an ECE student.

    $$\forall x\,[C(x) \rightarrow \sim E(x)]$$

  - There does not exist a CSE student who is also an ECE student.

    $$\sim\exists x\,[C(x) \wedge E(x)]$$

- If any ECE student is a smart student then he is also a CSE student.

  $$\forall x\,[(E(x) \wedge S(x)) \rightarrow C(x)]$$

MTH 2215

Chapter 1, Section 1.4
Nested Quantifiers

Nested Quantifiers

- Quantifiers that occur within the scope of other quantifiers
- Example:

$P(x,y)$: $x + y = 0$, U={**R**}

$\forall x \, \exists y \, P(x,y)$

Quantifications of Two Variables

- For all pairs x,y $\quad P(x,y)$.

  $\forall x \forall y\, P(x,y)$ $\qquad\qquad$ $\forall y \forall x\, P(x,y)$

- For every x there is a y such that $P(x,y)$.

  $\forall x \exists y\, P(x,y)$

- There is an x such that $P(x,y)$ for all y.

  $\exists x \forall y\, P(x,y)$

- There is a pair x,y such that $P(x,y)$.

  $\exists x \exists y\, P(x,y)$ $\qquad\qquad$ $\exists y \exists x\, P(x,y)$

Translating statements with nested quantifiers

U = {all real numbers}

$\forall x \, \forall y \, (x + y = y + x)$

Expressed in English:

"For all real numbers x, for all real numbers y, $x + y = y + x$"

This statement is true.

Now let's reverse the $\forall x$ and $\forall y$ ….

Translating statements with nested quantifiers

U = {all real numbers}

$\forall y \, \forall x(x + y = y + x)$

Expressed in English:

"For all real numbers y, for all real numbers x, $x + y = y + x$"

This statement is also true.

Reversing the quantifiers does not make any difference, because both are of the same type.

Translating statements with nested quantifiers

U = {all real numbers}

Express in English:

$$\forall x \, \exists y \, (x + y = 0)$$

"For every real number x there exists some real number y such that ($x + y = 0$)."

This is claiming that, given a real number x there is a real number y such that $x + y = 0$. It is easy to see that y must be $-x$. So this statement is true.

But check the next slide….

Translating statements with nested quantifiers

U = {all real numbers}

Express in English:

$\exists y \, \forall x \, (x + y = 0)$

"There exists some real number y such that for every real number x, $(x + y = 0)$."

This is claiming that there is some specific y to which we can add any real number x and have $x + y = 0$.

Obviously, there is no real number y for which it is true that $x + y = 0$ for all values of x. So this statement is false.

Translating statements with nested quantifiers

When we changed

$$\forall x \, \exists y \, (x + y = 0)$$

to

$$\exists y \, \forall x \, (x + y = 0)$$

we changed the meaning of the statement, and ended up with a false one.

Obviously, if the quantifiers are of different types, then order is important.

Translating statements with nested quantifiers

U = {all real numbers}

Express in English:

$\forall x \, \forall y \, (\, (x > 0) \wedge (y < 0) \rightarrow (xy < 0) \,)$

"For all x, for all y, if x is greater than zero and y is less than zero, then multiplying them together will produce a negative number."

This is a true stement.

Translating statements with nested quantifiers

U = {all students in MTH 2215}

Express in English:

$C(x)$: x has a computer

$F(x,y)$: x and y are friends

$\forall x \, (\, C(x) \vee \exists y \, (C(y) \wedge F(x,y)) \,)$

"For every student x in MTH 2215, x has a computer or there exists some student y such that y has a computer and x and y are friends."

Translating Sentences

- U = {all people}

"If a person is female and is a parent, then this person is someone's mother."

Translate this into a logical expression:

$\forall x ((F(x) \wedge P(x)) \rightarrow \exists y\ M(x,y))$

Can we move the existential quantification over to the left side? Yes (see the *null quantification rule* in exercise 47 on p. 49):

$\forall x\ \exists y ((F(x) \wedge P(x)) \rightarrow M(x,y))$

Translating Sentences

U = {all integers}

"The sum of two positive integers is positive."

Translate this into a logical expression:

$\forall x \forall y ((x > 0) \wedge (y > 0) \rightarrow ((x + y) > 0)$

BUT if we change the domain so that

U = {all positive integers}

then

$\forall x \forall y ((x + y) > 0)$

Is the order of quantifiers important?

- If the quantifiers are of the same type, then order does not matter.
- If the quantifiers are of different types, then order is important.

Example

U={**R**}

Q(x, y): x + y = 0

What are the truth values for $\exists y\ \forall x\ Q(x,y)$ and $\forall x\ \exists y\ Q(x,y)$?

$\exists y\ \forall x\ Q(x,y)$: There exists at least one *y* such that for every real number *x*, Q(x,y) is true, i.e., x + y = 0.

FALSE (not for every x, only when y is –x).

But…

$\forall x\ \exists y\ Q(x,y)$: For every real number *x*, there is a real number *y* such that Q(x,y) is true, i.e., x + y = 0.

TRUE (for every x when y is –x)

Negating Nested Quantifiers

- To negate nested quatifiers, apply De Morgan's Laws for Quantifiers successively for each quantifier.
- Example:

  "There does not exist a woman who has taken a flight on every airline in the world."

  First express the positive of this statement:

  "There is a woman who has taken a flight on every airline in the world."

Negating Nested Quantifiers

"There is a woman who has taken a flight on every airline in the world."

P(w, f) = "woman *w* has taken flight *f*"

Q(f, a) = "flight *f* is a flight on airline *a*"

$\exists w \; \forall a \; \exists f \; (P(w, f) \wedge Q(f, a))$

"There exists some woman *w* such that, for all airlines *a,* there exists some flight *f* such that *w* has taken this flight."

Negating Nested Quantifiers

Now we negate the previous logical expression to get:

$$\neg\exists w\ \forall a\ \exists f\ (P(w, f) \wedge Q(f, a))$$

Successively applying DeMorgan's laws we get:

$$\forall w\ \neg\forall a\ \exists f\ (P(w, f) \wedge Q(f, a))$$

$$\forall w\ \exists a\ \neg\exists\ f\ (P(w, f) \wedge Q(f, a))$$

$$\forall w\ \exists a\ \forall f\ \neg(P(w, f) \wedge Q(f, a))$$

$$\forall w\ \exists a\ \forall f\ (\neg P(w, f) \vee \neg Q(f, a))$$

Negating Nested Quantifiers

$\forall w \exists a \forall f (\neg P(w, f) \vee \neg Q(f, a))$

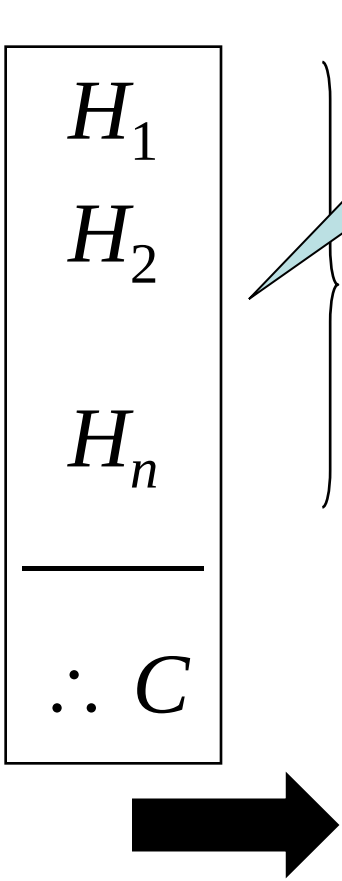
can be read as”

“For every woman there exists some airline such that for all flights either this woman has not taken that flight or that flight is not on this airline.”

MTH 2215

Chapter 1, Section 1.5
Rules of Inference

Rules of Inference



H_1
H_2
H_n
$\therefore C$

$H_1, H_2, \ldots H_n$ the hypotheses (premises)

We use conjunction: H1 ^ H2 ^ H3…

C is the conclusion.

“$\therefore$” means “therefore” or “it follows that”

Validity of an Argument

- An argument is valid if
  - whenever all hypotheses are true, the conclusion is also true
- To prove that an argument is valid:
  - Assume the hypotheses are true
  - Use the rules of inference *and* logical equivalences to determine that the conclusion is true

Some Rules of Inference

p $p \rightarrow q$ --- $\therefore q$	$[p \wedge (p \rightarrow q)] \rightarrow q$	Modus ponens *mode that affirms*
$\neg q$ $p \rightarrow q$ --- $\therefore \neg p$	$[\neg q \wedge (p \rightarrow q)] \rightarrow \neg p$	Modus tollens *mode that denies*
$p \rightarrow q$ $q \rightarrow r$ --- $\therefore p \rightarrow r$	$[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ --- $\therefore q$	$[(p \vee q) \wedge \neg p] \rightarrow q$	Disjunctive syllogism

Some Rules of Inference

p --- $\therefore p \vee q$	$p \rightarrow p \vee q$	Addition
$p \wedge q$ --- $\therefore p$	$p \wedge q \rightarrow p$	Simplification
p q --- $\therefore p \wedge q$	$[(p) \wedge (q)] \rightarrow (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ --- $\therefore q \vee r$	$[(p \vee q) \wedge (\neg p \vee r)] \rightarrow (q \vee r)$	Resolution

Example: Modus Ponens

from Latin: *mode that affirms*

p $p \rightarrow q$ $\therefore q$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus Ponens

- In other words:

  If the hypothesis p is true

  and the hypothesis $(p \rightarrow q)$ is true

  Then I can conclude q

Example: Modus Ponens

- p: "*n* is greater than 3"
- q: "n^2 is greater than 9"

- Assuming that p$\rightarrow$ q is true, then:

  if is n greater than 3, it follows that n^2 is greater than 9.

Example: Hypothetical syllogism

$p \rightarrow q$
$\underline{q \rightarrow r}$
$\therefore\ p \rightarrow r$

Hypothetical syllogism

- If it rains today, then we will not have a barbecue today.
- If we do not have a barbecue today, then we will have a barbecue tomorrow
- Therefore, if it rains today, then we will have a barbecue tomorrow.

Example: Simplification

$\frac{p \wedge q}{\therefore p}$	$(p \wedge q) \rightarrow p$	Simplification

p: “it is below freezing”

q: “it is raining now”

- It is below freezing and raining now.

  Therefore, it is below freezing.

Recap 1.2: Important Equivalences

$p \wedge \mathbf{T} \Leftrightarrow p$ $p \vee \mathbf{F} \Leftrightarrow p$	Identity
$p \vee \mathbf{T} \Leftrightarrow \mathbf{T}$ $p \wedge \mathbf{F} \Leftrightarrow \mathbf{F}$	Domination
$p \vee p \Leftrightarrow p$ $p \wedge p \Leftrightarrow p$	Idempotent
$\neg(\neg p) \Leftrightarrow p$	Double Negation

Recap 1.2: Important Equivalences

$p \vee q \Leftrightarrow q \vee p$ $p \wedge q \Leftrightarrow q \wedge p$	Commutative
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$ $(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$	Associative
$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	Distributive
$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$ $\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	De Morgan's

Recap 1.2: Important Equivalences

$p \vee (p \wedge q) \Leftrightarrow p$ $p \wedge (p \vee q) \Leftrightarrow p$	Absorption
$p \vee \neg p \Leftrightarrow \mathbf{T}$ $p \wedge \neg p \Leftrightarrow \mathbf{F}$	Negation

Example

- Consider the following logical argument:
  - If horses fly or cows eat artichokes, then the mosquito is the national bird.
  - If the mosquito is the national bird then peanut butter tastes good on hot dogs.
  - But peanut butter tastes terrible on hot dogs.
  - Therefore, cows don’t eat artichokes.

Example

- Assignments:

p	Horses fly
q	Cows eat artichokes
r	The mosquito is the national bird
s	Peanut butter tastes good on hot dogs

- Represent the argument using the variables

$$\left.\begin{array}{l}(p \vee q) \rightarrow r \\ r \rightarrow s \\ \neg s\end{array}\right\} \text{ Hypotheses}$$

$$\therefore \neg q \quad \text{Conclusion}$$

Example

Assertion		Reasons
1.	$(p \vee q) \rightarrow r$	Hypothesis
2.	$r \rightarrow s$	Hypothesis
3.	$(p \vee q) \rightarrow s$	Hypothetical syll. on 1. and 2.
4.	$\neg s$	Hypothesis
5.	$\neg(p \vee q)$	*Modus tollens* on 3. and 4.
6.	$\neg p \wedge \neg q$	DeMorgan on 5.
7.	$\neg q \wedge \neg p$	Commutative on 6.
8.	$\neg q$	Simplification on 7.

We have obtained our conclusion: *"cows don't eat artichokes"*

Example

- Show that the following argument is valid:
  - It is not sunny this afternoon and it is colder than yesterday.
  - We will go swimming only if it is sunny.
  - If we do not go swimming, then we will take a canoe trip.
  - If we take a canoe trip, then we will be home by sunset.
  - Therefore, we will be home by sunset.

Example: Put into propositional form

p = it is sunny this afternoon

q = it is colder than yesterday

r = we will go swimming

s = we will take a canoe trip

t = we will be home by sunset

Example: Represent hypotheses

$\neg p \wedge q$	It is not sunny this afternoon and it is colder than yesterday
$r \rightarrow p$	We will go swimming only if it is sunny
$\neg r \rightarrow s$	If we do not go swimming, then we will take a canoe trip
$s \rightarrow t$	If we take a canoe trip, then we will be home by sunset
t	We will be home by sunset

Example: Constuct logical argument

$\neg p \wedge q$	Hypothesis
$\neg p$	Simplification using previous step
$r \rightarrow p$	Hypothesis
$\neg r$	Modus tollens using steps 2 and 3
$\neg r \rightarrow s$	Hypothesis
s	Modus ponens using steps 4 and 5
$s \rightarrow t$	Hypothesis
t	Modus ponens using steps 6 and 7

Rules of Inference for Quantified Statements

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\dfrac{\forall x\, P(x)}{\therefore\ P(c)}$	Universal instantiation
$\dfrac{P(c) \text{ for an arbitrary } c}{\therefore\ \forall x\, P(x)}$	Universal generalization
$\dfrac{\exists x\, P(x)}{\therefore\ P(c) \text{ for some element } c}$	Existential instantiation
$\dfrac{P(c) \text{ for some element } c}{\therefore\ \exists x\, P(x)}$	Existential generalization

Rules of Inference for Quantified Statements

In Universal Instantiation, we know that P(x) is true for <u>all</u> values of x; therefore it must also be true of <u>any particular</u> value of x, c.

In Universal Generalization, we know that P(c) is true for <u>any</u> specific value of c; therefore it must be true for <u>all</u> values, so $\forall x$ P(x).

In Existential Instantiation, we know that P(x) is true for at least one specific value of x, c.

- In Universal Instantiation, we know that P(c) is true for <u>some</u> particular value of c, so $\exists x$ P(x). Here c need not be arbitrary but often is assumed to be.

Example

Show that the following argument is valid:

- Everyone in the Applied discrete mathematics class has taken a CSE course.
- Marla is a student in the Applied discrete mathematics class.
- Therefore, Marla has taken a CSE course.

Example:

Put into propositional form:

$D(x)$ = x is in the Applied discrete mathematics class

$C(x)$ = x has taken a CSE course

Represent hypotheses:

$\forall x(D(x) \rightarrow C(x))$	Everyone in the Applied discrete mathematics class has taken a CS course
D(Marla)	Marla is a student in the Applied discrete mathematics class

Example: Constuct logical argument

STEP	**JUSTIFICATION**
$\forall x(D(x) \rightarrow C(x))$	Premise
$D(\text{Marla}) \rightarrow C(\text{Marla})$	Universal Instantiation using step 1
$D(\text{Marla})$	Premise
$C(\text{Marla})$	Modus ponens using steps 2 and 3

Do as Exercise

- A student in this class has not read the book.
- Everyone in this class passed the first exam.
- Therefore, someone who passed the first exam has not read the book.

Fallacies

- Fallacies resemble rules of inference but are based on contingencies rather than tautologies. They are incorrect inferences.
- Three common fallacies
  - Affirming the Consequent
  - Denying the Hypothesis
  - Circular Reasoning (begging the question)

Fallacy of Affirming the Consequent

$$\begin{array}{l} p \to q \\ q \\ \hline \therefore\ p \end{array} \qquad\qquad ((p \to q) \wedge q) \to p$$

- This argument is fallacious. $((p \to q) \wedge q) \to p$ is not a tautology and therefore not a rule of inference.

Example

If you do every problem in this book, then you will learn Applied discrete mathematics.

You learned Applied discrete mathematics.

Therefore, you did every problem in this book.

- This is the "Fallacy of Affirming the Consequent". You might have learned discrete mathematics by paying attention in class instead of by doing all the problems.

Fallacy of Denying the Hypothesis

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

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

This argument is fallacious.

$((p \to q) \wedge \neg p) \to \neg q$ is not a tautology and therefore not a rule of inference.

Example

If you do every problem in this book, then you will learn Applied discrete mathematics.

You did not do every problem in this book.

Therefore, you did not learn Applied discrete mathematics.

This is the “Fallacy of Denying the Hypothesis”. Even though you did not do every problem in this book, you still might have learned Applied discrete mathematics by paying attention in class.

MTH 2215

Applied discrete mathematics

Chapter 1, Section 1.6

Introduction to Proofs

Definitions

- A *theorem* is a valid logical assertion which can be proved using
  - *Axioms*: statements which are given to be true
  - *Rules of inference*: logical rules allowing the deduction of conclusions from premises
- A *lemma* is a ‘pre-theorem’ or a result which is needed to prove a theorem.
- A *corollary* is a ‘post-theorem’ or a result which follows directly from a theorem.

Methods of Proof

- Direct proof
- Indirect proof
- Vacuous proof
- Trivial proof
- Proof by contradiction
- Proof by cases
- Existence proof

Proof Basics

- We want to establish the truth of $p \rightarrow q$
- p may be a conjunction of other hypotheses
- $p \rightarrow q$ is a *conjecture* until a proof is produced

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Direct Proof

- Assume the hypotheses are true
- Use rules of inference and any logical equivalences to establish the truth of the conclusion
- *HOW TO PROVE:*
  - *If p is true, then q has to be true for* $p \rightarrow q$ *to be true*
- Example: The proof we did earlier about cows not eating artichokes was an example of a direct proof

Example

- Give a direct proof of the theorem: "If n is an odd integer, then n^2 is an odd integer"

  (n is odd) $\rightarrow$ (n^2 is odd)

- Using the following definition:
  - *If n is even, then there exists an integer k such that n=2k, and if it is odd, if there exists an integer k such that n=2k+1.*

Example (Cont.)

Assume the hypothesis "*n* is odd" true:

n is odd

Since *n* is odd, then $\exists k\ n = 2k + 1$

Now, is the conclusion "n^2 is odd" true?

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$
$$= 2(m) + 1, \text{ where some integer } m = 2k^2 + 2k$$

Since $n^2 = 2(m)+1$, then "n^2 is odd" is true

Proof complete

Indirect Proof

- Proofs that are not direct proofs – that is, do start with the hypothesis and end with the conclusion – are called indirect proofs.

Indirect Proof

- One useful type of indirect proof is *proof by contraposition*
- Remember that $p \rightarrow q$ is equivalent to $\sim q \rightarrow \sim p$ (its contrapositive)
- Therefore, we can prove $p \rightarrow q$ indirectly by showing that its contrapositive, $\sim q \rightarrow \sim p$, is true.

Example

Give an indirect proof to the theorem:

"if $3n + 2$ is odd, then n is odd"

$(3n + 2 \text{ is odd}) \rightarrow (n \text{ is odd})$

p	$3n + 2$ is odd	~p	$3n + 2$ is even
q	n is odd	~q	n is even

The contrapositive is:

$\sim(n \text{ is odd}) \rightarrow \sim (3n + 2 \text{ is odd})$

or, in other words,

$(n \text{ is even}) \rightarrow (3n + 2 \text{ is even})$

Example (Cont.)

n is even	Assuming the hypothesis (of the contrapositive)
$n = 2k$	Def. of "even"
$3n + 2 = 3(2k) + 2 = 6k + 2$	Replacing n with $2k$ and simplifying
$3n + 2 = 2(3k + 1)$	Factoring
$3n + 2 = 2(m)$	Replacing $3k + 1$ with m
$3n + 2$ is even	Def. of "even"

Proof complete!

Example (Cont)

Since we now know that:

"$\sim$(n is odd) $\rightarrow$ ~ (3n + 2 is odd)"

is true, we also know that its contrapositive (our original statement):

"(3n + 2 is odd) $\rightarrow$ (n is odd)"

must be true.

Vacuous Proof

- If we know one of the hypotheses in p is false then $p \rightarrow q$ is *vacuously* true.
- $\mathbf{F} \rightarrow \mathbf{T}$ and $\mathbf{F} \rightarrow \mathbf{F}$ are both true.
- Example:
  - If I am both rich and poor, then hurricane Katrina was a mild breeze.
- The hypotheses $(p \wedge \neg p)$ form a contradiction, and therefore q follows from the hypotheses vacuously.
- If we start out assuming that a false premise is true, then we can prove almost anything we want!

Example

Given the proposition $P(n)$: if $n > 1$, then $n^2 > n$,

show that $P(0)$.

P(n): $(n > 1) \rightarrow (n^2 > n)$

P(0): $(0 > 1) \rightarrow (0^2 > 0)$

A conditional statement with a false hypothesis is guaranteed to be true. Since the hypothesis (0 >1) is false, P(0) is automatically true.

Trivial Proof

- If we know q is true, then $p \rightarrow q$ is true
- $\mathbf{F} \rightarrow \mathbf{T}$ and $\mathbf{T} \rightarrow \mathbf{T}$ are both true.
- Example:
  - If it's snowing today then the empty set is a subset of every set.
- The assertion is *trivially* true independent of the truth value of p.

Example

Given the proposition

$P(n)$: if $a \geq b > 0$, then $a^n \geq b^n$

show that $P(0)$ is true.

P(n): $(a \geq b > 0) \rightarrow (a^n \geq b^n)$

P(0): $(a \geq b > 0) \rightarrow (a^0 \geq b^0)$, in other words

P(0): $(a \geq b > 0) \rightarrow (1 \geq 1)$,

Since the conclusion $(1 \geq 1)$ is true, P(0) is true.

Proof by Contradiction

- Sometimes called "Reductio ad absurdum" (reduction to the absurd)
- We want to prove p. We do that by assuming the opposite, $\neg p$, and show that that implies a contradiction q (i.e., q is FALSE no matter what, or is absurd).
- Mathematical definition of the proof
  - Find a contradiction q such that

$$\neg p \rightarrow q \Leftrightarrow \neg p \rightarrow \mathbf{F} \Leftrightarrow \neg(\neg p) \Leftrightarrow p$$

Proof by Contradiction

Suppose that we want to prove that $\sqrt{2}$ is irrational.

Proof:

1. **By definition, if a real number *x* is *rational* then there exist two integers *m* and *n* such that *x* = *m*/*n*.**
2. **Assume that $\sqrt{2}$ is rational.**
3. **Then there are integers *m′* and *n′* such that $\sqrt{2}$ = *m′*/*n′*.**
4. **We divide *m′* and *n′* by all factors common to both *m′* and *n′*, giving us two integers, *m* and *n*, with no common factors, and $\sqrt{2}$ = *m*/*n*.**

Proof by Contradiction

5. Since $m/n = \sqrt{2}$, $m = n \cdot \sqrt{2}$
6. Squaring both sides of the equation gives us: $m^2 = n^2 \cdot 2$
7. Therefore, m^2 must be even, and consequently m must be even.
8. Since m is an even integer, $m = 2k$, where k is also an integer.
9. Substituting, we see that $(2k)^2 = 2n^2$.
10. Simplifying and canceling 2 from both sides gives us $2k^2 = n^2$.
11. Therefore, n^2 is even, and so n is even.

Proof by Contradiction

12. Since n is an even integer, $n = 2j$, where j is also an integer.
13. So we have now shown that m and n are both even, that is, $m = 2k$ *and* $n = 2j$.
14. But this is a contradiction, since line 4 of our proof showed that the two integers, m and n, had no common factors.
15. Thus, or initial assumption, that $\sqrt{2}$ is rational, must be false.
16. Hence, $\sqrt{2}$ is irrational: QED.

Proof by Contradiction (Cont..)

- An indirect proof of an implication $p \rightarrow q$ can be rewritten as a proof by contradiction.
- Assume that both p and $\neg q$ are true.
- Then use a direct proof to show that

$$\neg q \rightarrow \neg p$$

- This leads to the contradiction $p \wedge \neg p$.
- Example:
  - If $3n + 2$ is odd, then n is odd. (see p. 81)

Mistakes in proofs

- Sometimes we cause mistakes in our proofs by making a faulty assumtion.
- For example, there is a famous “proof” that 2 = 1 that is based on a faulty assumption.
- Given that a and b are positive integers and $a = b$, what is wrong with the following proof?

Mistakes in proof

Step	**Reason**
$a = b$	hypothesis
$a^2 = ab$	Multiply both sides by a
$a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides
$(a - b)(a + b) = b(a - b)$	Factor both sides
$a + b = b$	Divide by $(a - b)$
$2b = b$	Step 1, replace & simplify
$2 = 1$	Divide by b

Mistakes in proof

The problem here is in step 5, where we divide both sides of the equation by $(a - b)$. Our original hypothesis was that $a = b$, so dividing by $(a - b)$ is dividing by zero, which is undefined in our numbering system.

Circular Reasoning

- One or more steps of the proof are based upon the truth of the statement being proved.
- This fallacy arises when a stement is proven using itself or a statement that is equivalent to it.
- Also known as *begging the question.*

Circular Reasoning

- Suppose we want to prove that:

if n^2 is an even integer then n is an even integer

Assume that n^2 is even

$n^2 = 2k$ for some integer k

Let $n = 2j$ for some integer k

$\therefore$ n is even

Circular Reasoning

- Let's take a closer look at the "proof" of:

if n^2 is an even integer then n is an even integer

n^2 is even	hypothesis
$n^2 = 2k$ for some integer k	Def. of even
Let $n = 2j$ for some integer k	?
$\therefore$ n is even	Def. of even

The problem is line 3. We have no justification for assuming that $n = 2j$; in fact, that is what we are trying to prove!

MTH 2215

Applied discrete mathematics

Chapter 1, Section 1.7

Proof Methods and Strategies

Proof Basics

- We want to establish the truth of $p \rightarrow q$
- p may be a conjunction of other hypotheses
- $p \rightarrow q$ is a *conjecture* until a proof is produced

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

More Methods of Proof

- Proof by cases
- Exhaustive proof
- “Without loss of generality”
- Existence proof
- Uniqueness proof

Proof by Cases

- Break the premise of $p \rightarrow q$ into an equivalent disjunction of the form $p_1 \vee p_2 \vee \ldots \vee p_n$
- Then use the equivalence

  $[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \Leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$
- Each of the implications $p_i \rightarrow q$ is a *case*.
- You must
  - Convince the reader that the cases are inclusive (i.e., they exhaust all possibilities)
  - Establish all implications

Example

- Prove that if n is an integer, then $n^2 \geq n$
- The basic approach here is to observe that the problem consists of four cases: $n < 0$, $n = 0$, $n = 1$, $n > 1$
- If $n < 0$, then n^2 is positive and thus $n^2 \geq n$
- If n = 0, then n^2 and $n = 0$ and $n^2 \geq n$
- If n = 1, then n^2 and $n = 1$ and $n^2 \geq n$
- If n > 1, then $n^2 = n \bullet n$, which must be greater than n since $n > 1$, and thus $n^2 \geq n$
- Since the proposition is true for all 4 cases, it must be true in general

Exhaustive proof

- An exhaustive proof is a special type of proof by cases where each case involves checking a single example

Example

- Given that n is a positive integer and $n \leq 4$: prove that $(n + 1)^3 \geq 3^n$

Here we have only 4 cases, and each case involves a specific value of n: 1, 2, 3, and 4

- For $n = 1$, $(n + 1)^3 = 8$ and $3^n = 3$
- For $n = 2$, $(n + 1)^3 = 27$ and $3^n = 9$
- For $n = 3$, $(n + 1)^3 = 64$ and $3^n = 27$
- For $n = 4$, $(n + 1)^3 = 125$ and $3^n = 81$

These 4 cases exhaust all of the possibilities: QED

“Without Loss of Generality”

- By proving one case of a theorem, other cases follow by
  - making straightforward changes to the argument,
  - or by filling in some straightforward initial step.

Example

- Show that $(x+y)^r < x^r + y^r$ whenever x and y are positive real numbers and r is a real number with $0 < r < 1$.
- We say: “Without loss of generality we can assume that $x + y = 1$”
- Proof: (see next slide)

Example

- Proof:

$x + y = 1$	hypothesis
$0 < x < 1$ and $0 < y < 1$	x & y are positive
$0 < 1 - r < 1$	$0 < r < 1$ (given)
$x^{1-r} < 1$ and $y^{1-r} < 1$	
$x < x^r$ and $y < y^r$	
$x + y$ (which $= 1$) $< x^r + y^r$	
$(x + y)^r$ (which $= 1^r$) $< x^r + y^r$	

Example

- In the previous slide we said: “Without loss of generality we can assume that $x + y = 1$”
- How do we justify this? Well, ….

Example

We have proved the theorem assuming that $x + y = 1$. Suppose $x + y = t$. Then we can see that:

$(x / t) + (y / t) = 1$, and

$((x / t) + (y / t))^r = 1^r = 1$, so

$((x / t) + (y / t))^r < (x / t)^r + (y / t)^r$

Now we multiply both sides of this by t^r to get:

$(x + y)^r < x^r + y^r$

Existence Proof

- The proof of $\exists x P(x)$ is called an *existence proof*.
- Constructive existence proof
  - Find an element c in the universe of discourse such that $P(c)$ is true
- Non-constructive existence proof
  - Do not find c; instead, somehow prove $\exists x P(x)$ is true
  - Generally, we do this by contradiction
    - Assume no c exists that makes $P(c)$ true
    - Derive a contradiction

Example

- There is a positive integer that can be written as the sum of cubes of positive integers in two different ways

  $1729=10^3 + 9^3 =12^3 + 1^3$

- There exist irrational numbers x and y such that x^y is rational

Uniqueness Proof

- Sometimes we need to show that only one element of a set satisfies some particular condition
- A uniqueness proof has two parts:
  - Existence: show that an element x with the desired property exists
  - Uniqueness: show that, for any y, then either $y = x$, or y does not have the desired property

Example

- Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

The proof has two parts:

(1) Proof of existence:

$ar + b = 0$	hypothesis
$ar = -b$	subtract b from both sides
$r = -b/a$	divide both sides by a
$a(-b/a) + b = -b + b = 0$	*QED*

Example

(1) Proof of uniqueness:

Assume s is a real number and $as + b = 0$

$as + b = 0$	hypothesis
$ar + b = as + b$	since both equal 0
$ar = as$	subtract b from both sides
$r = s$	divide both sides by a
QED	

Proof strategy

- We can prove that there is no perfect strategy for constructing a proof!
- More of an art than a science
- Requires lots of practice
- Try both forward and backward reasoning
- Try looking for counterexamples
- Adapt existing proofs that are similar to what you want to prove

Forward and Backward Reasoning

- Forward reasoning:
  - Start with premises p
  - Construct a proof using a sequence of steps to
  - Arrive at a conclusion q
- Backward reasoning:
  - Don't start off by assuming p and proving that q follows
  - Instead, try to prove q by finding (or proving) a statement p for which we already know $p \rightarrow q$

Example

- See the handout on the “15-stones” game
- The game starts with a pile of 15 stones. The two players take turns removing 1, 2, or 3 stones at a time from the pile. The winner is the person who removes the last stone from the pile.
- By working backward, we can see what will happen if she leaves only 1 stone left, then 2, then 3, etc., all the way back to the original 15 stones.
- We deduce that the first player can always win.

Counterexamples

- Sometimes we are asked to prove something that we suspect is not true.
- In that case, look for a counterexample first, or you may end up wasting your time on something that cannot be proven to be true.
- Example: *"Every positive integer is the sum of three squares of integers."*
- True for 1 ($0^2 + 0^2 + 1^2$), 2 ($0^2 + 1^2 + 1^2$), 3 ($1^2 + 1^2 + 1^2$), 4 ($0^2 + 0^2 + 2^2$), 5 ($0^2 + 1^2 + 2^2$), 6 ($1^2 + 1^2 + 2^2$), but not for 7 – counterexample!

Adapting Existing Proofs

- In Section 1.6 we proved that $\sqrt{2}$ is irrational.
- Suppose that we are asked to prove that $\sqrt{3}$ is irrational.
- Instead of starting from scratch, you can adapt the proof for $\sqrt{2}$; this can save you lots of time and effort.

Recap: Direct Proof

- Assume the hypotheses are true
- Use rules of inference and any logical equivalences to establish the truth of the conclusion

Example

- Prove that if $m + n$ and $n + p$ are even integers, then $m + p$ is even.

Recap: Indirect Proof

- A direct proof of the contrapositive
  - Remember: p $\rightarrow$ q is equivalent to ~q $\rightarrow$ ~p
  - Proof ~q $\rightarrow$ ~p
    - Assume that $\neg q$ is true i.e., q is false
    - Use rules of inference and logical equivalences to show that $\neg p$ is true i.e., p is false

Example

- Prove that if m and n are integers and $m \bullet n$ is even, then m is even or n is even.

Recap: Vacuous Proof

- If we know one of the hypotheses in p is false then $p \rightarrow q$ is *vacuously* true.
- $\mathbf{F} \rightarrow \mathbf{T}$ and $\mathbf{F} \rightarrow \mathbf{F}$ are both true.

Recap: Trivial Proof

- If we know q is true, then $p \rightarrow q$ is true
- $\mathbf{F} \rightarrow \mathbf{T}$ and $\mathbf{T} \rightarrow \mathbf{T}$ are both true.

Recap: Proof by Contradiction

- We want to prove p. What if we can prove that $\neg p$ implies a contradiction q (i.e., q is FALSE no matter what, or is absurd)?
- Mathematical definition of the proof
  - Find a contradiction q such that

$$\neg p \rightarrow q \;\Leftrightarrow\; \neg p \rightarrow \mathbf{F} \;\Leftrightarrow\; \neg(\neg p) \;\Leftrightarrow p$$

Example

- Show that there is no rational number r for which $r^3 + r + 1 = 0$

Conclusion

We have covered the following topics in Logic:

- Propositional Logic
- Propositional Equivalences
- Predicates and Quantifiers
- Nested Quantifiers
- Rules of Inference
- Introduction to Proofs
- Proof Methods and Strategies