Discrete Mathematics

Logic & Proof

Propositional Logic

Propositions

- A proposition is a statement that can be either true or false
  - "Yongdae has an Apple laptop."
  - "Yongdae is a professor."
  - "3 = 2 + 1"
  - "3 = 2 + 2"

- Not propositions:
  - "Are you Bob?"
  - "x = 7"
  - "I am heavy."

Propositional variables

- We use propositional variables to refer to propositions
  - Usually are lower case letters starting with p (i.e. *p, q, r, s*, etc.)
  - A propositional variable can have one of two values: true (T) or false (F)

- A proposition can be…
  - A single variable: p
  - An operation of multiple variables: $p \wedge (q \vee \neg r)$

Introduction to Logical Operators

- About a dozen logical operators
  - Similar to algebraic operators + * - /
- In the following examples,
  - p = "Today is Friday"
  - q = "Today is my birthday"

Logical operators: Not

- A "not" operation switches (negates) the truth value
- Symbol: ¬ or ~
- $\neg p$ = "Today is not Friday"

p	$\neg p$
T	F
F	T

Logical operators: And

- An “and” operation is true if both operands are true
- Symbol: $\wedge$
  - It’s like the ‘A’ in And
  - $p \wedge q$ = “Today is Friday a
- today is my birthday”

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Logical operators: Or

- An “or” operation is true if either operands are true
- Symbol: $\vee$
- $p \vee q$ = “Today is Friday o
- today is my birthday (or
- possibly both)”

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

Logical operators: Exclusive Or

- An exclusive or operation is true if one of the operands are true, but false if both are true
- Symbol: $\oplus$
- Often called XOR
- $p \oplus q \equiv (p \vee q) \wedge \neg(p \wedge q)$

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

- $p \oplus q$ = "Today is Friday or today is my birthday, but not both"

Inclusive Or versus Exclusive Or

- Do these sentences mean inclusive or exclusive or?
  - Experience with C++ or Java is required
  - Lunch includes soup or salad
  - To enter the country, you need a passport or a driver's license

Logical operators: Conditional 1

- A conditional means "if p then q"
- Symbol: $\rightarrow$
- $p \rightarrow q$ = "If today is
- Friday, then today
- is my birthday"
- $p \rightarrow q \equiv \neg p \vee q$

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

the antecedent

the consequence

Logical operators: Conditional 2

- Let p = "I am elected" and q = "I will lowe
- I state: $p \rightarrow q$ = "If I
- am elected, then I
- will lower taxes"
- Consider all
- possibilities
- Note that if p is false, then
- the conditional is true regardless of whether q is true or false

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

Logical operators: Conditional 3

- Alternate ways of stating a conditional:
  - p implies q
  - If p, q
  - p only if q
  - p is sufficient for q
  - q if p
  - q whenever p
  - q is necessary for p

Logical operators: Conditional 4

				Conditional	Inverse	Converse	Contrapositive
p	q	$\neg p$	$\neg q$	$p \rightarrow q$	$\neg p \rightarrow \neg q$	$q \rightarrow p$	$\neg q \rightarrow \neg p$
T	T	F	F	T	T	T	T
T	F	F	T	F	T	T	F
F	T	T	F	T	F	F	T
F	F	T	T	T	T	T	T

Logical operators: Bi-conditional 1

- A bi-conditional means "*p* if and only if *q*"
- Symbol: $\leftrightarrow$
- Alternatively, it means
- "(if *p* then *q*) and
- (if *q* then *p*)"
- Note that a bi-conditional
- has the opposite truth values
- of the exclusive or

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

Logical operators: Bi-conditional 2

- Let p = "You take this class" and q = "You get a grade"
- Then $p \leftrightarrow q$ means
- "You take this class if
- and only if you get a
- grade"
- Alternatively, it means "If
- you take this class, then
- you get a grade and if you get a grade then you take (took) this class"

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

Boolean operators summary

		not	not	and	or	xor	conditional	Bi-conditional
p	q	$\neg p$	$\neg q$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \rightarrow q$	$p \leftrightarrow q$
T	T	F	F	T	T	F	T	T
T	F	F	T	F	T	T	F	F
F	T	T	F	F	T	T	T	F
F	F	T	T	F	F	F	T	T

memorize the table!

Precedence of operators

- Just as in algebra, operators have precedence
  - 4+3*2 = 4+(3*2), not (4+3)*2
- Precedence order (from highest to lowest):

  $\neg \; \wedge \; \vee \; \rightarrow \; \leftrightarrow$
  - The first three are the most important
  - This means that $p \vee q \wedge \neg r \rightarrow s \leftrightarrow t$
- yields: $(p \vee (q \wedge (\neg r)) \rightarrow s) \leftrightarrow (t)$
- Not is *always* performed before any other operation

Translating English Sentences

- Question 7 from Rosen, p. 17
  - p = "It is below freezing"
  - q = "It is snowing"

- It is below freezing and it is snowing — $p \wedge q$
- It is below freezing but not snowing — $p \wedge \neg q$
- It is not below freezing and it is not snowing — $\neg p \wedge \neg q$
- It is either snowing or below freezing (or both) — $p \vee q$
- If it is below freezing, it is also snowing — $p \rightarrow q$
- It is either below freezing or it is snowing,
- but it is not snowing if it is below freezing — $(p \vee q) \wedge (p \rightarrow \neg q)$
- That it is below freezing is necessary and sufficient for it to be snowing — $p \leftrightarrow q$

Translation Example

- “I have neither given nor received help on this exam”
- Let p = “I have given help on this exam”
- Let q = “I have received help on this exam”

- $\neg p \wedge \neg q$

Translation Example

- You can access the Internet from campus only if you are a computer science major or you are not a freshman.
- $a \rightarrow (c \lor \neg f)$

- You cannot ride the roller coaster if you are under 4 feet tall unless you are older than 16 years old.
- $(f \land \neg s) \rightarrow \neg r$
- $r \rightarrow (\neg f \lor s)$

Bit Operations

- Boolean values can be represented as 1 (true) and 0 (false)
- A bit string is a series of Boolean values. Length of the string is the number of bits.
  - 10110100 is eight Boolean values in one string
- We can then do operations on these Boolean strings
- Each column is its own
  - Boolean operation

$$\begin{array}{r} 01011010 \\ \oplus\ 10110100 \\ \hline 11101110 \end{array}$$

Propositional Equivalence

Tautology, Contradiction, Equivalence

- Tautology: a statement that’s always true
  - $p \lor \neg p$ will always be true
- Contradiction: a statement that’s always false
  - $p \land \neg p$ will always be false
- A logical equivalence means that the two sides always have the same truth values
  - Symbol is $\equiv$ or $\Leftrightarrow$ (we’ll use $\equiv$)

Examples

- Identity law $p \wedge T \equiv p$

p	T	$p \wedge T$
T	T	T
F	T	F

- Commutative law $p \wedge q \equiv q \wedge p$

p	q	$p \wedge q$	$q \wedge p$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

Examples

- Associative law $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$	$q \wedge r$	$p \wedge (q \wedge r)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	F	F	F
T	F	F	F	F	F	F
F	T	T	F	F	T	F
F	T	F	F	F	F	F
F	F	T	F	F	F	F
F	F	F	F	F	F	F

How to prove equivalence?

- Two methods:
  - –Using truth tables
    - Not good for long formula
    - In this course, only allowed if specifically stated!
  - –Using the logical equivalences
    - The preferred method
- $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Truth Table Solution

- $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

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

Logical Equivalences

$p \wedge T \equiv p$ $p \vee F \equiv p$	Identity Laws	$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee T \equiv T$ $p \wedge F \equiv F$	Domination Law	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent Laws	$\neg (p \wedge q) \equiv \neg p \vee \neg q$ $\neg (p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$\neg(\neg p) \equiv p$	Double negation law	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative Laws	$p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$	Negation lows
$p \rightarrow q \equiv \neg p \vee q$	Definition of Implication	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$	Definition of Biconditional

Proof using Logical Equivalence

$(p \to r) \vee (q \to r)$

$\equiv (\neg p \vee r) \vee (\neg q \vee r)$ Definition of implication

$\equiv \neg p \vee r \vee \neg q \vee r$ Associative

$\equiv \neg p \vee \neg q \vee r \vee r$ Commutative

$\equiv (\neg p \vee \neg q) \vee (r \vee r)$ Associative

$\equiv \neg (p \wedge q) \vee r$ De Morgan, Idempotent

$\equiv (p \wedge q) \to r$ Definition of implication

Example

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

(Proof)

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

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

$\equiv (\neg p \vee \neg q) \vee (p \vee q)$ De Morgan

$\equiv (\neg p \vee p) \vee (\neg q \vee q)$ Commutative, Associative

$\equiv T \vee T$ Negation

$\equiv T$ Identity

Example

- At a trial:
  - Bill says: "Sue is guilty and Fred is innocent."
  - Sue says: "If Bill is guilty, then so is Fred."
  - Fred says: "I am innocent, but at least one of the others is guilty."
- Let b = Bill is innocent, f = Fred is innocent, and s = Sue is innocent
- Statements are:
  - $\neg s \wedge f$
  - $\neg b \rightarrow \neg f$
  - $f \wedge (\neg b \vee \neg s)$

- Can all of their statements be true???

Example (cnt)

- $(\neg s \wedge f) \wedge (\neg b \rightarrow \neg f) \wedge (f \wedge (\neg b \vee \neg s)) \equiv T$

LHS $\equiv (\neg s \wedge f) \wedge (b \vee \neg f) \wedge (f \wedge (\neg b \vee \neg s))$

$\equiv ((\neg s \wedge f) \wedge (f \wedge (\neg b \vee \neg s))) \wedge (b \vee \neg f)$

$\equiv (\neg s \wedge f \wedge (\neg b \vee \neg s)) \wedge (b \vee \neg f)$

$\equiv ((\neg s \wedge f \wedge \neg b) \vee (\neg s \wedge f)) \wedge (b \vee \neg f)$

$\equiv (\neg s \wedge f) \wedge (b \vee \neg f)$

$\equiv (\neg s \wedge f \wedge b) \vee (\neg s \wedge f \wedge \neg f)$

$\equiv (\neg s \wedge f \wedge b) \vee F$

Predicates and Quantifiers

It is frequently necessary to reason logically about statements of the form everything has the property p or something has the property p. One of the oldest and most famous pieces of logical reasoning, which was known to the ancient Greeks, is an example:

All men are mortal. Socrates is a man. Therefore Socrates is mortal.

In general, propositional logic is not expressive enough to support such reasoning. We could define a proposition P to mean 'all men are mortal', but P is an atomic symbol—it has no internal structure—so we cannot do any formal reasoning that makes use of the meaning of 'all'.

Predicate logic, also called first order logic, is an extension to propositional logic that adds two quantifiers that allow statements like the examples above to be expressed. Everything in propositional logic is also in predicate logic: all the definitions, inference rules, theorems, algebraic laws, etc., still hold.

The formal language of predicate logic consists of propositional logic, augmented with variables, predicates, and quantifiers.

A predicate is a statement that an object x has a certain property. Such statements may be either true or false. For example, the statement ‘x > 5’ is a predicate, and its truth depends on the value of x. A predicate can be extended to several variables; for example, ‘x > y’ is a predicate about x and y.

In predicate logic, it is traditional to write predicates concisely in the form F(x), where F is the predicate and x is the variable it is applied to. A predicate containing two variables could be written G(x, y). A predicate is essentially a function that returns a Boolean result.

Any term in the form F(x), where F is a predicate name and x is a variable name, is a well-formed formula. Similarly, $F(x_1 , x_2 , . . . , x_k)$ is a well-formed formula; this is a predicate containing k variables.

When predicate logic is used to solve a reasoning problem, the first step is to translate from English (or mathematics) into the formal language of predicate logic. This means the predicates are defined; for example we might define:

$$F(x) \equiv x > 0$$

$$G(x, y) \equiv x > y$$

The universe of discourse, often simply called the universe or abbreviated U , is the set of possible values that the variables can have. Usually the universe is specified just once, at the beginning of a piece of logical reasoning, but this specification cannot be omitted.

For example, consider the statement ‘For every x there exists a y such that $x = 2 \times y$’. If the universe is the set of even integers, or the set of real numbers, then the statement is true. However, if the universe is the set of natural numbers then the statement is false (let x be any odd number). If the universe doesn’t contain numbers at all, then the statement is not true or false; it is meaningless.

Several notational conventions are very common in predicate logic. The universe is called U, and its constants are written as lower-case letters, typically c and p (to suggest a constant value, or a particular value).

Variables are also lower-case letters, typically x, y, z.

Predicates are upper-case letters F, G, H, ... For example, F(x) is a valid expression in the language of predicate logic, and its intuitive meaning is ‘the variable x has the property F ’.

- How can we express
  - “every computer in CS department is protected by intrusion detection system”
  - “There exists at least one student who has a red hair”.
- “x is greater than 3”
  - x: subject
  - “is greater than 3”: predicate
  - P(x): propositional function P at x

Propositional Functions

- Consider $P(x) = x < 5$
  - $P(x)$ has no truth values (x is not given a value)
  - $P(1)$ is true: The proposition $1<5$ is true
  - $P(10)$ is false: The proposition $10<5$ is false

- $P(x)$ will create a proposition when given a value

- Let $P(x)$ = “x is a multiple of 5”
  - For what values of x is $P(x)$ true?

- Let $P(x) = x + 3$
  - For what values of x is $P(x)$ true?

Anatomy of a propositional function

$$P(x) = \underbrace{x + 5 > x}_{\text{predicate}}$$

variable

Propositional functions 3

- Functions with multiple variables:
  - $P(x,y) = x + y == 0$
    - $P(1,2)$ is false, $P(1,-1)$ is true
  - $P(x,y,z) = x + y == z$
    - $P(3,4,5)$ is false, $P(1,2,3)$ is true
  - $P(x_1,x_2,x_3 \ldots x_n) = \ldots$

Quantifiers

- Why quantifiers?
  - Many things (in this course and beyond) are specified using quantifiers
    - In some cases, it's a more accurate way to describe things than Boolean propositions

- A quantifier is "an operator that limits the variables of a proposition"

There are two quantifiers in predicate logic; these are the special symbols ∀ and ∃.

- Universal ∀ - Everything in the universe has a certain property
- Existential ∃ - something in the universe has a certain property
  - -Existential quantifications are used to state properties that must occur at least once.

Universal quantifiers 1

- Represented by an upside-down A: $\forall$
  - It means “for all”
  - Let $P(x) = x+1 > x$

- We can state the following:
  - $\forall x\ P(x)$
  - English translation: “for all values of x, P(x) is true”
  - English translation: “for all values of x, x+1>x is true”

Universal quantifiers 2

- But is that always true?
  - $\forall x\ P(x)$
- Let x = the character ‘a’
  - Is ‘a’+1 > ‘a’?
- Let x = the state of Minnesota
  - Is Minnesota+1 > Minnesota?

- You need to specify your universe!
  - What values x can represent
  - Called the “domain” or “universe of discourse” by the textbook

Universal quantifiers 3

- Let the universe be the real numbers.

- Let $P(x) = x/2 < x$
  - Not true for the negative numbers!
  - Thus, $\forall x\ P(x)$ is false
    - When the domain is all the real numbers

- In order to prove that a universal quantification is true, it must be shown for ALL cases

- In order to prove that a universal quantification is false, it must be shown to be false for only ONE case

Universal quantification 4

- Given some propositional function P(x)

- And values in the universe x_1 .. x_n

- The universal quantification $\forall x\, P(x)$ implies:

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

Existential quantification 1

- Represented by an backwards E: ∃
  - It means “there exists”
  - Let P(x) = x+1 > x
- We can state the following:
  - ∃x P(x)
  - English translation: “there exists (a value of) x such that P(x) is true”
  - English translation: “for at least one value of x, x+1>x is true”

Existential quantification 2

- Note that you still have to specify your universe

- Let $P(x) = x+1 < x$
  - There is no numerical value x for which $x+1<x$
  - Thus, $\exists x\ P(x)$ is false

Existential quantification 3

- Let $P(x) = x+1 > x$
  - There is a numerical value for which $x+1>x$
  - In fact, it's true for all of the values of x!
  - Thus, $\exists\, x\, P(x)$ is true
- In order to show an existential quantification is true, you only have to find ONE value
- In order to show an existential quantification is false, you have to show it's false for ALL values

Existential quantification 4

- Given some propositional function P(x)
- And values in the universe x_1 .. x_n
- The existential quantification $\exists x\, P(x)$ implies:

$$P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$$

A note on quantifiers

- Recall that P(x) is a propositional function
  - Let P(x) be "x == 0"

- Recall that a proposition is a statement that is either true or false
  - P(x) is not a proposition
- There are two ways to make a propositional function into a proposition:
  - Supply it with a value
    - For example, P(5) is false, P(0) is true
  - Provide a quantification
    - For example, $\forall$x P(x) is false and $\exists$x P(x) is true
      - Let the universe of discourse be the real numbers

Binding variables

- Let $P(x,y)$ be $x > y$
- Consider: $\forall x\ P(x,y)$
  - This is not a proposition!
  - What is y?
    - If it's 5, then $\forall x\ P(x,y)$ is false
    - If it's x-1, then $\forall x\ P(x,y)$ is true
- Note that y is not "bound" by a quantifier

Binding variables 2

- $(\exists x\ P(x)) \vee Q(x)$
  - The x in Q(x) is not bound; thus not a proposition
- $(\exists x\ P(x)) \vee (\forall x\ Q(x))$
  - Both x values are bound; thus it is a proposition
- $(\exists x\ P(x) \wedge Q(x)) \vee (\forall y\ R(y))$
  - All variables are bound; thus it is a proposition
- $(\exists x\ P(x) \wedge Q(y)) \vee (\forall y\ R(y))$
  - The y in Q(y) is not bound; this not a proposition

Negating quantifications

- Consider the statement:
  - All students in this class have red hair
- What is required to show the statement is false?
  - There exists a student in this class that does NOT have red hair
- To negate a universal quantification:
  - You negate the propositional function
  - AND you change to an existential quantification
  - $\neg\forall x\ P(x) = \exists x\ \neg P(x)$

Negating quantifications 2

- Consider the statement:
  - There is a student in this class with red hair
- What is required to show the statement is false?
  - All students in this class do not have red hair
- Thus, to negate an existential quantification:
  - To negate the propositional function
  - AND you change to a universal quantification

Translating from English

- What about if the universe of discourse is all students (or all people?)
  - Every student in this class has studied calculus.
  - $\forall x\ (S(x) \wedge C(x))$
    - This is wrong! Why?
  - $\forall x\ (S(x) \rightarrow C(x))$

Translating from English 3

- Consider:
  - "Some students have visited Mexico"
  - "Every student in this class has visited Canada or Mexico"
- Let:
  - $S(x)$ be "x is a student in this class"
  - $M(x)$ be "x has visited Mexico"
  - $C(x)$ be "x has visited Canada"

Translating from English 4

- Consider: “Some students have visited Mexico”
  - Rephrasing: “There exists a student who has visited Mexico”

- $\exists x\ M(x)$
  - True if the universe of discourse is all students

- What about if the universe of discourse is all people?
  - $\exists x\ (S(x) \rightarrow M(x))$
    - This is wrong! Why?
  - $\exists x\ (S(x) \wedge M(x))$

Translating from English 5

- Consider: “Every student in this class has visited Canada or Mexico”

- $\forall x\ (M(x) \vee C(x))$
  - When the universe of discourse is all students

- $\forall x\ (S(x) \rightarrow (M(x) \vee C(x))$
  - When the universe of discourse is all people

Nested Quantifiers

Multiple quantifiers

- You can have multiple quantifiers on a statement

- $\forall x \exists y\ P(x, y)$
  - "For all x, there exists a y such that P(x,y)"
  - Example: $\forall x \exists y\ (x+y == 0)$

- $\exists x \forall y\ P(x,y)$
  - There exists an x such that for all y P(x,y) is true"
  - $\exists x \forall y\ (x*y == 0)$

Order of quantifiers

- $\exists x \forall y$ and $\forall x \exists y$ are not equivalent!

- $\exists x \forall y\ P(x,y)$
  - $P(x,y) = (x+y == 0)$ is false

- $\forall x \exists y\ P(x,y)$
  - $P(x,y) = (x+y == 0)$ is true

Negating multiple quantifiers

- Recall negation rules for single quantifiers:
  - $\neg\forall x\ P(x) = \exists x\ \neg P(x)$
  - $\neg\exists x\ P(x) = \forall x\ \neg P(x)$
  - Essentially, you change the quantifier(s), and negate what it's quantifying

- Examples:
  - $\neg(\forall x \exists y\ P(x,y)) = \exists x\ \neg\exists y\ P(x,y) = \exists x \forall y\ \neg P(x,y)$
  - $\neg(\forall x \exists y \forall z\ P(x,y,z)) = \exists x \neg\exists y \forall z\ P(x,y,z)$ $= \exists x \forall \neg y \forall z\ P(x,y,z) = \exists x \forall y \exists z\ \neg P(x,y,z)$

Negating multiple quantifiers 2

- Consider $\neg(\forall x \exists y\ P(x,y)) = \exists x \forall y\ \neg P(x,y)$
  - The left side is saying "for all x, there exists a y such that P is true"
  - To disprove it (negate it), you need to show that "there exists an x such that for all y, P is false"

- Consider $\neg(\exists x \forall y\ P(x,y)) = \forall x \exists y\ \neg P(x,y)$
  - The left side is saying "there exists an x such that for all y, P is true"
  - To disprove it (negate it), you need to show that "for all x, there exists a y such that P is false"

Translating between English and quantifiers

- The product of two negative integers is positive
  - $\forall x \forall y\ ((x<0) \wedge (y<0) \rightarrow (xy > 0))$
  - Why conditional instead of and?
- The average of two positive integers is positive
  - $\forall x \forall y\ ((x>0) \wedge (y>0) \rightarrow ((x+y)/2 > 0))$
- The difference of two negative integers is not necessarily negative
  - $\exists x \exists y\ ((x<0) \wedge (y<0) \wedge (|x-y| \geq 0))$
  - Why and instead of conditional?
- The absolute value of the sum of two integers does not exceed the sum of the absolute values of these integers
  - $\forall x \forall y\ (|x+y| \leq |x| + |y|)$

Translating between English and quantifiers

- $\exists x \forall y\ (x+y = y)$
  - There exists an additive identity for all real numbers
- $\forall x \forall y\ (((x \geq 0) \wedge (y<0)) \rightarrow (x-y > 0))$
  - A non-negative number minus a negative number is greater than zero
- $\exists x \exists y\ (((x \leq 0) \wedge (y \leq 0)) \wedge (x-y > 0))$
  - The difference between two non-positive numbers is not necessarily non-positive (i.e. can be positive)
- $\forall x \forall y\ (((x \neq 0) \wedge (y \neq 0)) \leftrightarrow (xy \neq 0))$
  - The product of two non-zero numbers is non-zero if and only if both factors are non-zero

Rules of Inference

Valid Arguments

- Assume you are given the following two statements:
  - "you are in this class"
  - "if you are in this class, you will get a grade"
  - Therefore,
  - "You will get a grade"

$$\begin{array}{l} p \rightarrow q \\ \underline{p \qquad\quad} \\ \therefore \quad q \end{array}$$

Definitions

- An Argument in propositional logic is a sequence of propositions.
- All but the final proposition are called premises.
- The final proposition is called conclusion.
- An argument is valid if the truth of all premises implies that the conclusion is true.
  - i.e. $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is a tautology.

Modus Ponens

- Consider $(p \land (p \to q)) \to q$

p	q	$p \to q$	$p \land (p \to q))$	$(p \land (p \to q)) \to q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

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

Modus Ponens example

- Assume you are given the following two statements:
  - "you are in this class"
  - "if you are in this class, you will get a grade"

- Let p = "you are in this class"
- Let q = "you will get a grade"

- By Modus Ponens, you can conclude that you will get a grade

Modus Tollens

- Assume that we know: $\neg q$ and $p \rightarrow q$
  - Recall that $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- Thus, we know $\neg q$ and $\neg q \rightarrow \neg p$
- We can conclude $\neg p$

$$\begin{array}{l} \neg q \\ \underline{p \rightarrow q} \\ \therefore \neg p \end{array}$$

Modus Tollens example

- Assume you are given the following two statements:
  - “you will not get a grade”
  - “if you are in this class, you will get a grade”
- Let p = “you are in this class”
- Let q = “you will get a grade”
- By Modus Tollens, you can conclude that you are not in this class

Addition & Simplification

- Addition: If you know that p is true, then $p \vee q$ will ALWAYS be true

$$\frac{p}{\therefore\ p \vee q}$$

- Simplification: If $p \wedge q$ is true, then p will ALWAYS be true

$$\frac{p \wedge q}{\therefore\ q}$$

Example Proof

- We have the hypotheses:
  - "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"
- Does this imply that "we will be home by sunset"?

- $((\neg p \wedge q) \wedge (r \rightarrow p) \wedge (\neg r \rightarrow s) \wedge (s \rightarrow t)) \rightarrow t$???
  - When
    - 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 of proof

1. $\neg p \wedge q$	1st hypothesis
2. $\neg p$	Simplification using step 1
3. $r \to p$	2nd hypothesis
4. $\neg r$	Modus tollens using steps 2 & 3
5. $\neg r \to s$	3rd hypothesis
6. s	Modus ponens using steps 4 & 5
7. $s \to t$	4th hypothesis
8. t	Modus ponens using steps 6 & 7

More Rules of Inference

- Conjunction: if p and q are true separately, then $p \wedge q$ is true
- Disjunctive syllogism: If $p \vee q$ is true, and p is false, then q must be true
- Resolution: If $p \vee q$ is true, and $\neg p \vee r$ is true, then $q \vee r$ must be true
- Hypothetical syllogism: If $p \rightarrow q$ is true, and $q \rightarrow r$ is true, then $p \rightarrow r$ must be true

Summary: Rules of Inference

Rule	Form	Rule	Form
Modus ponens	$\dfrac{p \qquad p \rightarrow q}{\therefore\ q}$	Modus tollens	$\dfrac{\neg q \qquad p \rightarrow q}{\therefore\ \neg p}$
Hypothetical syllogism	$\dfrac{p \rightarrow q \qquad q \rightarrow r}{\therefore\ p \rightarrow r}$	Disjunctive syllogism	$\dfrac{p \vee q \qquad \neg p}{\therefore\ q}$
Addition	$\dfrac{p}{\therefore\ p \vee q}$	Simplification	$\dfrac{p \wedge q}{\therefore\ p}$
Conjunction	$\dfrac{p \qquad q}{\therefore\ p \wedge q}$	Resolution	$\dfrac{p \vee q \qquad \neg p \vee r}{\therefore\ q \vee r}$

Example Proof

- Example
  - “If it does not rain or if it is not foggy, then the sailing race will be held and the lifesaving demonstration will go on”
    - $(\neg r \vee \neg f) \rightarrow (s \wedge l)$
  - “If the sailing race is held, then the trophy will be awarded”
    - $s \rightarrow t$
  - “The trophy was not awarded”
    - $\neg t$
- Can you conclude: “It rained”?

Example of proof

1. $\neg t$ 3rd hypothesis
2. $s \to t$ 2nd hypothesis
3. $\neg s$ Modus tollens using steps 2 & 3
4. $(\neg r \vee \neg f) \to (s \wedge l)$ 1st hypothesis
5. $\neg(s \wedge l) \to \neg(\neg r \vee \neg f)$ Contrapositive of step 4
6. $(\neg s \vee \neg l) \to (r \wedge f)$ DeMorgan's law and double negation law
7. $\neg s \vee \neg l$ Addition from step 3
8. $r \wedge f$ Modus ponens using steps 6 & 7
9. r Simplification using step 8

Rules of inference for the universal quantifier

- Assume that we know that $\forall x\, P(x)$ is true
  - Then we can conclude that $P(c)$ is true
    - Here c stands for some specific constant
  - This is called “universal instantiation”

- Assume that we know that $P(c)$ is true for any value of c
  - Then we can conclude that $\forall x\, P(x)$ is true
  - This is called “universal generalization”

Rules of inference for the existential quantifier

- Assume that we know that $\exists x\, P(x)$ is true
  - Then we can conclude that $P(c)$ is true for some value of c
  - This is called "existential instantiation"
- Assume that we know that $P(c)$ is true for some value of c
  - Then we can conclude that $\exists x\, P(x)$ is true
  - This is called "existential generalization"

Example of proof

- Given the hypotheses:
  - "Linda, a student in this class, owns a red convertible."
  - "Everybody who owns a red convertible has gotten at least one speeding ticket"
- Can you conclude: "Somebody in this class has gotten a speeding ticket"?

$C(\text{Linda})$

$R(\text{Linda})$

$$\frac{\forall x\, (R(x) \rightarrow T(x))}{\exists x\, (C(x) \wedge T(x))}$$

Example of proof

1. $\forall x\ (R(x) \rightarrow T(x))$	3rd hypothesis
2. $R(Linda) \rightarrow T(Linda)$	Universal instantiation using step 1
3. $R(Linda)$	2nd hypothesis
4. $T(Linda)$	Modes ponens using steps 2 & 3
5. $C(Linda)$	1st hypothesis
6. $C(Linda) \wedge T(Linda)$	Conjunction using steps 4 & 5
7. $\exists x\ (C(x) \wedge T(x))$	Existential generalization using step 6

Thus, we have shown that "Somebody in this class has gotten a speeding ticket"

How do you know which one to use?

- Experience!

- In general, use quantifiers with statements like “for all” or “there exists”

Introduction to Proofs

Proof Methods and Strategy

Terminology

- Theorem: a statement that can be shown true. Sometimes called facts.
  - Proposition: less important theorem
- Proof: Demonstration that a theorem is true.
- Axiom: A statement that is assumed to be true.
- Lemma: a less important theorem that is useful to prove a theorem.
- Corollary: a theorem that can be proven directly from a theorem that has been proved.
- Conjecture: a statement that is being proposed to be a true statement.

Direct proofs

- Consider an implication: $p \to q$
  - If p is false, then the implication is always true
  - Thus, show that if p is true, then q is true
- To perform a direct proof, assume that p is true, and show that q must therefore be true

- Show that the square of an even number is an even number
  - Rephrased: if n is even, then n^2 is even

(Proof) Assume n is even

Thus, $n = 2k$, for some k (definition of even numbers)

$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$

As n^2 is 2 times an integer, n^2 is thus even

Indirect proofs

- Consider an implication: $p \rightarrow q$
  - It's contrapositive is $\neg q \rightarrow \neg p$
    - Is logically equivalent to the original implication!
  - If the antecedent ($\neg q$) is false, then the contrapositive is always true
  - Thus, show that if $\neg q$ is true, then $\neg p$ is true
- To perform an indirect proof, do a direct proof on the contrapositive

Indirect proof example

- If n^2 is an odd integer then n is an odd integer
- Prove the contrapositive: If n is an even integer, then n^2 is an even integer
- Proof: n=2k for some integer k (definition of even numbers)
- $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$
- Since n^2 is 2 times an integer, it is even
- When do you use a direct proof versus an indirect proof?

Example of which to use

- Prove that if n is an integer and n^3+5 is odd, then n is even

- Via direct proof
  - $n^3+5 = 2k+1$ for some integer k (definition of odd numbers)
  - $n^3 = 2k-4$
  - Umm… ???

- So direct proof didn't work out. So: indirect proof
  - Contrapositive: If n is odd, then n^3+5 is even
  - Assume n is odd, and show that n^3+5 is even
  - $n=2k+1$ for some integer k (definition of odd numbers)
  - $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
  - As $2(4k^3+6k^2+3k+3)$ is 2 times an integer, it is even

Proof by contradiction

- Given a statement p, assume it is false
  - Assume ¬p
- Prove that ¬p cannot occur
  - A contradiction exists
- Given a statement of the form p→q
  - To assume it's false, you only have to consider the case where p is true and q is false

Proof by contradiction example 1

- Theorem (by Euclid): There are infinitely many prime numbers.

- Proof. Assume there are a finite number of primes
- List them as follows: p_1, p_2 …, p_n.
- Consider the number $q = p_1 p_2 \ldots p_n + 1$
  - This number is not divisible by any of the listed primes
    - If we divided p_i into q, there would result a remainder of 1
  - We must conclude that q is a prime number, not among the primes listed above
  - This contradicts our assumption that all primes are in the list
    - p_1, p_2 …, p_n.

Proof by contradiction example 2

- Prove that if n is an integer and n^3+5 is odd, then n is even
- Rephrased: If n^3+5 is odd, then n is even

- Assume p is true and q is false
  - Assume that n^3+5 is odd, and n is odd
- $n=2k+1$ for some integer k (definition of odd numbers)
- $n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+6 = 2(4k^3+6k^2+3k+3)$
- As $2(4k^3+6k^2+3k+3)$ is 2 times an integer, it must be even
- Contradiction!

Vacuous and Trivial proofs

- Vacuous proof
  - Consider an implication: $p \rightarrow q$
  - If it can be shown that p is false, then the implication is always true
    - By definition of an implication

- Trivial Proof
  - Consider an implication: $p \rightarrow q$
  - If it can be shown that q is true, then the implication is always true
    - By definition of an implication

Proof methods

- We will discuss ten proof methods:
  1. Direct proofs
  2. Indirect proofs
  3. Vacuous proofs
  4. Trivial proofs
  5. Proof by contradiction