Announcements

- Teaching Assistant: Pan Fang
  - Office: Stanley Thomas 309
  - Office hours: Tue 3:30-5:30 pm
  - Email: pfang@tulane.edu
- Quiz 1 is on this Thursday
- Class participation (5% - extra credit)
  - Raising and answering questions
  - Presenting solutions to homework problems in the labs
- Class enrollment: “free to all” after this Friday

Propositional Logic

CMPS/MATH 2170: Discrete Mathematics

Logic and Proofs

- Logic is the basis of mathematical reasoning
  - gives precise meaning to mathematical statements
  - provides rules to construct a correct mathematical argument: a proof
- Proofs are used in computer science to establish
  - correctness of a computer program
  - complexity of a computing problem
  - performance of an algorithm
  - security of a system
  - …

Outline

- Propositional logic (2 lectures)
- Predicate logic (2 lectures)
- Proofs (3-4 lectures)

Propositional logic

- Two building blocks (1.1)
  - Propositions
  - Logical operators
- Applications (1.2)
  - System specification, logical circuits, etc.
- Key learning outcome
  - Establish the logical equivalence of two mathematical statements (1.3)

Propositions

- Definition: A *proposition* is a declarative sentence that is either true or false, but not both
- Examples
  - The French Quarter is in located in New Orleans — proposition — true
  - $\sqrt{2}$ is rational — proposition — false
  - When is the midterm? — Not a proposition
  - $x^2 \geq 0$ for all real numbers x — proposition — true
  - $x + y = 5$ — Not a proposition

Propositions

- The value of a proposition is either true (T) or false (F), called its truth value
- Propositional variables: $p, q, r, s, \ldots$
- *Compound propositions* can be formed from simple propositions using connectives (logical operators)

Negation ¬

- Let p be a proposition. The *negation* of p, denoted by $\neg p$, is a proposition with the opposite truth value than the truth value of p.
  - Read $\neg p$ as: "not p" or "It is not the case that p"
- Example:
  - Let p denote "The French Quarter is located in New Orleans"
  - $\neg p$ can be stated as

    "The French Quarter is *not* located in New Orleans"

    "It is *not* the case that the French Quarter is located in New Orleans"

Truth Table

p	$\neg p$
T	F
F	T

Conjunction $\wedge$

- Let p and q be two propositions. The *conjunction* of p and q, denoted by $p \wedge q$, is true when both p and q are true, and is false otherwise.
  - Read $p \wedge q$ as "p and q"

Truth Table

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

- Example
  - p = "$\sqrt{2}$ is rational", q = "$x^2 \geq 0$ for all real numbers x"
  - $p \wedge q$ = "$\sqrt{2}$ is rational and $x^2 \geq 0$ for all real numbers x", which is false

Disjunction $\vee$

- Let p and q be two propositions. The *disjunction* of p and q, denoted by $p \vee q$, is false when both p and q are false, and is true otherwise.
  - Read $p \vee q$ as "p or q"

Truth Table

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

- Example

  p = "$\sqrt{2}$ is rational", q = "$x^2 \geq 0$ for all real numbers x"

  $p \vee q$ = "$\sqrt{2}$ is rational or $x^2 \geq 0$ for all real numbers x", which is true

Inclusive Or vs. Exclusive Or

- "Students who have taken calculus or intro to CS can take this class"
  - a student can take this class if the student has taken either calculus or intro to CS or both.
  - Inclusive Or corresponds to Disjunction
- "Students who have taken calculus or intro to CS, but not both, can take this class"
  - Exclusive Or
- Natural language can be ambiguous: e.g., "Soup or salad comes with an entrée"

Exclusive Or $\oplus$

- Let p and q be two propositions. The *exclusive or* of p and q, denoted by $p \oplus q$, is true when exactly one of p and q is true, and is false otherwise.
  - Read $p \oplus q$ as "p xor q", "p or q, but not both"

Truth Table

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

Conditional Statements $\rightarrow$

- Example: "If I am elected, then I will lower taxes"
  - We can write it as $p \rightarrow q$ where p = "I am elected", q = "I will lower taxes"
  - When is this proposition *true* and when is it *false*?
    - If I am elected and I lower taxes => *true*
    - If I am elected but I do not lower taxes => *false*
    - If I am not elected => *true*

Conditional Statements $\rightarrow$

- Let p and q be two propositions. The *conditional statement* $p \rightarrow q$ is false when p is true and q is false, and true otherwise. p is called hypothesis (or antecedent or premise) and q is called conclusion (or consequence)

Truth Table

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

  - Read $p \rightarrow q$ as "p implies q"
    "if p, then q"
    "q if p"
    "p only if q"
    "p is a sufficient condition for q"
    "q is a necessary condition for p", etc.

Biconditional Statements $\leftrightarrow$

- Let p and q be two propositions. The *biconditional statement* $p \leftrightarrow q$ is true when p and q have the same truth value, and is false otherwise.
  - Read $p \leftrightarrow q$ as "p if and only if q" "p iff q"
    "p is necessary and sufficient for q"

Truth Table

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

- Example
  - p = "it is sunny", q = "we will go to beach"

    $p \leftrightarrow q$ = "We will go to beach if and only if it is sunny", which means
    - If it is sunny, then we will definitely go to beach
    - If it is not sunny, then we will definitely not go to beach

Biconditional Statements

- Ex: check that $p \leftrightarrow q$ has the same truth value as $(p \rightarrow q) \wedge (q \rightarrow p)$

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow p)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Propositional Forms

- A *propositional form* (or *logical expression*) is an expression involving propositional variables and connectives such that, if all the variables are replaced by propositions then the form becomes a (compound) proposition.

- Ex: $(\neg p \rightarrow q) \vee (p \wedge q)$

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

Precedence of logical operators:

highest ¬
∧
∨
→
lowest ↔

System Specifications

- System and software engineers take requirements in English and express them in a precise specification language based on logic.
- Ex: Express in propositional logic:

"The automated reply cannot be sent when the file system is full"

- One possible solution
  - p – "The automated reply can be sent", q – "The file system is full."
  - We can write the statement as:

$$q \rightarrow \neg p$$

Consistent System Specifications

- **Definition**: A list of propositions is *consistent* if it is possible to assign truth values to the proposition variables so that each proposition is true.
- Ex: Are these specifications consistent?

"The diagnostic message is stored in the buffer **or** it is retransmitted." $p \vee q$

(p: "The diagnostic message is stored in the buffer"; q: "it is retransmitted")

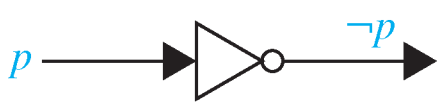
"The diagnostic message is **not** stored in the buffer." $\neg p$

"**If** the diagnostic message is stored in the buffer, **then** it is retransmitted." $p \rightarrow q$

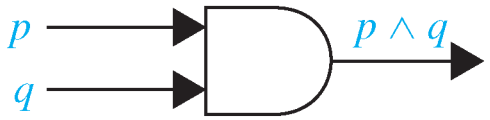
Yes, we can set $p = \text{F}, q = \text{T}$

Logical Circuits

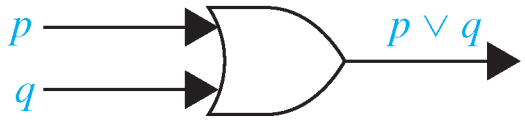
- A logical circuit (or digital circuit) receives input signals $p_1, p_2, \ldots, p_n$, each a bit [either 0 (off) or 1 (on)], and produces output signals
  - 0 – False, 1 – True
  - Focus on circuits with a single output signal
- Three basic circuits (gates)



Inverter



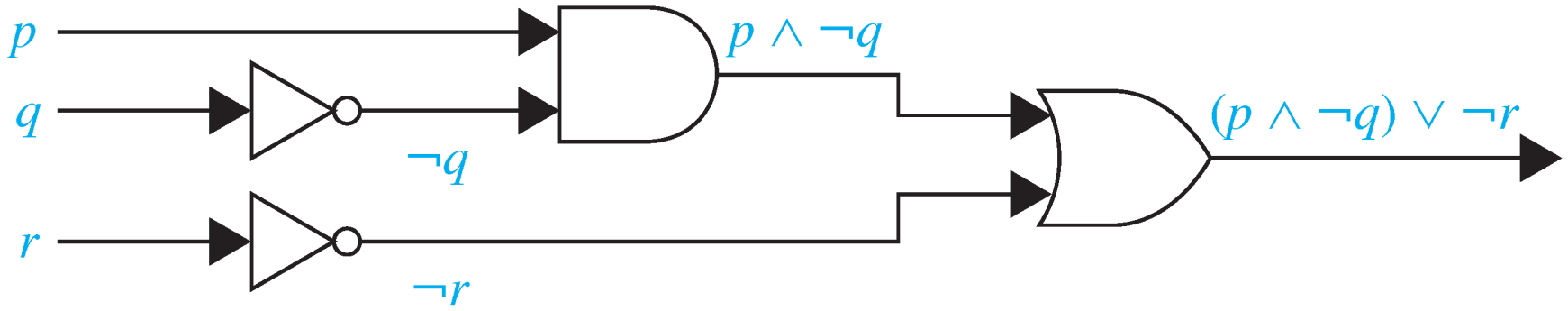
AND gate



OR gate

Logical Circuits

- A combinatorial circuit



- More in Section 1.2 and Chapter 12

Review

- *Proposition:* a declarative sentence that is either true or false, but not both
- *Compound propositions* can be formed from simple propositions using *connectives*: $\neg$, $\wedge$, $\vee$, $\oplus$, $\rightarrow$, $\leftrightarrow$
- *Propositional form:* an expression involving propositional variables and connectives
  - A propositional form is also called a compound proposition in the textbook
  - Can be studied using truth table
- Applications: system specifications, logical circuits

Logical Equivalences

- We have seen that $p \leftrightarrow q$ has the same truth value as $(p \rightarrow q) \wedge (q \rightarrow p)$, i.e., that are logically equivalent
- Two propositional forms A and B are logically equivalent if they have the same truth table, denoted by $A \equiv B$
- Why interested in logical equivalence?
  - Construct proofs: replacing a statement with another statement with the same truth value
  - Simplify logical expressions: circuit minimization

De Morgan's Laws

- Find the negation of

"Heather will go to the concert or Steve will go to the concert" $p \vee q$

p q

"It's not the case that Heather will go to the concert or Steve will go to the concert $\neg(p \vee q)$

$\equiv$ "Heather will not go to the concert and Steve will not go to the concert" $\neg p \wedge \neg q$

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

De Morgan's Laws

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

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

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

Augustus De Morgan
(from Wikipedia)

Using De Morgan's Laws

- Text Searching

  p = The document contains the word "laptop"

  q = The document contains the word "phone"

  $\neg(p \vee q)$ = The document does not contain the words "laptop" or "phone"

  $\neg p \wedge \neg q$ = The document does not contain the word "laptop" and the document does not contain the word "phone"

Logical Equivalences

- A propositional form is called a tautology if it is always true (**T**)
  - A propositional form is called a tautology if no matter what the truth values of the propositional variables that occur in it, the compound proposition obtained is always true.
  - E.g., $p \vee \neg p$
- Ex: Determine if $\neg(p \rightarrow q) \rightarrow p$ is a tautology
- A propositional form is called a contradiction if it is always false (**F**)
  - E.g., $p \wedge \neg p$
- A and B are logically equivalent if $A \leftrightarrow B$ is a tautology.

Logical Equivalences

- How to prove logical equivalence?
  - Using truth tables
    - A truth table with n variables has 2^n rows
  - Using known logical equivalence to establish new ones
    - First establish a list of key logical equivalences

Key Logical Equivalences

- Identity laws: $p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$
- Domination laws: $p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$
- Idempotent laws: $p \vee p \equiv p$ $p \wedge p \equiv p$
- Double negation law: $\neg(\neg p) \equiv p$
- Negation laws: $p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$

➢ p and q can be substituted by any propositional forms.

Key Logical Equivalences

- Commutative laws: $p \vee q \equiv q \vee p \quad p \wedge q \equiv q \wedge p$
- Associative laws: $(p \vee q) \vee r \equiv p \vee (q \vee r) \quad (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
- Distributive Laws: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
  $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
- De Morgan's laws: $\neg(p \wedge q) \equiv \neg p \vee \neg q \quad \neg(p \vee q) \equiv \neg p \wedge \neg q$
- Absorption laws: $p \vee (p \wedge q) \equiv p \quad p \wedge (p \vee q) \equiv p$

Key Logical Equivalences

- Implication law: $p \rightarrow q \equiv \neg p \vee q$
- Contrapositive law: $p \rightarrow q \equiv \neg q \rightarrow \neg p$
- Logical equivalences involving biconditional statements

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

$$p \leftrightarrow q \equiv \neg q \leftrightarrow \neg p$$

Announcement

- Office hours next week: Tuesday and Wednesday 11-12 pm

Proving Logical Equivalences

- Using truth tables
- Using known logical equivalences to prove new ones
  - Substitution

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

  - To prove $A \equiv B$, we produce a series of equivalences beginning with A and ending with B

$$A \equiv A_1$$
$$A_1 \equiv A_2$$
$$\vdots$$
$$A_n \equiv B$$

Constructing New Logical Equivalences

- Use known logical equivalences to prove the following:

$$\neg(p \rightarrow q) \equiv\ p \wedge \neg q$$

$$(p \wedge q) \rightarrow (p \vee q) \equiv \mathbf{T}$$

Representing Truth Tables

- Q: Given a truth table, how to find a logical expression that represents it?
  - E.g.: how to design a digital circuit that implements a given truth table?
- A: any truth table can be represented by a logical expression using only three operators: {$\wedge$, $\vee$, $\neg$}
  - Any logical expression has a Disjunctive Normal Form (DNF)
  - Section 1.3 Exercise 42, Section 12.2

Disjunctive Normal Form (DNF)

p	q	$f(p,q)$
T	T	F
T	F	T
F	T	T
F	F	T

$$f(p,q) \equiv (p \wedge \neg q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$$

p	q	r	$f(p,q,r)$
T	T	T	F
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	F

$$f(p,q,r) \equiv (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r)$$

Disjunctive Normal Form (DNF)

p	q	$f(p,q)$
T	T	F
T	F	T
F	T	T
F	F	T

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

- A literal: a propositional variable or its negation, e.g., p, $\neg p$, q, $\neg q$
- A minterm: a conjunction of distinct literals, $p \wedge \neg\, q$, $\neg p \wedge q$, $\neg p \wedge \neg q$
- A Disjunctive Normal Form: a disjunction of distinct minterms (disjunction of conjunctions)

Functional Completeness

- We have just shown that {∧, ∨, ¬} is functionally complete
  - A set of logical operators are called functionally complete if every truth table can be represented using them
  - Section 1.3 Exercise 43, Section 12.2
- {∧, ¬} is functionally complete
  - It is sufficient to show that $p \vee q \equiv \neg(\neg p \wedge \neg q)$
- {∨, ¬} is functionally complete
- {∧, ∨} is not functionally complete

Functional Completeness

- Q: Is it possible to use only one operator to represent all truth tables?
- A: Yes, use $NAND$ or NOR (see HW2)

Truth Table for NOR ($\downarrow$)

p	q	$p \downarrow q$
T	T	F
T	F	F
F	T	F
F	F	T

Propositional logic

- Two building blocks (1.1)
  - Propositions
  - Logical operators
- Applications (1.2)
  - System specification, logical circuits, etc.
- Key learning outcome
  - Establish the logical equivalence of two mathematical statements (1.3)
  - Functional completeness (12.2)

Predicate Logic

CMPS/MATH 2170: Discrete Mathematics

Predicates and Quantifiers

- Develop terminology to express more complicated statements mathematically

"Every computer in this network is functioning properly"

∀ Subject x Domain D Predicate $P(x)$ $\forall x \in D: P(x)$

"There exists an $x \in \mathbb{R}$ such that $x > 3$"

∃ x Domain $Q(x)$ $\exists x \in \mathbb{R}: Q(x)$

"There exist $x, y \in \mathbb{R}$ such that $x = y + 3$"

$R(x, y)$ $\exists\, x \in \mathbb{R}, y \in \mathbb{R}: R(x, y)$

Propositional Functions

- A statement $P(x_1, x_2, \ldots, x_n)$ is the value of a propositional function P at the the n-tuple $(x_1, x_2, \ldots, x_n)$
  - P is also called an n-place predicate
- Examples
  - Let $Q(x)$ denote the statement "$(x > 3) \vee (x < -1)$", then $Q(2) = F$ $Q(4) = T$
  - Let $R(x, y)$ denote the statement "$x = y + 3$", then $R(1,2) = F$
- Create a proposition from a propositional function
  - Assign values to $x_1, x_2, \ldots, x_n$
  - use quantifiers

Universal Quantifier

- Definition: The statement "$P(x)$ for all values x in the domain" is called the "universal quantification" of $P(x)$. We denote it by

  $\forall x\ P(x)$: read as "for all x $P(x)$" or "for every x $P(x)$"

  $\forall$ is called the "universal quantifier"

- $\forall x\ P(x)$ is true if $P(x)$ is true for every x in the domain
- $\forall x\ P(x)$ is false if there is an x in the domain for which $P(x)$ is false
  - an element x for which $P(x)$ is false is called a counterexample of $\forall x\ P(x)$

Universal Quantifier

- True or False?

$\forall x \in \mathbb{R}: x + 1 > x$ True

$\equiv \forall x: x + 1 > x$ where the domain is the real numbers

$\equiv \forall x\ (x + 1 > x)$ where the domain is the real numbers

Universal Quantifier

- True or False?

$\forall x:\ x^2 > 0$ where the domain is all integers $\mathbb{Z}$ False

$\forall x:\ x^2 > 0$ where the domain is all non-zero integers $\mathbb{Z}\backslash\{0\}$ True

Universal Quantifier

- True or False: $\forall x: x^2 < 10$ where the domain consists of the positive integers not exceeding 4 False
  - Let $P(x)$ denote the statement "$x^2 < 10$"
  - Then $\forall x\, P(x)$ is the same as $P(1) \wedge P(2) \wedge P(3) \wedge P(4)$
- If the elements in the domain can be listed, say, $x_1, x_2, \ldots, x_n$, then

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

Existential Quantifier

- Definition: The statement "There exisits an element x in the domain such that $P(x)$" is called the "existential quantification" of $P(x)$. We denote it by

  $\exists x\ P(x)$: read as "There is an x such that $P(x)$" or "For some x $P(x)$"

  $\exists$ is called the "existential quantifier"

- $\exists x\ P(x)$ is true if there is an x in the domain for which $P(x)$ is true
- $\exists x\ P(x)$ is false if $P(x)$ is false for every x in the domain
- True or False?

  $\exists x\ (x > 3)$ where the domain is the real numbers — True

  $\exists x\ (x = x + 1)$ where the domain is the real numbers — False

Existential Quantifier

- True or False: $\exists x: x^2 < 10$ where the domain consists of the positive integers not exceeding 4 True
  - Let $P(x)$ denote the statement "$x^2 < 10$"
  - Then $\exists x\ P(x)$ is the same as $P(1) \vee P(2) \vee P(3) \vee P(4)$
- If the elements in the domain can be listed, say, $x_1, x_2, \ldots, x_n$, then

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

Examples

Express these mathematical statements using predicates, quantifiers, logical connectives, and mathematical operators, where the domain consists of all real numbers.

"There exists a number that is equal to itself squared." $\exists x: x = x^2$

$\exists$ x $x = x^2$

"The square of any number is nonnegative." $\forall x: x^2 \geq 0$

x^2 $\forall$ x $x^2 \geq 0$

Quantifiers with Restricted Domains

"Every computer in this network is functioning properly"

$\forall$	x	Domain D	Predicate $P(x)$

$\forall x \in D\colon P(x) \equiv \forall x \left(x \in D \rightarrow P(x)\right)$

"For every computer, if it is in this network, then it is functioning properly"

"Some computer in this network is functioning properly"

$\exists x \in D\colon P(x) \equiv \exists x \left(x \in D \wedge P(x)\right)$

"There is a computer such that it is in this network and it is functioning properly"

Logical Equivalences

- Definition: Two statements involving predicates and quantifiers are logically equivalent if and only if they have the same truth value no matter which predicates are substituted into these statements and which domain is used for the variables

- Ex: $\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$ (where the same domain is used throughout)

Negating Quantified Expressions

"Every computer in this network is functioning properly" $\forall x\, P(x)$

"Not every computer in this network is functioning properly" $\neg\forall x\, P(x)$

$\equiv$ "There is a computer in this network that is not functioning properly" $\exists x\, \neg P(x)$

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

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

(De Morgan's laws for quantifiers)

Negating Quantified Expressions

De Morgan's laws for quantifiers

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

When the domain has n elements $x_1, x_2, \ldots, x_n$

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

$$\neg \forall x\, P(x) \equiv \neg \left(P(x_1) \wedge P(x_2) \wedge \ \ldots \wedge P(x_n)\right)$$

$$\equiv \neg P(x_1) \vee \neg P(x_2) \vee \ \ldots \vee \neg P(x_n) \qquad \text{(De Morgan's laws)}$$

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

Negating Quantified Expressions

- Ex.1: What is the negation of $\forall x\ (x^2 > x)$ $\exists x\ (x^2 \leq x)$

- Ex.2: Show that $\neg\forall x(P(x) \rightarrow Q(x)) \equiv \exists x\ (P(x) \wedge \neg Q(x))$

Nested Quantifiers

- Ex.1: Every real number has an inverse

  "For any $x \in \mathbb{R}$, there exist $y \in \mathbb{R}$ such that $x + y = 0$"

  $P(x) = \exists y \in \mathbb{R}\ (x + y = 0)$

$\forall x \in \mathbb{R}\ (\exists y \in \mathbb{R}\ (x + y = 0))$

$\forall x\ \exists\ y\ (x + y = 0)$ where the domain for x and y consists of all real numbers

Nested Quantifiers

- Ex.2: $\forall x \, \exists \, y \, (x + y = 0)$ True

  $\exists y \forall x \, (x + y = 0)$ false $\Rightarrow$ the order of quantifiers matters

  In general, $\forall x \exists y \, P(x, y) \not\equiv \exists y \forall x \, P(x, y)$

- Ex.3: Commutative law for the addition of real numbers

  $\forall x \forall y \, (x + y = y + x)$ where the domain consists of all real numbers

Nested Quantifiers

- Ex. 4: The sum of two positive integers is positive

  $\forall x \forall y: (x > 0 \wedge y > 0) \rightarrow (x + y > 0)$ where the domain is all integers

- Ex. 5 $\lim_{x \to a} f(x) = L$ where $f: \mathbb{R} \rightarrow \mathbb{R}$

  $\forall \epsilon > 0 \; \exists \delta > 0 \; \forall x: 0 < |x - a| < \delta \rightarrow |f(x) - L| < \epsilon$

  where the domain is real numbers

Negation of Nested Quantifiers

Q: What is the negation of $\exists y \forall x\ (x + y = 0)$?

A: $\neg \exists y \forall x\ (x + y = 0) \equiv \forall y \neg \forall x\ (x + y = 0)$

$\equiv \forall y \exists x\ \neg (x + y = 0)$

$\equiv \forall y \exists x\ (x + y \neq 0)$

Introduction to Proofs

CMPS/MATH 2170: Discrete Mathematics

Introduction to Proofs

- Rules of Inference (1.6)
- Basic Proof Techniques (1.7)
- More Proof Techniques (1.8)

Proofs and Valid Arguments

- Mathematical Proof = Sequence of valid arguments that establish the truth of a mathematical statement
- An argument: a sequence of propositions that end with a conclusion
- A valid argument: it is impossible for all the premises to be true and the conclusion to be false

$$\begin{array}{ll} p_1 & \\ p_2 & \text{premises (hypothesis)} \\ \vdots & \\ p_n & \\ \hline \therefore\ q & \text{conclusion} \end{array}$$

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q \equiv \mathbf{T}$$

- Rules of inference: simple valid argument forms (templates of valid arguments)

Rules of Inference

Ex.1:

premises
- "If you have a current password, then you can log onto the network."
  p q
- "You have a current password"
  p

Therefore,

conclusion "You can log onto the network"
q

$p \rightarrow q$

p

$\therefore \ q$

$\big((p \rightarrow q) \wedge p\big) \rightarrow q \equiv \mathbf{T}$ Modus ponens (Latin for "mode that affirms by affirming")

Rules of Inference

Ex.2 "If you have a current password, then you can log onto the network."

p q

$p \rightarrow q$

"You cannot log onto the network"

$\neg q$

$\neg q$

Therefore,

"You don't have a current password"

$\neg p$

$\therefore \neg p$

$((p \rightarrow q) \wedge \neg q) \rightarrow \neg p \equiv \mathbf{T}$ Modus tollens (Latin for "mode that denies by denying")

Rules of Inference

Ex.3:

It is below freezing now p

Therefore, it is either below freezing or raining now $p \vee q$

$$\frac{p}{\therefore\ p \vee q}$$ (addition)

Ex.4:

It is below freezing and raining now. $p \wedge q$

Therefore, it is below freezing now p

$$\frac{p \wedge q}{\therefore\ p}$$ (simplification)

TABLE 1 **Rules of Inference.**

Rule of Inference	*Tautology*	*Name*
p $p \rightarrow q$ $\therefore q$	$(p \wedge (p \rightarrow q)) \rightarrow q$	Modus ponens
$\neg q$ $p \rightarrow q$ $\therefore \neg p$	$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$	Modus tollens
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \rightarrow q$	Disjunctive syllogism

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

Using Rules of Inference to Build Arguments

Ex.5: Suppose all these statements are known:

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

Rules of Inference for Propositional Logic

Ex.6: Show that:

premises

"If you send me an e-mail message, then I will finish writing the program" — p, q — $p \rightarrow q$

"If you do not send me an e-mail message, then I will go to sleep early" — $\neg p$, r — $\neg p \rightarrow r$

"If I go to sleep early, then I will wake up feeling refreshed" — r, s — $r \rightarrow s$

conclusion

$\Rightarrow$ "If I do not finish writing the program, then I will wake up feeling refreshed" — $\neg q$, s — $\neg q \rightarrow s$

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

Ex.7: Show that

"A student in this class has not read the book", and — $\exists x: C(x) \wedge \neg B(x)$

($\exists x$: A student; $C(x)$: in this class; $\neg B(x)$: has not read the book)

"Everyone in this class passed the first exam" — $\forall x: C(x) \rightarrow P(x)$

($\forall x$: Everyone; $C(x)$: in this class; $P(x)$: passed the first exam)

imply the conclusion

"Someone who passed the first exam has not read the book" — $\exists x: P(x) \wedge \neg B(x)$

($\exists x$: Someone; $P(x)$: who passed the first exam; $\neg B(x)$: has not read the book)

$\exists x: C(x) \wedge \neg B(x)$

$\forall x: C(x) \rightarrow P(x)$

$\exists x: P(x) \wedge \neg B(x)$

1.	$\exists x: C(x) \wedge \neg B(x)$	Premise
2.	$C(a) \wedge \neg B(a)$	Existential instantiation from (1)
3.	$C(a)$	Simplification from (2)
4.	$\forall x: C(x) \rightarrow P(x)$	Premise
5.	$C(a) \rightarrow P(a)$	Universal instantiation from (4)
6.	$P(a)$	Modus ponens from (3) and (5)
7.	$\neg B(a)$	Simplification from (2)
8.	$P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9.	$\exists x: P(x) \wedge \neg B(x)$	Existential generalization from (8)

Introduction to Proofs

Proof: Sequence of valid arguments that establish the truth of a theorem

Theorem: A proposition that can be proved to be true

- Lemma: simple "helper" theorem
- Corollary: An almost immediate implication of a theorem
- Conjecture: proposition for which it is not known whether it is true or false

- Formal vs. informal proofs
- We will assume usual axioms regarding real numbers and integers (Appendix 1) and geometry.

Direct Proofs

- Want to show $p \rightarrow q$
- Assume p is true. Construct a sequence of implications using rules of inference, with the final step showing that q must also be true
- Give a direct proof of the theorem

  Theorem 1: If $\underbrace{n \text{ is an odd integer}}_{p}$, then $\underbrace{n^2 \text{ is odd}}_{q}$

  Theorem 1': For all integers $n \in \mathbb{Z}$, if n is an odd integer, then n^2 is odd

- To prove $\forall x: P(x) \rightarrow Q(x)$, show that $P(c) \rightarrow Q(c)$ for an arbitrary element c in the domain, and then apply universal generalization

Direct Proofs

- Theorem 1: If n is an odd integer, then n^2 is odd

- Definition: The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$.

Proof by Contraposition

- Want to prove: $p \rightarrow q$
- Actually prove: $\neg q \rightarrow \neg\, p$
- This is ok because $p \rightarrow q \equiv\ \neg q \rightarrow \neg\, p$ (contrapositive law)

Theorem 2: if n is an integer and n^2 is odd, then n is odd

Theorem 1': if n is an integer and n^2 is even, then n is even

Proofs by Contradiction

- Want to prove: p
- Actually prove: $\neg p \rightarrow \mathbf{F}$
- This is ok because $p \equiv \neg p \rightarrow \mathbf{F}$
- How to find a contradiction? $\neg p \rightarrow (q \wedge \neg q)$ for some q

Theorem 3: $\sqrt{2}$ is irrational

Fact: for every rational number r, there exist integers a and b with $r = a/b$, where $b \neq 0$ and a and b have no common factors.

Proofs of Equivalence

- Want to prove: $p \leftrightarrow q$
- Actually prove: $(p \rightarrow q) \wedge (q \rightarrow p)$
- This is ok because $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Theorem 4: If n is an integer, then $\underbrace{n \text{ is odd}}_{p}$ if and only if $\underbrace{n^2 \text{ is odd}}_{q}$

Proof:

$p \rightarrow q$: follows from Theorem 1 "If n is an odd integer, then n^2 is odd"

$q \rightarrow p$: follows from Theorem 2 "if n is an integer and n^2 is odd, then n is odd"

Proofs of Equivalence

- Want to prove: $p \leftrightarrow q \leftrightarrow r$
- Option 1: Prove $p \rightarrow q$

  $q \rightarrow p$

  $q \rightarrow r$

  $r \rightarrow q$

- Option 2: Prove $p \rightarrow q$

  $q \rightarrow r$

  $r \rightarrow p$

Proof by Cases

- Wants to show $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$
- Actually prove: $p_1 \rightarrow q$

  $p_2 \rightarrow q$

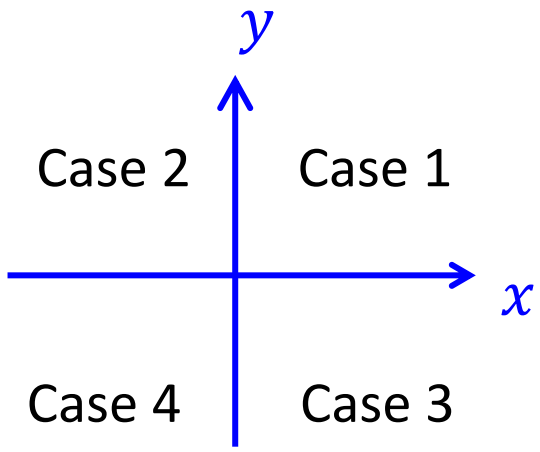
  $\vdots$

  $p_n \rightarrow q$
- This is ok because $(p_1 \vee p_2 \ldots \vee p_n) \rightarrow q$

  $\equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$

Proof by Cases

- Wants to show $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$
- Actually prove: $p_1 \rightarrow q$
  $p_2 \rightarrow q$
  $\vdots$
  $p_n \rightarrow q$



Theorem 5: $|xy| = |x||y|$ for any real numbers x and y

Theorem 6: there are no solutions in integers x and y of $x^2 + 3y^2 = 8$

Existence Proofs

- Want to prove $\exists x: P(x)$

Theorem 7: There is a positive integer that can be written as the sum of cubes of positives in two different ways.

Proof: Constructive existence proof: Find a such that $P(a)$ is true

Exhaustive search (computer):

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

Theorem 8: Show that there exist irrational numbers x and y such that x^y is rational

Proof: Non-constructive existence proof: consider $\sqrt{2}^{\sqrt{2}}$

Uniqueness Proofs

- Want to show there is a unique x such that $P(x)$
  - Existence: there is an x has the desired property
  - Uniqueness: for any $y \neq x$, y does not have the property

Theorem 9: if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Counterexamples

- Want to disprove $\forall x: P(x)$
- It is sufficient to find a counterexample a such that $P(a) = F$

Ex: Prove or disprove: every positive integer is the sum of squares of two integers

$3 \neq 0^2 + 0^2,\ 3 \neq 0^2 + 1^2, 3 \neq 1^2 + 1^2, 3 \neq 2^2 + x^2$ for any $x \in \mathbb{Z}$

$\Rightarrow 3$ is a counterexample

Forward Reasoning vs. Backward Reasoning

Theorem 10: $(x + y)/2 > \sqrt{xy}$ for all positive distinct x, y

Proof 1: backward reasoning

$$(x + y)/2 > \sqrt{xy}$$

$(x + y)^2/4 > xy \rightarrow (x + y)/2 > \sqrt{xy}$

$$(x + y)^2/4 > xy$$

true because x and y are positive

$$(x + y)^2 > 4xy$$

$$x^2 + 2xy + y^2 > 4xy$$

$$x^2 - 2xy + y^2 > 0$$

$$(x - y)^2 > 0$$

true because $x \neq y$

Proof 2: forward reasoning