Math/CSE 1019C:
Discrete Mathematics for Computer Science
Fall 2012

Jessie Zhao
jessie@cse.yorku.ca

Course page:
http://www.cse.yorku.ca/course/1019

Several announcements

- Lecture Notes, readings and exercises
  - Go to course website, and click on "Lectures"
- Assignment 1
  - Go to course website, and click on "Assignments"
  - Due on Sep 24th, 1:00pm
  - No late submissions
  - Read the academic honesty and the instructions before you work on your assignment.
- About Moodle
  - Include Announcements and links to the course website.
  - Course website is the best place to check.

- When update?
  - Lecture notes: One day before the lecture
  - Assignments: Same day of the lecture
  - Readings for the next lecture: One day after the lecture
  - Announcements
- TA office hours
  - Monday 1-2pm, Tuesday 7-8pm (LAS 2013)

Review (Ch 1.1 – 1.3)

- Proposition: Declarative & (True/False)
- Operations: $\neg \wedge \vee \rightarrow \leftrightarrow$
  - $p \rightarrow q \equiv \neg p \vee q$
  - $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$
- Logically Equivalence
  - Use truth table
  - Use laws to prove (Page27)

Think about this question:

- How many rows appear in a truth table?
  - $\neg p \vee p$
  - $p \wedge q$,
  - $\neg p \wedge q \wedge (r \vee q)$
  - More?
  - 2^n

- $p \rightarrow q \equiv \neg p \vee q$
  - Value is False when p is true and q is false (by definition & truth table)
  - Example:
    - p: Emily buys the ticket
    - q: she goes to the concert
    - $p \rightarrow q$: If Emily buys the ticket, she goes to the concert.

p	q	$p \rightarrow q$	$\neg p$	$\neg p \vee q$	
T	T	T	F	T	Emily buys the ticket, and she goes to the concert.
T	F	F	F	F	Emily buys the ticket, and she does not go to the concert.
F	T	T	T	T	Emily does not buy the ticket, and she goes to the concert.
F	F	T	T	T	Emily does not buy the ticket, and she does not go to the concert.

Review (Ch 1.4 – 1.5)

- Predicate: Proposition with variables
- Quantifiers
  - $\forall$ "For all…"
  - $\exists$ "There exists…"
- Negation of quantifiers:
  - $\neg \forall x\ P(x) \equiv \exists\ x\ \neg P(x)$
  - $\neg \exists\ x\ P(x) \equiv \forall\ x\ \neg P(x)$

Translation into predicates:

- Domain: all the people
- P(x): x is a York student
- Q(x): x can speak French
- Every York student can speak French.
  - $\forall x\ (P(x) \rightarrow Q(x))$
- Some York students can speak French.
  - $\exists\ x\ (P(x) \wedge Q(x))$

What Does the following formula mean?

- $\forall\ x\ (P(x) \wedge Q(x))$
  - All the people are York students and can speak French.

Scope of Quantifiers

- $\forall\ \exists$ have higher precedence than operators from Propositional Logic;
- so $\forall x\ P(x) \vee Q(x)$ is not logically equivalent to $\forall x\ (P(x) \vee Q(x))$
- Recall order of operations: $\forall\ \exists,\ \neg,\ \wedge,\ \vee,\ \rightarrow,\ \leftrightarrow$

Negation of Quantifiers

- Consider the statement Q: $\forall x\ P(x)$ where P(x) is a given predicate over a given domain.
- What does "Q is false" mean?
  - "Not for all x, P(x) is true"
  - "There is at least one x, P(x) is not true"
  - "There exists x, P(x) is false"
  - So Negation of $\forall x\ P(x)$ is $\exists\ x \neg P(x)$
- What does "$\exists\ x\ P(x)$ is false" mean?
  - "There does not exist x, such that P(x) is true"
  - "For all x, P(x) is not true"
  - So Negation of $\exists\ x\ P(x)$ is $\forall x \neg P(x)$

Nested Quantifiers

- One quantifier can be placed within the scope of the other
- Allows simultaneous quantification of many variables

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

$$\Downarrow$$

$$\forall x Q(x) \qquad Q(x): \exists y P(x,y)$$

- Think about loops in programming

- Example: Show $\forall x \exists y (x+y=1)$ is true over the integers.
- Proof:
  - Assume an arbitrary integer x.
  - To show that there exists a y that satisfies the requirement of the predicate, choose $y = 1-x$. Clearly y is an integer, i.e. in the domain.
  - So $x + y = x + (1-x) = 1$.
  - Since we assumed nothing about x (other than it is an integer), the argument holds for any integer x.
  - Therefore, the predicate is TRUE.

Order of Nested Quantifiers

- When there are only one kind of quantifiers (universal or existential) in a statement, then the change of order does not change the meaning of the statement:
  - ∀x∀yP(x,y) ≡ ∀y∀xP(x,y)
  - ∃x∃yP(x,y) ≡ ∃y∃xP(x,y)

- When there are different quantifiers, order matters
- In the Real Domain
  - ∀x∃y(x<y)
    - "For all x, there exists y, x<y", "there is no max integer"
  - ∃y∀x(x<y)
    - "There exists y, for all x, x<y", "there is a max integer"
  - ∀x ∃y (x+y=0)
    - "For every real number x there is a real number y such that, x+y=0"
  - ∃y ∀x (x+y=0)
    - "There is a real number y such that for every real number x, x+y=0"

Quantifications of Two Variables

	When true?	When false?
∀x∀yP(x,y) ∀y∀xP(x,y)	P(x,y) is true for every pair (x,y)	A pair (x,y) exists for which P(x,y) is false
∀x∃yP(x,y)	For every x, there is a y for which P(x,y) is true	There is an x such that P(x,y) is false for every y
∃x∀yP(x,y)	There is an x for which P(x,y) is true for every y	For every x, there is a y for which P(x,y) is false
∃x∃yP(x,y) ∃y∃xP(x,y)	There is a pair (x,y) for which P(x,y) is true	P(x,y) is false for all pairs (x,y)

Examples

- What is the truth value of the following:
  - ∃x∀y(x+y=0) domain: integers
  - ∃x∀y(xy=0) domain: integers
  - ∀x≠0∃y(y=1/x) domain: real numbers
  - ∀x∀y∃z(z=(x+y)/2) domain: integers

Negation of Nested Quantifiers

- Same rules as before
- Ex 1: ¬∀x∃y(x<y)
- ≡ ∃x¬∃y(x<y)
- ≡ ∃x∀y¬(x<y)
- ≡ ∃x∀y(x≥y)
- Ex 2: ¬∃x∀y(x+y=0)
- ≡ ∀x¬∀y(x+y=0)
- ≡ ∀x∃y¬(x+y=0)
- ≡ ∀x∃y(x+y≠0)

English -> Logical Expression

- "The sum of two positive integers is always positive."
  - Rewrite in English using quantifiers and domain
    - "For every pair of integers, if both integers are positive, then the sum of them is positive."
  - Introduce variables
    - "For integers x and y, if x and y are positive, then x+y is positive."
  - ∀x∀y((x>0)∧(y>0)→(x+y>0)) domain: integers

Logical Expression -> English

- $\exists x \forall y \forall z(friends(x,y) \wedge friends(x,z) \wedge (y \neq z) \rightarrow \neg friends(y,z))$
- Domain of x, y and z: all students
  - "There is a student x such that for all students y and all students z, if x and y are friends, x and z are friend and z and y are not the same student, then y and z are not friend."
  - "There is a student none of whose friends are also friends with each other."

Readings and notes

- Read Ch1.1-1.5
- Practice translating English sentences to propositions and predicates
- Practice to use truth tables
- Practice proving logical equivalence by manipulating compound propositions
- Understand the difference and relationship between propositions, predicates and quantifications.

Proofs-Inference Rules

- The reason for studying logic was to formalize derivations and proofs.
- How can we infer facts using logic?
- Let's start with Propositional logic.

- Simple inference rule (Modus Ponens) :

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

From (a) $p \rightarrow q$ and (b) p is TRUE, we can infer that q is TRUE.
  - (a) if these lecture slides are online then you can print them out
  - (b) these lecture slides are online
  - Conclusion: You can print lecture slides out.

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

- Similarly, From $p \rightarrow q$, $q \rightarrow r$ and p is TRUE, we can infer that r is TRUE.
- From $(p \wedge q) \rightarrow r$, p is TRUE, and q is TRUE, we can infer that r is TRUE
- Read more rules on Page 72
- Understand the rules

Inference Rules for quantified statements

- Universal instantiation

If $\forall x\, P(x)$ is true, we infer that $P(a)$ is true for any given a, where a is a particular member of the domain

$$\begin{array}{l} \forall x\, P(x) \\ \hline \therefore P(a) \end{array}$$

- Universal Generalization
  From P(c) is true for an **arbitrary c** in the domain, we can infer that $\forall x P(x)$ is true.

$$\frac{\text{P(c) is true for an arbitrary c}}{\therefore \forall x\ P(x)}$$

- Read more rules on Page 76

Proofs–Introduction

- Why are proofs necessary?
- What is a proof?
  - In Math, a proof is a step-by-step demonstration that a conclusion follows from some hypotheses.
  - In a each step use hypotheses, axioms, previously proven theorems, rules of inference, and logical equivalences such that the intermediate conclusion follows from previous step
- What details do you include/skip?
  - "Obviously", "clearly"…

Terminologies

- Theorem: A statement that can be proved to be true
- Axiom: A statement which is given to be true
- Lemma: A 'pre-theorem' that is needed to prove a theorem
- Corollary: A 'post-theorem' that follows from a theorem

Logic-based proof

- Every step should follow from axioms or previous step(s) using an inference rule.
- Problems:
  - Axiomatization is hard and often long (see Appendix 1)
  - Proofs are often very long and tedious

Types of Proofs

- Direct proofs (including Proof by cases)
- Proof by contraposition
- Proof by contradiction
- Proof by construction
- Proof by Induction
- Other techniques

Direct Proof

- Leads from hypothesis to the conclusion
- How to prove $p \rightarrow q$?
  - Assume p is true
  - Use rules of inference, axioms, lemmas, definitions, proven theorems, ...
  - Conclude that q must be true
- Q.E.D. (used to signal the end of a proof)

Direct Proof (example)

- The product of two odd integers is odd.
- Proof:
  - Assume m, n are two odd integers
  - By definition, $m=2i+1$ and $n=2j+1$ for some integers i and j.
  - $m \cdot n=(2i+1)(2j+1)=4ij+2i+2j+1=2(2ij+i+j)+1$
  - Let $k = 2ij+i+j$, $m \cdot n = 2k+1$
  - By definition, $m \cdot n$ is odd
  - Q.E.D.

Direct Proof (Proof by cases)

If n is an integer, then $n(n+1)/2$ is an integer

- Case 1: n is even.
  - $n = 2a$, for some integer a
  - So $n(n+1)/2 = 2a*(n+1)/2 = a*(n+1)$, which is an integer.
- Case 2: n is odd.
  - $n+1$ is even, or $n+1 = 2a$, for an integer a
  - So $n(n+1)/2 = n*2a/2 = n*a$, which is an integer.

Q.E.D.

Direct Proof (Proof by Exhaustion)

- Check a relatively small number of cases
- A special type of proof by cases
- Example: Prove $(n+1)^2 \geq 3n$ if n is a positive integer with $n \leq 4$

  Proof (by exhaustion):
  - $n=1$
  - $n=2$
  - $n=3$
  - $n=4$

Direct Proof (Limitation)

- Not all theorems can be proved by direct proof (Page 83, Example 3)
- Indirect Proofs:
  - Proof by contraposition
  - Proof by contradiction
  - Proof by construction
  - Proof by Induction
  - Other techniques

Proof by contraposition

- How to prove $p \rightarrow q$?
- Prove $\neg q \rightarrow \neg p$ is true

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

- Example: If $x+y \geq 2$, where x,y are real numbers, then $x \geq 1$ or $y \geq 1$
- Proof (by contraposition):
  - Assume "$x \geq 1$ or $y \geq 1$" is false. Then $x<1$ and $y<1$.
  - $X+y<2$. This is the negation of "$x+y \geq 2$", so the original conditional statement is true.
  - Q.E.D.

Proof by contraposition (example)

- Example: If n^2 is an even integer, then n is even.
- Proof:
  - Assume n is an odd integer. Then $n=2k+1$ (k is integer)
  - $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$
  - Let integer $m = (2k^2+2k)$, then $n^2=2m+1$.
  - So n^2 is odd.
  - Q.E.D.

Proof by Contradiction

- How to prove p is true?
- If we have a proposition r, such that $\neg p \rightarrow (r \wedge \neg r)$ is true.

p	r	¬p	r∧¬r	¬p→(r∧¬r)
T	T	F	F	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	F

Proof by Contradiction (example)

- $\sqrt{2}$ is irrational
- Proof (by contradiction):
  - Assume $\sqrt{2}$ is rational. Then $\sqrt{2}=a/b$ such that a and b have no common factors (definition)
  - Squaring and transposing: $2=a^2/b^2$, $a^2=2b^2$.
  - a^2 is even, so a is even (previous slide). i.e. $\exists k$ $a=2k$
  - $a^2 = 4k^2 = 2b^2$, so $b^2 = 2k^2$
  - b^2 is even, so b is even (previous slide). i.e. $\exists m$ $b=2m$
  - a and b have common factor 2 -- Contradiction! Q.E.D.

Proof by Contradiction (Conditional)

- How to prove $p \rightarrow q$?
- If we can find a contradiction q, such that $p \wedge \neg q$ is FALSE

p	q	p→q	¬q	p∧¬q
T	T	T	F	F
T	F	F	T	T
F	T	T	F	F
F	F	T	T	F

Proof by Contradiction (Conditional example)

- If n is a positive integer, then $n^2 \geq n$.
- Proof:
  - Assume $n^2 < n$
  - n is positive, so $n \neq 0$.
  - Divide both sides of $n^2 < n$ by n. Then $n < 1$.
  - Contradiction to "n is a positive integer"
  - Q.E.D.

Proof of Equivalences

- How to prove $p \leftrightarrow q$ is true?

  $$P \leftrightarrow r \leftrightarrow s \leftrightarrow \ldots \leftrightarrow q$$

  - Recall: to prove the logical equivalence of two formulas we can also use truth tables and developing a series of logical equivalences.
- Sometimes we need to prove $p \rightarrow q$ and $q \rightarrow p$

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

Proof of Equivalences (Example)

- Prove n is odd if and only if n^2 is odd.
  - Part 1: prove if n is odd then n^2 is odd (We have proved it in previous slides)
  - Part 2: prove if n^2 is odd then n is odd (by contraposition)
    - Assume n is even. Then $n=2k$ for some integer k
    - $n^2=(2k)^2=4k^2=2(2k^2)=2m$ for some integer m
    - Therefore n^2 is even
    - Q.E.D

Uniqueness proofs

- Sometimes we need to prove the existence of a unique element with a particular property.
- Prove by two parts
  - Existence: an element x with the property exists
  - Uniqueness: if $y \neq x$, then y does not have the property

Uniqueness proofs (Example)

- The equation $ax+b=0$, a,b real, $a \neq 0$ has a unique solution.
- Proof:
  - Step 1. $r=-b/a$ is a solution.
  - Step 2. Suppose $s \neq r$.

    Then $(as+b)-(ar+b) = a(s-r)$

    Since $a \neq 0$ and $s \neq r$, $a(s-r) \neq 0$.

    Then $as+b \neq ar+b \neq 0$

    s is not a solution.

  Q.E.D.

Disproof by counterexample

- One way to prove p is not true
- Find a counterexample such that p is false
- Show the following is FALSE: If x, y are irrational, x + y is irrational.
  - Proof: $x= \sqrt{2}$, $y= -\sqrt{2}$ are irrational, and $x+y=0$ is rational.

Readings and notes

- Read Ch1.5-1.8
- Understand the order and scope of the quantification
- Practice translating between English and logical expressions
- Understand the proof methods
- Practice proof a lot!
- Recommended book: "How to read and do proofs" by Daniel Solow

Examples

- Show that if n is an odd integer, there is a unique integer k such that n is the sum of $k-2$ and $k+3$.
- Prove that there are no solutions in positive integers x and y to the equation $2x^2 + 5y^2 = 14$.
- If x^3 is irrational then x is irrational