Math/EECS 1019C:
Discrete Mathematics for Computer Science

Fall 2014

Suprakash Datta

datta@cse.yorku.ca

Office: CSEB 3043

Phone: 416-736-2100 ext 77875

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

Administrivia

Lectures: Mon 7 - 10 pm (CLH A)

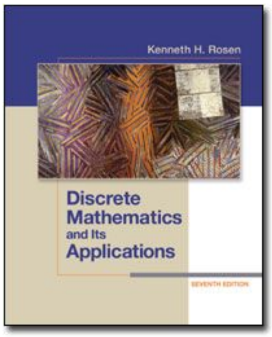
Exams: 3 tests, 15% each*(35%), final (40%)

Homework (25%): equally divided between several assignments.

Slides: should be available after the class

Office hours: Wed 4-6 pm or by appointment at CSEB 3043.

Textbook:



Kenneth H. Rosen. *Discrete Mathematics and Its Applications, 7th Edition*. McGraw Hill, 2012.

Administrivia – contd.

- Cheating will not be tolerated. Visit the class webpage for more details on policies.
- TA: Tutorials/office hours TBA.
- HW submitted late will not be graded.

Course objectives

We will focus on two major goals:

- Basic tools and techniques in discrete mathematics
  - Propositional logic
  - Set Theory, Functions and Relations
  - Simple algorithms
  - Induction, recursion
  - Sums
  - Introductory Graph Theory
- Precise and rigorous mathematical reasoning
  - Writing proofs

To do well you should:

- Study with pen and paper
- Ask for help **early**
- Practice, practice, practice…
- Follow along in class rather than take notes
- Ask questions in class or outside class
- Keep up with the class
- Read the book, not just the slides

Mathematical Reasoning

- What is Mathematics?
  - Mathematics as a precise language
- Motivation (for EECS)
  - Making precise, rigorous claims
- Procedure
  - Axioms
  - Inference
  - Facts/Theorems

Examples of reasoning about problems

- 0.999999999999999….=1?
- There exists integers a,b,c that satisfy the equation $a^2+b^2 = c^2$
- The program that I wrote works correctly for all possible inputs…..
- The program that I wrote never hangs (i.e. always terminates)…

Tools for reasoning: Logic

Ch. 1: Introduction to Propositional Logic

- Truth values, truth tables
- Boolean logic: $\vee$ $\wedge$ $\neg$
- Implications: $\rightarrow$ $\leftrightarrow$

Why study propositional logic?

- A formal mathematical "language" for precise reasoning.
- Start with propositions.
- Add other constructs like negation, conjunction, disjunction, implication etc.
- All of these are based on ideas we use daily to reason about things.

Propositions

- Declarative sentence
- **Must** be either True or False.

Propositions:

- York University is in Toronto
- York University is in downtown Toronto
- All students at York are Computer Sci. majors

Not propositions:

- Do you like this class?
- There are x students in this class.

Propositions - 2

- Truth value: True or False
- Variables: p,q,r,s,…
- Negation:
- ¬p ("not p")
- Truth tables

p	¬p
T	F
F	T

Caveat: negating propositions

¬p: "it is not the case that p is true"

p: "it rained more than 20 inches in TO"

p: "John has many iPads"

Practice: Questions 1-7 page 12.

Q10 (a) p: "the election is decided"

Conjunction, Disjunction

- Conjunction: $p \wedge q$ ["and"]
- Disjunction: $p \vee q$ ["or"]

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

Examples

Q11, page 13

p: It is below freezing

q: It is snowing

(a) It is below freezing and snowing

(b) It is below freezing but not snowing

(d) It is either snowing or below freezing (or both)

Exclusive OR (XOR)

- $p \oplus q$ – T if p and q have different truth values, F otherwise
- Colloquially, we often use OR ambiguously – “an entrée comes with soup or salad” implies XOR, but “students can take MATH XXXX if they have taken MATH 2320 or MATH 1019” usually means the normal OR (so a student who has taken both is still eligible for MATH XXXX).

Conditional

- $p \rightarrow q$ [“if p then q”]
- p: *hypothesis*, q: *conclusion*
- E.g.: “If you turn in a homework late, it will not be graded”; “If you get 100% in this course, you will get an A+”.
- TRICKY: Is $p \rightarrow q$ TRUE if p is FALSE?

YES!!

- Think of “If you get 100% in this course, you will get an A+” as a promise – is the promise violated if someone gets 50% and does not receive an A+?

Conditional - 2

- $p \rightarrow q$ ["if p then q"]
- Truth table:

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

Note the truth table of $\neg p \vee q$

Logical Equivalence

- $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent
- Truth tables are the simplest way to prove such facts.
- We will learn other ways later.

Contrapositive

- Contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$
- Any conditional and its contrapositive are logically equivalent (have the same truth table) – Check by writing down the truth table.
- E.g. The contrapositive of "If you get 100% in this course, you will get an A+" is "If you do not get an A+ in this course, you did not get 100%".

E.g.: Proof using contrapositive

Prove: If x^2 is even, x is even

- Proof 1: $x^2 = 2a$ for some integer a. Since 2 is prime, 2 must divide x.
- Proof 2: if x is not even, x is odd. Therefore x^2 is odd. This is the contrapositive of the original assertion.

Converse

- Converse of $p \to q$ is $q \to p$
- Not logically equivalent to conditional
- Ex 1: "If you get 100% in this course, you will get an A+" and "If you get an A+ in this course, you scored 100%" are not equivalent.
- Ex 2: If you won the lottery, you are rich.

Other conditionals

Inverse:

- inverse of $p \to q$ is $\neg p \to \neg q$
- How is this related to the converse?

Biconditional:

- "If and only if"
- True if p,q have same truth values, false otherwise. Q: How is this related to XOR?
- Can also be defined as $(p \to q) \wedge (q \to p)$

Example

- Q16c, page 14:

1+1=3 if and only if monkeys can fly.

Readings and notes

- Read pages 1-12.
- Think about the notion of truth tables.
- Master the rationale behind the definition of conditionals.
- Practice translating English sentences to propositional logic statements.

Next

Ch. 1.2, 1.3: Propositional Logic - contd

- Compound propositions, precedence rules
- Tautologies and logical equivalences
- Read only the first section called "Translating English Sentences" in 1.2.

Compound Propositions

- Example: $p \wedge q \vee r$: Could be interpreted as $(p \wedge q) \vee r$ or $p \wedge (q \vee r)$
- precedence order: $\neg\ \wedge\ \vee\ \rightarrow\ \leftrightarrow$ (IMP!) (Overruled by brackets)
- We use this order to compute truth values of compound propositions.

Tautology

- A compound proposition that is always TRUE, e.g. $q \vee \neg q$
- Logical equivalence redefined: p,q are logical equivalences if $p \leftrightarrow q$ is a tautology. Symbolically $p \equiv q$.
- Intuition: $p \leftrightarrow q$ is true precisely when p,q have the same truth values.

Manipulating Propositions

- Compound propositions can be simplified by using simple rules.
- Read page 25 - 28.
- Some are obvious, e.g. Identity, Domination, Idempotence, double negation, commutativity, associativity
- Less obvious: Distributive, De Morgan's laws, Absorption

Distributive Laws

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

Intuition (not a proof!) – For the LHS to be true: p must be true and q or r must be true. This is the same as saying p and q must be true or p and r must be true.

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

Intuition (less obvious) – For the LHS to be true: p must be true or both q and r must be true. This is the same as saying p or q must be true and p or r must be true.

Proof: use truth tables.

De Morgan's Laws

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

Intuition – For the LHS to be true: neither q nor r can be true. This is the same as saying q and r must be false.

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

Intuition – For the LHS to be true: $q \wedge r$ must be false. This is the same as saying q or r must be false.

Proof: use truth tables.

Using the laws

- Q: Is $p \rightarrow (p \rightarrow q)$ a tautology?
- Can use truth tables
- Can write a compound proposition and simplify

Inference in Propositional Logic

- in Section 1.6 pages 71-75
- Recall: the reason for studying logic was to formalize derivations and proofs.
- How can we infer facts using logic?
- Simple inference rule (Modus Ponens) :

  From (a) $p \rightarrow q$ and (b) p is TRUE,

  we can infer that q is TRUE.

Modus Ponens continued

Example:

(a) if these lecture slides (ppt) are online then you can print them out

(b) these lecture slides are online

Can you print out the slides?

- Similarly, From $p \to q$, $q \to r$ and p is TRUE, we can infer that r is TRUE.

Inference rules - continued

- $((p \to q) \wedge p) \to q$ is a TAUTOLOGY.
- Modus Tollens, Hypothetical syllogism and disjunctive syllogism can be seen as alternative forms of Modus Ponens
- Other rules like

  "From p is true we can infer $p \vee q$" are very intuitive

Inference rules - continued

Resolution: From

(a) $p \vee q$ and

(b) $\neg p \vee r$, we can infer that

$q \vee r$

Exercise: check that

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

is a TAUTOLOGY.

Very useful in computer generated proofs.

Inference rules - continued

- Read rules on page 72.
- Understanding the rules is crucial, memorizing is not.
- You should be able to see that the rules make sense and correspond to our intuition about formal reasoning.

Limitations of Propositional Logic

- What can we NOT express using predicates?

  Ex: How do you make a statement about all even integers?

  If $x > 2$ then $x^2 > 4$

- A more general language: Predicate logic (Sec 1.4)

Next: Predicate Logic

Ch 1.4

- Predicates and quantifiers
- Rules of Inference

Predicate Logic

- A predicate is a proposition that is a function of one or more variables.

  E.g.: P(x): x is an even number. So P(1) is false, P(2) is true,….
- Examples of predicates:
  - Domain ASCII characters - IsAlpha(x) : TRUE iff x is an alphabetical character.
  - Domain floating point numbers - IsInt(x): TRUE iff x is an integer.
  - Domain integers: Prime(x) - TRUE if x is prime, FALSE otherwise.

Quantifiers

- describes the values of a variable that make the predicate true. E.g. $\exists x\ P(x)$
- Domain or universe: set of values taken by a variable (sometimes implicit)

Two Popular Quantifiers

- Universal: $\forall x\, P(x)$ – "P(x) for all x in the domain"
- Existential: $\exists x\, P(x)$ – "P(x) for some x in the domain" or "there exists x such that P(x) is TRUE".
- Either is meaningless if the domain is not known/specified.
- Examples (domain real numbers)
  - $\forall x\ (x^2 >= 0)$
  - $\exists x\ (x > 1)$
  - $(\forall x > 1)\ (x^2 > x)$ – quantifier with restricted domain

Using Quantifiers

Domain integers:

- Using implications: The cube of all negative integers is negative.
  $\forall x\ (x < 0) \rightarrow (x^3 < 0)$
- Expressing sums :

$$\forall n\ \left(\sum_{i=1}^{n} i = n(n+1)/2\right)$$

Aside: summation notation

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 $\forall x\ (P(x) \vee Q(x))$
- $\exists\ x\ (P(x) \wedge Q(x)) \vee \forall x\ R(x)$

Say P(x): x is odd, Q(x): x is divisible by 3, R(x): $(x=0) \vee (2x > x)$

- Logical Equivalence: $P \equiv Q$ iff they have same truth value no matter which domain is used and no matter which predicates are assigned to predicate variables.

Negation of Quantifiers

- "There is no student who can …"
- "Not all professors are bad…."
- "There is no Toronto Raptor that can dunk like Vince …"
- $\neg\ \forall x\ P(x) \equiv \exists\ x\ \neg P(x)$ why?
- $\neg\ \exists\ x\ P(x) \equiv \forall\ x\ \neg P(x)$
- Careful: The negation of "Every Canadian loves Hockey" is NOT "No Canadian loves Hockey"! Many, many students make this mistake!

Nested Quantifiers

- Allows simultaneous quantification of many variables.
- E.g. – domain integers,
  - $\exists x \exists y \exists z \; x^2 + y^2 = z^2$ (Pythagorean triples)
  - $\forall n \exists x \exists y \exists z \; x^n + y^n = z^n$ (Fermat's Last Theorem implies this is false)
- Domain real numbers:
  - $\forall x \forall y \exists z \; (x < z < y) \vee (y < z < x)$ Is this true?
  - $\forall x \forall y \exists z \; (x=y) \vee (x < z < y) \vee (y < z < x)$
  - $\forall x \forall y \exists z \; (x \neq y) \rightarrow (x < z < y) \vee (y < z < x)$

Nested Quantifiers - 2

$\forall x \exists y \; (x + y = 0)$ is true over the integers

- Assume an arbitrary integer x.
- To show that there exists a y that satisfies the requirement of the predicate, choose y = -x. Clearly y is an integer, and thus is in the domain.
- So $x + y = x + (-x) = x – x = 0$.
- Since we assumed nothing about x (other than it is an integer), the argument holds for any integer x.
- Therefore, the predicate is TRUE.

Nested Quantifiers - 3

- **Analogy:** quantifiers are like loops:

  An inner quantified variable can depend on the outer quantified variable.

E.g. in $\forall x\ \exists y\ (x + y = 0)$ we chose $y=-x$, so for different x we need different y to satisfy the statement.

$\forall p\ \exists j$ Accept (p,j)   p,j have different domains

does NOT say that there is a j that will accept all p.

Nested Quantifiers - 4

- **Caution:** In general, order matters! Consider the following propositions over the integer domain:

  $\forall x\ \exists y\ (x < y)$ and $\exists y\ \forall x\ (x < y)$
- $\forall x\ \exists y\ (x < y)$: "there is no maximum integer"
- $\exists y\ \forall x\ (x < y)$: "there is a maximum integer"
- Not the same meaning at all!!!

Negation of Nested Quantifiers

- Use the same rule as before carefully.
- Ex 1: $\neg \exists x \forall y (x + y = 0)$
  - This is equivalent to $\forall x \neg\forall y (x + y = 0)$
  - This is equivalent to $\forall x \exists y \neg(x + y = 0)$
  - This is equivalent to $\forall x \exists y (x + y \neq 0)$
- Ex 2: $\neg \forall x \exists y (x < y)$
  - This is equivalent to $\exists x \neg\exists y (x < y)$
  - This is equivalent to $\exists x \forall y \neg(x < y)$
  - This is equivalent to $\exists x \forall y (x \geq y)$

Exercises

Check that:

- $\forall x \exists y (x + y = 0)$ is not true over the positive integers.
- $\exists x \forall y (x + y = 0)$ is not true over the integers.
- $\forall x$ <>0 $\exists y (y = 1/x)$ is true over the real numbers.

Readings and notes

- Read 1.4-1.5.
- Practice: Q2,8,16,30 (pg 65-67)

- Next: Rules of inference for quantified statements (1.6).

Inference rules for quantified statements

- Very intuitive, e.g. Universal instantiation – If $\forall x\, P(x)$ is true, we infer that $P(a)$ is true for any given a
- E.g.: Universal Modus Ponens:

  $\forall x\, P(x) \rightarrow Q(x)$ and $P(a)$ imply $Q(a)$

  If x is odd then x^2 is odd, a is odd. So a^2 is odd.
- Read rules on page 76
- Again, understanding is required, memorization is not.

Commonly used technique: Universal generalization

Prove: If x is even, x+2 is even

- Proof:

Prove: If x^2 is even, x is even

[Note that the problem is to prove an implication.]

- Proof: if x is not even, x is odd. Therefore x^2 is odd. This is the contrapositive of the original assertion.

Aside: Inference and Planning

- The steps in an inference are useful for planning an action.
- Example: your professor has assigned reading from an out-of-print book. How do you do it?
- Example 2: you are participating in the television show “Amazing race”. How do you play?

Aside 2: Inference and Automatic Theorem-Proving

- The steps in an inference are useful for proving assertions from axioms and facts.
- Why is it important for computers to prove theorems?
  – Proving program-correctness
  – Hardware design
  – Data mining
  – …..

Aside 3: Inference and Automatic Theorem-Proving

- Sometimes the steps of an inference (proof) are useful. E.g. on Amazon book recommendations are made.
- You can ask why they recommended a certain book to you (reasoning).

Next

- Introduction to Proofs (Sec 1.7)
- What is a (valid) proof?
- Why are proofs necessary?

Introduction to Proof techniques

Why are proofs necessary?

What is a (valid) proof?

What details do you include/skip?

"Obviously", "clearly"…

Assertions

- Axioms
- Proposition, Lemma, Theorem
- Corollary
- Conjecture

Types of Proofs

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

Direct Proofs

- The average of any two primes greater than 2 is an integer.

- Every prime number greater than 2 can be written as the difference of two squares, i.e. $a^2 – b^2$.

Proof by cases

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

- Case 1: n is even.
  or 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.

Proof by contraposition

If $\sqrt{(pq)} \neq (p+q)/2$, then $p \neq q$

Direct proof left as exercise

Contrapositive:

If $p = q$, then $\sqrt{(pq)} = (p+q)/2$

Easy:

$\sqrt{(pq)} = \sqrt{(pp)} = \sqrt{(p^2)} = p = (p+p)/2 = (p+q)/2.$

Proof by Contradiction

$\sqrt{2}$ is irrational

- Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = p/q$,
  such that p, q have no common factors.
  Squaring and transposing,
  $p^2 = 2q^2$ (even number)
  So, p is even (previous slide)
  Or $p = 2x$ for some integer x
  So $4x^2 = 2q^2$ or $q^2 = 2x^2$
  So, q is even (previous slide)
  So, p,q are both even – they have a common factor of 2. CONTRADICTION.
  So $\sqrt{2}$ is NOT rational. Q.E.D.

Proof by Contradiction - 2

In general, start with an assumption that statement A is true. Then, using standard inference procedures infer that A is false. This is the contradiction.

Recall: for any proposition p, $p \wedge \neg p$ must be false

Existence Proofs

There exists integers x,y,z satisfying $x^2+y^2 = z^2$

Proof: $x = 3$, $y = 4$, $z = 5$.

Existence Proofs - 2

There exists irrational b,c, such that b^c is rational (page 97)

Nonconstructive proof:

Consider $\sqrt{2}^{\sqrt{2}}$. Two cases are possible:

- Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational – DONE ($b = c = \sqrt{2}$).
- Case 2: $\sqrt{2}^{\sqrt{2}}$ is **irrational** – Let $b = \sqrt{2}^{\sqrt{2}}$, $c = \sqrt{2}$.
  Then $b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}*\sqrt{2}} = (\sqrt{2})^2 = 2$

Uniqueness proofs

- E.g. the equation $ax+b=0$, a,b real, $a\neq0$ has a unique solution.

The Use of Counterexamples

All prime numbers are odd

Every prime number can be written as the difference of two squares, i.e. $a^2 – b^2$.

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
- Prove or disprove – if x, y are irrational, x + y is irrational.

Alternative problem statements

- "show A is true if and only if B is true"
- "show that the statements A,B,C are equivalent"

Exercises

- Q8, 10, 26, 28 on page 91

What can we prove?

- The statement must be true
- We must construct a valid proof

The role of conjectures

- 3x+1 conjecture

  Game: Start from a given integer n. If n is even, replace n by n/2. If n is odd, replace n with 3n+1. Keep doing this until you hit 1.

e.g. n=5 $\rightarrow$ 16 $\rightarrow$ 8 $\rightarrow$ 4 $\rightarrow$ 2 $\rightarrow$ 1

Q: Does this game terminate for all n?

Elegance in proofs

Q: Prove that the only pair of positive integers satisfying a+b=ab is (2,2).

- Many different proofs exist. What is the simplest one you can think of?

Next

Ch. 2: Introduction to Set Theory

- Set operations
- Functions
- Cardinality