Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

MATH 240 - Discrete Structures

McGill University
Fall 2011

Contents

Course Information

- When/Where: MWF 10:35-11:35, Stewart Bio N2/2
- Instructor: Sergey Norin math.mcgill.ca/ snorin

Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

- Textbook: Discrete Mathematics, Elementary and Beyond by Lovasz, Pelikan and Vesztergombi
- Prerequisites:
- Grading:
  - 20 % assignments 20 % midterm and 60 % final
  - 20 % assignments 80 % final
  - (best of two above)

Introduction

Discrete vs. Continuous structures

- Objects in discrete structures are individual and separable
- An intuitive analogy is that discrete structures focus on individual trees in the forest whereas continuous structures care about the landscape airplane view.
- Discrete structure courses can be called "computer science semantics" in other universities. Mathematics for computer science.
- Naive examples
  - Counting techniques: There are two ice cream shops. One sells 20 different flavours whereas the other offers 1000 different combinations of three flavours. Which one has the most possible combinations of three flavours?
  - Cryptography: Two parties want to communicate securely over an insecure channel. Can they do it? Yes, using number theory. Discrete Structures are used in cryptography (what this question is about), coding theorem (compression of data) and optimization.
  - Graph Theory: Suppose you have 6 cities and you want to connect them with roads joining the least possible number of pairs, so that every pair is connected, perhaps indirectly. In how many ways can we connect these cities using 5 roads?
- Before we address these problems, we must agree upon a language to formalize them.

1 Sets

1.1 Definition

A set is a collection of distinct objects which are called the elements of the set.

Examples: We use a capital letter for sets.

- $A = \{Alice, Bob, Claire, Eve\}$
- $B = \{a, e, i, o, u\} = \{o, i, e, a, u\}$
- $\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$ (natural numbers)
- $\mathbb{Z} = \{.., -2, -1, 0, 1, 2, ..\}$ (integers)
- $\emptyset = \{\}$ (no elements, note: $\{\emptyset\} \neq \emptyset$)

Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

- If x is an element of A we write $x \in A$ which is read "belongs", "is an element of" or "is in" e.g. $Alice \in A, Alice \notin \mathbb{N}$
- We say that X is a subset of a set Y if for every $z \in X$ we have $z \in Y$ Notation: $X \subseteq Y$.
- $\emptyset \subseteq \{1, 2, 3, 4, 5\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

1.2 Operations on sets

$U = \{1, 2, 3, 4, 5, 6..10\} = \{x \in \mathbb{N} : x \leq 10\}$

$A = \{2, 4, 6, 8, 10\} = \{x \in U : x \text{ is even}\}$

$B = \{2, 3, 5, 7\} = \{x \in U : x \text{ is prime}\}$

An intersection $A \cap B$ is a set of all elements belonging to both A or B: $A \cap B = \{2\}$

A union $A \cup B$ is a set of all elements belonging to either A or B: $A \cap B = \{2, 3, 4, 5, 6, 7, 8, 10\}$

$|A| = 5, |B| = 4, |A \cap B| = 1, |A \cup B| = 8|\emptyset| = 0, |\mathbb{N}| = \infty$

$A - B$: all elements of A which do not belong to B $\{x : x \in A, x \notin B\}$

$A \oplus B, A \triangle B$: symmetric difference, set of all elements belonging to exactly one of A and B

1.3 Venn Diagrams

A way of depicting all possible relations between a collection of sets. For a set A, $|A|$ denotes the number of elements in it.

Typically, Venn diagrams are useful for 2 or 3 sets.

1.4 Theorems

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - Fact: For any two finites sets $|A| + |B| = |A \cap B| + |A \cup B|$
  - Proof:
    1. $x \in A \cap (B \cup C)$ then $x \in (A \cap B) \cup (A \cap C)$
       * $x \in A$ and ($x \in B$ or $x \in C$)
       * if $x \in B$ then $x \in (A \cap B)$ therefore $x \in (A \cap B) \cup (A \cap C)$
       * if $x \in C$ then $x \in (A \cap C)$ therefore $x \in (A \cap B) \cup (A \cap C)$
    2. $x \in (A \cap B) \cup (A \cap C)$ then $x \in A \cap (B \cup C)$
       * $x \in (A \cap B)$ therefore $x \in A$ and $x \in (B \cup C)$
- $A \oplus B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

2 Logic

Way of formally organizing knowledge studies inference rules i.e. which arguments are valid and which are fallacies.

2.1 Propositional Calculus

A proposition is a statement (sentence) which is either true or false.

Some examples:

- $2+2=4 \rightarrow$ true
- $2+3=7 \rightarrow$ false
- "If it is sunny tomorrow, I will go to the beach." $\rightarrow$ valid proposition
- "What is going on?" $\rightarrow$ not a proposition
- "Stop at the red light" $\rightarrow$ not a proposition
- We are given 4 cards. Each card has a letter (A-Z) on one side, a number (0-9) on the other side. "If a card has a vowel on one side then it has an even number on the other" Two ways to refute this proposition: Either turn over a vowel card and find an odd number. Or turn over an odd number and find a vowel.

2.2 Notation

- Letters will be used to denote statements: p, q, r
- $p \wedge q$: "and", "conjunction", "p and q" (are both true)
- $p \vee q$: "or", "disjunction", "either p or q" (is true)
- $\neg p$: "not", "p is false"

2.3 Truth Tables

2.4 Rules of Logic

1. Double negation: $\neg(\neg p) \leftrightarrow p$
2. Indempotent rules: $p \wedge p \leftrightarrow p \qquad p \vee p \leftrightarrow p$
3. Absorption rules: $p \wedge (p \vee q) \leftrightarrow p \qquad p \vee (p \wedge q) \leftrightarrow p$
4. Commutative rules: $p \wedge q \leftrightarrow q \wedge p \qquad p \vee q \leftrightarrow q \vee p$
5. Associative rules: $p \wedge (q \wedge r) \leftrightarrow (q \wedge p) \wedge r \qquad p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$
6. Distributive rules: $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r) \qquad p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$
7. De Morgan's rule: $\neg((\neg p) \vee (\neg q)) \leftrightarrow p \wedge q \qquad \neg((\neg p) \wedge (\neg q)) \leftrightarrow p \vee q$
   $p \vee (\neg((\neg p) \wedge (\neg q))) \leftrightarrow p \vee (p \vee q) \leftrightarrow (p \vee p) \vee q \leftrightarrow p \vee q$

Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

2.4.1 Conditional Statements

1. $p \to q$
   - Theorem: if (an assumption holds), then (the conclusion holds).
   - Implication: "if p then q"
     p = "a, b, & c are two sides and the hypthenuse of a triangle"
     q = "$a^2 + b^2 = c^2$"
   - $p \to q$ "If p then q" p implies q, p is sufficient for q
     $(p \to q) \leftrightarrow (q \vee (\neg p))$
   - Examples:
     - "If the Riemann hypothesis is true then 2 + 2 = 4" TRUE
       p = "the Riemann hypothesis"
       q = "2+2=4"
       True proposition is implied by any proposition.
     - "If pigs can fly then pigs can get sun burned" TRUE
       False statement implies any statement
     - "If 2+2 =4 then pigs can fly" FALSE
       The implication is false only if the assumption holds and the conclusion does not.
   - $p \to q \leftrightarrow (\neg p) \to (\neg q)$
   - $(p \to q) \wedge (q \to p) \leftrightarrow (p \leftrightarrow q)$

Puzzle There are three boxes A, B, C. Exactly one contains gold in it.

- Box A: Gold is not in this box
- Box B: Gold is no in this box
- Box C: Gold is in box A

Exactly one of these propositions is true. Where is the gold? Let us formalize the propositions.

- p: "Gold is in box A"
- q: "Gold is in box B"
- r: "Gold is in box C"
- Box A: $q \vee r$
- Box B: $p \vee r$
- Box C: p
- $p \to (p \vee r)$
- $\neg(p \vee r) \to q$

2.5 Tautologies & Contradictions

Definition

- A **tautology** is a statement that is always true (the rightmost column of the corresponding truth table has T in every row) e.g. $p \vee (\neg p)$
- A **contradiction** is a statement that is always false e.g. $p \wedge (\neg p)$

Notation

- 1 denotes a tautology
- 0 denotes a contradiction
- $1 \vee p \leftrightarrow 1$
- $0 \vee p \leftrightarrow p$
- $1 \wedge p \leftrightarrow p$
- $0 \wedge p \leftrightarrow 0$
- $p \wedge (p \vee q)$

p	1	$p \vee q$	$p \wedge (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	F	F

  $\rightarrow$ Not a tautology and not a contradiction
  $p \wedge (p \vee q) \leftrightarrow p$ (one of the rules)

- $p \vee (p \wedge q) \vee (p \rightarrow q) \leftrightarrow (p \vee (p \wedge q)) \vee (p \rightarrow q)$
  $(p \rightarrow q) \leftrightarrow (\neg p) \vee q \leftrightarrow p \vee (p \rightarrow q)$
  $\leftrightarrow p \vee ((\neg p) \vee q)(absorption)$
  $\leftrightarrow (p \vee (\neg p)) \vee q$
  $\leftrightarrow 1 \vee q \leftrightarrow 1$

2.6 Proofs

- $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ (always true)
- Implication is transitive: $p \rightarrow q \rightarrow r$
- A **proof** of a conclusion q given premise p is a sequence of implications (valid) $p \rightarrow p_2 \rightarrow p_3 \rightarrow .. \rightarrow p_k \rightarrow q$
- To prove $(p \leftrightarrow q)$
  $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$
- Theorem: Let p(x) be a polynomial then p(0) = 0 if and only if p(x) = x q(x) for some polynomial q(x)
- Proof: "p(0) = 0" and "p(x) = x q(x) for some polynomial q(x)"
  1. $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$
     $p(0) = 0 \rightarrow a_0 = 0 \rightarrow$
     $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x \rightarrow$
     $p(x) = x(a_n x^{n-1} + a_{n-1}x^{n-2} + ... + a_1$
     $p(x) = xq(x)$
     $q(x) = a)nx^{n-1} + a_{n-1}x^{n-2} + ... + a_2$
     True so proven.

2. $p(x) = xq(x) \to p(0) = 0 \cdot q(0) \to q(0) = 0$

- Proof by contradiction: $(p \to q) \leftrightarrow ((\neg q) \to (\neg p))$
- Pigeonhole principle: We place an objects into m bins. If $n > m$ then some bin contains at least 2 objects.
- Proof: p = "$n > m$" and q = "Some bin contains at least 2 objects"
  $\neg q$ = "every bin contains at most 1 object"
  $\neg p$ = "$n \leq m$" $\neg q \to \neg p$ is trivial
- Theorem: There are infinitely many prime numbers
  Direct proof of this theorem is unlikely, there is no known simple formula producing prime numbers
- Proof: Assume $\neg p$. There are infinitely many prime numbers $p_1, p_2, p_3..p_k$
  Consider $p = p_1 p_2 ... p_k + 1$ Every integer greater than 1 is divisible by a prime. (Prime number is the integer divisible by only 1 and itself). Suppose $p = p_i m$ for some $1 \leq i \leq k$ and an integer m, then $p_i(p_1 p_2 ... p_{i-1} p_{i+1} ... p_k) + 1 = p_i m$ $p_i(m - p_1 p_2 .. p_k) = 1$ (except p_1) "1 is divisible by p_i, a contradiction"

3 Circuit Complexity

3.1 Boolean Logic

- **Objects**: statements p, 1
- **Operators**: $\vee, \wedge, \neg$, etc

3.2 Logic Gates

Will insert logic gate diagrams later when I figure how to insert images.

p	q	r	$p \oplus q$	$(p \oplus q) \oplus r$
1	1	1	0	1
1	1	0	0	0
1	0	1	1	0
1	0	0	1	1
0	1	1	0	0
0	1	0	1	1
0	0	1	1	1
0	0	0	0	0

Majority Circuit (for 3 inputs) p, q, r $\to \begin{cases} \text{1 (or T) if at least 2 of p, q \& r are 1's} \\ \text{0 (or F) otherwise} \end{cases}$

Size A logical circuit has size equal to the number of gates in it and depth equal to the length (or number of gates) of the longest path from an input to the final output.

Given a boolean formula, what is the minimum size (or depth) of a circuit necessary to compute it? (depth is frequently assumed to be constant).

Given a circuit C with inputs $p_1, p_2, ..., p_n$

Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

Can we test if C is always a contradiction? The answer is trivially yes, if we test all possible inputs. It would take 2^n.

3.3 Algorithms

- Every logic formula can be represented as a combinational circuit
- Can we represent a given formula by a "simple" circuit
- Given a circuit (with inputs $p_1, p_2, ..., p_n$ can we test quickly if C is a contradiction? (we can test in $2^n steps$
- **Algorithm**: A step-by-step procedure for solving a problem, precise enough to be carried out on a computer

4 Polytime algorithms P# NP conjecture

4.1 Definition

Given algorithm A its running time $t_A(n)$ = maximum number of steps the algorithm can require on inputs of size n

A is a **polynomial time** algorithm if $t_A(n)$ is polynomially bounded $(t_A(n) = O(n^2)) \leftrightarrow$ fast, efficient

P is class of problem which allow polynomial time algorithms.

Examples

1. Evaluating the median of a set of numbers
    - Problem: $x_1, x_2, .., x_n \leftarrow$ Input
    - Question: decide whether the median of the list is ≤ 1000
    - Algorithm:
        - Sort the list going once through the list ($\leq n$ steps) we can find smallest x_i
        - Repeat to find the second smallest number and so on
        - Requires $O(n^2)$ time to sort
        - Check if $x_{\frac{n}{2}}(x_{\frac{n}{2}})$ is at most 1000 (roughly n^2 steps polytime).
2. Multiplication
    - Input: $2n$ digit numbers
    - Output: $a \times b$
      roughly n^2 steps
3. Problem Factoring
    - Input: a composite number C
    - Output: Find natural numbers $a, b > 1, c = a \times b$
    - Brute-Force search: Try all prime numbers up to C. Time: $10^{n/2} \rightarrow$ exponential time algorithm

- RSA ran contests until 2007 offering prizes for factoring (roughly 20 computer years for factoring 200 digit numbers)

4.2 NP problems (non-deterministic polynomial time)

- A **decision problem** is a problem with a yes/no answer. Example:
  - Input: a combinatorial circuit (with n inputs)
  - Output: Is C **not** a contradiction?
- A decision problem is in the class NP if a "yes" answer always has a certificate which can be verified in polynomial time.
- A problem is in NP when the answer is positive. A magician can quickly convince you that it is e.g. "testing that a circuit is not a contradiction" is in NP.
- If there exists a set of values for inputs so that the circuit outputs 1 (or T) then given this collection of inputs verifying that it works is fast.

Examples

1. Factoring:
   - Input: n digit number
   - output: Is this number composite and if it is, factor it.
2. Traveling Salesman problem:
   - Input: Collection of n cities and distances between them
   - Travelling salesman tour: An ordering of cities $c_1 \to c_2 \to ... \to c_n$ visiting each city once
   - Question: Is there a tour of total length $\leq$ 1000 miles $\to$ is in NP

4.3 $P \neq NP$

There exist problems which cannot be solved efficiently but for which a positive answer can be verified efficiently. There exists problems for which brute-force search is essentially the best possible strategy. If there are problems where you need a magician, then it is NP.

If there exists a problem in NP but not in P (if the conjecture is true) then testing if a circuit is a contradiction, travelling salesman problem, and a very large class of similar problems are all not in P

If P = NP then airline scheduling, protein folding, packing boxes, finding short proof for theorems all can be done efficiently but certain cryptography becomes impossible.

The universal opinion is that $P \neq NP$

4.4 Scott Aovonson's reasons for $P \neq NP$

Empirical: Problems in NP remain heuristically hard, however problems which are now known to be in P (linear programming, primality testing) but efficient heuristics existed long before.

Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

5 Proof Techniques: Predicate calculus

Reminder A proof is a sequence of implications deriving a conclusion q from a premise p: $p \to q$

- Direct Proof: $p \to p_1 \to p_2 \to p_3. \to ... \to p_k \to q$
- Proof by contradiction: $p \to q \leftrightarrow (\neg q \to \neg p)$
- Case Analysis: $(p \wedge q \to r) \leftrightarrow (p \to r) \wedge (q \to r)$ See below
- Counter Examples: See below

Case Analysis

- Proposition: For positive integer n: $3 \nmid n \to 3 \mid n^2 + 2$
  ($a \mid b \to$ "a divides b" there exists an integer c, b = ac) Proof: Divide n by 3 with remainder

Couter Example

- Proposition: $n^2 + n + 1$ is prime for every positive integer n ≤ 10
- $4^2 + 4 + 1 = 21 = 7 \cdot 3$
- This is a counter example: the statement is false
- Mathematical Notation
  - $p \to q \wedge r \to p \to q$
  - $\neg(p \to q) \to \neg(p \to q \wedge r)$
  - q is a counter example to the implication "$n^2 + n + 1$ is prime for all integers n "
  - "$n^2 + n + 1$ is prime" $\leftarrow$ P(n) predicate proposition depending on a variable $\forall n \in \mathbb{Z}(P(n))$
    Note: $\forall$ means "for all" e.g. "For all n in the set of integers the predicate "$n^2 + n + 1$"is prime" is true
  - "There exists an integer n so that $n^2 + n + 1$ is not prime" is noted $\exists n \in \mathbb{Z}(Q(n))$ where Q(n) "$n^2 + n + 1$ is not prime" i.e. $Q(n)\neg P(n)$

Goldback's conjecture Every even integer bigger than 2 is expressible as a sum of 2 primes.

- $\forall n \in$ "even integers", $n > 2 \to (\exists a, b \in \{primes\}(n = a + b)))$
- "71 is prime"
- $\forall a, b \in \mathbb{N}(a \cdot b = 71) \to ((a = 1) \wedge (b = 71))$

Limits

- "f(x) as a limit L as x $\to$ a" "$lim_{x \to a} f(x) = L$" As x approaches a f(x) becomes closer and closer to L"
- "For every $\epsilon > 0$, there exists $\delta > 0$ so that if $|x - a| < \delta then |f(x) - L| < \epsilon$"
- "$\forall \epsilon > 0(\exists \delta > 0(|x - a| < \delta \to |f(x) - L| < \epsilon))$
- "$lim_{x \to \infty} f(x) = L$"$\forall \epsilon > 0(\exists X \cdot (\forall x > X(|f(x) - L| < \epsilon)))$

Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

P(n) : "$n^2 + n + 1$ is prime"

- $\neg(\forall n \in A : P(n)) \leftrightarrow \exists n \in A(\neg P(n))$
- $\forall n \in A : P(n) \leftrightarrow \neg(\exists n \in A(\neg P(n))$

"$\sin x$ does not have a limit as $x \to \infty$"

$$\begin{aligned}
\neg(\exists L : lim_{x\to\infty} \sin x = L) &\leftrightarrow \forall L : (\neg(lim(\sin x) = L) \\
&\leftrightarrow \forall L(\neg(\forall \epsilon > 0(\exists X(\forall x > X(|\sin x - L| < \epsilon))))) \\
&\leftrightarrow \forall L(\exists \epsilon > 0(\neg(\exists X(\forall x > X(|\sin x - L| < \epsilon))))) \\
&\leftrightarrow \forall L(\exists \epsilon > 0(\neg(\exists X(\forall x > X(|\sin x - L| < \epsilon))))) \\
&\leftrightarrow \forall L(\exists \epsilon > 0(\forall X(\exists x > X(|\sin x - L| \geq \epsilon))))
\end{aligned}$$

5.1 Divisibility Problem

We want to prove the following theorem:

- Any collection of n+1 numbers chosen from the set {1,2,...,2n} contains two numbers so that one is divisible by the other.
- $\forall n \in \mathbb{N}(\forall s \subseteq \{1, 2, ..., 2n\}(|S| = n + 1) \to \exists a, b \in S((a|b) \wedge (a + b)))$

Reminder: the pigeonhole principle If $n + 1$ objects are placed into n boxes then some box contains ≥ 2 objects. To apply the principle we want to partition $\{1, 2, ..., 2n\}$ into n subjects.

Partition We say that a collection $A_1, A_2, ...A_k$ of subsets of a set B is a **partition** of B if

1. $\forall i, j : 1 \leq i <\leq k \qquad A_i \cap A_j = \emptyset$ (no element of B belongs to two different parts)
2. $A_1 \cup A_2 \cup ... \cup A_k = B$

Example: {1,2,3,4,5,6,7,8} {1,2,4,6,8} , {3, 5} , {7}

Proof By the pigeonhole principle it suffices to find a partition $A_1, A_2, ...A_n$ of {1,2,...,2n} so that $(\forall i(\forall a, b \in A_i(a|b \vee b|a)))$

Here is a construction: $A_i = \{(2i + 1), 2(2i - 1), 4(2i - 1), ..., 2^m(2i - 1)\}$ up to maximum m: $2^m(2i - 1) \leq 2n$

1. A_i satisfies the desired property for all i
2. $A_1, A_2, .., A_n$ is a partition of {1,2,...,2n}
   Ever positive integer can be uniquely written in a form $2^m(2i - 1)$ for some $i \geq 1, m \geq 0$

Note: Is it true for some n: "Every collection of n numbers chosen from {1,2,...,2n} contains 2 numbers one dividing the other"?

Counter-example: $n = 2 \quad \{1, 2, 3, 4\} \to \{3, 4\}$

Brought to you by WikiNotes. Join our facebook group or take a look at our website on wikinotes.ca

5.2 Strangers and Clubs

For a collection of people any two of them either have met or haven't . A club is a group of people who have pairwise met each other. A group of strangers is a group of people who pairwise have not met each other

Theorem: In any collection of 6 people rhwew is either a club of 3 people or a group of 3 strangers.

Proof Let x be one of the people in the collection. The following cases apply

1. x has at least 3 acquaintances
   (a) Some two of acquaintances of x, say y & z know each other. Then {x, y, z} form a club.
   (b) No two acquaintances of x know each other. Then they form a group of strangers.
2. x has at most 2 acquaintances there one ate least 3 people

5.3 Social Choice Function

3 candidates A, B & C:

- 49% of electorate A ¿ B ¿ C
- 48 % of electorate B ¿ A ¿ C
- 3% of electorate C ¿ B ¿ A