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
- 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

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

- 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: $\{\emptyset\} \neq \emptyset\}$)
- 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: $A \cap B = \{2, 3, 4, 5, 6, 7, 8, 10\}$

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

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

$A - B$: 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 $x \in (B \cup C)$
- $A \oplus B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

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

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

- 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: $\neg((\neg p) \vee (\neg q)) \leftrightarrow p \wedge q \qquad \neg((\neg p) \wedge (\neg q)) \leftrightarrow p \vee q$
   $p \vee (\neg((\neg p) \wedge (\neg q))) \leftrightarrow p \vee (p \vee q) \leftrightarrow (p \vee p) \vee q \leftrightarrow p \vee q$

2.4.1 Conditional Statements

1. $p \rightarrow q$
   - 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 = "$a^2 + b^2 = c^2$"
   - $p \rightarrow q$ "If p then q" p implies q, p is sufficient for q
     $(p \rightarrow q) \leftrightarrow (q \vee (\neg p))$
   - 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.

2. $p \to q \leftrightarrow (\neg p) \to (\neg q)$
3. $(p \to q) \wedge (q \to p) \leftrightarrow (p \leftrightarrow q)$