MATH 240 - Discrete Structures

McGill University
Fall 2011

Contents

Course Information 2

1 Sets 3
- 1.1 Definition . . . 3
- 1.2 Operations on sets . . . 3
- 1.3 Venn Diagrams . . . 4
- 1.4 Theorems . . . 4

2 Logic 4
- 2.1 Propositional Calculus . . . 4
- 2.2 Notation . . . 5
- 2.3 Truth Tables . . . 5
- 2.4 Rules of Logic . . . 5
  - 2.4.1 Conditional Statements . . . 5
- 2.5 Tautologies & Contradictions . . . 6
- 2.6 Proofs . . . 7

3 Circuit Complexity 7
- 3.1 Boolean Logic . . . 7
- 3.2 Logic Gates . . . 8
- 3.3 Algorithms . . . 8

4 Polytime algorithms P# NP conjecture 8
- 4.1 Definition . . . 8
- 4.2 NP problems (non-deterministic polynomial time) . . . 9
- 4.3 $P \neq NP$ . . . 10
- 4.4 Scott Aovonson's reasons for $P \neq NP$ . . . 10

5 Proof Techniques: Predicate calculus 10
- 5.1 Divisibility Problem . . . 11
- 5.2 Strangers and Clubs . . . 12

6 Social Choice Function 12
- 6.1 Definition . . . 12
- 6.2 Arrow's impossibility Theorem (1951) . . . 13

7 Proofs 14
- 7.1 The well-ordering principle . . . 14
  - 7.1.1 Proofs using the well-ordering principle . . . 14

7.1.2 Method . . . 14
7.2 Induction . . . 15
7.2.1 A few examples . . . 16

8 Number Theory **16**
8.1 Primes . . . 17
8.2 Greatest common divisors and linear combinations . . . 18
8.3 Linear Combinations . . . 19
8.4 Greatest common divisors . . . 20

9 Euclid's algorithm **21**
9.1 Computing gcd with prime factorization . . . 21
9.2 Computing gcd with Euclid's algorithm . . . 21
9.3 Statement of Euclid's algorithm . . . 22
9.4 Analysis of Euclid's algorithm . . . 22
9.5 Expressing gcd(a,b) as a linear combination of a & b . . . 22
9.6 Homework problem . . . 23

10 Modular arithmetic **24**
10.1 Notation . . . 24

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

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

$A - B$: 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

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

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
- 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.

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

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.
   - $p \rightarrow q \leftrightarrow (\neg p) \rightarrow (\neg q)$
   - $(p \rightarrow q) \wedge (q \rightarrow p) \leftrightarrow (p \leftrightarrow q)$

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

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

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

- $(p \to q) \wedge (q \to r) \to (p \to r)$ (always true)
- Implication is transitive: $p \to q \to r$
- A **proof** of a conclusion q given premise p is a sequence of implications (valid) $p \to p_2 \to p_3 \to .. \to p_k \to q$
- To prove $(p \leftrightarrow q)$
  $(p \leftrightarrow q) \leftrightarrow (p \to q) \wedge (q \to p)$
- 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. $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$
     $p(0) = 0 \to a_0 = 0 \to$
     $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x \to$
     $p(x) = x(a_n x^{n-1} + a_{n-1}x^{n-2} + ... + a_1$
     $p(x) = xq(x)$
     $q(x) = a)nx^{n-1} + a_{n-1}x^{n-2} + ... + a_2$
     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

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

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

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 $p_1, p_2, ..., p_n$

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.

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

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.

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 $\leq$ 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" ← P(n) predicate proposition depending on a variable $\forall n \in \mathbb{Z}(P(n))$
  Note: ∀ 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 → 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 $|x - a| < \delta then|f(x) - L| < \epsilon$"
- "$\forall\epsilon > 0(\exists\delta > 0(|x - a| < \delta \to |f(x) - L| < \epsilon))$
- "$lim_{x\to\infty}f(x) = L$"$\forall\epsilon > 0(\exists X \cdot (\forall x > X(|f(x) - L| < \epsilon)))$

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.
- $\forall n \in \mathbb{N}(\forall s \subseteq \{1, 2, ..., 2n\}(|S| = n + 1) \to \exists a, b \in S((a|b) \wedge (a + b)))$

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

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: $n = 2 \quad \{1, 2, 3, 4\} \rightarrow \{3, 4\}$

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

6 Social Choice Function

6.1 Definition

3 candidates A, B & C:

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

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

Given a collection of voters $v_1, v_2, ..., v_n$ and several candidates A, B, C, D, ...

Each voter ranks the candidates according to his preferences:

$A >^{v_2} B >^{v_2} C >^{v_2} D \qquad >^{v_i} is the ordering produced by the i^{th} voter$

Permutation (A, D, B, C) of the set of candidates {A, B, C, D }

Social choice function takes as an input voter's ordering and produces a consensus ordering and produces a consensus ordering $f(>^{v_1}, >^{v_2}, , ..., >^{v_n}) = \quad >$

What conditions should a good SCF satisfy?

1. **Unanimity**: If every voter prefers α to β then the consensus ordering must rank α above β $(\forall \vee (\alpha >^{v} \beta)) \to (\alpha > \beta)$
2. **Independence on irrelevant alternatives (IAA)** The final relative ordering of α and β should depend only on relative orderings of α and β (If a candidate withdraws from election this doesn't affect the order of others).

Which social choice functions satisfy these properties?

What happens with majority? $\alpha > \beta$ if more than half of the voters prefer α to β:

- $v_1 : A >^{v_1} B >^{v_1} C$
- $v_2 : C >^{v_2} A >^{v_2} B$
- $v_3 : B >^{v_3} C >^{v_3} A$

How does this work? There is a conflict here...

Dictatorship: For some fixed voter d we have $(\alpha > \beta)$ if and only if $(\alpha >^{d} \beta)$

6.2 Arrow's impossibility Theorem (1951)

The only social choice function satisfying unanimity and IIA is a dictatorship.

Proof Unanimity $\wedge$ IIA $\to$ dictatorship

Let $>$ satisfy these two properties β is called a polarizing candidate if every voter ranks him.her at the very top or the very bottom of the list.

Claim A polarizing candidate ranks first or last in the consensus ordering $>$

Proof Suppose not $\alpha > \beta > \gamma$ where β is a polarizing candidate

$$\left|\begin{array}{c|c|c|c} \beta & \beta & \alpha & \gamma \\ \alpha & \gamma & \gamma & \alpha \\ \gamma & \alpha & \beta & \beta \end{array}\right|$$

Switch α and γ in voter's preferences so that every voter prefers γ to α. We should still have $\alpha > \beta > \gamma$ because relative positions of α and β and relative positions of β and γ are unchanged. By unanimity we should now have $\gamma > \alpha$ (contradiction QED)

Choose a candidate β

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

$$\begin{vmatrix} \beta \\ \alpha \\ \beta \\ v_1 \end{vmatrix} \begin{vmatrix} \beta \\ \gamma \\ \beta \\ v_2 \end{vmatrix} \begin{vmatrix} \alpha \\ \gamma \\ \dots \\ \dots \end{vmatrix} \begin{vmatrix} \gamma \\ \alpha \\ \beta \\ v_n \end{vmatrix} \rightarrow \begin{vmatrix} \beta \\ \alpha \\ - \\ v_1 \end{vmatrix} \begin{vmatrix} - \\ \gamma \\ \beta \\ v_2 \end{vmatrix} \begin{vmatrix} - \\ \gamma \\ \dots \\ \dots \end{vmatrix} \begin{vmatrix} - \\ \alpha \\ \beta \\ v_n \end{vmatrix}$$

So there exists a voter v^* so that $\begin{vmatrix} \beta \\ \alpha \\ - \\ v_1 \end{vmatrix} \begin{vmatrix} - \\ \gamma \\ \beta \\ v_2 \end{vmatrix} \begin{vmatrix} - \\ \gamma \\ \dots \\ \dots \end{vmatrix} \begin{vmatrix} - \\ \alpha \\ \beta \\ v_n \end{vmatrix}$

Goddammit. Disregard this last section (the whole theorem). I will fix it later.

7 Proofs

7.1 The well-ordering principle

- **The well-ordering principle**
  Every non empty subset of non-negative integers has a smallest element.
- **The induction principle**
  "P(n) is true for all natural numbers b"

7.1.1 Proofs using the well-ordering principle

Claim There exists subsets of non-negative rational numbers with no smallest element.

$\{x \in \mathbb{Q} | x > 1\}$ ($\mathbb{Q}$ is the set of rational numbers}

Suppose $x_0 < x_1$, $x_0 \in \mathbb{Q}$ is a smallest element of this set $x_0 = \frac{m}{n} \quad m > n$

(missed)

Proving the irrationality of $\sqrt{2}$

- **Theorem** $\sqrt{2}$ is irrational.
- **Proof** Suppose $\sqrt{2}$ is rational (Proof by contradiction)
  $c = \{m \in \mathbb{N} | \exists n \in \mathbb{N}(\sqrt{2} = m/n)\}$
  Our assumption is equivalent to the statement $C \neq \emptyset$
  By the well-ordering principle there exists m_0 the smallest element of C
  $\sqrt{2} = \frac{m_0}{n_0} \rightarrow 2 = \frac{m_0^2}{n_0^2} \rightarrow 2n_0^2 = m_0^2 \rightarrow m_0 = 2m' \rightarrow 2n_0^2 = 4m'^2 \rightarrow n_0^2 = 2m'^2 \rightarrow n_0 = 2n' \rightarrow (2n')^2 = 2m'^2 \rightarrow 2n'^2 = m'^2 \rightarrow \sqrt{2}n' = m' \rightarrow \sqrt{2} = \frac{m'}{n'} \rightarrow m \in C$ but $m' < m_0$
- There is a contradiction as m_0 was chosen to be the smallest element of C.

7.1.2 Method

Structure of the proofs using well-ordering principle:
"P(n) is true for all positive integeres n" (In our theorem P(m) := "$\neg(\exists n \in \mathbb{N} \quad \sqrt{2} = \frac{m}{n})$"

1. $C = \{n \in \mathbb{N} |$ P(n) is False $\}$
2. Assume for a contradiction that $C \neq \emptyset$

3. By the well-ordering principle we can choose n_0 the smallest element of C
4. Obtain the contradiction to this choice (for example show that $n_0 \notin C$)

Theorem Every positive integer bigger than 1 can be expressed as a product of prime numbers (being prime counts).

Statement P(n) = "If n ¿ 1, then n can be expressed as product of prime numbers

C = $\{n \in \mathbb{N} : n > 1$ n can be expressed as such a product$\}$

Choose n_0 to be a smallest element of C (We are using proof by contradiction)

- Case 1: n_0 is prime
  This can't happen. n_0 by itself would be a valid product
- Case 2: n_0 is not prime
  $n_0 = ab \qquad 1 < a, b < n_0 \qquad a, b \in \mathbb{N}$
  Therefore as $a, b \notin C$, so $a = p_1 p_2 p_3 ... p_k \quad p_i$ is prime and $b = q_1 q_2 ... q_i \quad q_j$ is prime
  $n = p_1 p_2 p_3 ... p_k . q_1 q_2 q_3 ... q_k$ So n is a product of primes
  $n \notin C \rightarrow$ contradiction

What is the sum of the first n odd (+) integers? 1 + 3+ 5 +... + (2n-1)

$$1 = 11 + 3 \qquad = 41 + 3 + 5 = 91 + 3 + 5 + 7 \qquad = 16$$

It looks like the answer is n^2 (but this is not enough to prove it)

Theorem: $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$

Proof: Suppose for a contradiction that n_0 is the smallest positive integer for which this formula is false

$1 + 3 + 5 + ... + 2n - 1 \neq n_0$

The formula is true for $n_0 - 1 \qquad (n_0 \neq 1)$

$1 + 3 + 5 + ... + 2(n_0 - 1) - 1 = (n_0 - 1)^2$

So $1 + 3 + 5 + ... + (2n - 1) = (n_0 - 1)^2 + 2n_0 - 1 = n_0^2 \rightarrow$ contradiction!

7.2 Induction

Method "P(n) is true for all n $\in \mathbb{N}$ if

1. Base of induction: "P(1) is true"
2. Induction steps: "P(n-1) implies P(n) for all $n \geq 2$
   (Equivalently "P(n) implies P(n+1) for all $n \geq 1$"

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

7.2.1 A few examples

Sum of n first Integers

- **Theorem**: $1 + 2 + ... + n = \frac{n(n+1)}{2}$
- **Proof**: By induction on n
- **Base case n =1**: $1 = \frac{1}{1+1}/2 = 1$
- **Induction step:** $P(n) \rightarrow P(n+1) for n \geq 1$
  $1+2+...+n = \frac{n(n+1)}{2}$ $P(n+1) : 1+2+...+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = (n+1)\cdot(\frac{n}{2}+1) = \frac{(n+1)\cdot(n+2)}{2}\square$

$2^n \geq n^2$

- **Theorem**: $2^n \geq n^2 \forall n \geq 4$
- Base case: $n = 4, 2^4 = 16 = 4^2$
- Induction step: $(2^n \geq n^2) \rightarrow (2^{n+1} \geq (n+1)^2)$

$$\begin{aligned}
2^{n+1} &= 2^n \cdot 2 \\
&\geq 2n^2 = n^2 + n^2 \\
&\geq n^2 + 4n \qquad (n \geq 4) \\
&\geq n^2 + 2n + 1 = (n+1)^2 \qquad (2n \geq 1)
\end{aligned}$$

A flawed induction proof

- Theorem: All horses are the same colour
- Base Case: One horse is the same colour as its self
- Induction step: Any n horse are the same colour. Any n + 1 horses are the same colour.

Flaw: P(n) does not imply P(n+1)

8 Number Theory

Definition Studies properties of integers: divisibility, primes. an integer a divides an integer b $if \exists x \in \mathbb{Z}(xa = b)$

Division with remainder: for any two integers $a > 0$ and b there exists integers q and d so that $b = qa + r \rightarrow$ r is the remainder with $0 \leq r \leq a$

We write $a|b$, if and only if $r = 0$

A positive integer $p > 1$ is prime if the only positive integers dividing p are 1 and p

An integer $n > 1$ is composite if it is not prime

Expression of a positive as product of primes is called prime factorization. We have shown that every integer greater than 1 admits a prime factorization.

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

The fundamental theorem of arithmetic Every integer greater than 1 admits unique prime factorization

Proof using contradiction: Suppose some n admits at least two distinct prime factorizations. Choose the minimum such n.

$n = p_1p_2p_3...p_k = q_q1_2...q_l$

We may assume that p_1 is the smallest prime among all the primes p_i and q_j

Suppose $p_1 = q_1$ then $\frac{n}{p_i} = p_2...p_i = q_2...q_l$ It is a smaller number admitting two different factorizations

So $p_1 < q_1 soq1 = xp_1 + r \qquad 0 \leq r \leq p_1$

$pn = (xp_1 + r)q_2...q_i alsowemayassumeq_2, q_3, ...q_l \neq p_1$

$p_1|n$

$n = xp_1p_2...q_l + rq_2....q_l$

$nisdivisiblebyp_1$

$n > m > 1m = rq_2...q_l$ is divisible by p

$m < n$ as $x > 0$ because $q_1 > p_1 > r$

We will sow that m also has two different prime factorizations

$m = p_1m = p_1r_1r_2...r_s \rightarrow$ there exists a prime factorization of m which includes

A contradiction to the choice of..

8.1 Primes

Fundamental theorem of arithmetic Every integer greater than 1 can be uniquely expressed as a product of primes

$a = p_1^{r1}p_2^{r_2}...p_k^{r_k}$ $b = p_1^{s_1}p_2^{s_2}...p_k^{s_k}$

$1200 = 2^4 \cdot 3 \cdot 5^2$

$[ab = p_1^{r_1+s_1}p_2^{r_2+s_2}...p_k^{r_k+s_k}]$

$a|b$ if and only if $r_i \leq s_i$ for all $1 \leq i \leq k$

- **Theorem** $\sqrt{2}$ is irrational
- **Proof**: Suppose $\sqrt{2}$ is not
  then $\sqrt{2} = \frac{m}{n} = 2 = \frac{m^2}{n^2}$
  $(m = 2^r p_1^{r_1} \ldots p_i^{r_k})$
  $(m = 2^s p_1^{s_1} \ldots p_i^{s_k})$
  $(2n^2 = m^2)$
  $(2n^2 = 2^{2s+1} p_1^{2s_1} \ldots p_k^{2s_k})$
  $(2m^2 = 2^{2r} p_1^{2r_1} \ldots p_k^{2r_k})$
  Contradiction as $(2s + 1 \neq 2r)$
- **Theorem:** $\sqrt{n}$ is rational for any integer n if and only if $n = k^2$ for some k

Proof: Exercise. Modify the proof for $\sqrt{2}$

- **Theorem**: If a prime $p|ab$ then either p — a or p— b

- **Proof**: if p is not present in the prime factorization of either a or b, then it is not present in the prime factorization of $a \cdot b \cdot m$ and so $p \nmid ab\square$
- Is this true when p is not prime? Suppose we have $p_1 \cdot p_2$ instead of p_1 then $p_1|a$ or $p_1|b$ $\quad p_2|1$ or $p_2|b$

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$

1. There are infinitely many prime numbers.
2. Prime numbers are not everywhere dense in natural numbers. There are large gaps

- **Theorem** For any positive integer k there exists two consecutive prime numbers with difference $\geq k$
- **Proof** It suffices to exhibit a sequence of $\geq k$ consecutive composit numbers
  $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (n-1) \cdot n$
  Let $n = k + 1$
  $n! + 2, n! + 3, n! + 4, n! + 5, ..., n! + n \rightarrow k$ consecutive integers all composite $n! + m$ is composite for all $2 \leq m \leq n \qquad m|n! + m \leftarrow m|n! \qquad 2 \leq m \leq n! + m$
- **Twin prime conjecture** There exist infinitely many pairs $p, p+2$ so that they are both primes. (This question has been asked more than 2000 years ago.)
- **The prime number theorem:** For a number n let $\pi(n)$ denote the number of primes $\leq n$. Then $\pi(n)\ \frac{n}{\ln n} \qquad lim_{n\rightarrow\infty}\frac{\pi(n)}{n/\ln n} = 1$
  Average gaps between primes are $\tilde{\ln} n$
- **Conjecture** For every positive integer n there exists a prime p $n^2 \leq p \leq (n+1)^2$
  1. It is possible to efficiently test whether a number is prime or composite.
  2. It is believed not to be possible to efficiently produce prime factorisations.

8.2 Greatest common divisors and linear combinations

Die Hard 3 Problem A jug containing precisely 4 gallons of water deactivates the bomb. He has a 3 gallon, a 5 gallon jug and 5 minutes. Given an a-gallon jug and a b-gallon jug, what ammounts can we get?

$a \leq b$ let (x,y) record current amounts of water in jugs of size a and b respectively

Here is an example of our approach

1. (a,0) - fill in the first jug
2. (0,a) - pour first jug into the second
3. (a,a) - fill in the first one again
4. (2a-b, b) - pour first into second
5. (2a-b, 0) - empty the second jug
6. (0, 2a-b)
7. (a, 2a-b)
8. (0, 3a-b) $\rightarrow$ John Mclane survives

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

8.3 Linear Combinations

- A linear combination of a and b is an integer expressible as $sa + tb$ where both s and t are integers.
- **Claim 1** The amounts of water in jugs are always linear combinations of a and b.
  (By induction on the number of operations performed)
- **Question:** Which numbers can we express as linear combinations of a and b?

Theorem The amount of water in jugs is always a linear combination of a and b.

Let $L = \{m : m = sa + tb$ for some $s, t \in \mathbb{Z}$

1. $0, a, b \in L$ $0 = o \cdot a + 0 \cdot b$ $a = 1 \cdot a + 0 \cdot b$
2. $j_1, j_2 \in L$ then $j_1 + j_2 \in L, -j \in L$

Proof By induction on # steps performed

- Base case (0 steps): $(0, 0)$ $\quad 0 \in L$
- Induction step: Assume that after n steps we have amounts j_1, j_2 and $j_1, j_2 \in L$. we want to show that after the next step the amounts are still a linear combination.
  $(j_1, j_2) \rightarrow (0, j_2)$ or $(j_1, 0)$ or (a, j_2) or (j_1, b) or $(0, j_1+j_2)$ or $(j_1+j_2, 0)$ or (j_1+j_2-b, b) or (a, j_1+j_2-a)
  $j_1 + j_2 - b \in L$ and $j_1 + j_2 - a$
- Theorem If $a \leq b$, $c \leq b$. Then if c is a linear combination of a and b, it is possible to measure exactly c liters.
- Proof: $c = sa + tb$ for some $s, t \in \mathbb{Z}$
  - Case 1: $c = b$
  - Case 2: $c < b$ We may assume that $s > 0, t \leq 0$
    $c = (s + kb)a + (t - ka)b = sa + tb + kba - kab$
    Choose k large so that $s + kb > 0$
    $c = sa - tb \rightarrow$ fill in the jug with capacity a s times repeatedly and pour it into a jug with capacity b as soon as the jug with capacity b becomes full pour it out
    $sa = t'b + c'$
    $sa = tb + c$
    $0 \leq c, c' < b$
    $c' = sa - t'b \rightarrow$ amount we poured out
    $s \rightarrow$ total amount we took
    In the end we have amounts $(0, c')$
    Example:
    $b = 5, a = 3, c = 4$
    $4 = 3 \times 3 - 5$
    $(0, 0) \rightarrow (3, 0) \rightarrow (0, 3) \rightarrow (3, 3) \rightarrow (1, 5) \rightarrow (1, 0) \rightarrow (0, 1) \rightarrow (3, 1) \rightarrow (0, 4)$
    There are many more ways to achieve the same result.

What about $b = 6, a = 3, c = 4$ Do there exist integers s and t such as 3s + 6t = 4? d is a common divisor of a and b if d — a and d—b

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

Definition If d is a **common divisor** of a & b then every linear combination of a & b is divisible by d.

The largest common divisor of a and b is denoted by gcd(a, b) and is called the **greatest common divisor**.

Theorem $gcd(a, b)$ is the smallest positive linear combination of a and b.

Proof $d = gcd(a, b)$, let m be the smallest positive linear combination of an and b
$m = sa + tb$. We want to show that d = m.

1. $d \leq m$
   $d|m$ Because d is a common divisor of a and b and m is a linear combination
   $d \leq m$ as they are both positive
2. $m \leq d$
   It is enough to show that m is a common divisor of a and b.
   We'll show $m|a$ (showing $m|b$ is exactly the same).
   Proof:
   - Suppose not $m \nmid a$ dividing with remainder
     $a = qm + r \qquad 0 < r < m$ ($r \neq 0$ because $m \nmid a$)
   - $r = a - qsa - qtb = a(1 - qs) + (-qt)b$
   - r is a linear combination of a & b, contradicting the choice of m.

Corollary An integer c is a linear combination of a and b if and only if gcd(a,b) — c
Proof:

- If $c = sa + tb$ then $gcd(a, b)|sa$ and $gcd(a, b)|tb$ so $gcd(a, b)|c$
- On the other hand, we know $gcd(a, b) = s'a + t'b$ for some $s', t' \in \mathbb{Z}$
- If $c = dgcd(a, b) thenc = d(s'a + t'b) = (ds')a + (dt')b$

Midterm information

- **Material**:
  1. Logic and Proofs
  2. Number theory (up to modular arithmetic at the end of the week)

8.4 Greatest common divisors

Let a and b be positive integers. $c = gcd(a, b)$ is the largest integer c such as $c|a$ & $c|b$.

- **Theorem**:gcd(a, b) is the smallest positive linear combination of a & b.
- **Corollary**: c is a linear combination of a & b if and only if $gcd(a, b)|c$
- **Theorem**:
  1. $gcd(a, b)$ is divisible by every common divisor of a & b

2. $gcd(ka, kb) = k \cdot gcd(a, b)$ for any positive integer k
3. $gcd(a, b) = 1, \quad gcd(a, c) = 1 \rightarrow gcd(a, bc) = 1$
   If a and b do not have a common divisor and a and c do not have a common divisor then a and bc do not have anything in common either.
4. $gcd(a, b) = 1, a|bc \rightarrow a|c$
5. $a = qb + r \rightarrow gcd(a, b) = gcd(b, r)$

Proof of 3 $s_1 a + t_1 b = 1 \qquad s_2 a + t_2 c = 1$

It suffices to show that 1 is a linear combination of a and bc.

$1 = (s_1 \cdot a + t_1 \cdot b)(s_2 \cdot a + t_2 \cdot c) = a(s_1 \cdot s_2 \cdot a + s_1 \cdot t_2 \cdot c + s_2 \cdot t_1 \cdot b) + bc(t_1 \cdot t_2 \qquad)$ (can also be derived from prime decomposition)

Proof of 5 $d_1 = gcd(a, b) \qquad d_2 = gcd(b, r)$

- $d_1 \leq d_2$ It is enough to show that $d_1|b$ and $d_1|r$
  $d_1|b$ is trivial since d_1 is gcd(a, b)
  $r = a - qb$ a is divisble by d_1 and b is divisible by d_1 therefore d_1 divides r
- $d_2 \leq d_1$ It is enough to show that $d_2|a$ and $d_2|b$
  $d_2|b$ is trivial
  $a = r + qb$ since d_2 is a divisor of r and b then d_2 is a linear combination of r and b and $d_2|a$

9 Euclid's algorithm

9.1 Computing gcd with prime factorization

- $a = p_1^{r_1} \cdot p_2^{r_2} ... p_k^{r_k}$
- $b = p_1^{s_1} \cdot p_2^{s_2} ... p_k^{s_k} = p_1^{r_1} \cdot p_2^{r_2} ... p_k^{s_k}$
- $gcd(a, b) = p_1^{min(r_1, s_1)} \cdot p_2^{min(r_2, s_2)} ... p_k^{min(r_k, s_k)}$
- **Example**: $1200 = 2^4 \cdot 3 \cdot 5^2$
- $280 = 2^3 \cdot 5 \cdot 7$ $a = p_1^{r_1} \cdot p_2^{r_2} ... p_k^{s_k} =$
- $gcd(1200, 280) = 2^3 \cdot 5 = 40$

9.2 Computing gcd with Euclid's algorithm

$a = qb + r \qquad gcd(a, b) = gcd(b, r)$
$gcd(962, 230) = \qquad 962 = 4 \cdot 230 + 42$
$gcd(230, 42) = \qquad 230 = 5 \cdot 42 + 20$
$gcd(42, 20) = \qquad 42 = 20 \cdot +2$
$gcd(20, 2) =$
2

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

9.3 Statement of Euclid's algorithm

GCD(a, b)
Input: integers a & b (in binary)
Steps:

1. $a \geq b$
2. Divide with remainder $a = qb + r, 0 \leq r < b$
3. $If r = 0 \rightarrow$ **output** : b
4. Otherwise, run GCD(b,r)

9.4 Analysis of Euclid's algorithm

1. It is valid by part 5 of the preceding theorem ($a = qb + r \rightarrow gcd(a, b) = gcd(b, r)$)
2. It terminates in at most a + b $\rightarrow$ in each recursive step we replace a by r.
   So the sum of the inputs decreases.
3. Is it efficient (polytime)?
   We want to show that it terminates in $O((loga + logb)^k)$
   - **Claim**: $a = qb + r \qquad 0 \leq r \leq b, a \geq b$ then $ab \geq 2br$
   - **Proof**: We need to show that $a \geq 2r$
     $q \geq 1 \rightarrow a \geq b + r \rightarrow a \geq r + r = 2r$
   - The claim implies that the product of the inputs is reduced by at least a factor of 2 in each step.
     So there are at most $\log(ab)$ steps in recursion
     $\log(ab) = \log a + \log b \rightarrow$ **linear algorithm**

9.5 Expressing gcd(a,b) as a linear combination of a & b

$gcd(962, 230) = \qquad 962 = 4 \cdot 230 + 42$
$gcd(230, 42) = \qquad 230 = 5 \cdot 42 + 20$
$gcd(42, 20) = \qquad 42 = 20 \cdot +2$
$gcd(20, 2) =$
2

$$\begin{aligned} 2 &= 42 - 2 \cdot 20 \\ &= 42 - 2 \cdot (230 - 5 \cdot 42) \\ &= 11 \cdot 42 - 2 \cdot 230 \\ &= 11 \cdot (962 - 4 \cdot 230) - 2 \cdot 230 \\ &= 11 \cdot 962 - 46 \cdot 230 \end{aligned}$$

```
Wesley's notes. Will format later.

== Euclid's Algorithm ==
```

The algorithm takes at most <> iterations to terminate.

Each individual step can also be performed quickly. (Division with remainder)

Arithmetic operations: additions, multiplication, division with remainder take time polynomial in input

Input is usually in binary.

=== Adding ===

<>

<>

<>

Adding a & b takes <>

=== Multiplication ===

Multiplication is similar. At most <>

=== Division ===

Division with remainder can also be done efficiently

Each individual step can also be performed quickly. (Division with remainder)

Aritmetic operations addition, multiplication, division with remainder take time polynomial in input si

9.6 Homework problem

:

Show that deciding whether $ax^2 + by = c$ has an integer solution for given $a, b \leq c$ in NP.

Size of the input; $log_2 a + log_2 b + log_2 c$

Certificate $x \& y$ such that $ax^2 + by = c$

Essence of the problem : If there exists x & y which solve the solution, then there exist x_0, y_0 so that $ax_0 + b \cdot y \cdot b_{y_0} = c$ and x_0 and y_0 are not too large

$x_0 y_0 = 0((a + b + c)^n)$

General diophantine equation :

$P(x_1, x_2, ..., x_k) = 0$ where P is polynomial with integer coefficients.

E.g. $x_1 x_2 x_3 - 5x_1 + 1000 = 0$

Not in NP in general, there is no systemic algorithm to figure out if it has a solution or not.

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

Euclid's algorithm takes at most $log_2 a + log_2 b$ steps (but maybe it always terminates in 5 or $\log(\log a)$

In worst case scenario is takes $\Omega(log_2 a + log_2 b)$ steps

Example: Fibonacci numbers: $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3$

1, 1, 2, 3, 5, 8, 13, 21 $\rightarrow F_n = F_{n-1} + F_{n-2}$

Running Euclid's algorithm to compute $gcd(F_n, F_n + 1)$

$F_n = F_{n-1} + F_{n-2}$

$F_{n-1} = F_{n_2} + F_{n-3}$

$F_n = 1 + \sqrt{5}/2^{n+1}/\sqrt{5}$

10 Modular arithmetic

10.1 Notation

We say that a is **congruent** to b **modulo** m if $m|a-b$. We note it $a \equiv b(modm)$

$rem(a,m)$: the remainder of a after division by m

$a = km + rem(a,m)$

$0 \leq rem(a,m) < m$

Fact: $a \equiv b(modm)$ if and only if $rem(a,m) = rem(b,m)$ **Proof**: $a = k_1 m + rem(a,m)$

$b = k_2 m + rem(b,m)$

$0 \leq rem(a,m), rem(b,m) < m$

If $rem(a,m) = rem(b,m)$ then $a - b = (k_1 - k_2)m$. Therefore $a = b(modm)$

$a - b = (k_1 - k_2)m + (rem(a,m) - rem(b,m)$

Therefore r$em(a,m) = rem(b,m) = 0$.

In many senses you can operate with congruences as with equations.

Theorem: (Properties of congruences)

1. **Reflexitivity** $a \equiv a(\mod m)$
2. **Symmetry** $a \equiv b(\mod m)$ if and only if $b \equiv a(\mod m)$
3. **Transitivity** if $a \equiv b(\mod m) \quad \& \quad b \equiv c(\mod m)$ then $a \equiv c(\mod m)$

Suppose $a \equiv b(\mod m), c \equiv d(\mod m)$:

Then:

1. $a + b \equiv b + d(\mod m)$
2. $ac \equiv bd(\mod m)$

Proof: 1, 2, 3: is based on the preceding fact 3. If $rem(a,m) = rem(b,m) and rem(b,m) = rem(c,m), then rem(a,m) = rem(c,m)$.4.m — a - b,m — c - d$therefore$m — (a-b) + (c-d) = (a + c) - (b + d)