MATH 240 - Discrete Structures

McGill University
Fall 2011

Last Updated: December 17, 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
- 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

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.” → valid proposition
- ”What is going on?” → not a proposition
- ”Stop at the red light” → 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

Making tables in LaTeX is so tedious. Check out Wesley’s notes.

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

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. $p(x) = xq(x) \rightarrow p(0) = 0 \cdot q(0) \rightarrow q(0) = 0$
- Proof by contradiction: $(p \rightarrow q) \leftrightarrow ((\neg q) \rightarrow (\neg p))$
- 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"
  $\neg p$ = "$n \leq m$" $\neg q \rightarrow \ \neg p$ 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 $\rightarrow \begin{cases} 1 \text{ (or T) if at least 2 of p, q \& r are 1's} \\ 0 \text{ (or F) otherwise} \end{cases}$

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 and the P $\neq$ 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 $x_{\frac{n}{2}}$ 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 $a, b > 1$ such that $c = a \times b$
   - 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 P problems

A **polytime algorithm** is an algorithm whose running time is in order p(n) for some polynomial p.

A **decision problem** is a problem with a yes/no answer.
Example:

- Input: a combinatorial circuit C (with n inputs)
- Output: Is C **not** a contradiction? In other words, will C output T.

Given a decision problem D, D is in class P if there exists a polytime algorithm which solves D. It is considered to be ”fast” or ”efficient”.

4.3 NP problems (non-deterministic polynomial time)

A decision problem is in the class NP if a ”yes” answer always has a certificate which can be verified in polynomial time. In other words, if there is an easy way to check that the answer is yes **when** the answer is yes.

4.3.1 The magician

Suppose that King Arthur poses a yes/no problem to his magician Merlin. To answer such a question seems to require a tremendous amount of toil. On the other hand, if the answer to the problem is yes, there is a piece of evidence or **certificate** to quickly verify the yes-ness.

Examples

- In the circuit example above, if there exists a set of values for inputs so that the circuit outputs 1 (or T) then given this collection of inputs, we can easily verify that the circuit is not contradictory.
- Traveling salesman problem:
  - Input: Collection of n cities where the ith city is located at (x_i, y_i) and the distances between them
  - Output: A tour such that each city is visited exactly once and the total length ≤ 1000 miles
  - Checking each possible tour amounts to (a) fixing some city from which to start then (b) choosing a second city (999 choices) and a third city (998 choices and so on. Thus the number of tours is 999!. This requires a tremendous amount of computation that is way beyond polynomial time.
  - If however, you somehow come up with a tour (use magic), you can easily test if it matches the requirements by computing the sum of distances between two adjacent cities i.e. $\sqrt{(x_{1000} - x_1)^2 + (y_{1000} - y_1)^2} + \sum \sqrt{(x_i - x_{i+1})^2 + (y_i - y_{i+1})^2} \leq 1000$
  - It doesn't matter if Merlin didn't heck all 999! possible tours, only that he found one that worked and that we could prove quickly that it did work
- Factoring
  - Input: n digit number
  - Output: Is this number composite and if it is, factor it.
  - If the magician comes up with a set of factors, it is easy to check if the factors are prime and easy to check if their product is the n-digit number.

4.3.2 Definition

A decision problem D is in class NP if there is a polytime algorithm M (called the checking algorithm) and a polynomial p which given an input and some ”extra information” called certificate can verify that x is indeed in L.

It is easy to see that $P \subseteq NP$ i.e. every P-class decision problem is in class NP since if A is a polytime algorithm which solves the decision problem D, then it will also suit as the checking algorithm in the definition of NP. We do not even need a certificate to prove it.

4.4 $P \neq NP$

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 $P \neq NP$

4.4.1 Scott Aoronson'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.

(N.B. I don't know what this is supposed to mean. Here's a Scott Aoranson quote though:

If P = NP, then the world would be a profoundly different place than we usually assume it to be. There would be no special value in "creative leaps," no fundamental gap between solving a problem and recognizing the solution once it's found. Everyone who could appreciate a symphony would be Mozart; everyone who could follow a step-by-step argument would be Gauss...)

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 such as $n = 3q + r \qquad q \in \mathbb{N}, 0 < r < 3$
  - $r = 1 \to n = 3q + 1$
    $n^2 + 2 = 9q^2 + 1 + 6q + 2 = 3 \cdot (3q^2 + 2q + 1)$
    therefore divisible by 3
  - $r = 2 \to n = 3q + 2$
    $n^2 + 2 = 9q^2 + 4 + 12q + 2 = 3 \cdot (3q^2 + 6q + 2)$
    therefore divisible by 3

Counter 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
  - $p \to q \wedge r \to p \to q$ if $\neg(p \to q) \to \neg(p \to q \wedge r)$
  - 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", $n > 2 \to (\exists a, b \in \{primes\}(n = a + b)))$
- In predicate calculus, "71 is prime" is equivalent to the notation:
  $\forall a, b \in \mathbb{N}(a \cdot b = 71) \to ((a = 1) \wedge (b = 71))$

Limits Various ways to say the same thing:

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

Negation

- $\neg(\forall n \in A : P(n)) \leftrightarrow \exists n \in A \quad (\neg P(n))$
- $\forall n \in A : P(n) \leftrightarrow \neg(\exists n \in A \quad (\neg P(n)))$
- This is very useful in proofs, since proving $(\forall n \quad (p(n))$ might be hard if we consider all values of n, whereas checking that there can't be a value of n such that p(n) does not hold could be easier.

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

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

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

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. $\forall i, j : 1 \leq i < j \leq k \qquad A_i \cap A_j = \emptyset$ (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} can be partitioned into {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 $(\forall i \quad (\exists a, b \in A_i \quad (a|b \vee b|a)))$

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 there 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 are at least 3 people that x does not know. Now the argument is in case 1 with acquaintances replaced by strangers.

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 $C > B > A$

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:

$A >^{v_2} B >^{v_2} C >^{v_2} D$ where $>^{v_i}$ 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 $f(>^{v_1}, >^{v_2}, , ..., >^{v_n}) = \;\; >$

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
$(\forall v \quad (\alpha >^{v} \beta)) \rightarrow (\alpha > \beta)$
2. **Independence on irrelevant alternatives (IAA)** The final relative ordering of α and β (higher, lower or indifferent) should depend only on relative orderings of α and β by every individual (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 $(\alpha >^{d} \beta)$ i.e. society prefers α to β whenever d strictly prefers α to β

6.2 Arrow's impossibility Theorem (1951)

Theorem: Any constitution that respects independence of irrelevant alternatives and unanimity is a dictatorship.

Proof Unanimity $\wedge$ IIA $\rightarrow$ 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

$$\left|\begin{array}{c|c|c|c} \beta & \beta & \alpha & \gamma \\ \alpha & \gamma & \gamma & \alpha \\ \beta & \beta & \dots & \beta \\ v_1 & v_2 & \dots & v_n \end{array}\right| \rightarrow \left|\begin{array}{c|c|c|c} \beta & - & - & - \\ \alpha & \gamma & \gamma & \alpha \\ - & \beta & \dots & \beta \\ v_1 & v_2 & \dots & v_n \end{array}\right|$$

So there exists a voter v^* so that $\left|\begin{array}{c|c|c|c} \beta & - & - & - \\ \alpha & \gamma & \gamma & \alpha \\ - & \beta & \dots & \beta \\ v_1 & v_2 & \dots & v_n \end{array}\right|$

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
  $n = p_1 p_2 p_3 ... p_k . q_1 q_2 q_3 ... q_k \quad$ 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)

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

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 $n \geq 1$"

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:** $P(n) \to P(n+1) for n \geq 1$
  $1+2+...+n = \frac{n(n+1)}{2}$ $P(n+1) : 1+2+...+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = (n+1)\cdot(\frac{n}{2}+1) = \frac{(n+1)\cdot(n+2)}{2}\square$

$2^n \geq n^2$

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

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

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 $(\exists x \in \mathbb{Z} : \quad (xa = b)$

Division with remainder: for any two integers $a > 0$ and b there exists integers q and d so that $b = qa + r \to$ 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 integer as product of primes is called prime factorization.

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.

$n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_l$

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 $\dfrac{n}{p_i} = p_2 \cdot ... \cdot p_k = q_2 \cdot ... \cdot q_l$

It is a smaller number admitting two different factorizations

$p_1 < q_1$ so $q1 = xp_1 + r \qquad 0 \leq r \leq p_1$

$n = (xp_1 + r)q_2...q_i$ also we may assume $q_2, q_3, ...q_l \neq p_1$

$p_1|n$

$n = xp_1 \cdot q_2 \cdot ... \cdot q_l + r \cdot q_2 \cdot .... \cdot q_l$

n is divisible by p_1

$n > m > 1 \qquad m = r \cdot q_2...q_l$ is divisible by p_1

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

We will sow that m also has two different prime factorizations

$m = p_1 m = p_1 r_1 r_2 ... r_s \rightarrow$ there exists a prime factorization of m which includes

A contradiction to the choice of..

(missed)

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 $\sqrt{2} = \frac{m}{n} = 2 = \frac{m^2}{n^2}$
  $(m = 2^r p_1^{r_1} \dots p_k^{r_k})$
  $(n = 2^s p_1^{s_1} \dots p_k^{s_k})$
  $(2n^2 = m^2)$
  $(2n^2 = 2^{2s+1} p_1^{2s_1} \dots p_k^{2s_k})$
  $(m^2 = 2^{2r} p_1^{2r_1} \dots p_k^{2r_k})$
  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 $a \cdot b$ and so $p \nmid ab$
- 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 composite 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
  $\pi(n) \cong \frac{n}{\ln n} \qquad lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\ln n} = 1$
  Average gaps between primes are $\cong \ln n$
- **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) → John Mclane survives $3 \cdot 3 - 5 = 4$!

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.
  $(j_1, j_2) \to (0, j_2)$ 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 $s + kb > 0$
    $c = sa - tb \to$ 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

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

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 → 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

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

$gcd(42,20) =$ $\quad 42 = 20 \cdot +2$
$gcd(20,2) =$
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; $log_2a + log_2b + log_2c$

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

Essence of the problem : If there exists x & y which solve the solution, then there exist some x_0, y_0 so that $ax_0^2 + b \cdot y_0 = c$ and x_0 and y_0 are not too large

With x_0 and y_0 of polynomial size of some power of fixed size k

$x_0andy_0 = O((a + b + c)^k)$

General diophantine equation : It is not always the case that a certificate is of reasonable size. Famous example:

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

E.g. $x_1x_2x_3 - 5x_1 + 1000 = 0$

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

Back to Euclid Euclid's algorithm takes at most $log_2a + log_2b$ steps (but maybe it always terminates in 5 or $\log(\log a)$

In worst case scenario is takes $\Omega(log_2a + log_2b)$ 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**: $a = k_1m + rem(a, m)$

$b = k_2m + rem(b, m)$

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

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 $rem(a,m) = rem(b,m) = 0$.

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 $a \equiv b(\mod m)$ & $b \equiv c(\mod m)$ 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 $m|(a - b) + (c - d) = (a + c) - (b + d)$

Reminder: Congruences $a \equiv b(modm)$ if $m|a - b$

1. $a \equiv b(modm)$ if and only if a and b have the same remainde after division by m
2. $a \equiv b(modm)$ $c \equiv d(modm)$ then
   $a + c \equiv b + d(modm)$
   $a \cdot c \equiv b \cdot d(modm)$
   Proof: $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$
   Since $(a - b)$ and $(c - d)$ are divisible by m then $(ac - bd)$ is divisible by m

10.2 Multiplicative inverses

What about division for congruences? Turing's code:
Select p: a large prime number.
Let a message be represented by a number $0 \leq m \leq p$.
Choose a key k which also is going to be $0 \leq k \leq p$, transmit the remainder of mk after division by p.

$0 \leq m^* \leq p$
$m^* = m(modp)$

Two questions:

1. Can our counterpart decode m from p, m^*, k?
2. How vulnerable is this code? (How easy is it to figure out k?)

We say that $\bar{k}$ is a multiplicative inverse for k modulo p

$\bar{k} \cdot k = a(modp)$

If we have a multiplicative inverse, then we can decode m.

$$m^* \equiv mk(mod p)$$
$$m^*\bar{k} \equiv m(k \cdot \bar{k}) \equiv m(mod p)$$

So m is just the remainder of $m^*\bar{k}$ after division by p

Theorem If p is a prime, k is non divisible by p, then there exists a multiplicative inverse for k (mod p).

Proof: We want to find $\bar{k}$ such that:
$k\bar{k} - 1 = tp$
$k\bar{k} - tp = 1 \rightarrow$ linear combination of k and p equal to 1

We can find such $\bar{k}$ and t if and only if $gcd(k,p) = 1$.

Why is the greatest common divisor of k and p?

$gcd(k,p)|p$ so $gcd(k,p) = 1$ or $gcd(k,p) = p$ Second is impossible as $p \nmid k$

Example:

Find a multiplicative inverse for 10 modulo 17.

We need to express 1 as a linear combination of 10 and 17.

We use Euclid's algorithm:

$17 = 10 + 7$ (remainder of the division of 17 by 10)
$10 = 7 + 3$
$7 = 2 * 3 + 1$

We track-back to get:

$1 = 7 - 2 \cdot 3$
$1 = 7 - 2 \cdot (10 - 7) = 3 \cdot 7 - 2 \cdot 10$
$1 = 3 \cdot (17 - 10) - 2 \cdot 10 = 3 \cdot 17 - 5 \cdot 10$

-5 is a multiplicative inverse for 10
$-5 \equiv -5 + 17(mod 17) \equiv 12(mod 17)$

Decoding Turing's code :

$p = 17, k = 10, m = 3$
We send m^* remainder $3 \cdot 10 = 30$ after division by $17 \rightarrow 13$
Counterparty receives **13**.

$13 \cdot 12 = 156 = 17 \cdot 9 + 13$

Corollary If p is a prime,

$p + k$ $xk \equiv yk(mod p)$ then $x \equiv (mod p)$

Proof $(xk)\bar{k} \equiv (yk)\bar{k}(modp)$ where $\bar{k}$ is multiplicative

$x(k\bar{k}) \equiv y(k\bar{k})(modp)$

$x \equiv y(modp)$ Q.E.D.

If $p \neq 2$, $2x \equiv 2y(modp)$ then $x \equiv y$

Note: Cancellation does not work on modulo composite numbers.

- $2 \neq 0(mod4)$

- $2 \times 2 \equiv 0(mod4)$

10.3 Fermat's Little Theorem

Let p be a prime $p \nmid k$

then $k^{p-1} \equiv 1(modp)$. (e.g. 2^{1000} has remainder 1 after division by 101)

Proof: $1, 2, ..., p-1$ for every number i in this collection. Let r_i be the remainder of k_i after the division by p

$(r \equiv k_i(modp) \quad 0 \leq r_i < p$

We get a collection of members, $r_1, r_2, r_3, ..., r_{p-1}$.

- $1 \leq r_i \leq p-1$ because $p \nmid k_i$ for $i = 1, 2, ..., p-1$
- $r_i \neq r_j$ for $i \neq j \qquad k_i \neq k_j$ for $i \neq j \qquad i \leq i, j < p-1$
  So $r_1, r_2, ..., r_{p-1} = 1, 2, ..., p-1$ (perhaps in different order)
  $r_1, r_2, ..r_{p-1} = 1 \cdot 2 \cdot ... \cdot (p-1) = (p-1)!$ On the other hand, $r_i \equiv k_i(modp)$
  $(p-1)! = r_1, r_2, ..r_{p-1} \equiv (1 \cdot k)(2 \cdot k)(3 \cdot k)....(p-1)k = k^{p-1} \cdot (p-a)!$
  $(p-1)! = k^{p-1} \cdot (p-1)!(modp)$
  We can cancel (p-1)! as long as $p \nmid (p-1)!$
  The product of numbers all smaller than p. So none of them is divisible by p, therefore the product is not.
  Cancelling $(p-1)!$ gives the theorem.

Corollary: $k \cdot k^{p-2}$ is a multiplicative inverse for k modulo p if $p \nmid k$.

Fermat's test if $2m \nmid t^{m-1} - 1$ then m is composite or $m = 2$.

10.4 Side-Note: The proof on the midterm exam

$$gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right)$$

Incorrect proof:

You cannot just say $gcd(\frac{a}{gcd(a,b)}, b) = 1$, as it can be greater than 1.

If $a = 16$ and $b = 24$, then $gcd(\frac{16}{8}, 24) = 2$.

Proof 1:

For every positive integer k, $gcd(ka, kb) = k \cdot gcd(a, b)$

$$gcd(a, b)gcd(\frac{a}{gcd(a, b)}, \frac{b}{gcd(a, b)}) = gcd(\frac{gcd(a, b) \cdot a}{gcd(a, b)}, \frac{gcd(a, b) \cdot b}{gcd(a, b)}) = gcd(a, b)$$

$$\rightarrow gcd(\frac{a}{gcd(a, b)}, \frac{b}{gcd(a, b)}) = 1$$

Proof 2: By contradiction

Suppose $d = gcd\left(\frac{a}{gcd(a, b)}, \frac{b}{gcd(a, b)}\right) > 1$

$d|gcd\left(\frac{a}{gcd(a, b)}\right) \qquad d|gcd\left(\frac{b}{gcd(a, b)}\right)$

$d \cdot gcd(a, b)|a \qquad d \cdot gcd(a, b)|b$

$d \cdot gcd(a, b)$ is a common divisor of $a\&b \rightarrow$ Contradiction ■

Proof 3

$a = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot ... \cdot {p_k}^{r_k}$

$b = {p_1}^{s_1} \cdot {p_2}^{s_2} \cdot ... \cdot {p_k}^{s_k}$

$gcd(a, b) = {p_1}^{min(r_1,s_1)} \cdot {p_2}^{min(r_2,s_2)} \cdot ... \cdot {p_k}^{min(r_k,s_k)}$

$\frac{a}{gcd(a, b)} = {p_1}^{r_1 - min(r_1,s_1)} \cdot {p_2}^{r_2 - min(r_2,s_2)} \cdot ... \cdot {p_k}^{r_k - min(r_k,s_k)}$

$\frac{b}{gcd(a, b)} = {p_1}^{s_1 - min(r_1,s_1)} \cdot {p_2}^{s_2 - min(r_2,s_2)} \cdot ... \cdot {p_k}^{s_k - min(r_k,s_k)}$

$$gcd\left(\frac{a}{gcd(a, b)}, \frac{b}{gcd(a, b)}\right) = p_1^{min(r_1 - min(r_1,s_1), s_1 - min(r_1,s_1))} \cdot ... \cdot p_k^{min(r_k - min(r_k,s_k), s_k - min(r_k,s_k))}$$

$$\forall(1 \leq i \leq k) \begin{cases} r_i \leq s_i \rightarrow min(r_i - min(r_i, s_i), s_i - min(r_i, s_i)) = min(r_i - r_i, s_i - r_i) = min(0, s_i - r_i) = 0 \\ s_i \leq r_i \rightarrow min(r_i - min(r_i, s_i), s_i - min(r_i, s_i)) = min(r_i - s_i, s_i - s_i) = min(r_i - s_i, 0) = 0 \end{cases}$$

$$gcd\left(\frac{a}{gcd(a, b)}, \frac{b}{gcd(a, b)}\right) = p_1^0 \cdot p_2^0 ... \cdot p_k^0 = 1$$

10.5 Applications of Fermat's Little Theorem

Theorem: If p is prime, $p \nmid a$ then $a^{p-1} \not\equiv 1(modp)$

Corollary: a^{p-2} is a multiplicative inverse for $a(modp)$
(Our previous method computed multiplicative inverse for a by expressing 1 as a linear combination of $p\&a$.)

Example 1: Multiplicative inverse for 5 (modulo 17)

How can we compute $5^{15}(mod 17)$ quickly?

1. Let's first compute $5^5(mod17)$:
   $5^2 = 25 \equiv 8(mod17)$
   $5^4 = (5^2)^2 \equiv 8^2 = 64 = 3 \cdot 17 + 13 \equiv 13(mod17)$
   $5^4 \cdot 5 = 13 \cdot 5 = 65 \equiv 14(mod17) \quad 5^5 = 5^4 \cdot 5 \equiv 135 = 65 \equiv 14(mod17)$

2. Compute $(5^5)^3 = 14^3(mod 17)$
   $14^3 \equiv (-3)^3 = -27 \equiv 10 \equiv 17 - 10 = 7(mod 17)$

Conclusion: $7 \cdot 5 \equiv 1(mod 17)$

Example 2: Compute $3^{100}(mod 7)$

$$\begin{aligned} 3^6 &\equiv 1(mod 7) \\ (3^6)^k &\equiv 1^k = 1(mod 7) \\ 100 &= 6k + r = 6 \cdot 16 + 4 \\ 3^{6k+r} &\equiv 1 \cdot 3^r = 3^r(mod 7) \\ 3^100 &\equiv 3^4(mod 7) = 81(mod 7) = 4(mod 7) \end{aligned}$$

Example 3: Compute $3^{100}(mod 21)$

$$\begin{aligned} 3^{100} &\equiv r(mod 21 = 7 \cdot 3) \to 0 \le r < 21 \\ 21|3^100 - r &\to 3|r \\ r &= 3s \to 0 \le s \le 6 \\ 3^{100} &\equiv 3^4 \equiv 81 = 77 + 4 \equiv 4(mod 7) \\ 3^{100} &\equiv r(mod 7) \\ r &\equiv 4(mod 7) \\ r &= 3s \equiv 4(mod 7) \end{aligned}$$

$\to$ Solve $3s \equiv 4(mod 7)$
Find multiplicative inverse for $3(mod 7)$

$$\begin{aligned} 3^5 &\equiv (3^2)^3 \cdot 3 \equiv 9^2 \cdot 3 \equiv 2^2 \cdot 3 \equiv 42 \equiv 5(mod 7) \\ s &= 5 \cdot 3s \equiv 4 \cdot 5 = 20 \equiv 6(mod 7) \\ s &= 6 \end{aligned}$$

Answer: $3^{100} \equiv 3 \cdot 6 \equiv 18(mod 21)$

In our computations, we implicitly relied on number,the fact that if we know the remainder of a number (3^100) modulo 3 and modulo 7, then we can compute the remainder modulo $3 \cdot 7 = 21$.

10.6 Testing primality

10.6.1 Fermat's test

Corollary: If $2^{n-1} \not\equiv 1(mod n)$ then n is not prime or $n = 2$.

Algorithm: Fermat's test

1. Compute $2^{n-1}(modn)$
2. If the remainder of $2^{n-1}(modn)$ is not 1 (and $n \neq 2$), output "n is composite".

Issues with this algorithm:

1. We want to efficiently compute the remainder of $2^{n-1}(modn)$
2. We don't have guarantees that this algorithm detects all composite numbers.
   In fact, $2^{560} \equiv 1(mod561)$ and 561 is composite.

Questions:

1. Is this algorithm efficient (polytime)?
2. Does it recognize all composite numbers?

Answers

1. We can compute $2^{n-1}(modn)$ (the remainder of 2^{n-1} after division by n) in time polynomial in $log_2 n$

   Procedure:

   (a) Write down binary representation of $n-1$
   $n-1: \quad n-1 = 2^{k_1} + 2^{k_2} + ...2^{k_r} \qquad k_1 > k_2 > ... > k_r$
   $2^{n-1} = 2^{2^{k_1}} \cdot 2^{2^{k_2}} \cdot ... \cdot 2^{2^{k_r}} \qquad k_1 \leq log_2 n, \quad r \leq log_2 n$

   (b) Computing 2^{2^k} quickly: → Using at most $O((\log_2 n)^3)$ elementary operations
   $2^{2 \cdot 2 \cdot 2 \cdot ... \cdot 2} = ((((2^2)^2)^2)^2)$
   Thus we can square a number efficiently (in time $\leq (log_2 n)^2$) and we need to repeat this procedure $k \in log_2 n$ time).
   (We work with congruence classes modulo n and so never perform arithmetic with numbers larger than n).
   This procedure takes time $\leq O(log_2 n^4)$.

   Example: Use Fermat's test for $n = 35$.

   Compute $2^{34}(mod\ 35)$

   $$34 = 32 + 2$$
   $$2^{34}\ (mod\ 35) = 2^{32} \cdot 2^2\ (mod\ 35) = 2^{2^5} \cdot 2^2\ (mod\ 35)$$

   1 : $2^2 = \mathbf{4}\ (mod\ 35)$

   2 : $4^2 = \mathbf{16}\ (mod\ 35)$

   3 : $16^2 = 256 = 7 \cdot 35 + \mathbf{11}\ (mod\ 35)$

   4 : $11^2 = 121 = 3 \cdot 35 + \mathbf{16}\ (mod\ 35)$

   5 : $(16^2)^2 \equiv \mathbf{11}^2\ (mod\ 35) \equiv 16\ (mod\ 35)$

   6 : $16^{2^3} = (16^{2^2})^2 \equiv \mathbf{16}^2\ (mod\ 35) \equiv 11\ (mod\ 35)$

   $16^{2^3} = (2^4)^{2^3} = 2^{2^5} \equiv 11\ (mod\ 35)$

   $2^{34} = 2^{32} \cdot 2^2 \equiv 11 \cdot 4 = 44 \equiv 9\ (mod\ 35)$

2. Fermat's test does not detect all composite numbers (example: $n = 561$)
   $2^{560} \equiv 1(mod\ 3 \cdot 11 \cdot 17 = 561) foralla : gcd(a, 561) = 1$
   $3 \cdot 11 \cdot 17 | 2^{560} - 1 \rightarrow 3 | 2^{560} - 1 \qquad 11 | 2^{560} - 1 \qquad 17 | 2^{560} - 1$

$2^{560} \equiv 1(mod\ 3)$
$2^{10} = 1(mod\ 11)$
$2^{560} = 2^{10\cdot 56} = (2^{10})^{56} \equiv 1^{56} = 1(mod\ 11)2^{16} \equiv 1(mod 17)$
$2^{560} \equiv 2^{16\cdot 35} \equiv 1^{35} = 1(mod\ 17)$
$\rightarrow a^{560} \equiv 1(mod\ 3\cdot 11\cdot 17 = 561)$
A number n with the property that n is composite but $a^{n-1} \equiv 1(mod\ n)$ for all a such that $gcd(a, n) = 1$ is called a **Carmichael number**. There are infinitely many of such numbers.

10.6.2 Miller-Rabin's test

Definition Miller-Rabin's test is an improvement of Fermat's test

if $n-1$ is even test if $n \mid a^{\frac{n-1}{2}} - 1$ or $n \mid a^{\frac{n-1}{2}} + 1$

if $\dfrac{n-1}{2}$ is even instead of working with $a^{\frac{n-1}{2}} - 1$ repeat the procedure again.

If none of the terms in the factorization is divisible by n → n is composite.

Example:

$$\begin{aligned}561|a^{560} - 1 &= (a^{280})^2 - 1 = (a^{280} - 1)(a^{280} + 1)\\ &= ((a^{140})^2 - 1)(a^{280} + 1) = (a^{140} - 1)(a^{140} + 1)(a^{280} + 1)\\ &= (a^{70} - 1)(a^{70} + 1)(a^{140} + 1)(a^{280} + 1)\\ &= (a^{35} - 1)(a^{35} + 1)(a^{70} + 1)(a^{140} + 1)(a^{280} + 1)\end{aligned}$$

For $a = 2$, none of the factors is divisible by 561.

At least $\frac{3}{4}$ of all numbers $2 \leq a \leq n$ work for Miller-Rabin's test.

Performing the test once has probability $\dfrac{3}{4}$ of success, but performing the test twice has probability of failure $1 - (\dfrac{1}{4})^2$. More generally, performing the test k times has probability of failure $(\dfrac{1}{4})^k$

Probabilistic algorithms← typically easy to implement.

If Generalized Riemann's Hypothesis is true, then testing all numbers a between 1 and $c(\log n)^2$ always works.

11 Crytography

Alice wants to send Bob a message M, but is warned that a counterparty (Eve) might intercept the message.

One way of performing this;

- Alice encrypts M and sends f(M)
- Bob receives f(M), decrypts it by computing $f^{-1}(f(M))$
- If Eve intercepts f(M), she sees gibberish

f is called the encryption key (lock). f^{-1} is called the decryption key.

1. f(M) should not contain any useful information about M. We should be really careful with the encryption procedure.
   Example 1: Caesar's code (letter shifting)

   - A → D
   - B → E
   - Z → C

Replace each letter by a letter three places further in the alphabet.
This can be broken by trying all 26 possible shifts.
Example 2: Substitution ciphers
f(A, B, C, ..., Z) → A, B, C, ..., Z → a one-to-one function with a permutation of the alphabet
Replace every letter in a message by f(.)
With 26 letters, how many possible substitution ciphers are there? Answer: 26! roughly 10^{26}
26 choices for f(A), 25 choices for f(B), 24 choices for f(C), ...
Substitution ciphers are still breakable by frequency analysis. Most common letters in order: E, T, A, O, U, I
We could try to match up letters according to their frequencies. The msot common combination of 2 consecutive letters → TH
Repeated letters: SS or TT
FZJRM YYJFP VGHLJ UFZJD MFFUJ VV
FZJ → most common letters → THE

- F, J → 5
- V → 3
- M, Y, Z, V → 2

Example 3: Unbreakable method (One-time pad)
Alice and Bob agree on a key K = 0110101110
Alice encodes the message M in binary and M = 1100010111 and then sends $M \oplus K$

$$\begin{aligned} M &= 1100010111 \\ K &= 0110101110 \\ M \oplus K &= 1010111001 \end{aligned}$$

Since $(p \oplus q) \oplus q \leftrightarrow p$, Bob can retrieve the original message by performing $(M \oplus K) \oplus K$
For Eve, decoding the message amounts to guessing K and there is no statistical information present in $(M \oplus K)$.
This code becomes vulnerable is a key is repeated.
If Eve intercepts $M_1 \oplus K$ and $M_2 \oplus K$:
She can compute $(M_1 \oplus K) \oplus (M_2 \oplus K) = M_1 \oplus M_2$ → vulnerable to statistical analysis

Alice & Bob need to exchange keys

- Exchanging keys over secure channel (i.e. meeting in person) Not always possible
- Exchaning keys over insecure channel.

11.1 Diffie-Hallman encryption

Let p be a large prime number (100 digits). We will work using modulo p.

Discrete logarithm problem $a^x \equiv b \ (mod\ p)$
Given a, b compute x.
No fast algorithms are known for this problem.

Our goal is to produce a key k which Alice and Bob know but Eve cannot guess (or compute).
Alice chooses some prime p, a small number g, and Alice's part of the key a.
Alice calculates:
$A = g^a$
And sends p, g, and A to Bob.
Bob chooses Bob's part of the key b.
Bob calculates:
$B = g^b$
And sends B to Alice.
Now both Alice and Bob have p, g, A, B. These variables can be publicly available.
Alice can compute:
$K = B^a = (g^b)^a = g^{ab}$
Bob can compute:
$K = A^b = (g^a)^b = g^{ab}$

Note that Bob still does not know a and Alice still does not know b, but they can both use a combination of both keys.
Note: p is sent because the calculations are all done in base p

Notation: $x(mod\ n) \rightarrow$ the remainder of x after division by n

11.1.1 Diffie-Hellman key exchange

- Alice:
  P is prime
  p is large (10^{100})
  g - "base"
  a - Alice's private key
  A = $g^a(mod\ p)$

- Alice sends to bob $\{g, p, A\}$
- Bob:
  b - Bob's private key
  B = g^b
- A can be computed efficiently even if g^a itself is proibitively large.
- Now g, p, A, B are public information.
- Alice knows a, Bob knows b

- Alice and Bob can both compute $K = g^{ab}(mod\ p)$
- $K \equiv (g^b)^a \equiv B^a(mod\ p) \rightarrow$ Alice can compute K
- $K \equiv A^b \equiv (g^a)^b(mod\ p) \rightarrow$ Bob can compute K
- Knowing $\{g, p, g^a(mod\ p), g^b(mod\ p)\}$ it is impossible to compute g^{ab} efficiently (assuming the discrete logarithm problem is hard).

11.1.2 Sending a message using K

- Alice has a message: $0 \leq m \leq p$
- Alice $\xrightarrow{m^*=mk(mod\ p)}$ Bob
- Bob computes multiplicative inverse for $k(mod\ p)$. $\bar{K}K \equiv 1(mod\ p)$
- Bob then computes $m^*K(mod\ p)$
- $mK\bar{K} \equiv m$

11.2 RSA encryption

Also known as **Rivest-Shamir-Adleman**.
Public key (Public lock) system:

- Bob runs an online store (Amazon) and wants to receive encrypted messages from multiple parties.
- Bob makes the public key available to all the parties so that there exists a simple procedure (which is also made public) to encode messages and send them to Bob, but only he can decrypt them.
- Bob generates two large prime numbers p and q and an exponent which is commonly denoted as e (let's use 3) so that $e \nmid q - 1(e\ prime)$
- Bob computes $N = pq$ and makes (e, N) available (the public key)
- Alice (or anyone else who wants to send a message M) to Bob, $gcd(m, N) = 1, \quad 0 \leq m \leq N$
- Alice transmits $m^* = m^e = m^3(mod\ N)$
- Bob can now decrypt m from m^*

1. Compute k:

   $$3k \equiv 1(mod\ (p-1)(q-1)$$
   $$3k = S(p-1)(q-1) + 1$$
   $$3k = s(p-1)(q-1) = 1$$

   (Express 1 = gcd(3, (p-1)(q-1)) as a linear combination of 3 and (p-1)(q-1))

2. Compute $(m^*)^k(mod\ N) \rightarrow$ This will produce m

   $$(m^*)^k = m^{3k} = m^{s(p-1)(q-1)+1}$$
   $$s(p-1)(q-1) \equiv m(mod\ N)$$

Equivalently $m^{(p-1)(q-1)} \equiv 1(mod\ N = pq)$
We want to show:
$pq|m^{(p-1)(q-1)} - 1 \leftrightarrow (p|m^{(p-1)(q-1)} - 1) \wedge (q|m^{(p-1)(q-1)} - 1))$
$m^{(p-1)(q-1)} \equiv 1(mod\ p) \quad \rightarrow m^{(p-1)(q-1)} \equiv (1)^{q-1} = 1(mod\ p)$

Why can't Eve do the same thing?
Eve knows pq. If Eve can compute $(p-1)(q-1)$, she can use the same encryption procedure.

Eve can then compute $pq - (p-1)(q-1) + 1 = p + q$

One can compute $p + q$ from knowing these two numbers, and then compute p and q.

Note: You can calculate p and q from pq and $p + q$ by solving for x in the quadratic equation:

$x^2 - (p+q)x + pq = 0 = (x-p)(x-q)$

Security of RSA is based on the fact that computing p and q from $N = pq$ is hard.

Example: $p = 5, q = 17, N = 85, e = 3$
Public key (lock): (3, 85)
Alice wants to transmit m = 7.
$m* = 7^3(mod\ 85) = 49 \times 7 = 343(mod\ 85) = 3$
Alice transmits 3
Bob's decryption process:

1. Compute k: $3k \equiv 1(mod\ (5-1)(17-1) = 64)$ A typical way to do this is to use Euclid's algorithm on 64:
   $64 = 3 \cdot 21 + 1 \qquad 1 = 64 - 3 \cdot 21$
   $(-21) \cdot 3 \equiv 1(mod\ 64)$
   $(64 - 21) \cdot 3 \equiv 1(mod\ 64$
   $\rightarrow$ **k = 43**
2. $3^{43}(mod\ 85)$
   $43 = 32 + 8 + 2 + 1 = 101011_2$
   $3^{43} = 3^{32} \cdot 3^8 \cdot 3^2 \cdot 3(mod\ 85)$
   $3^1 = 3(mod\ 85)$
   $3^2 = 3 \cdot 3 = 9(mod\ 85)$
   $3^4 = 81 \equiv -4(mod\ 85)$
   $3^8 \equiv (-4)^2 \equiv 16(mod\ 85)$
   $3^{16} \equiv 16^2 = 256 \equiv 1(mod\ 85)$
   $3^{32} \equiv 1^2 \equiv 1(mod\ 85)$
   Going back to our message, we have:
   $3^{43} = 3^{32} \cdot 3^8 \cdot 3^2 \cdot 3(mod\ 85) \equiv 1 \cdot 16 \cdot 9 \cdot 3 = 27 \cdot 16 = 432 = 85 \cdot 5 \cdot 85 + 7 \equiv 7(mod\ 85)$
   We succesfully decoded our message.

12 Combinatorics

The art of couting

- how many 5 card poler hands are two pairs?
- how many bridge hands (13 cards) have all 4 aces in them and at least 6 cards in the same suit?

12.1 Functions

A function from a set X to a set Y: $f : X \to Y$ assings to every element of X an element $y < f(x)$ in Y

A function f

- is **surjection** (on to) if every element of Y is a value of the function f for some x $\forall y \in Y(\exists x \in X(y = f(x)))$
- is an **injection** (1-to-1) if every element of Y is a value of f for at most one $x \in X$ $\forall x_1, x_2 \in X((f(x_1) = f(x_2)) \to (x_1 = x_2))$
- is a **bijection** if it is both on to and 1-to-1
- **Examples:** $f : \mathbb{R} \to \mathbb{R}$
  - $f(x) = x$ i.e. identity function → bijection
  - $f(x) - x^2 \to$ neither injection or surjection
  - $f(x) = x^3 \to$ bijection
  - $f(x) = x^3 - x$ missed last example

$f : X \to Y \qquad g : Y \to Z$

12.2 Compositions

We can define a **composition** $gf : X \to Z$

$gf(x) = g(f(x))$

If f is a bijection and g is a bijection then so is gf. Similarly, if f is a surjection and g is a surjection then so is gf; if f is a injection and g is a injection then so is gf.

Given a function $f : X \to Y$ a function $f^{-1} : Y \to X$ is called an **inverse** of f if $f^{-1}f(x) = x$ for all $x \in X$ and $f(f^{-1}(y)) = y$ for all $y \in Y$.

Fact: A function has an inverse if and only if it has a bijection

Example: $f : \mathbb{R} \to \mathbb{R} \qquad f(x) = x + 1 \qquad f^y(x) = x - 1$

12.3 Counting

If X is a finite set, $|X|$ denotes the number of elements in X.

We say that $|X| = k$ if there exists a bijection between X and the set $[k] = 1, 2, ..., k$.

Bijection rule: If there exists a bijection $f : X \to Y$ for two finite sets, X and Y then $|X| = |Y|$.

Proof: $|X| = k$ means existence of a bijection $g : X \to [k]$ Consider a map $gf^{-1} : Y \to [k]$. This is a bijection, so $|Y| = k$.

Suppose we have an alphabet with k letters in it. How many distinct words of length n are there? How many sequences $(x_1, x_2, ..., x_n)$ where each $x_i \in [k]$ are there?

- If $n = 1$: There are k sequences.
- If $n = 2$: There are k^2 sequences

- For general n: There are k^n sequences.

Product rule: Let $X_1, X_2, X_3, ..., X_n$ sets, then the number of sequences $(x_1, x_2, ..., x_n)$ such that $x_i \in X_i$ is $|X_1||X_2|...|X_n|$

Example: Ordering pizza $\left\{\begin{array}{c}\text{thin crust}\\ \text{regular}\\ \text{stuffed crust}\end{array}\right\}\left\{\begin{array}{c}\text{cheese}\\ \text{no cheese}\end{array}\right\}\left\{\text{ 6 different toppings }\right\} \rightarrow 36$ choices

Generalized product rule: We want to count sequences $(x_1, x_2, x_3, ...k_m)$ so that

- there are k_1 choices for the first element
- given the first element there are k_2 choices of the 2^{nd} element
- given the choices of first i elements there are k_{i+1} choices for the $(i+1)^st$ element

Then there are $k_1k_2k_3k_4...k_n$ sequences

Example: Competition with 10 teams in it how many ways are there to assign gold, solver & bronze medals?
$10 \cdot 9 \cdot 8 = 720$ choices
How many ordered sequences of k distinct elements can be selected from an n-element set?
$n(n-1)(n-2)...(n-k+1) = \dfrac{n!}{(n-k)!}$

12.4 Subsets, Binomial Theorem

Bijection rule: If $f : X \rightarrow Y$ is a bijection, then $|X| = |Y|$

(Generalized) product rule: $x_1, x_2, x_3..., x_n$. If given $x_1, x_2, x_3..., x_i$ there are k_{i+1} ways of choosing x_{i+1} then there are $k_1, k_2, ..., k_n$ in total.

Example: In how many ways can we put a pawn (P), a knight (N) and a bishop (B) on a chessboard so that no two pieces share a row or a column?

We can record the position of the pieces as the following sequence:

$$(r_p, c_p, r_n, c_n, r_b, c_b) \begin{cases} r_p : \text{the number of a row in which we put a pawn} \\ c_p : \text{the number of the column of a pawn} \end{cases}$$

Note that all of the row numbers must be different and all of the column numbers must be different. Thus, we apply the product rule:

Note that all of the row numbers must be different and all of the column numbers must be different. Thus, we apply the product rule:

$8 \times 8 \times 7 \times 7 \times 6 \times 6 = (8 \cdot 7 \cdot 6)^2$

Ordered subsets: There are $(n(n-1)...(n-k+1) = \frac{n!}{(n-k)!}$ ways of choosing k different elements **in order** from a set of size n.

There are $n!$ ways of ordering elements of a set of size n. These orderings are called **permutations**.

A function $f : X \rightarrow Y$ is called **k-to-one** if there are exactly k elements of X mapped to every element of Y.

Division rule: If $f : X \rightarrow Y$ is k-to-one, then $|X| = k|Y|$.

Example: In how many ways two black rooks can be placed on a chessboard so that they don't share a row or a column?

$(r_1, c_1, r_2, c_2) \rightarrow 8 \times 8 \times 7 \times 7 = 56^2$

The two sequences $(1, 1, 2, 2)$ and $(2, 2, 1, 1)$ record the same position.

The function mapping sequences to positions of the rooks is 2-to-1, because the rooks are indistinguishable. Consequently,
Answer: $56^2 \div 2$

The number of k element subset of a set of size n:

Notation: $\binom{n}{k}$ - "n choose k"

Theorem: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Proof: There are $\frac{n!}{(n-k)!}$ ordered subsets of an n-element set. Every ordered subset corresponds to an unordered one. There is a function which maps ordered subsets into unordered ones. All ordered subsets which correspond to the same unordered subset can be described as just orderings or permutations of this subset.

Suppose we select an unordered 3-element subset $\{1, 3, 5\}$, then there are 6 ordered subsets corresponding to it namely $(1, 2, 5), (1, 5, 2)(2, 1, 5)(2, 5, 1)(5, 1, 2)(5, 2, 1)$

So there are k!-to-1 functions.

Therefore there are $\frac{k!}{(n-k)!k!}$ unordered subsets.

How many subsets in an n-element set: The number of subsets of an n-element set is 2^n.

$$S \rightarrow (x_1, x_2, ..., x_n) \qquad x_i = \begin{cases} 0 \text{ if } i \notin S \\ 1 \text{ if } i \in S \end{cases}$$

If we look at subsets of $\{1, 2, 3\}$:

- $\{1, 3\} \rightarrow (1, 0, 1)$
- $\{2\} \rightarrow (0, 1, 0)$
- $\emptyset \rightarrow (0, 0, 0)$

2^n choices in total by the product rule. $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + ... + \binom{n}{n-1} + \binom{n}{n} = 2^n$

12.5 Binomial theorem

$(x + y)^n$ - Our goal is to understand coefficients in the expansion of $(x + y)$.

$$(x + y^1 = x + y$$
$$(x + y)^2 = x^2 + 2xy + y^2$$
$$(x + y)^3 = (x + y)(x + y)^2 = (x + y)(x^2 + 2xy + y^2) = x^3 + 3x^2y + 3xy^2 + y^3$$

Theorem: $(x + y)^n = \sum_{k=0}^{n}(\binom{n}{k}x^ky^{n-k}) = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \binom{n}{2}x^2y^{n-2} + ... + \binom{n}{n-1}x^{n-1}y + \binom{n}{n}x^ny^0$

Proof: $(x + y)^n = \underbrace{(x + y)(x + y)...(x + y)}$ n times

Every term in the expansion corresponds to a choice of one of the two summands in each of the n factors.

How many terms will be equal to $x^k y^{n-k}$?

These terms correspond to choices where we selected x in exactly k out of n factors. There are exactly as many such selections as there are subsets of size k in the set of n factors which is $\binom{n}{k}$

12.6 Relations involving binomial coefficients

12.6.1 Pascal's triangle

$\binom{n}{k} = \frac{n!}{(k!)(n-k)!}$ - the number of size k subsets of a set of size n

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} = \binom{n}{0} x^0 y^n + \binom{n}{1} x y^{n-1} + \binom{n}{2} x^2 y^{n-2} + \ldots + \binom{n}{n-1} x^{n-1} y + \binom{n}{n} x^n y^0$$

1. $x = y = 1$

   $2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n-1} + \binom{n}{n}$

   Both the left and the right side of this equation count the number of all subsets of a set of sixteen.

2. $x = -1, y = 1$

   $0 = \sum_{k=0}^{n} \binom{n}{k} (-1)^k = \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots + (-1)^n \binom{n}{n}$ Total number of subsets of even size: $\binom{n}{1} + \binom{n}{3} + \ldots =$ Total number of subsets of odd size: $\binom{n}{0} + \binom{n}{2} + \ldots$

   The number of subsets of odd size is the same as the number of subsets of even size.

   Bijective proof:

   f: subsets of odd size → subsets of even size $f(A) = A \oplus 1 = \begin{cases} A \cup 1 \text{ if } 1 \notin A \\ A - 1 \text{ if } 1 \in A \end{cases}$

   If $(A)| = |A| \pm 1 \rightarrow$ maps subsets of odd size into subsets of even size.

   This is a bijection, because f has an inverse. In fact, f is an inverse of itself.

   $f(f(A)) = (A \oplus 1) \oplus 1 = A$

3. $\binom{n}{k} = \binom{n}{n-k}$ for all $0 \leq k \leq n$

   $\binom{n}{k} \rightarrow x^k y^{n-k}$ $\binom{n}{n-k} \rightarrow x^{n-k} y^k$ If we switch the roles of x and y, these terms replace each other.

   Bijective proof: $X = 1, 2, ..., n$

   Given a set of size n, $X = \{1, 2, \ldots, n\}$ and a collection of k elements, is there a natural way of choosing k elements?

   $f(A) = X - A \rightarrow$ the complement of A, subset of all elements in X but not in A

   The function maps sets of size k into sets of size $n - k$ bijectively

4. $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$

   Proof: We want to show that this equality holds: $\frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n+1-k)!} = \frac{(n+1)!}{k!(n+1-k)!}$

We multiply both sides by $k!(n+1-k)!$ and obtain:

$n! \cdot (n+1-k) + k \cdot n! = (n+1)!$

We divide by n!

$(n+1-k)+k = (n+1) \quad \leftrightarrow n+1 = n+1$

The equality holds.

Bijective proof:
We need to describe a correspondence (bijective) between k element subsets of a set of size $(n+1$ and k and $(k-1)$ elemeBnt subsets of set of size n.

[PICTURE OF AN OVAL THAT HAS N IN IT SURROUNDED BY ANOTHER OVAL THAT'S LABELED N + 1 WITH A POINT ALSO LABELED N + 1]

If we consider an n-element set x' inside of our $(n+1)$-element set x, then intersection with X' produces a k' or $(k-1)$ element subset of X' from a k-element subset of X.

$n = 0$:										1									
$n = 1$:									1		1								
$n = 2$:								1		2		1							
$n = 3$:							1		3		3		1						
$n = 4$:						1		4		6		4		1					
$n = 5$:					1		5		10		10		5		1				
$n = 6$:				1		6		15		20		15		6		1			
$n = 7$:			1		7		21		35		35		21		7		1		
$n = 8$:		1		8		28		56		70		56		28		8		1	
$n = 9$:	1		9		36		84		126		126		84		36		9		1

n^{th} row of the triangle lists binomial coefficients:

$\binom{n}{0}, \binom{n}{1}, \binom{n}{2} \dots \binom{n}{n}$ in order.

Example

$(x+y)^2 = y^2 + 2xy + x^2$
$(x+y)^3 = y^3 + 3xy^2 + 3x^2y + x^3$
$(x+y)^8 = 1x^8 + 8xy^7 + 28x^2y^6 + 56x^3y^5 + 70x^4y^4 + 56x^5y^3 + 28x^2y^6 + 8xy^7 + y^8$

(a) The sum of the elements in n^{th} row is 2^n

(b) The sum of the squares of the elements in the n^{th} row is:

$$0^{th} : 1^2 = 1 = \binom{0}{0}$$

$$1^{st} : 1^2 + 1^2 = 2 = \binom{2}{1}$$

$$2^{nd} : 1^2 + 2^2 + 1^2 = 6 = \binom{4}{2}$$

$$3^{th} : 1^2 + 3^2 + 3^2 + 1^2 = 20 = \binom{6}{3}$$

$$4^{th} : 1^2 + 4^2 + 6^2 + 4^2 + 1^2 = 1 + 16 + 36 + 16 + 1 = 70 = \binom{8}{4}$$

Proof: $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}$

$$\binom{n}{k} = \binom{n}{n-k}, \qquad \binom{n}{k}^2 = \binom{n}{k}\binom{n}{k} = \binom{n}{k}\binom{n}{n-k}$$

$$\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \binom{n}{2}\binom{n}{n-2} + \ldots + \binom{n}{n}\binom{n}{0} = \binom{2n}{n}$$

$$\ldots + \binom{2n}{n}x^n y^n + \ldots = (x+y)^{2n} = (x+y)^n(x+y)^n$$

$$= \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \ldots \binom{n}{k}x^ky^{n-k} + \ldots + \binom{n}{n-k}x^{n-k}y^k + \binom{n}{n}x^ny^0$$

The term x^my^n in the expansion of the right side is exactly the sum we want.

We want to show that the sum of each diagonal in the representation of Pascal's Triangle is the sum of the two previous diagonals. They are fibonacci numbers $F_{n+1} = F_n + F_{n-1}$

1 - 1
1 1 - 1, 2
1 2 1 - 3, 5
1 3 3 1 - 8, 13
1 4 6 4 1 - 21,
1 5 10 10 5 1 -
1 6 15 20 15 6 1 -
1 7 21 35 35 21 7 1
1

Proof: By induction ($S_n = F_{n+1}$)

Let S_k denote the corresponding sum:

Base of the induction: $S_o = 1_1 S_1 = 1$

Induction step: We want to show that $S_{n+1} = S_n + S_{n-1}$. Let us do the proof when n is odd, $n = 2k-1$ (The other case is similar). $S_{2k} = S_{2k-1} + S_{2k-2}$

$S_{2k} = \binom{2k}{0} + \binom{2k-1}{1} + \binom{2k-2}{2} + \binom{2k-3}{3} + \ldots + \binom{k+1}{k+1} + \binom{k}{k}$

$S_{2k-1} = \binom{2k-1}{0} + \binom{2k-2}{1} + \binom{2k-3}{2} + \ldots + \binom{k}{k-1}$

$S_{2k-2} = \binom{2k-2}{0} + \binom{2k-3}{1} + \binom{2k-4}{2} + \ldots + \binom{k}{k-2} + \binom{k-1}{k-1}$

We group the terms in $S_{2k}, S_{2k-1}, S2k-2$:

- $\binom{2k}{0} + \binom{2k-1}{0}$
- $\binom{2k-1}{1} + \binom{2k-2}{1} + \binom{2k-3}{1}$
- $\ldots$
- $\binom{k+1}{k+1} + \binom{k}{k-1} + \binom{k}{k-2}$
- $\binom{k}{k} + \binom{k-1}{k-1}$

12.7 Further Examples using Fibonacci Numbers

1. How many ways are there to ascend a staircase with n steps taking 1 or 2 steps at a time?
   Example: For n = 3, the answer is 3; for n = 2, the answer is 2; for n = 1, the answer is 1
   In general, there are F_{n+1} ways.
   Proof:
   - Base case: works for n = 1 and n = 2
   - **Induction step**: We want to show there are F_{n+2} ways to ascend a staircase with $(n+1)$ steps given that there are F_{k+1} ways of ascending a staircase with k steps for $k \leq n$ (we will need this for n steps, and $n+1$ steps.
     If we start with a single step then there are (by induction hypothesis) F_{n+1} ways to go up the remaining n steps. If we start by taking two steps, we have F_n ways to go up. We have $F_n + F_{n+1}$ ways in total $F + n + F_{n+1} = F_{n+2}$ ■
2. How many subsets of the set $\{1, 2, 3, \ldots, n\}$ contain no two consecutive integers?
   $n = 1, 2(\emptyset, \{1\})$
   $n = 2, 3(\emptyset, \{1\}, \{2\})$
   $n = 3, 5(\emptyset, \{1\}, \{2\}, \{3\}, \{1, 3\})$
   General suspicion:
   F_{n+2}
   Proof by induction: We are done with the base case.

   Induction step: We want to prove the formula holds for $1, 2, 3, \ldots, n+1$
   Let us divide all possible subsets which do not contain two integers into two classes:

   (a) Subsets which don't contain $n+1$. There are F_{n+2} such subsets by the induction hypothesis.

   (b) Subsets which contain $n+1$. Those subsets do not contain n, and otherwise can contain any subset of $1, 2, \ldots, n-1$ with no two consecutive elements. There are F_{n+1} of those subsets by the induction hypothesis. We have $F_{n+2} + F_{n+1} = F_{n+3}$ subsets in total.

A formula for F_n:

$F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89

Let us calculate $\frac{F_{n+1}}{F_n}$:

-	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$n=7$
$\frac{F_{n+1}}{Fn}$	$\frac{1}{1} = 1$	$\frac{2}{1} = 2$	$\frac{3}{2} = 1.5$	$\frac{5}{3} = 1.666$	$\frac{8}{5} = 1.6$	$\frac{13}{8} = 1.625$	$\frac{21}{13} = 1.61...$

It is likely that $F_n \approx c\lambda^n$ where $\lambda \approx 1.6108...$ (the golden ratio).

Suppose we had an exact equality. What would λ be?

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} \\ c\lambda^{n+1} &= c\lambda^n + c\lambda^{n-1} \\ \lambda^2 &= \lambda + 1 \end{aligned}$$

$$\lambda^2 - \lambda - 1 = 0$$

$$\lambda_{1,2} = \frac{1 \pm \sqrt{5}}{2}$$

Fibonacci numbers $\lim_{n\to+\infty} \frac{F_{n+1}}{F_n}$

Suppose $c\lambda^n$ satisfies $c\lambda^{n+!} = c\lambda^n + c\lambda^{n-1}$ then:

$\lambda = \frac{1\pm\sqrt{5}}{2} = 1.6108$

$F_n = c_1(\frac{1+\sqrt{5}}{2})^n + c_2(\frac{1-\sqrt{5}}{2})^n$ satisfies the relation $F_{n+1} = F_n + F_{n-1}$

for any choice of c_1 and c_2.

$0 = F_0 = c_1 + c_2$
$1 = F_1 = c_1(\frac{1+\sqrt{5}}{2}) + c_2(\frac{1-\sqrt{5}}{2}) \to c_2 = -c_1$
$1 = c_1(\frac{1+sqrt5}{2} - \frac{1-\sqrt{5}}{2})$
$c_1 = \frac{1}{\sqrt{5}}, c_2 = \frac{-1}{\sqrt{5}}$

Theorem: $F_n = \frac{1}{\sqrt{5}}[(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n]$

One can use the binomial formula to explicit show that this expression is an integer.

Explicit formulas for recursively defined sequences.

$x_0 = a_0, x_1 = a_1, x_{n+1} = bx_n + cx_{n-1}$ We are given a_0, a_1, b, and c. Our goal is to find a formula for x_n.

(Which exponential function $x_n = \lambda^n$ satisfies $x_{n+1} = bx_n + cx_{n-1}$?

$$\lambda^{n+1} = b\lambda^n + c\lambda^{n-1}$$

$$\lambda^2 - b\lambda - c = 0 \to \text{quadraticequation}$$

$$\lambda_{1,2} = \frac{b \pm \sqrt{b^2 - 4c}}{2}$$

More generally $x_n = \alpha_1\lambda_1^n + \alpha_2\lambda_2^n$ satisfies the recurrence for all $\alpha_1, \alpha 2$

Example: $x_0 = 2, x_1 = 7, x_{n+1} = x_n + 2x_{n-1}$

1. Solve $\lambda^2 - \lambda - 2 = 0$
   $(\lambda + 1)(\lambda - 2) = 1 \qquad \to \lambda_1 = 2 \qquad \lambda_2 = -1$

2. $x_n = d_1 2^n + d_2(-1)^n$
   $\begin{bmatrix} 2 = x_0 = \alpha_1 + \alpha_2 \\ 7 = x_1 = 2\alpha_1\alpha_2 \end{bmatrix} \to 3d_1 = 9, d_1 = 3, d_2 = -1$
   Answer:$x_n = 3 \cdot 2^n - (-1)^n]$
   $x_2 = 7 + 22 = 11 = 3 \cdot 4 - (-1)^2$

1, 1, 2, 3, 4, 8, 13, 21, 34, 55, 89, 144

Theorem: F_n is even if and only if n is divisible by 3.

Proof: Induction on n

- **Base case**: $n = 1, n = 2$ ✓
- **Induction step**: $F_{n+1} = F_n + Fn_1$
  Cases:
  1. $3|n+1 \to 3$ does not divide n or $n-1$ so F_n, F_{n-1} are odd, F_{n+1} is even
  2. $3 \nmid n+1$ so exactly one of n and $n-1$ is divisible by 3. By induction hypothesis, one of F_n and F_{n-1} is even, and another one is odd, so the sum is odd.
- Second way of doing induction step $F_{n+1} = F_n + F_{n-1} = (F_{n-1} + F_{n-2}) + F_{n-1} = 2F_{n-1} + F_{n-2}$
  $F_{n+1} \equiv F_{n-2}$ $(mod\ 2)$

12.8 Inclusion-Exclusion I

Given $|A|$, $|B|$ we want to find $|A \cup B|$

If A and B are disjoint $(A \cap B = \emptyset)$ then $|A \cup B| = |A| + |B|$

In general $|A \cup B| = |A| + |B| - |A \cap B|$

Every element of A is ”counted” in $|A|$ but not in $|B|$ or $|A \cap B|$. Same for elements of $B - A$. Elements of $A \cap B$ are counted twice with a positive sign and once with a negative sign.

Three sets :

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$

Examples In a group of 40 students,

- 10 take Art
- 22 take Biology
- 16 take Computer Science
- 4 take Art + Biology
- 8 take Biology + Computer Science
- 4 take Art + Computer Science
- 2 take Art + Biology + Computer Science

How many students don't take either of of three courses.

The number of students taking at least one of those courses is $|A \cup B \cup C|$

A = { all students taking Art } B = { all students taking Biology } C = { all students taking Computer Science }

$|A \cup B \cup C| = 10 + 22 + 16 - 6 - 8 - 4 + 2 - 32$

Answer = 40 - 32 = 8 students not taking anything

12.9 Inclusion-Exclusion Principle II

$|A \cup B| = |A| + |B| - |A \cap B|$

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| = |A \cap C| - |B \cap C| + |A \cap B \cap C|$

Example: Suppose you have a group people $\begin{cases} \text{20 can play the flute} \\ \text{8 can play the piano} \\ \text{25 play the violin} \\ \text{20 play at least two instruments} \\ \text{6 play all three} \end{cases}$

How many people play at least one instrument?

F = { people who can play the flute }
P = { people who can play the piano }
V = { people who can play the violin }

We are interested in $|F \cup P \cup V| = |F| + |P| + |V| - |F \cap P| - |F \cap V| - |V \cap P| + |V \cap P \cap F|$

We know that $||F \cap P| \cup |F \cap V| \cup |V \cap P|| = 20$

Let us denote $\begin{cases} A = F \cap P \\ B = F \cap V \\ C = V \cap P \end{cases}$

$20 = |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

How large is $|A \cap B| = |(F \cap P) \cap (F \cap V)| = |F \cap P \cap V|$

Therefore,

$$20 = |A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$
$$20 = |A \cup B \cup C| = |A| + |B| + |C| - |F \cap P \cap V| + |A \cap B \cap C|$$

$|F \cap P| + |F \cap V| + |V \cap P| = 20$

Answer: 20 + 8 + 25 - 32 + 6 = 27

Another Example:

Make a 4 by 7 grid and locate p and q on the opposite ends of its diagonal i.e. p = (0,0) and q = (7,4). Travelling from p to q takes 11 blocks.

1. How many optimal ways are there to travel from p to q (using exactly 11 blcoks)?

   Every route we take corresponds to a sequence of 11 blocks in each of these blocks we drive up or to the right, driving up exactly 4 times.

Answer: $\binom{11}{4} = \frac{11!}{7!\,4!} = \frac{11 \cdot 10 \cdot 9 \cdot 8}{4 \cdot 3 \cdot 2 \cdot 1} = 330$

First: UUUURRRRRRR
Second: RURUURRURRR

2. Suppose one street is blocked. How many was are there now to travel from p to q?

   How many ways out of those routes used uv? Ways to travel from v to q? $\binom{5}{2} = 10$

   Routes from p to n and from v to q → ($\binom{5}{2}\binom{5}{2} = 10 \times 10 = 100$)

   Therefore, $330 - 100 = 230$

3. How many ways are there to travel from p to q (going up and to the right) avoiding streets uv, wx and yz knowing they have the following coordinates: w = (2,1), x = (3,1), u = (3,2), v = (4,2), y = (5,2), z = (5,3)?
   A = { all routes including uv}
   B = { all routes inclduing wx}
   C = { all routes inclduing yz}
   We are interested in $330 - |A \cup B \cup C|$
   $|A| = 100$

   $|B| = \binom{3}{1}\binom{7}{3} = 105$

   $|C| = \binom{7}{2}\binom{3}{1} = 63$

   $|A \cap B| = pw, xu, vq = \binom{3}{1}\binom{1}{1}\binom{5}{2} = 30$

   $|A \cap C| = pu, vy, zq = \binom{5}{2}\binom{1}{1}\binom{3}{1} = 30$

   $|B \cap C| = pw, xy, zq = \binom{3}{1}\binom{3}{1}\binom{3}{1} = 27$

   $|A \cap B \cap C| = \binom{3}{1}\binom{3}{1} = 9$

   Answer $= 330 - |A \cup B \cup C| = 330 - 100 - 105 - 63 + 30 + 30 + 27 - 9 = 140$

For n sets: $|A_1 \cup A_2 \cup ... \cup A_n|$ = the sum of all the sets

minus the sums of all pairwise intersections $\binom{n}{2}$ terms

plus the size of all three way interesections $\binom{n}{3}$ terms

minus sum of the sizes of all four way intersections $\binom{n}{4}$

plus the sum of the sizes of all five way intersections $\binom{n}{5}$.. etc

$$\begin{aligned}|A_1 \cup A_2 \cup ... \cup A_n| &= \sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| \\ &+ \sum_{1\leq i<j<k\leq n} |A_i \cup A_j \cap A_k| - \ldots + (-1)^{n-1}|A_1 \cap A_2 \ldots \cap A_n| \\ &= \sum_{I\subseteq\{1,2,...,n\} \quad I\neq\emptyset} (-1)^{|I|-1}| \cap_{i\in I} A_i|\end{aligned}$$

Proof: We need to show that every element of $A_1 \cup A_2 \cup \ldots \cup A_n$ is counted exactly once in the right side of our formula. Suppose the element we are considering belongs to exactly k of the sets.

It will appear with the coefficient $\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} + \ldots + (-1)^{k-1}\binom{k}{k} = 1$

Number of all odd subsets of the k-element set - number of all non-empty even subsets

12.10 Inclusion/Exclusion Principle III

$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{1\leq i<j<k\leq n} |A_i \cup A_j \cap A_k| - \ldots + (-1)^{n-1}|A_1 \cap A_2 \ldots \cap A_n|$

Example:

A postman wants to deliver n letters to n houses. (There is exactly one letter addressed to each of the houses).

How many ways are there for the postman to deliver every letter to deliver every letter to the wrong house? (Still 1 letter per house)

Counting bijections [permutations] $f : \{1, 2, ..., n\} \to \{1, 2, ..., n\}$ so that $f(k) \neq k$ for all $k = 1, 2, ..., n$.

Derangements: $D(n)$: # of derangements of $\{1, 2, ..., n\}$

D(1) = 0

D(2) = 1

D(3) = ?

$A_1 = \{\#$ of permutations $\{1, 2, 3\}$ which preserve the position of $1\}$

$A_2 = \{\#$ of permutations $\{1, 2, 3\}$ which preserve the position of $2\}$

$A_3 = \{\#$ of permutations $\{1, 2, 3\}$ which preserve the position of $3\}$

$D(3) = 3! - |A_1 \cup A_2 \cup A_3| = 3! - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|$

We know that $|A_1| = |A_2| = |A_3| = 2$ and $|A_1 \cap A_2| = |A_1 \cap A_3| = |A_3 \cap A_2| = |A_1 \cap A_2 \cap A_3| = 1$

Therefore, $D(3) = 3! - 6 + 3 - 1 = 2$

What about D(4) ?

$A_k = \#$ of permutations of 1, 2, ... , n which preserve the position of k

$D(n) = n! - |A_1 \cup A_2 \cup ... \cup A_n| = n! - \sum_{i=1}^{n} |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| - \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^n |A_1 \cap A_2 \ldots \cap A_n|$

where $n!$ is the total # of ways to deliver letters

$|A_i| = (n-1)!$

$|A_i \cap A_j| = (n-2)!$

In general, $|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| = (n-k)!$

Therefore,

$$\begin{aligned}
D(n) &= n! - |A_1 \cup A_2 \cup ... \cup A_n| = n! - \sum_{i=1}^{n} |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cap A_j| - \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\
&+ \ldots + (-1)^n |A_1 \cap A_2 \ldots \cap A_n| \\
&= n! - n \cdot (n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n=3)! + \binom{n}{4}(n-4)! - \ldots + (-1)^n \binom{n}{n} 0! \\
&= n! - n! + \frac{n!}{\cancel{(n-2)!}2!}\cancel{(n-2)!} - \frac{n!}{\cancel{(n-3)!}3!}\cancel{(n-3)!} + \ldots \\
&= n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} \cdots + (-1)^n \frac{1}{n!}) \\
&\approx \frac{n!}{e} \pm \frac{1}{n+1}
\end{aligned}$$

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \qquad \frac{1}{e} \approx 0.37$$

Proposition: $D(n) = (n-1)(D(n-1) + D(n-2))$ has a purely combinatorial proof.

How many ways are there to deliver **exactly** one letter correctly? (For at least one letter the answer is $n! - D(n) \approx n!(1 - \frac{1}{e})$)

Delivering only the first letter correctly: $D(n-1)$

Delivering only the second letter correctly: $D(n-1)$

It is impossible to "deliver only the first letter correctly" and "deliver only the second letter correctly". These sets are disjoint, hence allowing us to use the inclusion-exclusion principle.

Delivering the first and second letters correctly → $n\ D(n-1)$ ways $\approx n\ \frac{(n-1)!}{e} \approx \frac{n!}{e} \approx 0.37n!$

12.11 Euler's phi function (totient function)

$\varphi(n) = |\{k : 1 \leq k \leq n, gcd(k,n) = 1\}|$

$\varphi(12) = |\{1, 5, 7, 11\}| = 4$

$A_1 = \{\text{even numbers in } \{1, 2, \ldots, 12\}\}$

$A_2 = \{\text{numbers in } \{1, 2, 3, \ldots, 12\} \text{ divisible by } 3\}$

$\varphi(12) = 12 - |A_1 \cup A_2| = 12 - |A_1| - |A_2| + |A_1 \cap A_2| = 12 - \frac{12}{2} - \frac{12}{3} + \frac{12}{6} = 4$

Theorem: Let n be a positive integer and let $p_1, p_2, \ldots, p_k$ be all distinct prime divisors n. Then $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k})$

Example:

$\varphi(36000) = 3600 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{5}) = \frac{3600}{30} \cdot 8 = 960$

Proof:

$A_i = \{m : 1 \leq m \leq n, \quad p_i \mid m\}$

$\varphi(n) \ = n - |A_1 \cup A_2 \cup \ldots \cup A_n| \ = n - \sum_{i=1}^{n} |A_i| + \sum_{1 \leq i < j \leq n} |A_i \cup A_j| - \sum_{1 \leq < i < j < k \leq n} |A_i \cup A_j \cup A_k| + \ldots + (-1)^n |A_1 \cap A_2 \ldots \cap A_n|$

$A_i = \{p_i, 2p_i, 3p_i, \ldots, \frac{n}{p_i} \cdot p_i\}$

$|A_i| = \frac{n}{p_i}$

$|A_i \cap A_j| = \frac{n}{p_i p_j}$

$|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_s}| = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_s}}$

$$\begin{aligned}\varphi(n) &= n(1 - \frac{1}{p_1} - \frac{1}{p_2} - \ldots - \frac{1}{p_k} + \frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \ldots + \frac{1}{p_1 p_k} - \frac{1}{p_1 p_2 p_3} - \frac{1}{p_1 p_2 p_3} - \frac{1}{p_1 p_2 p_4} - \ldots - \frac{1}{p_1 p_2 p_k} + \ldots) \\ &= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \ldots (1 - \frac{1}{p_k})\end{aligned}$$

Corollary: If $gcd(m, n) = 1$ then $\varphi(m \cdot n) = \varphi(m) \ \varphi(n)$

13 The mutlinomial theorem

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

- # of ways to select k objects out of a set of size n
- # of ways of dividing n objects into two piles, 1^{st} one containing k objects, 2^{nd} one containing (n-k)
- # of n-bit sequences which contain exactly k 1's
- a coefficient of $x^k y^{n-k}$ in the expansion of $(x + y)^n$

Example We have n distinguishable presents which we want to distribute among k children so that:
1^{st} child gets n_1 presents
2^{nd} child gets n_2 presents
...
k^{th} child gets n_k presents
$(n_1 + n_2 + \ldots + n_k = n)$

How many ways are there to accomplish this?

There are $\binom{n}{n_1}$ ways to select n_1 presents for the first child.

$(n-n_1)$ presents remain. In particular there are $\binom{n-n_1}{n_2}$ ways to select presents for the 2^{nd} child continuing the process we get (by the generalized product rule).

$$\begin{aligned}
&\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\dots\binom{n-n_1-n_2-\ldots-n_{k-1}}{n_k}\\
&=\frac{n!}{n_1!(n-n_1)!}\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!}\dots\\
&=\frac{n!}{n_1!\cancel{(n-n_1)!}}\frac{\cancel{(n-n_1)!}}{n_2!\cancel{(n-n_1-n_2)!}}\frac{\cancel{(n-n_1-n_2)!}}{n_3!(n-n_1-n_2-n_3)!}\dots\\
&=\frac{n!}{n_1!n_2!n_3!\dots n_k!}\\
&=\binom{n}{n_1,n_2,n_3,\ldots,n_k}\qquad\text{(multinomial coefficient)}
\end{aligned}$$

Note: $\binom{n}{k}=\binom{n}{k,n-k}$

Let us order the presents and then give first n_1 to the 1^{st} child, next n_2 to the 2^{nd} child etc.

There are $n!$ orderings in total.

Each ordering corresponds to a unique distribution of presents, however each distribution of presents corresponds to $n_1!n_2!\dots n_k!$ orderings (there are $n_i!$ ways to order presents given to the i^{th} child).

By the division rule there are $\frac{n!}{n_1!\cdot n_2!\cdot\ldots\cdot n_k!}$ ways to distribute presents.

13.1 Statement of the theorem

$$(x_1+x_2+\ldots+x)k)^n=\sum_{n_1+n_2+\ldots+n_k=n(s.t.n_1\geq 0)}\binom{n}{n_1,n_2,n_3,\ldots,n_k}x_1^{n_1}\cdot x_2^{n_2}\cdot\ldots\cdot\cdot\cdot x_k^{n_k}$$

Proof:

$$(x_1+x_2+\ldots+x_k)^n=\overbrace{(x_1+x_2+\ldots+x_k)(x_1+x_2+\ldots+x_k)\ldots(x_1+x_2+\ldots+x_k)}^{\text{n times}}$$

In the expansion we select our summand from each of the terms and multiply.

There are (by definition) exactly $\binom{n}{n_1,n_2,\ldots,n_k}$ ways of selecting x_k n_1 times, x_2 n_2 times, etc.

Example 1: What is the coefficient of $x^2y^3z^4$ in the expansion of $(x+y+z)^9$?

Answer: $\binom{9}{2,3,4}=\frac{9!}{2!3!4!}=\frac{9\cdot8\cdot7\cdot\cancel{6}\cdot5\cdot\cancel{4\cdot3\cdot2\cdot1}}{2\cdot\cancel{6}\cdot\cancel{4!}}=9\cdot\cdot7\cdot4\cdot5=1260$

Example 2: How many anagrams of the word

```
MISSISSIPPI
```

M occurs 1 time, I occurs 4 times, S occurs 4 times, P occurs 2 times → we need to distribute 11 available positions among the letters so that M gets 1 position, I gets 4 etc.

Answer: $\binom{11}{1,4,4,2}=\frac{11\cdot10\cdot9\cdot\cancel{8\cdot7\cdot6\cdot5\cdot4!}}{1!\cancel{4!\cdot4!\cdot2!}}=50\cdot99\cdot7=350\cdot99=34650$

13.2 Distributing money

We want to distribute n dollars among k children so that every child gets at least 1 dollar.

How many ways are there to do this?

Let us give out money one dollar at a time to children in order. When to stop giving money to our current child and start giving it to the next one?

The distribution is completely described by the choices of $k-1$ out of $n-1$ gaps in which we move on to the next child.

Answer: $\dbinom{n-1}{k-1}$

Another way of stating the same problem:

$x_1 + x_2 + \ldots x_k = n$

The number of positive integer solutions of this equation is $\binom{n-1}{k-1}$.

What about non-negative integer solutions (i.e. relaxing the requirement that every child gets a dollar)?

If $x_1 + x_2 + \ldots + x_k = n$ is a non-negative integer solution then.

$(x_1+1)+(x_2+1)+\ldots+(x_k+1) = n+k$ is a positive integer solution of the corresponding equation.

There are $\binom{(n+k)-1}{k-1}$ solutions to the 2^{nd} equation.

Example:

30 identical balls are to be distributed among jugglers so that each juggler has at least 3 balls and at most 7 balls. How many ways are there to do this?

Suppose we relax the second requirement. How many ways are there to do this?

An integer solution to $x_1 + x_2 + x_3 + x_4 + x_5 = 30 \qquad x_i \geq 3$

$(x_1 - 3) + (x_2 - 3) + \ldots + (x_5 - 3) = 15 \qquad \rightarrow \dbinom{15+5-1}{4} = \dbinom{19}{4}$

14 Graphs (section under construction)

14.1 Definition

Informally, a graph is a collection of dots with pairs of dots joined by lines

Dots: vertices

Lines: edges

Vertices can represent objects, computer programs, cities, people, web pages. Edges can represent pairwise relationships between the objects: two poeple know each other, etc.

A **simple graph** $G = (V, E)$ where V is a non-empty set and E is a set of pairs of elements of V.

V is the set of vertices of G.

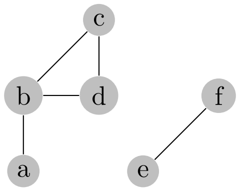
E is the set of edges of G.

$V = \{a, b, c, d, e, f\}$ $E = \{\{a, b\}, \{b, c\}, \{b, d\}, \{c, d\}, \{e, f\}\}$

Two vertices are **adjacent** if there exists an edge joining them.

An edge is **incident** to the two vertices which are its ends.

Degree of a vertex $v \in V$ is the number of edges incident to it. It is denoted by $deg(v)$.



- Vertex a has degree 1
- Vertex b has degree 3
- Vertex c has degree 2
- Vertex d has degree 2
- Vertex e has degree 1
- Vertex f has degree 1

At a party of 51 people, there is always a person who knows an even number of other people?

If G is a graph $G = (V, E), |V| = 51$, then $\exists v \in V$, $deg(v)$ is even.

Case 1: $|V| = 50$: Not true, because it is possible that $deg(v) = 49$ for all $v \in V$. This works for any even number $|V|$.

Case 2: $|V| = 1$: $|V|$ is always one, and so always odd.

→ We must prove that *At a party with an odd number of people, there is always a person who knows an even number of others.*

This is the equivalent of *if a graph has an even number of vertices, then the number of vertices of even degree is even.*. In such a case, the number of vertices with odd degree is the total number of vertices $|V|$ minus the number of nodes with even degree, which is an even number as well ($even - even = even$).

Theorem: In every graph, there is an even number of vertices of odd degree. [This statement implies the one above]

Proof: G = (V, E)

Let $|E| = m$, and prove the theorem by induction on m.

Base case:

- $m = 0 \rightarrow$ all degrees are 0 ✓
- $m = 1 \rightarrow$ all vertices have degree 1 ✓

Induction step: Suppose $|E| = m + 1$. By the induction hypothesis, the theorem is true for every graph on m edges. Pick two vertices $u, v \in V$ joined by an edge $\{u, v\}$

1. If $deg(u), deg(v)$ are both even in G, then in the new graph (after deleting uv), we have two more vertices of odd degree, so the parity of the number of vertices of odd degree is unchanged.
2. Exactly of one of u and v had an odd degree → the number of vertices of odd degree is unchanged.

3. If $deg(u), deg(v)$ are both odd → deleting the edge decreases the number of vertices of odd degree by two.

$\sum_{v\in V} deg(v)$ is even ↔ there is an even number of vertices of odd degree

Theorem: $\sum_{v\in V} deg(v) = 2|E|$

Proof: Both sides of this identity enumerate ends of edges.

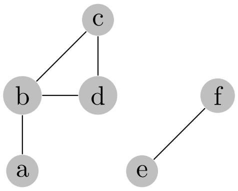
Example: In a simple graph $G = (V, E)$, there are always $u, v \in V, u \neq v, deg(u) = deg(v)$ $(|V| \geq 2)$

Proof: $|V| = n$ Maximum possible degree of a vertex in G is $n - 1$. The set of possible degrees is $\{0, 1, 2, \ldots, n - 1\}$.

We are done by the pigeonhole principle unless the degrees of vertices in the graph are $\{0, 1, 2, \ldots, n - 1\}$.

It is impossible to have two vertices v and u such as $deg(v) = 0$ and $deg(u) = n - 1$, we cannot have at the same time a person knowing nobody and a person knowing everybody.

English explanation: For each vertex, we count the edges that leave that vertex (this the degree of the vertex). If we sum these numbers, we count every edge twice. So dividing the sum by two, we get the number of edges.



A **walk** in a graph is a sequence of vertices so that two consecutive vertices are adjacent. **Example**: The sequence of vertices $[a, b, c, d, b, c]$ is a walk.

A walk is **closed** if its first and last vertices are the same. **Example**: The sequence of vertices $[a, b, c, d, b, a]$ is a closed walk.

A walk is a **path** if it doesn't repeat any vertices. **Example:** The sequence of vertices $[a, b, c, d]$ is a path.

A **circuit** is a closed walk which does not repeat any edges. **Example**: The sequence of vertices $[b, c, d, b, a]$ is a circuit.

A **cycle** is a closed walk which does not repeat any vertices except for the first and last one. **Example**: The sequence of vertices $[b, c, d, b]$ is a cycle.

1736 Euler: Koninsberg bridges

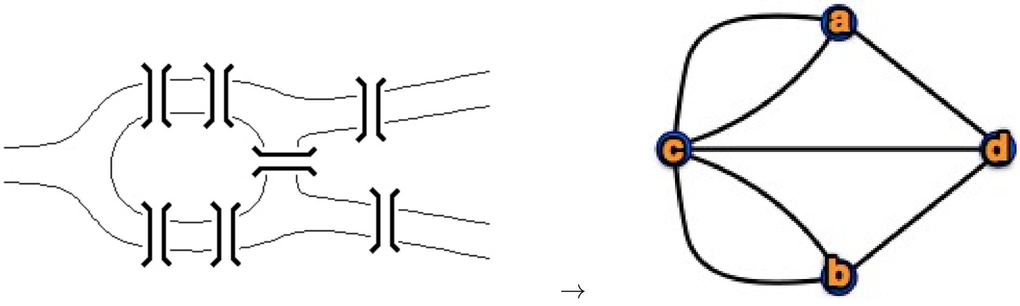
Is there a way to walk around Koninsberg passing along every bridge exactly once? Is there a walk in this graph using every edge exactly once?

14.2 Cycles & Circuits

Simple graphs: there is at most one edge joining any pair of vertices

In general graphs this condition is relaxed.

Koninsberg bridges: Is it possible to walk around Koninsberg crossing each of its seven bridges exactly once?



Each land parcel is represented by a vertex (labelled with a letter) and each edge represents one of Koninsberg's seven bridges.

Does there exist a walk which uses every edge exactly once?

14.2.1 Eulerian circuit

Defintion: A circuit in a graph using every edge exactly once.

In a circuit, every time we visit a vertex, we use two edges incident to this vertex.

A graph is called **connected** if there is a path (or walk) between any pair of vertices.

Theorem: A connected graph contains an Eulerian circuit if and only if every vertex in it has an even degree.

Proof: We already established the "only if" part of the statement, now for the if part.

"If" part: Choose a circuit in our graph using as many edges as possible. If it uses all of the edges, this is an Eulerian circuit.

If not, there exists an edge not in our circuit, and because the graph is connected, we can choose an edge incident to some vertex of this circuit.

Every vertex is incident to an even number of edges not in the chosen circuit.

Starting with the original edge, we can construct a walk using only edges not belong to the circuit.

We can continue until we reach the vertex we started at, i.e., we constructed a circuit, say C', which contains no edges of C, but shares a vertex v with the original circuit C.

We can trace C (starting and ending at v), and then trace C', so $C \cap C'$ also correspondings to a circuit, contradicting the choice of C.

14.2.2 Eulerian Walk

An **Eulerian walk** is a walk (not necessarily closed) which uses every edge exactly once.

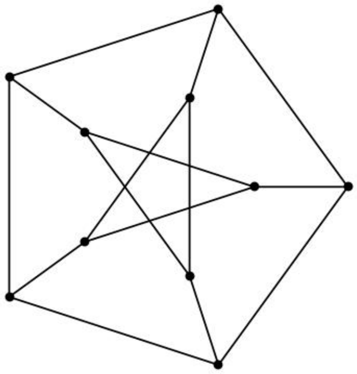
Corollary: A connected graph has an Eulerian walk if and only if it has at most two vertices of odd degree.

Proof:

- **"Only if"**: Let an Eulerian walk start at u and end at v. If $u = v$, this is an Eulerian circuit, so by the theorem, all degrees are even. If $u \neq v$, add an edge to the walk, and the graph. We have an Eulerian circuit in the new graph, so all degrees are even, so only $u \& v$ had an odd degree before.
- **"If"**: If all degrees are even, we are done. If exactly two vertices $u \& v$ have an odd degree, add an edge $u - v$. In the new graph, there is an Eulerian circuit, which corresponds to an Eulerian walk in the original graph.

A **Hamiltonian cycle** is a cycle in a graph that uses all of the vertices. The problem of determining whether a graph has a Hamiltonian circuit is **NP-complete**. (if $P \neq NP$, it is not possible to find Hamiltonian circuits efficiently)

14.2.3 The Petersen graph



This graph has no Hamiltonian cycle.

A graph is **3-regular** of every vertex has degree 3.

A **3-edge colouring** of a 3-regular graph is a way of assigning colours $\{1, 2, 3\}$ to the edges of the graph so that every vertex is incident to the edges of all 3 colours. If a 3-regular graph has a Hamiltonian cycle, then it has a 3-edge colouring (use colours 1 and 2 on the cycle)

However, the Petersen graph does not have a 3-edge colouring. Suppose there is a 3-edge colouring.

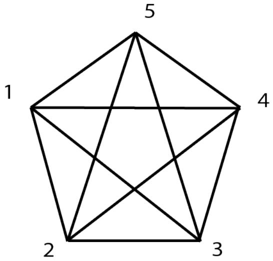
1. There is an edge of every colour on the outer cycle.
2. It follows that the inner cycle has at least two edges of every colour, but there are 3 colours and only 5 edges.

14.2.4 Hamiltonian Cycles

A cycle which uses every vertex exactly once.

Complete graph on n vertices K_n

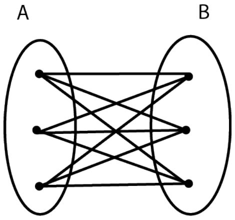
Example:K_s a graph where every pair of vertices is joined by an edge



K_n has n vertices $\binom{n}{2}$ edges $= \frac{n(n-1)}{2}$.

Complete Bipartite graph K_{n_1,n_2}

A complete bipartite graph $K_{n_1,n_2} = (V, E)$



K3,3

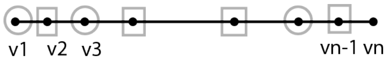
$V = A \cup B \qquad A \cap B = \emptyset \qquad |A| = n_1 \qquad |B| = n_2$

Every vertex of A is joined to every vertex of B and there are no other edges ($n_1 n_2$ edges in total)

If $n_1, n_2 \geq 2$, K_{n_1,n_2} has a Hamiltonian cycle if and only if $n_1 = n_2$ (the vertices of the parts A & B must alternate along the cycle).

Theorem (Dirac): Let G be a simple graph on n vertices, $n \geq 3$, then if $deg(v) \geq \frac{n}{2}$ for every vertex v of G then G has a hamiltonian cycle.

Proof: Assume that G does not have a Hamiltonian cycle. Further, assume that G has as many edges as possible subject to all of the above (Adding an edge between any pair of non-adjacent vertices of G creates a Hamiltonian cycle.)

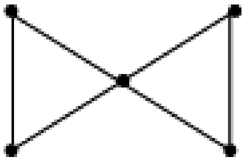


There are $\geq \frac{n}{2}$ squares neighbours of v_i

Let the circles in the picture denote vertices to the left of the squares.

There are $\geq \frac{n}{2}$ circles. If v_n is adjacent to one of these vertices say v_k then: $v_1 \rightarrow v_k \rightarrow v_n \rightarrow v_{k+1} \rightarrow v_1$ is a hamiltonian cycle. So we may assume that v_n is adjacent to any of these vertices.

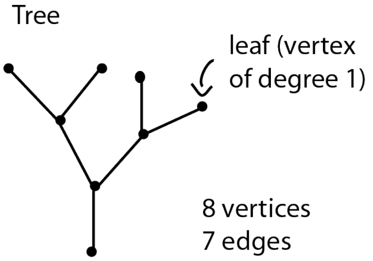
So there are only $n - 1 - \frac{n}{2} < \frac{n}{2}$ vertices which v_n can be adjacent to → contradiction ■

Example: 

$deg = \lfloor n/2 \rfloor \rightarrow$ No hamiltonian cycle.

15 Trees (section under construction)

A **tree** is a connected simple graph without any cycles.



Theorem:

1. In a tree there exists a unique path between any pair of vertices.
2. Deleting any edge from a tree disconnects it.
3. Adding an edge between non-adjacent vertices of a tree to a tree creates a cycle.
4. If a tree has at least ≥ 2 vertices then it has ≥ 2 leaves.
5. The number of edges in a tree is one less then the number of vertices.

Proofs for the above:

1. Suppose not, for some pair of verties x, y there exist two paths between them. Let p_1, p_2, denote those paths. Let $x^{'}$ be the first vertex where p_2 deviates from p_1. Let $y^{'}$ be the next vertex along p_1 which belongs to p_2. Then, if $x^{'} \rightarrow (p_2) \rightarrow y^{'} \rightarrow (p_1) \rightarrow x^{'}$ is a cycle → contradiction
2. If we delete an edge $e = \{x, y\}$. e was the edge of the unique path from x to y after deleting it there are no paths from x to y ✓
3. Adding an $x - y$ edge together with the existing path from x to y in a tree creates a cycle.
4. Considering the longest path in a tree, then x and y are both leaves.
5. Induction on the number of vertices.
   Base case:1 vertex three has no edges
   Induction step: Consider a tree on $(n+1)$ vertices. Let v be a leaf of this tree. Delete v (this removes 1 vertex and 1 edge). The remaining graph clearly has no cycles and is connected. (no path without an end in v can use v).
   By the induction hypothesis it has n vertices and $n - 1$ edges so our graph had n edges. ■

15.1 Counting trees

How many different trees are there with n vertices?

V = {0,1,2}

Unlabeled Trees

$G_1 = (V_1, E_1), \quad G_2 = (V_2, E_2)$ - simple graphs

G_1 and G_2 are **isomorphic** if there exists $f : V_1 \rightarrow V_2$ a bijection, such that $u - v \in E_1$ if and only if $f(u) - f(v) \in E_2$. In other words, two nodes in the first tree that are connected by an edge correspond to nodes in the second tree that are connected by an edge and vice-versa.

How many different (non-isomorphic) trees are there?

n =1 , n = 2

There is no closed form expression of the # of unlabeled trees.

Labeled trees

How many trees are there with the vertex set V ={0,1,2,. . . , n-1}? (what about simple graphs?)

There are $\binom{n}{2}$ possible edges and $2^{\binom{n}{2}}$ different simple graphs.

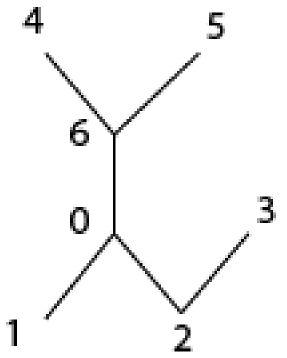
- n = 1: 1 way
- n = 2: 1 way
- n = 3: 3 ways
- n = 4: 4 ways to label linear tree, 24 ways to label the non-linear tree if we fix the left end but this way we count every tree twice so 24/2. $12 + 4 = 16$

15.1.1 Number of labeled trees

Theorem (Cayley): There are n^{n-2} labeled trees with n vertices.

How can we represent trees in the computer?

Adjacency matrix



can be represented by the adjacency matrix:

$$\begin{array}{ccccccc} 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{array} \quad \begin{cases} 1 \text{ if and only if corresponding vertices are adjacent} \\ 0 \text{ otherwise} \end{cases}$$

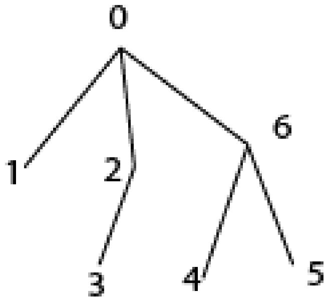
$\rightarrow \binom{n}{2}$ bits

There is no way to represent a general graph with fewer bits. But for trees we can do better.

The Incidence List: A tree has $n - 1$ edges. Let us write down the ends of the edges.

$\begin{pmatrix} 0 & 0 & 0 & 2 & 4 & 5 \\ 1 & 2 & 6 & 3 & 6 & 6 \end{pmatrix} \rightarrow$ a sequence of $2(n - 1)$ numbers (takes $2(n - 1)\lceil log_2 n\rceil$ bits)

There are at most $n^{2(n-1)}$ labeled trees on n vertices.



The Parent List: For every vertex (except the root) there exists a unique edge from it along the path towards the root. We call the second end of this edge the **parent** of the vertex. Every edge joins some vertex to its parent.

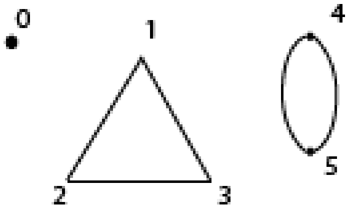
1	2	3	4	5	6
0	0	2	6	6	0.

The second row completely records the tree as the first row is just 0 to n in order $\leq n^{n-1}$ trees

Every tree corresponds to a parent list, but the converse is not true. Example:

1	2	3	4	5
2	3	1	5	4

corresponds to a disconnected non-simple graph.



Prüfer codes

At each step we record the leaf with the smallest label, we record its parent and then we erase the leaf and recurse (extended Prüfer code).

1	3	5	2	6	8	7	4	9
2	2	2	0	7	7	4	0	0

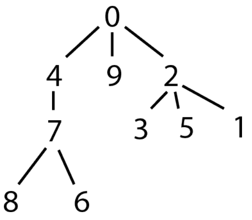
$2(n-1)$ numbers

It is possible to reconstruct the first row from the second one.

Justification: i^{th} entry of the 1^{st} row is the smallest number which is not yet in the 1^{st} row, and does not appear in the 2^{nd} row in the i^{th} or greater position.

Furthermore, we do not need the last column since the last vertex will always be 0 (the root).

Every tree can be recorded as a sequence of $n-2$ numbers.



Cayley's theorem: There are n^{n-2} labeled trees on n vertices.

Proof: Prufer codes

1 3 5 2 6 8 7 4 9 → Extended Prufer code

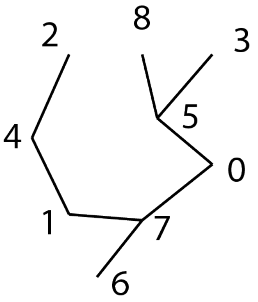
2 2 2 0 7 7 4 0 0 → Prufer code

Reconstructing extended Prufer code from the Prufer code

1. Last digit of the 2nd row is 0
2. Every entry of the first row is the smallest (non-zero) number that does not appear to the left of it in the 1st row or underneath and to the right in the 2nd row (there is always a choice)

Example: Tree with 9 vertices. Prufer code: 7 numbers from 0 to 8

2	3	4	1	6	7	8	5
4	5	1	7	7	0	5	0



Every Preufer code corresponds to a graph with $n-1$ edges and n vertices

[picture of connections between first row] → Every vertex (except for 0) is joined to exactly one vertex to the right of it.

15.1.2 Number of unlabeled trees

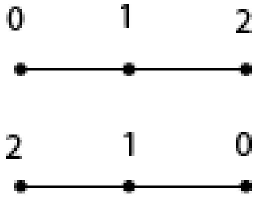
Unlabeled trees: let T_n be the number of unlabeled trees on n vertices $T_1 = T_2 = T_3 = 1, \quad T_4 = 2, \quad T_5 = 3$ (draw them out to see)

Theorem:

$$\frac{n}{n!} \leq T_n \leq 2^{2(n-1)} = 4^{n-1}$$

→ Lower bound on the number of unlabeled trees

$$\underbrace{n^{n-2}}_{\text{\# of labeled trees}} \leq \underbrace{n!\cdot T_n}_{\substack{\text{\#of ways of labeling}\\ \text{unlabeled tree}}}$$



Each unlabeled tree can be labeled in at most $n!$ ways. Since the number of labeled trees is n^{n-2}, the number of unlabeled trees is at least $\frac{n^{n-2}}{n!}$

Stirling's formula

$$n! \approx \sqrt{2\pi n}(\frac{n}{e})^n$$

$$\lim_{n\to\infty} \frac{n!}{\sqrt{2\pi n}(\frac{n}{e})^n} = 1$$

$$\frac{n^{n-2}}{n!} \approx \frac{n^{n-2}}{\sqrt{2\pi n}\frac{n^n}{e^n}} = \frac{e^n}{\sqrt{2\pi}n^{5/2}} = \frac{1}{\sqrt{2\pi}}n^{-5/2}e^n$$

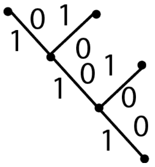
→ Upper bound on the number of unlabeled trees

$$T_n \leq 2^{2(n-1)} = 4^{n-1}$$

Trace the tree drawn in the plane. It takes 2(n-1) steps, at each step, let us record 1 if we go away from the root and 0 if we go towards the root.

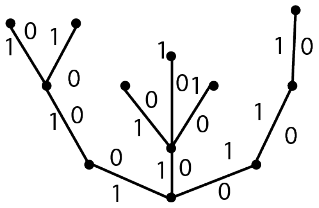
The tree is completed described by a sequence:

1 1 1 0 1 0 0 1 0 0



Another example:

111010001101010100111000



There are $n-1$ edges in a tree and each edge must be recorded by a 0 and a 1. The length of the sequence is therefore $2(n-1)$. There are $2^{2(n-1)} = 4^{n-1}$ such sequences.

Note that a sequence of 0's and 1's does not necessarily produce a tree. Example: 1 1 0 0 0 1 1 0

$$\underbrace{11000}_{\text{in every initial segment the \# 1's must be at least as large as the \# of 0's}} \qquad 110$$

Furthermore, there must be an equal number of 0s and 1s.

15.2 Minimum cost (or spanning) tree

We have n cities, 8 want to build a road netwrok connecting them. We want to be able to get from every city to every other city possibly passing some cities in between. We know costs (on distances) for building roads between cities. How can we build the network spending as little as possible.

Let $d : \{0,1,\ldots,n-1\} \times \{0,1,2,\ldots,n-1\} \to \mathbb{R}_+$ be the distance function $d(0,1) = 1 \qquad d(1,2) = 2\ldots$

We want to construct a tree on these n vertices, with the sum of distances over its edges as small as possible.

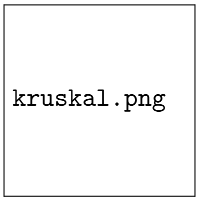
Enumerating all the trees takes too much time.

Greedy algorithm: "Be as greedy as possible at each step." At each step of the algorithm build the road which is as cheap as possible (i.e. connects two cities at the shortest distance) joining two cities not connected by the network.

Given a weighted graph $G = (V,E)$ find a spanning tree:

$T = (V,S)$ of G with $\sum_{e \in S} d(e)$ minimum

Kruskal's (Greedy) algorithm



Grow S step by step. Start with $S = \emptyset$. At each step add to S an edge of G with the minimum weight (value of d) so that the graph formed by edges in S remains acyclic.

(If G was connected this algorithm produces a tree, if not we can add edges)

Theorem: Kruskal's algorithm produces a minimal cost tree.

Proof: We will prove by induction on the # of steps performed that S belongs to some minimum cost tree. (This suffices)

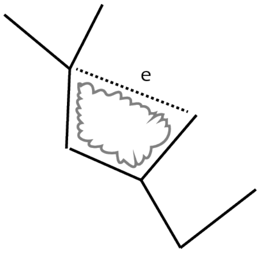
Base case: In the beginning, $S = \emptyset$.

Induction step: By the induction hypothesis S belongs to some MCT T', we add an edge e to S. Our goal is to show that $S \cup \{e\}$ belongs to some MCT.

- **Case 1**: e belongs to T (the edge of set of T'), then so does $S \cup \{e\}$, and we are done.

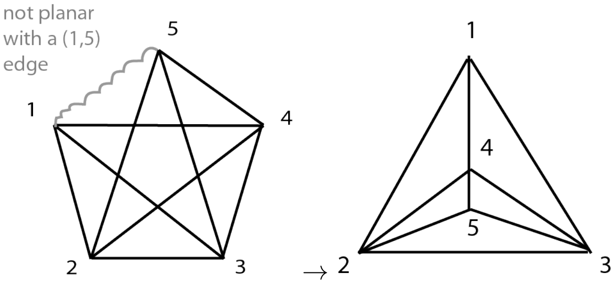
- **Case 2**: e does not belong to T'. Adding e to T' creates a cycle C. Is it possible that all edges of C belong to S? No, because in our algorithm S never contains any cycles. So consider e' in C, $e' \notin S$. We added e and not e' so $d(e') \geq d(e)$.
  Consider deleting e' from T' and adding e.

Proof: We end up with a new tree. The cost of this tree is minimal.



16 Planar graphs

Graphs which can be drawn in the plane without crossings.



Theorem (Fary 48): A planar graph always has a drawing where all the edges are represented by straight lines.

If a graph is drawn on the plane, it partitions it into regions called **faces**.

Theorem (Euler's formula): Let G be a connected graph drawn in the plane with n vertices, m edges and f faces then $f = m - n + 2$

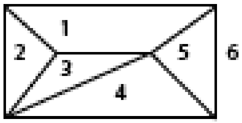
Proof: By induction on the number of edges m

Base case: 0 edges → 1 vertex → 1 face ✓

Induction step: We are assuming that the formula holds for all graphs with $< m$ edges.

- **Case 1**: G has no cycles → G is a tree. There is one face and $m = n - 1 \rightarrow 1 = (n-1) - n + 2$ ✓
- **Case 2**: G has a cycle C. Delete an edge of C. The two sides of the deleted edge belonged to different faces. Deleting e decreases the number of faces by 1.
  By the induction hypothesis: $(f-1) = (m-1) - n + 2$ ✓

Example:



6 vertices = n
10 edges= m
6 faces = f

What is the maximum number of edges in a planar simple graph with n vertices?

Euler's formula n -m + f = 2 for every planar graph

Theorem: A planar graph on n vertices has edges $m \leq 3n - 6$ (can be achieved for all $n \geq 3$)

Proof:

- Every edge belongs to at most two faces (1)
- Every face is bounded by at least 3 edges (2)

Count pairs (edge, face) such that the edge belongs to the face.

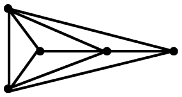
Say there are L such pairs.

$$\begin{cases} L \leq 2m \text{ from } (1) \\ L \geq 3f \text{ from } (2) \end{cases} \quad \rightarrow 3f \leq 2m$$

$3(m - n + 2) \leq 2m$

$m - 3n + 6 \leq 0$

$m \leq 3n - 6$



This is a complete graph on 5 vertices with one edge deleted.

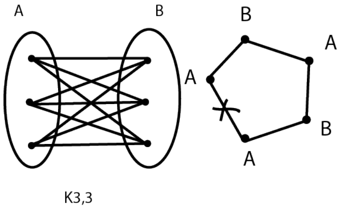
Corollary: K_5 is not planar

10 edges 5 vertices $\quad 10 > 3 \cdot 5 - 6$

fig20.png

A **subdivision** of a graph G is a graph obtained from G replacing some of the edges by paths, that is dividing those edges using new vertices of degree 2.

Clearly a subdivision of a non-planar graph is non-planar. So any graph with a subdivision of k_5 as a subgraph is non planar.



Bipartite graphs: A graph $G = (V, E)$ is bipartite if there exists a partition $V = A \cup B$, $A \cap B = \emptyset$ so that every edge joins a vertex of A to a vertex of B.

(In a bipartite graph every cycle has even length). In particular, it has length ≥ 4.

Theorem: $m \leq 2n - 4$ for a planar simple bipartite graph G with n vertices and m edges. $n \geq 4$

Proof:

- Every face contains at least 4 edges

$$\begin{aligned} 2m &\geq 4f \to m \geq 2f \\ m &= n + f - 2 \leq n + \frac{m}{2} - 2 \\ 2m &\leq 2n + m - 4 \\ m &\leq 2n - 4 \end{aligned}$$

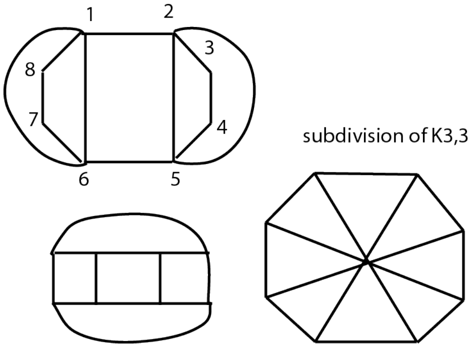
- **missed**

Theorem (Kuratowski): A graph G is non-planar if and only if it contains a subdivision of K_5 or $K_{3,3}$ as a subgraph.

Being planar is in NP → a drawing is a certificate.

Being non-planar is also in NP → a subdivision of K_5 or $K_{3,3}$ is a certificate.

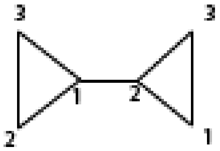
It is possible to test planarity very efficiently (in fact, in linear time $O(n)$)



16.1 Coloring graphs

A **(proper) k-coloring** of a graph $G = (V, E)$ is a function $c : V \to \{1, 2, \ldots, k\}$ so that $c(u) \neq c(v)$ for every pair of adjacent vertices $u, v \in V$.

Chromatic number: $\chi(G)$ of a graph G is the smallest positive integer k such that G allows a k-coloring.



x(G) = 3 x(G) ≥ 3 → 2 is not enough. x(G) ≤ 3 (just color the graph to show)

Graph coloring **k-coloring**: c - V $\rightarrow \{1, 2, \ldots k\} : c(u) \neq c(v)$ if u is adjacent to v

$X(G)$ [chromatic number] - minimum k such that G can be k-colored.

[$X(G) = 1$ if and only if G has no edges] When is $X(G) = 2$?

G is **bipartite** if V can be partitioned:

$V = A \cup B$ $A \cap B = \emptyset$

so that every edge joins a vertex of A to a vertex of B.

Claim:

A graph is 2-colorable if and only if it is bipartite.

A graph is not bipartite if it contains an odd cycle (a cycle with an odd number of vertices).

Theorem: A graph is bipartite (or two-colorable) if and only if it contains no odd cycles.

Proof: A graph is not bipartite if and only if it contains an odd cycle.

We already know the 'if' part, so it only remains to show the 'only if' part.

Suppose that G is not bipartite (or two-colorable), we may assume that G is connected. Let V be some vertex of G.

Let $d(u, v)$ denote the length of the shortest path between u and v for any other vertex u. Color v in color 1, and color every other vertex u in color 1 if $d(u, v)$ is even, and color 2 if $d(u, v)$ is odd

This doesn't produce a two coloring. So there are adjacent vertices u_1 and u_2 of the same color.

$d(x, v)$ - differ by at most 1 $d(y, v)$

something.png

This is the closest vertex to u_1 and u_2 along the shortest paths along the shortest paths from u_1 and u_2 to v to belongs to both paths.

$d(u_1, v) = k_1 + L$ $d(u_2, v) = k_2 + L$ $k_1 = k_2 = k$

[BOTTOM OF FIGURE] - an odd cycle of length 2k.

The problem of determining whether $X(G) \leq 3$ is NP-hard (at least as hard as every problem in NP)

16.2 What obstructions are there to k-coloring?

K_{k+1} as a subgraph → There exist non k-colorable for any k with [missing]?

Theorem (Brooks): If a graph has maximum degree k then it is $(k + 1) - colorable$.

Proof: By induction on the number of vertices.

- **Base Case:** (1 vertex) ✓

- **Induction Step:** Let G be a graph with n+1 vertices. Choose some vertex v in G and remove it. The graph that remains has n vertices, has maximum degree $\leq k$ so is $(k+1)$-colorable by the induction hypothesis.

Neighbors of v use at most k colors, so there is at least one color that is not yet used, and we can color v in this color.

16.3 Coloring of planar maps

: In a map every country is a contiguous region of the plane. We want to colour the map so that any two countries which share a border (non-zero length segment) receive different colors. How many colours suffice?

The Four colour theorem: Every map is 4-colourable (Francis Guthrie 1852). Appel & Hakken published a non human-readable proof in 1976 (solved by computer-assistance using case-analysis)

Dual graph:

- Vertices correspond to regions
- Two vertices are joined by an edge if regions share the segment of the border
- We get a planar graph.
- It now suffeces to show that $\chi(G) \leq 4 (\leq 5) foreveryplanar(simple)graphG$

17 Coloring planar graphs

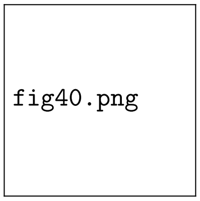
Four-colour theorem: $\chi(G) \leq 4$ for every planar (simple) graph G.

Six-color theorem: $\chi(G) \leq 6$

- **Claim:** Every planar simple graph contains a vertex of degree ≤ 5
- **Proof of thTe claim:** $\sum_{v \in V} deg(v) = 2e \leq 2(3n-6) = 6n - 12$
  Suppose the graph has n vertices

$$\frac{\sum_{v \in V} deg(v)}{n} \leq 6 - \frac{12}{n} < 6$$

- **Proof of the 6-color theorem:** By induction on the number of vertices in G.
  - **Base case:** 1 vertex ✓
  - **Induction Step:** Let v be a vertex of degree ≤ 5 in G. By the induction hypothesis if we delete v from G we can colour the vertices in 6 colours, but then we can also colour v, because at most 5 colours are used on its neighbours.

  Proof of the 5-color theorem: $\chi(G) \leq 5$ 

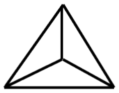
  Note: K_6 is not 5-colorable but every vertex has degree 5.

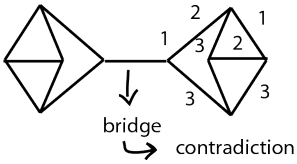
Proof: By induction as the previous theorem.

- **Base case**: same as before
- **Induction step**: Let v be the vertex of the smallest degree in G.
    - **Case 1**: $deg(v) \leq 4 \rightarrow$ then the argument from the 6 colour theorem works.
    - **Case 2**: $deg(v) =$
    - The new graph can be coloured in 5 colours by the induction hypothesis. Let $u_1 \& u_3$ inherit the colour of the new vertex in the smaller graph. Neighbours of v now receive at most 4 colours, so there is a colour available for v.
      The only possible difficulty in this step is that $u_1 \& u_3$ are adjacent. But we could have chosen any pair of neighbours of v instead. There exists some pair of non-adjacent neigbours as otherwise G would have contained a subgraph isomorphic to K_5.

3-edge coloring of a graph with all vertices of degree 3 $\rightarrow$ cubic graphs

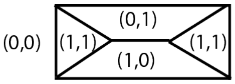
Coloring of edges in colours 1,2,3 so that every vertex is incident to an edge in every colour.





A **bridge** in a graph is an edge so that deleting it disconnects the graph.

Theorem: Every cubic planar graph with not bridges can be 3-edged colored.



Proof: By the 4.C.T. the faces of the graph can be coloured in 4 colours. (0,0), (0,1), (1,0), (1,1) Now we assign colours to edges (0,1),(1,0),(1,1). If an edge forms a border of regions with colours $(a_1, b_1) \& (a_2, b_2)$ we give it colour (c, d) so that:

- $c = 0$ if $a_1 = a_2$ and $c = 1$ otherwise
- $d = 0$ if $b_1 = b_2$ and $d = 1$ otherwise
- No edge receives a (0,0) colour.
  Why no two edges incident to the same vertex receive the same colour?
  TWo edges of the same colour would imply that two faces have the same colour.

18 Review

18.1 Bijective proofs of combinatorial formulas

Find a bijective proof of $\binom{n}{r}\binom{r}{k} = \binom{n}{k} n - k \; chooser - l$

For $n \leq r \leq k$.

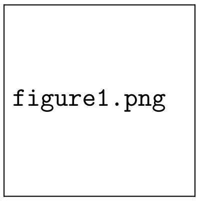
$[n] = \{1, 2, \dots, n\}$

$A \in [n], |A| = r, B \in A, |B| = k$

We can think of the left side as counting the pairs of subsets (A, B):

$\{(A, B) : |A| = r, |B| = k, B \in A \in [n]\}$

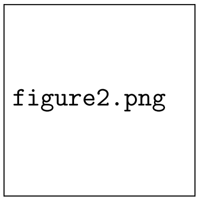
That is the set that is counted on the left.



We can think of the right side as counting the pairs of subsets (C, D):

$\{(C, D) : |C| = k, |D| = r - k, C \cap D - \emptyset, C, D \leq [n]\}$

This is the set that is counted on the right.



We want a bijection f such that:

$f : (A, B) \to (B, A - B)$

maps the pairs from "the left side" to pairs on "the right side".

$(C, D) \to (C \cup D, C)$

is an inverse map, so f is a bijection.

18.2 Example problem from final

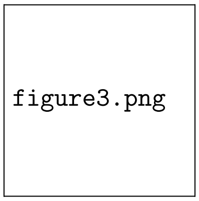
Prove $\binom{2n}{n} + \binom{2n}{n+1} = \frac{1}{2}\binom{2n+2}{n+1}$

$\frac{\cancel{(2n)!)}}{n!n!} + \frac{\cancel{(2n)}!}{(n+1)!(n+1)!} = \frac{1}{2}\frac{(2n+2)!}{(n+1)!(n+1)!}$

$\cancel{(n+1)}(n+1) + \cancel{(n+1)}(n) = \cancel{\frac{1}{2}}(2n+1)\cancel{(2n+2)}$

$(n+1) + n = 2n + 1\checkmark$

Find a bijective proof of the above combinatorial equation:



$$\binom{2n+2}{n+1} = \underbrace{\binom{2n}{n-1}}_{\text{Number of ways of selecting of the last two elements}} + \underbrace{2\binom{2n}{n}}_{\text{Number of ways of selecting one of the last two elements}}$$

Dividing by half:

$\frac{1}{2}\binom{2n+2}{n+1} = \binom{2n}{n} + \frac{1}{2}(\binom{2n}{n-1} + \binom{2n}{n+1} = \binom{2n}{n} + \binom{2n}{n+1}$

18.3 Another problem

$$\sum_{i=0}^{k} \binom{n+i}{n} = \binom{n+k+1}{n+1}$$

This is selecting a $(n+1)$ element subset out of the set of size $(n+k+1)$.

figure4.png

Consider the position of the last selected element. It is between the $(n+1)^{st}$ and $(n+k+1)^{st}$ position, so it is position is $n+i+1$ for $0 \leq i \leq k$

There are $\binom{n+i}{n}$ ways of selecting the other k elements.

18.4 Logic

Know how to prove logical formulas using the rules of logic or logic tables.

Example:

Show $(p \wedge (p \rightarrow q)) \rightarrow q$ is a tautology.

p	q	$p \rightarrow q$	$p \wedge (p \rightarrow q)$	$(p \wedge (p \rightarrow q)) \rightarrow q$
1	1	1	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	1

Show that $P \vee (q \rightarrow r))$ is equivalent to $q \rightarrow (p \vee r)$

Now $p \vee ((\neg q) \vee r) \Leftrightarrow \neg q \vee (p \vee r)$ by communitativy and associativity of v

Write down the negation of $\forall n \in \mathbb{N}((n^3 + 6n + 5$ is odd $) \rightarrow ($n is even$))$

So bascially $\forall n \in \mathbb{N}(p(n)) \exists n \in \mathbb{N} \neg((n^3 + 6n + 5)$ is odd$) \rightarrow ($ n is even$))$

Negation is $\exists n \in \mathbb{N}(\neg p(n)) \exists n \in \mathbb{N}((n^3 + 6n + 5)$ is odd $) \wedge (n$ is odd$)) \rightarrow$ false

$n \equiv 1(mod\ 2) \rightarrow$ odd $n^3 \equiv 1(mod\ 2)$ $n^3 + 6n + 5 \equiv 1 + 0 + 1 \equiv 0(mod\ 2)$

18.5 Number theory review

Euclid's algorithm not on the final because it was on the midterm?

Fermat's Little Theorem: $a^{p-1} \equiv 1(mod\ p)$ for all primes $p, p \nmid a$

Compute $302^{303}(mod 11)$

$302 \div 11 = 27$ remainder 5

$302 \equiv 5(mod\ 11)$ $302^{302} \equiv 5^{302} = 5^{300} \cdot 5^2 = (5^{10})^{30} \cdot 5^2 \equiv 5^2 = 25 \equiv 3(mod\ 11)$

Show that for every prime p and integer $k \qquad 1 < k \leq p$

(a)

$p | \binom{p}{k}$

$\binom{p}{k} = \frac{p!}{k!(p-k)!}$ → the numerator is divisble by p and the denominator is not divisible by p so the ratio is divisible by p (only true for primes)

(b)

Show that the product of all primes strictly between n and $2n$ is no greater than $\binom{2n}{n} = \frac{(2n)!}{n!\ n!}$

By the same argument as in $\binom{2n}{n}$ is divisible by every prime $p: \quad n < p \leq 2n$

So the product of these primes divides $\binom{2n}{n}$, so it's at most $\binom{2n}{n}$

Show that

$$\sum_{k=0}^{n} k(n-k) = \binom{n+1}{3}$$

Proof by induction on n:

- **Base case** (n=1): $0 \cdot 1 + 1 \cdot 0 = \binom{2}{3} \qquad \checkmark$
- **Induction step:**

$$\sum_{k=0}^{n+1} k((n+1)-k) = \sum_{k=0}^{n+1} k(n-k) + k = \sum_{k=0}^{n+1} k(n-k) + \sum_{k=0}^{n+1} k$$

$$\binom{n+1}{3} = \sum_{k=0}^{n} k(n-k) + (n+1)n(n-1) - (n+1) \text{ (by induction hypothesis)}$$

$$= \frac{(n+1)n(n-1)}{3!} - (n+1) + \frac{(n+1)(n+2)}{2} =? \binom{n+2}{3} = \frac{(n+2)(n+1)n}{3!}$$

Multiply by 6 $n(n-1) - 6 + 3(n+2) = (n+2)n$
$n^2 - n - 6 + 3n + 6 = n^2 + 2n \qquad \checkmark$

Show that $\sum_{k=0}^{n} = \frac{n!2^k}{k!(n-k)!} = 3^n$

$\sum_{k=0}^{n}\binom{n}{k}2^k1^{n-k} = 3^n$ $\sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k} = (x+y)^n$ $x = 2y = 1$ (binomial theorem with x = 2 y = 1)

How many pairs of subset $A, B \subseteq \{1,2,3,4,5\}$ are there so that $A \subseteq B$

Product rule: Every element can

- belong to neither A nor B
- belong to A and B
- belogn to just B (3^5 choices in total → 243)

How many solutions are there to $x_1 + x_2 + x_3 + x_n = 30$ with $3 \leq x_i \leq 1$ and x_i is an integer

$x_1 + x_2 + \dots x_k = n$

it has $\binom{n+k-1}{k-1}$ non-negative integer solutions

$(x_1 - 3) + (x_2 - 3) + (x_3 - 3) + (x_4 - 3) = 30 - 3 \cdot 4 = 18$

$y_i = x_i - 3$

$y_1 + y_2 + y_3 + y_4 = 18$

$0 \leq y_i \leq 7$ without and upper bound we have $\binom{18+4-1}{4-1} = \binom{21}{3}$

Let $A_i = \{\text{solutions with } y_i \geq 8\}$

In total we have $\binom{21}{3} - |A_1 \cup A_2 \cup A_3 \cup A_4|$ solutions which satisfy the bound.

$|A_i| = \binom{13}{3}$ $|A_i \cap A_j|$

$y_1 \geq 8 \rightarrow (y_1 - 8) + y_2 + y_3 + y_4 = 10$ $\binom{10+3}{3} = \binom{13}{3}$

$y_1 \geq 8, \quad y_2 \geq 8 \rightarrow (y_1 - 8) + (y_2 - 8) + y_3 + y_4 = 18 - 2 \times 8 = 2$

$\binom{21}{3}\sum_{i=1}^{4}|A_i| + \sum_{1\leq i<j\leq 4}|A_1 \cap A_j| = \binom{21}{3} - 4\binom{13}{3} + 6\binom{5}{3}$

Notes: Remember brufer codes, kruskal's algorithm and how to count anagrams (e.g. mississipi)

Let G be a planar connected graph with every vertex of degree 3 and 46 vertices. We add 30 edges to G arbitrarily.

How many edges and faces will there be in the resulting graph?

Twice the number of edges in $G = \sum \deg(V) = 46 \cdot 3 = 138$

number of edges $= \frac{46\cdot 3}{2} = 23 \cdot 3 = 69 \rightarrow$ after adding 30 edges we get 99.

By Euler's formula: $F = E - V + 2 = 99 - 46 + 2 = 55$

Does there exist a simple planar graph so that its edges can be coloured in colours red, blue and green so that every edge of every colour form a spanning tree (a tree on the same set of vertices).

No.A tree on n vertices has $(n-1)$ edges. Three trees have $3(n-1) = 3n - 3$ edges in total. But a planar graph has at most $3n - 6$ edges (for $n \geq 3$).

A **bridge** in a connected graph is an edge whose deletion disconnects the graph.

Show that a connected graph is a tree if and only if every edge is a bridge.

→ If G is a tree, consider an edge $u - v$, there exists an unique pass between u and v consisting only of this edge, so after deleting it, there is no path between u and v, so G is disconnected.

← It suffices to show that G has no cycles. Suppose not.

Deleting an edge from a cycle does not disconnect G.

That's because if you had any path that used the edge, you could instead use the remainder of the cycle to connect the same pair, so you can use that other path instead to connect u and v.