

MATHEMATICS FOR COMPUTER SCIENCE

LECTURE 1: Introduction & Proofs

What is a proof? A proof is a method for ascertaining the truth. There are many methods across society & science.

- Experimentation & observation
- Sampling & counterexamples
- Juries or judges
- Mathematical proof - a verification of a proposition by a chain of logical deductions from a set of axioms

Definition: A proposition is a statement which is either True or False

ex: $2+3=5$ natural numbers $\in \{0,1,2,\dots\}$

for all $\rightarrow \forall n \in \mathbb{N}, \underline{n^2 + n + 41 \text{ is prime}}$
a predicate proposition whose truth depends on the value of a variable

n	$n^2 + n + 41$	prime
0	41	✓
1	43	✓
2	47	✓
3	53	✓
$\vdots$		
20	461	✓

But this isn't necessarily true just because our examples all check out:

$n=41$ obviously fails

Ex. $a^4 + b^4 + c^4 = d^4$ has no positive integer solutions

Euler conjecture, disproved 28 years later.

$a = 95800$; $b = 217,619$; $c = 414,560$, $d = 432,481$

$\exists a, b, c, d \in \mathbb{N}$, $a^4 + b^4 + c^4 = d^4$ ← true!

Ex. $313(x^3 + y^3) = z^3$ has no positive integer solutions.

Fake, but smallest counterexample has more than 1000 digits

This equation is an elliptic curve, important in large integer factorisation & therefore cryptography

Ex. The regions of any map can be coloured in four colours such that adjacent regions have different colours. Many false proofs, brute forced by computer in the 70s.

Ex. Every positive even integer except 2 is the sum of two primes. Goldbach's conjecture; still unproven. Riemann hypothesis remains unproven

Ex. $\forall n \in \mathbb{Z}$, $n \geq 2 \Rightarrow n^2 \geq 4$

← implies

WHAT DOES "IMPLIES" MEAN?

An implication $p \Rightarrow q$ is true if p is F or q is T. Very awkward!

Ex. $\forall n \in \mathbb{Z} \quad n \geq 2 \iff n^2 \geq 4$ ^{if & only if} False!

Truth table

p	q	$p \Rightarrow q$	$p \iff q$
T	T	T	T
F	T	T	F
T	F	F	F
F	F	T	T

Axioms: A proposition assumed to be true. Our basic mathematical assumptions!

Ex If $a=b$ & $b=c$, $a=c$

Ex Euclidean geometry - given a line l & a point p not on l , there is exactly one line through $p \parallel l$

Spherical geometry - given a line l & a point p not on l , there is no line through $p \parallel l$

Hyperbolic geometry - given a line l & a point p not on l , there are infinitely many lines through $p \parallel l$

Each field is working off different axioms

Axioms should be

1. consistent
2. complete

A set of axioms is consistent if no statement can be proved both true & false

A set of axioms is complete if it can be used to prove that every proposition in the theory's language is decidable from the axioms.

Gödel's incompleteness proof shows that there is no set of axioms that is both consistent & complete which is strong enough to encode basic arithmetic

LECTURE 2: Induction

Direct proof: start with axioms, work through logic, find your way to destination

Indirect proof: alternate strategy

Proof by contradiction: assume the opposite of what you want to prove, work through it until you manage to derive a contradiction. If false = true, starting assumption is wrong!

if $\neg P \Rightarrow F$ is true
then $F \Rightarrow P$ true

Ex. Theorem: $\sqrt{2}$ is irrational

Proof (by contradiction):

① Assume that $\sqrt{2} = \frac{a}{b}$; fraction in lowest terms

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2 \Rightarrow a^2 \text{ is even} \Rightarrow a \text{ even } (2|a)$$

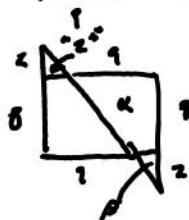
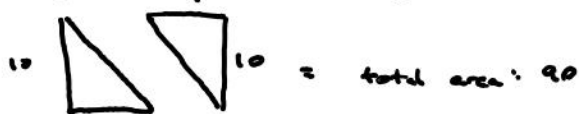
$$(4|a^2) \Rightarrow (4|2b^2) \Rightarrow (2|b^2) \Rightarrow b \text{ even}$$

$\therefore \frac{a}{b}$ is not a fraction in lowest terms

② False! $\sqrt{2}$ is not rational. QED

false

Ex. A _{naïve} proof that $90 > 92$. We take two triangles with total area 90 & divide them into four triangles with area greater than 90. By "conservation of area" axiom, $90 > 92$.



$$\Rightarrow \text{total area: } 2\alpha + 2\beta, 2\alpha = 8 \times (9 + 2^2)$$

$$2\alpha = 2 \times (2^2)$$

$$\therefore \text{total area} > 92 \text{ :P}$$

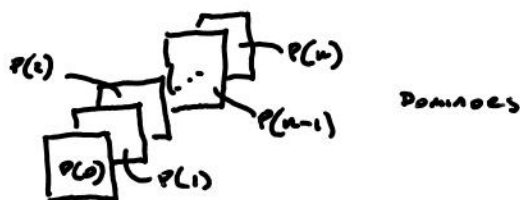
The trick here is " 2^2 " - if you did the math it would be i.e. then $10 \times 8 = 8 + 18 \times 2 = 90$ which is

fine

Don't draw pictures for proofs :>

Induction: The most powerful & commonly used proof technique in computer science.

Induction axiom: let $P(n)$ be a predicate. if $P(0)$ is true and $\forall n \in \mathbb{N} (P(n) \Rightarrow P(n+1))$ is true then $\forall n \in \mathbb{N} P(n)$ true
 i.e. if $P(0), P(0) \Rightarrow P(1), P(1) \Rightarrow P(2), \dots, P(n-1) \Rightarrow P(n)$ are true then $P(1), P(2) \dots P(n+1)$ are true



Theorem: $\forall n \geq 0 \quad 1+2+3+\dots+n = \frac{n(n+1)}{2}$

if $n=1 \quad 1+2+\dots+n=1$ (don't get caught out by notation)

if $n=0 \quad 1+2+\dots+n=0$

check $n=4 \Rightarrow 1+2+3+4=10, (4 \cdot 5)/2 = 10 \quad \checkmark$

Proof (by induction):

Let $P(n)$ be the proposition that $\sum_{i=1}^n i = \frac{n(n+1)}{2}$

Base case: $P(0)$ is true? $\sum_{i=1}^0 i = 0 = \frac{0(1)}{2} = 0 \quad \checkmark$

Inductive step: for $n \geq 0$, show $P(n) \Rightarrow P(n+1)$ is true

Assume $P(n)$ true for purposes of induction
 (i.e. assume $1+2+\dots+n = \frac{n(n+1)}{2}$)

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

$$\frac{n(n+1)}{2} + n+1 = \frac{(n^2+3n+2)}{2} = \frac{(n+1)(n+2)}{2} \quad \checkmark \quad QED$$

Induction didn't really help us understanding why the theorem was true. A proof of correctness, not of detail

Ex Theorem: $\forall n \in \mathbb{N} \quad 3 \mid (n^3 - n)$

Proof (by induction)

Let $P(n)$ be $3 \mid (n^3 - n)$

BASE CASE: $n=0$, $3 \mid (0-0)$ ✓

INDUCTIVE STEP: For $n \geq 0$, show $P(n) \Rightarrow P(n+1)$ is true

Assume $P(n)$: i.e. $3 \mid (n^3 - n)$

$$\text{EXAMINE } (n+1)^3 - (n+1) \Rightarrow n^3 + 3n^2 + 2n$$

use predicate: $\underbrace{n^3 - n}_{3 \mid \text{assumed by } P(n)} + \underbrace{3n^2 + 2n}_{\text{multiple of 3}}$

$$\therefore 3 \mid [(n+1)^3 - (n+1)]$$

Our base case doesn't have to be $P(0)$. Maybe it's

$P(b)$ is true. Then inductive step would be $\forall n \geq b$

$P(n) \Rightarrow P(n+1)$ & conclusion would be that $\forall n \geq b \quad P(n)$

Verify starting point & verify implications for n beyond that point

False Theorem: All horses are the same colour!

Proof by induction

$P(n)$: $n \geq 1$ any set of n horses, the horses are all the same color

Base case: $n=1$ for any set of one horse, horses of same color

Inductive step: Assume $P(n)$ to prove $P(n+1)$

Consider ^{any} set of $n+1$ horses $H_1, H_2, \dots, H_{n+1}$

$\underbrace{H_1, H_2, \dots, H_n}_{\text{same color}}$ & by symmetry $\underbrace{H_2, \dots, H_{n+1}}_{\text{same color}}$

since H_{n+1} has same color as H_1 , all horses in set share colour. QED $\Rightarrow$

$P(1) \Rightarrow P(2)$: $H_1, \dots, H_n$ is just H_1 } this is base case, not $n=1$
 $H_2, \dots, H_{n+1}$ is just H_2

H_n, H_2 is empty set!

$\therefore P(1) \not\Rightarrow P(2)$

Best example will use induction to show that there is a solution to a problem & also find that solution.

Ex: Courtyard 

need to tile courtyard
with -shaped tiles
possible for $n=2^1$.

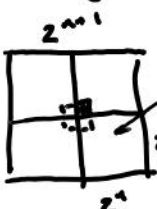
Theorem: for all n , there exists a way to tile a
 $2^n \times 2^n$ courtyard with a center square missing
using L-shaped tiles

Proof: $P(n)$ 

Base case: $P(0) \rightarrow$  1 missing tile $\checkmark$

Inductive step: For $n \geq 0$, assume $P(n)$ to prove $P(n+1)$

show $P(n+1)$ is true

$2^{n+1} \times 2^{n+1}$ courtyard - show that we can tile
new space 

inductive hypothesis can't be
used since no tile missing.
but... take a corner out of
each, fill w/ 1 tile, then
use ind. hypothesis... but
the static unit in the centre!

Go back to hypothesis!

Prove we can do it with any square

missing - this is true. Now we can do $n+2$
center by rotation. This makes $P(n)$ more
powerful!

General rule: if you're struggling, try a stronger hypothesis

Problem Set 1

i) Translate the following sentences from English to predicate logic. The domain you are working over is x , the set of people. You may use the function $S(x)$, meaning that " x has been a student of 6.042," $A(x)$, meaning that " x received an A in 6.042," $T(x)$, meaning they're a 6.042 TA, $E(x, y)$, meaning " x & y are the same person."

a) There are people who have taken 6.042 and have gotten As in 6.042.

$$\exists x \in X (S(x) \wedge A(x))$$

b) All people who are 6.042 TAs & have taken 6.042 received As,

$$\forall x \in X (S(x) \wedge T(x)) \Rightarrow A(x)$$

c) There are no people who are 6.042 TAs who did not receive As in 6.042

$$\nexists x \in X (T(x) \wedge \neg A(x))$$

d) There are at least three people who are TAs in 6.042 & have not taken 6.042

$$\exists x, y, z \in X (\neg E(x, y) \wedge \neg E(y, z) \wedge \neg E(z, x) \wedge T(x) \wedge T(y) \wedge T(z) \wedge \neg S(x) \wedge \neg S(y) \wedge \neg S(z))$$

2) Use a truth table to prove or disprove the following statements:

$$a) \neg(P \vee (Q \wedge R)) \stackrel{①}{=} (\neg P) \wedge (\neg Q \vee \neg R) \stackrel{②}{=}$$

using truth table below, column ① & ② identical;

so statement is TRUE

$$b) \neg(P \wedge (Q \vee R)) \stackrel{①}{=} \neg P \vee (\neg Q \vee \neg R) \stackrel{②}{=}$$

using truth table below, column ① & ② not

identical, so equality is FALSE

P	Q	R	①	②	③	④
T	T	T	F	F	F	F
T	F	T	F	F	F	T
T	T	F	F	F	F	T
F	T	T	F	F	T	T
F	F	T	T	T	T	T
F	T	F	T	T	T	T
T	F	F	F	F	T	T
F	F	F	T	T	T	T

3) The binary logical connectives $\wedge$ (and), $\vee$ (or), and $\Rightarrow$ (implies) appear often not just in computer programs but also ordinary speech. In chip design, however, it is often simpler to construct these from nand, which has the following

truth table:

P	Q	$P \nmid Q$
T	T	F
T	F	T
F	T	T
F	F	T

a) For each of the following expressions, find an equivalent expression using only nand $\nmid$ $\neg$ (not).

i) $A \wedge B \Rightarrow \neg \text{nand}(A, B)$

ii) $A \vee B \Rightarrow \text{nand}(\neg A, \neg B)$

iii) $A \Rightarrow B \Rightarrow \text{nand}(A, \neg B)$

b) It is actually possible to express each of the above using only nand without the $\neg$ operator. Find an equivalent expression for $\neg A$ using only nand $\nmid$ parentheses.

$\text{nand}(A, A)$ should cover it?

c) The constants true $\nmid$ false themselves may be expressed using only nand. Construct expressions ^{using nand} that always evaluate to true or false regardless of input A.

3) c) cont) True will always fire if we read $A \in \{T, F\}$

$\therefore T \rightarrow \text{nand}(A, \text{nand}(A, A))$

$F \rightarrow \text{nand}(T, T)$

4) You have 12 cans, one of which is false, and a balance scale. All real coins weigh the same; the false can is lighter. They are otherwise indistinguishable. Determine a strategy to identify the false can using at most 3 weighings.

WEIGHING 1: take four random cans & weigh against four random cans. If one side is lighter, we know can is in group. If equal, we know can is in unweighed group

WEIGHING 2: pick two random cans from the four we know to contain the false can. If one weighs less than the other, we've found the false can. Otherwise, weigh the two leftover cans

WEIGHING 3: we have two cans left, so we're guaranteed to find the false one here if we haven't already

- 5) Prove the following statement by proving its contrapositive:
if r is irrational, then $r^{1/5}$ is irrational.

Contrapositive: if r is rational, then $r^{1/5}$ is rational

$$r^{1/5} = a/b$$

$$(r^{1/5})^5 = a^5/b^5 ; a^5 \in \mathbb{N}, b^5 \in \mathbb{N}$$

$\therefore r$ can be expressed by integers, proving contrapositive statement, so original statement is also true

- 6) Suppose that $w^2 + x^2 + y^2 = z^2$, where $w, x, y, z \in \mathbb{N}^+$.

Prove the proposition that z is even if & only if w, x, y are even.

CASE 1: ALL EVEN: $(2i)^2 + (2j)^2 + (2k)^2 = (2l)^2$

$$\underbrace{4i^2 + 4j^2 + 4k^2}_{\text{even}} = \underbrace{4l^2}_{\text{even}} \quad \checkmark$$

by symmetry

CASE 2, 3, 4: ONE ODD: $(2i+1)^2 + 2j^2 + 2k^2 = z^2$

$$4i^2 + 4i + 1 + 4j^2 + 4k^2 = z^2$$

$$1 + \underbrace{4i^2 + 4i + 4j^2 + 4k^2}_{\text{even}} = z^2$$

by symmetry

$$1 + \text{even} = \text{odd} \therefore z^2 \text{ is odd}$$

CASE 5, 6, 7: TWO ODD: $4i^2 + 4j^2 + 4k^2 + 4i + 4j + 2 = z^2$

$$z = \sqrt{4 \left(\underbrace{i^2 + j^2 + k^2 + i + j}_{\text{integers}} + \frac{1}{2} \right)}$$

$\uparrow$ not an integer
 $\therefore$ whole group not int
or $1/2 \Rightarrow z$ can't be int

CASE 8: ALL ODD: As 234 but + 3 qed

LECTURE 3: Strong induction

A proof will have seven characteristics (ideally)

- correct
- brief
- in order!
- complete
- "elegant"
- clear
- well-organised (leaves like subroutines)

A good proof is like good code; we want to be able to prove our code works! see r.006 :). Obviously software bugs can be very bad! 1/3rd of published proofs are estimated to have flaws! Even the world's best mathematicians make mistakes

Proof "techniques" to avoid

- #10: Proof via kitchen sink
- #9: Proof via example ($n=2$ as general)
- #8: Proof via vigorous handwaving
- #7: Proof via cumbersome notation
- #6: Proof via exhaustion
- #5: Proof via omission: "the details may be easily supplied"
- #4: Proof via picture
- #3: Proof via vehement assertion
- #2: Proof via appeal to intuition
- #1: Proof via reference to authority

Fermat's Last Theorem:

$$\forall n > 2 \quad \neg \exists x, y, z \in \mathbb{N}^+ \\ x^n + y^n = z^n$$

"I have discovered a marvelous proof of this result that cannot fit in this margin."

Problem: Find a sequence of moves to go from ① to ②

①

A	B	C
D	E	F
H	G	

②

A	B	C
D	E	F
G	H	

Legal move: slide a letter into adjacent blank square.

(I assume there's a proof that this is unsolvable)

↑
correct! There is no sequence of legal moves to invert

G & H and also return other letters to original positions. ①

we use an invariant which holds at ① & every possible step, so that only steps which preserve the invariant are reachable

Two kinds of move: row & col. Row moves cannot change relative ordering of items! (Take this as Lemma 1).

Proof of Lemma 1: In row move, we move an item in cell i to empty adjacent cell $i-1$ or $i+1$. Nothing else moves.

Hence the order of the items is invariant.

Column moves:

change order: shifts

item by +2 or -2

so $(1, 2, 3) \rightarrow (2, 3, 1)$

column move changes

relative order of

precisely two pairs

of items $\leftarrow$ Lemma 2

A	B	C
D	F	
H	G	E

A	B	C
D	F	E
H	G	

HGB
↓
ENG

A	B	C
D		G
H	E	F

A		C
D	B	G
H	E	F

BCD
↓
CDB

Proof of Lemma 2: In a column move, we move an

item in cell i to a blank spot in cell $i-3$ or $i+3$.

when an item moves three positions, it changes relative order with items in $i-2, i-1$ or $i+1, i+2$.

Invariant: A pair of items L_1, L_2 form an inverted pair

if L_1 precedes L_2 in the alphabet but appears after L_2

in the puzzle. Lemma 2 says that during a move, the

number of inversions can only increase by 2, decrease by 2, _{count}

or remain the same. $\therefore$ parity of inversion, invariant on moves

Row move: no changes (Lemma 1)

Col move: A: both inverted pairs in order originally: Inv +2

B: both pairs inverted originally: Inv -2

C: one pair inverted, one not: Inv

Adding or subtracting 2 does not change parity. (Corollary 1)

In every configuration reachable from start state, the parity of number of inversions remains the same. Proof will be by induction (invariant proofs always by induction).

Proof (by induction):

$P(n)$: After any sequence of n moves, the parity of the number of inversions remains the same as starting point

Base Case: $n=0 \Rightarrow$ # inversions retains parity of starting state $\checkmark$

Inductive Step: For $n \geq 0$, $P(n) \Rightarrow P(n+1)$

Consider any sequence of $n+1$ moves $m_1, m_2, \dots, m_{n+1}$

By $P(n)$ we know parity after move m_n is same as starting state. By Corollary 1, m_{n+1} move cannot change parity of number of inversions.

$\therefore$ parity of number of inversions after m_{n+1} moves is same as n starting state $\therefore P(n) \Rightarrow P(n+1)$

We now have the tools to prove ①.

The parity of the number of inversions of the target state is even. By above, desired state cannot be reached from start state using legal moves, because starting parity of inversions is odd. QED

Use invariants to ensure you never reach undesirable or hazardous states.

STRONG INDUCTION AXIOM

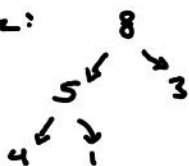
Let $P(n)$ be any predicate. If $P(0)$ is true $\wedge \forall n$

$(P(0) \wedge P(1) \wedge \dots \wedge P(n)) \Rightarrow P(n+1)$ is true, then $\forall n$ $P(n)$ is true.

Difference is the chain of implication - many more assumptions!

All strong induction proofs can be done with "standard" induction

Unstacking game:



pts: 15
+4

go until you have 8×1 stack
28 points available, that?

All strategies for an n -block game produce the same

score S_n . Ex $S_2 = 28 = \frac{n(n-1)}{2}$

Proof by strong induction

$P(n)$ all strategies of n -block game produce score $\frac{n(n-1)}{2}$

Base Case: $n=1$ $S(1) = 0$

Inductive Step: Assume $P(1) \wedge P(2) \wedge \dots \wedge P(n) \Rightarrow P(n+1)$

look at $n+1$ blocks $\overset{n+1}{k} \quad n+1-k \Rightarrow$ score is $(n+1-k)k$
+ $P(k) + P(n+1-k)$

expand score: $(2k + 2k + 2k^2 + k^2 - k \cdot (n+1) - k - k - k - k + k^2) / 2$

ALL THE k 's CANCEL! $n(n+1)/2 = S_{n+1}$

Problem Set #2

1) Define a 3-chain to be a (not necessarily contiguous) subsequence of three integers, which is either monotonically increasing or decreasing. We will show here that any sequence of five distinct integers will contain a three-chain. Write the sequence as a_1, a_2, a_3, a_4, a_5 . Note that a monotonically increasing sequence is one in which each term is greater than or equal to the previous term. Decreasing subsequences are similar. Finally, a subsequence is a sequence derived from the original by deleting some elements without otherwise reordering.

a) Assume that $a_1 < a_2$. Show that if there is no three chain in our sequence, then a_3 must be less than a_1 .

$a_2 > a_3$ or immediately there is a 3-chain

$a_4 > a_3$ or immediately 3-chain

$\therefore$ if $a_3 > a_1$, 3-chain of $a_1 < a_3 < a_4$

$\therefore a_3 > a_1$ or 3-chain guaranteed

b) Show that if $a_1 < a_2$ & there is no 3-chain in our sequence, then $a_3 < a_4 < a_2$

if $a_4 > a_2$, $a_1 < a_2 < a_4$ immediately is 3-chain

if $a_4 > a_3$, $a_1 > a_3 > a_4$ "

1 cont) c) Assuming $a_1 < a_2$ & $a_3 < a_4 < a_2$, show that any value of a_5 must result in a 3-chain

option 1: $a_5 > a_4$: $a_1 < a_2 > \overbrace{a_3 < a_4}^{\text{3-chain}} < a_5$

option 2: $a_5 < a_4$: $a_1 < a_2 > \overbrace{a_3 < a_4}^{\text{3-chain}} > a_5$
3-chain since $a_2 > a_4$

d) Using the previous parts, prove by contradiction that any sequence of five distinct integers must contain a 3-chain

Proof: Assume some sequence S does not contain a 3-chain

- if $a_1 < a_2$, previous work shows S must contain a 3-chain

- if $a_1 > a_2$, set $S' = \{a_1, a_2, a_3, a_4, a_5\}$

$\neq$ 3-chain in $S' \neq$ 3-chain in S

in S' , a_1 now $< a_2$; guaranteed a 3-chain

$\therefore$ 3-chain guaranteed for all sequences

2) Prove by either the Well Ordering Principle or induction that for all nonnegative integers, n :

$$\textcircled{1} \sum_{i=0}^n i^3 = \left(\frac{n(n+1)}{2} \right)^2$$

$$P(n) = \textcircled{1}$$

$$\text{Base Case: } n=0 \Rightarrow 0^3 = \left(\frac{0(1)}{2} \right)^2 \quad \checkmark$$

2 cont) Show $P(n) \Rightarrow P(n+1)$

$$\begin{aligned}
 \sum_{i=0}^{n+1} i^3 &= \sum_{i=0}^n i^3 + (n+1)^3 \\
 &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \\
 &= \frac{n^2(n+1)^2 + 4(n+1)^3}{4} \\
 &= \frac{n^2(n+1)^2 + 4(n+1)(n+1)^2}{4} \\
 &= \frac{(n+1)^2(n^2 + 4(n+1))}{4} \\
 &= \frac{(n+1)^2(n+2)^2}{4} \\
 &= \left(\frac{(n+1)(n+2)}{2}\right)^2
 \end{aligned}$$

$\therefore$ true for all positive n by induction

3) The following problem is fairly tough until you hear a certain one-word clue. The solution is elegant but tricky. During C.O.R, the students are sitting in an $n \times n$ grid. A sudden outbreak of beaver flu causes some students to get infected. Here is an example where $n=6$ & infected students are marked "x"

x				x	
	x				
		x	x		
		x			
			x		x

Now the infection begins to spread every minute, in discrete time-steps. Two students are considered adjacent if they share an edge; each student is adjacent to 2, 3, or 4 others. A student is infected in $t+1$ if either

- They were already infected OR
- They're adjacent to 2+ infected students

3 cont) in the example, the infection spreads as below:

x				x	
	x				
		x	x		
		x			
			x		x

=>

x	x			x	
x	x	x			
	x	x	x		
		x			
		x	x		
		x	x	x	x

=>

x	x	x		x	
x	x	x	x		
	x	x	x		
	x	x	x		
		x	x	x	
		x	x	x	x

In this example, over the next few time-steps all the students in the class become infected.

Theorem: if fewer than n students are initially infected, the whole class will never be completely infected.

The invariant is the infection perimeter. If this is truly invariant, we can show we need n or more initial infections to cover whole board by

$$P_{\text{TARGET}} = 4n \quad P_{\text{I MAX}} = i \cdot 4$$

if $i < n$, $(n-1) \cdot 4 = 4n-4 < P_{\text{TARGET}} \therefore$ Target unreachable

Next step is to show via induction that the infection perimeter is invariant.

3 cont) Let I_0 be initial infection perimeter

$P(t)$ is the proposition that after t steps $I_t \leq I_0$.

Base case: $P(0) \Rightarrow I_0 \leq I_0$ by definition ✓

Inductive step: $P(t) \Rightarrow I_t \leq I_0$

$$P(t+1) \Rightarrow \underbrace{I_{t+1}}_{\text{show this}} \leq I_t$$

I_{t+1} only changes with infections. For each infected square, I_{t+1} can grow by at most 2. But in that case, it decreases by 2 simultaneously. $\therefore I_{t+1} \leq I_t$

$\therefore$ Theorem is proved

4) Find the flaw in the following bogus proof that $a^n = 1$ for all nonnegative integers n , whenever a is a nonzero real number.

Proof: (by induction) $P(n): \forall k \leq n; a^k = 1$ where k is a nonnegative integer

Base Case: $a^0 = 1$ ✓

Inductive step: $a^k = 1$ for all $k \in \mathbb{N}$ such that $k \leq n$

$$\text{Then } a^{n+1} = \frac{a^n a^1}{a^{n+1}} = \frac{1 \cdot 1}{1} = 1$$

$\therefore P(n+1)$ holds

Flaw: take $n=1$. Then $n-1$ is not a nonnegative integer, and the inductive step no longer holds

LECTURE 4: NUMBER THEORY I

Number theory: study of integers $0, 1, 2, 3, \dots$

Extremely important in cryptography

Def: $m \mid a$ (m divides a)

iff $\exists k$ such that $a = k \cdot m$

$a = 0 = 0 \cdot m \therefore m \mid 0$ for all m

Suppose we have an a -gallon jug & a b -gallon jug,
with $a = 3$ & $b = 5$

① If $m \mid a$ & $m \mid b$, then $m \mid$ any result we can get by manipulating the jugs

State machine: States - pairs (x, y) , where

$x = \#$ gallons in a -jug; $y = \#$ gallons in b -jug

Starting state: $(0, 0)$

Transitions: Fill jug, empty jug, pour one jug into another

$$\begin{array}{ccc} \Downarrow & \Downarrow & \Downarrow \\ x, y \rightarrow a, y & x, y \rightarrow 0, y & x, y \rightarrow \begin{cases} 0, x+y; & x+y \leq b \\ x+y-b, b; & \text{else} \end{cases} \\ x, y \rightarrow x, b & x, y \rightarrow y, 0 & \end{array}$$

$$x, y \rightarrow \begin{cases} x-y, 0; & x+y \leq a \\ a, x-y-a; & \text{else} \end{cases}$$

① We can show this using induction

& invariance on the above states.

$a = 3, b = 5 \quad (0, 0) \rightarrow (0, 5) \rightarrow (3, 2) \rightarrow (0, 2) \rightarrow (2, 0) -$
 $\rightarrow (2, 5) \rightarrow (3, 4)$

get four
gallons in b

Show by induction: Assume $m|a$, $m|b$

Invariant: $P(n) =$ "if (x, y) is the state after n transitions,
then $m|x \wedge m|y$ "

Base case: $(0, 0) \in m|0$ in all cases; $P(0)$ is true $\checkmark$

Inductive step: Show $P(n) \Rightarrow P(n+1)$

(x_n, y_n) is the state after n transitions
 $\therefore m|x_n \wedge m|y_n$ are assumed

After another transition x_{n+1} can be ...

$\{0, a, x_n, y_n, x_n - y_n - b, x_n + y_n\} \in y_{n+1}$ can be ...

$\{0, b, y_n, x_n, y_n - x_n - a, y_n + x_n\}$

$x_{n+1} \wedge y_{n+1} = \{0, a, b, x_n, y_n, x_n + y_n, x_n - y_n - b, y_n - x_n - a\}$
 $m|0, m|a, m|b, m|x_n, m|y_n$

everything in $x_{n+1} \wedge y_{n+1}$ is a linear combination
of $m \Rightarrow m|x_{n+1} \wedge y_{n+1}$

$\therefore P(n) \Rightarrow P(n+1)$ QED

using this result

Problem, $a=28 \nmid b=55$ - can we get 4 gallons out? no;

$m=4$

Def: GCD of (a, b) is the greatest common divisor of $a \wedge b$

$a=3, b=5, \rightarrow \gcd(3, 5) = 1$

$\gcd(44, 52) = 4$

Def: Relatively prime numbers are pairs (a, b) with $\text{GCD}(a, b) = 1$

Assertion: any linear combination $L = sa + tb$ of $a \in \mathbb{Z}$ with $0 \leq L \leq b$; $a \leq b$ can be reached.

Ex: $4 = (-2)3 + 2 \cdot 5 \therefore 4$ can be reached (already seen)

But we ideally want s positive! $\frac{s'}{3} \cdot 3 - 1 \cdot 5 = 4$

Show: Notice we can rewrite $L = sa + tb = (s + mb)a + (t - ma)b$

So $\exists s', t'$ such that $L = s'a + t'b$ with $s' > 0$

Assume $0 < L < b$

Algorithm: To obtain L gallons, repeat s' times the following:

- Fill the a -jug
- Pour the a -jug into the b -jug
- When b -jug becomes full, empty it & continue pouring until a -jug empty.

First loop: $(0, 0) \rightarrow (3, 0) \rightarrow (0, 3)$

Second: $(0, 3) \rightarrow (3, 3) \rightarrow (1, 5) \rightarrow (1, 0) \rightarrow (0, 1)$

Third: $(0, 1) \rightarrow (3, 1) \rightarrow (0, 4)$

We've filled the a -gallon jug s' times

Suppose b -jug has been emptied n times

Let r be the remainder in the b -jug

$$0 \leq r \leq b; 0 \leq L \leq b \quad r = s'a - u \cdot b$$

$L = s'a + t'b$; we want to express r in L

$$r = \underbrace{s'a + t'b}_L - t'b - ub = L + b(\underbrace{t' - u}_{\text{must be zero to fit in bounds}})$$

$\therefore t' = -u \quad \therefore r = s'a + t'b = L$; the algorithm can reach any linear combination L .

$$\begin{matrix} \nwarrow s' & \swarrow t' \\ 1 = 2 \cdot 3 - 1 \cdot 5 \end{matrix} \Rightarrow \text{any number of gallons can be reached}$$

Euclid's Algorithm

for any $b \nmid a$, there exists a unique q ^{quotient} $\nmid$ r ^{remainder $\text{rem}(b,a)$} such that
 $b = q \cdot a + r$ with the property that $0 \leq r < a$

① Lemma: $\gcd(a, b) = \gcd(\text{rem}(b, a), a)$

$$\gcd(105, 224) = \gcd(\text{rem}(224, 105), 105)$$

$$= \gcd(14, 105)$$

$$= \gcd(\text{rem}(105, 14), 14)$$

$$= \gcd(\underbrace{\text{rem}(105, 14)}_{14 \cdot 7 = 98}, 14) = \gcd(7, 14) = 7$$

Show ①: suppose $m \mid a \nmid b$, then $m \mid (b - q \cdot a = \text{rem}(b, a))$

this shows $\gcd(a, b) \leq \gcd(\text{rem}(b, a), a)$

get lower bound If $\text{rem}(b, a) \neq 0$, then $[m \mid a \wedge m \mid b] \Rightarrow$

$$[m \mid \text{rem}(b, a) = (b - qa)]$$

else, $b - qa = 0$, $m \mid 0$; $b = qa$, $m \mid a \Rightarrow m \mid b$

$\gcd(a, b)$ is a linear combination of a & b

Show with induction/invariant

$P(n)$: if Euclid's algorithm reaches $\gcd(x, y)$ after n steps, both x & y are linear combinations of a & b ;
 $\gcd(a, b) = \gcd(r, y)$

Base case: @ 0 steps $x=a, y=b$; all conditions hold
by inspection ✓

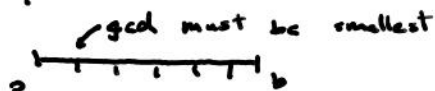
Inductive step: Assume $P(n)$; show $P(n) \Rightarrow P(n+1)$

Notice $\exists q, r \text{ s.t. } r = y - qx \rightarrow$ linear combination of a & b
Euclid's Lemma shows r case

$$\therefore P(n) \Rightarrow P(n+1)$$

Final step: $\gcd(0, y) = y$

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



LECTURE 5: Number Theory II

- Encryption
- Modular Arithmetic
- Euler's totient function
- RSA

Encryption: beforehand, keys are exchanged between receiver & sender. Encryption is an algorithm which transforms messages using these keys. $m' = E_{\text{keys}}(m)$

Decryption: reversing m' back into plaintext. $m = D_{\text{keys}}(m')$
Agents intercepting m' should not be able to extract any information from these messages. Use of number theory for encryption proposed by Alan Turing.

Turing's Code V1

"victory"
↓↓↓ ↘ ← changes m into a prime number
 $m = 220103...2513$

Easy to force m & prove n is prime

Beforehand exchange secret prime k . Enc: $m' = mk$

Dec: $m = \frac{m'}{k}$

m' is the product of two very large primes. It's hard to factor the product of two large primes.

Problem: attacker has m'_1 & $m'_2 \Rightarrow m, k, m_2 k$.

find k by $\text{gcd}(m'_1, m'_2) = k \leftarrow \text{Euclid's algorithm}$

$\therefore V_1$ not secure

Turing's Code V2

Beforehand: exchange a public prime p & a secret prime k . Encryption: message as a number $m \in \{0, 1, \dots, p-1\}$
 $m' = \text{rem}(mk, p) \Rightarrow m = ? \leftarrow \text{need modular arithmetic}$

Hard to factor product of two large primes

a, b relatively prime iff $\gcd(a, b) = 1$ iff $\exists s, t$ s.t. $s \cdot a + t \cdot b = 1$

$$s \cdot a = 1 - t \cdot b \Rightarrow s \cdot a \equiv 1 \pmod{b}$$

① $\xrightarrow[\text{not approx}]{\text{sort of F.}}$ $s \approx 1/a$

x is "congruent" to y mod-to n : $x \equiv y \pmod{n}$ iff $n \mid (x - y)$

Ex: $31 \equiv 16 \pmod{5}$,

← reflexive, symmetric; transitive

The multiplicative inverse of x mod n is a number x^{-1} in $\{0, 1, \dots, n-1\}$ such that $x x^{-1} \equiv 1 \pmod{n}$.

$$\text{Ex: } 2 \cdot 3 \equiv 1 \pmod{5}$$

$$2 \equiv 3^{-1} \pmod{5} \Rightarrow 3 \equiv 2^{-1} \pmod{5}$$

$$5 \cdot 5 \equiv 1 \pmod{6} \Rightarrow 5 \equiv 5^{-1} \pmod{6} \leftarrow 5 \text{ is its own mult. inverse in mod 6.}$$

$$\underbrace{\text{rem}(mk, p)}_{m'} \equiv mk \pmod{p} \text{ or}$$

we can use this to think about the encryption problem

$$\text{If } \underbrace{k \cdot k^{-1}} \equiv 1 \pmod{p} \Rightarrow m' k^{-1} = mk \cdot k^{-1} \equiv m \pmod{p}$$

i.e. if we have a mult. inverse; not always the case!

since $m \in \{0, \dots, p-1\}$, $m = \text{rem}(m' k^{-1}, p)$ ← decryption for

Attack: if we know an example of plaintext m ^{Turing v2!}

if an encryption of the same message $m' = \text{rem}(mk, p)$

$$m' \equiv m \cdot k \pmod{p} \quad \text{known}$$

$\gcd(m, p) = 1$; use ① to compute mult. inverse such that

$$m m^{-1} \equiv 1 \pmod{p}$$

$$m' m^{-1} \equiv k m m^{-1} \equiv k \pmod{p}$$

compute $k' \pmod{p}$; all future messages are decryptable
 so we need to go much deeper to make more secure encryption schemes.

Euler's Totient Function

ϕ_n denotes the number of integers in $\{1, 2, 3, \dots, n-1\}$ that are relatively prime to n .

$$\text{Ex: } n=12: \underline{1}, \underline{2}, 3, 4, \underline{5}, 6, \underline{7}, 8, 9, 10, \underline{11}, 12 \quad \phi(12)=4$$

$$n=15: \underline{1}, \underline{2}, 3, \underline{4}, 5, 6, \underline{7}, 8, 9, 10, \underline{11}, \underline{12}, \underline{13}, \underline{14}, 15 \quad \phi(15)=8$$

$$\text{Compute } \phi(n) \text{ by: } \phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

where $p_1, p_2, \dots, p_k$ are distinct prime factors of n

$$\text{Ex } \phi(12) = 12 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 4$$

Euler's Theorem: if $\gcd(n, k) = 1$, then $k^{\phi_n} \equiv 1 \pmod{n}$

① Lemma: if $\gcd(n, k) = 1$, then $a \cdot k \equiv b \cdot k \pmod{n} \Rightarrow a \equiv b \pmod{n}$

② Lemma: $\gcd(n, k) = 1$, iff k has a multiplicative inverse

③ pf: $\gcd(n, k) = 1$ iff $\exists_{r,s} ns + kt = 1 \Leftrightarrow \exists_{+} n \mid (kt - 1) \Leftrightarrow kt \equiv 1 \pmod{n}$

④ Lemma: suppose the $\gcd(n, k) = 1$. Let $k_1, \dots, k_r$ in $\{1, 2, \dots, n-1\}$

denote integers relatively prime to n ($r = \phi(n)$).

$$\text{Then } \underbrace{\{\text{rem}(k_1, n), \dots, \text{rem}(k_r, n)\}}_{\neq r} = \underbrace{\{k_1, \dots, k_r\}}_{\subseteq}$$

$\neq r$

$\subseteq$ ← but if subset lengths are same, equal

③

$$\text{Pf: } \text{rem}(k_i, k, n) = \text{rem}(k_j, k, n)$$

show only possible if $k_i = k_j \leftarrow$ then we have exactly r remainders
 $k_i k \equiv k_j k \pmod{n}$

$$\Rightarrow \text{Lemma ① } k_i \equiv k_j \pmod{n}$$

$$\Rightarrow k_i = k_j \text{ because } k_i, k_j \in \{0, \dots, n-1\}; \underbrace{n \mid (k_i - k_j)}_{\text{only possible if this term is 0}}$$

$\therefore$ exactly r remainder terms in $\{\text{rem}(k_1, k, n), \dots, \text{rem}(k_r, k, n)\}$

$$\text{then } \gcd(n, \underbrace{\text{rem}(k_i, k, n)}_{k_i k - an}) = \gcd(n, k_i k) =$$

$k_i k - an$ from Euclid's algorithm work

$$\gcd(n, k) = 1, \gcd(n, k_i) = 1 \leftarrow \text{no common divisor}$$

$\therefore \text{rem}(k_i, k, n)$ relatively prime to n ; must be $\in \{k_1, \dots, k_r\}$

since $\{\text{rem}(k_1, k, n), \dots, \text{rem}(k_r, k, n)\} \subseteq \{k_1, \dots, k_r\}$

$\hat{=}$ r terms in $\{\text{rem}(k_1, k, n), \dots, \text{rem}(k_r, k, n)\}$

$$\{\text{rem}(k_1, k, n), \dots, \text{rem}(k_r, k, n)\} = \{k_1, \dots, k_r\} \quad \checkmark$$

Proof of Euler's Theorem -

$$\underbrace{k_1 \cdot \dots \cdot k_r}_{\text{product rel. prime to } n} = \text{rem}(k_1, k, n) \cdot \dots \cdot \text{rem}(k_r, k, n)$$

$$\hat{=} k_1 k \cdot k_2 k \cdot \dots \cdot k_r k \pmod{n}$$

$$\therefore \text{has mult. inverse} \quad \hat{=} k_1 k_2 \dots k_r \cdot k^r \pmod{n}$$

$$1 = k^r \pmod{n}, \quad r = \phi(n) \quad \square \Rightarrow$$

Fermat's Little Theorem: Suppose p is prime and $k \in \{1, \dots, p-1\}$

$$\text{Then } k^{p-1} \equiv 1 \pmod{p}$$

Proof: $\{1, 2, \dots, p-1\}$ relatively prime to p because p prime;

$$k^{\phi(p)} \equiv 1 \pmod{p}; \phi(p) = p-1$$

$$k^{p-1} \equiv 1 \pmod{p}$$

$$k \cdot k^{p-2} = k^{p-1} \equiv 1 \pmod{p}$$

$$\therefore k^{p-2} \equiv k^{-1} \pmod{p}$$

receiver

RSA: Beforehand, n generates public key e ; secret key

1. generate two distinct large primes p & q

2. let $n = pq$

3. select e such that $\gcd(e, (p-1)(q-1)) = 1$

$\Rightarrow$ public key is the pair (e, n)

4. compute d such that $d \cdot e \equiv 1 \pmod{(p-1)(q-1)}$

$\Rightarrow$ secret key is pair (d, n)

Encryption: $m' = \text{rem}(m^e, n)$

Decryption: $m = \text{rem}((m')^d, n)$

Proof: $m' = \text{rem}(m^e, n) \equiv m^e \pmod{n} \Rightarrow (m')^d \equiv m^{ed} \pmod{n}$

by ③ $\exists e, d = 1 + r(p-1)(q-1)$

$$\text{So, } (m')^d \equiv m^{ed} \equiv m m^{r(p-1)(q-1)} \pmod{n}; n = pq$$

if $m \not\equiv 0 \pmod{p}$, apply F.L.T. $\Rightarrow m^{p-1} \equiv 1 \pmod{p}$ [& similar]

$$(m')^d \equiv m m^{r(p-1)(q-1)} \pmod{p} \quad [\& \text{ similar }]$$

$$\text{So, } (m')^d \equiv m \pmod{p} \Rightarrow p \mid (m')^d - m; q \mid (m')^d - m; pq \mid (m')^d - m$$

$$(m')^d \equiv m \pmod{n} \Rightarrow m = \text{rem}((m')^d, n) \quad \checkmark$$

Problem Set 3

1) a) Use the Pulveriser to find integers s, t such that

$$135s + 59t = \gcd(135, 59)$$

$$\text{rem}(135, 59) = 17 = 135 - 2 \cdot 59$$

$$\text{rem}(59, 17) = 8 = 59 - 3 \cdot (135 - 2 \cdot 59)$$

$$\text{rem}(17, 8) = 1 = (135 - 2 \cdot 59) - 2(59 - 3(135 - 2 \cdot 59))$$

$$= 7 \cdot 135 - 16 \cdot 59$$

$$\therefore s = 7, t = -16$$

b) Use the previous part to find the inverse of $59 \bmod 135$ in the range $\{1, \dots, 134\}$

$$1 \equiv -16 \cdot 59 \pmod{135}, \text{ but } -16 \notin \{1, \dots, 134\}$$

$$\text{rem}(-16, 135) = 119$$

c) Use Euler's theorem to find the inverse of $17 \bmod 31$ in the range $\{1, \dots, 30\}$.

$$31 \text{ is prime, so } 17^{30} \equiv 1 \pmod{31}$$

$$17^{29} 17^{-1} \Rightarrow \text{rem}(17^{29}, 31) = 17^{-1}$$

i don't know how to compute this

d) Find the remainder of 34^{82248} divided by 83

$$34 \not\equiv 0 \pmod{83} \Rightarrow 34^{\phi(83)} \equiv 1 \pmod{83} \quad 82248/82 = 1003 \text{ rem } 2$$

$$\therefore 34^{82248} = 34^2 \cdot 34^{1003 \cdot 82} \equiv 34^2 \cdot 1 \pmod{83}$$

$$\equiv 77 \pmod{83}$$

2) prove the following statements, assuming all numbers are positive integers.

a) if $a|b$ then $\forall c, a|bc$

$$b = ak \quad \leftarrow \text{some positive integer}$$

$$\therefore bc = akc; \quad a|akc \quad \checkmark$$

b) if $a|b$ and $a|c$, then $a|sb+tc$

$$b = ak_1, \quad c = ak_2 \quad a|sak_1 + tak_2 \Rightarrow a|a(sk_1 + tk_2) \quad \checkmark$$

c) $\forall c, a|b \iff ca|cb$

This is just true by linearity?

d) $\gcd(ka, kb) = k \cdot \gcd(a, b)$

$ka + kb$ can reach $\gcd(ka, kb)$ with some linear

combo $s \cdot ka + t \cdot kb$. $k(sa + tb) = \gcd(ka, kb)$. then

$sa + tb = \gcd(a, b)$ by assuming $sa + tb \neq \gcd(a, b)$;

proving by contradiction. Then $ua + vb = \gcd(a, b)$;

$$0 < u(ka) + v(kb) < s(ka) + t(kb) \therefore ua + vb \text{ is not } \underline{\text{greatest}}$$

$$\text{Then } k(\gcd(a, b)) = \gcd(ka, kb) \quad \checkmark$$

3) In this problem, we investigate numbers which are squares modulo a prime number p .

a) An integer n is a square modulo p if there exists another integer x such that $n \equiv x^2 \pmod{p}$. Prove that

$$x^2 \equiv y^2 \pmod{p} \text{ iff } x \equiv y \pmod{p} \text{ or } x \equiv -y \pmod{p}$$

3) a) cont) $x^2 \equiv y^2 \pmod{p}$ iff $p \mid x^2 - y^2 \Rightarrow p \mid (x-y)(x+y)$

since p prime; $p \mid x-y \parallel p \mid x+y$ ✓

b) There is a simple test we can perform to see if a number is square modulo p . It states that:

Theorem 1: Euler's Criterion

1. If n is a square modulo p then $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

2. If n is not a square modulo p then $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Prove the first part

$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ if n is a square modulo p

$\therefore x^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem

c) Assume that $p \equiv 3 \pmod{4}$ and $n \equiv x^2 \pmod{p}$. Given $n \not\equiv 0 \pmod{p}$, find one possible value of x

$n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ since $p = 4k+3 \Rightarrow \frac{p-1}{2} = 2k+1$

$n^{2k+1} \equiv 1 \pmod{p}$

$(n^{2k+1})^2 \equiv 1 \pmod{p} \Rightarrow x^2 \equiv n \pmod{p} \Rightarrow x = n^{\frac{p+1}{4}}$

4) Prove that for any prime p , $\forall$ integer $k \geq 1$: $\phi(p^k) = p^k - p^{k-1}$

There are p^{k-1} numbers between 0 and p^k-1 that are divisible by $p \rightarrow$ every such number takes the form sp $\therefore$ there are p^{k-1} possible values of s in the interval. Then: $\phi(p^k) = p^k - p^{k-1}$ since it's counting numbers not divisible by p .

LECTURE 6: GRAPH THEORY & COLOURING

Graph theory - scheduling, communication, Google page rank

Claim (U. Chicago): on average, American men have 74%

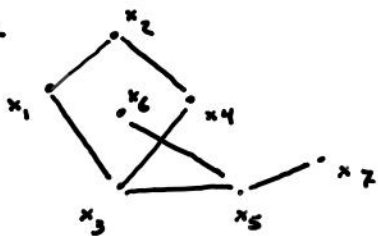
more opposite-gender partners than women

Claim (ABC News): on average, American men have 238%

more opposite-gender partners than women

These claims can actually be handled with graph theory rather than pure polling

Graph



Definition: a graph G is a

pair of sets (V, E) , where

V is a non-empty set of items

called "vertices" or "nodes" & E is a

set of two-item subsets of V

called "edges"

$$V = \{x_1, \dots, x_7\}$$

$$E = \{\{x_1, x_2\}, \dots, \{x_5, x_7\}\}$$

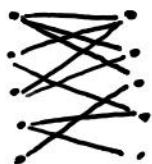
$$E_x: \begin{matrix} & x_1 & \\ x_2 & & x_3 \end{matrix} \quad G = (V, E), \quad V = \{x_1, x_2, x_3\}, \quad E = \emptyset$$

A graph with three vertices & no edges

For a graph with edges two nodes are adjacent if they're connected by edges: $\{x_i, x_j\} \in E$. An edge $E_i = \{x_i, x_j\}$ is said to be incident to its endpoints x_i & x_j . The degree of a node is the number of edges incident to that node.

A graph is simple if it has no loops or multiple edges between the same nodes. "Loops" here means an edge which connects one node to itself.

Back to "opposite partner" problem. Take nodes as people: Men Women $|V| \approx 300$ million



$$|V_m| \approx 147.6 \text{ million}$$

$$|V_w| \approx 152.4 \text{ million}$$

$\therefore$ graph is slightly unbalanced towards right side.

$$|E| = ??$$

Let A_m = average number of opposite-gender partners for men

$$A_w =$$

"

women

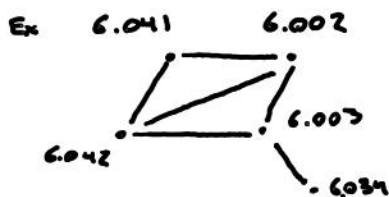
What is A_m/A_w ? U Chicago say 1.74. ABC News say 2.33

$$\text{But we can work out directly: } A_m = \frac{\sum_{v \in V_m} \deg(v)}{|V_m|} = |E|/|V_m|$$

$$A_w = |E|/|V_w|$$

$$\therefore A_m/A_w = |V_w|/|V_m|$$

$$= \underline{1.0325}$$



Classes/student overlap

Even Slots

w: 5-7

w: 7-9

w: 9-11

v: 11-1

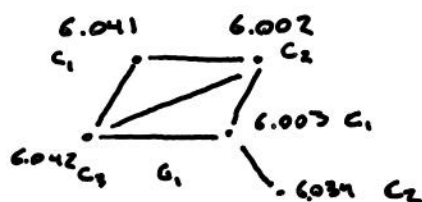
v: 1-3

} assign slots to nodes

The scheduling problem is an example of a graph colouring problem. Given a graph G & k colours, assign a colour to each node so that adjacent nodes all get different colours. The minimum value of k for which such a colouring exists is called the chromatic number of G : $\chi(G)$

Let's call our slots $\{c_1, \dots, c_5\}$

No fast algorithm for determining a chromatic number - np complete!



Basic Graph-Colouring Algorithm

1. Order the nodes from $v_1, v_2, \dots, v_n$ ← this choice matters!
2. Order the colours $c_1, c_2, \dots$
3. Process nodes from $i = 1, 2, \dots, n$

Assign lowest legal color

This is a greedy algorithm.

Theorem: if every node in graph G has degree $\leq d$, basic algorithm uses at most $d+1$ colours. (in G , $d=3$)

Proof by induction: (try to induct on nodes or edges)

$P(n)$: if every node in an n -node graph G has degree $\leq d$, basic algorithm uses at most $d+1$ colours

Base case: G_1 : 1-node graph uses $d+1$ colours

Inductive step: n -node graph w/ degree $\leq d$ uses $d+1$ colours. $\{v_1, \dots, v_n\}$

$$\{v_1, \dots, v_n, v_{n+1}\}$$

inductive step (cont): new node is adjacent to at most



d other nodes, with at most d colours;

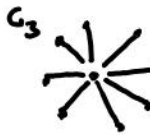
$\exists c \in \{c_1, \dots, c_{d+1}\}$ available for node $n+1$

$\therefore$ Basic algorithm uses at most $d+1$ colours
for graph of degree d . $\therefore$



$$\chi(G_2) = 2!$$

$$BGA = 2$$

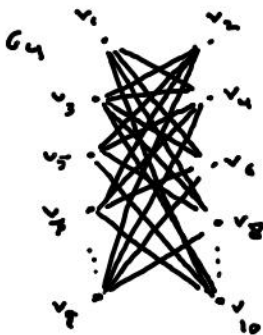


$$\chi(G_3) = 2!$$

$$BGA = 2$$

algorithm does better than bound here

and here



what about here?

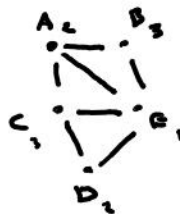
two pieces $\chi(G) = 2$
this ordering of G_4 (a bipartite graph) results
in $n/2$ colours after BGA applied!

Ex:

overlapping
radio towers
can't use same
frequency



$\Rightarrow$



$$\chi(G) = 3$$

LECTURE 7: Matching Problems

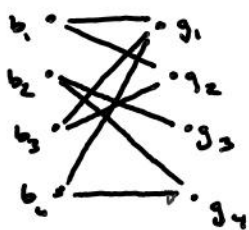
Def: Given graph $G=(V,E)$ a matching is a subgraph of G where every node has degree 1.



$\{x_1-x_6, x_2-x_5\}$ is a matching of size 2

This graph also supports matching of size 3, but not 4.

Def: A matching is perfect if it has size $|V|/2$.

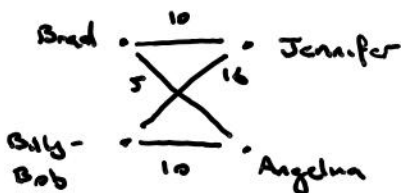


$\{b_1-g_1, b_2-g_3, b_3-g_2, b_4-g_4\}$ is a perfect matching.

In general we might prefer some matchings over others; we can represent this with weights.

Def: The weight of a matching M is the sum of the weights on the edges of M .

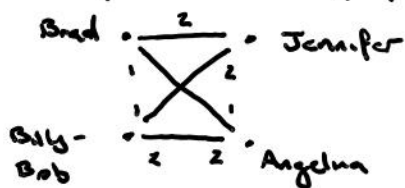
Def: A min-weight matching for graph G is a perfect matching for G that has the lowest weight of all perfect matchings.



ms: Brod-Jennifer (10)

Billy-Bob-Angelina $\frac{(10)}{20}$

We'll look at a version of the problem with preferred orders rather than weights.

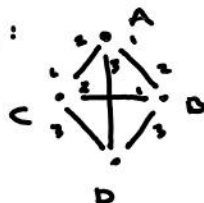


Def: Given a matching M ,

u, v form a rogue couple if they prefer each other over their pairing in M . creates instability. A matching is stable if there aren't any rogue couples. (we treat preferences as fixed over time)

Goal: Find a perfect matching that is stable.

For bipartite graphs always possible to create stable matching. For non-bipartite graph G :

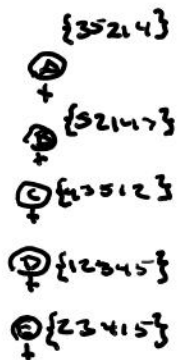
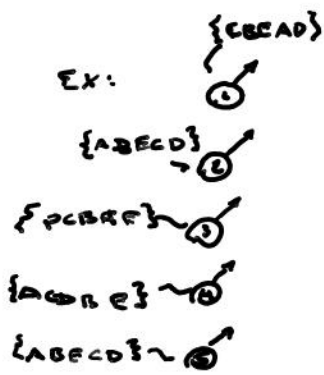


Theorem: $\nexists$ a stable matching for G

Proof (by contradiction). Assume $\exists M$.

Then D matched with some node. Wlog (by symmetry), assume $D-A$. But then A is C 's preferred choice over B & C is A 's preferred choice over D . $\therefore A-C$ is a rogue couple, and M is unstable. QED.

Stable Marriage Problem: N boys & N girls; each girl has a ranked preference list of all boys & vice versa. List is complete, no ties. Goal: find perfect matching without rogue couples.



Try a greedy algorithm?
 1: C, 2: A, 3: D, 4: B, 5: E
 4-C, 5-B def rogue couples here!
 There's no simple algorithm
 that works here but a more
 complex one does.

Matching algorithm (Gale-Shapley):

- 1) Propose: Unmatched proposers offer matching to top choice on their list (if list not null)
- 2) Accept/Reject: Recipients tentatively accept the best offer available, reject others
- 3) Update: Rejected proposers remove respondent from list
- 4) Repeat until only one proposer per recipient.

Use G-S on example:

	P	D ₁	D ₂	D ₃	D ₄	R
1: ^{2,3} C B E A D	2,4,5	5	5	5	A: 35214	
2: ¹ A B E C D	-	2	2,1	2	B: 52143	
3: D C B A E	1	1,4	4	4	C: 43512	
4: ¹ A C D B E	3	3	3	3	D: 12345	
5: A B E C D	-	-	-	1	E: 23415	

no rogue couples despite 1-E being "unhappy" ∴ stable matching!

would also like the
analysis

Proof of correctness: Need to show - ① Termination,
② Full matching $\frac{1}{2}$; ③ No rogue couples

Theorem ①: Alg. terminates in at most $n^2 + 1$ steps

Proof by contradiction: suppose alg. fails to terminate in $n^2 + 1$ days. If we don't terminate, there was a recipient with two proposers who rejects one; therefore a proposer removes recipient from their list. $\therefore$ progress is measurable by crossouts. Is it possible to cross out $n^2 + 1$ names? n lists with n names means n^2 names; $n^2 + 1$ crossouts is impossible. $\checkmark$

Let P : "If a respondent G ever rejects proposer B , respondent has a proposer they prefer to B ."

Lemma 1: P is an invariant for alg

Proof by induction on #. days

Base case: Day 0 "vacuously true" $\checkmark$

Induction step: Assume P holds at the end of step s . Show holds at end of $s+1$

Case 1: G rejects B on step $s+1$

$\hookrightarrow$ only possible if P true! $\checkmark$

Case 2: G rejected B before step $s+1$

But P assumed! $\therefore G$ had better proposer on step s , and so they have better proposer than B on step $s+1$ $\checkmark$

Theorem ②: Full pairing after alg. terminates

Proof (by contradiction): Assume that some proposer B is not paired at termination. B must have been rejected by every respondent. Therefore all respondents must have better suitors than B! So every respondent is paired; but can't occur without B is paired. QED

Theorem ③: Alg. produces stable matching

Proof (by contradiction): Let $B \notin G$ be any unmatched pair. Case 1: G has rejected B. In this case, G is paired with proposer they prefer to B ^{by lemma 1}. $\therefore$ no rogue couples possible for case 1. Case 2: G did not reject B. In this case, B never proposed to G, so they were paired with someone higher on B's preference list! $\therefore$ no rogue couples possible for case 2. All cases covered, QED.

Is this algorithm fair? Does it favor proposers or respondents?

Let S be set of all stable matches. $S \neq \emptyset$. For each person we define the "realm of possibility" for P to be $\{Q \mid \exists M \in S, \{P, Q\} \in M\}$

For $G = \begin{matrix} A & & B \\ & \times & \\ C & & D \end{matrix}$, A is not in r.o.p for B, because any A-B coupling creates unstable matching.

Def: A person's optimal mate is their favor within r.o.p. Person is least!

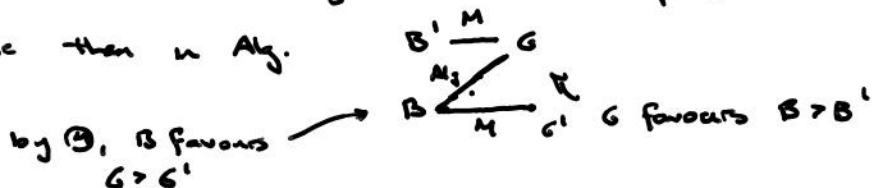
Theorem ④: Alg. matches every proposer with optimal mate

Theorem ⑤: " respondent with personal mate

We'll assume ④ True & prove ⑤

Proof of ⑤ (by contradiction):

Suppose $\exists$ stable matching M where $\exists$ respondent who fares worse than in Alg.



Since B favours G & G favours B , they create a rogue couple, so M is not stable, which contradicts original supposition.

Applications of Alg: Matching medical students to hospitals

Online dating

Traffic load balancing (P: servers, R: requests)

Problem Set 4

- i) Let $G = (V, E)$ be a graph. A matching in G is a set $M \subseteq E$ s.t. no two edges in M are incident on a common vertex. Let M_1, M_2 be matchings of G . Consider the new graph $G' = (V, M_1 \cup M_2)$. Show G' is bipartite.

If no two edges are incident on a common vertex, every node must be degree 1. Split every pairing into sets

$L \subseteq R$ st L is the leftmost node of the pairing & R is the rightmost. Thus our matching only pairs nodes from L with those from R & must be bipartite.

2) Let $G(V, E)$ be a graph. Recall that the degree of a vertex $v \in V$, denoted d_v , is the number of vertices w s.t. there is an edge between v & w

a) Prove that $2|E| = \sum_{v \in V} d_v$

By induction: For graph G of $|V| = 1$, $2|E| = \sum_{v \in V} d_v$

Base Case: $n = 1 \Rightarrow d = 0$ by def, no edges, $0 = 0 \checkmark$

Inductive step: Assume $G(|V| = n) \Rightarrow 2|E| = \sum_{v \in V} d_v$

Add node v^* of degree d^* to graph to make G'

For every connection of v^* some other node gets degree $+1$

$\therefore$ Total degrees in G' is $G + 2 \cdot d^*$, i.e. $\sum_{v \in V} d_v = d_v + 2d^*$

For every connection of v^* there is an extra edge

i.e. $|E_{G'}| = |E_G| + d^*$ need to add twice to balance $2d^*$ on other side of equality

so $2|E_{G'}| = \sum_{v \in V'} d_v \checkmark$

b) At a 6.042 study session, 111 students showed up.

During the session, some students shook hands with each other. A Chicago performed a study that claims each student shook hands with exactly 17 other students. Can you debunk this?

If each student shook hands with exactly 17 other students, we have $\sum_{v \in V} d_v = 1887$ for a student handshake graph. Note that from the result above, this would require fractional edges! $\therefore$ claim is false

2 cont) c) On a more dull note, how many edges does K_n , the complete graph on n vertices have?

For a complete graph, every node must connect to every other node. This means every node has degree $n-1$. $\therefore \sum_{v \in V} d_v = (n-1)n$ & there are $(n-1)n/2$ edges in K_n . This is, of course $\binom{n}{2}$

3) Two graphs are isomorphic if they are the same up to a relabelling of their vertices. A property of a graph is said to be preserved under isomorphism if whenever G has that property, every graph of G isomorphic to G also has that property. For example, the property of $|V|=5$ is preserved under isomorphism.

a) Which of these properties is preserved under isomorphism?

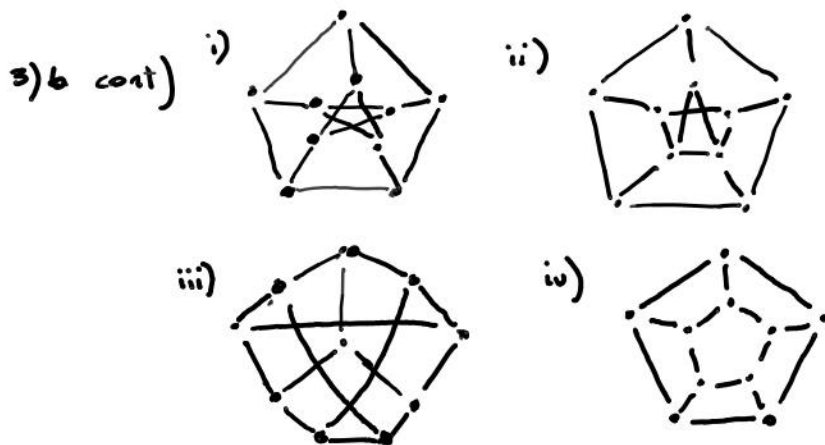
i) G has an even number of vertices ✓

ii) None of the vertices of G is an even integer ✗

iii) G has a vertex of degree 3 ✓

iv) G has exactly one vertex of degree 3 ✓

b) Which of the four graphs pictured on the next page are isomorphic.



i) & iii) are isomorphic; every node is degree 3

4) A colouring of a simple graph is an assignment of a colour to each vertex such that no two adjacent nodes have the same colour. A k -colouring uses at most k colours.

False Claim: Let G be a simple graph with maximum degree k . If G also has a vertex of degree $< k$, G is k -colourable.

a) Give a counterexample of the false claim for $k=2$. A separated node has degree 0, so G is not k -colourable.

b) We are provided a false proof (by induction) of the false claim. This proof relies on $P(n)$ = "Let G be a graph with n vertices and degree at most k . If G also has a vertex of degree less than k , G is k -colourable." The inductive step relies on removing vertices and claims that doing so will always reduce the degree of the other vertices. This is false when we remove vertices of degree zero.

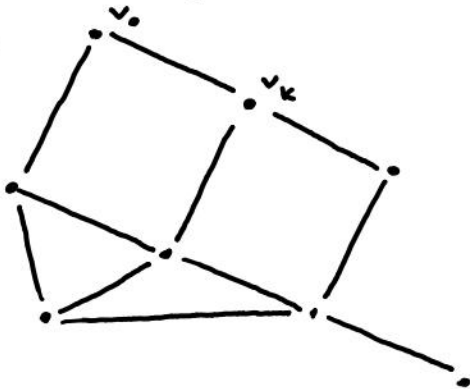
LECTURE 8: GRAPH THEORY II

Walks & Paths

A walk is a sequence of vertices that are connected by edges. $v_0 \xrightarrow{\text{start}} v_1 \rightarrow \dots \rightarrow v_k \xleftarrow{\text{end}}$. This is a walk from v_0 to v_k with length k .

A path is a walk where all vertices v_i 's are different.

If we delete loops we end up with a path.



Lemma 1: If $\exists$ walk from u to v , there also exists a path from u to v .

Proof: $\exists$ walk from $u \rightarrow v$, by well-ordering principle $\exists$ walk of minimal length. $u = v_0 - v_1 - \dots - v_{k-1} - v_k$. If this is not a path, there must be repeated nodes in the

shortest walk

Case 1: $k=0$ $\checkmark$ $k=1$ $\checkmark$

$k \geq 2 \leftarrow$ suppose walk is not a path

$\exists i \neq j \quad v_i = v_j$

$u = v_0 - \dots - v_i = v_j - \dots - v_k$ would be a shorter walk, contradicting assumption.

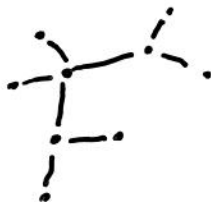
We define u, v as connected if there is a path from $u \rightarrow v$. We define a graph as connected when every pair of vertices in a graph are connected.

Cycles & Closed Walks

A closed walk is when a walk starts & ends at the same vertex. If $k \geq 3$ & $v_0, v_1, \dots, v_{k-1}$ are distinct, then the closed walk is a cycle.

Trees

A connected & acyclic graph is called a tree.



In a tree, a node with degree 1 is called a "leaf". Any ^{connected} subgraph of a tree is also a tree.

Proof: Suppose the connected subgraph is not a tree. $\therefore$ it must have a cycle. But a cycle in a subgraph must be present in the original graph, so the original graph cannot be acyclic. But it's a tree!

Lemma: A tree with n vertices has $n-1$ edges. ①

Proof: By induction - $P(n)$ ① Base case: $n=1$, no edges $\checkmark$

Induction step: $G(n)$ has $n-1$ edges. Adding a node can be leaf (1 new edge) or branch (1 old edge, one new edge)

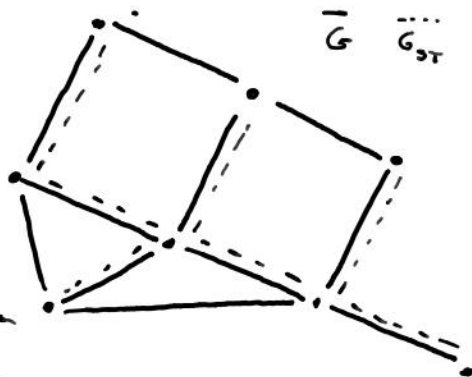
$$\therefore |E(G(n+1))| = |E(G(n))| + 1$$

(the proof in the lecture is more involved; it's not clear to me why the extra steps are required)

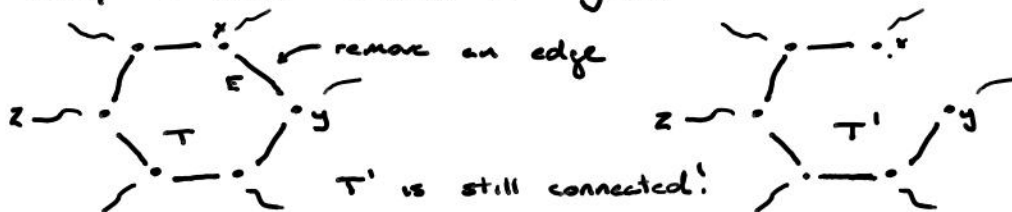
Spanning Trees

A spanning tree of a connected graph is a tree with the same vertices as the whole graph

Theorem: Any connected graph has a spanning tree



Proof. (by contradiction): Suppose there exist a ^{connected} graph G which does not contain a spanning tree. Let T be a connected subgraph of G with the same nodes as G & w/ smallest number of edges possible. If T is not a spanning tree, T must contain a cycle.

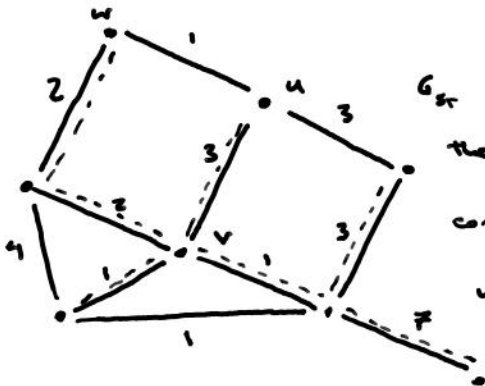


Case 1: $x \leftrightarrow y$ connected in T' .

Case 2: $x \leftrightarrow z$ & $y \leftrightarrow z$ in T' . $\therefore T'$ is a connected subgraph with fewer edges than T and no cycles; we've built a subgraph that breaks the original assumption.

$\therefore$ for all connected graphs there exists a spanning tree

Weighted Minimum Spanning Tree

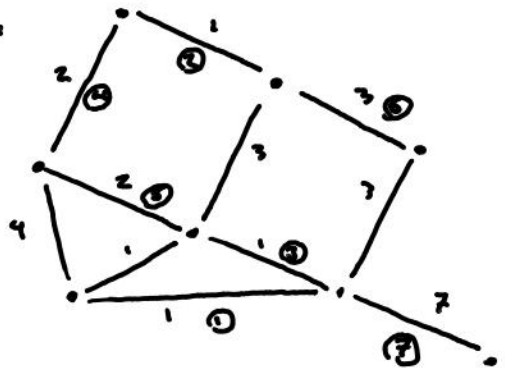


G_{ST} has total weight of 12. But there are other ways we can construct a spanning tree - we use $w \leftrightarrow u$ which is 3, but we can delete that edge & use

$w \leftrightarrow x$ instead to create a minimum-weight spanning tree:

Definition: The MST of a weighted-edge graph is a spanning tree of G that has the smallest possible sum of edge weights.

Alg: Grow a subgraph one edge at a time. At each step we add the minimum edge that keeps the subgraph acyclical. **Ex:**



Theorem: for any weighted connected graph G , the algorithm produces a weighted spanning tree.

Lemma 1: Let S' consist of the first m edges selected by the algorithm. Then $\exists_{MST} T = (V, E)$ for G such that $S' \subseteq E$

Proof: # $V = n$
(of theorem)

- 1) If $k < n-1$ edges are picked, then $\exists$ edge in $E-S'$ which can be added without creating a cycle.
- 2) once $m = n-1$, we know S' is a MST by Lemma 1
So we need to prove Lemma 1!

Proof by induction: (on m)

$P(m) = \forall G, \forall S$ consisting of the first m selected edges, $\exists \text{ MST}_G$ s.t. $S' \subseteq E$

Base Case: $m=0$; $S' = \{\}$ - empty set always $\subseteq E$ for any MST
we also know all graphs have a minimum spanning tree (proved earlier) ✓

Inductive step: $P(m) \Rightarrow \exists \text{ MST}_G$ s.t. $S'(m) \subseteq E$;

Let e denote the edge added in the $n^{th}+1$ step. Let S' denote the first m selected edges.

Let $T^* = (V, E^*)$ be a MST such that $S' \subseteq E^*$

Case 1: $e \notin E^* \Rightarrow S \cup \{e\} \subseteq E^* \rightarrow P(m+1)$ ✓

Case 2: $e \notin E^*$:

$S' \text{ --- } \bullet$
 $T' \text{ --- } \bullet \text{ --- } \bullet \text{ --- } \bullet$
 $G \text{ --- } \bullet \text{ --- } \bullet \text{ --- } \bullet$

e not in T' : how do we maintain tree property?

Alg $\Rightarrow S' \cup \{e\}$ has no cycle

T^* is a tree $\Rightarrow (V, E^* \cup \{e\})$ has a cycle

i.e. if you add an edge to a tree we create a cycle

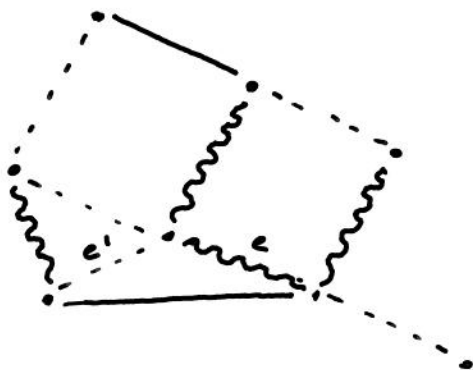
Therefore this cycle must have an edge $e' \in E^* - S'$
 $e' \in E^*$, $e' \notin S'$. We must swap e & e'

Since the algorithm could have selected e' , $w_e \leq w_{e'}$

Let $T^{**} = (V, E^{**})$. $E^{**} = (E^* - \{e'\}) \cup \{e\}$

T^{**} is acyclic because removed e' from the only cycle in $E^* \cup \{e\}$. T^{**} is connected because we removed an edge within a cycle. T^{**} contains all nodes of G . $\therefore T^{**}$ is a spanning tree.

Weight of $T^{**} \leq T^*$; T^* is MST; T^{**} is a minimum spanning tree; case 2 shown true! $\therefore$ lemma 1 shown true & theorem is true.



LECTURE 9: Communications Networks

$N \times N$ networks	Diameter	Switch Size	# Switches	Congestion
Binary Tree ①	$2(1 + \log N)$	3×3	$2N - 1$	N
2D Array ②	$2N$	2×2	N^2	2
Butterfly ③	$2 + \log N$	2×2	$N(1 + \log N)$	$\sqrt{N} \parallel \sqrt{N/2}$
Benes ④	$1 + 2 \log N$	2×2	$2N \log N$	1

① COMPLETE BINARY TREE

D: switch

direct packets through
network, fixed-sized
pieces of data

Π : terminal: source ϵ

destination of data

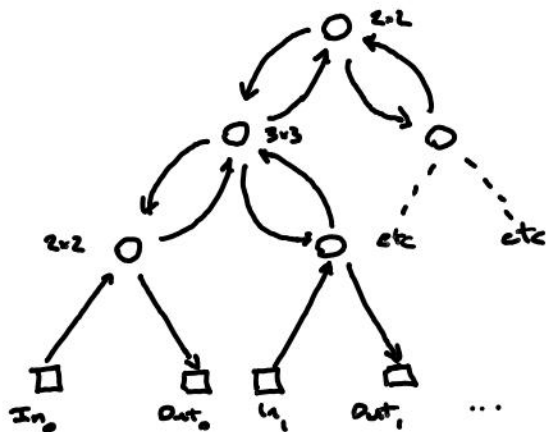
We want efficient

terminal $\rightarrow$ terminal routing

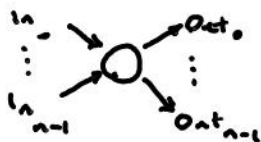
Latency: time required for a packet to travel from an input to an output. We measure this by number of wires traversed.

Diameter of a network: length of the shortest path between input & outputs which are furthest apart. For NW B.T.

$$2(1 - \log 2)$$



Switch size: Number of inputs & outputs being handled by a switch. Equivalent to degree of node. Increasing switch size will reduce diameter! So why not just use a monster switch?



switch size: $n \times n$, diameter: 1!

But the big switch just obscures the problem because we don't know how it works - the network is about building the monster switch.

For binary trees we use $1+2+4+8+\dots+N$ switches, which is $2N-1$.

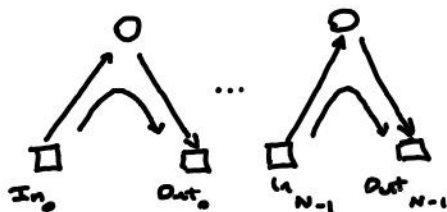
Congestion: Packages may all have to travel through the root node! Root is overloaded & if it fails the left & right sides of the tree can't even talk to each other.
i.e. the same net

A permutation is a function $\pi: \{0, \dots, N-1\} \rightarrow \{0, \dots, N-1\}$ such that no two numbers are mapped to the same value; i.e. $\pi(i) = \pi(j)$ iff $i = j$

Ex: $\pi(i) = N-1-i$; $\pi(i) = i$. How do we get from permutation to congestion?
identity permutation

Permutation Routing Problem for π :

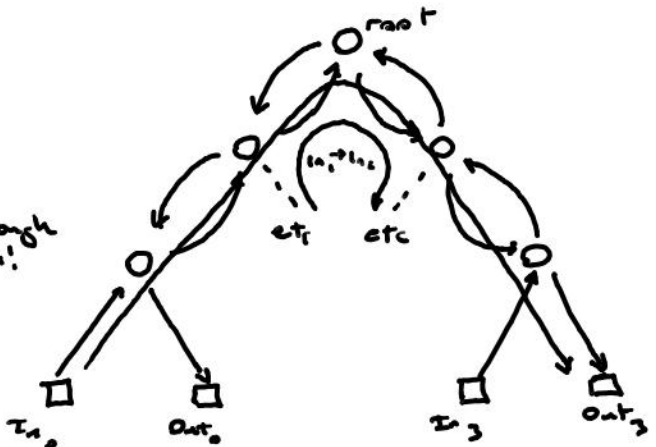
For each i , we want to direct the packet at input i to output $\pi(i)$ for all i . for identity permutation, looks like:



What about $N-1-i$?

$I_{n_0} \rightarrow out_3$
 $I_{n_1} \rightarrow out_2$
 $I_{n_2} \rightarrow out_1$
 $I_{n_3} \rightarrow out_0$

all or through root switch!



The path taken

is denoted by $P_{\pi(i)}$. The congestion of paths

$P_{\pi(0)}, \dots, P_{\pi(N-1)}$ is now defined as the largest number of paths that pass through a single switch.

For $\pi(i) = i$, congestion is 1.

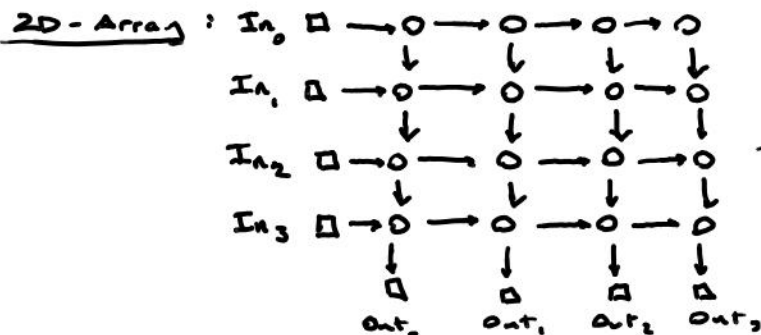
For $\pi(i) = N-1-i$ on four-terminal tree, congestion is 4

Binary trees always have a permutation that leads to worst-case congestion

Max congestion = $\max_{\pi} \min_{\text{solution } P_{\pi(0)} \dots P_{\pi(N-1)}} \text{congestion } P_{\pi(0)} \dots P_{\pi(N-1)}$

we want best solution over worst case

For a binary tree we've seen this is N. Can we do better?



Largest path $I_{n_0} \rightarrow out_3$

switches N^2

①

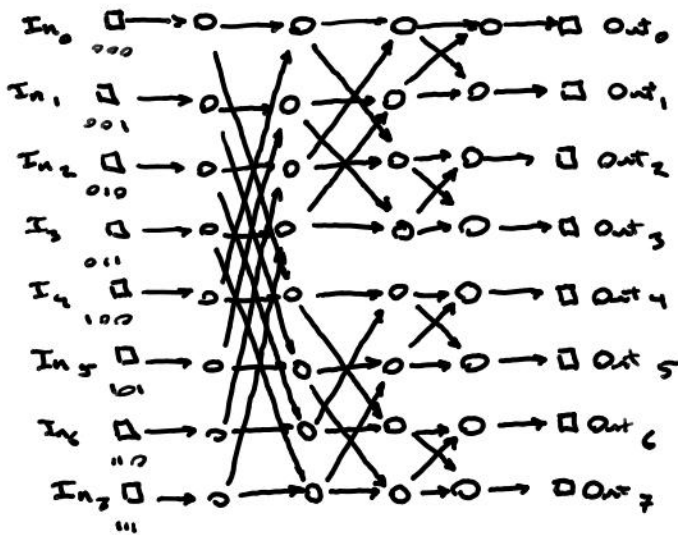
Theorem: congestion of an N -input array $= 2$

Proof of ①: Let π be a permutation $P_i, \pi(i)$; the path from In_i is rightward to column π_i , then downward to output. Switch in row i , column π_i transmits at most two packets.

The identity permutation causes crossover, so congestion two is a lower bound as well as an upper.

Can we condense these network paradigms?

Butterfly Network (Ex 8×8)



Tree structure w/in grid! we label switches by row & column.
Row: binary 000, 001, etc
Col: Depth 0, 1, ... etc

Switches uniquely identified by row & column # bits

$(b_1, \dots, b_{\log_2 N}, l)$ level

Routes to $(b_1, \dots, b_{l-1}, \dots, b_{\log_2 N}, l+1)$

$(b_1, \dots, b_{l-1}, \dots, b_{\log_2 N}, l+1)$

eg. $(010, 0) \rightarrow (010, 1) \rightarrow (110, 1)$

Getting from input to output:

$$\begin{aligned}
 (x_1, \dots, x_{\log N}, 0) &\rightarrow (y_1, x_2, x_3, \dots, x_{\log N}, 1) \\
 &\quad \downarrow \\
 &\quad (y_1, y_2, x_3, \dots, x_{\log N}, 2) \\
 (y_1, \dots, y_{\log N}, \log N) &\leftarrow \text{swap bits one by one}
 \end{aligned}$$

Each switch can flip one row bit corresponding to level,

In our example, going from input 011 $\rightarrow$ 101 requires flips between level 0 & 1 and then 1 & 2, i.e.:

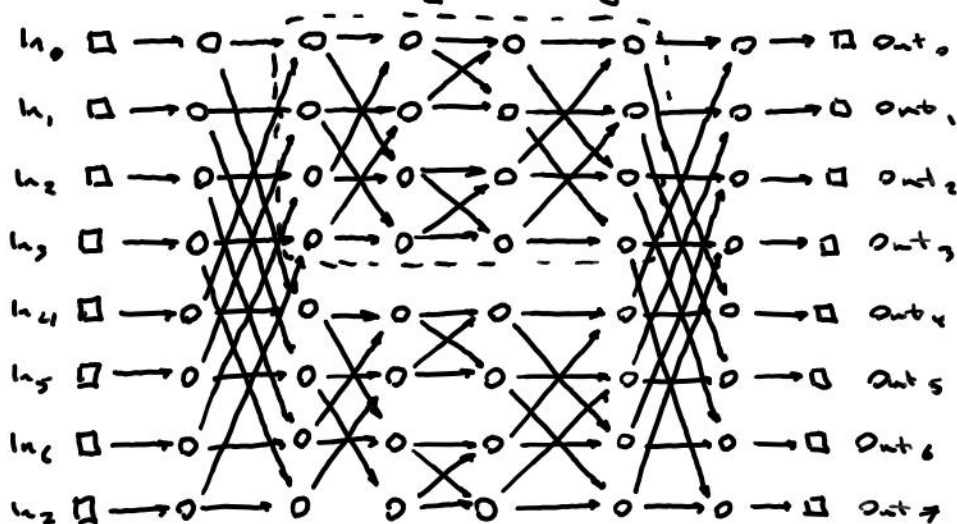
$$\text{input} \rightarrow (011, 0) \xrightarrow{\text{start}} (111, 1) \rightarrow (101, 2) \rightarrow (101, 3) \rightarrow \text{output}$$

$\underbrace{\hspace{15em}}_{\log N \text{ layers}}$

$\therefore$ diameter is $2 + \log N$; # switches is $N(1 + \log N)$

congestion is $\sqrt{N}$ or $\sqrt{N/2}$ (I'll show this for homework)

Benes network: repeating Butterfly



Note recursive structure - highlighted region also Benes Net

Theorem: N -input Benes network has congestion of one
 when $N=2^a$ for some $a \geq 1$

Proof by induction on a .

$P(a)$: Theorem true for a $\therefore$

Base Case: $N=2^1$



Either $0 \rightarrow 0 \ \& \ 1 \rightarrow 1$ or $0 \rightarrow 1 \ \& \ 1 \rightarrow 0$; in both cases each switch only sees one packet $\checkmark$

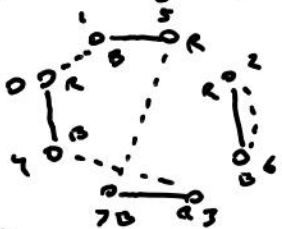
Inductive Step: Assume $P(a)$ true

Build a constraint graph with the reqs for congestion = 1

Example: $\pi(0)=1 \ \pi(1)=5 \ \pi(2)=4 \ \pi(3)=7 \ \pi(4)=3 \ \pi(5)=6 \ \pi(6)=0 \ \pi(7)=2$

① If two packets must pass through different subnetworks, there is an edge between them.

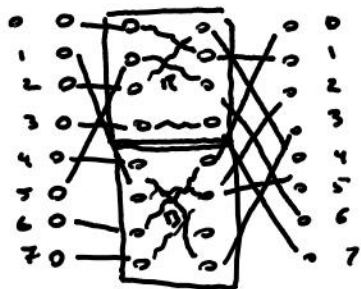
input —
 output ---



Ex: The packet destined for Out_0 ($\pi(6)=0$) $\& \$ the packet for Out_1 ($\pi(2)=4$)

Insight: 2-colouring of the constraint graph

cannot pass through same subnetwork



$\therefore$ congestion of first $\& \$ last levels = 1
 since $P(a)$ applies to interior subnetworks, theorem is true

LECTURE 10: Graph Theory III

Euler Tours (Koenigsburg bridges problem)

An Euler Tour is a walk that traverses every edge exactly once. It also starts & finishes at the same vertex.

Theorem: A connected graph has an Euler Tour if & only if every vertex in the graph has even degree.

Proof: Assume $G=(V,E)$ with an Euler Tour.



Since every edge is traversed once, every node entry must be paired with a node exit along an unused edge.

$\deg(u) = (\# \text{ of appearances in tour}) \cdot 2 \therefore \deg(u)$ must be even.

Now we assume every vertex has even degree.

Let $W: v_0 - v_1 - \dots - v_k$ be the longest walk that traverses no edge more than once.

① if v_k has an unused edge $\notin W$, we can add to W

$\therefore$ all edges of v_k are traversed by W

② $v_k = v_0$, otherwise $v_k \neq v_0$ have odd degree in W , and in

G as well by ①. Since we have assumed even degree for all nodes, this is a contradiction $\therefore v_0 = v_k$

Suppose W is not an Euler tour. G is connected, so $\exists$ edge not in W but incident to some node in W . Let $u-v$ be this edge. If we start the tour at u , this gives us an extra edge, contradicting W as the longest walk. QED

Directed Graphs (digraphs)



Edges are directional, so vertices now have an in-degree and an out-degree. v_1 in G above has in-degree 1 & out-degree 3.

Theorem: Let $G = (V, E)$ be an n -node graph with $V = \{v_1, \dots, v_n\}$. Let $A = \{a_{ij}\}$ denote the adjacency matrix for G .

$$a_{ij} = \begin{cases} 1 & \text{if } v_i \rightarrow v_j \in E \\ 0 & \text{else} \end{cases}$$

Let $a_{ij}^{(k)}$ be equal to the number of directed walks of length k from v_i to v_j . Then $A^n = \{P_{ij}^{(k)}\}$

For G above: $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$; $A^2 = \begin{bmatrix} 1 & 2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$; $A^3 = \begin{bmatrix} 1 & 3 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

Proof

$a_{ij}^{(k)}$ denotes the $(i, j)^{\text{th}}$ entry in A^k

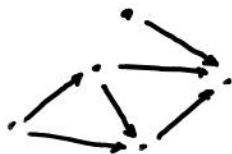
$$P(k) = \forall_{i,j}, a_{ij}^{(k)} = P_{ij}^{(k)}$$

Base case: $k=1$. Edge $v_i \rightarrow v_j$: $P_{ij}^{(1)} = 1 = a_{ij}^{(1)}$

No edge $v_i \rightarrow v_j$: $P_{ij}^{(1)} = 0 = a_{ij}^{(1)}$ ✓

Inductive step: Assume $P(k)$. $P_{ij}^{(k+1)} = \sum_{h: v_h \rightarrow v_j} P_{ih}^{(k)} = \sum_{h=1}^n P_{ih}^{(k)} \cdot a_{hj}^{(1)} = \sum_{h=1}^n A_{ih} \cdot A_{hj} = A_{ij}^{(k+1)}$ ✓

A directed graph $G=(V,E)$ is strongly connected if: all nodes are reachable from all other nodes; i.e. $\exists$ a directed path $\forall u,v \in V$ from u to v .



Directed acyclic graphs (DAGs) do not contain any directed cycles.

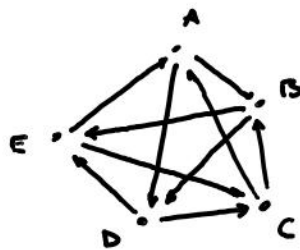
Tournament Graphs

either u beats v : $u \rightarrow v$

or v beats u : $u \leftarrow v$

Ex: $A \rightarrow B \rightarrow D \rightarrow E \rightarrow C$

$\downarrow$
 $C \rightarrow B \rightarrow D \rightarrow E \rightarrow A$



degree $u + \text{out}$
 $= |V| - 1$

so is A the strongest player?
(No!)

A directed Hamiltonian path is a directed walk that visits every vertex exactly once.

Theorem: Every tournament graph contains a directed Hamiltonian path

Proof by induction on nodes

$P(n)$: Every tournament graph of n nodes contains a DHP

Base case: $n=1$ ✓

Inductive step: Assume $P(n)$; show $P(n+1)$

Consider tournament graph on $n+1$ nodes. Look at n -node subgraph - remove a node! still have a tournament graph of size n , which must have a DHP by $P(n)$

Our DHP can be $v_1 \rightarrow v_2 \rightarrow \dots \rightarrow v_n$ ①

Now we add the deleted node back u .

Case 1: $v_{n+1} \rightarrow v_1$. Then v_{n+1} inserted at start of ① ✓

Case 2: $v_n \rightarrow v_{n+1}$. Find first node beaten by v_{n+1} . Call this

node v_q . Then v_{q+1} beats v_{n+1} . So

we know v_{q-1} beats v_{n+1} because v_q is first node that loses to v_{n+1} $\dots \rightarrow v_{q-1} \rightarrow v_{n+1} \rightarrow v_q \dots$, which is valid DHP. If no node beaten by v_{n+1} , $\dots \rightarrow v_n \rightarrow v_{n+1}$ also valid DHP ✓

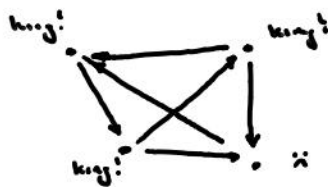
Ex: Chicken Tournament

Either chicken u pecks v ; $u \rightarrow v$ or $v \rightarrow u$

u virtually pecks v if $u \rightarrow v$ OR $\exists_w u \rightarrow w \rightarrow v$

A chicken that virtually pecks every other chicken is a Chicken King.

Theorem: The chicken with the most outgoing edges is a chicken king



By contradiction, suppose it is not. Let u have highest out degree & not be king. $\exists_v: v \rightarrow u$, and $\underbrace{\exists_w: w \rightarrow u \text{ or } v \rightarrow w}_{\text{if } u \rightarrow w, \text{ then } v \rightarrow w}$

$\therefore$ for all outgoing edges from u , v must have an outgoing edge. $\deg^+(v) \geq \deg^+(u) + 1$, so u does not have the highest out degree, which contradicts original assumption

LECTURE 11: Relations, Partial Orders, & Scheduling

Relations: A relation from set A to set B is a subset $R \subseteq A \times B$

Example: $R = \{(a, b) : \text{student } a \text{ is taking class } b\}$

$$(a, b) \in R: \underbrace{a R b, a \sim_R B}$$

notation: "a is related to b"

A relation on A is a subset $R \subseteq A \times A$ you might imagine these as edges!

Example: $A = \mathbb{Z} : x R y \text{ iff } x \equiv y \pmod{5}$

$$A = \mathbb{N} : x R y \text{ iff } x | y$$

$$A = \mathbb{N} : x R y \text{ iff } x \leq y$$

} These are all different relations
∴

Set A together with R is a directed graph

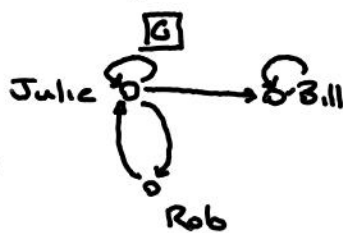
$$G = (V, E), \text{ with } V = A \text{ \& \; } E = R$$

In example G , the relation

is "likes": Julie likes Rob & Bill;

Bill only likes himself; Rob likes

Julie but not himself.



Properties

A relation R on A is reflexive if $x R x$ for all $x \in A$. A relation R on A is symmetric if $x R y \Rightarrow y R x \forall x, y$, and anti-symmetric if $x R y \wedge y R x \Rightarrow x = y$.

Transitivity occurs if $x R y \wedge y R z \Rightarrow x R z$

Examples

<u>Relation</u>	<u>Reflexive?</u>	<u>Symmetric?</u>	<u>Anti-Symmetric?</u>	<u>Transitive?</u>
$x \equiv y \pmod{5}$	✓	✓	✗	✓
$x \mid y$	✓	✗	✓	✓
$x \leq y$	✓	✗	✓	✓

These sets of properties lead to more definitions.

The $x \equiv y \pmod{5}$ example - reflexive, symmetric & transitive - is representative of an "equivalence relation", while the $x \mid y$ & $x \leq y$ examples represent "partial orders".

The most obvious example of an equivalence relation is equality ($=$) itself. We've also seen that $x \equiv y \pmod{n}$ is an equivalence relation. The equivalence class of $x \in A$ is equal to the set of all elements $u \in A$ related to x by R ; denoted $[x]$

$$\text{(i.e. } [x] = \{y : x R y\})$$

Example: $x \equiv y \pmod{5}$

$$[7] = \{\dots, -3, 2, 7, 12, 17, 22, \dots\}$$

$$[7] = [12] = [17] = \dots$$

A partition of A is a collection of disjoint, non-empty sets $A_1, \dots, A_n, \subseteq A$ whose union is A

Ex: $\left[\{-5, 0, 5, \dots\}, \{-4, 1, 6, \dots\}, \{-3, 2, 7, \dots\}, \right. \\ \left. \{-2, 3, 8, \dots\}, \{-1, 4, 9, \dots\} \right]$ is a partition of $x \equiv y \pmod{5}$

Theorem: The equivalence class of an equivalent relation on a set A form a partition on set A .
(asserted only)

Partial Orders

A relation is a (weak) partial order if it is reflexive, anti-symmetric, & transitive.

A partial order relation is denoted with $\leq$, not R .

$(A, \leq)$ is called a partially ordered set, or a poset.

A poset is a directed graph with vertex set A and edge set $\leq$

Example: Dressing formally as a partial order



This is a
Hasse Diagram

A Hesse Diagram for poset $(A, \leq)$ is a directed graph with vertex set A and edge set $\leq$ minus all self-loops & all edges implied by transitivity.

Theorem: A poset has no directed cycles other than self-loops.

Proof: (by contradiction)

Suppose $\exists_{n \geq 2}$ distinct elements $a_1, \dots, a_n$ such that $a_1 \leq a_2 \leq a_3 \leq \dots \leq a_{n-1} \leq a_n \leq a_1$. The anti-symmetric definition of relations requires that $a_1 \leq a_n$ only holds when $a_n \leq a_1$ if $a_n = a_1$, and the transitive property shows that $a_1 \leq a_n$. If all elements are distinct, we have a contradiction.

① This property would be a lemma, proved by induction

$\therefore$ There are no directed multi-element cycles in a poset. So after deleting self-loops from a poset, we must have a directed acyclic graph (DAG).

Note that we have a partial ordering; there will be incomparable elements here. a & b are incomparable if neither $a \leq b$ nor $b \leq a$ (they are comparable otherwise).

A total order is a partial order in which every element is comparable. A Hasse Diagram of a total order must be a straight line! This is obviously trivial to rank - but how would we do this for more standard posets?

A total order consistent with a partial order is called a topological sort. A topological sort of a poset $(A, \leq)$ is formally defined as a total order $(A, \leq_T)$ such that the original relation is a subset of the new: $\leq \subseteq \leq_T$ ($x \leq y \Rightarrow x \leq_T y$)

Theorem: Every finite poset has a topological sort.

$x \in A$ is called minimal if $\nexists y \in A, y \neq x$ such that $y \leq x$. $x \in A$ is similarly maximal if under the same conditions $x \leq y$.

Not every poset has a minimal element; e.g. $(\mathbb{Z}, \leq)$

Lemma: Every finite poset has a minimal element

A chain is a sequence of distinct elements

$$a_1 \leq a_2 \leq a_3 \leq \dots \leq a_n \leftarrow n = \text{length}$$

Proof of Lemma:

Let $a_1 \leq a_2 \leq \dots \leq a_n$ be a maximum-length chain. Case 1: $a \notin \{a_1 \leq \dots \leq a_n\}$: if $a \leq a_1$, then there must be a bigger chain, which is false. So $a \leq a_1$.

Case 2: $a \in \{a_1 \leq \dots \leq a_n\}$: if $a \leq a_1$, then there is a cycle in our poset, which cannot be!

$\therefore$ Every finite poset contains a minimal element a_1 .

Proof of topological order in finite poset:

Let $(A, \leq)$ be a finite poset with $n = |A|$ elements.

By lemma 1, one of these elements is a minimal element.

$P(n)$: Every poset $(A, \leq)$ with length $< n$ has a valid topological ordering.

Base Case: $n=2$ (true by inspection) $\checkmark$

Inductive Step: Let a be the minimal element of A . Remove a to create $(n-1)$ -length poset A' . This has a valid topological ordering by $P(n)$. Add a to start of A' to create n -length poset, which is a valid topological ordering because $a \leq \{A'\}$ $\checkmark$

LECTURE 12: Sums

An n -year, $\$m$ -payment annuity pays $\$m$ at the start of each year, lasting for n years. What is it worth? $\$50,000$ yr/ 20 years vs. $\$1,000,000$ up front. Obviously the cash up front is better. What about $\$50k/yr$ for 20 years vs. $\$700k$? $\$500k$?

What is the future value of one dollar?

Assumption: fixed interest rate p

So $\$1$ today $\Rightarrow \$ (1+p)$ in 1 year

$\$(1+p)^2$ in 2 years

what is $\$1$ in one year worth today? $1/(1+p)$

two years? $1/(1+p)^2$

Value

$\$m$

$\$m/(1+p)$

$\$m/(1+p)^2$

$\vdots$

$\$m/(1+p)^{n-1}$

Payments

$\$m$ now

$\$m$ yr+1

$\$m$ yr+2

$\vdots$

$\$m$ yr+n-1

$$\therefore \text{Total current value} = \$ \sum_{i=0}^{n-1} m/(1+p)^i$$

Alternate expression: $V = m \sum_{i=0}^n x^i$; $x = 1/(1+p)$

$$= m \frac{(1-x^{n+1})}{1-x}$$

Theorem: for all $n \geq 1$ & $x \neq 1$, $\sum_{i=0}^n x^i = \frac{1-x^{n+1}}{1-x}$

How do we turn sums into closed-form solutions?

Many methods, but we'll start with...

Perturbation Method

$$\begin{aligned} S &= 1 + x + x^2 + \dots + x^{n-1} \\ xS &= x + x^2 + \dots + x^{n-1} + x^n \end{aligned} \quad \left. \vphantom{\begin{aligned} S &= 1 + x + x^2 + \dots + x^{n-1} \\ xS &= x + x^2 + \dots + x^{n-1} + x^n \end{aligned}} \right\} \text{subtract!}$$

$$S - xS = 1 - x^n$$

$$S = (1-x^n)/(1-x) \quad \text{i.e. method is jiggling the sum around a little bit!}$$

Back to V : $V = m \left(\frac{1-x^{n+1}}{1-x} \right)$

$$= m \left(\frac{1 - (1/(1+p))^{n+1}}{1 - (1/(1+p))} \right)$$

$$= \frac{m}{p} \left(1+p - 1/(1+p)^n \right)$$

For $m = \$50k$, $n = 20$ years, $p = 0.06$, $V = \$607,906$

Claim: if $n = \infty$, $V = m \left(\frac{1+p}{p} \right) (1/(1+p)^n) \rightarrow 0$
as $n \rightarrow \infty$

For $m = \$50k$, $n = \infty$, $p = 0.06$, $V = \$883,333$

Corollary: If $|x| < 1$, $\sum_{i=0}^{\infty} x^i = 1/(1-x)$

Proof: $\lim_{n \rightarrow \infty} x^n = 0$ for $|x| < 1$

Example: $1 + 1/2 + 1/4 + 1/8 + \dots = 1/(1-1/2) = 2$

$1 + 1/3 + 1/9 + 1/27 + \dots = 1/(1-1/3) = 3/2$

These are all decaying geometric series, which tend to sum to the largest term. They can get a little more complicated than our examples e.g.: $\sum_{i=1}^n i x^i = x + 2x^2 + 3x^3 + \dots + nx^n$. Can we turn this into a closed-form expression? Try perturbation?

$$S = x + 2x^2 + 3x^3 + \dots + nx^n$$

$$xS = x^2 + 2x^3 + \dots + (n-1)x^n + nx^{n+1}$$

← this is obviously not going to cancel with straight subtraction. but...

$$(1-x)S = \underbrace{x + x^2 + x^3 + \dots + x^n}_{\text{geometric series!}} + nx^{n+1}$$

This is a geometric series!

$$\therefore (1-x)S = (1-x^{n+1})/(1-x) - 1 - nx^{n+1}$$

$$\Rightarrow S = \frac{x - (n+1)x^{n+1} + nx^{n+2}}{(1-x)^2} \quad \textcircled{1}$$

Another sums technique is the derivative method:

For $x \neq 1$, $\sum_{i=0}^{\infty} x^i = 1/(1-x)$ from theorem; take

derivative of both sides $\Rightarrow \sum_{i=0}^{\infty} i x^{i-1} = \frac{1 - (n+1)x^n + nx^{n+1}}{(1-x)^2}$

↳ multiply by x , and then we'll get $\textcircled{1}$!

Theorem: If $|x| < 1$, $\sum_{i=1}^{\infty} i x^i = x/(1-x^2)$ (proof trivial) $\nwarrow$ x still $1/p$

Example: An annuity that pays \$im at the end of each year $i \in \mathbb{N}$ is worth:

$$m \left[\frac{1/1+p}{(1 - 1/(1+p))^2} \right] = m(1+p)/p^2 \quad \text{for } m = \$50,000 \text{ \& } p = 0.06, V = \$14.7m$$

So a company that might grow linearly forever has a finite current value because the p term is bleeding it geometrically.

$$\sum_{i=1}^{\infty} i 2^{-i} = \frac{1}{2} + \frac{2}{4} + \frac{3}{8} + \frac{4}{16} + \dots = \frac{1/2}{(1-1/2)^2} = \frac{1/2}{1/4} = 2$$

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}; \quad \sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6} \quad \leftarrow \text{this one is hard to remember! do we have any tricks?}$$

Guess: $\forall n, \sum_{i=1}^n i^2 = an^3 + bn^2 + cn + d$

Plug in: $n=0 \Rightarrow 0 = d$

$n=1 \Rightarrow 1 = a + b + c + d$

$n=2 \Rightarrow 5 = 8a + 4b + 2c + d$

$n=3 \Rightarrow 14 = 27a + 9b + 3c + d$

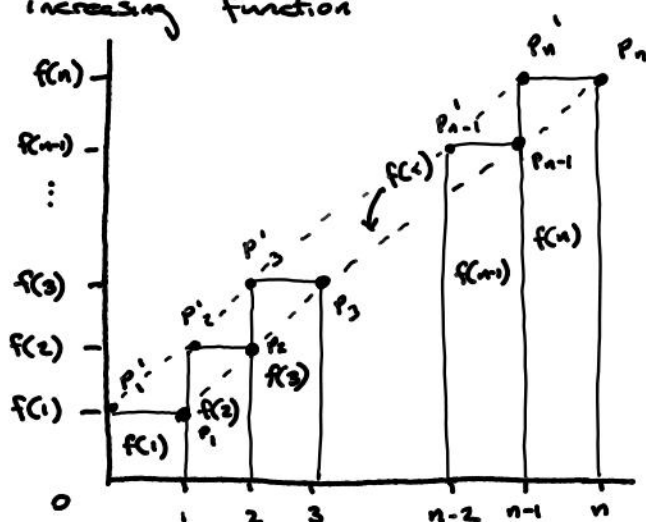
} solvable system!

$a = 1/3, b = 1/2, c = 1/6, d = 0 \Rightarrow \text{matches } \textcircled{2}$
(not a proof :))

Don't always expect a closed-form solution for every sum!

$\sum_{i=1}^n \sqrt{i}$ ← no easy solutions here, but some bounding tricks.

Integration Bounds for $\sum_{i=1}^n f(i)$ when f is a positive increasing function



low bound on our sum!

$$\sum_{i=1}^n f(i) \geq f(1) + \int_1^n f(x) dx$$

obviously some rects. are trimmed here

also

$$\sum_{i=1}^n f(i) \leq f(n) + \int_1^n f(x) dx \quad (3)$$

Why is (3) true? Imagine our curve translated left by 1 unit. This is now more than what is shown in first $n-1$ rectangles! So now we have upper & lower bounds on the sum.

$$f(i) = \sqrt{i} \Rightarrow \int_1^n \sqrt{x} dx = \frac{x^{3/2}}{3/2} \Big|_1^n = \frac{2}{3} (n^{3/2} - 1)$$

$$\sum_{i=1}^n \sqrt{i} \geq f(1) + \frac{2}{3} (n^{3/2} - 1)$$

$$\leq f(n) + \frac{2}{3} (n^{3/2} - 1)$$

$$\frac{2}{3} n^{3/2} + \frac{1}{3} \leq \sum_{i=1}^n \sqrt{i} \leq \frac{2}{3} n^{3/2} + \sqrt{n} - \frac{2}{3}$$

Let $n = 100$

$$667 \leq \text{sum} \leq 678 \leftarrow \text{tight gap!}$$

note that the gap scales with $\sqrt{n}$, but answer grows faster. So relative error shrinks!

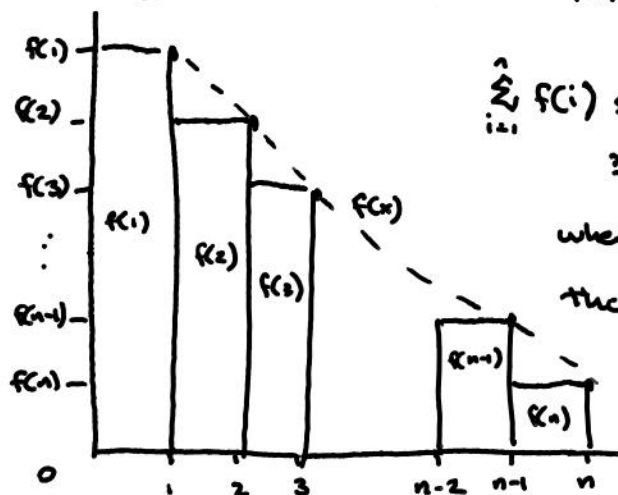
$$\sum_{i=1}^n \sqrt{i} = \frac{2}{3} n^{3/2} + \delta(n) \text{ where } \frac{1}{3} \leq \delta(n) \leq \sqrt{n} - \frac{2}{3}$$

$\sum_{i=1}^n \sqrt{i} \sim \frac{2}{3} n^{3/2}$ this notation needs formalising what it's doing here is neglecting $\delta(n)$ because it is small when n large; not a driving term

Formally, $g(x) \sim h(x)$ means that $\lim_{x \rightarrow \infty} \frac{g(x)}{h(x)} = 1$

$$\lim_{n \rightarrow \infty} \frac{\frac{2}{3} n^{3/2} + \delta(n)}{\frac{2}{3} n^{3/2}} = \frac{\delta(n)}{\frac{2}{3} n^{3/2}} \rightarrow 0 \checkmark$$

What happens to the integration bounds when f is decreasing (but positive)? Ex: $\sum_{i=1}^n \frac{1}{\sqrt{i}}$



$$\sum_{i=1}^n f(i) \leq f(1) + \int_1^n f(x) dx$$

$$\geq f(n) + \int_1^n f(x) dx$$

when function is decreasing the bounds flip!

$$f(i) = 1/\sqrt{i}$$

$$\int_1^n \frac{dx}{\sqrt{x}} = \frac{\sqrt{x}}{1/2} \Big|_1^n = 2(\sqrt{n} - 1) = 2\sqrt{n} - 2$$

$1/\sqrt{n}$ (drop this off & weaken bound)

$$\cancel{f(n)} + 2\sqrt{n} - 2 \leq \sum_{i=1}^n 1/\sqrt{i} \leq \cancel{f(1)} + 2\sqrt{n} - 2$$

$$2\sqrt{n} - 2 < \leq 2\sqrt{n} - 1$$

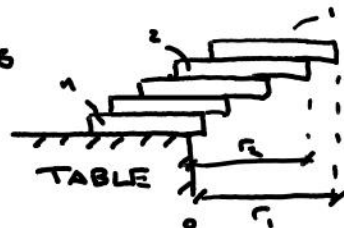
$$\therefore \sum_{i=1}^n 1/\sqrt{i} = 2\sqrt{n} - \delta(n); \quad 1 \leq \delta(n) \leq 2$$

$$\sum_{i=1}^n 1/\sqrt{i} \sim 2\sqrt{n} \quad \left(\lim_{n \rightarrow \infty} \frac{2\sqrt{n} - \delta(n)}{2\sqrt{n}} \right) = 1 - \lim_{n \rightarrow \infty} \frac{\delta(n)}{2\sqrt{n}} = 1 \quad \checkmark$$

LECTURE 13: Sums & Asymptotics

Block contest: greedy strategy

Given: n blocks of length 1



Def: r_i = amount by which i^{th} block extends beyond the table

Stability Constraint: The center of mass C_k of the top k blocks must lie on the $(k+1)^{\text{th}}$ block (or the table).

For greedy stacking, which pushes each block as far as it can go from $1 \rightarrow n$, $C_k = r_{k+1}$.

How do we get a formula for C_k ?

Since every block is extended as far as possible, we know that the centre of mass of the k^{th} block is at $r_k - 1/2$. Therefore the centre of mass of the top k blocks is $C_k = \frac{(k-1)C_{k-1} + 1(r_k - 1/2)}{k-1+1}$ (remember block length is 1)
 $= \frac{(k-1)C_{k-1} + r_k - 1/2}{k}$

After simplifying, $r_k - r_{k+1} = 1/2k$, which tells us how far the k^{th} block extends past the $k+1^{\text{th}}$ block

$$\left. \begin{array}{l} \Delta r_1 r_2 : 1/2 \\ \Delta r_2 r_3 : 1/4 \\ \vdots \\ \Delta r_{n-1} r_n : 1/2n \end{array} \right\} \text{obviously a geometric sum}$$

$$r_1 = \sum_{i=1}^n 1/2i \Rightarrow 1/2 \sum_{i=1}^n 1/i \quad \textcircled{D}$$

Note that the sum $\textcircled{D}$ comes up so often that it has a special name: the harmonic sum. Values associated with this series are harmonic numbers.

$$H_n = \sum_{i=1}^n 1/i \quad H_1 = 1, \quad H_2 = 1 + 1/2 = 3/2, \quad H_3 = 7/6, \quad H_4 = 25/12$$

note that this shows the top block can escape the table

Harmonic numbers grow to infinity

but we don't have a closed-form expression.

Need to use integration bounds for decreasing sums.

$$f(n) + \int_1^n f(x) dx \leq \sum_{i=1}^n \frac{1}{i} \leq f(1) + \int_1^n f(x) dx \quad [f(i) = 1/i]$$

$$\int_1^n \frac{1}{x} dx = \ln x \Big|_1^n = \ln(n) \quad \leftarrow \text{very slowly goes to infinity}$$

$$\therefore \frac{1}{n} + \ln(n) \leq H_n \leq 1 + \ln(n)$$

$$H_n \sim \ln(n)$$

H_n has had a lot of work done; the equality is actually $H_n = \ln(n) + \delta + \frac{1}{2n} + \frac{1}{12n^2} + \frac{\epsilon(n)}{120n^4}$

where $\forall_n 0 < \epsilon(n) < 1$ & $\delta = \text{Euler's constant} = \underline{0.577215664...}$
rationality of δ unknown!

Given all this, how many blocks do we need to make $r_1 = 100$? e^{100} a lot of blocks :)

Is greedy optimal? Yes & no - there is a counterweight tactic that matches it for blocks used. (nb: maths changes significantly if multiple blocks per stacking level are permitted)

Products: $n! = \prod_{i=1}^n i$; obviously not closed-form... but take logs...

$$\ln(n!) = \ln(1 \cdot 2 \cdot 3 \cdot \dots \cdot n)$$

$$= \ln(1) + \ln(2) + \dots + \ln(n)$$

$$= \sum_{i=1}^n \ln(i) \quad \leftarrow \text{an approx will be derived via integration bounds for increasing } \sum n$$

$$f(1) + \int_1^n \ln(x) dx \leq \sum_{i=1}^n f(i) \leq f(n) + \int_1^n \ln(x) dx$$

$$\int_1^n \ln(x) dx = (x \ln(x) - x) \Big|_1^n = n \ln n - n + 1$$

$$\therefore n \ln n - n + 1 \leq \ln(n!) \leq \ln n + n \ln n - n + 1 \leftarrow \text{then exponentiate}$$

$$n^n / e^{n-1} \leq n! \leq n^{n+1} / e^{n-1}$$

Stirling's formula: $n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n} e^{\epsilon(n)}$ where
 $\frac{1}{12n+1} \leq \epsilon(n) \leq \frac{1}{12n}$

$$\begin{aligned} 100! &\geq \left(\frac{100}{e}\right)^{100} \sqrt{200\pi} e^{1/1201} \\ &\leq \left(\frac{100}{e}\right)^{100} \sqrt{200\pi} e^{1/1200} \end{aligned} \quad \left. \vphantom{\begin{aligned} 100! &\geq \left(\frac{100}{e}\right)^{100} \sqrt{200\pi} e^{1/1201} \\ &\leq \left(\frac{100}{e}\right)^{100} \sqrt{200\pi} e^{1/1200} \end{aligned}} \right\} \text{stirling bounds are extremely tight}$$

$$n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

Asymptotic Notation

We've already seen $\sim$ hide: $f(x) \sim g(x)$ if $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$

Big-O: $f(x) = O(g(x))$ if $\lim_{x \rightarrow \infty} \left| \frac{f(x)}{g(x)} \right| < \infty$ (i.e. finite)

$$f(x) \leq O(g(x)); f(x) \text{ is } O(g(x)); \underline{f(x) \in O(g(x))}$$

formal, rarely used

Theorem: Let $f(x) = x$, $g(x) = x^2$, then $f(x) = O(g(x))$

$$\lim_{x \rightarrow \infty} \frac{x}{x^2} = 0, \text{ which is less than infinity}$$

Theorem: Let $f(x) = x^2$, $g(x) = x$, then $f(x) \neq O(g(x))$

$$\lim_{x \rightarrow \infty} \frac{x^2}{x} = \infty$$

Is $x^2 = O(10^6 x)$? No! Take limits, don't trust big constants! Is $10^6 x^2 = O(x^2)$? Yes, for some reason: $\lim_{x \rightarrow \infty} \frac{10^6 x^2}{x^2} < \infty$
 $x^2 + 100x + 10^3 = O(x^2)$

Theorem: $x^{10} = O(e^x)$

Proof: $\lim_{x \rightarrow \infty} \frac{x^{10}}{e^x} = 0$

Big-O notation tells you about the relationship between input size & running time in an algorithm.

Is $4^x = O(2^x)$? No: $\lim_{x \rightarrow \infty} \frac{4^x}{2^x} \rightarrow 2^x$

Is $10 = O(1)$? Yes

$H_n = \ln n + \delta + O(1/n)$

$H_n - \ln n - \delta = O(1/n)$ ← the technically correct way to write it; very easy to have sloppy notation

Big-O is not a lower bound. $f(x) \geq O(g(x))$ is meaningless

The correct asymptotic notation for an upper bound is Ω .

$f(x) = \Omega(g(x))$ if $\lim_{x \rightarrow \infty} \left| \frac{g(x)}{f(x)} \right| > 0$

Theorem: $f(x) = O(g(x))$ iff $g(x) = \Omega(f(x))$

$x^2 = \Omega(x)$, $2^x = \Omega(x^2)$, $x/100 = \Omega(100x + 25)$

$T(n) = \Omega(n^2)$ says "the running time is at least n^2 "

$f(x) = O(g(x))$ if $\lim_{x \rightarrow \infty} \left| \frac{g(x)}{f(x)} \right| > 0 \text{ \& } < \infty$

Theorem: $f(x) = \Theta(g(x))$ if $f(x) = O(g(x))$ & $f(x) = \Omega(g(x))$

Examples: $10x^3 - 20x + 1 = O(x^3)$

$$x/\ln x \stackrel{?}{=} O(x)$$

$$\lim_{x \rightarrow \infty} \frac{x/\ln x}{x} = 1/\ln x = 0 \quad \therefore x/\ln x \neq O(x)$$

$T(n) = O(n^2)$ means $\uparrow$ is guaranteed (both upper & lower bound) to grow quadratically in n

Summary (up to constant factors)

O means $\leq$

Ω means $\geq$

Θ means $=$

o means $<$ $f(x) = o(g(x))$ if $\lim_{x \rightarrow \infty} \left| \frac{f(x)}{g(x)} \right| = 0$

ω means $>$ $f(x) = \omega(g(x))$ if $\lim_{x \rightarrow \infty} \left| \frac{f(x)}{g(x)} \right| = \infty$

Examples: $x/\ln(x) = o(x)$; $x/100 = O(x)$; $x^2 = \omega(x)$

False proof: Let $f(n) = \sum_{i=1}^n i$. Then $f(n) = O(n)$

By induction on n ; $P(n)$ is that $f(n) = O(n)$

Base case: $f(1) = 1 = O(n)$

Inductive step: $P(n) \Rightarrow f(n) = O(n)$

$$f(n+1) = f(n) + (n+1)$$

$$= O(n) + O(n) = 2O(n) \Rightarrow O(n)$$

Flaw: hypothesis is treating $f(n)$ as a function but it's creating a scalar! Never use asymp. notation in inductive proofs!

LECTURE 14: Divide & Conquer Recurrences

T_n is the minimum number of moves to complete a Hanoi game of n discs

$$T_1 = 1$$

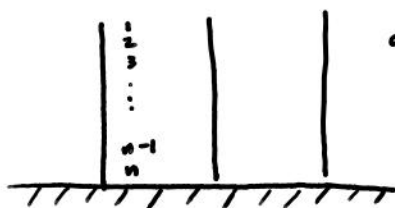
$$T_2 = 3$$

$$T_3 = 7$$

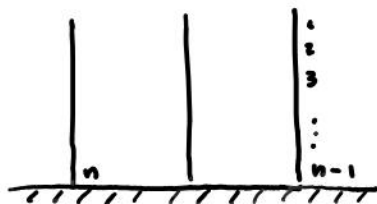


Note that we can solve Hanoi recursively: $T_n \leq 2T_{n-1} + 1$

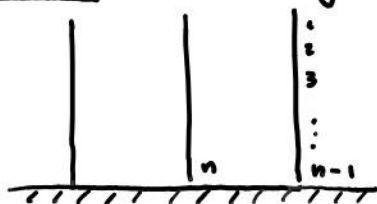
Phase 1



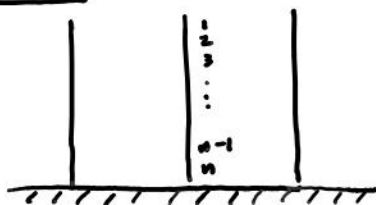
after T_{n-1}
steps
 $\Rightarrow$



Phase 2: Move Largest Disc (1 step)

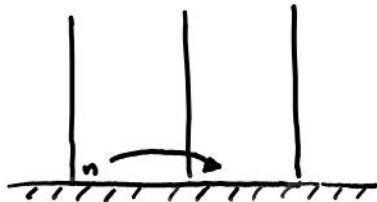


Phase 3: Move Substack (T_{n-1} steps)



$$T_n \leq 2T_{n-1} + 1$$

Note that this is an upper bound algorithm - it's not a proof of optimality. We need to find a lower bound.



For the lowest disc move to be valid, we must have taken no fewer than T_{n-1} steps already. Then the big disc moves (1 step), and we're left with a minimum of T_{n-1} steps left. So $T_n = 2T_{n-1} + 1$. How do we calculate recurrences? What is T_{64} ?

Method 1: Guess and verify

For T_{64} we might guess $T^{n-1} - 1$ and then verify by induction. $P(n)$ is $T_n = 2^{n-1} - 1$

Base case: $n=1$, $T_1 = 2^1 - 1 \checkmark$

Inductive step: $T_{n-1} = 2^{n-2} - 1$

$$\begin{aligned} T_n &= 2T_{n-1} + 1 \\ &= 2(2^{n-2} - 1) + 1 \\ &= 2^{n-1} - 1 \checkmark \end{aligned}$$

So $T_{64} = 2^{63} - 1$ - a very large number!

Method 2: Expansion

$$T_n = 1 + 2T_{n-1}$$

$$= 1 + 2(1 + 2T_{n-2})$$

$$= 1 + 2 + 4T_{n-2}$$

$$= 1 + 2 + 4(1 + T_{n-3})$$

$$= 1 + 2 + 4 + 8(T_{n-3})$$

$\therefore$ (A pattern has emerged)

$$= 1 + 2 + 4 + 8 + \dots + 2^{i-1} + 2^i T_{n-i}$$

$$= 1 + 2 + 4 + 8 + \dots + 2^{n-2} + 2^{n-1} \cancel{T_1}$$

$$= 2^n - 1$$

Let's apply this to a more interesting recurrence:

Merge Sort! To sort $n > 1$ $x_1, x_2, \dots, x_n$ (where n is a power of 2)

1) sort $x_1, x_2, \dots, x_{n/2}$ & $x_{n/2+1}, \dots, x_n$ recursively

2) merge

Example: Sort $\{10, 7, 23, 5, 2, 4, 3, 9\}$

1) sort $\{10, 7, 23, 5\}$ & $\{2, 4, 3, 9\}$

$\hookrightarrow \{5, 7, 10, 23\}$ $\hookrightarrow \{2, 3, 4, 9\}$

2) merge: look at first entries in both lists

and compare: $\{5, 7, 10, 23\}$
(remove after success) $\{2, 3, 4, 9\}$

$\{2, 3, 4, 5, \dots\}$

How many comparisons do we have to perform per merge? $\underline{n-1}$ ← because last item never needs comparison

Obviously we need to dive down to make this valid or it's just bubble sort!

Let $T(n)$ = # comparisons used by merge sort in worst case

merging takes $n-1$ comparisons, $2T(n/2)$ comparisons for recursive layer.

$$\therefore T(n) = 2T(n/2) + n - 1; \quad T(1) = 0$$

$$T(2) = 1, \quad T(4) = 5, \quad T(8) = 17, \quad T(16) = 49$$

Doesn't look like a good candidate for guess & verify
so we'll try expansion

$$T(n) = n - 1 + 2T(n/2)$$

$$= n - 1 + 2(n/2 - 1 + 2T(n/4))$$

$$= n - 1 + n - 2 + 4T(n/4)$$

$$= n - 1 + n - 2 + n - 4 + 8T(n/8)$$

$$= n - 1 + n - 2 + n - 4 + 8T(n/8)$$

} don't collapse terms! want to see patterns

we can guess that pattern looks like

$$T(n) = n - 1 + n - 2 + n - 3 + n - 4 + \dots + n - 2^{i-1} + 2^i T(n/2^i)$$

$$= n - 1 + n - 2 + \dots + n - 2^{\log n - 1} + 2^{\log n} T(1)$$

$$= \sum_{i=0}^{\log n - 1} (n - 2^i) = \sum_{i=0}^{\log n - 1} n + \sum_{i=0}^{\log n - 1} -2^i = n \log n - (2^{\log n} - 1)$$
$$= \underline{n \log n - n + 1}$$

