[2/4/25 - 1ST CLASS - PROOFS]

PROOF: method of ascertaining the truth
→ experiment, evidence, experts, jury trial, statistical analysis

MATHEMATICAL PROOF: verification of a proposition ★ by a chain of logical deductions (next lec.) from a base set of axioms ★

→ **PROPOSITION:** statement that is true or false (ex: $1=1$, ice is cold, i can fly, etc.)
-NOT proposition: "i will pass this class", "this statement is false." ← self-referential (breaks all)

→ **PREDICATE:** statement whose truth depends on a variable
→ "$n+n^2+41$ is prime" (predicate) ↗
→ "for $n=1$, n^2+n+41 is prime" (proposition)
→ ex: $\forall n \in \mathbb{N}$, n^2+n+41 is prime (proposition)

"for all" (universal quantifier)
"in"
"the natural numbers" (set of non-neg #)
* 0 is natural # in this class!

n	n^2+n+41	prime?
0	41	✓
1	43	✓
2	47	✓
⋮	⋮	⋮
39	1601	✓
40	$1681 = 41^2$	✗
41	$41^2+41+41$	✗

ex: "$a^4+b^4+c^4=d^4$ has no pos. integer solution - T or F?"
- conjectured by Euler (1769)
- disproved by Noam Elkies (1987)
  - $a=95800$, $b=217519$, $c=414560$, $d=422481$

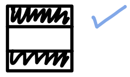
* took over 200 yrs to solve

* to refute $\forall$, just need to find one incorrect

ex: Goldbach's conjecture: every even # > 2 is sum of 2 primes
→ **CONJECTURE:** not sure if true
- $20=13+7$

ex: Poincare's conjecture: prove that rabbits are spheres (things can be deformed into other things w/o tears)
- solved! by grigori p.

ex: Four color theorem: regions in map can be colored in 4 colors such that adjacent regions have diff. colors
→ there is a map w/ at least 3 regions for which 2 colors are enough



→ three colors enough for all maps

→ 5-color theorem proved in 1800s
→ 4-color theorem proved in 1976 via theorem-proving software

PROPOSITIONS from propositions: combine w/ logical operators
→ NOT, AND, OR, XOR, IMPLIES, IF

A	B	$A \land B$ A and B	$A \lor B$ A or B	"exclusive or", $\oplus$ A xor B	A implies B	A iff B	"exclusive and" A xand B
T	T	T	T	F	T		T
T	F	F	T	T	F		F
F	T	F	T	T	T		F
F	F	F	F	F	T		T

Ex: window or aisle ? → XOR
→ can only get one or other

Ex: coffee or tea? → NAND
→ one or the other or none
→ just not both

"to be xor not to be?"

A	not A
T	F
F	T

IMPLIES: "A implies B", "$A \Rightarrow B$", "$A \rightarrow B$"
→ if A is T, B should be T
→ if not A, don't worry about B → will be T

RULE: if wed, then wear pink

wed: T	Pink: T	✓
T	F	✗
F	T	✓
F	F	✓

← rule doesn't apply today

SET: collection of objects
- → order doesn't matter
- → no duplicates

ex: $A = \{6, 1, 2, 0\} = \{6, 1, 2, 0, 0\} = \{2, 1, 6, 0\}$

$\mathbb{N} = \{0, 1, 2 \ldots\}$

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3 \ldots\}$

$\mathbb{Q}$ = rationals

$\emptyset$ = empty set = $\{\}$

$B = \{2, \{3, 4\}, \emptyset\}$ ← NOTE: 3 is <u>NOT</u> element of B. it is in a set in B

SET NOTATION:

$\exists$ = "there exists"

$x \in A$ "x is element of A"

$x \notin A$ "x NOT element of A"

$A \subseteq B$ "A subset of B" (every element in A is also in B)

union: $A \cup B$ (elements in either)

intersection: $A \cap B$ (elements in both)

set difference: $A \setminus B$ or $A - B$ (in A but not B)

set builder notation: elements of a set which satisfy predicate

$\{n \in \mathbb{N} \mid isprime(n)\} = \{2, 3, 5, 7 \ldots\}$

QUESTIONS:

$\emptyset \in B$? ✓ → in B!

$\emptyset \subseteq B$? ✓

$\emptyset \subseteq A$? ✓

→ $\emptyset$ is subset of every set b/c there's nothing in it

$\emptyset \in A$? ✗ → not in A

$A \cup B = \{6, 1, 2, 0, \{3, 4\}, \emptyset\}$

$A \cap B = \{2\}$

$A \setminus B = \{6, 1, 0\}$

★ $\{1, 2, 3, 4\} \setminus \{1, \{3, 4\}\} = \{2, 3, 4\}$

AXIOM: proposition we assume is true

ex: for every point p & line ℓ, with $p \notin \ell$, $\exists$ unique line ℓ' through p parallel to ℓ (Euclidean geo.)

→ set of axioms is <u>consistent</u> when you <u>CANT prove false = true</u>

→ set of axioms is <u>complete</u> when <u>every true proposition can be proved from axioms</u>

[2/6/25 - LECTURE 2 - CONTRADICTION + INDUCTION]

* be suspicious when ppl use absolute terms

LOGICAL DEDUCTION: combine true statements w/ other true statements

→ modius ponens: $((P \to Q) \text{ and } P) \to Q$

P	Q	((P → Q) and P) → Q				
T	T	T	T	T	T	T
T	F	F	F	T	T	F
F	T	T	F	F	T	T
F	F	T	F	F	T	F

$((P \to Q) \text{ and } \overline{Q}) \to \overline{P}$ not

$((P \to Q) \text{ and } (Q \to R)) \to (P \to R)$

$(\overline{P} \to \text{False}) \to P$

* state proved props. you're using

* can rely on high school reasonable axioms

FUNDAMENTAL PROOF TECHNIQUES:

PROVING $\exists$ (there exists):

THM: $\exists n \in \mathbb{N}.$ (n is prime and $n > 10$)

PF: 11 is prime and > 10 ☺

THM: $\exists x \in S.\ P(x)$

PF: we'll show that [some value] works. This value is in S b/c [reasons] and P(x) is true b/c [reasons].

PROVING $\forall$ (for all):

THM: $\forall x \in \mathbb{R}.\ x^2 - 6x > -10$

PF: suppose x is real #. ← introduce generic example (give it a name)

$(x^2 - 6x + 9) = (x-3)^2 \geq 0$ b/c squares are ≥ 0

so $x^2 - 6x \geq -9 > -10$ $\square$ ← indicates proof is done!

PROVING $P \to Q$, direct:

THM: if $\underbrace{n \text{ is multiple of } 10}_{P}$, then $\underbrace{n \text{ is a mult. of } 2}_{Q}$

PF: assume P; wts Q   solve/look for

assume n is mult. of 10: $n = 10k$ for some int k

$n = 2 \cdot \underbrace{(5k)}_{\text{int}}$, so n is mult. of 2. ü

PROVING $P \to Q$, contrapositive:

$P \to Q$ is equivalent to $\bar{Q} \to \bar{P}$

THM: $\forall n \in \mathbb{Z}\ (n^2 \text{ even}) \to (n \text{ even})$

PF: suppose $n \in \mathbb{Z}$ PF by contrapositive:

assume $\bar{Q}$; wts $\bar{P}$

assume n is odd; WTS n^2 is odd

$n = 2k+1$ for some $k \in \mathbb{Z}$

$n^2 = 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$

= odd ✓

PF by CONTRADICTION: "indirect pf"

IDEA: show P is not false

TECHNIQUE: to prove P, start by assuming P. then, find a contradiction i.e. some other start Q that is both T & F, conclude P = true

*won't usually know what the contradiction is until you see it - let the thm guide you.

THM: $\sqrt{2}$ is irrational

PF: pf by contradiction: assume $\sqrt{2}$ is rational.

so $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}, b \neq 0$, and $\frac{a}{b}$ in lowest terms i.e. a & b have no common factors > 1

$2 = \frac{a^2}{b^2} \to 2b^2 = a^2 \to a^2$ is even

a is even $\to a = 2k$ for some $k \in \mathbb{Z}$

$2b^2 = 4k^2 \to b^2 = 2k^2$

$\to b^2$ is even $\to$ b is even

So, both a & b have 2 as a factor this contradicts a/b being in lowest terms =x=

so $\sqrt{2}$ is not rational. ü

*look @ high-level proof outline first before looking @ terms

THM: $\forall n \in \mathbb{Z}$. n is fooish iff n+1 is bacsome

PF: suppose $n \in \mathbb{Z}$

$P \leftrightarrow Q$ means $P \to Q$ & $Q \to P$

WTS (n fooish) → (n+1 barsome)

(n+1 barsome) → (n fooish)

first assume n is fooish [WTS: n+1 is barsome]

instead, assume n+1 is barsome [WTS: n+1 is fooish]

common proof outline - letting theorems tell you what evidence they need

be skeptical of ...'s

THM: $\forall n \in \mathbb{N}.\ 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

n=0: $0 = 0(1)/2$ +1

n=1: $1 = 1(2)/2$ +2

n=2: $1+2 = 2(3)/2$ +3

n=3: $1+2+3 = 3(4)/2$ +4

n=4: $1+2+3+4 = 4(5)/2$ +5

n=5: $1+2+3+4+5 = 5(6)/2$

n $1 + 2 + \ldots + n \overset{?}{=} n(n+1)/2$

n+1 $1 + 2 + \ldots + n + (n+1) \overset{?}{=} (n+1)(n+2)/2$

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

$$\frac{n}{2} + 1 \overset{?}{=} \frac{n+2}{2} \checkmark$$

if row n, then row n+1

INDUCTION PRINCIPLE: ok!

if $P(0)$ and $\forall n \in \mathbb{N}.\ P(n) \rightarrow P(n+1)$

then $\forall n \in \mathbb{N}.\ P(n)$ ← we will only use for natural #'s.

$P(n) := 1+2+\ldots+n = n(n+1)/2$

THM: $\forall n \in \mathbb{N}.\ P(n)$ ← predicate

PF by induction, using $P(n)$.

BASE CASE: WTS $P(0)$: $0 = 0(1)/2$ ✓

INDUCTIVE STEP: suppose $n \geq 0$ and assume $P(n)$; WTS $P(n+1)$.

*induction hides details by design.

you must do ~~we did:~~	you get for free ~~we want:~~
$P(0)$	$P(0)$
$P(0) \rightarrow P(1)$	$P(1)$
$P(1) \rightarrow P(2)$	$P(2)$
$P(2) \rightarrow P(3)$	$P(3)$
$P(3) \rightarrow P(4)$	$P(4)$
	$P(5)$
⋮	⋮

★ part of checklist that person needs to go through

assume $1+2+\ldots+n = n(n+1)/2$

WTS $1+2+\ldots+n+(n+1) = (n+1)(n+2)/2$

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

$$= \frac{(n+1)(n+2)}{2} \text{ by algebra}$$

by induction, we conclude $P(n)$ is true for every $n \geq 0$

[2/11/25] - lecture: casework + strong induction

EX: $2^n \times 2^n$ garden grid

- 1 statue in middle cell
- cover remaining cells w/ L-trominoes

etc...

$P(n) :=$ it is possible to fill whole $2^n \times 2^n$ garden (except statue in middle) with L-trominoes

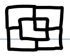
$Q(n) :=$ solve $2^n \times 2^n$ with one statue anywhere ← gives you more "power" (can choose anywhere)

$P(0)$: 1x1 ✓ □ (no work to do)

$P(1)$: 2x2

✓

$P(2)$: 4x4



✓

$P(3)$: 8x8 ← think of it as 4 seperate 4x4 cases

*induction is useful for iterative, repetitive things. all you have to explain is going from one step to the others

- set up so that it doesn't get repetitive
- inductive proof has strong relationship w/ recursion

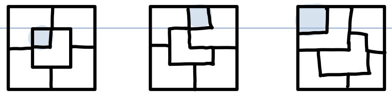
How To KNOW when to strengthen P to Q?

- takes practice, experience, cleverness
- you just need to know how to write proof.

$Q(0)$ ✓

$Q(1)$ ✓

$Q(2)$ ✓



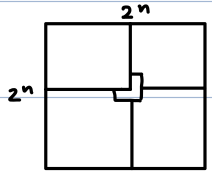
$Q(3)$

$Q(4)$

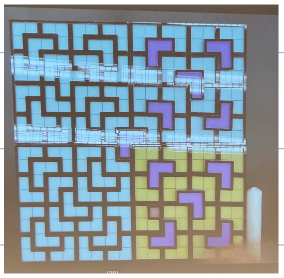
$Q(n-1) \rightarrow Q(n)$

assume we know how to solve $2^{n-1} \times 2^{n-1}$ minus one cell.

WTS:



by $Q(n-1)$, can fill in each quadrant (w/o the missing cell)



can also do an 8-row truth table (2^3)

PROOF BY CASES:

THEOREM: P is true.

PF by cases on the truth value of C:

CASE 1: assume C is true. then P is true b/c...

CASE 2: assume C is false. then P is true b/c...

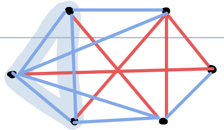
THM: $(A \rightarrow B)$ or $(B \rightarrow C)$ is always true.

PF by cases: B is either true or false.

CASE 1: B is true. then $A \rightarrow B$ is true.

CASE 2: B is false. then $B \rightarrow C$ is true. so formula is still true.

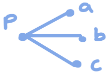
EX: 6 ppl, each pair either friends or strangers (goes both ways)



THM: there will always be 3 ppl who are all friends or all strangers

PF: pick a single person p. thus p either has ≥ 3 friends or not.

CASE 1: p has ≥ 3 friends



case 1a: some pair of a, b, c are friends
- then p and these 2 form a triangle

case 1b: a, b, c are all strangers
- then a, b, c is a red triangle

CASE 2: p has <3 friends, aka p has ≥ 3 strangers
by same argument as case 1 (with white & red swapped)
∃ white or red △ ü

Since one of case 1 or 2 must happen, the theorem holds.

* cases must be exhaustive (include all possible)

PF. by cases, general form:

THM: P is true

PF by cases:

case 1: assume C_1. then P is true b/c...
case 2: assume C_2. then P is true b/c...
⋮
case k: assume C_k. then P is true b/c...

at least one of $C_1, C_2, \dots C_k$ must be true b/c... ——
(aka, $C_1, \dots, C_k$ are exhaustive)

*need to check that possibilities are exhaustive, even if the cases are thousands.

Axiom of Induction:

If P(n) is a predicate defined over $n \in \mathbb{N}$,
If P(0) is true, and
for all $n \geq 0$, $(P(n) \rightarrow P(n+1))$ is true,
Then P(n) is true for all $n \in \mathbb{N}$

* induction is unrolling and proving more P(n)

P(0)	P(0)
P(0) → P(1)	P(1)
P(1) → P(2)	P(2)
P(2) → P(3)	P(3)
P(3) → P(4)	

* in principle, only ever need strong induction

Axiom of STRONG Induction:

If P(n) is a predicate defined over $n \in \mathbb{N}$,
If P(0) is true, and
for all $n \geq 0$, $(P(0) \wedge P(1) \wedge P(2) \wedge \dots \wedge P(n)) \longrightarrow P(n+1)$
Then P(n) is true for all $n \in \mathbb{N}$

*get to make more assumptions (more help)

PF. by strong induction
BASE CASE: P(0) is true b/c... ——
IND. STEP: assume P(0), P(1), P(2), ..., P(n) are all true
WTS: P(n+1)

* can be strong induction even we just use P(n)

EX: start w/ a stack of n blocks. repeatedly find a stack w/ k > 1 and split into two piles p, q with total size p+q=k, earning p·q points.

~~8~~
4, ~~4~~ → 16 points
~~4~~, 3, 1 → 3 points
2, 2, ~~3~~, 1 → 4 pts
~~2~~, ~~2~~, 2, 1, 1 → 2 pts
1, 1, 1, 1, 1, 1, 1, 1 → 1+1+1

28 points

8
1, 7 → 7 points
1, 1, 6 → 6
1, 1, 1, 5 → 5
1, 1, 1, 1, 4 → 4
1, 1, 1, 1, 1, 3 → 3
1, 1, 1, 1, 1, 1, 2 → 2
1, 1, 1, 1, 1, 1, 1, 1 → 1

28 points

* will always get 28 pts. no matter how you split!

GUESS: stack of size n always yields $\underbrace{1+2+\dots+(n-1)}_{\frac{(n-1)(n)}{2}}$ pts

THM: stack of size n always yields $1+2+\ldots+(n-1)$ pts $\frac{(n-1)(n)}{2}$

* VARIABLES must be defined:
$\forall x \in \mathbb{R} (\cdots)$
$\exists y \in \mathbb{R} (\cdots)$
$P(n) :=$ talk about n

PF. by strong induction

$P(n) :=$ a stack of size n always yields exactly $\frac{(n-1)(n)}{2}$ points

we'll prove $\forall n \in \mathbb{N}.\ P(n)$
or: $\forall n \geq 1.\ P(n)$

BASE CASE: $P(1)$ is true b/c stack of size 1 gives $\frac{(0)(1)}{2} = 0$ pts ✓

*can show $P(n-1) \rightarrow P(n)$ or $P(n) \rightarrow P(n+1)$, whichever is easier.

Assume $P(1), P(2), \ldots, P(n-1)$. (assume $n \geq 2$) ← rewrite in context

WTS: $P(n)$

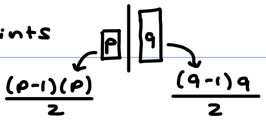
Assume size k pile (for every $1 \leq k \leq n$) gives $\frac{(k-1)(k)}{2}$ points.

WTS: size n pile always gives exactly $\frac{(n-1)(n)}{2}$ points

WE DO	WE GET
$P(1)$	
$P(1) \rightarrow P(2)$	
$(P(1) \wedge P(2)) \rightarrow P(3)$	
$(P(1) \wedge P(2) \wedge P(4)) \rightarrow P(4)$	

start with pile of size $n \geq 2$.

say first move is $p+q=n$, earning $p \cdot q$ points



using all assumptions b/c don't know size

we'll earn $\frac{(p-1)(p)}{2}$ & $\frac{(q-1)(q)}{2}$

total: $pq + \frac{(p-1)(p)}{2} + \frac{(q-1)(q)}{2}$ pts

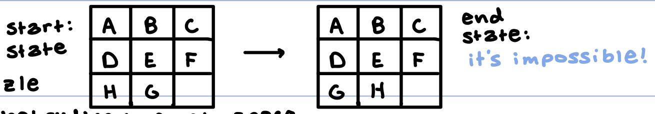
$\Big\}$ algebra

$\frac{(p+q-1)(p+q)}{2} = \frac{(n-1)(n)}{2}$ ✓

[2/13/25] - lecture 4 - state machines

STATE MACHINE: a state machine is defined by a collection of states, a specified initial state, and for each state s, a set (possibly empty) of possible transitions to other states.

EX: the 8 puzzle



it's impossible!

·horizontal/vertical sliding in empty space

states: (D A B E F E C H G *) i.e. all permutations of these 9 symbols
← empty

initial: (A,B,C,D,E,F, H,G, *)

transitions: steps according to the game

* an execution of a state machine is a sequence of states, starting @ initial state, following transitions.

$S_0 \rightarrow S_1 \rightarrow S_2 \rightarrow \ldots \rightarrow S_k \rightarrow S_{k+1} \rightarrow \ldots$ can stop when needed, or have infinite
initial

a state is reachable if it is part of some execution

PRESERVED PREDICATE: a predicate $P(\cdot)$ defined on states, such that for every state $s \rightarrow t$, if $P(s)$ is true, then $P(t)$ is true. ← steps after preserved states will be & stay true.
- similar to induction

EX state predicate: "A in top left"
→ not preserved b/c A does not always stay in top left

preserved property = preserved predicate

INVARIANT: state predicate that is true for all reachable states only if the property is true in start state.

invariant principle → THM: if P is a preserved property and P(initial state) is true, then P is invariant.

IDEA: find a state property P such that:
- P(A B C D E F H G *) is true] invariant (reachable state)
- P is preserved
- P(A B C D E F G H *) is false (unreachable state)

INVERSION: in a list, an inversion is a pair of entries such that the larger entry has a smaller index in the list.

EX: [2, 5, 3, 4, 1] 1 & 4, 5 & 4,

thm. statement,
but stepping stone

LEMMA: when swapping two unequal adjacent elements of a list, the # of inversions changes by ±1.

PF: $[a_1, \ldots, a_{k-1}, \overbrace{a_k, a_{k+1}}, \ldots, a_n]$
$[a_1, \ldots, a_{k-1}, \underbrace{a_{k+1}, a_k}, \ldots, a_n]$

* only 1 pair of elements whose relative order has changed

only (a_k, a_{k+1}) changes their relative order.

if $a_k < a_{k+1}$, # inversions increase by 1

if $a_k > a_{k+1}$, # inversions decrease by 1 □

P(S) := remove *, count #inversions, true if odd.

P(ABCDEFHG *) = # inversions $(\text{ABCDEF}\underbrace{\text{HG}}_{1})$ is odd ✓ true

P(ABCDEFGH *) = 0 × false

PF through state machines

EX: CLAIM: P is preserved.

PF: suppose we have a transition $s \to t$,

and assume P(S) is true. WTS: P(t) is true.

DABFECH*G
DABFECHG*

CASE 1: $s \to t$ is a horizontal slide
this just swaps * with letter next to it. so after removing *, lists are same.

By P(S), #inversions of the list was odd.

Still true for t, since reduced list didn't change.

CASE 2: $s \to t$ is a horizontal slide.

DABFECH*G
DABF*CHEG

* moves to other side of 2 symbols

—— xyz —— 2 adjacent swaps

—— yxz —— so #invs changes by ±1, ie by 2,0,2 ← over 2 swaps

—— yzx ——

since odd for s, add + {0, 2, -2} is still odd, so odd for t.

$s \to t$ must be horizontal or vertical, so cases are exhaustive.

since P(init) is true & P is preserved, by invariant principle, P is invariant.

.... since ... unreachable, ...

DEF: a state machine terminates if there are no infinite executions.

DEF: a final state is a state w/ no outgoing transitions

DEF: a derived variable is a function mapping states to numbers.

DEF: a derived variable f is strictly decreasing when for every $s \to t$, $f(s) > f(t)$
weakly decreasing : ≥

IF f is a derived variable s.t.:
- f(s) is always in $\mathbb{N}$
- f is strictly decreasing

then the state machine terminates after at most f(initial state) steps.

ex: f = 17 @ state 0 strictly decr.

$S_0 \longrightarrow S_1 \longrightarrow S_2 \longrightarrow S_3 \longrightarrow \underset{\smile}{S_4}$ ← f can't go lower than 0, and it can also end.

17 15 14 11 4

SIMPLE SORT:

list of n distinct integers

EX: $\underbrace{2\ \ 1}\ \ 5\ \ 3\ \ 4$

$1\ \ 2\ \ \underbrace{5\ \ 3}\ \ 4$

$1\ \ 2\ \ 3\ \ \underbrace{5\ \ 4}$

$1\ \ 2\ \ 3\ \ 4\ \ 5$

STATES: permutations of those integers.

TRANSITIONS: $(a_1, a_2, \dots, a_n)$

if $a_i > a_{i+1}$, can transition to $(a_1, \dots a_{i+1}, a_i, \dots, a_n)$

CLAIM: always terminates on a sorted list.

if no more moves possible, then list is sorted.

$(a_1, \dots, a_n)$ w/ no moves available means $a_1 < a_2 < \dots < a_n$ } sorted list ✓

so # steps is $\leq$ f(initial state)

worst case: every pair is inverted,

in which #invs is $\frac{(n-1)(n)}{2}$

$f(a_1, \dots, a_n)$ = # inversions

f has values in $\mathbb{N}$: yes.

f is strictly decreasing: in fact, f decreases by exactly 1 on every step.

[2/20/25] - lecture 5 - sums (closed forms)

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + \dots + n^2$$

QUESTION: is an mit degree worth more than a Harvard degree?

Ⓗ

year 1	\$1	$= \$(1+p)^{n-1}$
year 2	\$2	$= \$2(1+p)^{n-2}$
year 3	\$3	$= \$3(1+p)^{n-3}$
⋮	⋮	
year n	\$n	$\forall n$

total earnings after n years: $H_n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Ⓜ

year 1	\$1
year 2	\$1.3
year 3	$\$(1.3)^2 = 1.69$
⋮	⋮
year n	$\$(1.3)^{n-1}$

$\forall n$ $x = 1.3$

total earnings after n years: $M_n = \sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}$

HOW TO FIND ANSWER?

TOOL 1: **PERTURBATION METHOD**

$H = 1 + 2 + \dots + n$

$H = n + (n-1) + (n-2) + \dots + 1$ n+1 n+1

$2H = (n+1) + (n+1) + \dots + (n+1) = n \cdot (n+1)$. so $\boxed{H = \frac{n(n+1)}{2}}$

n = 10: \$55

n = 20: \$210

n = 30: \$465

n = 40: \$820

$M = 1 + x + x^2 + \dots + x^{n-1}$

$x \cdot M = \quad x + x^2 + \dots \dots + x^n$ ← shifted

$(x-1)M = x^n - 1$ so $\boxed{M = \frac{x^n - 1}{x - 1}}$??

✗

n = 10: \$42

n = 20: \$630

n = 30: \$8729

n = 40: \$120393

POINT: \$1 is worth > \$1 tomorrow (w/o rate p) 2.5%

\$1 year 1 = $\$(1+p)$ in year 2

$= \$(1+p)^2$ in year 3

$= \$(1+p)^{n-1}$ in year n

$$\sum_{k=0}^{n-1} x^k = \frac{1-x^n}{1-x}$$

$$\sum_{k=1}^{n} x^k = \frac{1-x^{n+1}}{1-x} \qquad \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \qquad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

total earnings $T = \sum_{i=1}^{n} i(1+p)^{n-i} = (1+p)^n \sum_{i=1}^{n} i(1+p)^{-i}$ ← call $\frac{1}{1+p} = y$

$$= y^{-n} \underbrace{\sum_{i=1}^{n} i y^{i}}_{=S}{}^{:=S} = y^{-n} S$$

$$S = y + 2y^2 + 3y^3 + \dots + ny^n$$
$$yS = \phantom{y+{}} y^2 + 2y^3 + \dots + (n-1)y^n + ny^{n+1}$$

$$(1-y)S = y + y^2 + y^3 + \dots + y^n - ny^{n+1}$$
$$= y(1 + y + y^2 + \dots + y^{n-1}) - ny^{n+1}$$
$$= y\frac{y^n - 1}{y-1} - ny^{n+1} = \frac{y - (n+1)y^{n+1} + ny^{n+2}}{(1-y)} \longrightarrow \boxed{S = \frac{y-(n+1)y^{n+1} + ny^{n+2}}{(1-y)^2}}$$

TOOL 2: ANSATZ METHOD (guess & check)

can calculate these!

$$S = \sum_{i=1}^{n} i^2 \overset{\text{guess}}{=\!=} an^3 + bn^2 + cn + d = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$

$n=0$: $0 = d$

$n=1$: $1 = a+b+c+d$

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

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

$\Big\}$ $a = \frac{1}{3}$, $b = \frac{1}{2}$, $c = \frac{1}{6}$

the formula works for $n = 0-3$, but must use induction to prove for rest

$\frac{n^3}{8} \le S \le n^3$ guesses!

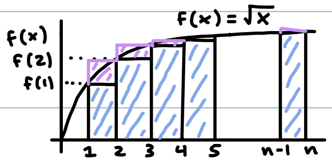
$$S \ge \left(\frac{n}{2}\right)^2 + \left(\frac{n}{2}+1\right)^2 + \dots + n^2$$
$$\ge \left(\frac{n}{2}\right)^2\left(\frac{n}{2}\right) = \frac{n^3}{8}$$

$f(x) = \sqrt{x}$

$$S = \sum_{i=1}^{n} \sqrt{i} \approx \int_1^n x\,dx = \left[\frac{2}{3}x^{3/2}\right]_1^n = \frac{2}{3}(n^{3/2} - 1)$$

" $f(1) + f(2) + \dots + f(n)$

$S \sim \frac{2}{3}n^{3/2}$



$f: \mathbb{R}^+ \to \mathbb{R}^+$ weakly increasing if $y > x$, $f(y) \ge f(x)$

*NEED TO CHECK:
- ·is f positive
- ·is f weakly incr.

blue: $f(1) + f(2) + \dots + f(n-1) \le \int_1^n f(x)\,dx := I$ ← sum of strips is @ most sum under curve

where $S = \sum_{i=1}^{n} f(i)$

(upper bound) $S - f(n) \le I$

$S \le I + f(n)$

$I = \int_1^n f(x)\,dx$

purple: $f(2) + f(3) + \dots + f(n) \ge I$

$S - f(1) \ge I$

$S \ge I + f(1)$ ← lower bound

putting lower & upper bound together: $I + f(1) \le S \le I + f(n)$ when f is positive & weakly increasing

★ $\frac{2}{3}(n^{3/2} - 1) + 1 \le S \le \frac{2}{3}(n^{3/2} - 1) + \sqrt{n}$

$\frac{2}{3}n^{3/2} - \frac{1}{3}$ $\quad = \frac{2}{3}n^{3/2} + \sqrt{n} - \frac{2}{3}$ ← relative error shrinks as n increases

DEF: $f \sim g$ means that $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$

$$S(n) = \frac{2}{3}n^{3/2} + s(n)$$
$$\lim \frac{S(n)}{\left(\frac{2}{3}n^{3/2}\right)} = \lim \frac{2/3\,n^{3/2} + s(n)}{\frac{2}{3}n^{3/2}} = 1 + \lim \frac{\sqrt{n} - 2/3}{2/3\,n^{3/2}} = 1$$

EX: $S = \sum_{i=1}^{n} \frac{1}{\sqrt{i}}$ $\quad f(i) = \frac{1}{\sqrt{i}}$

weakly incr. $g(i) = f(n+1-i)$ ← flipped

$$\sum_{i=1}^{n} g(i) = \sum_{i=1}^{n} f(i) = S$$

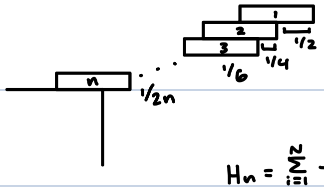
$I + g(1) \le S \le I + g(n)$

$I + f(n) \le S \le I + f(1)$

$$\int_1^n g(x)\,dx = \int_1^n f(x)\,dx$$

$I + f(n) \le S \le I + f(1)$ when f is positive & weakly decreasing.

[2/25/25]-lecture 6 - SUMS (cont.) & ASYMPTOTES



n blocks → overhang = $\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \dots + \frac{1}{2n}$

$= \frac{1}{2}\left(\sum_{i=1}^{N} \frac{1}{i}\right) = \frac{1}{2} H_n$ ← nth Harmonic number (sum of reciprocals)

$H_n = \sum_{i=1}^{N} \frac{1}{i}$

SUMS:

$I_n = \int_1^n \frac{1}{x}\,dx = [\ln x]_1^n = \ln n$

$I_n + f(n) \le H_n \le I_n + f(1)$ // INTEGRAL BOUND

how far you can go for n blocks → $\ln n + \frac{1}{n} \le H_n \le \ln n + 1$

- 2007 paper
- "overhang"
- mike peterson
- n blocks → $\sqrt[3]{n}$ overhang

(from lec. 5): $f \sim g$ means $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$ ← f(n) is asymptotically equivalent to g(n) precisely when $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$

but.. doesn't tell us how fast

THM: $H_n \sim \ln n$

PROOF: $\lim_{n\to\infty} 1 + \cancelto{0}{\frac{1}{n\ln n}} \le \lim_{n\to\infty} \frac{H_n}{\ln n} \le \lim_{n\to\infty} 1 + \cancelto{0}{\frac{1}{\ln n}}$

$\boxed{\lim_{n\to\infty} \frac{H_n}{\ln n} = 1}$ (squeeze theorem) ← squeezed by 1 on top & bottom

$f: \mathbb{N} \to \mathbb{R}^+$

f overhang ≥ 10

→ $H_n \ge 20$

$\sim \ln \ge 20$

$n \ge e^{20}$

PRODUCTS:

$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n$ ← how to approximate for products? integrals are for sums. → write product as sums!

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

$S = \sum_{i=1}^{n} \ln i$

$I = \int_1^n \ln x\,dx = [x\ln x - x]_1^n = n\ln n - n + 1$

$I + f(1) \le S \le I + f(n)$ ← $\ln n$

$(n\ln n - n + 1) + 0 \le S \le (n+1)\ln n - n + 1$ ← $n\ln n - n + 1 + \ln n$

$(e^{n\ln n - n + 1}) \le e^S \le e^{(n+1)\ln n - n + 1}$

$\underset{n^n}{(e^{\ln n})^n} \cdot e^{-n} \cdot e^1 \le e^S \le n^{n+1} \cdot e^{-n} \cdot e$ ★ review maff. $e^{\ln n} = n$

$\frac{n^n}{e^{n-1}} \le \underset{n!}{\underset{\shortparallel}{e^S}} \le \frac{n^{n+1}}{e^{n-1}}$

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

THM [rate] $e^{\frac{1}{12n+1}} \le \frac{n!}{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n} \le e^{\frac{1}{12n}}$

ASYMPTOTICS:

simple sort/swapsort:

$n, n-1, n-2, \dots 1$
$n-1, n-2, n-3, \dots, 1, n$ } & so on

#swaps $\le (n-1) + (n-2) + \dots + 1$

$S(n) = \frac{n(n-1)}{2} = \underset{\substack{\uparrow \\ \text{grows faster}}}{\frac{n^2}{2}} - \frac{1}{2}$ worst case

merge sort:

$M(n) \le \underbrace{n\log_2 n}_{\text{grows faster}} - n + 1$

★ only care about large terms

- ignore small n // focus on large n
- ignore lower-order terms
- ignore constant factors

→ $6 \cdot \frac{n^2}{2}$ instructions

→ $420 \cdot \frac{n^2}{2}$ clock cycles

→ $\frac{420\ n^2/2}{5\times10^9}$

incr	5 cycles
cmp	15 cycles
r/w	100 cycles

BIG-O NOTATION:

NOTATION: $f(n) \in O(g(n))$ "$f(n) \le g(n)$ with caveats"

DEF: $f(n) \in O(g(n))$ means $\exists n_0.\ \forall n \ge n_0\ \ f(n) \le cg(n)$. ← Fine as long as constant apart

$\xcancel{f(n) = O(g(n))}$

NEVER WRITE THIS! not equal.

EX: $n \in O(n^2)$? YES → n is at most n^2 for $n > 1$ ✓

$n \le n^2$

EX: $n^2 \notin O(n)$? ← negation of statement ✓

$\forall c\ \forall n_0\ \exists\ n \ge n_0\ \ n^2 > cn$

EX: $\underset{f(n)}{5n} \in O(\underset{g(n)}{2n})$ ← constants don't matter! ✓

$c = \frac{5}{2}$ $5n \le \frac{5}{2} \cdot 2n$

THM: $f, g : \mathbb{N} \to \mathbb{R}^+$

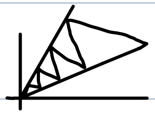
if $\lim_{n\to\infty} \frac{f(n)}{g(n)}$ exists, $= \infty$ $f(n) \notin O(g(n))$

if $\lim_{n\to\infty} \frac{f(n)}{g(n)}$ exists, $< \infty$ $f(n) \in O(g(n))$

if $\lim_{n\to\infty} \frac{f(n)}{g(n)}$ doesn't exist, inconclusive

works for some problems

EX: $f(n) = \begin{cases} 5n, & n \text{ odd} \\ 7n, & n \text{ even} \end{cases}$



$f(n) \in O(\underset{\shortparallel\, g(n)}{n})$? $g(n) = n$

$\lim_{n\to\infty} \frac{f(n)}{g(n)}$ DOES NOT EXIST! does not converge to a single # (keeps switching)

$f(n) \in O(g(n))$ ✓

$f(n) \le 7n$ ✓ ← for all n, f(n) less than 7n

★ try to use thm, if doesn't work, find another way.

$f \sim g$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$ ← asymptotically equivalent
$f \in O(g)$	$\exists c > 0 \;\; \exists n_0 \ge 0 \;\; \forall n \ge n_0 \;\; f(n) \le c g(n)$
$f \in \Omega(g)$	$g \in O(f)$ ← g(n) "at least" f(n)
$f \in \Theta(g)$	$f \in O(g)$ and $g \in O(f)$ ← f & g grow about same, up to constant factors
$f \in o(g)$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$ ← f grows much slower than g
$f \in \omega(g)$	$g \in o(f)$ ←

MIDTERM: lectures up to today, warm ups, psets,
- like psets but shorter
- ~ 90 mins
- cheat sheet 1sided

[2/27/25] - lecture - ASYMPTOTICS & RECURRENCES

ASYMPTOTIC NOTATION:		MEANING
1. $f \sim g$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$	"$f \approx g$ up to lower order terms
2. $f \in O(g)$	$\exists c > 0.\ \exists n_0 \ge 0 \ \forall n \ge n_0 \ \ f(n) \le c \cdot g(n)$	"$f \le g$ up to lower order & constant factors
3. $f \in \Omega(g)$	$g \in O(f)$	"$f \ge g$...
4. $f \in \Theta(g)$	$f \in O(g)$ and $f \in \Omega(g)$	"$f \approx g$...
5. $f \in o(g)$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$	"$f \ll g$..
6. $f \in \omega(g)$	$g \in o(f)$	"$f \gg g$...

$$\begin{tikzcd}
& f \sim g \arrow[d, Rightarrow] & \\
& f = \Theta(g) \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & \\
f = O(g) & & f = \Omega(g) \\
f = o(g) \arrow[u, Rightarrow] & & f = \omega(g) \arrow[u, Rightarrow]
\end{tikzcd}$$

$f \sim g \Leftrightarrow \lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$

$f = O(g) \Leftrightarrow \exists c > 0.\ \exists n_0 \ge 0, \forall n \ge n_0, f(n) \le c \cdot g(n)$

$f \sim g$ implies $f = O(g)$, but NOT other way around

★ — how is this diff?

THM: $2^n \in O(1)$

PROOF: Base: $n=1$: $2^1 = 2 = O(1)$ ✓

INDUCTION: suppose for $n \Rightarrow 2^n \in O(1)$.
w.t prove it for $n+1$
$2^{n+1} = 2^n + 2^n \in O(1) + O(1) = O(1)$

proved that $\exists n \;\; 2^n \in O(1)$ ← for every n, $\overset{\text{constant}}{2^n}$ is a constant

$\shortparallel$

$\forall n \; \exists c \ldots \; 2^n \le c$

but we wanted to prove:

$\exists c \; \forall n \;\; 2^n \le c$

order...

RECURRENCE: sequence of numbers defined inductively

1, 2, 3, 4... $T_i = T_{i-1} + 1$

1, 1, 2, 3, 5... $F_i = F_{i-1} + F_{i-2}$ → $F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$ ← check w/ induction

EX: TOWERS OF HANOI RECCURENCE CALL: 3 blocks

$[1]_{AC} = 1_{AC}$ // 1 move

$[1,2]_{AC} = 2_{AB}, 1_{AC}, 2_{BC}$ // 3 moves ← this is recurrence!

$[1,2,3]_{AC} = [2,3]_{AB}, 1_{AC}, [2,3]_{AC}$ // 7 moves

$[1,2,3,4] = [2,3,4]_{AB}, 1_{AC}, [2,3,4]_{BC}$

ALGORITHM (recursive):

$[1,2,\dots n]_{AC}$:

- $[2,3,4,\dots,n-1]_{AB}$
- 1_{AC}
- $[2,3,4,\dots,n-1]_{BC}$

$T(1) = 1$

$T(2) = 3$

$T(3) = 7$

$T(4) = 15$

$T(5) = 31$

$T(n) = 2T(n-1) + 1$ describes runtime of tower of hanoi

$T(n) = 2^n - 1$ "guess & check"

EX: SORTING

SELECTION SORT: GIVEN NUMBERS:

- find smallest #
- pull it out
- repeat

$$S(n) = (n-1) + (n-2) + \dots + 1 = \frac{(n-1)n}{2} = \frac{n^2}{2} - \frac{n}{2} \in \Theta(n^2)$$

MERGE PROCEDURE:

have sorted lists A & B

want: combine into single sorted list

2-finger algorithm

- compare smallest elements in each list
- pull out smaller of the two
- continue until a list becomes empty
- put the non-empty list @ the end.

MERGE SORT: input list with n numbers

- if $n=1$ → done
- sort the first $\left[\frac{n}{2}\right]$ elements using merge sort
- sort the next $\left[\frac{n}{2}\right]$ elements using merge sort
- merge

*induction for algorithms

$\text{Time}_{merge} = n-1$

worst-case #comparisons in mergesort w/ n elements // say $n = 2^k$

$$M(n) = M\left(\frac{n}{2}\right) + M\left(\frac{n}{2}\right) + (n-1)$$

$$= 2M\left(\frac{n}{2}\right) + (n-1)$$

base case $M(1) = 0$

$1 + 2 + 4 + \dots + 2^{k-1} = 2^k - 1$

$$M(n) = 2M\left(\frac{n}{2}\right) + (n-1)$$

$$= 2\left(2M\left(\frac{n}{4}\right) + \left(\frac{n}{2} - 1\right)\right) + (n-1) = 4M\left(\frac{n}{4}\right) + (n-2) + (n-1) \dots$$

⋮

$$= (n-1) + (n-2) + (n-4) + \dots + (n - 2^{k-1}) + 2^k \cdot \cancel{M(1)}$$

0

$$= kn - \left(1 + 2 + 4 + \dots + 2^{k-1}\right)$$

$2^k - 1$

$$= kn - 2^k + 1$$

$$= n\log_2 n - n + 1$$

lower order terms

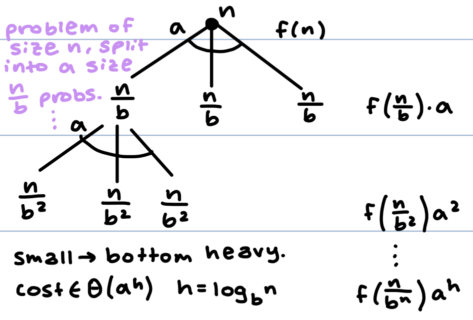
$n = 2^k$

$k = \log_2 n$

$$= \Theta(n \log n)$$

n	1	2	4	8	6
Sel.	0	1	6	28	120
merge	0	1	5	17	49

problem of size n, split into a size $\frac{n}{b}$ probs.

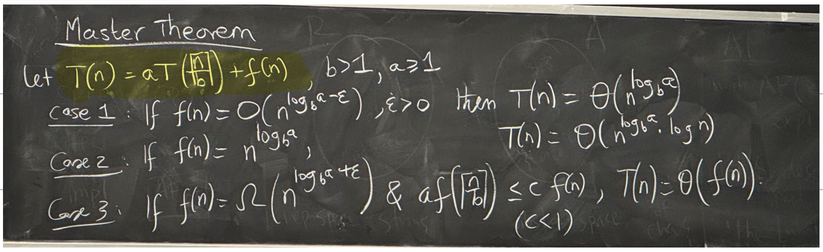


CASE 1: f(n) small → bottom heavy.

cost $\in \Theta(a^h)$ $h = \log_b n$

$= \Theta(n^{\log_b a})$

MASTER THM:



Master Theorem

let $T(n) = aT\left(\left\lceil\frac{n}{b}\right\rceil\right) + f(n)$, $b > 1$, $a \geq 1$

Case 1: If $f(n) = O(n^{\log_b a - \varepsilon})$, $\varepsilon > 0$ then $T(n) = \Theta(n^{\log_b a})$

Case 2: If $f(n) = n^{\log_b a}$, $T(n) = \Theta(n^{\log_b a} \cdot \log n)$

Case 3: If $f(n) = \Omega(n^{\log_b a + \varepsilon})$ & $af\left(\left\lceil\frac{n}{b}\right\rceil\right) \leq c f(n)$, $T(n) = \Theta(f(n))$.
$(c<1)$

← write thm in crib sheet & remember how thm came to be

MASTER THEOREM: figures out asymptotics for recurrence

$T(n) = aT(\frac{n}{b}) + f(n)$ ← recursively does a function on terms

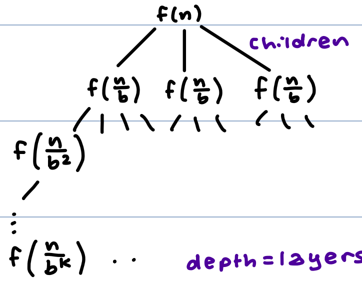
- can plug in what we know already (plug & chug method)

$T(\frac{n}{b}) = aT(\frac{n}{b^2}) + f(\frac{n}{b})$

$a^2T(\frac{n}{b}) + af(\frac{n}{b}) + f(n)$

⋮

$a^kT(\frac{n}{b^k}) + \dots$ ← keep recursing until b^k becomes n & $T(1)$ base case is met.



depth=layers of tree

[3/4/24]-lecture - DIVISIBILITY & GCD

NUMBER THEORY: study of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

DIVISIBILITY: $a|b$ "a divides b"

"only includes multiplication"

$0|0 = T$

DEF: $a|b$ iff there's an integer $k \in \mathbb{Z}$ s.t. $b = ka$

- n is even: $2|n$
- $n|0$ for all $n \in \mathbb{Z}$
- $n|-n$

PROP 1: $d|a \Rightarrow d|ca$ for all $c \in \mathbb{Z}$

PROP 2: $d|a$, $d|b \Rightarrow d|a+b$, $d|a-b$

PF: $a = k \cdot d$ for some $k \in \mathbb{Z}$, $b = k' \cdot d \Rightarrow a+b = (k+k')d \Rightarrow d|a+b$ ☐

PROP 3: $d|a$, $d|b \Rightarrow d|(sa+tb)$ $\forall s, t \in \mathbb{Z}$

PF: use prop 1: $d|sa$, $d|tb \xrightarrow[\text{prop 2}]{\text{use}} d|sa+tb$ ☐

INTEGER LINEAR COMBO (ILC) of a & b: $sa+tb$ for some $s, t \in \mathbb{Z}$

$$\overset{\text{5-gal}}{(0,} \overset{\text{3-gal}}{0)} \rightarrow (5,0) \rightarrow (2,3) \rightarrow (2,0) \rightarrow (0,2) \rightarrow (5,2) \rightarrow (4,3)$$

STATE MACHINE: $\begin{cases} x \leq a \\ y \leq b \end{cases}$ (wlog $a \geq b$. a-gal, b-gal $\xrightarrow{\text{want}}$ c-gal)

- state (x,y) means x gal in a-jug, y gal in b-jug
- final (desired) state: $(c, 0)$
- transitions:
  - $(x,y) \xrightarrow{\text{fill}} (a,y), (x,b)$
    $\xrightarrow{\text{empty}} (0,y), (0,y)$
  - $(x,y) \xrightarrow{\text{pour } 1\to 2} (0, x+y)$ if $x+y \leq b$
    $(x+y-b, b)$ otherwise $x+y > b$
  - $(x,y) \xrightarrow{\text{pour } 2\to 1} (x+y, 0)$ if $x+y \leq a$
    $(a, x+y-a)$ otherwise

$a=9$, $b=6$, $c=4$?

LEMMA: all reachable amounts are an ILC of a & b

PF: by induction

BASE CASE: $(0,0)$

IND. STEP: x, y are ILC of a&b $\Rightarrow$ $x+y$ is an ILC of a&b

$x = sa+tb$, $y = s'a+t'b \Rightarrow x+y = (s+s')a + (t+t')b$

$\Rightarrow x+y-b$ is ILC of a&b

$\Rightarrow x+y-a$

$a=5$, $b=3$, $c=4$:

$4 = 2 \cdot 5 + (-2) \cdot 3$

LEMMA: can obtain value c in water jug problem iff c is ILC of a & b and $0 \leq c \leq \max(a,b)$

CLAIM: c is ILC of a & b iff $\gcd(a,b) \mid c$.

DEF: greatest common divisor $\gcd(a,b)$ is largest integer d s.t. $d \mid a$, $d \mid b$

any int divides 0

EX: $\gcd(9,6)=3$, $\gcd(5,3)=1$, $\gcd(5,0)=5 \rightarrow \gcd(a,0)=|a|$ for all $a \in \mathbb{Z}$

$\gcd(-5,0)=5 \nearrow$

BIG IDEA
· SUBTRACTION

GCD SUBTRACTION LEMMA: $\gcd(a,b)=\gcd(a-b,b)$

LEMMA: $\gcd(a,b)=\gcd(b,a)$

$\gcd(5,3)=\gcd(2,3)=\gcd(3,2)=\gcd(1,2)=\gcd(2,1) \xrightarrow{2\times} \gcd(0,1)=1$

PF (of gcd subtraction lemma):

$S_{a,b}$ = set of all common div. of a & b

$S_{a-b,b}$ = · · · a-b & b

we will show $S_{a,b}=S_{a-b,b} \Rightarrow S_{a,b} \overset{\text{subset}}{\subseteq} S_{a-b,b}$ &

$S_{a,b} \supseteq S_{a-b,b}$

"$\subseteq$" if $g \in S_{a,b} \Rightarrow g \mid a,\ g \mid b \Rightarrow g \mid a-b$
$\Rightarrow g \in S_{a-b,b}$

"$\supseteq$" ex: QED □

$\gcd(100,1)=\gcd(99,1)=\gcd(98,1)=\ldots=\gcd(0,1)=1$

division faster LMAO

DIVISION: $\forall n \in \mathbb{Z}$, $\forall d \in \mathbb{Z}^+$ $(d>0)$ there is a unique pair (q,r) s.t.

1) $n=qd+r$ | $q = n$ div d
2) $0 \le r < d$ | $r = n$ rem d

GCD DIVISION LEMMA: if $a \ge b \ge 1$, $\gcd(a,b)=\gcd(a \text{ rem } b, b)$

PF: $a=qb+r$

$\gcd(a,b)=\gcd(a-b,b)$
$=\gcd(a-qb,b)$
$=\gcd(a \text{ rem } b, b)$ □

EUCLID'S ALGORITHM to compute $\gcd(a,b)$:

- start @ (a,b)
- states (x,y), $x \ge y \ge 0$
- transition $(x,y) \rightarrow (y, x \text{ rem } y)$
  $(x,0) \rightarrow$ return x

INVARIANT: $\forall (x,y)$ that appears in Euclid, $\gcd(x,y)=\gcd(a,b)$

PARTIAL CORRECTNESS: when terminates, outputs $\gcd(a,b)$

TERMINATION: derived variable $< x+y$

$(x \text{ rem } y)+y < x+y$ ←decr. & ends ≥ 0

better derived variable: bits(x) + bits(y) ←tracks digits

[3/11/25]-lecture - MODULAR ARITHMETIC

1. EVEN + ODD = ODD (mod 2)
2. 999 × 998 - has last digit 2 (mod 10) $9 \times 8 = 7\underline{2}$
3. currenty 2:39. in 75 hr, it's 5:39 (mod 24)
4. today is tuesday. 100 days from now... thursday (mod 7)
5. $x = 2025^{2024}$ $(2023 + 2022 \times 2021)$ - what is rem 7?

THEME: ignore multiples of n (here, 7). focus on the remainder

DEF: $a \equiv b_n$ iff $n \mid (a-b)$

(a is congruent to b mod n)

EX: $17 \equiv_5 12$? ✓

$17 \equiv_5 30$? ×

$17 \equiv_5 -3$ ✓ $17-(-3)=20$ = multiple of 3!

$[0] = \{0, \pm 5, \pm 10, \cdots\}$
$[1] = \{\cdots, -9, -4, 1, 6, \cdots\}$
$[2] = \ldots$
$[3] = \cdots$

GIVEN a number a, which congruence class does a belong to?

$a \in [a \text{ rem } 5]$ (or) $a = 5 \cdot q + r \Rightarrow a \in [r]$

THM [division thm from last class]: for every $(n,d) \in \mathbb{Z}^2$, $d>0$, there is a unique pair (q,r) such that:

1) $n = q \cdot d + r$ $\quad q = n \text{ div } d$
2) $0 \leq r < d$ $\quad r = n \text{ rem } d$ ← always ⊕

Ex: $n = 15$, $d = 7$

$$15 = \underset{q}{2} \cdot 7 + \underset{r}{1}$$

$$= 3 \cdot 7 - 6$$

THM: $a \equiv_n b$ iff $a \text{ rem } n = b \text{ rem } n$ ← need to prove if/then, & only if (2 directions)

PF: "if" $a \text{ rem } n = b \text{ rem } n$, then $a \equiv_n b$ (WANT TO PROVE)

$a = q \cdot n + r$ $\quad b = q' \cdot n + r$

same remainder

$a - b = (q - q')n \Rightarrow n \mid (a-b) \Rightarrow a \equiv_n b$

"if" $a \equiv_n b$, then $a \text{ rem } n = b \text{ rem } n$ (WANT TO PROVE)

$n \mid (a-b) \rightarrow a - b = q' \cdot n$

$a = qn + r$ ← put together

$b = a - q'n = (q - q')n + r \Rightarrow a \text{ rem } n = b \text{ rem } n = r$

$\overbrace{b = a \text{ mod } n}^{\text{THROW AWAY!}} \rightarrow b = a \text{ rem } n \rightarrow b \equiv_n a$

* can only **add, subtract, multiply** in mod. NOT divide.

THM: $a \equiv_n b$ and any integer c.

add: $a + c \equiv_n b + c$

subtract: $a - c \equiv_n b - c$

multiply: $ac \equiv_n bc$

exponentiate: $a^c \equiv_n b^c$ (w/ base)

THM: if $a \equiv_n b$, $a^c \equiv_n b^c$ for any + integer c.

PF: by strong induction on C

BASE CASE: $(c=1)$: by assumption.

IH: $a^{c-1} \equiv_n b^{c-1}$, WTS. $a^c \equiv_n b^c$

$a^c = a \cdot a^{c-1}$

$a^{c-1} \equiv_n b^{c-1}$

⇓

$a \cdot a^{c-1} \equiv a \cdot b^{c-1} \equiv_n b^c$

$a \equiv_n b \Rightarrow a \cdot b^{c-1} \equiv_n b \cdot b^{c-1} \equiv_n b^c$

WHAT DOESN'T WORK: if $a \equiv_n b$, $c^a \equiv_n c^b$

PF by counterexample: (small)

$a = 2, b = 7, c = 2 \rightarrow 2 \equiv_5 7 \qquad 2^2 \equiv_5 2^7 ? \qquad 4 \equiv_5 128$ NO!

SOLVE: $x = 2025^{2024}(2023 + 2022 \times 2021)$ - what is rem 7 - which congruence class does x belong to?

$2025 \text{ rem } 7 = 2$ ← replace w/ base

$= 2^{2024}(2023 + 2022 \times 2021)$

$2023 \text{ rem } 7 = 0$, $2022 \text{ rem } 7 = 6$, $2021 \text{ rem } 7 = 5$

$= 2^{2024}(\underbrace{0 + 6 \times 5}_{\text{rem}=2}) = 2^{2024}(2) \text{ rem } 7 = 2^{2025} \text{ rem } 7$

$2^1 \equiv_7 2$, $\quad 2^2 \equiv_7 4$, $\quad 2^3 \equiv_7 1$, $\quad 2^4 \equiv 2 \quad \ldots$

$2^{3k} \equiv_7 1$ for any integer k.

$2^{2025} \text{ rem } 7 = 2^{675 \times 3} \equiv_7 1$

DIVISION:

Ex: $3x = 3 \rightarrow x = 1$ (divide both sides by 3)

Ex: $3x \equiv_6 3$ $\quad a \cdot 2x \equiv_5 a \cdot 3 \quad x \equiv_5 a \cdot 3 \equiv_5 4$ Ⓐ

$2x \equiv_5 3$ $\quad$ want a s.t. $a \cdot 2 \equiv_5 1$

PULVERIZER THM: for any integers a & b, there are integer l.c. (s,t) s.t. $as + bt = \gcd(a,b)$.

RECAP: gcd(42,24)

linear combos

42	24	(1,0)	(0,1) $42 = 1 \cdot 42 + 0 \cdot 24$
24	18	(0,1)	(1,-1)
18	6	(1,-1)	(-1,2)
6	0	(-1,2)	———

gcd = 6

THM: a has a multiplicative inverse mod n iff $\gcd(a,n) = 1$.

DEF: multiplicative inverse of a mod n is a number $0 \le b < n$ s.t. $a \cdot b \equiv_n 1$

PF: a has multiplicative inverse mod n iff there is int b s.t. $ab \equiv_n 1$ $\quad n \mid ab-1 \leftarrow$ n divides $ab-1$

iff $n \mid (ab-1)$

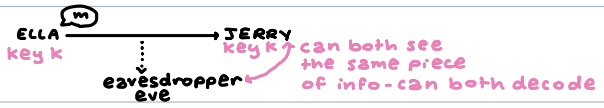
iff there is an integer q s.t. $ab - 1 = qn$

iff $1 = a \cdot b - n \cdot q$ ← b tells you inverse!

THM: if n is prime & $a \not\equiv_n 0$, then a^{-1} mod n exists $\quad$ *REVIEW WARM-UP 9 (hard)

[3/13/25] - CRYPTOGRAPHY - science of secret writing; encoding/decoding

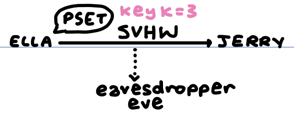
- achieving paradoxical notions
- how to communicate securely w/ someone you never met before? → public key
  - ex: website & user - 2 parties who haven't met, but still need to send info
  - go through public servers - potentially ppl eavesdropping
- how to prove a theorem w/o revealing the proof? - zero knowledge
- how to compute a function w/o revealing inputs? - secure multiparty
- made possible w/ modular arithemetic



can both see the same piece of info - can both decode

HISTORY:

- CAESAR CIPHER (A=0, B=1, etc.) - english letters mod 26
  - key k = random # in 0,...,25
  - shifts each letter by k, send ciphertext



EX:
ciphertext: VW
plaintext: H I
key = 14?

- VERNAM CIPHER (ONE-TIME PAD) - key $(k_1, \dots, k_n)$: n random #'s mod 26
  - shift by k_i for ℓ_i letter to encrypt
  - perfectly secure b/c eve doesn't know key & words can be anything
  - however, cannot send multiple msgs, or else eve will know the difference shift b/t the letters

  EX: PSET $(k_1, k_2, k_3, k_4) = (1,5,9,12)$

- ENIGMA (GERMANS)

WHAT IF ELLA & JERRY HAVE NEVER MET?

GOAL: { anyone can encode to bob
only bob can decode

IDEA:

- bob generates a key-pair: a public key & private key.
- anyone can encrypt to bob w/ public key
- only bob can decrypt w/ private key.

→ easy = $O(n^2)$ ← polynomial
→ hard = $O(10^n)$ ← exponential

FERMAT'S LITTLE THM: statement ab. when number will hit 1.

mod 7: 3^1 3^2 3^3 3^4 3^5 3^6 3^7 3^8

$\underbrace{3 \quad 2 \quad 6 \quad 4 \quad 5 \quad 1}$ 3 2

mod 7: 2^1 2^2 2^3 2^4

$\underbrace{2 \quad 4 \quad 1}$ 2

for any prime number p & a relatively prime to p, $a^{p-1} \equiv_p 1$

PF:

CLAIM: for every $i \not\equiv_p j$, $a \cdot i \not\equiv_p a \cdot j$, $a \not\equiv_p 0$

SAME AS: if $a \cdot i \equiv_p a \cdot j$, then $i \equiv_p j$

(contrapositive) $A \to B \leftrightarrow \overline{B} \to \overline{A}$

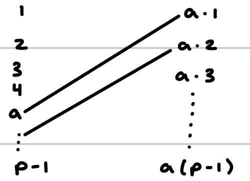
$$a^{-1} \cdot a \cdot i \equiv_p a^{-1} \cdot a \cdot j \Rightarrow i \equiv_p j$$

$$1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv_p (a \cdot 1)(a \cdot 2) \cdots (a \cdot (p-1))$$

$$\equiv_p a^{p-1}(1 \cdot 2 \cdot \ldots \cdot (p-1))$$

$$1 \equiv_p a^{p-1} \quad ▨$$

$S = \{1, 2, \ldots p-1\}$ $S = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$



$9 \cdot 2 \equiv_{18} 9 \cdot 4$

a i j

RSA ENCRYPTION: private

PRIVATE KEY: (P, Q, d)

PUBLIC KEY: (N = PQ, e)

- P-1 & Q-1 will both be even b/c P&Q relatively prime & 2 digits (2 cannot be e)

gcd(e, (P-1)(Q-1))

$d \cdot e \equiv_{(P-1)(Q-1)} 1$

ENCRYPTION OF A MESSAGE m ($0 \leq m < N$)

$c = m^e \text{ rem } N$

DECRYPTION OF CIPHERTEXT c:

$c^d \bmod n$

EX: Jerry (N = 667, e = 5)

Ella $\xrightarrow{32}$ Jerry $32 = n^5 \text{rem} 667$

Jerry: $(32)^{(d)} \text{rem} 667$

WHY DOES THIS WORK?

$c^d \equiv_p (m^e)^d \equiv_p m^{1+k(p-1)}$

$\equiv_p m \cdot \underbrace{m^{k(p-1)}}_{\text{1 by fermat}}$

$c^d \equiv_p (m^e)^d \equiv_p m^{1+k(q-1)} \equiv_q m$

$c^d \equiv_N m$

$(p-1)(q-1) \mid (e \cdot d - 1)$

$p-1 \mid (e \cdot d - 1)$

$q-1 \mid (e \cdot d - 1)$

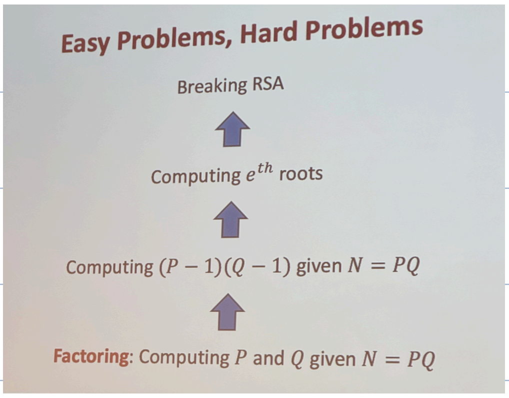
$e \cdot d - 1 = k(p-1)$

m = 2 $2^5 = 32$ $e \cdot d = 615 - 1 = 614$

p = 23, q = 29

$(p-1)(q-1) = 22 \cdot 28$

$d = 123 = 3 \cdot 41$



Easy Problems, Hard Problems

Breaking RSA

↑

Computing e^{th} roots

↑

Computing $(P-1)(Q-1)$ given $N = PQ$

↑

Factoring: Computing P and Q given $N = PQ$

HISTORY (cont):

- merkle (1974) - paper had core ideas
- diffie & hellman (1976) - public key cryptography
- rivest, shamir, adleman (1978)
- goldwasser & micali (1982) - probabilistic encryption
- RSA claimed to be invented in secret in early 1970s @ GCHQ

LECTURE 11 - GRAPHS & COLORING

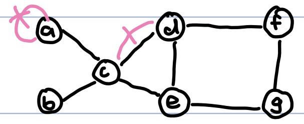
SIMPLE UNDIRECTED GRAPH: a pair (V, E) where V is a nonempty set (elements called "nodes" or "vertices") and E is a set of size 2 subsets of V.

- 2 elements must share smthg

V: {a, b, c, d, e, f, g}

E = {{a, b}, {a, c}, {b, c}, {c, d}, {d, f}, {e, g}, {f, g}}

{e, c} = {c, e} = ce = c - e



*self loops NOT allowed

*duplicate edges NOT allowed

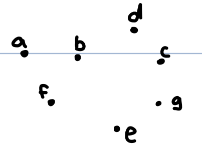
*empty V = {} NOT allowed (no vertices = no valid graph)

$\deg_G(b) = 2$

$\deg_G(c) = 4$

V= {a, b, c, d, e, f, g}

E = { } ✓ valid graph



$deg_G(c) = 0$

EXAMPLES of simple graph:
- friendship (2 ppl - friends)
- conflict graph (2 classes - conflict)
- brain (neurons / neural network)
- internet (routers talking)

NOT simple graphs (directed):
- links on website (doesn't guarentee other link links back)
- followers = directed, NOT this (they follow you, but do you follow them?)

DEF: 2 nodes A & B are **adjacent** if they're connected by an edge, i.e. $\{a, b\} \in E$

the edge $\{a, b\}$ is **incident** to a & b

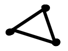
a & b = **endpoints** of $\{a, b\}$

DEF: **$deg_G(v)$** = # edges incident to v

DEGREE SEQUENCE: all node degrees in G listed

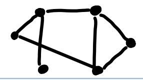
ex: (2,2,4, 3, 3, 2,2)

Q: does there exist a graph w/ degree seq (2,2,1)
- 3 vertices, two with 2 degs, one w/ 3 deg



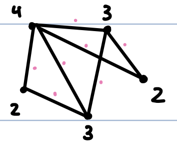
NO ×

Q: what about (2,2,2,2,2,1)?



× no b/c handshake lemma

HANDSHAKE:



edges connect 2 vert

So $\frac{\text{degree total}}{2}$ = edges = 7

HANDSHAKE LEMMA: for a graph $G = (V, E)$, $\boxed{\sum_{v \in V} deg(v) = 2|E|}$

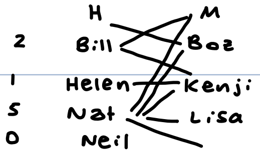
Def: $G = (V, E)$ is **bipartite** iff V can be partitioned into L & R s.t. every edge in G has one endpoint in L, one in R.

EX: AVG. # of Harvard friends for MIT undergrad vs. vice versa

MIT: H:

H = set of Harvard ugrads

M = MIT



*edges have 1 endpt on each side

(H friend has M → M will have H)

$$\sum_{h \in H} deg(h) = |E| = \sum_{m \in M} deg(m)$$

$$A_M = \frac{\sum_{m \in M} deg(m)}{|M|} = \frac{|E|}{|M|} \quad A_H = \frac{\sum_{h \in H} deg(h)}{|H|} = \frac{|E|}{|H|}$$

$\frac{A_M}{A_H} = \frac{|H|}{|M|} \approx 1.6$ (not 1 b/c more H students)

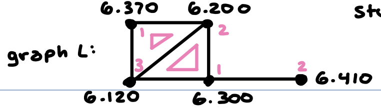
*REVIEW buildup

EX: men & women relationships: $\frac{|W|}{|M|}$ = 1.03, 3.3, 1.74, 1.75

EX: goal: schedule exams

edge {u,v} means classes u & v have student in common (conflict)

graph L:



← graph coloring problem

$\chi(L) = 3$

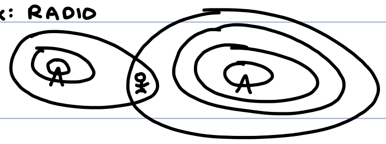
GRAPH COLORING PROBLEM: given G & K colors, want to assign a color to each node s.t. every edge has 2 distinct colors @ its endpoint.

DEF: a **proper k-coloring** of G is a function $f: V \to C$ where $|C| \leq K$ s.t. for all edges $\{u, v\} \in E$, $f(u) \neq f(v)$

DEF: **Chromatic Number** of G is smallest # of k s.t. G has a proper k-coloring, denoted by Chi $\chi(G)$

→ NEED to prove χ works & $< \chi$ does NOT work

EX: RADIO



- conflict graph
- 2 towers can't be on same frequency or else garbles

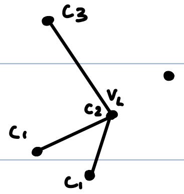
POSSIBLE COLORINGS = $(\text{\# colors})^{|V|}$

→ NP complete problem ∴

* algorithms find colorings, even if they are not optimal.

GREEDY ALGORITHM: (to color graph)

- order nodes $(v_1, \dots, v_n)$
- order colors $(c_1, c_2, c_3 \dots)$
- for each v_i in order, choose lowest color that doesn't introduce conflicts
  - greedily choose earliest color that works



* vertex order matters (algo. <u>not</u> always optimal)

\#graphs never have 0 vertices

* <u>WARNING</u>: induction on graphs is different - do proof outline

THEOREM: if every v_i has $\deg(v_i) \leq k$, then greedy algo. uses $\leq k+1$ colors.

→ try inducting on # nodes

<u>P(n)</u> := for every graph G with <u>n</u> nodes s.t. all vertices have deg ≤ k, alg. uses ≤ k+1 colors.

<u>BASE CASE</u>, P(1): graph has no edges; algo gives it 1 color. ✓ •c_1

<u>IND. STEP</u>: assume P(n), WTS P(n+1):

assume all n-vertex, max degree k graphs use ≤ k+1 colors.

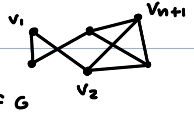
WTS all (n+1)-vertex, max degree k graphs use ≤ k+1 colors.

"Build-up error"
(not proving theorem for <u>all</u> graphs)

suppose G is an (n+1)-vertex graph where all nodes have deg ≤ k

WTS alg on G uses ≤ k+1 colors

$G = (V, E)$



$V = \{v_1, \dots, v_{n+1}\}$

define G' as subgraph of G

$G' = \left(\{v_1, \dots, v_n\} \left\{ \begin{array}{l} \text{all edges of G} \\ \text{that don't use } v_{n+1} \end{array} \right\} \right)$

all nodes in G' have deg ≤ k

so by P(n), greedy algo on G' use at most k+1 colors.

Note that alg. on G does same first n steps as alg on G'.

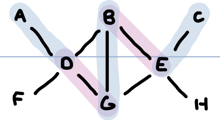
so first n steps use ≤ k+1 colors

v_{n+1} has ≤ k neighbors, so @ most k colors forbidden to v_{n+1}

Greedy algo. will use one of $c_1, c_2, \dots, c_{k+1}$ for v_{n+1} □

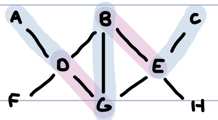
[3/20/25] - MATCHING & STABLE MATCHING

DEF: a matching in a graph G(V, E) is a subgraph in which each node has degree 1.
i.e. a subset of edges in G that have no endpoints in common.



→ a matching M is maximal if ∄ M' s.t. $M \subseteq M'$
- local max (can't choose more

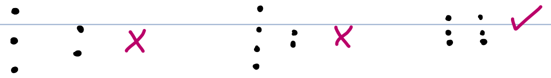
→ M is maximum if ∄ M' s.t. $|M| < |M'|$
- max # edges possible
- A-D, B-G, C-E



- RED matching is maximal, not maximum
- BLUE matching is maximal & maximum-3
  - → if a matching w/ 4 edges, would need to use all nodes
  - → there isn't 4 edge (A & F can't both have D)

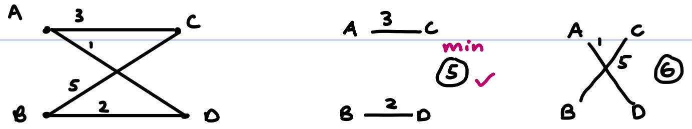
bipartite matching - finding max matches in a graph
- planes & terminals
- servers & tasks (each can only do some tasks)
- dating websites (binary hetero.)

perfect matching: size |V| / 2 (use all pairs)
- both sides must have equal vertices



DEF: weighted graph is a graph G = (V, E) together with function w: E → R

MIN / MAX weighted matching problem:
- find a perfect matching M w/ min/max total weight, $\sum_{e \in M} w(e)$

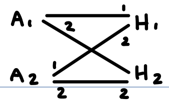


5<6 → better!

→ brute force for this is not possible
→ unlike color theory, this has an efficient algo!

MAX MATCHING: find a maximum matching
- min/max weight perfect paths
- have efficient algos! can get perfect

STABLE MATCHING PROBLEM:



diagonals:
A_1 - H_2
A_2 - H_1

however, A & H_1 prefer each other

* if applicant a & evaluator e both prefer each other over their assigned partners in some perfect matching M, then (a, e) is rogue pair, & M is called unstable.

is it possible to make matching stable?

→ if both don't want each other (there is a "better" match)

Ex: n applicants, n evaluators

each applicant specifies full ranking of all n evaluators, vice versa.

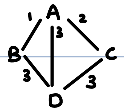
GOAL: find perfect matching that is stable

→ does a stable matching exist? how can we find one? how fair is it?

YES!

what if graph isn't bipartite? just ppl rating each other

→ no stable matching exists. (symmetric)



→ imagine: D prefers & matches w/ A.

(D, A), (B, C)

rogue pair

→ no stable matching no matter what.

→ for BIPARTITE: stable matching always exists

aka "deferred acceptance"

GALE-SHAPLEY ALG: (stable matching alg)

EACH DAY:

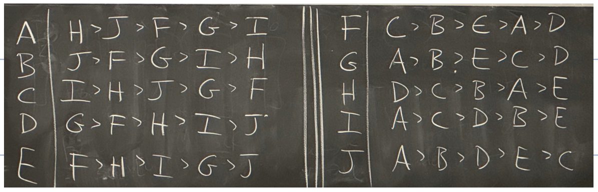
- **MORNING:** applicant applies to favorite evaluator that hasn't rejected them
- **EVENING:** evaluators rejects all except current favorite applicant (tentative).
- if nothing changes (no rejections), stop.

* applicant starts w/ fav & goes down

eval starts w/ worse & goes up!

EX:

EVALUATORS: APPLICANTS:



A	H > J > F > G > I	F	C > B > E > A > D
B	J > F > G > I > H	G	A > B > E > C > D
C	I > H > J > G > F	H	D > C > B > A > E
D	G > F > H > I > J	I	A > C > D > B > E
E	F > H > I > G > J	J	A > B > D > E > C

PROVE:

- algo finishes
- algo stable
- algo provides perfect matchings

DAY	1:	2:	3:	4:
A	G, I, J	J	J	J
B	none	G	G, F	F
C	F	F, I	I	I
D	H	H	H	H
E	none	none	none	G

all matched!

claim GS algo finishes quickly & returns perfect matching that is stable.

- check stable: go through pairs & make sure they aren't rogue pairs

THM: G.S. terminates by day n^2+1

PF: consider # of uncrossed out prefs on app. preferences

this is strictly decr. derived var. w/ values in $\mathbb{N}$

starts @ n^2

@ most n^2 steps possible

LEMMA: $\forall a \in A, \forall e \in E$, if e has rejected a ever, then e has an applicant they like better than a.

- each evaluator's choices get better over time.

PF: e only ever trades up.

THM: GS ends up w/ perfect matching.

PF: if not, some applicant a rejected by all n evaluators.

every evaluator thus has some applicant they like better than a.

n evals, n-1 applicants other than a. contradiction! ✓

CLAIM: the G.S. perfect matching is stable

PF: by way of contradiction. BWOC, assume M is not stable, so it has a rogue pair (a, e) $\{a, e\} \in M$, so consider: did e ever reject a, or did they never meet?

CASE 1: e rejected a
then e is matched with someone better than a,
so e doesn't want to run away w/ a.
so (a, e) is not rogue

CASE 2: if a & e never met
then a has their fav. eval that hasn't rejected them.
so a is happier with their current match than w/ e.

DEF: a & b are feasible partners if ∃ a stable w/ (a, e).

DEF: participant p's optimal match is their most preferred feasible partner.

DEF: participant p's pessimal match is their least possible feasible partner.
-not necessarily last

THM: G.S. matching gives every applicant their optimal match.
and finally, gives each evaluator their pessimal match.

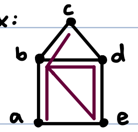
[4/1/25]-lec

RECALL: simple undirected graph $G = (V, E) \leftarrow \subseteq \{ \{u, v\} \mid u, v \in V + u \neq v \}$ → only 1 edge b/t $\{u, v\}$ & no "self-loops" $\{u, u\}$

WALKS "walk" from v_0 to v_k is sequence of vertices
$(v_0, v_1, \ldots, v_k)$ s.t. $\{v_i, v_{i+1}\} \in E$
length is k (# edges)

*k can be 0 (allow walks of 0)

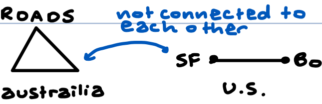
Ex:



a b d e b d c ← length=6
→ NOT a path tho

def: **PATH** is a walk with no repeated vertices. a, b "connected" if ∃ walk from a to b
- may not be most efficient, but not repeating

EX: ROADS



GRAPH PROPERTIES:
- **REFLEXIVE:** A is connected to itself
- **SYMMETRIC:** A connected to B iff B connected to A
- **TRANSITIVE:** A connected to B & B connected to C implies A connected to C

"6 degrees of seperation": all pairs of ppl are connected by @ most 6 hops

CONNECTED COMPONENT of V: subgraph induced $V' = \{u \in V \mid u, v \text{ connected}\}$ some walk b/t them
$E': \{(u, v) \in E \mid u, v \in V'\}$
- if all of G is connected, only 1 connected → G
- no node can be in 2 connected components (then you need to connect total)

EX: ROADS

sydney NOT adjacent, but IS connected.

~ 2 connected components distinct

THM: if there is a walk from a to b, there is a path from a to b.

PROOF: take shortest walk from a to b.

$a = v_0, v_1, \dots, v_K = b$

must be a path.

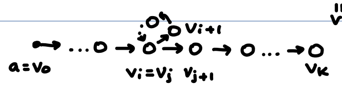
assume not a path (BY CONTRADIC)

then ∃ vertex that appears twice $i \neq j$

$v_i = v_j$, $i < j$ (note $j - i > 0$)

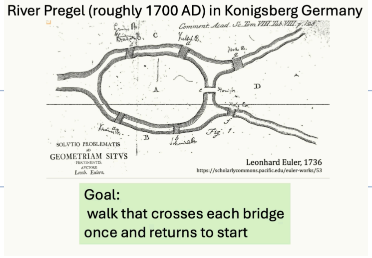
$a = v_0, v_1, \dots v_i, \overbrace{v_{i+1}, \dots, v_j}, v_{j+1}, \dots v_K$ $\overset{}{v_j} = v_i$

taking the blue parts away, path is shorter



Contradicts "shortest walk"

BRIDGES OF KONIGSBERG: goal to walk & cross each bridge once & get back to start.

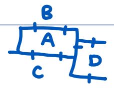

River Pregel (roughly 1700 AD) in Konigsberg Germany

Comment. Acad. Sc. Tom VIII. Tab. VIII. p. 128.

SOLVTIO PROBLEMATIS
AD
GEOMETRIAM SITVS
PERTINENTIS.
AVCTORE
Leonh. Eulero.

Leonhard Euler, 1736
https://scholarlycommons.pacific.edu/euler-works/53

Goal:
walk that crosses each bridge once and returns to start



def: walk is "closed" if begins & ends @ same vertex

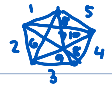
def: cycle is closed walk

1) length ≥ 3  X
2) no repeated vertices  X

def. a closed walk is a "Eulerian tour" if it uses every edge exactly once & visits every vertex 

def. graph is Eulerian if has Eulerian tour

→ every vertex must have even degree



Ex: postman

THM: G is connected & G has Euler tour $\overset{\text{iff}}{\Leftrightarrow}$ all degrees even

PF: Euler tour W

PROVE connected & Euler tour → degrees even

let $v \in V$. every time W enters V, leaves V on next step

#departures = # arrivals

each departure/arrival is on distinct edge,

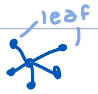
W visits all edges → degree of $v = \#dep(v) + \#arr(v) = 2 \cdot \#dep(v)$

⋮

prove other direction ←

TREES:

- connected
- acylic (no cycles)
- any tree w/ n vertices has n-1 edges (induction)



Ex: phone trees
sorting
ancestry

LEAF = any vertex with degree = 1

- deleting leaf from tree → it's still a tree

LEAF LEMMA: every tree with $n \geq 2$ vertices has ≥ 2 leaves

* tree w/ 100 vertices must have @ least 2 leaves

PF: take longest path $v_0, v_1, \dots, v_K$

@ least 1 edge $(K \geq 1)$, so $V_K = 1 V_0$

CLAIM: $V_0 + V_0$ leaves

PF BY CONTRA: if not, v_0 connects to some w other than v_1

if $w \in \{v_2, \dots, v_K\}$ then cycle (contrad.)

if NOT, then $w\ v_0, v_1, \dots v_K$ is longer (contra.)

[4/3/25] - DIGRAPHS & DAGS

TREES: connected, acylic (no cyles) graph

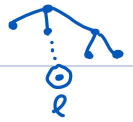
LEAF: vertex of deg = 1

- **LEAF LEMMA:** every tree w/ n≥2 vertices has at least 2 leaves

TREE PRUNING: for any leaf ℓ in tree T, T-ℓ is also a tree

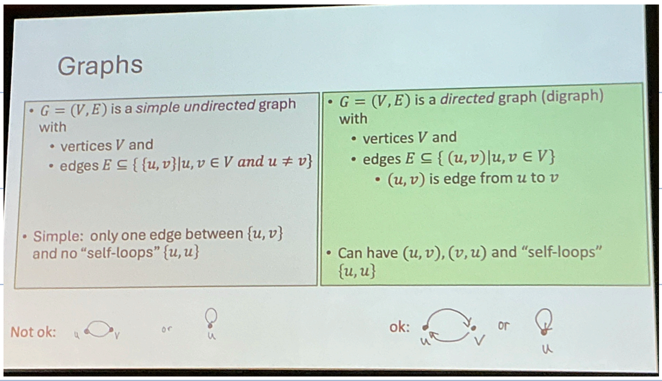
TREE SIZE: tree w/ n vertices has n-1 edges

- pf by induction:
  - BASE CASE: n = 2 → 1 edge
  - IND. STEP: assume true for n ≥ 2
    - given tree T w/ n+1 vertices:
      - by leaf lemma, T has leaf ℓ
      - by pruning, T-ℓ is also tree on n nodes
      - by ind. hypo, T-ℓ has n-1 edges
      - adding back leaf ℓ & its adjacent edge gives T w/ n edges



DIRECTED GRAPHS:

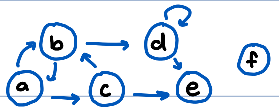
EX: one way vs. 2 way roads
insta (following) vs. facebook (friends)



Graphs

- $G = (V, E)$ is a *simple undirected* graph with
  - vertices V and
  - edges $E \subseteq \{ \{u, v\} | u, v \in V \text{ and } u \neq v\}$
- Simple: only one edge between $\{u, v\}$ and no "self-loops" $\{u, u\}$

- $G = (V, E)$ is a *directed* graph (digraph) with
  - vertices V and
  - edges $E \subseteq \{ (u, v) | u, v \in V\}$
    - (u, v) is edge from u to v
- Can have $(u, v), (v, u)$ and "self-loops" $\{u, u\}$



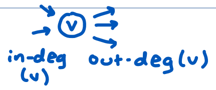
V = {a, b, c, d, e, f}

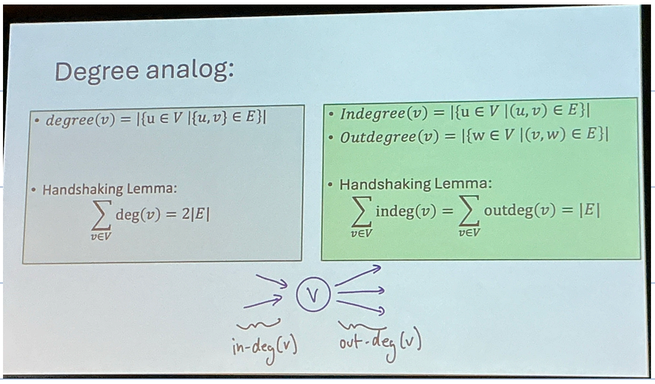
E = {(a, b), (b, a), (a, c), (c, b), (b, d), (d, d), (d, e), (c, e)}

(a to b) (self loop)

INDEGREE(v) = |{u∈V | (u, v) ∈ E}|

OUTDEGREE(v) = |{w∈V | (v, w) ∈ E}|





Degree analog:

- $degree(v) = |\{u \in V\ |\{u, v\} \in E\}|$
- Handshaking Lemma:

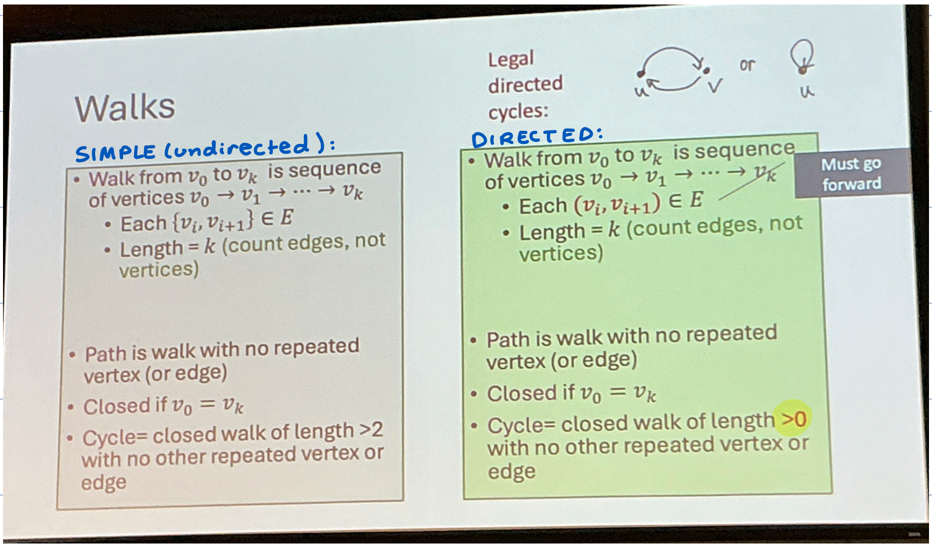
$$\sum_{v \in V} \text{deg}(v) = 2|E|$$

- $Indegree(v) = |\{u \in V\ |(u, v) \in E\}|$
- $Outdegree(v) = |\{w \in V\ |(v, w) \in E\}|$
- Handshaking Lemma:

$$\sum_{v \in V} \text{indeg}(v) = \sum_{v \in V} \text{outdeg}(v) = |E|$$

HANDSHAKE LEMMA (directed):

$$\sum_{v \in V} \text{indeg}(v) = \sum_{v \in V} \text{outdeg}(v) = |E|$$



Walks

SIMPLE (undirected):

- Walk from v_0 to v_k is sequence of vertices $v_0 \to v_1 \to \cdots \to v_k$
  - Each $\{v_i, v_{i+1}\} \in E$
  - Length = k (count edges, not vertices)
- Path is walk with no repeated vertex (or edge)
- Closed if $v_0 = v_k$
- Cycle= closed walk of length >2 with no other repeated vertex or edge

Legal directed cycles:

DIRECTED:

- Walk from v_0 to v_k is sequence of vertices $v_0 \to v_1 \to \cdots \to v_k$
  - Each $(v_i, v_{i+1}) \in E$
  - Length = k (count edges, not vertices)
- Path is walk with no repeated vertex (or edge)
- Closed if $v_0 = v_k$
- Cycle= closed walk of length >0 with no other repeated vertex or edge

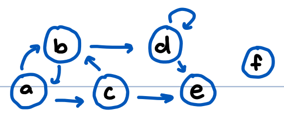
Must go forward

→ can have cycles of length >0 in directed

✓ (self-loops allowed)

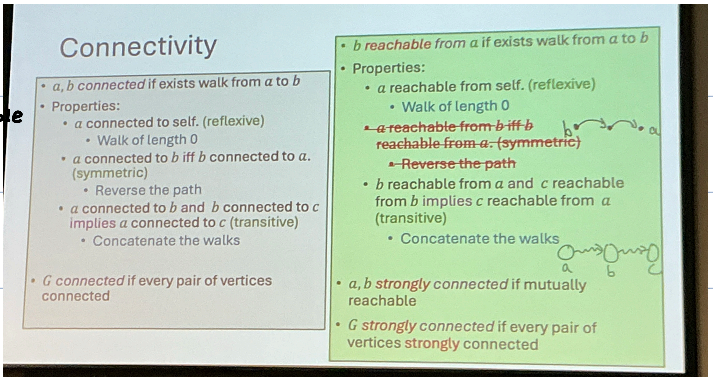
✓

CONNECTIVITY:



- b, c, d reachable from a | a not reachable from d
- unlike undirected graph,
  - not symmetric
  - not reversible
  - transitive!

- {a, b}, {b, c} & {a, c} strongly connected



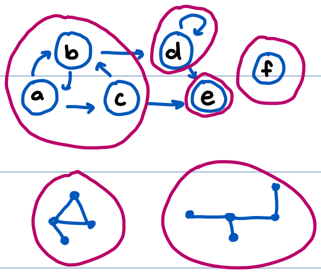
Connectivity

- *a, b connected* if exists walk from *a* to *b*
- Properties:
  - *a* connected to self. (reflexive)
    - Walk of length 0
  - *a* connected to *b* iff *b* connected to *a*. (symmetric)
    - Reverse the path
  - *a* connected to *b* and *b* connected to *c* implies *a* connected to *c* (transitive)
    - Concatenate the walks
- *G connected* if every pair of vertices connected

- *b reachable* from *a* if exists walk from *a* to *b*
- Properties:
  - *a* reachable from self. (reflexive)
    - Walk of length 0
  - ~~*a* reachable from *b* iff *b* reachable from *a*. (symmetric)~~
    - ~~Reverse the path~~
  - *b* reachable from *a* and *c* reachable from *b* implies *c* reachable from *a* (transitive)
    - Concatenate the walks
- *a, b strongly connected* if mutually reachable
- *G strongly connected* if every pair of vertices strongly connected

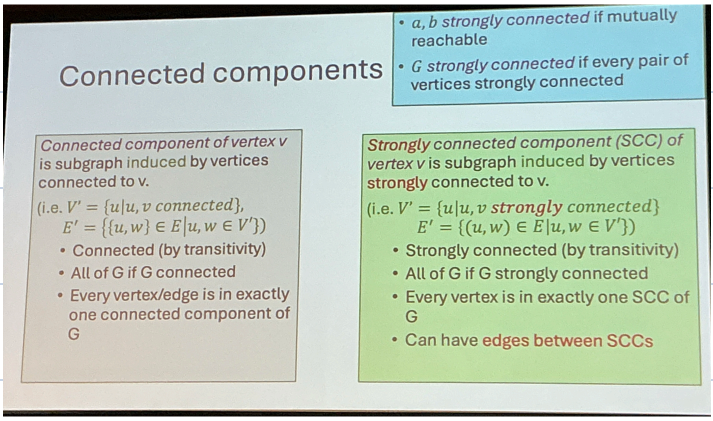
STRONGLY CONNECTED:

- a, b (vertices) strongly connected if mutually reachable
- graph G strongly connected if every pair of vertices is strongly connected.



strongly connected components
→ can have edges go b/t strongly connected components
(DIFFERENT from connected comp.)

connected comp.



Connected components

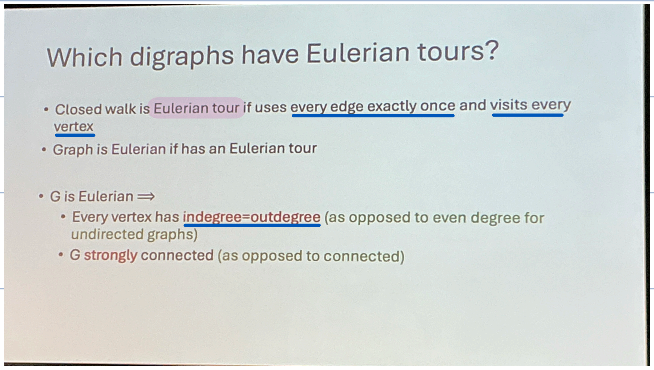
- *a, b strongly connected* if mutually reachable
- *G strongly connected* if every pair of vertices strongly connected

Connected component of vertex v is subgraph induced by vertices connected to v.
(i.e. $V' = \{u | u, v \; connected\}$, $E' = \{\{u, w\} \in E | u, w \in V'\}$)
- Connected (by transitivity)
- All of G if G connected
- Every vertex/edge is in exactly one connected component of G

Strongly connected component (SCC) of vertex v is subgraph induced by vertices strongly connected to v.
(i.e. $V' = \{u | u, v \; strongly \; connected\}$ $E' = \{(u, w) \in E | u, w \in V'\}$)
- Strongly connected (by transitivity)
- All of G if G strongly connected
- Every vertex is in exactly one SCC of G
- Can have edges between SCCs

THM: if there is a walk from a to b, then there is a path from a to b.

EULERIAN:



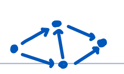
Which digraphs have Eulerian tours?

- Closed walk is Eulerian tour if uses every edge exactly once and visits every vertex
- Graph is Eulerian if has an Eulerian tour

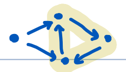
- G is Eulerian ⟹
  - Every vertex has indegree=outdegree (as opposed to even degree for undirected graphs)
  - G strongly connected (as opposed to connected)

DIRECTED ACYLIC GRAPHS: (DAG) directed graph with NO cycles

Ex: tree, state machines



DAG!
(no cycles)



not DAG
(loop)

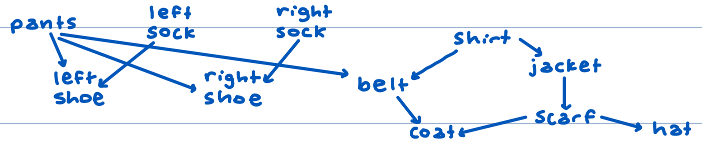
DAG!

CONSTRAINT GRAPH:

Ex: getting dressed has constraints

a → b iff put on a before b

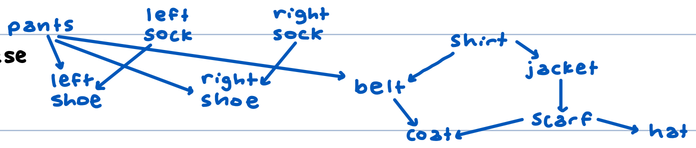
b reachable from a iff must put on a before b



REVIEW (W.U. (4)

COVERING EDGES: ONLY path b/t endpoints
-Hasse diagram only has these

REDUNDANT EDGES: edge that doesn't give new info



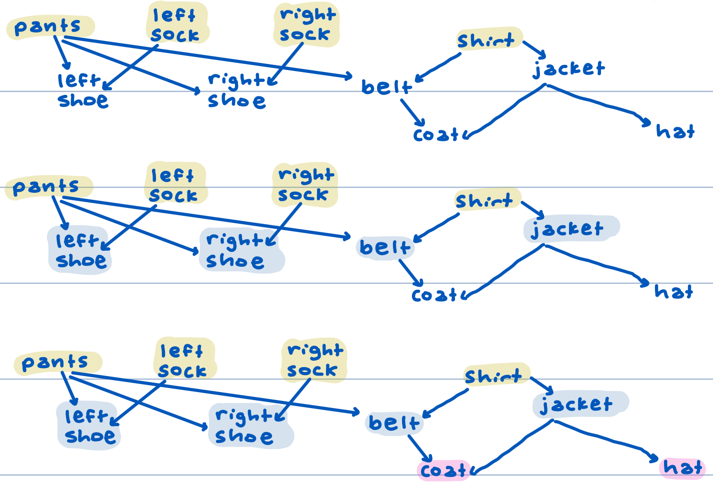
MINIMAL ELEMENT (SOURCE): no "in-arrows" (pants, socks, shirt)
- can start with any of these
- LEMMA: a minimal element always exists
- Dressing Algorithm: repeatedly put on minimal element (TOPOLOGICAL SORT)

MAXIMAL ELEMENT (SINK): no "out-arrows" (shoes, coat, hat)

TOPOLOGICAL SORT:
- minimal element (source): no "in-arrows"
- topological sort of DAG: list of all nodes in graph s.t. each node appears earlier in the list than every other node reachable from v
  - every DAG has one
  - topological sort algo: pick minimal element, put next on list, remove from graph

NOTES:
- some previously non-minimal elements might now become minimal

Ex: how fast can a team of dressers dress you? **PARALLEL TASK SCHEDULING**



3 stages, 4 servants is fastest for parallel tasks.
- depth of tree = 3

COMPRABLE:
- u can reach v or v can reach u
- some ordering b/t
- cannot process @ same time (one first, then later on the other)

CHAIN: set of nodes s.t. any pair is comparable
Ex: shirt → belt → coat

CRITICAL PATH: longest chain – length = # vertices
Ex: shirt → jacket → scarf → coat

ANTICHAIN: set of uncomparable nodes
- can process @ same time

★ THM: # rounds needed = $\underbrace{\text{length of critical path}}_{\substack{\text{max len. of chain} \\ \equiv \\ c}}$ (max node length of a chain)

PF: (≥) must do in order

(≤) Dressing Strategy: Repeat
- process all minimum elements until done

≡
- depth(v) = length of longest path that ends in v (at start time)
- for i=1 to $\underline{c-1}$:
  process all tasks v s.t. depth(v) = i

- v minimal iff depth(v) = 0

start @ 0

$\forall v$, depth(v) $\in \{0, 1, 2, 3, \dots, c-1\}$

if v can reach u ($u \neq v$), then depth(v) < depth(u)

→ all prereqs for u have strictly smaller depth than u

[4/8/25] - lecture - RELATIONS & COUNTING

- number theory, graphs, counting
- induction, proofs, sets, etc.
- won't focus on quiz 1 content tho.

def: a binary **RELATION** $R \subseteq A \times B$ has 3 parts:

- domain, set A
- codomain, set B (NOT range)
- set $R \subseteq A \times B$ (subset)

$A \times B$ notation: "cartesian product of A & B"

$= \{(a,b) \mid a \in A, b \in B\}$ set of all possible pairs

smallest: $\emptyset$ empty set

Ex: S: {luke, ..., ...}

C = {chem, ..., ...}

P = {Galad, ..., ...}

L(earning) $\subseteq S \times C$ ← ORDER MATTERS! (directional)

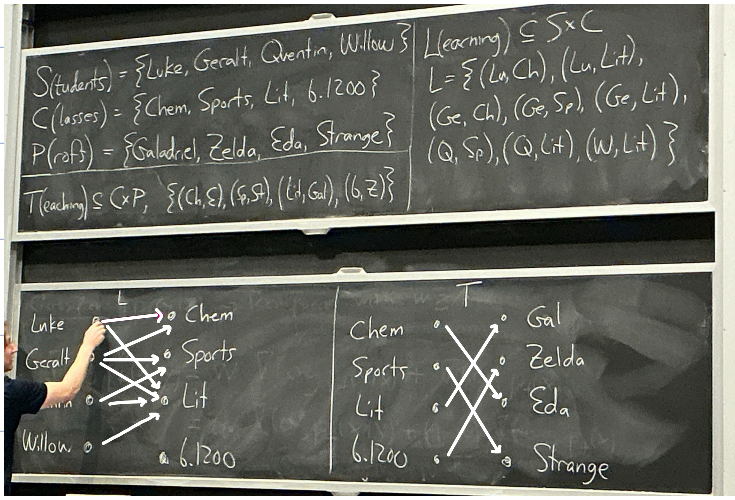
L = {(Luke, Chem), (Luke, sports), ... }

T(each) $\subseteq C \times P$

T = {(Galad, chem) ... }

shows relationships b/t two sets

VISUALLY:



S(tudents) = {Luke, Geralt, Quentin, Willow}

C(lasses) = {Chem, Sports, Lit, 6.1200}

P(rofs) = {Galadriel, Zelda, Eda, Strange}

T(eaching) ≤ C×P, {(Ch,E), (Sp,St), (Lit,Gal), (6,Z)}

L(earning) ⊆ S×C

L = {(Lu,Ch), (Lu,Lit), (Ge,Ch), (Ge,Sp), (Ge,Lit), (Q,Sp), (Q,Lit), (W,Lit)}

*need to know which comes on left / right

left = domain, right = codomain

NOT a function (>1 arrow out)

→ all nodes must satisfy

→ is a total

→ NOT injective or surj.

- IS a function! @ most 1 arrow out for all nodes!
- is a total
- is surjective
- is injective

RELATIONS Ex:

- $a \leq b$
- $a \mid b$
- $x \subseteq y$
- $x \in y$

these are all the same!

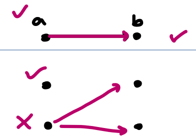
- aRb — a is related to b
- $(a,b) \in R$
- $R(a,b)$

say $R \subseteq A \times B$

def: R is a **FUNCTION** iff every $a \in A$ has at most one $b \in B$ s.t. aRb

i.e. every $a \in A$ has at most one arrow out

we write $R: A \to B$ for functions *R(a) means the unique b that a relates to (if it exists)



Ex: $f: \mathbb{R} \to \mathbb{R}$, $f(x) = \frac{1}{x^2}$

domain codomain

pairs: $\{(x,y) \mid x, y \in \mathbb{R}$ and $y = \frac{1}{x^2}\}$

$= \{(x, \frac{1}{x^2}) \mid x \in \mathbb{R} \setminus \{0\}\}$

- is not surjective
- is not injective (ex: 3 & -3)

def: $R \subseteq A \times B$ is **TOTAL** iff every $a \in A$ has ≥ 1 arrow out

→ L & T above are both total

→ f is not a total ($x=0 \to \frac{1}{0}$ ... undef.)

R is a **total function** iff every $a \in A$ has =1 arrow out

→ f is func. But not total.

→ g is a total function!

* "function" often means "total function"

"partial function" synonymous w/ function

- can have inputs w/ missing outputs
- at most one arrow out

careful with names!

$g: \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$

$g(x) = \frac{1}{x^2}$

$\{(x, \frac{1}{x^2}) \mid x \in \mathbb{R} \setminus \{0\}\}$

func & total ✓

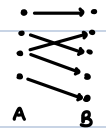
- not surjective
- not injective

def. $R \subseteq A \times B$ is **INJECTIVE** iff every $b \subseteq B$ has ≤ 1 arrow in
i.e. $\exists$ at most one $a \in A$ s.t. aRb

def. $R \subseteq A \times B$ is **SURJECTIVE** iff every $b \subseteq B$ has ≥ 1 arrow in

THM: if A, B are finite sets and $R \subseteq A \times B$ is total & injective, then $|A| \leq |B|$.
if instead, R is func. & surjective, $|A| \geq |B|$

Ex: total + injective:
A ≥ 1 out B ≤ 1 in



$|A| \leq$ # arrows
$\leq |B|$ ✓

def. if $R \subseteq A \times B$ is inj, surj, func, & total, then R is a **BIJECTION.**
· one arrow pointing into each B, one arrow out of each B.
→ if A, B finite, this implies $|A| = |B|$

matchings are for undirected graphs, but these are directed.
sometimes $A = B$ (same set)

def: $R \subseteq \overbrace{A \times A}^{\text{same set}}$ is called a **relation** on A.
$a \leq b$ $\quad a | b \quad a \equiv_{10} b \quad x \subseteq y$ ← examples of relations on sets
ex: aRb when $a \leq b$

if G is a graph, the reachability relation G^* $\quad uG^*v$ iff $\exists$ walk from u to v.

DIRECTED GRAPH:

STRONG CONNECTIVITY RELATION: uSv iff uG^*v and vG^*u
in same strongly connected component

EQUIVALENCE RELATIONS:
generalize meaning of "=" "sameness"
if $R \subseteq A \times A$,
- R is **REFLEXIVE** iff $\forall a \in A$, aRa ← same as itself
- R is **SYMMETRIC** iff $\forall a, b \in A$, $aRb \Leftrightarrow bRa$ ← sameness don't depend on order
- R is **TRANSITIVE** iff $\forall a, b, c \in A$, $(aRb \wedge bRc) \Rightarrow (aRc)$

def: R is an **EQUIVALENCE RELATION** iff R is reflexive, symmetric, transitive.

THM: if R is equivalence relation, there is a **PARTITION** of A into subsets s.t. every $a \in A$ belongs to precisely one of these subsets s.t. aRb iff a, b in same subset.

WEAK PARTIAL ORDER:
GOAL: generalize "$\leq$" "ordering"

reflexive! $\quad$ Ex: $a \leq b$ $\quad$ a is weakly less than b ← we will only have this
transitive! $\quad$ $a < b$ $\quad$ a is strictly less than b

def: R is **ANTISYMMETRIC** iff $\forall a, b \in A$, $(aRb$ and $bRa) \Rightarrow (a = b)$ ← only exception to this rule if same element

R is a **WEAK PARTIAL ORDER** iff its reflexive, anti-symmetric, & transitive.
→ only diff b/t this & equiv. rel. is antisymm vs. symm.
→ partial

THM: if G is a digraph, then G^* is WPO iff G is a DAG (directed acylic graph)
→ only way to break this is to have a cycle

def. a, b are **COMPERABLE** iff aRb or bRa

WPO R is **TOTAL ORDER** aka LINEAR ORDER iff all pairs are comparable

ex: a|b on $\mathbb{N}$ = weak partial order that is not total ordering

~ COUNTING ~

- how many shuffled decks of cards? → 52!
- how many trees w/ nodes $\{1, 2, \ldots, n\}$? → n^{n-2}

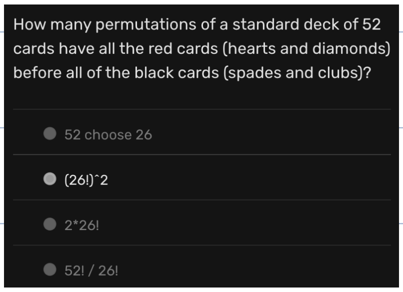
PRODUCT RULE: $|A \times B| = |A| \times |B|$

$|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \times |A_2| \times \ldots \times |A_n|$

Ex: # binary sequences of length n

$\{0,1\} \times \{0,1\} \times \ldots \times \{0,1\} = \{0,1\}^n = 2 \times 2 \times \ldots \times 2 = 2^n$

Ex:



How many permutations of a standard deck of 52 cards have all the red cards (hearts and diamonds) before all of the black cards (spades and clubs)?

- ● 52 choose 26
- ● (26!)^2
- ● 2*26!
- ● 52! / 26!

1st card: 26 choices
2nd: 25
⋮
26th: 1
27th: 26 choices
⋮
52nd 1

BIJECTION RULE: if ∃ bijection A→B, then |A| = |B|

Ex: # subsets are there of $\{1, 2, \ldots, n\}$?

f: $Bin_n \to$ subsets of $\{1, n\}$

$f(a_1, a_2, \ldots, a_n) = \{i \in \{1, n\} \mid a_i = 1\}$

$f(\underset{1}{0}, \underset{2}{1}, \underset{3}{1}, \underset{4}{1}, \underset{5}{0}, \underset{6}{1}) = \{2, 3, 4, 6\}$ → f is bijection (need proof)

so, # subsets is 2^n

SUM RULE: if $A_1, \ldots A_n$ are pairwise disjoint, then $|A_1 \cup \ldots \cup A_n| = |A_1| + \ldots + |A_n|$

Ex: 6 shirts
10 pants
4 pairs of shoes] 6 + 10 + 4

Ex: $S \subseteq \{1, 2, \ldots, n\}$

sets of size 0, 1, ..., n

↑ ↑ disjoint (diff. bins)

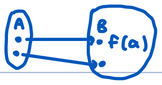
$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$

[4/10/25] - COUNTING

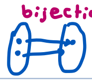
*** REVIEW W.U. 16**

PRODUCT RULE: $|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$

BIJECTION RULE: if f: A→B is bijection, then |A| = |B|

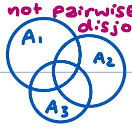


NOT bijection



SUM RULE: if $A_1 \ldots A_n$ pairwise disjoint, then $|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1| + |A_2| + \ldots + |A_n|$

✗ not pairwise disjoint



*remember: $n! = n \cdot (n-1) \cdot (\ldots) \cdot 3 \cdot 2 \cdot 1$

tools:

GENERALIZED PRODUCT RULE: (counting orderings / sequences)

A = set of length k sequences

n_1 possible 1st entries

n_2 possible 2nd entries - no matter which 1st entry chosen

⋮

n_k possible kth entries - no matter which first k-1 entries chosen

then $|A| = n_1 \cdot n_2 \cdot \ldots \cdot n_k$

Ex: order deck of cards

- 52 options for 1st card
- 51 for 2nd...
- ⋮
- 1 for last card

TOTAL COUNT: 52!

EX: DECK OF CARDS, how to order?

13 ranks {A, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K}

4 suits {♢, ♡, ♤, ♧}

D H S C

x

52

\# orders: $52 \cdot 51 \cdot 50 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 = 52!$

* set of remaing cards depends on previous choices, but # of remaining choices does not depend on previous choices

Ex: dollar bills with no repeated digits

total # 8 digit serial #s = 10^8

total # w/o repeated digits = $10 \cdot 9 \cdot 8 \cdot \ldots \cdot 4 \cdot 3$ ← only 8 digits

fraction w/o repeats ≈ 0.018

Ex: $9\,2\,\underline{4}\,\underline{5}\,6\,7\,\underline{4}\,\underline{5}$

CAN'T ALWAYS USE PRODUCT RULE!

Ex: how many length 3 serial codes have distinct digits increasing left → right

OK: 123, 049, 278, 789

BAD: 312, 987, 334

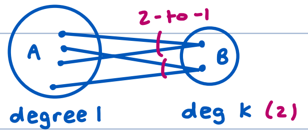
Ex $0\,\underset{8}{\_\_}$ options

Ex: $7\,\underset{1}{\_\_}$ option

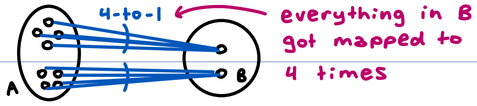
DIVISION RULE: (counting subsets)

if $f: A \to B$ is k-to-1, then $|A| = k \cdot |B|$

How to use: we know $|A|$, k so can figure out $|B| = \frac{|A|}{k}$



Ex:

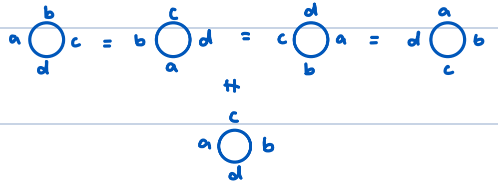


$|A| = 4 \cdot |B|$

$\overset{\shortparallel}{8}$ $\overset{\shortparallel}{2}$

EX: KNIGHTS OF ROUND TABLE

- n knights sit around round table
- seating is equivalent if rotation

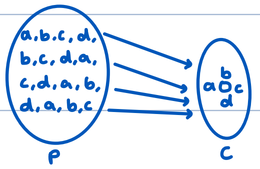


let P = set of permutations 1, …, n

C = set of cyclic orderings 1, …, n

f maps permutation in P to cyclic order in C

- f is total
- each $c \in C$ mapped to by n permutations in P
  - f is n-to-1
  - $|C| = \frac{|P|}{n} = \frac{n!}{n} = (n-1)!$



EX: COUNTING UNORDERED SUBSETS

→ equivalent question: how many size 3 subsets of {0, 1, … 9}

- bijection: for each size 3 subset, map it to sequence of elements in incr. order

$f(\{2,9,7\}) = f(\{9,2,7\}) = f(\{2,7,9\}) = (2,7,9)$

let P: # permutations of {0, 1, …, 9}

let S = # size 3 subsets of {0, …, 9}

$f(a_0, a_1, \ldots a_9) = \{a_0, a_1, a_2\}$ ← set of first 3 digits

f is total

$|S| = \frac{|P|}{3!\,7!} = \frac{10!}{3!\,7!}$

SIZE 3 SUBSET: 3 DIGS INCR

$\{1,0,2\} = \{0,1,2\} = \{2,1,0\} \xrightarrow{f} 0,1,2$

⋮

CAREFUL: subsets vs. sequences

GENERALIZE: COUNTING UNORDERED SUBSETS

- let P = # permutations of $\{0,1,\dots,n\}$
- let S = # of size k subsets of $\{0,1,n\}$
- $\underbrace{f(a_0, a_1, \dots, a_n)}_{\text{seq.}} = \underbrace{\{a_0, a_1, \dots, a_k\}}_{\text{set}}$ ← first k digits
- f is total
- how many $a_0, a_1, \dots, a_n$ map to specific = $\{a_0, a_1, \dots a_k\}$? → $k!(n-k)!$

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

$\binom{n}{k}$ = "n choose k"

EX: $7361528049 \longrightarrow \{3,6,7\}$

$7362801549 \longrightarrow \{3,6,7\}$

$376281549 \longrightarrow \{3,6,7\}$

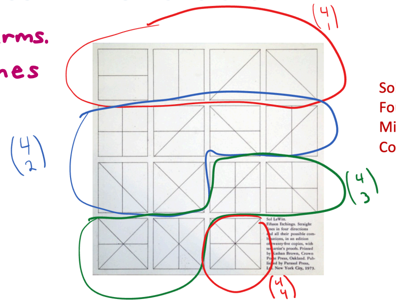
f maps $\overset{b_0,\dots,b_9}{\text{sequence}}$ to $\{3,6,7\}$ if:

1) $\{b_0, b_1, b_2\} = \{a_0, a_1, a_2\}$ # options for $b_0, b_1, b_2 = \overset{3!}{\overset{\shortparallel}{3 \cdot 2 \cdot 1}} = 6$

n choose k in the world of art

n = # perms.

k = # lines



Sol Lewitt:
Founder of both
Minimal and
Conceptual Art

OTHER EXAMPLES:

- select 3 toppings of 15 for pizza $\binom{15}{3}$
- 4 volunteers from class of 250 $\binom{250}{4}$
- flip 100 coins & get 50 heads $\binom{100}{50}$

COUNTING VIA SEQUENCES OF DECISIONS (# recipes):

- DECK OF CARDS:
  - 13 ranks
  - 4 suits
  - each hand = 5 cards
    - set

- how many 5-card hands are there? $\binom{52}{5}$

54!/12

125

30

(26!)^2

x 52 c 2,

x 1, x

- how many hands with 4-of-a-kind?

RECIPE: describes function mapping (rank x remaining card) to 4-of-a-kind hands

- pick rank of 4 of a kind 13 $\in \{A, \dots, Q\}$ 6♢, 6♡, 6♤, 6♧
- pick remaining card × 48 remaining

f(rank, remaining card) → hand w/ 4 of a kind

* b/c bijection, # 4 of a kind = 13×48 (exactly 1 way)

- must be same #.

sometimes not the same! not bijection Ex: 2-to-1 function

[4/15/24] - MORE COUNTING

what if coefficient of $x^k y^{n-k}$ in expansion $(x+y)^n$

Ex $(x+y)^2 = (x+y)\cdot(x+y)$

$= x\cdot(x+y) + y\cdot(x+y)$

$= x^2 + xy + xy + y^2$

Ex: $(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$

$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$

group together terms with same # of x's & same # of y's

→ how many ways to pick terms with k x's & (n-k) y's

$(x+y)^n = (x+y)\cdot \ldots \cdot(x+y) = ?\cdot x^n + ?\, x^{n-1}y + \dots + y^n$

$1\,x^n,\ 1\,y^n,\ n\cdot x\cdot y^{n-1}$

BINOMIAL THEOREM: $(x+y)^n = \Sigma_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

Ex: $(a+b+c)^{10}$ → what is $a^5b^2c^3$

A: # permut: aaaaa bbccc

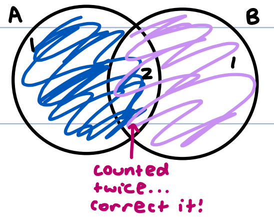
BOOKEEPER: $\frac{10!}{5!\,2!\,3!} = \binom{10}{5,2,3}$ ← MULTINOMIAL COEFFICIENT (diff. notation)

INCLUSION / EXCLUSION:

Ex: how many ♡ or queens in deck?

Sum rule: |hearts ∪ queens| = |♡| + |Q| = 13+4 = 17 ×

BUT! sum rule only applies when sets disjoint. one Q & ♡



UNION:

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

Ex: $n = p\cdot q$ where $p \neq q$ both prime. how many #s in set $\{1, 2, \dots, n\}$ are relatively prime to n?

let $A_p \subseteq \{1,\dots,n\}$ be #s divisible by p i.e. $\{p, 2p, 3p\}$

let $A_q \subseteq \{1,\dots,n\}$ be #s divisible by q

HOW MANY #s not relatively prime? $|A_p \cup A_q| = |A_p| + |A_q| - |A_p \cap A_q|$

$= q+p-1$

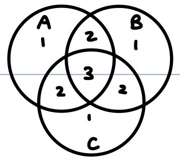
WHAT IS $|A_p|$? $\frac{n}{p} = q$

WHAT IS $|A_q|$? $\frac{n}{q} = p$

WHAT IS $|A_p \cap A_q|$? n (1 intersection)

relatively prime = $n-(q+p-1)$

Ex: size of union of 3 sets

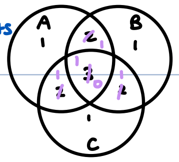


$|A\cup B\cup C| = |A|+|B|+|C|$ ← each set

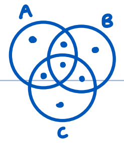
subtract intersect of 2 sets

$-|A\cap B| - |B\cap C| - |A\cap C|$

$+|A\cap B\cap C|$ ← all sets add



Ex:



$\overbrace{|A\cup B\cup C|} = |A|+|B|+|C|$

$= 4+4+4 = 12$

$-|A\cap B| - |B\cap C| - |C\cap A|$

$= -2-2-2 = -6$

$+|A\cap B\cap C|$

$= 1$

→ 12−6+1 = 7 ☺

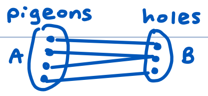
INCLUSION/EXCLUSION *important!

$$\bigcup_{i=1}^{n} A_i = \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} |A_i\cap A_j| + \sum_{1\le i<j<k\le n} |A_i\cap A_j\cap A_k| + \dots + (-1)^{n-1}|A_1\cap A_2 \cdots \cap A_n|$$

on a test: if given large n, think, don't try to do it

PIGEON-HOLE PRINCIPLE (PHP):

if $|A|>|B|$ and $f: A\to B$ is total, then f is $\underbrace{\text{NOT injective.}}_{\exists a_1\neq a_2 \in A \text{ s.t. } f(a_1)=f(a_2)}$



Ex: 10 pigeons & 9 holes, at least one hole will have >1 pigeon

Ex: cake walk / musical chairs

Ex: if >26 ppl in room, @ least 2 ppl have names starts w/ same letter

→ A = ppl B = 1st letter f = mapping of person w/ 1st letters

Ex: n colors socks. how many socks to guarantee a matching pair?

→ A = socks in drawer; B = color of sock; f = map of each sock to a color

→ n+1 by Pigeyhole Princ.

Ex: at least 2 non-bald Bostonians have same #hairs on head

→ ~650K Bostonians

→ ≥500K not bald

→ max hair ≈ 300K

→ more Bostonians than hair counts so must be T by P.H.

EX: graph of n vertices, take walk length > n, visit some vertex ≥ 2

EX: large video files

- can send all bits for each frame (HUGE)
- or compress then send

f: n bit strings → ≤ n bit strings

f is "lossless" if injective (i.e. $a_1 \neq a_2$ implies $f(a_1) \neq f(a_2)$)

f is "strictly compressive" if f: n-bit strings → < n bit strings

CAN we have both lossless & strictly compressive?

PF:

2^n n-bit strings

$2^{n-1} + 2^{n-2} + \ldots + 1 = 2^n - 1$ # < n bit strings (strictly less)

any strictly compressive map cannot be injective

GENERALIZED PIGEONHOLE PRINCIPLE:

if $|A| > k \cdot |B|$, then every total function A→B must have at least k+1 inputs in A that map to some output in B.

EX: 8x8 chess, place 33 rooks anywhere, can always find ≥ 5 diff. rows/cols

$33 = |A| > 4 \cdot 8$

so $|B| = 8$?

$k+1 = 5$? → $k = 4$

f: rook→label of location

PHP says there is a label with @ least 5 rooks!

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

PIGEONS:

PIGEONHOLES:

entries w/ same label are in diff. rows/cols

COMBINATORIAL PROOFS:

Show $|A| = x$

Show $|A| = y$

Conclude $x = y$

EX: what is $\Sigma_{k=0}^{n} \binom{n}{k}$

S = set of subsets of $\{1, \ldots, n\}$ e.g. n=2, $\{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

$|S| = 2^n = |S_0| + |S_1| + \ldots + |S_n| = \sum_{k=0}^{n} \binom{n}{k}$ → $2^n = \sum_{k=0}^{n} \binom{n}{k}$

S_k = set of subsets of $\{1, \ldots, n\}$ of size k

$|S_k| = \binom{n}{k}$

CLAIM:

(1) if $i \neq j$, then $S_i \wedge S_j = \emptyset$ ← if in one, def. not in the other

(2) $\bigcup_{i=0}^{n} S_i = S$

so, S_i's are a partition

PSET 9: $\sum_{r=0}^{k} \binom{n}{r}\binom{n}{k-r} = \binom{2n}{k}$

EX: prove $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

- let B = set of all k-element subsets of n-elemental set $\{a_1, \ldots, a_n\}$
- size of B = $\binom{n}{k}$

another way to compute size of B:

- let B_1 = set of k-element subsets containing a_1
- let B_2 = set of k-element subsets not containing a_1

disjoint! direct proof

- $B = B_1 \cup B_2$ & B_1, B_2 disjoint, so $\binom{n}{k} = |B| = |B_1| + |B_2|$
- $|B_1| = \binom{n-1}{k-1}$ since after a_1 place in set, need to pick another k-1
- $|B_2| = \binom{n-1}{k}$ since a_1 not in set, so need to pick k elements from remaining n-1.

Ex: Pascal's Triangle

$$\binom{0}{0}=1$$

$$\binom{1}{0}=1 \quad \binom{1}{1}=1$$

$$\binom{2}{0}=1 \quad \binom{2}{1}=2 \quad \binom{2}{2}=1$$

$$\left.\binom{3}{0}=1 \quad \binom{3}{1}=3 \quad \binom{3}{2}=3 \quad \binom{3}{3}=1\right] \rightarrow \text{every row sums to } 2^n$$

[4/22/25] - PROBABILITY -18

- monty hall game show question
- based on real game show

TREE METHOD: (4 step method)

step 0, assumptions:

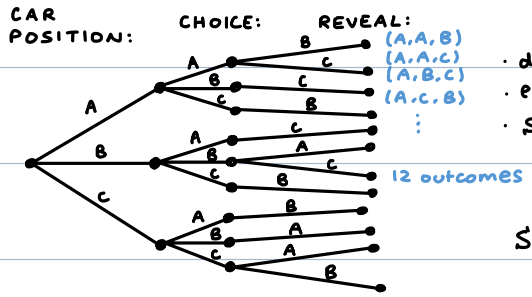
- car is equally likely in each of 3 doors
- contestant equally likely to choose each door no matter where car is
- host (monty) must pick unpicked goat door with equal probability

step 1: sample space

DEF: (discrete) **probability space** is a pair (S, Pr) where:

- S is a non-empty finite (countable) set called **Sample Space**
- Pr is a total function from $S \rightarrow [0,1]$ representing the probability that each outcome occurs

AXIOM: want $\sum_{w \in S} Pr(w) = 1$ (total probability = 1)

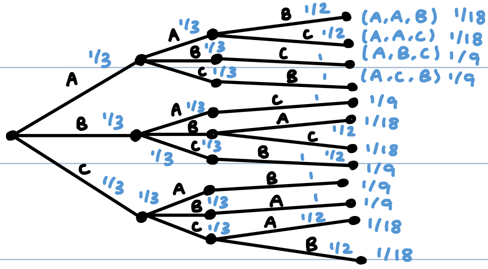


- draw tree to reveal all transcripts
- each transcript aka leaf is an outcome
- S = set of leafs

$$S = \{(x,y,z) \mid z \neq x \text{ and } z \neq y\}$$

STEP 2: probability function

assign a "probability" to each edge of tree, the chance of following that edge starting from its left endpoint



$Pr(w) :=$ product of values on edges that lead to w.
leaf

SANITY CHECK: $\sum_{w \in S} Pr(w) = 1$ ✓

STEP 3: events

DEF: an **EVENT** is a subset $A \subseteq S$

ex: [monty reveals door C]

$= \{(A,A,C),(A,B,C),(B,A,C),(B,B,C)\}$ ← set of outcomes

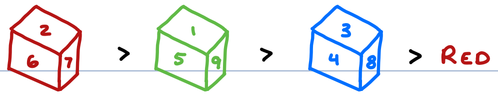
ex: [win by switching] = $\{(A,B,C),(A,C,B),(B,A,C),(B,C,A),(C,A,B),(C,B,A)\}$

STEP 4: Compute answer

for an event $A \subseteq S$, $Pr(A) := \sum_{w \in A} Pr(w)$

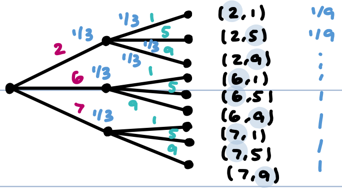
$\{(A,B,C),(A,C,B),(B,A,C),(B,C,A),(C,A,B),(C,B,A)\} = \frac{1}{9} + \frac{1}{9} + \frac{1}{9} + \ldots + \frac{1}{9}$ 6 times $= \boxed{\frac{2}{3}}$

STRANGE DICE: (not transitive)



NOT TRANSITIVE!!

RED VS. GREEN: winner = larger roll



assume dice are fair & don't influence each other.

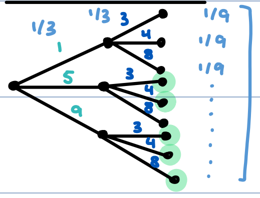
$\Pr([\text{red win}]) = \frac{1}{9}+\frac{1}{9}+\frac{1}{9}+\frac{1}{9}+\frac{1}{9} = \boxed{\frac{5}{9}} > \frac{1}{2}$ ← red more likely to win

$[\text{red win}] = \{(2,1),(6,1),(6,5),(7,1),(7,5)\}$

a prob. space is uniform when all outcomes are equally likely

in this case, $\Pr(A) = \frac{1}{n}+\frac{1}{n}+\dots+\frac{1}{n} = \frac{|A|}{|S|}$ ← ONLY when uniform

GREEN VS. BLUE:

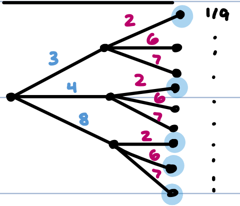


uniform!
1/9 per outcome

$[\text{green wins}] = \{(5,3),(5,4),(9,3),(9,4),(9,8)\}$

$\Pr(G \text{ wins}) = \frac{1}{9}+\frac{1}{9}+\frac{1}{9}+\frac{1}{9}+\frac{1}{9} = \boxed{\frac{5}{9}}$

BLUE VS. RED:



$\Pr(\text{blue wins})$

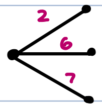
$= \Pr(\{(3,2),(4,2),(8,2),(8,6),(8,7)\})$

$= \boxed{\frac{5}{9}}$

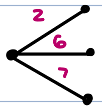
∴ no single best die – want to be 2nd player & pick die that beats 1st players

GAME UPDATE: red ×2 vs. green ×2

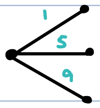
RED 1



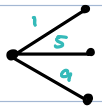
RED 2



GREEN 1



GREEN 2



→ 89 leaves (3^4)

$\{(r_1, r_2, g_1, g_2) \mid r_1, r_2 \in \{2,6,7\} \text{ and } g_1, g_2 \in \{1,5,9\}\}$

$\Pr(\text{red wins})$ = look @ sums red can get
(4, 8, 8, 9, 9, 12, 12, 13, 13, 14)

$\Pr(\text{green wins}) = (\dots)$

$\Pr(\text{red wins}) = \frac{37}{81}$

$\Pr(\text{green wins}) = \frac{42}{81}$

$\Pr(\text{tie}) = \frac{2}{81}$

∴ green wins more often

[4/24/25] - CONDITIONAL PROB

"what's the probability of event A given that i know that event B happens?"

$$\underset{\text{want } A}{\Pr(A} \mid \underset{\text{conditioning on } B}{B)}$$ → what's probability of A given B?

if $\Pr(B) \neq 0$, then $\Pr(A \mid B) = \dfrac{\Pr(A \cap B)}{\Pr(B)}$

Why?

stuff outside B no longer possible when given that B occurs

What is $\Pr(B|B)$?
$= \Pr(B)/\Pr(B) = 1$

PRODUCT RULE: $\Pr(A \cap B) = \Pr(A \mid B) \cdot \Pr(B)$

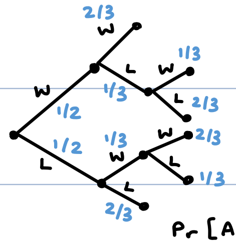
Ex: $\Pr(A \cap B \cap C) = \Pr(A \cap B \cap C) \cdot \Pr(C) = \Pr(A \mid B, C) \cdot \Pr(B \mid C) \cdot \Pr(C)$

GENERALIZED PRODUCT RULE: $\Pr(A_1 \cap A_2 \cap \ldots \cap A_n) = \Pr(A_1) \cdot \Pr(A_1 \mid A_2) \cdot \Pr(A_3 \mid \underbrace{A_1, A_2}_{\text{given both } A_1 \,\&\, A_2}) \cdot \ldots \cdot \Pr(A_n \mid A_1, \ldots, A_{n-1})$ (proof by induction)

Ex: in tree method: <u>multiply</u> probabilities on path to calculate probability of reaching a leaf

Ex: HALTING PROBLEM

- hockey team best 2-out-of-3 series
- $P(W \,\&\, W) = 2/3$
- $P(W \,\&\, L) = 1/3$



sample pts:	prob:	event A (win series)	event B (win 1st game)	A ∩ B
WW	1/3	WW	WW	WW
WLW	1/18	WLW	WLW	WLW
WLL	1/9	—	WLL	
LWW	1/9	LWW	—	
LWL	1/18	—	—	
LL	1/3	—	—	

$$\Pr[A \mid B] = \frac{\Pr[A \cap B]}{\Pr[B]} = \frac{\overbrace{1/3 + 1/18}^{7/18}}{\underbrace{1/3 + 1/18 + 1/9}_{1/2}} = \boxed{\frac{7}{9}}$$

$$\Pr[WW] = \underbrace{\Pr[\text{win 1st game}]}_{= 1/2} \cdot \underbrace{\Pr[\text{win 2nd game} \mid \text{win 1st game}]}_{\cdot\, 2/3} = \boxed{\frac{1}{3}}$$

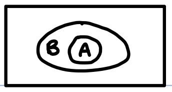
$$\Pr[B \mid A] = \frac{\Pr[A \cap B]}{\Pr(A)} = \frac{7/18}{1/2} = \boxed{\frac{7}{9}}$$

$$\Pr[B \mid A] = \frac{\Pr[A \cap B]}{\Pr[A]}$$

$$\Pr[A \mid B] = \frac{\Pr[A \cap B]}{\Pr[B]}$$

when they're equal: if $\Pr[A \cap B] = 0$ or $\Pr[A] = \Pr[B]$

when not equal:

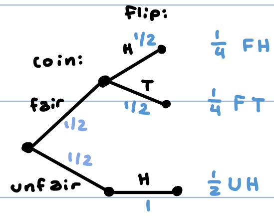


$A \subset B$
$\Pr(A \mid B) < 1$
$\Pr(B \mid A) = 1$

EX: TWO COINS

fair coin: $Pr[H] = Pr[T] = \frac{1}{2}$

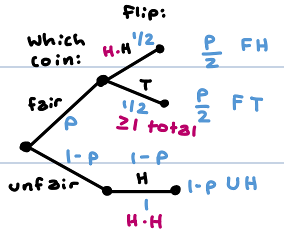
unfair coin: $Pr[H] = 1$, $Pr[T] = 0$



A: fair	B: heads
FH	FH
FT	UH

see heads, pick fair coin

$$Pr[A \mid B] = \frac{\frac{1}{4}}{\frac{1}{4}+\frac{1}{2}} = \boxed{\frac{1}{3}}$$



$$\frac{p/2}{p/2 + (1-p)} = \frac{p}{2-p}$$

k coinflips = heads

$$\underset{\text{k hands}}{Pr[A \mid B]} = \frac{p \cdot 2^{-k}}{p \cdot 2^{-k} + 1 - p} = \frac{p}{p + 2^{k}(1-p)}$$

POLLING:

- sample thousands & 60% say green
- tells you nothing ab. electorate
  → either most vote green or polling was unlucky

EX: medical testing

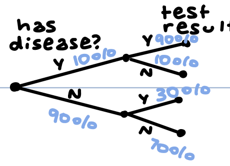
known: 1% of population has disease

if have:
- 1% false neg.
- 9% positive

if don't have:
- 3% false pos.
- 7% negative

EVENTS: A: person has disease
B: person tests positive

if +, what is probability you have it? $Pr[A \mid B]$



	A(disease)	B(pos)	A∩B
0.09	x	x	x
0.01	x	–	–
0.27	–	x	–
0.63	–	–	–

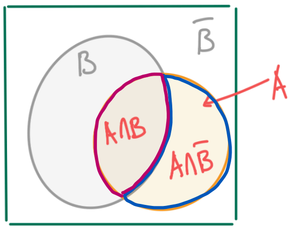
$$Pr[A \mid B] = \frac{Pr[A \cap B]}{Pr[B]} = \frac{9/100}{9/100 + \frac{27}{100}} = \frac{1}{4}$$

$$Pr[\text{test correct}] = \frac{9}{100} + \frac{63}{100} = \frac{72}{100}$$

LAW OF TOTAL PROBABILITY: $Pr(A) = \underbrace{Pr(A \mid B) \cdot Pr(B)}_{Pr(A \cap B)} + \underbrace{Pr(A \mid \bar{B}) \cdot Pr(\bar{B})}_{Pr(A \cap \bar{B})}$

- different way of figuring out A

disjoint events whose union is A



*when events NOT disjoint, must use inclusion/exclusion principle!

Ex: probability that when tossing 3 dice, 1 of them is $N \in \{1, \dots, 6\}$?

claim: $Pr(win) = 1/2$

pf: $A_i :=$ event that ith dice matches N for $i = 1,2,3$

$Pr(win) = Pr(A_1 \cup A_2 \cup A_3) = Pr(1) + Pr(2) + Pr(3) = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$

X WRONG: they are NOT disjoint. need to do inclusion/exclusion

Tools from counting are so important for reasoning about probabilities!!!!!!!!

- Look at (typed) lecture notes for probability rules (analogues from counting)
  - Sum rule
  - complement rule
  - difference rule
  - Inclusion-exclusion
  - Union bound
  - Monotonicity rule

[4/29/25] - INDEPENDENCE

CONDITIONAL PROB: $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]}$ if $Pr[B] \neq 0$

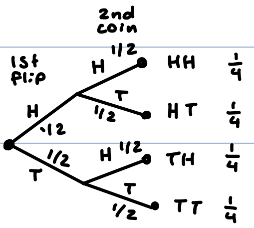
rewritten

(general) PRODUCT RULE: $Pr[A \cap B] = Pr[B] \cdot Pr[A|B] = Pr[A] \cdot Pr[B|A]$

DEF: event A is INDEPENDENT of B if $Pr[A|B] = Pr[A]$ or $Pr[B] = 0$

i.e. knowing B doesn't impact $Pr[A]$

Ex: 2 fair, ind coins → sanity check



EVENTS:

A: 1st flip is heads

B: 2nd flip is heads

SAMPLE SPACE: $\{H, T\}^2$

$A = \{(H,H), (H,T)\}$

$B = \{(H,T), (T,H)\}$

CHECK $\underbrace{Pr[B|A]}_{\frac{1}{2}} = \underbrace{Pr[B]}_{\frac{1}{2}}$ ✓

GAMBLER'S FALLACY: if 100 flips comes out H, next must be T → wrong! still 50/50

ARE COIN TOSSES FAIR? pearsi diacoins

Ex: TWO BIASED COINS: HH

flip 2 ind. biased coins

EVENTS:

A: 1st flip is H (probability q)

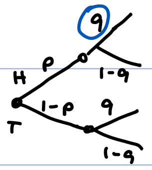
B: 2nd flip is H (probability q)

SAMPLE SPACE: $\{H, T\}^2$

$A = \{(H,H), (H,T)\}$

$B = \{(H,T), (T,H)\}$

weird part



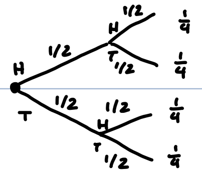
is S independent of A:

$$\left.\begin{aligned} Pr[S] &= \overset{HH}{pq} + \overset{TT}{(1-p)(1-q)} \\ &= 2pq - p - q + 1 \\ Pr[S|A] &= q \end{aligned}\right] = \boxed{\text{when } q = \tfrac{1}{2} \text{ or } p = 1 \text{ or } p = 0 \text{ (edge case)}}$$

always H

Ex: event S = 2nd flip is same as first {HH, TT}

is S ind. A?



$$\left.\begin{aligned} Pr[S] &= \tfrac{1}{2} \\ Pr[S|A] &= \tfrac{1}{2} \end{aligned}\right]$$

independent! even though seems like should be dependent

Ex: flip 2 independent fair coins

EVENTS:

A: 1st flip = H

B: 2nd flip = H

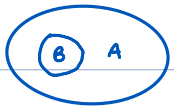
SAMPLE SPACE: $\{H,T\}^2$

A: $\{(H,H),(H,T)\}$

B: $\{(H,H)\}$

$Pr[B] = \frac{1}{4}$

$Pr[B|A] = \frac{1}{2}$ $\therefore$ B ≠ ind. of A



if $B \subseteq A$

$Pr[A|B] = 1$

not independent unless $Pr[A]=1$ or $Pr[B]=0$

$$Pr[A|B] = \frac{\overset{B\subseteq A}{Pr[A\cap B]}}{Pr[B]} = Pr[B]$$

Ex: A, B disjoint

$$Pr[A|B] = \frac{Pr[A\cap B]}{Pr[B]} = 0$$

not independent unless $Pr[A]=0$ or $Pr[B]=0$

more examples:

- bank failures
- winning states in prez elections
- drawing 2 cards from deck
  - after see 1st card, know second card won't be
  - if shuffle many times, will it be independent?
- skirt lengths vs. stock market??
- shopping for beer & diapers??

(INDEPENDENT version) PRODUCT RULE: event A is independent of event B iff $Pr[A\cap B] = Pr[A]\cdot Pr[B]$

- this calculation is a way to show independence
- use carefully! independence

PROOF: two cases

1) $Pr[B] = 0$

- Since $Pr[A\cap B] \overset{\text{monotonicity rule (L19)}}{\leq} Pr[B]$, $Pr[A\cap B]=0$
- $Pr[A]\cdot Pr[B] = 0$

2) $Pr[B] \neq 0$

- $Pr[A\cap B] \overset{\text{general product rule}}{=} Pr[B]\cdot Pr[A|B] = Pr[B]\cdot Pr[A]$ → iff A independent of B

COROLLARY: "independent of" is symmetric

PROOF: $Pr[A\cap B] = Pr[B\cap A]$ and $Pr[A]\cdot Pr[B] = Pr[B]\cdot Pr[A]$

if A independent of B, then:

by assump. ⟶ $Pr[A] = Pr[A|B] = Pr[A\cap B]/Pr[B]$ ← cond. prob.

so $Pr[B] = \frac{Pr[A\cap B]}{Pr[A]} = Pr[B|A]$

so B independent of A too!

COROLLARY: A, B independent iff A, $\bar{B}$ independent

PF: (only ⇒, other side symm): by cases:

LAW of total probability:

$Pr(A) = Pr(A|B)\cdot Pr(B) + Pr(A|\bar{B})\cdot Pr(\bar{B})$

if $Pr[B]=1$:

$Pr[A|\bar{B}]\cdot Pr[\bar{B}] = 0 = Pr[A]\cdot Pr[\bar{B}]$ since $Pr[\bar{B}] = 0$

equivalently, $Pr[A\cap B] = Pr[A]\cdot Pr[B]$

*account for edge cases! (0, etc.)

if $Pr[B] \neq 1$:

$Pr[A] = Pr[B]\cdot \overbrace{Pr[A|B]}^{\text{assumed A \& B are independ.}} + Pr[\bar{B}]\cdot Pr[A|\bar{B}]$

$Pr[A] = Pr[B]\cdot Pr[A] + (1-Pr[B])\cdot Pr[A|\bar{B}]$

$(1-\cancel{Pr}[B])Pr[A] = \cancel{Pr}[B]\cdot Pr[A|\bar{B}] \rightarrow Pr[A] = Pr[A|\bar{B}]$

(for >2 events)

MUTUAL INDEPENDENCE: if for $E_1, E_2, \dots E_n$, $\forall J \subseteq \{1, 2, \dots, n\} \setminus \{i\}$ we have that E_i is independent from $\cap_{j \in J} E_j$

- check every subset

i.e. $Pr[E_i] = Pr[E_i \mid \cap_{j \in J} E_j]$ or $Pr[\cap_{j \in J}] = 0$

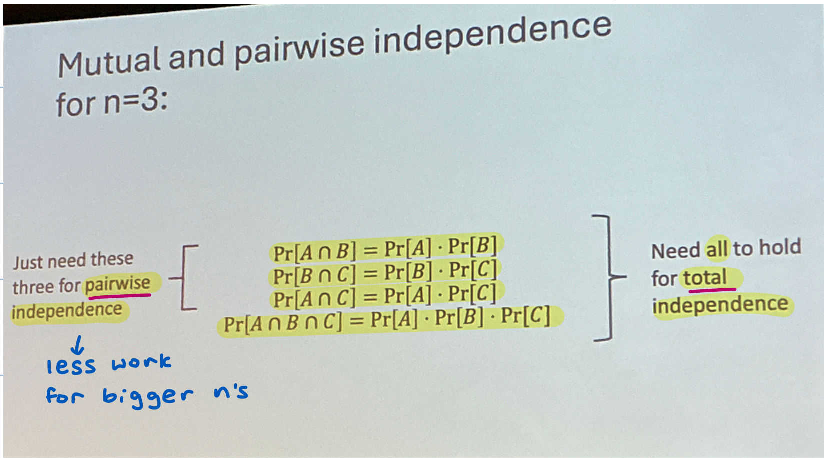
$\forall J \subseteq \{1, 2, \dots n\}$ $Pr[\cap_{j \in J} E_j] = \prod_{j \in J} Pr[E_j]$

PAIRWISE INDEPENDENCE: if for $E_1, E_2, \dots E_n$, $\forall i,j \subseteq \{1, 2, \dots, n\}, i \neq j$ we have that E_i is independent from E_j

- check every pair

equivalently $\forall i,j \subseteq \{1, 2, \dots n\}$, $i \neq j$ we have $Pr[E_i \cap E_j] = Pr[E_i] \cdot Pr[E_j]$

weaker property than mutual ind. but still useful!



Mutual and pairwise independence for n=3:

Just need these three for pairwise independence

$Pr[A \cap B] = Pr[A] \cdot Pr[B]$

$Pr[B \cap C] = Pr[B] \cdot Pr[C]$

$Pr[A \cap C] = Pr[A] \cdot Pr[C]$

$Pr[A \cap B \cap C] = Pr[A] \cdot Pr[B] \cdot Pr[C]$

Need all to hold for total independence

↓ less work for bigger n's

Ex: 9 biomarkers, M_i = human matches marker i

$Pr[M_i] = \frac{1}{10}$ (10% pop. match)

what is $Pr[M_1 \cap M_2 \cap \dots \cap M_9]$?

if mutually ind? → $\frac{1}{10^9}$

if not → $\leq \frac{1}{10}$

if pairwise ind → $\leq \frac{1}{100}$ $(\frac{1}{10} \cdot \frac{1}{10})$

Ex: 3 mutually ind. coins

A: 1st coin = 2nd

B: 2nd = 3rd

C: 3rd = 1st

$Pr[A] = Pr[C] = Pr[B] = \frac{1}{2}$

A, B, C = pairwise ind. e.g. A, B (other pairs similar)

$Pr[A \cap B] = Pr[\text{all same}] = Pr[HHH] + Pr[TTT] = \frac{1}{4}$

are they mut. ind?

$Pr[A \cap B \cap C] = Pr[HHH] + Pr[TTT] = \frac{1}{4}$

$Pr[A] \cdot Pr[B] \cdot Pr[C] = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$

BIRTHDAY PARADOX:

- m ppl
- n possible bdays
- what's probability 2 ppl have same bday?
- assume mut. ind (no twins / catastrophic events)
- uniformly distributed

sample space $S = \{(b_1, \dots b_m) \mid b_i \in \{1 \dots n\}\}$, $|S| = n^m$

event $E = \{(b_1, b_2, \dots b_m) \in S \mid \exists i \neq j \text{ s.t. } b_i = b_j\}$

for d = 365, m = 23 → prob ≥ 50%

30 ≥ 70%

60 ≥ 99.4%

→ important for **HASHING** (map big space to smaller space)

ex: cryptography

[5/11 25] - RANDOM VARS

3 independent coins:

	R	C_1	M
	#heads	1st = H	all same
HHH	3	1	1
HHT	2	1	0
HTH	2	1	0
HTT	1	1	0
THH	2	0	0
THT	1	0	0
TTH	1	0	0
TTT	0	0	1

roll 2 fair dice:

$D_1 :=$ value of 1st dice

$D_2 :=$ value of 2nd dice

$S := D_1 + D_2$

$T := (1$ if $S = 7$, 0 otherwise$)$

example outcome: (5, 3)

$D_1 = 5$

$D_2 = 3$

$S = D_1 + D_2 = 8$

$T = 0$

$X = D_1 + D_1 = 10$

DEF: an **RV** is a a total function from outcomes to R

$S \to \mathbb{R}$ (think of them as a measurement)

if $f(w)$ is always 0 or 1, f is called an **INDICATOR RV**

given an RV f, we get events such as $[f = 4] = \{$outcomes w s.t. $f(w) = 4\}$

$[f \leq 4] = \{$ outcomes w s.t. $f(w) \leq 4\}$

*every RV is a func. from $w \to f(w)$

"what are all the outcomes that $f(w)$ gets __ ?"

RANDOM VARIABLE: ← **FUNCTIONS** from outcomes → variables, generalizations

Ex: $\Pr(R = 2 \mid M = 1) = \Pr(2 \text{ Heads} \mid \text{all 3 coins match}) = \dfrac{\Pr(R=2 \cap M=1)}{\Pr(M=1)} = \boxed{0}$

DEF: two RVs X, Y are **independent** iff for all $x, y \in \mathbb{R}$, $[X = x]$ & $[Y = y]$ are independent events.

i.e. $\Pr[X = x \text{ and } Y = y] = \Pr(X = x) \cdot \Pr(Y = y)$

Ex: are R and M independent?

$\Pr(R=2 \text{ and } M=1) = 0$

$\Pr(R=2) \cdot \Pr(M=1) = \frac{3}{8}$ } these are NOT equal ∴ NOT independent

Ex: D_1 & S independent?

$[D_1 = 4]$ and $[S = 3]$ not independent b/c $\Pr(D_1 = 4 \text{ and } S = 3) = 0$

but $\Pr(D = 4) \cdot \Pr(S = 3) > 0$

Ex: S & T independent?

not independent

Ex: T & D_1?

is $[T=1]$ ind. of $[D_1 = a]$ for each $1 \leq a \leq b$ ✓

is $[T=0]$ ind. of $[D_1 = a]$ for each $1 \leq a \leq b$ ✓

$\Pr(\underbrace{T=1}_{1/6} \text{ and } \underbrace{D_1 = a}_{1/6}) = \Pr(\{a, 7-a\}) = \frac{1}{36} = \Pr(T=1) \cdot \Pr(D_1 = a)$ ✓

∴ independent!

DEF: a collection of RVs $X_1, \ldots, X_n$ is **mutually independent** if for all values $x_1, \ldots, x_n \in \mathbb{R}$,

$\Pr(X_1 = x_1 \text{ and } X_2 = x_2 \text{ and } \ldots \text{ and } X_n = x_n) = \Pr(X_1 = x_1) \cdot \ldots \cdot \Pr(X_n = x_n)$

similarly for **k-wise independence**, need this kind of product identity for every subset of size k.

DISTRIBUTION:

define **$PMF_R(x) = \Pr(R = x)$** for every possible value, check probability that R equals that value

↑ probability mass function = PDF

$CDF_R(x) = \Pr(R \leq x)$ → function (takes in 8 spits out #s)

cumulative distribution func.

Ex: $PMF_R(\#\text{heads}) = \begin{cases} 1/8 & \text{if } x = 0 \\ 3/8 & \text{if } x = 1 \\ 3/8 & \text{if } x = 2 \\ 1/8 & \text{if } x = 3 \\ 0 & \text{else} \end{cases}$ | $CDF_R(x) = \begin{cases} 0 & \text{if } x < 0 \\ 1/8 & \text{if } 0 \leq x < 1 \\ 1/2 & \text{if } 1 \leq x < 2 \\ 7/8 & \text{if } 2 \leq x < 3 \\ 1 & \text{if } x \geq 3 \end{cases}$ ← cumulative given an event A, $\mathbb{1}_A$:= RV defined by $\mathbb{1}_A(w) = \begin{cases} 1 \text{ if } w = A \\ 0 \text{ if } w \notin A \end{cases}$

$C_1 = 1$ with probability 1/2, 0 w/p 1/2

$C_2 = 1$ w/p 1/2, 0 w/p 1/2

$\mathbb{1}_{[C1=C2]} = 1$ w/p 1/2, 0 w/p 1/2 (2nd coin has 1/2 chance of matching 1st)

* should focus on how RVs effect the outcomes

indicator RVs have **BERNOULLI DISTRIBUTIONS** for some $0 \le p \le 1$,

$$PMF = \begin{cases} 0 \text{ w/p } p \\ 1 \text{ w/p } 1-p \end{cases}$$

given event A,

$\mathbb{1}_A$:= RV defined by

$$\mathbb{1}_A(w) = \begin{cases} 1 \text{ if } w \in A \\ 0 \text{ if } w \notin A \end{cases}$$

uniform dist. on $\{1, 2, \ldots, n\}$

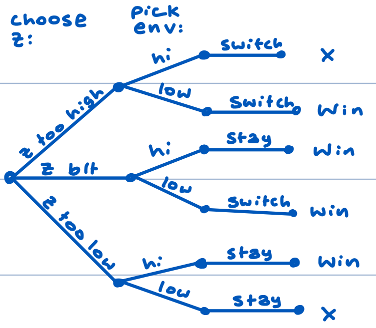
$$PMF = \begin{cases} 1 & \text{w/p } \frac{1}{n} \\ 2 & \text{w/p } \frac{1}{n} \\ \vdots & \\ n & \frac{1}{n} \end{cases}$$ ← equal probability

Ex: 2 envelopes, each with different int in $\{0, 1, \ldots, 100\}$

1) pick an envelope & lost
2) keep or switch
3) win if you have larger

if we knew some threshold z b/t the envelopes, we can win.

1) pick z uniformly from $\{0.5, 1.5, 2.5, \ldots, 99.5\}$
1.5) pick one of envelopes uniformly
2) behave as if z is b/t envelopes (lower than z: switch; higher: stay)



win w/p ≥ 50.5 %

* can use randomness to advantage

BINOMIAL DISTRIBUTION:

- flip n mutually independent coins, each H w/p p.
  how many H did we get?

PMF

Pr(exactly k Heads from the n flips)

= Pr({all H/T strings w/ k H, n-k T)

$$f_{n,p}(k) = \binom{n}{k} \cdot p^k (1-p)^{n-k}$$

[5/7/25] - EXPECTATION

events, value, probability

$Ex[R] = \sum_{\omega \in S} \underset{\text{value}}{R(\omega)} \cdot \underset{\text{probability}}{Pr[\omega]}$ weighted avg.

Ex: $R = \begin{cases} 1 \text{ if } H \\ 0 \text{ if } T \end{cases}$ coin has "bias" p

$\rightarrow Ex[R] = R(H) \cdot Pr[H] + R(T) \cdot Pr[T]$

$= 1 \cdot p + 0(1-p) = p$

EXPECTATION: indicator vars

$I_A = \begin{cases} 1 \text{ if } \omega \in A \\ 0 \text{ if } \omega \notin A \end{cases}$

✪ $Ex[I_A] = \sum_{\omega \in S} I_A(\omega) \cdot Pr(\omega)$

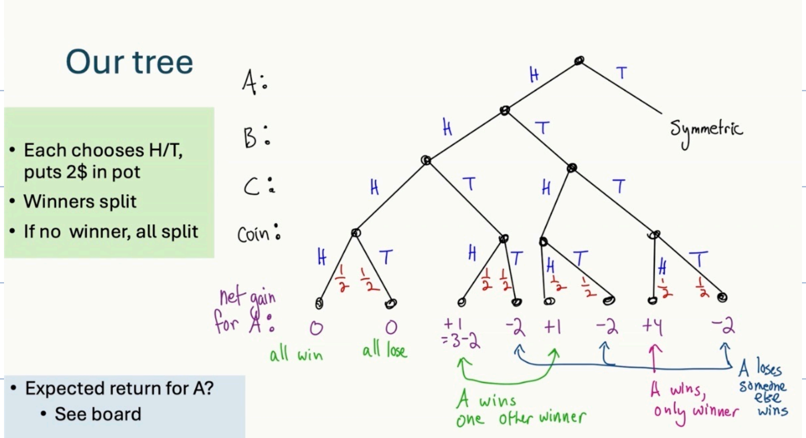
$= \sum_{\omega \in \bar{A}} 0 \cdot Pr(\omega) + \sum_{\omega \in A} 1 \cdot Pr(\omega)$

$= 0 \cdot Pr(I_A = 0) + 1 \cdot Pr(I_A = 1) = Pr[I_A = 1]$

useful for any 0/1 r.v. R, $Ex[R] = Pr[R=1]$

Ex: R = val from roll of 6-sided die

$Ex[R] = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} = 3.5$



Our tree

- Each chooses H/T, puts 2$ in pot
- Winners split
- If no winner, all split

- Expected return for A?
  - See board

Ex: gambling game → 3 players, 1 coin tosser

- player chooses H/T & puts \$2 into pot
- toss coin
- those that "win" split pot. if no wins, all split pot

EXPECTED RET:

if all picked uniformly, prob. reach any leaf $= \frac{1}{16}$

$E[\text{Brendan's win}] = \frac{2}{16} \cdot [0 + 0 + 1 - 2 + 1 - 2 + 4 - 2] = 0$ "fair"

if Christine + Sean "collude": always pick opposite; some leaves prob 0

prob 1/8 ← HT, TH

$E[\text{Brendan's winnings}] = \frac{2}{8}[+1 - 2 + 1 - 2] = -\frac{1}{2}$

equivalent definition of EXPECTATION: $Ex[R] = \sum_{x \in range(R)} x \cdot Pr[R = x]$

COROLLARY: if $R: S \rightarrow \{0,1\}$, $Ex[R] = 0 \cdot Pr[R=0] + 1 \cdot Pr[R=1] = Pr[R=1]$

COROLLARY: if $R: S \rightarrow \mathbb{N}$, $Ex[R] = \sum_{i=1}^{\infty} i \cdot Pr[R=i]$

THM: if $R: S \rightarrow \mathbb{N}$, $Ex[R] = \sum_{i=1}^{\infty} i \cdot Pr[R>i]$

$\sum_{i=0}^{\infty} Pr[R>i] = Pr[R>0] = Pr[R=1] + Pr[R=2] + \ldots$

$+ Pr[R>1] = \qquad Pr[R=2] + Pr[R=3] + \ldots$

$+ \ldots$

$\underline{1 \cdot Pr[R=1] + 2 \cdot Pr[R=2] + 3 \cdot Pr[R=3] + \ldots}$

$= \sum_{i=1}^{\infty} i \cdot Pr[R=i] = Ex[R]$

MEAN TIME TO "FAILURE:"

- flip coin w/ bias p. what is expected # flips until heads?
- computer crashes each hr w/ probab. p (indep.). what is expected # hrs until it crashes?

ANSWER TO ALL: $\frac{1}{p}$

✪ internalize

Ex: coin of bias p: $Ex[R] = \sum^{\infty} Pr[R > i]$

R = # flips until see H

$= \sum_{i=0}^{\infty} (1-p)^i$ ← 1st i flips need to be T for $R > i$

$= \frac{1}{1-(1-p)} = \frac{1}{p}$

GEOM. DIST: $Pr[c = i] = (1-p)^{i-1} \cdot p$ ← probability "fail" i-1 times before success @ time i

LINEARITY: $Ex[x+y] = Ex[x] + Ex[y]$ & $Ex[c \cdot x] = c \cdot Ex[x]$ & $Ex[\sum_{1 \le i \le n} c_i \cdot x_i] = \sum_{1 \le i \le n} c_i \cdot E[x_i]$

Pf: $E[X+Y] = \sum_{w \in S} (X+Y)(w) \cdot Pr(w)$ def Exp

$= \sum_{w \in S} (X(w) + Y(w)) Pr(w)$

$= \sum_{w} X(w) Pr(w) + \sum_{w} Y(w) Pr(w) = E[X] \cdot E[Y]$ ← only do this w/ expectation!

Ex: given 2 6 fair-sided die, what is expectation of sum of rolls?

R_1 = outcome of 1st roll

R_2 = outcome of 2nd roll

$Ex[R_1 + R_2] = Ex[R_1] + Ex[R_2] = 3.5 + 3.5 = 7$

no independence required!

Ex: coin of bias p, expected time until 2 H:

R_1 = # toss until 1st H

R_2 = afte 1st H, # toss until 2nd H

$Ex[R_1 + R_2] = Ex[R_1] + Ex[R_2] = \frac{1}{p} + \frac{1}{p} = \frac{2}{p}$

LINEARITY OF EXPECTATIONS: sums of indicators

Ex: given n coins, bias p, what is expected total # heads?

R_i = 1 of coin i is H, 0 otherwise

$Ex[R_i] = p$

$Ex[\#H] = Ex[\sum_i R_i] = \sum_i Ex[R_i] = n \cdot p$

SUM: indicator vars

$R_i = \begin{cases} 1 \text{ if ith person gets cellphone} \\ 0 \text{ otherwise} \end{cases}$

$R = R_1 + R_2 + \ldots + R_n$

$Ex[R] = Ex[R_1 + \ldots + R_n] = Ex[R_1] + Ex[R_2] + \ldots + Ex[R_n] = n \cdot \frac{1}{n} = 1$

Ex: n diner orders

waiter randomly spins food

expected # ppl that get dish back?

let $R_i = \begin{cases} 1 \text{ if ith person gets phone back} \\ 0 \text{ otherwise} \end{cases}$

let $R = R_1 + R_2 + \ldots + R_n$

$Ex[R] = Ex[R_1 + R_2 + \ldots + R_n]$

$= Ex[R_1] + Ex[R_2] + \ldots Ex[R_n]$

$= n \cdot \frac{1}{n} = 1$ (diff. distribution, only tells averages)

Ex: bday paradox: n days in yr, s ppl

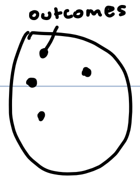
- bdays uniformly dist, mut. dep.
- "collision": 2 ppl same bday
- how many collisions?

$R_{ij} = \begin{cases} 1 & \text{if ith \& jth ppl same bday} \\ 0 & \text{otherwise} \end{cases}$

let $R = \Sigma_{i<j} R_{ij}$

$$Ex[R] = Ex\left[\Sigma_{i<j} R_{ij}\right]$$
$$= \Sigma_{i<j} Ex[R_{ij}]$$
$$= \binom{s}{2} \cdot \frac{1}{n} \approx \frac{s^2}{2n}$$

[5/18/25] - EXPECTATION & VARIANTS



sample space S

events $A \subseteq S$

probability $Pr: S \rightarrow [0,1]$

rv: $S \rightarrow$ range

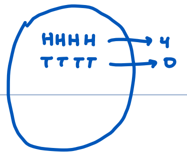
EXPECTATION:

$$\overset{\text{rv}}{\overset{\shortparallel}{Ex(R)}} = \sum_{x \in S} Pr(x) \cdot R(x)$$

$Ex(R+R') = Ex(R) + Ex(R')$ ← linearity

avg. of sum = sum of avgs.

expectation = "weighted average"



Ex: toss n coins $Pr(\text{heads}) = p$, $Pr(\text{tails}) = 1-p$

R = # heads in n tosses

$$Ex(R) = \sum_{x=\{H,T\}^n} Pr(x) \cdot R(x) = \sum_{i=\{0,1\}} \left(\sum_{\substack{x \text{ with} \\ i \text{ heads}}} Pr(x) \cdot R(x) \right) = \sum_i i \cdot p^i (1-p)^{n-i} \binom{n}{i} = np$$ ← assuming independence

Ex: $I_j = \begin{cases} 1 & \text{if jth toss is H} \\ 0 & \text{otherwise} \end{cases}$

$R = I_1 + I_2 + \dots + I_n$

$Ex(R) = \sum_{j=1}^{n} Ex(I_j) = \sum_{j=1}^{n} p = np$ ← linearity

THM 1: let S be probability space and $A_1, \dots, A_j$ be events.

$Ex(T) = \sum_{i=1}^{n} Pr(A_i)$ ← T = # events that happen

Pf: (notes)

THM 2: $Pr[T>0] \leq Ex(T)$

Pf: $Ex(T) = 0 \cdot Pr(T=0) + 1 \cdot Pr(T=1) + 2 \cdot Pr(T=2) + \dots + n \cdot Pr(T=n)$

$\geq Pr(T=1) + Pr(T=2) + \dots + Pr(T=n)$

$= Pr(T>0)$

Ex: $\left. \begin{array}{l} n = 1000 \\ p = 1/10^9 \end{array} \right] \rightarrow Pr(\text{at least 1 of n events happen}) \leq 1/10^9$

COROLLARY 3: $Pr(T>0) \leq \Sigma Pr(A_i)$

(union bound)

Pf: Thm 1 + Thm 2

THM 4: (murphy's law) given n mutually independent events $A_1, \dots A_n$, $Pr(T>0) \geq 1 - e^{-Ex(T)}$

Pf: $Pr(T=0) = Pr(\bar{A}_1 \cap \bar{A}_2 \dots \cap \bar{A}_n)$

by ind $\longrightarrow = \prod_{j=1}^{n} Pr(A_j)$

$= \prod_{j=1}^{n} (1 - Pr(A_j)) \leq \prod_j e^{-Pr(A)} = e^{-\Sigma Pr(A_j)} = e^{-Ex(T)}$

	assumptions:	conclusion:
THM 1:	nothing	
THM 2:	nothing	
COR 3:	nothing	
THM 4:	mutual ind.	
THM 5:	independence	

THM 5: $Ex(R_1, R_2) = Ex(R_1)\cdot Ex(R_2)$ if R_1, R_2 are independent

pf: $$Ex(R_1)\cdot Ex(R_2) = \left(\sum_x x\cdot Pr(R_1 = x)\right)\cdot\left(\sum_y y\cdot Pr(R_2=y)\right)$$

$$= \sum_{x,y} xy\ Pr(R_1 = x)\cdot Pr(R_2 = y)$$

$$= \sum_{x,y} xy\ Pr(R_1 = x \wedge R_2 = y)$$ ← uses independence

$$= \sum_z z \sum_{\substack{x,y, \\ \text{st.} \\ xy=z}} \underbrace{Pr(R_1 = x \cap R_2 = y)}_{Pr(R_1R_2 = z)} = Ex(R_1R_2)$$

R_1, R_2 are rolls of a dice

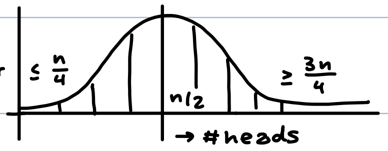
if independent: $Ex(R_1, R_2) = (3\frac{1}{2})^2$

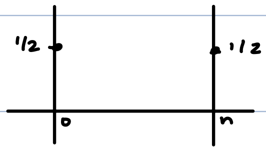
if $R_1 = R_2$: $Ex(R_1, R_2) = Ex(R_1^2) = \frac{1}{6}(1^2 + 2^2 + \dots + 6^2) = \frac{91}{6} \approx 15\frac{1}{6}$

coin: $$? \underset{\substack{| \\ \text{undefined} \\ \infty}}{Ex\left(\frac{1}{R}\right)} \overset{?}{=} \underset{\substack{\| \\ 2}}{\frac{1}{Ex(R)}} \times$$

linearity always works, product rule

TAILBOUNDS:





bitcoin:	Pr	1/2	+ 202
		1/2	- 200
nvidia		1/2	+ 20
		1/2	- 20
USD		1/2	+ 3
		1/2	- 1

want to measure spread
(how far r.v. deviates
from mean)

VARIANCE of rv R: $Var(R) = Ex(\underbrace{R - Ex(R)}_{\text{spread rv}}) = Ex(R) - Ex(\overbrace{Ex(R)}^{Ex(R)}) = 0$ ← times R went above cancel with R below

$$var(R) = Ex((R - Ex(R))^2)$$

STANDARD DEVIATION: $\sigma(R) = \sqrt{Var(R)}$

1: 1

2: 2, 2, 4.4, 8+

3: 1/4

[5/13/25]- TAIL INEQUALITIES

① MARKOVS INEQUALITY

② CHEBYSHEV INEQUALITY

③ CHERNOFF INEQUALITY

① MARKOVS INEQUALITY - "not everyone is above average"

* upper bound is correct but not tight - true prob. is much smaller

THM: if R is non-negative rv, then $\forall x > 0$,

$$\Pr[R \geq x] \leq \frac{Ex[R]}{x}$$

← large deviation ineq.

← inversely corr.

"probability that R is at least 2x its expected val is @ most 1/2"

COR: if R is a non-neg. rv, $\forall c > 0$, $[R \geq c \cdot Ex(R)] \leq \frac{1}{c}$

F & $\bar{F}$: 2 mutually exclusive & disjoint events

$$\left.\begin{array}{l}\Pr[E] = \Pr[E \mid F] \cdot \Pr[F] + \\ \Pr[E \mid \bar{F}] \cdot \Pr[\bar{F}]\end{array}\right] \text{law of total prob.}$$

$$= \Pr[E \wedge F] + \Pr[E \wedge \bar{F}]$$

PF: $Ex(R) = Ex(R \mid R \geq x) \cdot \underbrace{\Pr(R \geq x)}_{\text{what we care about}} + Ex(R \mid R < x) \cdot \Pr(R < x)$] law of total prob.

$$\geq x \cdot \Pr(R \geq x)$$

$$\Pr[R \geq x] \leq \frac{E(R)}{x}$$

$$Ex(R) = Ex(R \mid R > Ex(R)) \cdot \Pr(R > Ex(R)) + \underbrace{Ex(R \mid R \leq Ex(R)) \cdot \Pr(R \leq Ex(R))}_{} \geq 0$$

$$> Ex(R) \cdot \Pr(R > Ex(R))$$

Ex 1: let x = "lazy Susan" counting # ppl who get cell phones back.

$Ex(R) = 1$

$\underset{\text{by markov}}{\Pr(R \geq n) \leq \frac{1}{n}}$, in reality $\Pr(R \geq n) = \frac{1}{n}$ "markov is tight"

Ex 2: cellphone check problem

$Ex(R) = 1$ (R = sum of n indicator rv)

$\Pr(R \geq n) \leq \frac{1}{n}$
by markov

$\Pr(R \geq n) = \frac{1}{n!}$ ← in reality (everyone gets phone back)

Ex 3: R = rv that counts heads in n random coin tosses.

$Ex(R) = \frac{n}{2}$

$$\Pr\left(R \geq \frac{3n}{4}\right) \leq \frac{n/2}{3n/4} = \frac{2}{3}$$

why non-negativity in markov?

$$R = \begin{cases} +1 & \text{wp } 1/2 \\ -1 & \text{wp } 1/2 \end{cases}$$

$Ex(R) = 0$

THM: if $R \leq u$ for some $u \in \mathbb{R}$, then $\forall x < u$, $\Pr(R \leq x) \leq \frac{u - Ex(R)}{u - x}$

PF: $\Pr(R \leq x) = \Pr(\underbrace{u - R}_{R} \geq u - x) \underset{\text{markov}}{\leq} \frac{Ex(u - R)}{u - x} = \frac{u - Ex(R)}{u - x}$

$u - R \geq u - x$

$-R \geq -x$

CHEBYSHEV: $\forall x > 0$ & any rv R,

$$\Pr(|R - Ex(R)| \geq x) \leq \frac{var(R)}{x^2} = \left(\frac{\sigma(R)}{x}\right)^2$$

dist. from mean

"better bound"

① no assumptions

② 2-sided bound

reminder: $var(R) = \mathbb{E}x((R - Ex(R))^2)$

$= var(R_1 + R_2) = var(R_1) + var(R_2)$

IF INDEPENDENT

$\sigma(R) = \sqrt{var(R)}$

COR: $\Pr(|R - Ex(R)| \geq c \cdot Ex(R)) \leq \frac{1}{c^2}$

$var(R) = var(R_1 + R_2 + \ldots + R_n)$

assume ind. $= var(R_1) + var(R_2) + \ldots + var(R_n)$

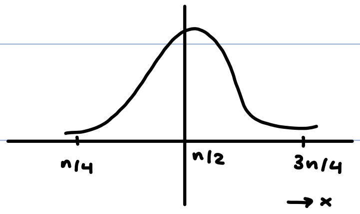
$= \frac{1}{4} + \frac{1}{4} + \ldots = \frac{n}{4}$

$\Pr(R \geq \frac{3n}{4}) \leq \Pr(R \geq \frac{3n}{4} \text{ or } R \leq \frac{n}{4})$

$= \Pr(|R - \frac{n}{2}| \geq \frac{n}{4})$

$\leq \frac{n/4}{(n/4)^2} = \frac{4}{n}$ ← assume ind.

(by cheb.)



PF: $\Pr(|R - Ex(R)| \geq x)$

$= \Pr((R - Ex(R))^2 \geq x^2)$

$\leq \frac{Ex((R - Ex(R))^2)}{x} = \frac{var(R)}{x^2}$ ▭

CHERNOFF: let $R_1, \ldots, R_n$ be any mutually independence rvs s.t. $0 \leq R_j \leq 1$ * one-sided bound

let $R = R_1 + R_2 + \ldots + R_n$

for any $c > 1$, $\Pr(R \geq c \cdot Ex(R)) \leq e^{-z \cdot Ex(R)}$ where $z = c \ln c - c + 1$

$\Pr(R \geq \frac{3n}{4}) \leq e^{-(0.1)(\overset{Ex(R)}{\frac{n}{2}})} = e^{-n/20}$ as n grows, prob. shrinks

$\frac{3n}{4} = \frac{3}{2}Ex(R)$

$z = \frac{3}{2}\ln\frac{3}{2} - \frac{3}{2} + 1 \approx 0.1$

PF: apply Markov to c^R