cattu - 964684110

AXIOM: proposition assumed to be T

PROPOSITIONS: T/F statement

LEMMA: "stepping stone" theorem statement

PREDICATE: statement whose truth depends on variable $P(n) ::=$

STIRLINGS APPROX: $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ | for large n: $\binom{n}{k} \sim \frac{n^k}{k!}$

els of set satisfying a predicate

SET BUILDER: $\{n \in \mathbb{N} \mid \text{isprime}(n)\} = \{2, 3, 5, \dots\}$

$x \in A$ - x is element of A | $A \subseteq B$ - A is subset of B (every el of A is in B)
$x \notin A$ - x not element of A | $A \cap B$ - intersection (els in both A & B)
$A \cup B$ - union (els in either) | $A \setminus B$ - set difference (in A but not in B)

TRUTH TABLE

$\wedge$ and | $p \Leftrightarrow q$ iff "if & only if"
$\vee$ or
xand exclusive and (TT=T, FF=T, TF=F)
xor, $\oplus$ exclusive or (TT=F, FT=T, FF=F)

x	y	left ($x \to y$)	right ($\neg y \to \neg x$)	whole
T	T	T	T	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

PROOFS:

∃ (there exists)
THM: ∃ .....
PF: Show that some val works

∀ (for all)
THM: ∀ .....
PF: introduce generic example & solve.

∀ counterexample
THM: ∀...
PF: not true b/c ... (give counter)

P→Q contrapos $(P \to Q) \to (\bar{Q} \to \bar{P})$
THM: ∀...
PF: suppose $n \in \mathbb{Z}$. pf by contra: assume $\bar{Q}$; wts $\bar{P}$
...

CONTRADICTION "indirect"
THM: ...
PF: pf. by contradiction. assume opposite
→ find a contradiction
___, contradicting the fact that ___.

INDUCTION:
$P(n) ::= \dots$
THM: $\forall n \in \mathbb{N}.\ P(n)$
PF: by induction, using $P(n)$.
BASE CASE(S): $P(\_) = \_\_$, $P(\_) = \_\_$
INDUCTIVE STEP: suppose $n \geq 0$ and assume $P(n)$; WTS $P(n+1)$ ...
CONCLUSION: since we found ___ by induction, we proved $P(n)$ holds for $n \geq 0$.

STRONG INDUCTION:
$P(n) ::= \dots$
THM: $\forall n \in \mathbb{N}.\ P(n)$
PF: by induction, using $P(n)$.
BASE CASE(S): $P(\_) = \_\_$, $P(\_) = \_\_$
INDUCTIVE STEP: assume $P(0), P(1), P(2), \dots, P(n)$ are all true. WTS: $P(n+1)$

CASEWORK:
THM: ...
PF: by cases
CASE 1: assume ... then, ___ is true b/c ___
CASE 2: assume ... then, ___ is true b/c ___
at least one of ___ must be true b/c ___
(aka, these cases are exhaustive)

STATE MACHINES: collection of states, specified initial state, and for each state S, a set of possible transitions to other states.

PRESERVED PRED $P(\ )$: for every state $S \to t$, if $P(S) = T$, $P(t) = T$. ↗ can typically prove w/ casework

INVARIANT: state pred. T for all reachable states if pred. T in start state (P holds for S_0 & P is preserved for possible transitions)

MONOTONIC DERIVED VARIABLE $f(s)$: f always in $\mathbb{N}$ and f strictly incr/decr. & terminates after @ most $f(\text{initial})$ steps

TERMINATION: set of states w/ no possible transitions & prove machine reaches those states

RUNTIME: $|f(S_0) - \text{bound}|$

PROVE INVARIANT: #ONE-SIDED TEST (satisfying invar. NOT guarantee a state's reachability)
- define invariant $Q(n_a, n_b, \dots) ::= \dots$. we'll prove that Q is invariant.
- @ start state: $Q(\_, \_) = \dots$, so property holds.
- CASES: (can also use induction)
  - transition $(\_, \_)$: ...
  - transition $(\_, \_)$: ...

#can also define predicate P & prove P is invar.

since ___, these cases are exhaustive. since $P(n_a, n_b)$ true @ the start state & preserved across transitions, the Invariant Principle shows it is true @ all reachable states.
(OR: since ..., ... is unreachable, ...)

Ex: $P(x,y) ::= y - x$ is a multiple of 3.

function mapping states to values

PROVE DERIVED VARIABLE: ↑ + TERM.
$f(s) = \dots$
- prove $f(s)$ always in $\mathbb{N}$
- prove $f(s)$ strictly incr/decr.
  - if decr: 1st is highest, has lower bound
  - if incr: 1st is lowest, has upper bound
- max steps $= \frac{\text{initial} - \text{bound}}{\#\text{steps}\ (1)}$
- so, we found a derived var. that ___ by at least 1 @ every step (& can't ___ past ___).
- if value starts @ m, no more that $\underline{m}$ steps possible, otherwise derived var will be ___

STATES: the states are $(x, y, \dots)$ for $x, y, \dots \in \mathbb{Z}$ (with restriction $x > y > 0$)

INITIAL STATE: (...)

TRANSITIONS: $(x+2, y-1), (x.., y..)$..

SUMS:

$$\sum_{k=1}^{n} k = 1 + 2 + \dots + k = \frac{n(n+1)}{2}$$

$$\sum_{k=0}^{n-1} x^k = 1 + x + x^2 + \dots = \frac{(1 - x^n)}{1 - x} \text{ or } \frac{a(1 - x^n)}{1 - x}$$

a = 1st term, n = # terms

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

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

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

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

PERTURBATION: manipulate
Ex: $S = \sum_{k=1}^{n} k^2 x^k = x + 4x^2 + 9x^3 + \dots$
$xS = \qquad\qquad x^2 + 4x^3 + \dots$
$S - xS = \dots$
TRY: +/-, x/÷, basic ops.

GUESS/CHECK (ANSATZ):
- look @ small terms
- common: pow of 2, squares, fib
- find pattern & prove w/ induction

INTEGRAL METHOD: squeeze thm.
when $f = +$ & weakly incr: $I + f(1) \leq S \leq I + f(n)$
when $f = -$ & weakly decr: $I + f(n) \leq S \leq I + f(1)$ only diff!
incr: $f(1) + \dots + f(7) + \int_8^\infty \dots \leq \dots \leq f(1) + \dots + f(7) + \int_8^\infty + f(8)$
decr: $f(n) + \int_1^n \dots \leq S \leq \int_1^n \dots + f(1)$
since lower $\leq S \to S \in \Omega(\_)$
since upper $\geq S \to S \in O(\_)$ → so, $S \in \Theta(f(n))$

ASYMPTOTICS:
- focus on dominant term
- ignore constants/lower order

$\log < x^n < n^x < n!$
poly exp fact.

$f \in \Theta(g)$ ≈	$f \sim g$ =	$f \in O(g)$ ≤	$f \in o(g)$ <	$f \in \omega(g)$ >	$f \in \Omega(g)$ ≥
$f \in O(g)$ & $f \in \Omega(g)$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$	$\exists c > 0\ \exists n_0 \geq 0\ \forall n \geq n_0\ f(n) \leq c g(n)$; $\lim f/g$ = finite	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$	$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty$	$g \in O(f)$
EXAMPLES: $2n + \log n \in \Theta(n)$; $n \in \Theta\left(\frac{3n^3}{(n+1)(n-1)}\right)$ b/c $\lim_{n\to\infty} \frac{f}{g} = \frac{1}{3}$ & $\lim_{n\to\infty} \frac{g}{f} = 3$	$n+1 \sim n$; $n^2 + n \sim n^2$	$\log n \in O(n)$; $f(n) = \frac{3n-7}{n+4}$, $g(n) = 4$; $\lim_{n\to\infty} f(n) = 3$, $3 < 4 \to f \in O(g)$	$n^7 \in o(1.01^n)$	$\sqrt{n} \in \omega(\log^{300} n)$; $n2^n \in \omega(n)$	Ex: $f(n) = 1 + (n \sin(n\pi/2))^2$, $g(n) = 3n$; $f \notin g$ b/c $f(2n+1) = (2n+1)^2$ & $\lim f/g = \infty$; $g \notin f$ b/c $f(2n) = 1$ & $\lim g/f = \infty$ → ∴ not asymptotically comp.

$f \sim g \to f \in \Theta(g)$
$f \in \Theta(g) \to f \in O(g),\ f \in \Omega(g)$
$f \in o(g) \to f \in O(g)$
$f \in \omega(g) \to f \in \Omega(g)$

$o \to O$
$\omega \to \Omega$
O & $\Omega \leftrightarrow \Theta$

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

MASTER'S THM: let $T(n) = aT\left(\lceil \frac{n}{b} \rceil\right) + f(n)$, $b > 1$, $a \geq 1$

≤ CASE 1: if $f(n) \in O(n^{(\log_b a) - \varepsilon})$, for some $\varepsilon > 0$, $T(n) \in \Theta(n^{\log_b a})$

= CASE 2: if $f(n) \in \Theta(n^{\log_b a})$, $T(n) \in \Theta(n^{\log_b a} \cdot \log n)$

≥ CASE 3: if $f(n) \in \Omega(n^{(\log_b a) + \varepsilon})$ for some $\varepsilon > 0$ & $af(\lceil \frac{n}{b} \rceil) \leq c f(n)$, $c < 1$, $T(n) \in \Theta(f(n))$

* NOT work for <, >

* NOT exhaustive

L'HOPITALS: if $\lim_{x\to a} \frac{f(x)}{g(x)} = 0$ or ∞, then $\lim_{x\to a} \frac{f'(x)}{g'(x)}$

RECURRENCES: inductive sequence
$T(n) = aT\left(\frac{n}{b}\right) + f(n)$

PLUG & CHUG:
$T(n) = aT\left(\frac{n}{b}\right) + f(n)$
$T\left(\frac{n}{2}\right) = a\left(aT\left(\frac{n}{b^2}\right) + f\left(\frac{n}{b}\right)\right) + f(n)$
⋮
$= a^k T\left(\frac{n}{b^k}\right) + \_\_ n^{?} \sum_{i=\_} \_\_$ ↖ get closed form
$= \dots$ simplify
let $k = \log_b n$ and we know $b^k = n$
$T(n) = a^{\log_b n} T(1) + \dots$
(if prove): let $P(n) ::= T(n) = \dots$ (induction)

LOG PROPERTIES:
$\log_a b = \frac{\log_x b}{\log_x a}$
$\log(x^2) = 2\log x$
$\log(ab) = \log a + \log b$
$\log_a b = \frac{1}{\log_b a}$

DERIVATIVES:
$\frac{d}{dx}(\log_a x) = \frac{1}{x \ln a}$
$\frac{d}{dx}(\ln x) = \frac{1}{x}$
$\frac{d}{dx}(a^x) = a^x \ln a$

EXAMPLES:

Problem 6. Recurrences

Use the Plug and Chug method to find an exact closed form formula for $a(n)$ as a function of n, where $a(n) = 2a(n-1) + 3^n$ for $n \geq 1$, and $a(0) = 5$.

Solution. We perform a few substitutions to look for a pattern:

$$\begin{aligned} a(n) &= 3^n + 2a(n-1) \\ &= 3^n + 2(3^{n-1} + 2a(n-2)) \\ &= 3^n + 2 \cdot 3^{n-1} + 4a(n-2) \\ &= 3^n + 2 \cdot 3^{n-1} + 2^2 \cdot 3^{n-2} + 8 \cdot a(n-3) \\ &\vdots \end{aligned}$$

After k expansions, we can guess that the formula takes the form

$$\begin{aligned} a(n) &= 3^n + 2 \cdot 3^{n-1} + \dots + 2^k 3^{n-k} + 2^{k+1} a(n-k-1) \\ &= \left(\sum_{i=0}^{k} 3^n \cdot (2/3)^i\right) + 2^{k+1} a(n-k-1). \end{aligned}$$

Choosing $k = n - 1$, we find that

$$\begin{aligned} &= \left(\sum_{i=0}^{n-1} 3^n \cdot (2/3)^i\right) + 2^n \cdot a(0) \\ &= 3^n \cdot \frac{1 - (2/3)^n}{1 - (2/3)} + 5 \cdot 2^n, \end{aligned}$$

which is in closed form!

This can optionally be simplied, to $a(n) = 2^{n+1} + 3^{n+1}$.

(a) There exists a *nonconstant* function $f(n)$ that is $\Theta(1)$.

Solution. True. There are many! Any function that is eventually bounded within some interval $[c_0, c_1]$, for some positive numbers $0 < c_0 \leq c_1$, is $\Theta(1)$. For example, $f(n) = 61 + \frac{20}{n}$. Then $f(n) \sim 61$ and therefore $f(n) \in \Theta(1)$. ■

(b) Suppose we start with 100 of each token. Prove carefully that the state (50,8) is unreachable. If you would like to use a fact from the previous part, you must prove it here.

Solution. Define the predicate $P(n_a, n_b) ::= \text{rem}(n_a + n_b, 3) = 2$; we'll prove that P is invariant.

0, 100), the property $P(100, 100)$ holds because $100 + 100 = 200 \equiv 2$
we have any state (n_a, n_b) where $P(n_a, n_b)$ holds; we must show that
owing any transition from (n_a, n_b). The first kind of transition takes
), and $(n_a - 1) + (n_b + 1) = n_a + n_b$, which has remainder 2 when
umption), so the property holds. For the second kind of transition,
$n_a + n_b - 3$, which has the same remainder as $n_a + n_b$, namely, 2.
e at the start state and is preserved across transitions, the Invariant
it is true at all reachable states.

■) + 8, which has remainder 1, thus it is unreachable. ■

(d) Explain why the Master Theorem **cannot** be used to analyze $T(n) = 2T(\lfloor n/2 \rfloor) + n \log n$. (You don't need to find a Θ-bound yourself, but it could be a fun optional challenge!)

Solution. Since $a = b = 2$, the critical exponent is $\log_b a = 1$. The ratios $(n \log n)/n^1$ and $n^{1+\epsilon}/(n \log n)$ both limit to ∞ as $n \to \infty$, no matter how small $\epsilon > 0$ is chosen, so $f(n)$ grows too fast to belong to $\Theta(n^1)$ (so cases 1 and 2 don't apply), and at the same time, $f(n)$ grows and too slow for $\Omega(n^{1+\epsilon})$ (so case 3 doesn't apply).

This example shows that the **Master Theorem is not exhaustive**: there are cases like this one that can "fall through the cracks" by being simultaneously too big for case 2 but too small for case 3. It's possible to fit between cases 1 and 2 similarly; try to come up with such an example. ■

DAYS 8-16; PSETS 5-8

MOD RULES:

1) $a \equiv a \pmod n$
2) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$
3) $a \equiv_n b$ & $b \equiv_n c \Rightarrow a \equiv_n c$
4) $a \equiv_n b \Rightarrow a + c \equiv_n b + c$
5) $a \equiv_n b \Rightarrow ac \equiv_n bc$
6) $a \equiv_n b$ & $c \equiv_n d \Rightarrow a + c \equiv_n b + d$
7) $a \equiv_n b$ & $c \equiv_n d \Rightarrow ac \equiv_n bd$

MODULAR EXS:

Ex: Find last digit of $12^{202} \bmod 10$

$12 \equiv_{10} 2$, $2^1 \equiv_{10} 2$, $2^2 \equiv_{10} 4$, $2^3 \equiv_{10} 8$, $2^4 \equiv_{10} 6$, $2^5 \equiv_{10} 2$ — cycle

$202 = 4 \cdot 50 + 2$, remainder 2

$12^{202} \equiv_{10} 2^2 \equiv_{10} \boxed{4}$

Ex: $123^{57} \bmod 124$

$\equiv_{124} (-1)^{57} \equiv_{124} -1 \equiv_{124} \boxed{123}$

Ex: $\text{rem}(96^{123456789}, 97)$

$96 \equiv_{97} -1 \rightarrow (-1)^{\cdots} \equiv_{97} -1 \equiv_{97} \boxed{96}$

Ex: HANDSHAKE - bipartite graph (L, R, E), L vertexes = deg 10, R vertexes = deg 12. is there a matching covering L?

$10 \cdot |L| = 12 \cdot |R|$

$|L| = \frac{12}{10}|R| \rightarrow$ more vertices in L than R.

DIVISIBILITY: $a \mid b$ (smaller, bigger) $ak = b$

Ex: $3 \mid 12$, $-5 \mid 100$ "b is divisible by a" "a divides b"

properties:
- → if $a \mid b$, $b \mid c$, then $a \mid c$
- → if $a \mid b$, then $a \mid bc$
- → if $a \mid b$ & $a \mid c$, then $a \mid b + c$ → $xa + ya = (x+y)a$
- → if $a \mid b$ & $a \mid c$, then $a \mid sb + tc$ for $\forall s, t \in \mathbb{Z}$ ($sb + tc$ known as integer linear combo of b & c) (ILC)
- → for all $c \neq 0$, $a \mid b$ iff $ca \mid cb$
- → $n \mid -n$ & $n \mid 0$

GCD: largest (non-neg.) integer d s.t. $d \mid a$, $d \mid b$ $\gcd(a,b)$
- → lemma: $\gcd(a, 0) = |a|$
- → lemma: $\gcd(a,b) = \gcd(a, b-a)$
- → lemma: $\gcd(a,b) = \gcd(a, b \text{rem} a)$
- → $\gcd(ka, kb) = k \cdot \gcd(a,b)$
- → if $\gcd(a,b) = 1$ & $\gcd(b,c) = 1$, then $\gcd(a,c) = 1$ (invars)
- → if $a \mid bc$ & $\gcd(a,b) = 1$, then $a \mid c$

EUCLID'S ALGO: for gcd

START: (a, b)

STATES: (x, y), $x \geq y \geq 0$

TRANSITION: $(x,y) \rightarrow (y, x \text{rem} y)$

END STATE: $(x, 0) \rightarrow$ return x

INVAR: $P(x,y) := \gcd(x,y) = \gcd(a,b)$

TERMIN: $x + y$ strictly decr. b/c $x \text{rem} y < x$ when $y \leq x$. # steps @ most $a + b$

PULVERIZER: (extended Euclid's GCD algo) maintains:

$\gcd(x,y) = \gcd(a,b)$, $x = as + bt$, $y = au + bv$

FOR: · gcd · linear combo · mult. inverses

x	y	(rem(x,y)) = x - q · y	
259	70	49	= 259 - 3·70
70	49	21	= 70 - 1·49 = 70 - (259 - 3·70) = 4·70 - 1·259
49	21	7	= 49 - 2·21 = 49 - 2(4·70 - 259) = (259 - 3·70) - 2(4·70 - 259) = $\boxed{3 \cdot 259 - 11 \cdot 70}$ (s a t b)
21	GCD $\boxed{7}$	0	gcd(a,b) = sa + tb

WHEN GCD = 1: EX:

x	y	r = 5x - ty
19	17	2 = 19 - 17
17	2	1 = 17 - 8·2 = 17 - 8(19 - 17) = 9·17 - 8·19
2	GCD $\boxed{1}$	0

$\rightarrow 1 = 9 \cdot 17 - 8 \cdot 19$ → $-8 \cdot 19 \equiv 1 \bmod 17$, $9 \cdot 17 \equiv 1 \bmod 19$

∗ exists when coprime

aka. relatively prime

CHINESE REMAINDER THM: if $\gcd(p, q) = 1$, then there is a unique solution mod pq to $x \equiv_p a$ & $x \equiv_q b$

let q^{-1} = inverse of q mod p, p^{-1} = inverse of p mod q

$x = a \cdot q^{-1} q + b \cdot p^{-1} p$

MODULAR ARITHMETIC: $a \equiv_n b$ iff $n \mid a - b$ (a is congruent to b mod n iff $n \mid (a-b)$)

Ex: $17 \equiv_5 12$, $17 \equiv_5 -3$ $(17 - -3 = 20)$

if $a \equiv_n b$, then for any c,
- → $a + c \equiv_n b + c$ ← add
- → $ac \equiv_n bc$ ← multiply
- → $a - c \equiv_n b - c$ ← subtract
- → $c - a \equiv_n c - b$
- → $a^c \equiv_n b^c$ ← exponentiate

NO WORK $c^a \not\equiv_n c^b$

MULTIPLICATIVE INVERSE: of a mod n is a number $0 \leq b < n$ s.t. $a \cdot b \equiv_n 1$ → if $n \mid (ab - 1)$

if $1 = a \cdot b - q \cdot n$ ← b tells the inverse

$\gcd(a, n) \equiv_n 1$ & $\gcd(b, n) \equiv_n 1$

FERMAT'S LITTLE THM: $a^{p-1} \equiv_p 1$ for a, p coprime ($\gcd$ is 1) → good for RSA + large powers

Ex: $\text{rem}(24^{78}, 79) = 1$ b/c 79 is prime & 24 is not multiple. $24^{79-1} \equiv 1 \bmod 79$

MODULAR INVERSE:

$(1 = ax + by) \bmod x \rightarrow by \equiv_x 1$ ← b is the mod inverse of y mod x

$(1 = ax + by) \bmod y \rightarrow ax \equiv_y 1$ ← a is the mod inverse of x mod y

a x + b y

if $\gcd(a,b) = 1 \rightarrow sa + tb = 1$

$a \equiv_y x^{-1}$ and $b \equiv_x y^{-1}$

Ex: $19y \equiv 3 \bmod 17$ what is y?

$-8 \cdot 19y \equiv_{17} 3 \cdot -8$

$y \equiv_{17} -24$ +17 +17

$y \equiv_{17} \boxed{10}$

∃x s.t. $ax \equiv_b 1$ only happens when $\gcd(a,b) = 1$. Symm: $\gcd(b,a) = 1$

IDEA:
- bob has public + priv. key
- anyone can encrypt to bob w/ public key
- only bob can decrypt w/ private key

CRYPTOGRAPHY: HISTORY:
- CAESAR CIPHER: shifts each letter by certain # in 0-25. (A=0, B=1...)
- VERNAM CIPHER: shifts each letter by random #, cannot send multiple msgs

RSA
- PRIVATE KEY: (P, Q, d)
- PUBLIC KEY: (N = PQ, e) · P & Q = relatively prime

BEFORE:
1) generate 2 distinct primes, p & q. (kept hidden)
2) $n = pq$
3) integer e s.t. $\gcd(e, \phi(n)) = 1 \rightarrow \phi(n) = (p-1)(q-1)$
4) public key: (e, n)
5) $d \equiv_{\phi(n)} 1$ using Pulverizer. secret key: (d, n)

ENCRYPTION:
- message m, $0 \leq m < N$
- check $\gcd(m, n) = 1$
- encode message m to produce public key

$\text{Enc}(m) = m^e \bmod N$

DECRYPTION:
- receiver decrypts message m' back to m using the secret key

$\text{Dec}(c) = c^d \bmod N$

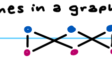
FLT $\text{Dec}(\text{Enc}(m)) = m^{de} \bmod N = m \bmod N$

BIPARTITE: iff V can be partitioned into disjoint sets L & R s.t. every edge has 1 endpoint in each L & R, but no edges connect vertices within the same set. $X(G) = 2$

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

BIPARTITE MATCHING: finding max matches in a graph

avg. $A_M = \frac{\sum_{m \in M} \deg(m)}{|M|} = \frac{|E|}{|M|}$



GREEDY ALG:
- give each vertex smallest possible color. if $\deg s = n$
- guarantees upper bound of colors = n+1

GRAPHS:

SIMPLE GRAPHS: G is a pair (V, E) where V = non-empty set of vertices & E = set of 2 element subsets of V called edges (undirected)

NOT ALLOWED:
- self-loops
- duplicate edges
- empty $V = \{\}$

$V = \{a, b, c, d, \ldots\}$

$E = \{\{a,b\}, \{a,c\}, \ldots\}$

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

Ex: deg. seq. can't be (2, 2, 1) b/c ∑ odd

MATCHING: each node has deg = 1

MAXIMAL: ∄ M' s.t. $M \subseteq M'$

MAXIMUM: ∄ M' s.t. $|M| < |M'|$

PERFECT MATCHING: size |V|/2 (use all pairs) — n n has n! pms

STABLE MATCHING: GALE-SHAPLEY → gives 1-2 possible stable mat. → might be more stable match.

UNSTABLE if rogue pair

ROGUE PAIR: a & e prefer each other over their assigned partners
- provides up to 2 stable matchings
- prove algo finishes, is stable, provides perfect matchings

FEASIBLE: if there exists a stable matching where a & e paired

OPTIMAL: most preferred feasible partner

PESSIMAL: least possible feasible partner
- gives every applicant their optimal match
- gives every evaluator their pessimal match

INVARIANT: for every pokemon p & trainer t, if t crossed off t's list, t's current is preferred.

ADJACENT: if 2 nodes a & b connected by edge

INCIDENT: if an edge {a,b} connected to a & b.

DEGREE: of vertex v is # edges incident to v

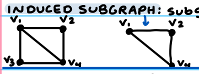
DEGREE SEQUENCE: all node degs in G listed ex: (2,2,4)

PROPER K-COLORING: function $f: V \rightarrow C$ where $|C| \leq k$ s.t. for all edges $\{u,v\} \in E$, $f(u) \neq f(v)$

X(G) CHROMATIC NUMBER: smallest k s.t. G = proper k-col.
- → prove X works & < X does not work

BUILD-UP ERROR: not proving theorem for all graphs

INDUCED SUBGRAPH: subgraph w/ all edges in E b/t V'



INDUCTION on graphs: (s

P(n) ::= ...

BASE CASE: start P(1) for V, P(0) for E (multiple for ind.)

IND. STEP: assume P(...), ..., P(n) for n ≥ ...
- WTS $P(n) \rightarrow P(n+1)$ for all n ≥ ...
- take graph G with n+1 nodes.
- ∗FIND PROPERTY∗ remove an ___ & incid.
- we get ∗RESTATE PROPERTIES, for G'
- we know we can apply ind. hyp on induced subgraph G', with PROPERTY
- add back ___ & relate PROPERTY

since we found ___ by induction, we have proved P(n) for all n ≥ ...

TREES:
- connected + acyclic
- adding edge creates cycle
- n vertex, n-1 edges
- remove any edge disconnects graph
- every pair of vertices connected by unique path

LEAF: vertex w/ deg = 1

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

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

can repeat vertices/edges [WALK: sequence of vertices $(v_0, \ldots, v_k)$; length = k (# edges)

CLOSED WALK: begins & ends @ same vertex (length ≥ 3)

CYCLE: closed walk of length ≥ 3 with no repeats except start/end

CONNECTED: a & b iff exists a walk from a to b

not necessarily closed [PATH: walk with no repeated vertices (may not be most efficient)

vertices can repeat; closed (tour) [EULERIAN TOUR: use every edge exactly once & visit all vertexes

TOUR: closed trail (starts/ends on same vertex)
- tour: all vertexes = even deg; path: even except start/end

CONNECTED COMPONENT: subgraph induced by vertices reachable by v

PROPERTIES-GRAPH

REFLEXIVE: A connected to itself

SYMMETRIC: A connect to B iff B connect to A

TRANSITIVE: A connect B, B to C implies A to C

DIRECTED GRAPHS:

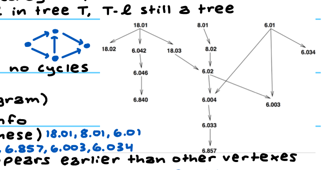
INDEG(v) = {u ∈ V | (u,v) ∈ E}

OUTDEG(v) = {w ∈ V | (v,w) ∈ E}

indeg(v) → ⓥ → outdeg(v)

HANDSHAKE LEMMA (directed): $\sum_{v \in V} \deg(v) = 2 \cdot |E|$

DIRECTED ACYCLIC GRAPHS (DAG): directed graphs with no cycles



CONSTRAINT GRAPHS:

COVERING EDGES: only path b/t endpoints (Hasse Diagram)

REDUNDANT EDGES: edge that doesn't give new info

MINIMAL ELEMENT (SOURCE): no in-arrows (start w/ these) 18.01, 8.01, 6.01

MAXIMAL ELEMENT (SINK): no out-arrows (end) 6.840, 6.857, 6.003, 6.034

TOPOLOGICAL SORT: list of nodes s.t. every vertex appears earlier than other vertexes reachable from it. Ex: 1801, 801, 601, 1802, 6042, 1803, 802, 6034, 602, 6840, 6003, 6033, 6857

COMPARABLE: a can reach v, but can't be processed @ same time (ordering)

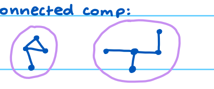
CHAIN: set of nodes s.t. any pair is comparable {1801, 1803, 602, 6004, 6033, 6857}

CRITICAL PATH: longest chain (length = # vertices) = min # terms req. to grad → 6

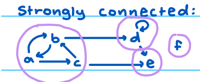
ANTICHAIN: set of uncomparable nodes (can process @ same time) {1802, 6042, 1803, 802, 6034}

- max # of classes possibly take @ once = antichain → 5

connected comp:



Strongly connected:



edges can go b/t

UNDIRECTED:
- vertices V & edges $E \subseteq \{\{u,v\} \mid u, v \in V$ & $u \neq v\}$
- only 1 edge b/t {u,v}
- no self loops
- $\sum_{v \in V} \deg(v) = 2|E|$
- walk is $v_0 \ldots \rightarrow v_k$ (len = edges)
- each $\{v_i, v_{i+1}\} \in E$
- path has no repeated vertexes or edges
- closed if $v_0 = v_k$
- cycle: closed walk len > 2 with no other repeated vertex/edge
- could be reflexive (walk len 0)
- symmetric (reverse path)
- transitive (concat. walks)
- G connected if every pair of vertices connected

DIRECTED:
- vertices V & edges $E \subseteq \{(u,v) \mid u, v \in V\}$
- can have self loops {u,u}
- can have (u,v), (v,u)
- $\sum_{v \in V} \text{indeg}(v) = \sum_{v \in V} \text{outdeg}(v) = |E|$
- each $(v_i, v_{i+1}) \in E$
- path has no repeated vertexes or edges
- closed if $v_0 = v_k$
- cycle: closed walk len > 0 with no other repeated vertex/edge
- NOT symmetric
- reflexive (walk len = 0)
- transitive (concat. walks) a b c — not mut.
- strongly connected if mutually reachable (for vertices a, b) (cycle)
- G strongly connected if every pair of vertices strongly connected
  - can have edges b/t SCCs
- Euclidean means indeg = outdeg for every vertex & G is strongly conn.

RELATIONS: $R \subseteq A \times B$ has 3 parts
- domain, set A (left) {(a,b) | a ∈ A, b ∈ B}
- codomain, set B (right)
- set $R \subseteq A \times B$ (subset)

a R b, (a,b) ∈ R, R(a,b) — same

$R \subseteq A \times B$ is a...

FUNCTION: iff every a ∈ A has at most one b ∈ B s.t. aRb

TOTAL: iff every a ∈ A has ≥ 1 arrow out → every a ∈ A has at most 1 arrow out

TOTAL FUNCTION: iff every a ∈ A has =1 arrow out

INJECTIVE: iff b ∈ B has ≤ 1 arrow in

SUBJECTIVE: iff b ∈ B has ≥ 1 arrow in

BIJECTION: iff injective, surjective, func, & total

EQUIVALENCE: if $R \subseteq A \times A$

REFLEXIVE: iff a ∈ A, aRa (same as itself)

SYMMETRIC: iff ∀a, b ∈ A, aRb ⇔ bRa (no order)

TRANSITIVE: iff ∀a, b, c ∈ A, (aRb ∧ bRa) → aRc

ANTISYM: iff ∀a, b ∈ A, (aRb and bRa) ⇒ (a=b) prove: outdeg = 1 & indeg = 1 (excl. always)

EQUIVALENCE RELATION: if R is reflexive, symmetric, transitive Ex:

WEAK PARTIAL ORDER: if R is reflexive, antisymmetric, transitive Ex: DAG,

COMPARABLE: iff aRb or bRa (unless a = b)

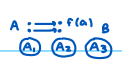
TOTAL (LINEAR) ORDER: iff all pairs comparable

COUNTING:

PRODUCT RULE: $|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \times |A_2| \times \ldots \times |A_n|$ ← multiply ways within a case

BIJECTION RULE: if ∃ bijection A → B, then |A| = |B| ← same # elements

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



DIVISION RULE: if $f: A \rightarrow B$ is k-to-1, then $|A| = k \cdot |B|$, and $|B| = \frac{|A|}{k}$

arrows out = k · arrows in

4-to-1 (everything in B gets mapped 4x) · divide when order does not matter

GENERALIZED PRODUCT RULE: S = set of length-k sequences
- n_1 possible 1st entries
- n_2 possible 2nd ...

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

n choose k:

P = n # permutations

S: k # subsets

$f(a_0, \ldots, a_n) = \{a_0, \ldots, a_k\}$ (seq → set)

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

DONUTS & DIVIDERS:

n donuts, k flavors → k-1 dividers

$$\binom{n+k-1}{n} = \binom{n+k-1}{k-1} = \frac{(n+k-1)!}{n!(k-1)!}$$

- donuts & dividers not distinct
- choosing position

PROPERTY: $2^n = \sum_{i=0}^{n} \binom{n}{i}$ "at least one" = full set of permutations - "none"

RSA:

Problem 2. Something about RSA [10 points]

Alicekazam has public RSA key $(n_a, e_a) = (9995, 17)$.
Bobasaur has public RSA key $(n_b, e_b) = (9997, 17)$.
Help Alicekazam encrypt the message 10 so she can send it to Bobasaur. Show your work.

Solution. Alicekazam needs to use Bobasaur's public key. To encrypt, she computes rem$(10^{17}, 9997)$. Using repeated squaring:

$$\begin{aligned}
10^1 &\equiv_{9997} 10 \\
10^2 &\equiv_{9997} 100 \\
10^4 &\equiv_{9997} 100^2 \equiv_{9997} 10000 \equiv_{9997} 3 \\
10^8 &\equiv_{9997} 3^2 \equiv_{9997} 9 \\
10^{16} &\equiv_{9997} 9^2 \equiv_{9997} 81 \\
10^{17} &\equiv_{9997} 10^{16} \cdot 10^1 \equiv_{9997} 81 \cdot 10 \equiv_{9997} 810
\end{aligned}$$

EX: diff. arrangements of 12 letters DISTRIBUTION s.t. T in beginning/end, 3 III's never next to each other

$10!/3!$ of remaining letters (2 T's beginning/end) and 8! contain III → $\boxed{\frac{10!}{3!} - 8!}$

EX: DISTRIBUTION w/ 7 consonants alphabetical not necessarily consecutive $\binom{12}{7}$

choose 7 of 12 spots for consonants & fill remaining 5 slots w/ 5 vowels, $\frac{5!}{3!}$ b/c I's are same → $\boxed{\binom{12}{7}\frac{5!}{3!}}$

EX: DISTRIBUTION where I's always have @ least 2 chars b/t them?

map first 2 I's to 3 letters: I-- I-- ------ total = 8 "slots"

choose $\binom{8}{3}$ where I's are seperated by @ least 2 x's

fill remaining 9 slots (omitting I's) with remaining letters: $\frac{9!}{2!}$ ← T's dupe

$\boxed{\binom{8}{3}\frac{9!}{2!}}$

DAYS 17-24 + previous
PSETS 9-10
CATTU

PROBABILITY:
$\dfrac{\#\text{successful outcomes}}{\#\text{ total outcomes}}$

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

MULTINOMIAL COEFF:
bookeeper: $\frac{10!}{5!\,2!\,3!} = \binom{10}{5,2,3}$

UNION: if disjoint: $|A \cup B| = |A| + |B|$
if not disjoint: $|A \cup B| = |A| + |B| - |A \cap B|$
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

INCLUSION / EXCLUSION:
$\bigcup_{i=1}^{n} A_i = \sum_{i=1}^{n} |A_i| - \sum_{1\le i<j\le n} |A_i \cap A_j| + \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| + \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|$

COMBINATORIAL PROOFS:
$2^n = \sum_{k=0}^{n} \binom{n}{k}$
$\sum_{r=0}^{k} \binom{n}{r}\binom{n}{k-r} = \binom{2n}{k}$
pascal's id: $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
$\sum_{j=k}^{n} \binom{j}{k} = \binom{n+1}{k+1} = \sum_{t=k+1}^{n+1} \binom{t-1}{k}$

HARMONIC #S:
$H_n = \sum_{k=1}^{n} \frac{1}{k} \sim \ln n$

MONOTONICITY:
event $A \subseteq B$,
$Pr[A] \le Pr[B]$
"adding possibilities can't make event less likely"

PIGEON-HOLE PRINCIPLE: if $|A| > k \cdot |B|$ & if $A \to B$ is total, then f is not injective. @ least $k+1$ inputs in A map to some output in B.
(pigeons A, holes B; $\exists a_1 \ne a_2$ s.t. $f(a_1) = f(a_2)$)

TREE:
0: assumptions
PROB SPACE: $\{R, B\} \times \{1,2,3\} \times \{1,2\}$ → for each layer of tree
$Pr[w] = 1/12$ for every $w \in S$

COMPLEMENT: $1 - Pr[B] = Pr[\bar{B}]$
$Pr[A|B] + Pr[\bar{A}|B] = 1$

1: SAMPLE SPACE
S: non-empty finite set called Sample Space → list possible outcomes $\{1, 2, H, T, \dots\}$
Pr: total func. from $S \to [0,1]$ representing prob. that each outcome occurs (should add to 1)
$\sum_{w \in S} Pr(w) = 1$ · uniform if all outcomes equally likely
2: probability func. (assign each edge a Pr)
3: events subset $A \subseteq S$

outcomes: pairs H, C where H = ..., C = ... in ... (can also list all)
$G_2 = \{GGE, \dots\}$ etc.
probs: put by tree, or "each outcome has prob. ___"

DISJOINT: events that cannot happen together (mut. ex.) $Pr[A \cap B] = 0$
DIFFERENCE RULE: $Pr[A \cap \bar{B}] = Pr[A \setminus B] = Pr[A] - Pr[A \cap B]$
SUM RULE: $Pr[A_1 \cup \dots \cup A_n] = Pr[A_1] + \dots + Pr[A_n]$ ← for mut. ex.

CONDITIONAL PROB: $Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]}$ if $Pr[B] \ne 0$

BAYES RULE: $Pr[A|B] \cdot Pr[B] = Pr[B|A] \cdot Pr[A]$

LAW OF TOTAL PROB: $Pr(A) = \underbrace{Pr(A|B) \cdot Pr(B)}_{Pr(A \cap B)} + \underbrace{Pr(A|\bar{B}) \cdot Pr(\bar{B})}_{Pr(A \cap \bar{B})}$ ← for disjoint (can have more events - sum all)

PRODUCT RULE: $Pr(A \cap B) = Pr(A|B) \cdot Pr(B)$
GENERALIZED: $Pr(A_1 \cap A_2 \cap \dots \cap A_n) = Pr(A_1) \cdot Pr(A_1 | A_2) \cdot Pr(A_3 | A_1, A_2) \cdot \dots \cdot Pr(A_n | A_1, A_2 \dots A_{n-1})$

(knowing B doesn't impact Pr[A]) → **INDEPENDENCE:** event A ind. event B if $Pr[A|B] = Pr[A]$ or $Pr[B] = 0$
(occurence of one does not affect the other
1) $Pr[B] = 0$: $A \cap B \subseteq$
$Pr[A \cap B] \le Pr[B]$, $Pr[A \cap B] = 0$ (monotonicity)
$Pr[A] \cdot Pr[B] = 0$ (Pr can't be neg.)
2) $Pr[B] \ne 0$:
$Pr[A \cap B] = Pr[A] \cdot Pr[B]$ (general prod. rule) if A ind. B

MUTUAL INDEPENDENCE:
$Pr[H_2 | H_1] = Pr[H_2]$

PAIRWISE IND: collection of events $A_1, A_2, \dots, A_n$ where every pair $Pr[A_i \cap A_j] = Pr[A_i] \cdot Pr[A_j]$ for all $i \ne j$
TOTAL MUTUAL IND: every subset is ind (check pairs, triples, etc.) → implies pairwise, but not vice versa

RANDOM VAR: total function whose domain is sample space
INDEPENDENT: rvs X & Y, $P[X=x \cap Y=y] = P[X=x] \cdot P[Y=y]$
MUTUALLY IND: every subset ind. (all combos)

common rvs:
INDICATOR RV: value 1 with prob. p, 0 with 1-p
UNIFORM: takes on each val $\{1, \dots, n\}$ with $\frac{1}{n}$

INDICATORS: given event i, $I_A :=$ RV defined by $I_i(w) = \begin{cases} 1 & \text{if } i = A \\ 0 & \text{if } i \notin A \end{cases}$

Pr @ a point: $PMF_R(x) = Pr(R = x)$ → property: $PMF_R(k) = CDF_R(k) - CDF_R(k-1)$
Pr of all vals up to pt: $CDF_R(x) = Pr(R \le x)$

X EVENTS: $Ex[X] = Pr[I_1] + Pr[I_2] + \dots + Pr[I_n]$
for $X = I_1 + \dots + I_n$ = # events that occur

BINOMIAL DIST: PMF: $Pr[X=k] = \binom{n}{k} p^k (1-p)^{n-k}$
(n # items/coins, k successes, p = prob. correct)
CDF: $Pr[X \le k] = \sum_{j=0}^{k} \binom{n}{j} p^j (1-p)^{n-j}$
· fixed # trials
· each trial ind.
· 2 outcomes
· Pr[success] stays same b/t trials
(same for geometric distribution)

X = # successes in n ind. trials, each with success prob. p (sum of indicators)
$Ex[X] = n \cdot p$ (what to expect on avg, NOT a specific outcome)
$var[X] = np(1-p)$ n = # trials, p = success rate

"weighted avg" **EXPECTATION:** $Ex[R] = \sum_{x \in range(R)} x \cdot Pr[R = x]$ (rv, events, val, prob.)
if independent: $E[X \cap Y] = E[X]E[Y]$
$E[aX + b] = aE[X] + b$ ← linearity

CONDITIONAL EXP: $Ex[X | Y = y] = \sum_{x \in range(X)} x \cdot P[X = x | Y = y]$ (rv, event)

TOTAL EXPECTATION: $Ex[R] = Ex[R|E_1] \cdot Pr[E_1] + Ex[R|E_2] \cdot Pr[E_2] \dots$
$Ex[D_1 + D_2] = Ex[D_1 + D_2 | E] \cdot Pr[E] + Ex[D_1 + D_2 | \bar{E}] \cdot Pr[\bar{E}]$

MEAN t to FAIL:
$P[fail] = \frac{1}{p}$ p = failing
$E[\#\text{iterations}] = 1/1p = p$ (includes failure)
· independent trials
· each trial: fixed success prob. p
· how many trials until 1st success? p-1

VARIANCE of rv R: $var(R) = Ex[[R - Ex(R)]^2] = Ex[R^2] - Ex^2[R]$
$var(ax + b) = a^2 var(x)$ (as found in rec.)

STD. DEV: $\sigma(R) = \sqrt{var(R)}$ if rvs pairwise independent: $var(R_1 + R_2) = var(R_1) + var(R_2)$

GEOM. DIST: $Pr[c = i] = (1-p)^{i-1} p$ → fails i-1 times until ith success → "keep flipping until get H"
$E[X] = \frac{1}{p}$ exp. tries until 1st suc. p = prob. correct

Pr any event happens, loose but simple → **UNION BOUND:** events E: $Pr[E_1 \cup \dots \cup E_n] \le Pr[E_1] + \dots + Pr[E_n]$

known Ex of rv ≥ 0 → **MARKOVS:** if R is non-neg. rv, then
$\forall x > 0$, $Pr[R \ge x] \le \frac{Ex[R]}{x}$
$x = c \cdot E[R]$
$Pr[R \ge c \cdot E[R]] \le \frac{1}{c}$ (neater)

CHEBYSHEV: $\forall x > 0$ & any rv R, $Pr(|R - Ex(R)| \ge x) \le \frac{var(R)}{x^2} = \left(\frac{\sigma(R)}{x}\right)^2$
($Pr[X \ge \#]$ → shift)
known Ex & var of rv, bound how far from mean
$x = c \cdot \sigma(R)$
$Pr[|R - Ex(R)| \ge c \cdot \sigma(R)] \le \frac{1}{c^2}$

CHERNOFF: $R_1, \dots, R_n$ = mutually ind. rvs s.t. $0 \le R_j \le 1$
let $R = R_1 + R_2 + \dots + R_n$
for any $c > 1$, $Pr(R \ge c \cdot Ex(R)) \le e^{-(c \ln c - c + 1)Ex[X]}$ ← good for summing independent indicator vars

rv-NOT indicator:
$Ex[M^2] = \sum_{k=1}^{N} Pr[M=k] \cdot k^2$
* basically multiply each prob by x^2 instead of x & add!
$1 \cdot \frac{7}{16} + 2 \cdot \frac{5}{16} + 3 \cdot \frac{3}{16} + 4 \cdot \frac{1}{16}$
becomes
$1^2 \cdot \frac{7}{16} + 2^2 \cdot \frac{5}{16} + 3^2 \cdot \frac{3}{16} + 4^2 \cdot \frac{1}{16}$

MURPHYS LAW: $Pr[E_1 \cup \dots \cup E_n] \ge 1 - e^{-Ex[X]}$
for events $E_1 \to E_n$ & X events occur

EX: var - R_i = indicator vars - ind
$var(R) = Ex[R^2] - Ex^2[R]$
$R^2 = \left(\sum_{i=1}^{N} R_i^2\right) + \left(\sum_{1 \le i < j \le N} 2 \cdot R_i \cdot R_j\right)$
$Ex[R^2] = Ex\left[\sum_{i=1}^{N} R_i^2 + 2\sum_{i \ne j} R_i R_j\right]$
$Ex[R_i^2] = Ex[R_i]$ b/c R_i = ind. var.
$= \sum_{i=1}^{N} Ex[R_i]^2 + 2\sum_{i \ne j} Ex[R_i R_j]$
pairwise ind: $E[I_i I_j] = E[I_i]E[I_j]$
$= E[I_i]^2$ for all $i \ne j$
$= N\,Ex[R] + N(N-1)(E[R])^2$
$= N\,Ex[R] + (NE[R])^2 - N(E[R])^2$
$var[R] = Ex[R^2] - Ex[R]^2 = N\,Ex[R] + (NE[R])^2 - N(E[R])^2 - (N \cdot Ex[I]^2)$
$= N \cdot Ex[I_i](1 - Ex[I_i])$

$\binom{N}{2} = \frac{N(N-1)}{2}$
$\sum_{1 \le i < j \le N} E[I_i I_j] = \binom{N}{2} \cdot E[I_i]^2$

EX: indicators & expectation:
For each ___ S_i, indicator rv $I_i = 1$ if ..., $I_i = 0$ otherwise, i ranges from — to —. we can express rv $Y = \sum_{i=1}^{\_} I_i$. For all i, we have $Ex[I_i] = Pr[I_i = 1] =$ ___. by linearity of expectation, $Ex\left[\sum_{i=1}^{\_} I_i\right] = \sum Ex[I_i] = \dots = \#$.

EX: markov & shift
Average body temperature in the herd is 85 degrees. Cow will die if its temperature below 90 degrees F, and temperatures low as 70 degrees, but no lower, were actually found in the herd.
(a) Use Markov's Bound to prove that at most 3/4 of the cows could survive
apply to T-70
$Pr[T - 70 \ge 20] \le \frac{Ex[T-70]}{x} \to \frac{Ex[T] - 70}{20}$
original: $T \ge 90$
$\le \frac{85 - 70}{20} \le \frac{3}{4}$

COROLLARY / THMS:

- $Pr[A \cap B] = Pr[B \cap A]$
- A, B ind. iff A, $\bar{B}$ ind.
- if $R: S \to \{0,1\}$, $Ex[R] = 0 \cdot Pr[R=0] + 1 \cdot Pr[R=1] = Pr[R=1]$
- if $R: S \to \mathbb{N}$, $Ex[R] = \sum_{i=1}^{\infty} i \cdot Pr[R > i] = Ex[R]$
- $Ex(T) = \sum_{i=1}^{n} Pr(A_i)$
- $Pr[T>0] \leq Ex(T)$
- $Pr(T>0) \leq \sum Pr(A_i)$
- $Pr(T>0) \geq 1 - e^{-Ex(T)}$ for n mut. ind. events (Murphys)
- $Ex(R_1, R_2) = Ex(R_1) \cdot Ex(R_2)$ if R_1, R_2 ind.
- C ind of A, C ind. B, C ind $A \cap B$. $\to$ C ind $A \cup B$

- $var[R] = Ex[R^2] - Ex^2[R]$
- $var[aR+b] = a^2 \, var[R]$
- $var[R_1 + R_2] = var[R_1] + var[R_2]$ IF INDEPENDENT RVS!