SP'24 CS70

TEACHING NOTES

DISCUSSION 0A

01/16/24

welcome!

- We will start Berkeley Time ☺
- Grab a worksheet from the front desk.

About Me

- 2nd-year, studying CS + physics.
- Robotics + reinforcement learning research!
- Email me: jennifer-zhao@berkeley.edu

↳ about CS70 or otherwise! I'll do my best to help.

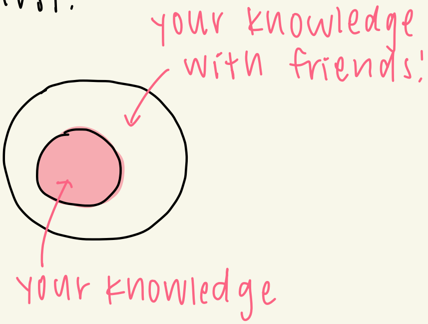
Discussion 0A Notes

- Read the course site: eecs70.org
- course email: sp24@eecs70.org
- HW0 is due: 1/20, saturday

- My notes & much more are on Ed.

CS 70 Advice

- keep up with pace of class.
- conceptual understanding first.
- study with others:
  - ↳ office Hours
  - ↳ Discussion section!



- Review regularly.

Discussion logistics

- Review + exam problems (BerkeleyTime).
- Mini-lecture.
- worksheet + group-work.

sets

not always

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

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

rational numbers $\mathbb{Q} = \{ a/b \mid a, b \in \mathbb{Z},\ b \neq 0 \}$

all real numbers $\mathbb{R}$

set builder notation, refers to property ("such that")

set notations & operations

$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

proper subset

cartesian product: $A \times B = \{(a, b) \mid a \in A,\ b \in B\}$

ex: $\mathbb{N} \times \mathbb{N} = \{(0,0), (1,0), (0,1), (1,1) \ldots\}$

power set: $\mathcal{P}(S) = \{\text{all subsets of } S\}$

ex: $S = \{1, 2\}$, $\mathcal{P}(S) = \{\{\}, \{1\}, \{2\}, \{1,2\}\}$

$|S| = 2$ $\quad |\mathcal{P}(S)| = 4$

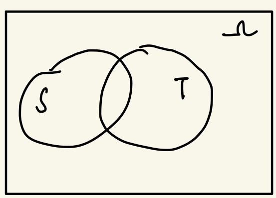
cardinality of power set

$|S| = k \Rightarrow |\mathcal{P}(S)| = 2^k$

is cardinality always finite? $|\mathbb{Q}| = \infty$. What about $|\mathbb{R}|$? Also ∞...

Notation examples

$2 \mid 4 \rightarrow$ two divides four



$S \cup T$

$S \cap T$

quantifiers

$(\forall x \in \mathbb{Z}) \quad (\exists y \in \mathbb{Z})(y > x)$

$(\forall x \in \mathbb{Z})$: for all integers x

$(\exists y \in \mathbb{Z})$: there exists an integer y

nested quantifiers

it can be helpful to think of nested quantifiers as nested for loops.

ex: $\forall x \forall y \; P(x, y) \longrightarrow$

```
for all x:
    for all y:
        P(x,y) == True
```

$\equiv$ used for logical equivalence

swapping quantifiers

$\forall x \forall y \; P(x,y) \equiv \forall y \forall x \; P(x,y)$

$\exists x \exists y \; P(x,y) \equiv \exists y \exists x \; P(x,y)$

$\forall x \exists y \; P(x,y) \not\equiv \exists y \forall x \; P(x,y)$

problem-solving approach: translate logical statement to words

And, or, Not

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	$\neg P$
T	F
F	T

implication

$p \Rightarrow q \equiv$ if p, then q

ex: it rained $\Rightarrow$ sidewalk is wet

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

if p is not satisfied, value of q is irrelevant (vacuously true)

converse: $\boxed{q \Rightarrow p} \rightarrow \not\equiv (p \Rightarrow q)$ unless $(p \Leftrightarrow q)$

contrapositive: $\boxed{\neg q \Rightarrow \neg p} \rightarrow \equiv (p \Rightarrow q)$

ex: sidewalk wet $\Rightarrow$ it rained ✗

ex: sidewalk not wet $\Rightarrow$ did not rain ✓

same truth table

logical equivalence of $\Rightarrow$

$(p \Rightarrow q) \equiv (\neg p \vee q)$

rewriting implication as disjunction can allow us to apply De Morgan's!

De Morgan's laws

$\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$

$\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$

$\downarrow$

$\neg(\forall x P(x)) \equiv \exists x(\neg P(x))$

$\neg(\exists x P(x)) \equiv \forall x(\neg P(x))$

$\longrightarrow$ questions?

DISC. 0B

(θ) 01/18/24

Implication as Disjuction

$\boxed{P \Rightarrow q \equiv (\neg P \vee q)}$

they have the same truth table

Propositional Logic Review

$$(\neg P \vee (P \implies Q)) \equiv (P \implies Q)$$

← prove statement.

$\neg P \vee (\neg P \vee Q) \equiv \neg P \vee Q \equiv P \Rightarrow Q$ □

Quantifiers Review

$$(\forall y \in S)(\exists x \in S)(Q(x) \wedge P(y)) \implies (\exists x \in S)(\forall y \in S)(Q(x) \wedge P(y))$$

← prove statement.

$(\forall y \in S) P(y) \wedge (\exists x \in S) Q(x)$

$(\forall y \in S) P(y) \wedge (\exists x \in S) Q(x)$

these two statements are equivalent □

Disc. 0B Notes

- Read: note 0, 1, 2
- OH starts next week! :)
- Mini-vitamins 0A & 0B are due: $\boxed{\text{Tomorrow, 11:59}}$
- HW 0 is due: $\boxed{\text{Saturday, 4:00PM}}$

how do we prove something?

1. direct proof
2. proof by contraposition
3. proof by contradiction

possibly used with proof by cases

direct proof

assume P

$\downarrow$

logical steps

$\downarrow$

therefore Q

proof by contraposition

recall: $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$ → proving the contrapositive = proving the original implication

set of positive integers

ex: if $n = ab$, $a, b \in \mathbb{Z}_{++}$, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

pf: suppose $a > \sqrt{n}$ and $b > \sqrt{n}$] assume $\neg Q$

$ab > \sqrt{n} \cdot \sqrt{n} = n$

$ab > n$

$ab \neq n$] therefore, $\neg P$

□

proof by contradiction

ex: at least 4 of any 22 days must fall on same day of the week.

pf: suppose < 4 of 22 days falls on same day of the week.] assume $\neg P$

① at most 3 of the same day of the week

② 7 days of the week

③ at most $3 \times 7 = 21$ days of week

→← contradicts premise!] $R \wedge \neg R$, therefore P

□

pigeonhole principle

if $n > k \Rightarrow$ for n objects placed into k boxes, at least 1 box has > 1 objects

proof by cases

ex: $n \in \mathbb{Z} \Rightarrow n^2 \geq n$

PF: case $(n = 0)$:

$0 = 0$ ✓

case $(n \geq 1)$:

$n \cdot n \geq n \cdot 1$

$n^2 \geq n$

case $(n \leq -1)$:

$n^2 \geq 0 \geq -1 \geq n$

$\square$

WLOG

"without loss of Generality":

1. prove case 1.
2. assume same argument applies to other cases.
3. done.

proving uniqueness

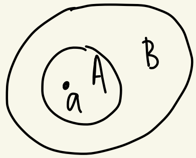
1. Assume $\exists x$ s.t. $P(x)$
2. Assume another solution, x'
3. show $x = x'$, which is a contradiction

Proofs with sets

prove $A \subseteq B$:

1. take $a \in A$
2. show $a \in B$

formal definition of subset



prove $A = B$:

1. prove $A \subseteq B$
2. prove $A \supseteq B$

Images & pre-images

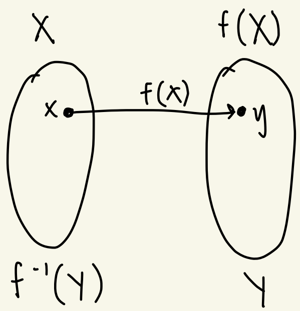


image of X

$f(X) = \{ y \mid y = f(x) \text{ s.t. } x \in X \}$

preimage of Y

$f^{-1}(Y) = \{ x \mid f(x) \in Y \}$

review: proving logical equivalence

showing $p \equiv q$ is showing $p \Leftrightarrow q$ is true

1. prove $p \Rightarrow q$ $(\Rightarrow)$
2. prove $q \Rightarrow p$ $(\Leftarrow)$

DISC. 1A

(T) 1/23/24

contrapositive review

$$\boxed{p \Rightarrow q \equiv \neg q \Rightarrow \neg p}$$

① identify p & q

② swap & negate both, remember to use De Morgan's!

ex: $\neg(a \leq b \text{ and } c \geq d)$

$\neg(a \leq b)$ or $\neg(c \geq d)$ ← distribute neg. & flip and → or

$a > b$ or $c < d$

contraposition review

prove: If 4 $\nmid a^3$ then 2 $\nmid a$. (By $a \nmid b$, we mean a does not divide b.)

pf: ① suppose $2 \mid a$

② a^3 contains $2 \cdot 2 \cdot 2$ in its prime factorization

③ a^3 contains 4 in its factorization

④ $4 \mid a^3$

$\therefore$ $4 \nmid a^3 \Rightarrow 2 \nmid a$. □

Discussion 1A Notes

- HW 1 Due: $\boxed{\text{saturday, 1/27, 4:00 PM}}$
- Read: Notes 3 & 4
- Office hours have begun
- No more TA notes, Attendance taken!

proof by induction

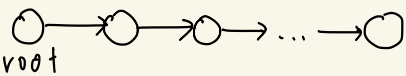
base case not necessarily 0, but usually "smallest" case

proof structure for $P(n)$

1. base case: prove $P(0)$
2. IH: assume $P(k)$ is true
3. IS: show $P(k) \Rightarrow P(k+1)$ is true

→ works for proofs over discrete cases

ex: prove that every node of a linked list can be accessed:



pf: BC: can access root. $\boxed{P(0)}$

IH: assume kth node can be accessed. $\boxed{P(k)}$

IS: from kth node, (k+1)th node can be accessed from the next pointer.

$\boxed{P(k) \Rightarrow P(k+1)}$

□

inductive hypothesis!

≈

recursive leap of faith

→ in both cases, assume $P(k)$ is true.

strong induction

might need multiple base cases

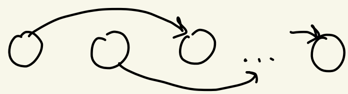
proof structure

① BC: prove $P(0)$, etc.

② IH: assume $P(0) \wedge P(1) \wedge \ldots \wedge P(k)$

③ IS: show $IH \Rightarrow P(k+1)$ is true

<u>ex:</u> consider a linked list with pointers to <u>next_next node</u>:



prove: every node can be accessed.

<u>pf:</u> BC: can access <u>root</u> & <u>1st</u>. $\boxed{P(0) \wedge P(1)}$

IH: assume 0th, 1st, ..., kth nodes can <u>all</u> be accessed.

$\boxed{P(0) \wedge P(1) \wedge \ldots \wedge P(k)}$

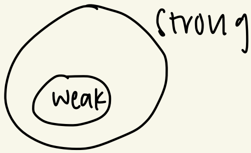
IS: <u>(k+1)th node</u> can be accessed from <u>(k-1)th</u>.

$(k-1) \leq k$, so IH holds. $\boxed{IH \Rightarrow P(k+1)}$

$\square$

$\boxed{\text{weak induction fails because } P(k) \not\Rightarrow P(k+1)!}$

strong vs. weak induction?



weak induction is a special case of strong induction
↓
when in doubt, strong induction.

axiom of weak induction

$P(0) \wedge \forall k[P(k) \Rightarrow P(k+1)] \Rightarrow \forall n P(n)$

algebraic example

ex: prove $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \quad \forall n \in \mathbb{N}$

pf: BC: $n=1 \rightarrow 1^2 = 1 = \frac{(1)(1+1)(2+1)}{6} = \frac{(2)(3)}{6} = 1$ ✓

IH: assume $\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}$ for some $k \in \mathbb{N}$

IS: $\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2$

$= \frac{1}{6}\left(k(k+1)(2k+1) + 6(k+1)^2\right) = \frac{1}{6}(k+1)[k(2k+1) + 6(k+1)]$

$= \frac{1}{6}(k+1)(2k^2+7k+6) = \frac{1}{6}(k+1)[2(k+1)+1](k+1+1)$ ✓ □

Example from Notes

<u>ex:</u> every $n \in \mathbb{N}$ where $n > 1$ can be written as product of 1 or more primes.

<u>pf:</u> BC: $n = 2$ ✓   IH: assume $2 \leq n \leq k$, $P(n)$

IS: can $n = k+1$ be written as product of primes?

<u>case 1:</u>

$k+1$ is prime ✓

<u>case 2:</u> $k+1$ is not prime $\rightarrow k+1 = xy$

$x \leq k$, $y \leq k \Longrightarrow xy$ is a product of primes ✓

example: recursive definition of a^n

```
f(a, n):
    if n=0:
        return 1
    else:
        return a·f(a, n-1)
```

→ prove correctness using <u>induction</u>

$\boxed{\text{recursive leap of faith}}$

<u>pf:</u> BC: $n = 0 \rightarrow f(a,0) = 1 = a^0$ ✓

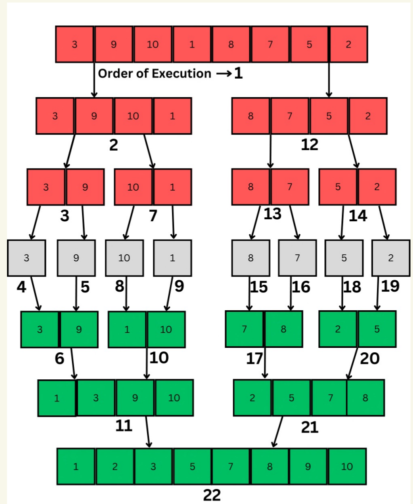
IH: assume $f(a,k)$ is correct $\rightarrow f(a,k) = a^k$

IS: $f(a,k+1) = a \cdot f(a,k) = a \cdot a^k = a^{k+1}$ ✓

$\square$

Example: Mergesort

```
mergesort(L):
    if len(L) ≤ 1:
        return L
    else:
        m = ⌊len(L)/2⌋
        L1 = mergesort(L[:m])
        L2 = mergesort(L[m+1:])
        return merge(L1, L2)
```



pf. of correctness:

BC: $len(L) = 1 \rightarrow mergesort(L) = L =$ sorted list ✓

IH: $len(L) = 0, 1, \dots, k \rightarrow$ assume $mergesort(L) =$ sorted list

IS: $len(L) = k+1 \rightarrow mergesort(L) =$

$merge(\, mergesort(L[:m]),\; mergesort(L[m+1:])\,)$

list of len. $= \left\lfloor \frac{k+1}{2} \right\rfloor \le k+1$
✓ by IH

list of len. $= \left\lceil \frac{k+1}{2} \right\rceil \le k+1$
✓ by IH

$merge(L_1, L_2)$ contains elements of L_1 & L_2 in sorted order

↳ $mergesort(L)$ for $len(L) = k+1$ is in sorted order. □

DISC. 1B

(θ) 1/25/24

strong induction review

① base case ($n=0$)

② IH ($n=0,1,2,\ldots,k$)

③ IS ($n=k+1$)

proof by induction review

4. Fibonacci

Recall the Fibonacci numbers are defined by $F_0 = 0, F_1 = 1, F_i = F_{i-1} + F_{i-2}$ for all $i \geq 2$.

Show that for all integers $n \geq 1$, $\sum_{i=1}^{n} F_i = F_{n+2} - 1$.

BC ($n=1$): $F_1 = F_3 - 1 = 2 - 1 = 1$ ✓

IH ($n=k$): assume $\sum_{i=1}^{k} F_i = F_{k+2} - 1$

IS ($n=k+1$): $\sum_{i=1}^{k+1} F_i = F_{k+1} + \sum_{i=1}^{k} F_i$

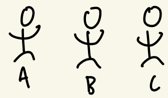
$= F_{k+1} + F_{k+2} - 1 = F_{(k+1)+2} - 1$ ✓

Discussion 1B Notes

- Homework 1: Due this Saturday
- Read: Notes 3 & 4
- No TA notes
- would still recommend reading disc. solutions

Stable Matching Premise

n jobs: 1 2 3

n candidates: 

→ optimal way to pair everyone up?

Propose-Reject Algorithm

loop:

1. all J propose to most preferred c that hasn't yet rejected them
2. each c rejects all but most preferred J
3. if each c is matched w/ a J:
   break

1 Stable Matching

Consider the set of jobs $J = \{1, 2, 3\}$ and the set of candidates $C = \{A, B, C\}$ with the following preferences.

Jobs	Candidates
1	A > B > C
2	B > A > C
3	A > B > C

Candidates	Jobs
A	2 > 1 > 3
B	1 > 3 > 2
C	1 > 2 > 3

Run the traditional propose-and-reject algorithm on this example. How many days does it take and what is the resulting pairing? (Show your work.)

	Day 1	Day 2	Day 3	Day 4	Day 5
A	1 3	1	1 2	2	2
B	2	2 3	3	3 1	1
C					3

resulting pairing: {(A, 2), (B, 1), (C, 3)}

terminates in $\boxed{\text{5 days}}$

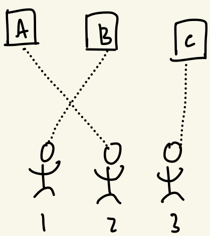
Stable Matching

- algorithm always halts

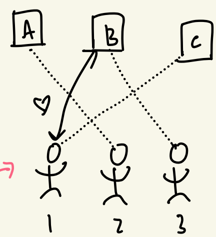
$\boxed{\text{for } n \text{ elements, maximum of } n^2 \text{ days}}$

↳ hasn't halted? At least 1 J was rejected.
  n^2 possible rejections.

- matching, S, is stable if <u>no rogue couples</u>



stable!



B: 1 > 3

1: B > C

unstable!

↓

$\boxed{\text{(B,1) is a rogue couple}}$

B prefers 1 over 3, and 1 prefers B over C

Jobs	Candidates
1	A > B > C
2	B > A > C
3	A > B > C

Candidates	Jobs
A	2 > 1 > 3
B	1 > 3 > 2
C	1 > 2 > 3

rogue couple = J & C <u>prefer each other</u> over their <u>actual partner</u>

improvement lemma

on each day, C's offer either stays same or gets better.

→ candidate's offers improve

	Day 1	Day 2	Day 3	Day 4	Day 5
A	1 3	1	1 2	2	2
B	2	2 3	3	3 1	1
C					3

algorithm ends when you meet in middle :)

→ job's options get worse

Jobs	Candidates
1	A > B > C
2	B > A > C
3	A > B > C

Candidates	Jobs
A	2 > 1 > 3
B	1 > 3 > 2
C	1 > 2 > 3

stable matching proofs

- induction on # of days → what holds on day k+1?
- proof by contradiction → does ¬P violate stability, halting, improvement lemma?

- direct → consider (J, C), (J', C'), etc.

Optimality

- could be more than 1 matching that is stable.

↳ ex: what if candidates proposed instead? or different algorithm?

job optimal / candidate pessimal } job proposes

job gets best candidate it can hope to get in a stable matching.

job pessimal / candidate optimal } candidate proposes

candidate gets best job it can hope to get in a stable matching.

proof Example

thm: when jobs propose $\rightarrow$ job optimal matching

pf: suppose ~~not~~ job optimal $\Big] \boxed{\neg P}$

$\Downarrow$

matching S:

$J \not\rightarrow C^*$

$J^* \leftrightarrow C^*$

C'

matching T:

$J \leftrightarrow C^*$

$J^* \leftrightarrow C'$

day k: C^* rejects J ~~for~~ J^* $\Rightarrow$ $\boxed{\begin{array}{l} C^* : J^* > J \\ J^* : C^* > C' \end{array}}$

$J \leftrightarrow C^*$

$J^* \leftrightarrow C'$

$J^* \leftrightarrow C^*$ ♡

implies (J^*, C^*) is rogue in T

$\Rightarrow$ unstable $\Rightarrow$ contradiction. $\rightarrow\leftarrow$ A

DISC. 2A

jobs propose = job-optimal / candidate pessimal

job paired with most preferred candidate of all possible stable matchings.

Stable Matching Review

If a candidate is paired with the kth job on its preference list in a stable matching, this candidate must not be first in the preference list for at least ___ jobs.

$C: \underbrace{J_1 > J_2 > \dots > J_{k-1}} > \underline{J_k} > \dots J_n$

if any of these preferred C most, (J_i, C) would be rogue pair. → $\boxed{k-1}$

If a candidate rejects a job in the job propose and reject algorithm, there is *no* stable pairing where that candidate and job are paired.

→ T/F?

pf: suppose in S: (J, C') because C rejects J

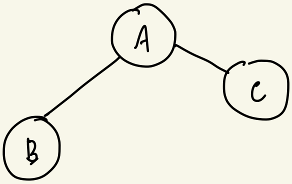
in S': (J, C)

1. J: $C > C'$ because it proposed to C first
2. C more optimal than C'
3. S is supposed to be job-optimal →← □ $\boxed{\text{True}}$

Discussion 2A Notes

- Questions from lecture?
- Read: Note 5
- HW2 released!
- some OH will be online

Graph Terminology



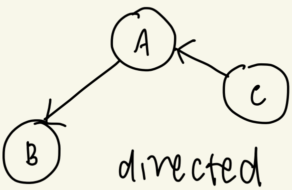
$G = \{V, E\}$

vertex set: $\{A, B, C\}$

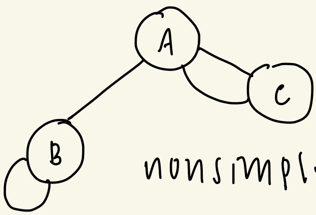
edge set: $\{(A,B), (A,C)\}$

$\boxed{E \subseteq V \times V}$

<u>simple</u>, <u>undirected</u> graph



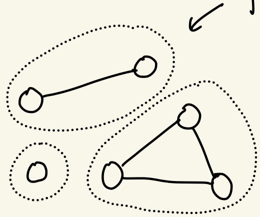
directed



nonsimple

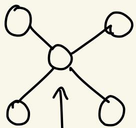
connectivity

connected = $\exists$ path b/t any two vertices



graph with <u>three</u> connected components

Degrees of Vertices



deg(V) = 4

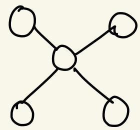
degree of vertex

edges incident to it

handshake lemma

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

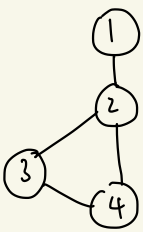
ex:



$1+1+4+1+1=8$

$|E|=4$

Graph Traversals



	repeats ok	no repeat vertex/edge
start ≠ end ok	walk	path
start = end	tour	cycle

except start/end

ex:

path {1, 2, 3}

tour {3, 2, 1, 2, 3}

cycle {3, 2, 4, 3}

Eulerian walk/Tour → every edge used exactly once!

tour exists for connected, even-degreed graph

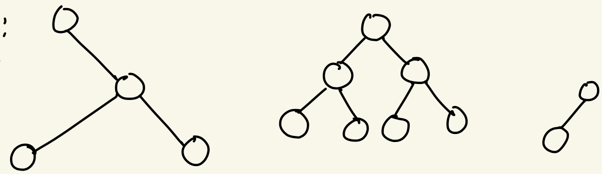
Hamiltonian walk/Tour → every vertex used exactly once!

trees

equivalent definitions of trees

1. connected & no cycles
2. connected & $|V| = |E| + 1$ — size of sets V & E
3. connected & removing any edge disconnects.
4. no cycles & adding an edge creates cycle.

ex:



leaf

node of degree 1

proofs by induction

- on # of vertices or # edges
- for IS, go from $\boxed{k+1 \to k \to k+1}$ — remove + add arbitrary vertex/edge

build-up error

incorrectly assuming n+1 graph must be built from n graph of same property.

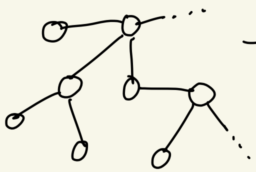
Induction Example

ex: tree w/ n vertices has $n-1$ edges

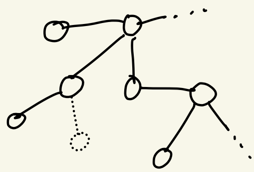
pf: BC: $n=1$ → O → has 0 edges ✓

IH: assume tree w/ k vertices has $k-1$ edges

IS: consider tree w/ $k+1$ vertices:



→ remove leaf



← tree w/ $n=k$, IH holds

↓

$\boxed{k-1 \text{ edges}}$

↓

to achieve $n=k+1$, must add $(k+1)$th vertex w/ 1 edge

← $\boxed{k \text{ edges}}$

∴ IS ✓ □

build-up error

do NOT go straight from $k \rightarrow k+1$!

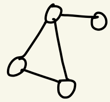
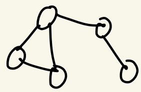
ex: if every vertex $\deg(v) \geq 1$, graph is connected.

pf: BC: $n=1$

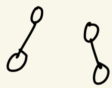
IH: $n=k$

IS:

! this proof is not correct

1. consider graph of k vertices →  → connected by IH
2. add $(k+1)$th vertex → 
3. connected?

↓

consider counter-example: 

what went wrong?

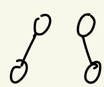
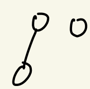
build-up error

incorrectly assuming n+1 graph must be built from n graph of same property.

↓

let's try again! this time, use $k+1 \rightarrow k \rightarrow k+1$.

pf: IS:

1. consider graph of $k+1$ vertizes: 
2. remove a vertex → graph of k vertizes: 

graph contains vertex with $\deg(v) = 0$!
IH can't apply, so proof can't work out.

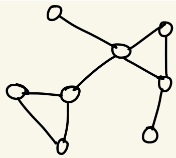
DISC. 2B

Connectivity & Trees Review

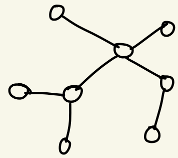
Consider a connected n-vertex graph G with exactly k cycles.

Remove $2k$ edges from G produces a graph with at least ______________ connected components.

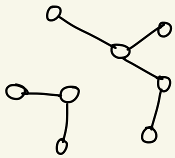
lower bound scenario:



1. remove k edges to eliminate the k cycles:



2. graph is connected & no cycles → tree!
3. remove 1 edge:



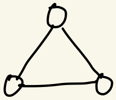
→ 2 components

4. remove k edges → $\boxed{k+1 \text{ components}}$

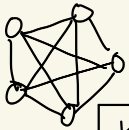
Discussion 2B Notes

- Reading: Note 5
- HW2 due this Saturday
- Graph coloring no longer in scope :(

Complete Graphs



$\boxed{K_3}$



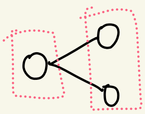
$\boxed{K_5}$

every vertex is connected to every other vertex.

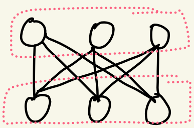
 # edges in complete graph

$$\frac{n(n-1)}{2}$$

Bipartite Graphs



$\boxed{K_{1,2}}$



$\boxed{K_{3,3}}$

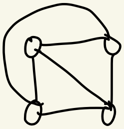
$V =$ union of $L \cup R$

no edges between vertices in L,

no edges between vertices in R.

$$\boxed{E \subseteq L \times R}$$

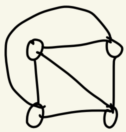
Planar Graphs



can be drawn without crossing edges.

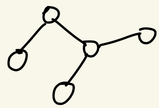
faces = subdivisions of the plane

ex:



4 faces

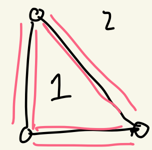
ex:



1 face

all trees are planar.

$$\sum_{i=1}^{f} s_i = 2e \quad \Big\} \text{ \# of sides} = 2 \times \text{ \# edges}$$



assume 3 sides per face

Euler's formula

planar & connected $\Rightarrow v + f = e + 2$

corollary

if planar $\Rightarrow e \leq 3v - 6$

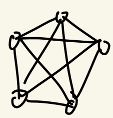
converse is not true!

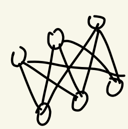
e.g. $K_{3,3}$ passes.

Non-Planar Graphs

Kuratowski's Thm.

contains $K_{3,3}$ or $K_5 \Longleftrightarrow$ non-planar

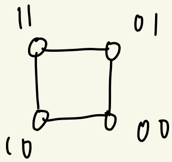




Hypercubes

ex: 1-dimension:

ex: 2-dimensions:

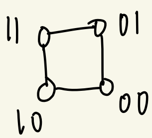


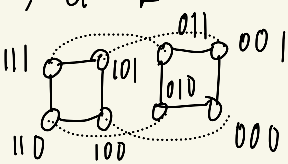
each vertex given by n-length bit-string.

edges between bit-strings that differ by 1-bit.

Induction on Hypercubes

dimension = k-1 → d = k





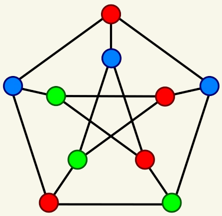
1. two copies of k-1 hypercubes
2. connect corres. vertizes.

n-dimension hypercube

$|V| = 2^n$, $|E| = n \cdot 2^{n-1}$

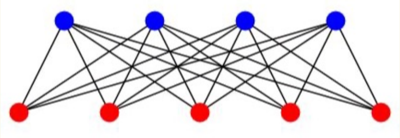
start with two, duplicate with each additional dimension

Graph coloring



premise: no two adjacent vertices can share a color.
↓
min. # of colors necessary?

ex: 2-colorable ⟺ bipartite.



4-color thm.

planar graph is 4-colorable.

DISC. 3A

Graphs in CS70 (Non-exhaustive)

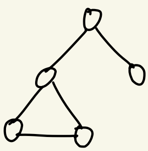
name	# vertices	# edges	# faces
complete	V	$\frac{V(V-1)}{2}$	not always planar
tree	V	$V-1$	1
planar	V	$e \leq 3V-6$	$e-V+2$
hypercube	2^d	$d2^{d-1}$	not always planar

Planar Graphs Review

T/F: For all $n \geq 3$, any connected graph with n vertices and n edges is planar.

$\boxed{\text{True.}}$ n vertices, $n-1$ edges $\rightarrow$ tree. so
n vertices, n edges $\rightarrow$ tree w/ one edge.

ex:



$\leftarrow$ planar. adding an edge creates cycle, but is not sufficient to create crossing.

Discussion 3A Notes

- coloring/duality not in scope, but bipartite graphs are.
- Read: Note 6 & 7.
- HW3 released.

working in mod space

ex: (mod 5) → allowed integer values : $\{0, 1, 2, 3, 4\}$

to represent #s ≥ 5, circle back around:

→ $5 \equiv 0 \pmod{5}$

→ $6 \equiv 1 \pmod{5}$

→ $7 \equiv 2 \pmod{5}$, etc.

modular congruence

$x \equiv r \pmod{m} \iff$

$x = km + r \iff$

$x \% m = r$

remainder

values in mod m

$\{0, 1, \ldots, m-1\}$

integers only.

ex: $17 \pmod{5} = ?$

$17 \% 5 = 2 \iff 17 = 3 \cdot 5 + 2 \iff \boxed{17 \equiv 2 \pmod{5}}$

↓

more generally: $17 \equiv 12 \equiv 7 \equiv 2 \equiv -3 \pmod{5}$

Operations in Mod Space

addition, multiplication, subtraction → <u>same as usual</u> :)

<u>ex:</u> $8 \times 17 \pmod 5 \equiv 136 \equiv 1 \pmod 5$

↳ $3 \times 2 \equiv 6 \equiv 1 \pmod 5$

(c) $3^{641} \equiv 3 \cdot (3)^{640} \equiv 3 \cdot (3^2)^{320} \equiv 3 \cdot (9)^{320}$

$\equiv 3 \cdot (-1)^{320} \equiv 3 \cdot 1 \equiv 3 \pmod{10} \rightarrow \boxed{3}$

modular exponentiation

- can mod <u>base</u>, but not <u>exponent</u>
- negative integers

division in mod space?

↳ unlike $+, -, \times$, division does <u>not</u> guarantee integer result.

<u>ex:</u>

how to represent $3/2 \pmod 5$ using $\{0, 1, 2, 3, 4\}$?

different approach: $\boxed{\text{division} \equiv \text{multiplying by inverse}}$

multiplicative inverse

$$x^{-1} \equiv a \pmod m \iff ax \equiv 1 \pmod m$$

just like how $2 \cdot \frac{1}{2} = 1$ in regular arith.

<u>ex:</u>

$3/2 \equiv 3 \cdot 2^{-1} \pmod 5$, where $\underline{2 \cdot 2^{-1} \equiv 1 \pmod 5}$.

$$2 \cdot 3 \equiv 6 \equiv 1 \pmod 5$$

$$\Downarrow$$

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

$$3 \cdot 2^{-1} \equiv 3 \cdot 3 \equiv 9 \equiv 4 \pmod 5$$

Exponentiation in Mod Space

reducing base during exponentiation

if $a \equiv b \pmod{m}$, $a^k \equiv b^k \pmod{m}$

→ can only reduce base, not power!

ex: $17^3 \pmod{5} \equiv 2^3 \equiv 8 \equiv \boxed{3 \pmod{5}}$

ex: $3^{10} \pmod{5}$

→ $3^2 \equiv 9 \equiv 4 \pmod{5}$

→ $(3^2)^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{5}$

→ $(3^4)^2 \equiv 1^2 \equiv 1 \pmod{5}$

$\boxed{\text{repeated squaring}}$

$3^{10} \equiv 3^8 \cdot 3^2 \equiv (3^4)^2 \cdot 3^2 \equiv 1 \cdot 4 \equiv \boxed{4 \pmod{5}}$

Greatest Common Denominator

$\gcd(x,y)$ = largest shared factor b/t x & y

ex: $\gcd(6,4) = \boxed{2}$ $\quad\quad$ $\gcd(7,4) = \boxed{1}$

$$\boxed{\gcd(x,y) = 1 \iff x \text{ \& } y \text{ are co-prime}}$$

ex: $\gcd(86, 24) = ?$

Euclid's Algorithm

replace (x,y) with $(y, x \pmod y)$ until = 0

$\gcd(24, 14)$

$= \gcd(14, 10)$

$= \gcd(10, 4)$

$= \gcd(4, 2)$

$= \gcd(2, 0) = \boxed{2}$

$24 \pmod{14} = 10$

because $\underbrace{14}_{m} \cdot \underbrace{1}_{k} + \underbrace{10}_{r} = 24$

strategy : convert to regular integer space.

$x \equiv r \pmod{m} \iff x = r + km, \quad k \in \mathbb{Z}$

Euclid's Algorithm

$\gcd(x, y) = \gcd(y, x \bmod y)$

DISC. 3B

Modular Arithmetic Review

- instead of division → we <u>multiply by inverse!</u>
- multiplicative inverse satisfies: $\boxed{ab \equiv 1 \pmod m}$

$$a^{-1} \equiv b \pmod m$$

- inverse of a exists when $\boxed{\gcd(a,m) = 1}$
- $a^{-1} \pmod m$ is <u>unique.</u>

gcd Review

True or False: If $\gcd(m,n) = d$, then $\frac{mn}{d} = 0 \pmod m$.

$d \mid n \Rightarrow n = kd \Rightarrow \frac{mn}{d} = \frac{mkd}{d} = mk \Rightarrow mk \pmod m = 0$

$\boxed{\text{True}}$

What is $a \times n(n^{-1} \pmod m) \pmod m$ if $gcd(n,m) = 1$?

$$\underbrace{n(n^{-1} \pmod m)}_{\equiv 1 \pmod m} \Rightarrow a \times 1 \equiv \boxed{a \pmod m}$$

Discussion 3B Notes

- Read: Notes 6 & 7
- HW3 due on Saturday

Review: Euclid's Algorithm

- use to find $\gcd(a, m)$

$$\boxed{\begin{array}{l} ① \ \gcd(a,m) \longrightarrow \gcd(m, a \pmod m) \\ ② \text{ repeat until 2nd term} = 0 \end{array}}$$

why do we want gcd?

- check if $a^{-1} \pmod m$ exists
  - ↳ i.e., is $\gcd(a, m) = 1$?

- find $a^{-1} \pmod m$
  - ↳ i.e. what is b s.t. $ab + mk = 1$?

finding a^{-1}

$$\boxed{\underbrace{ab}_{a^{-1}} + \underbrace{mk}_{\text{integer multiple of } m} = 1}$$

Extended Euclid's Algorithm

goal:
$\gcd(a, m) = ab + mk$

- recursive version
- iterative version

Extended Euclid's Recap

- recursive & iterative both give same result

- **iterative method:**

① $m = 1 \times m + 0 \times a$

$a = 0 \times m + 1 \times a$

② multiply 2nd row (LHS and RHS) by constant

③ subtract from 1st row:

$$
\begin{array}{rl}
m &= 1 \times m + 0 \times a \\
-\big[\, ca &= c(0 \times m) + c(1 \times a) \,\big] \\
\hline
m - ca &= 1 \times m + (-c) \times a
\end{array}
$$

$\vdots$

④ repeat with newest row until LHS $= 0$

Chinese Remainder Theorem

$x \equiv r_1 \pmod{m_1}$ ← where m_i are pairwise co-prime

$x \equiv r_2 \pmod{m_2}$ → **goal:** find x, a unique solution $\pmod{m_1 m_2 m_3}$

$x \equiv r_3 \pmod{m_3}$

CRT Intuition

suppose: $b_1 \equiv 1 \pmod 3$, $b_1 \equiv 0 \pmod 5$

$b_2 \equiv 0 \pmod 3$, $b_2 \equiv 1 \pmod 5$

if $y = r_1 b_1 + r_2 b_2$:

$y = r_1 b_1 + r_2 b_2 \pmod 5$

$y = r_2 \pmod 5$

$y = r_1 b_1 + r_2 b_2 \pmod 3$

$y = r_1 \pmod 3$

CRT recap

① goal: find x s.t.
$$x \equiv r_1 \pmod{m_1}$$
$$x \equiv r_2 \pmod{m_2}$$
$$x \equiv r_3 \pmod{m_3}$$

② find a_1, a_2, a_3 s.t:

	mod m_1	mod m_2	mod m_3
a_1	1	0	0
a_2	0	1	0
a_3	0	0	1

③ solve
$$a_1 = (m_2 m_3)\left([m_2 m_3]^{-1} \bmod m_1\right)$$
$$a_2 = (m_1 m_3)\left([m_1 m_3]^{-1} \bmod m_2\right)$$
$$a_3 = (m_1 m_2)\left([m_1 m_2]^{-1} \bmod m_3\right)$$

④ sum together: $\boxed{x = r_1 a_1 + r_2 a_2 + r_3 a_3}$

general CRT

$$a_i = \left(\frac{m_1 \cdot m_2 \cdot \ldots \cdot m_k}{m_i}\right)\left(\left[\frac{m_1 \cdot m_2 \cdot \ldots \cdot m_k}{m_i}\right]^{-1} \bmod m_i\right)$$

$$x = r_1 a_1 + r_2 a_2 + \ldots + r_k a_k = \sum_{i=1}^{k} r_i a_i \pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_k}$$

CRT parting thoughts

- why do $m_1, m_2, \ldots, m_k$ need to be pairwise co-prime?

↳ so $\left[\dfrac{m_1 \cdot m_2 \cdot \ldots \cdot m_k}{m_i}\right]^{-1} \bmod m_i$

can exist!

- solution will be unique $(\bmod\ m_1 \cdot m_2 \cdot \ldots \cdot m_k)$
- try to understand what each term represents; don't just memorize.

Fermat's Little Theorem

$a^p \equiv a \pmod p$

if p is prime, $a \neq 0$:

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

↓

next time: use to prove RSA works!

Extended Euclid's Algorithm

$2(0) + 5(1) = 5$

$2(1) + 5(0) = 2$

$\longrightarrow$

$$\begin{array}{r} 2(0) + 5(1) = 5 \\ -2[2(1) + 5(0)] = -4 \\ \hline 2(-2) + 5(1) = 1 \end{array}$$

$$\underset{(2^{-1})}{\uparrow} \qquad \underset{k'}{\uparrow}$$

multiply 2nd line by 2, add to first line

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

$\boxed{\text{Extended Euclid's Alg. solves } \gcd(x,y) = ax + by}$

Multiplicative Inverse

$3 \cdot 2^{-1} \equiv 3 \cdot 3 \equiv 9 \equiv \boxed{4 \pmod 5}$

existence of mult. inverse

$\boxed{a^{-1} \pmod m \text{ exists} \iff \gcd(a,m) = 1}$

only when a & m are <u>coprime</u>

DISC. 4A

CRT review

$$\left.\begin{aligned} x &\equiv r_1 \mod m_1 \\ x &\equiv r_2 \mod m_2 \end{aligned}\right\} \text{ if } \gcd(m_1, m_2) = 1,$$

x has unique solution mod $m_1 m_2$.

$$\boxed{x = r_1 a + r_2 b}$$

where:

$a \equiv 1 \mod m_1$ & $a \equiv 0 \mod m_2$

$b \equiv 0 \mod m_1$ & $b \equiv 1 \mod m_2$

$$\boxed{x = r_1(m_2 \underbrace{[m_2^{-1} \mod m_1]}_{a}) + r_2(m_1 \underbrace{[m_1^{-1} \mod m_2]}_{b})}$$

Discussion 4A Notes

- HW/no HW info coming soon
- read: Note 7 & Note 8
- HW 4 due this saturday, 2/17

RSA premise

$$\text{Alice } \xrightarrow{E(x)} \text{ Bob}$$

x $\qquad\qquad$ $D(y) = x$

private knowledge:

d

public knowledge:

$N, e, E(x)$

Eve can access public keys & encrypted message, but can't decrypt without private key!

key features

$N = pq$ = product of primes

$\boxed{\begin{array}{l} e \text{ is } \underline{\text{coprime}} \text{ to } (p-1)(q-1) \\ d \equiv e^{-1} \bmod (p-1)(q-1) \end{array}}$

Alice sends encryted message: $y = E(x) = x^e \bmod N$

Bob recovers original message: $x = D(y) = y^d \bmod N$

Encryption → Decryption

$D(E(x)) = D(x^e) = x^{ed} \bmod N \equiv x \bmod N$

Review

Fermat's Little Theorem
$a^{p-1} \equiv 1 \pmod p$ for p is prime, $a \neq 0$

Why Does RSA work for Bob?

$(x^e)^d \equiv x \mod N \rightarrow x^{ed} - x \equiv 0 \mod N$

1. $x^{ed} - x$ must be divisible by p
2. $x^{ed} - x$ must be divisible by q

pf:

$ed \equiv 1 \mod (p-1)(q-1) \rightarrow ed = k(p-1)(q-1) + 1$

$x^{ed} - x \equiv x\left(x^{k(p-1)(q-1)} - 1\right) \overset{?}{\equiv} 0 \mod p$

case 1: $x \mid p$ trivial ✓

case 2: $(x \nmid p)$

$x\left(\left[x^{p-1}\right]^{k(q-1)} - 1\right) \equiv x\left(1^{k(q-1)} - 1\right) \equiv x(1-1) \equiv 0 \mod p$

WLOG, $x^{ed} - x$ is divisible by p, q & therefore N. □

Why does RSA help encrypt from Eve?

- N is large $\rightarrow$ hard to brute force $y = x^e \mod N$
- hard to factor $pq = N$

DISC. 4B

RSA Review

public keys: $\begin{cases} N = pq & \text{s.t. } \underline{p \text{ \& } q \text{ are prime}} \\ e & \text{s.t. } \underline{\gcd(e, (p-1)(q-1)) = 1} \end{cases}$

private key: d s.t. $\underline{d \equiv e^{-1} \bmod (p-1)(q-1)}$

$$\boxed{x^{ed} \equiv x \mod N}$$

Review Problems

Let a be an integer and p and q be primes. Then $a(a^{(p-1)(q-1)} - 1)$ is a multiple of ______. (Answer should be as large as possible and cannot be 1 or involve a. It may involve p and q.)

answer: $\boxed{pq}$

Discussion 4B Notes

- HW 2 grades released!
- More info about HW/no HW soon
- Read: Note 7 & 8
- HW 4 due on Saturday

Polynomials

$$\boxed{p(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0} \Big\} \; d+1 \text{ terms}$$

d = degree of polynomial
= largest power

roots
r is root iff $p(r) = 0$

degree d ⇒ at most d unique roots

ex: $p(x) = x^2 - 5x + 6 \rightarrow$ degree = 2

$= (x-2)(x-3)$

$$\left.\begin{aligned} p(2) &= 4 - 10 + 6 = 0 \\ p(3) &= 9 - 15 + 6 = 0 \end{aligned}\right\} \underbrace{2 \,\&\, 3}_{\text{2 unique roots}} \text{ are roots of } p(x)$$

Polynomial Representations

1. d+1 coefficients: $a_d, a_{d-1}, \ldots, a_1, a_0$
2. d+1 points: $(x_1, p(x_1)), \ldots, (x_{d+1}, p(x_{d+1}))$

Finite Fields

GF(p) = all operations (mod p), p is prime

↳ fractions or division → multiply by inverse!

polynomial interpolation

goal: given $\underline{d+1}$ points, $(x_i, P(x_i)) \longrightarrow$

$p(x) =$ $\underline{\text{degree } d}$ polynomial that goes through all $d+1$ points.

Approach: Lagrange Interpolation

1 $P(x_1) = y_1$

$P(x_2) = y_2$

$P(x_3) = y_3$

} given 3 points $\rightarrow$ solution is unique degree 2 polynomial!

2 suppose polynomials $\Delta_1(x), \Delta_2(x), \Delta_3(x)$ s.t.:

$\underline{\Delta_1(x_1) = 1}$, $\Delta_1(x_2) = 0$, $\Delta_1(x_3) = 0$ } x_2 & x_3 are $\underline{\text{roots}}$ of $\Delta_1(x)$

$\Delta_2(x_1) = 0$, $\underline{\Delta_2(x_2) = 1}$, $\Delta_2(x_3) = 0$

$\Delta_3(x_1) = 0$, $\Delta_3(x_2) = 0$, $\underline{\Delta_3(x_3) = 1}$

3 $$\Delta_1(x) = \frac{(x-x_2)(x-x_3)}{(x_1-x_2)(x_1-x_3)} = \begin{cases} 1 & \text{when } x = x_1 \\ 0 & \text{when } x \neq x_1 \end{cases}$$

scale so that $\Delta_1(x_1) = 1$

4 $$\boxed{P(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) + y_3 \Delta_3(x)}$$

Lagrange Interpolation Recap

given d+1 points $\longrightarrow$ $\boxed{p(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)}$

linear comb. of d+1 degree d polynomials, $\Delta_i(x)$

$$\boxed{\Delta_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)} = \left[\prod_{j \neq i} (x - x_j)\right] \underbrace{\left[\prod_{j \neq i} (x_i - x_j)\right]^{-1}}}$$

in GF(p), division is multiplying by <u>inverse in (mod p).</u>

This sounds familiar...

$\boxed{\text{same process as } \underline{\text{CRT}}!}$

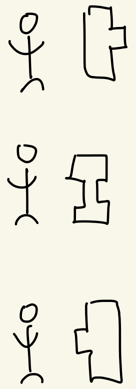
CRT: $x = r_1 a_1 + r_2 a_2 + r_3 a_3$

$$a_i = \left[\prod_{j \neq i} m_j\right] \left(\left[\prod_{j \neq i} m_j\right]^{-1} \bmod m_i\right)$$

LI: $p(x) = y_1 \Delta_1(x) + y_2 \Delta_2(x) + y_3 \Delta_3(x)$

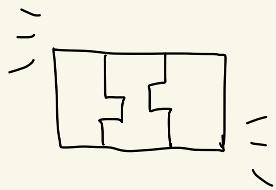
$$\Delta_i = \left[\prod_{j \neq i} (x - x_j)\right] \left(\left[\prod_{j \neq i} (x_i - x_j)\right]^{-1} \bmod p\right)$$

secret sharing premise



k officers, each officer gets one piece of information

secret can be recovered if all k people are present. →



Approach: polynomials!

$(1, P(1))$

$(2, P(2))$

$(3, P(3))$

$\boxed{\text{each officer gets one point on } P(x)}$

use Lagrange Interpolation to recover polynomial $P(x)$

↓

evaluate $P(0)$ = secret

$\boxed{k \text{ officers} \rightarrow k \text{ points} \rightarrow \text{degree } k-1 \text{ polynomial}}$

can $k-1$ officers recover $P(0)$? nope!

DISC. 5A

Error correcting codes

Message: $(1, r_1), (2, r_2), (3, r_3) \dots (n, r_n)$

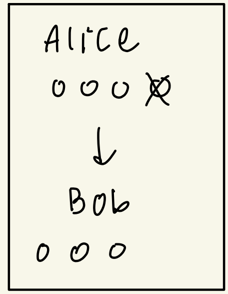
↳ can represent as <u>polynomial w/ deg. n-1</u>

n points through a <u>noisy channel</u> →	can we <u>recover P(X)?</u>

Erasure Errors

problem: <u>lose k</u> out of n points

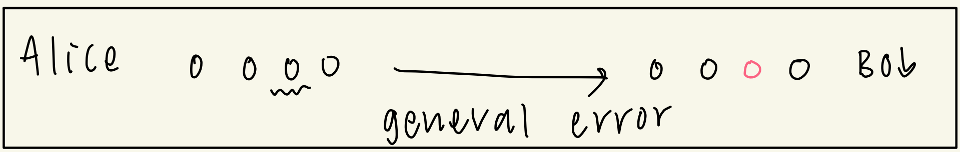
solution: send <u>n+k</u> points



General Errors

problem: channel <u>changes k</u> out of n points

solution: send <u>n+2k</u> points → <u>Berlekamp-Welch</u>



Berlekamp-Welch

<u>Bob has...</u>

n+2k points, → k are corrupted

<u>Bob wants...</u>

P(x)

P(1), P(2), ..., P(n)

Bob doesn't know <u>which points</u> are corrupted!

Berlekamp-Welch Main Ideas

$E(x) = (x-e_1)(x-e_2)\dots(x-e_k)$

- deg. k
- roots at error locations
- 1st coefficient is 1

$Q(x) = P(x)E(x)$ $\longrightarrow$ $\boxed{P(x) = \frac{Q(x)}{E(x)}}$

- deg. $n-1+k$

BKW Procedure

1. $E(x) = x^k + b_{k-1}x^{k-1} + \dots + b_1 x + b_0$

   $Q(x) = a_{n-1+k}x^{n-1+k} + \dots + a_1 x + a_0$

2. set-up system of equations

   $Q(i) = P(i)E(i) = r_i E(i)$ for $1 \dots n+2k$

3. solve for coefficients of $Q(x)$

4. solve for coefficients of $E(x)$

5. solve $P(x) = \frac{Q(x)}{E(x)}$ $\rightarrow$ recover $P(1) \dots P(n)$

DISC. 5B

Review: Berlekamp-Welch

n-length message $\rightarrow \deg[P(x)] = n-1$

k errors $\rightarrow \deg[E(x)] = k$

$Q(i) = r_i E(i) \rightarrow \deg[Q(x)] = n-1+k$

ECC Midterm Problems

Consider a channel that has at most e erasure errors and k corruptions. How many packets should one send to ensure that an n packet message can be recovered?

$\boxed{n+2k+e}$

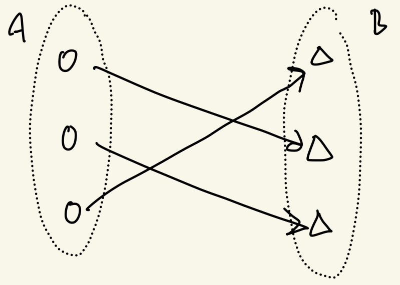
Consider the Berlekamp-Welch error correction scheme where the error polynomial is $E(x) = x^2 - 1 \pmod{13}$. Where are the errors? That is, for which x-values do you have $P(x) \neq r_x$? (Answer should be a list of value(s) from $\{0, 1, \ldots, 12\}$.)

$\boxed{x=1,\ x=12}$

Week 5 Notes

- Read: Note 9, 11, 12
- HW 5 due Saturday
- no HW option released on Ed
- Midterm in 2 weeks :)

Review: Bijections



$f: A \mapsto B$

Cardinality of sets

bijection $\Rightarrow |A| = |B|$

$f: A \to B$ one-to-one $\Rightarrow$
$|A| \leq |B|$

1. onto: $\forall b \in B, \exists a \in A$ s.t. $f(a) = b$

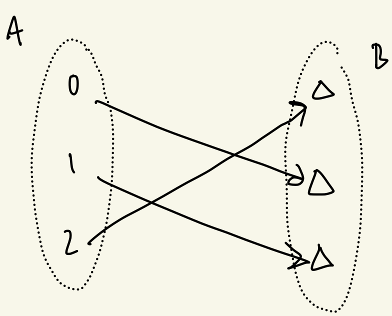
   Every element in B corresponds to at least one value in A.

2. one-to-one: $\forall a_1, a_2 \in A,\ a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

   unique elements in A correspond to unique elements in B.

Countability

counting = defining bijection with $\mathbb{N}$ (or some subset of $\mathbb{N}$)



Bijection b/t A & B, s.t. $A \subseteq \mathbb{N} \Rightarrow$

B is countable!

cantor-bernstein

$f: A \to B$ is one-to-one & $g: B \to A$ is one-to-one

$\Rightarrow$ bijection between A & B

countable sets

subsets of countable sets, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\underbrace{\mathbb{N} \times \mathbb{N}}_{\text{cartesian product}}$

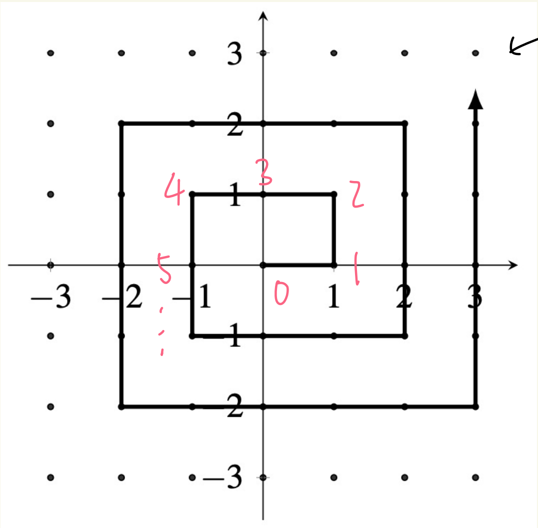
uncountable sets

supersets of uncontable sets, $\underbrace{\mathcal{P}(\mathbb{N})}_{\text{power set}}$, $\mathbb{R}$

∞-length binary strings

proof: $\mathbb{Q}$ is countable

show: $f: \mathbb{Q} \to \mathbb{N}$



each point corresponds to $(a,b) \in \mathbb{Z} \times \mathbb{Z}$

can enemerate elements in $\mathbb{Z} \times \mathbb{Z}$

$\downarrow$

$\mathbb{Z} \times \mathbb{Z}$ is <u>countable</u>.

$\mathbb{Q} \subseteq \mathbb{Z} \times \mathbb{Z} \Rightarrow \mathbb{Q}$ is <u>countable</u>.

proof: $\mathbb{R}$ is uncountable

$\boxed{\text{proof by contradiction}}$ assume: $f: \mathbb{N} \to \mathbb{R}$

$$
\left.
\begin{array}{l}
f(0) = 0\,.\,5\,2\,1\,4\,9\,3\,5\,6\,\cdots \\
f(1) = 0\,.\,1\,4\,1\,6\,2\,9\,8\,5\,\cdots \\
f(2) = 0\,.\,9\,4\,7\,8\,2\,7\,1\,2\,\cdots \\
f(3) = 0\,.\,5\,3\,0\,9\,8\,1\,7\,5\,\cdots \\
\quad\vdots \qquad\qquad\qquad \vdots
\end{array}
\right\}
$$

enemerate every real number.

① is f surjective? let's make a new #!

$$0.\ \underset{0}{\underline{5}}\quad \underset{1}{\underline{4}}\quad \underset{2}{\underline{7}}\quad \underset{3}{\underline{9}}\quad \cdots\quad \underset{n+1}{\underline{k}}\quad \cdots$$

② change each digit (ex: d+2 mod 10)

$$0.\ \underset{0}{\underline{7}}\quad \underset{1}{\underline{6}}\quad \underset{2}{\underline{9}}\quad \underset{3}{\underline{1}}\quad \cdots\quad \underset{n+1}{\underline{(k+2 \bmod 10)}}\quad \cdots$$

③ if f is bijective, $f(n) = 0.7691\ldots$ for some n

④ but decimal place n+1 is different in $0.7691\ldots$ vs. $f(n)$!

⑤ $0.7691\ldots$ is <u>not</u> enumerated $\Rightarrow$ f is not surjective!

$\boxed{\text{Cantor's Diagonalization Argument}}$

DISC. 6A

Review: countability

types of sets:

1. finite, ex: $\{0, 1\}$
2. countably infinite, ex: $\{0, 1, 10, 11, 100, \dots\}$
3. uncountably infinite, ex: $\{010\dots, 101\dots, \dots\}$

finite-length bit-strings

∞-length bit-strings

Sp'23 #15

The set of all finite subsets of a countably infinite set is uncountable.

○ True ○ False

The set of all subsets of a countably infinite set is uncountable.

○ True ○ False

1. False, 2. True

Week 6 Notes

- Midterm: Wed., 3/6, 7-9 pm
  - ↳ no HW, no Tues. lecture, no wed. discussion
- Read: Notes 12 & 10
- HW 6 due Saturday

Computability

some problems can't be solved with a program!

Example: Halting problem

1. suppose TestHalt exists and performs:

TestHalt (P, X) : $\begin{cases} \text{True} & \text{if } P(X) \text{ halts} \\ \text{False} & \text{if } P(X) \text{ loops forever} \end{cases}$

2. suppose Turing exists and performs:

```
Turing (P):
    if TestHalt (P, P):
        loop
    else:
        return/halt
```

3. execute Turing (Turing)

4. case 1: Turing (Turing) loops.

- TestHalt (Turing, Turing) = True
- Turing (Turing) halts

$\Big\}$ contradiction!

5. case 2: Turing (Turing) halts

- TestHalt (Turing, Turing) = False
- Turing (Turing) loops

$\Big\}$ contradiction!

6. By contradiction, TestHalt <u>does not exist</u>.

Halting problem takeaways

- TestHalt does not exist
- Any prog. that could be used to construct TestHalt does not exist!

proof: P(X) is uncomputable

1. suppose TestOther exists.
2. show TestOther solves TestHalt.

```
def TestHalt(P, x):
    def Q(y):
        P(x)
        do what TestOther is checking
    return TestOther(Q, y)
```

3. contradiction: TestHalt can't exist.
4. conclude: TestOther can't exist.

Intuition

- can prog. return in finite # steps/loops?
  → probably computable...
- will prog. potentially take ∞ steps?
  → probably uncomputable...

counting rules

① ___ ___ ___ ... ___ k choices

1 2 3 ... k

n_1 options, n_2 options ... n_k options

multiplication rule

$n_1 \times n_2 \times \ldots \times n_k$ total ways to choose

② divide by # of duplicate ways when distinguishing between them doesn't matter

division rule

A ways, but m of the A ways are equivalent → divide by m

combination

choose k out of n, order doesn't matter

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

DISC. 6B

Review: computability

- Halting problem is uncomputable
- If TestOther can be used to make TestHalt $\Rightarrow$ TestOther is uncomputable

Sp'23 Final

3. The number of computer programs is countable.

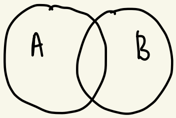
4. The number of outputs for any computer program on any finite length input is countable. (Note that the output of a computer program could be an infinite sequence of digits, for example, a square root program could run forever while printing the digits of $\sqrt{2}$.)

$\boxed{\text{3. True, 4. True}}$

Week 6 Notes

- Midterm: Wed., 3/6, 7-9 pm
- Read: Notes 12 & 10
- HW 6 due Saturday

Principle of Inclusion-Exclusion

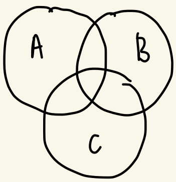


$$\boxed{|A \cup B| = |A| + |B| - |A \cap B|}$$

amt. in A

amt. in B

amt. in A and B



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

- alternately subtract / add back intersections to avoid double counting

Permutations, Combinations

$\frac{n!}{(n-k)!}$ = # ways to choose k out of n where order matters

---

$\frac{n!}{(n-k)!\,k!}$ = # ways to choose k out of n where order doesn't matter

AKA $\binom{n}{k}$ ← "n choose k"

$$\boxed{\binom{n}{k} = \binom{n}{n-k} \text{ in general}}$$

combinotorial proofs

ex: $\binom{2n}{2} = 2\binom{n}{2} + n^2$

proof: tell equivalent stories for LHS & RHS

LHS: I have 2n actors, and I cast 2 of them to be leads

RHS: I have n short actors & n tall actors.

case 1: I cast 2 short actors $\rightarrow \binom{n}{2}$ ways

case 2: I cast 2 tall actors $\rightarrow \binom{n}{2}$ ways

case 3: I cast 1 short & 1 tall $\rightarrow n^2$ ways

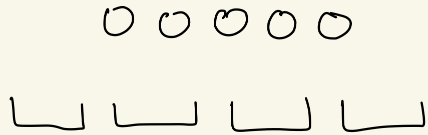
$\therefore \binom{2n}{2} = 2\binom{n}{2} + n^2$

strategies

- addition means multiple cases
- multiplication means simultaneous choices

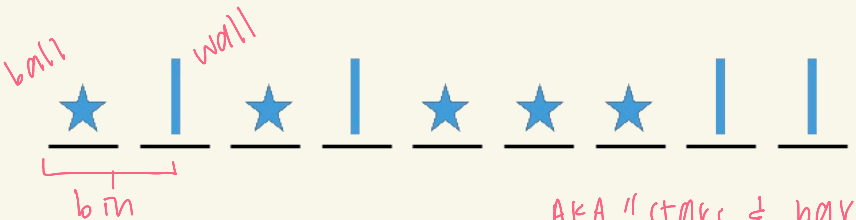
Balls & Bins

k balls, n bins



$$\boxed{\binom{n-1+k}{k} = \binom{n-1+k}{n-1} = \text{ways to arrange}}$$

ex: 5 balls, 4 bins $\rightarrow \binom{4-1+5}{5} = \binom{8}{5} = \frac{8!}{5!\,3!} = 54$



AKA "stars & bars"

equivalently: k balls, $n-1$ walls

$$\binom{n-1+k}{n-1}$$

$n-1+k \leftarrow$ # positions available

$n-1 \leftarrow$ choose $n-1$ positions to be walls!

equivalently:

$$\binom{n-1+k}{k}$$

$k \leftarrow$ choose k positions to be balls!

$\boxed{\text{DISC. 7B}}$

Review: counting

How many ways to ...

- choose k objects out of n? $\boxed{\dfrac{n!}{k!(n-k)!}}$
- choose k objects out of n with order? $\boxed{\dfrac{n!}{(n-k)!}}$
- place n objects in m bins? $\boxed{\dfrac{(n+m-1)!}{n!(m-1)!}}$
- select any subset from n items? $\boxed{2^n}$

SP'23 Final #10

4. How many Hamiltonian paths are there on K_n?

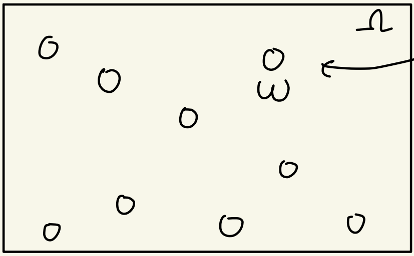
5. How many Hamiltonian cycles are there on K_n?

$\boxed{4.\ n!,\quad 5.\ (n-1)!}$

week 7 Notes

- congrats on midterm! ☺
- Read: Note 13
- Feedback? Let me know in Attendance form

probability space



sample point = outcome of random event (ω)

sample space = set of all sample points (Ω)

each sample point, $\omega \in \Omega$, occurs with probability $\mathbb{P}[\omega]$.

probability law properties

① $0 \leq \mathbb{P}[\omega] \leq 1$

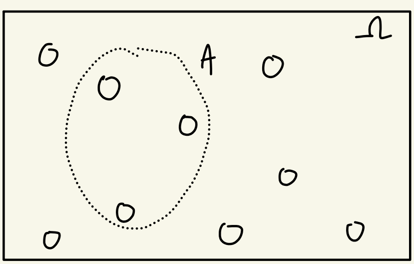
② $\sum_{\omega \in \Omega} \mathbb{P}[\omega] = 1$

uniform probability space

- every $\omega \in \Omega$ is equally likely

$\boxed{\mathbb{P}[\omega] = \frac{1}{|\Omega|}}$ → how to get $|\Omega|$? counting!

Events



event = subset of sample space ($A \subseteq \Omega$)

ex: $\mathbb{P}[A] = \frac{3}{9} = \frac{1}{3}$

probability of event in unif. Ω

$$\mathbb{P}[A] = \sum_{\omega \in A} \mathbb{P}[\omega] = \frac{|A|}{|\Omega|}$$

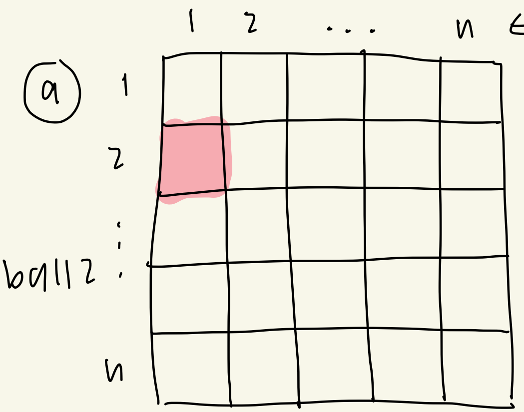
3 Sampling

Suppose you have balls numbered $1, \ldots, n$, where n is a positive integer ≥ 2, inside a coffee mug. You pick a ball uniformly at random, look at the number on the ball, replace the ball back into the coffee mug, and pick another ball uniformly at random.

(a) What is the probability that the first ball is 1 and the second ball is 2?

(b) What is the probability that the second ball's number is strictly less than the first ball's number?

(a)

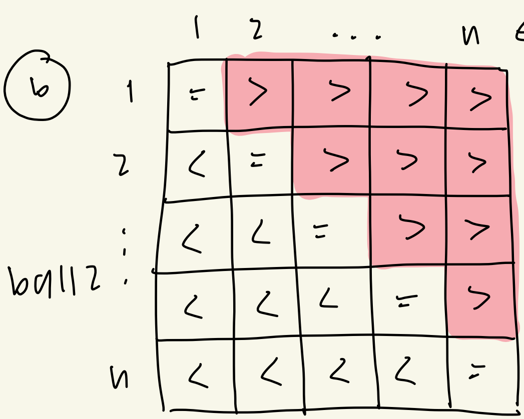


# of total pairs =

$|\Omega| = n^2$

$\mathbb{P}[(1,2)] = \frac{1}{|\Omega|} = \boxed{\frac{1}{n^2}}$

(b)



pairs where ball 1 $\neq$ ball 2:

$n^2 - n$

# of pairs where ball 1 > ball 2:

$\frac{1}{2}(n^2 - n)$

$\mathbb{P}[\text{ball } 1 > \text{ball } 2] = \frac{\frac{1}{2}(n^2-n)}{n^2} = \boxed{\frac{n-1}{2n}}$

(c) What is the probability that the second ball's number is exactly one greater than the first ball's number?

(d) Now, assume that after you looked at the first ball, you did *not* replace the ball in the coffee mug (instead, you threw the ball away), and then you drew a second ball as before. Now, what are the answers to the previous parts?

c

	1	2	...		n ← ball 1
1	=	>	>	>	>
2	<	=	>	>	>
⋮	<	<	=	>	>
ball2	<	<	<	=	>
n	<	<	<	<	=

$$\mathbb{P}[\text{ball } 2 = \text{ball } 1 + 1] = \boxed{\frac{n-1}{n^2}}$$

d

	1	2	...		n ← ball 1
1		>	>	>	>
2	<		>	>	>
⋮	<	<		>	>
ball2	<	<	<		>
n	<	<	<	<	

$$\text{new } |\Omega| = n^2 - n$$

$$= n(n-1)$$

$$\mathbb{P}[(1,2)] = \boxed{\frac{1}{n(n-1)}}$$

$$\mathbb{P}[\text{ball } 1 > \text{ball } 2] = \frac{n-1}{2(n-1)} = \boxed{\frac{1}{2}}$$

$$\mathbb{P}[\text{ball } 2 = \text{ball } 1 + 1] = \frac{n-1}{n(n-1)} = \boxed{\frac{1}{n}}$$

$\boxed{\text{DISC. 8A}}$

Review: Discrete Probability

event = subset of sample space

$\mathbb{P}[A] = \frac{|A|}{|\Omega|}$ for discrete uniform space

complement = $\overline{A} = \Omega \setminus A$

$\mathbb{P}[\overline{A}] = \frac{|\Omega \setminus A|}{|\Omega|} = 1 - \mathbb{P}[A]$

SP'22 Final # 10.1

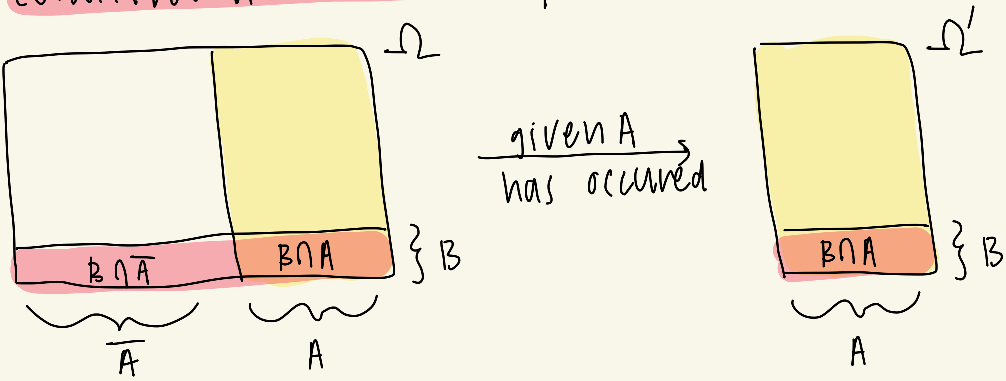
1. $\mathbb{P}[A \cap B] = 1 - \mathbb{P}[\overline{A} \cup \overline{B}] -$ __?__.

$\boxed{\mathbb{P}[A \cap B]}$

Week 8 Notes

- regrade requests open! due 3/18
- TA 1:1s open
- HW 8 due sat.
- Read Notes 13 & 14

conditional probability



renormalize probability! we're in a new sample space:

$$\boxed{\mathbb{P}[B \mid A] = \frac{\mathbb{P}[B \cap A]}{\mathbb{P}[A]}}$$

Bayes Rule

$$\mathbb{P}[B \mid A] = \frac{\mathbb{P}[B \cap A]}{\mathbb{P}[A]} = \frac{\mathbb{P}[A \mid B]\,\mathbb{P}[B]}{\mathbb{P}[A]}$$

↳ relates $\mathbb{P}[B \mid A]$ & $\mathbb{P}[A \mid B]$

Law of Total Probability

$$\mathbb{P}[B] = \mathbb{P}[B \cap A] + \mathbb{P}[B \cap \bar{A}]$$

complement of event A! i.e. $\Omega \setminus A$

General Total probability

$A_1, A_2, \ldots, A_n$ partition Ω → they cover all Ω & don't intersect

$$\Rightarrow \mathbb{P}[B] = \sum_{i=1}^{n} \mathbb{P}[B \cap A_i] = \sum_{i=1}^{n} \mathbb{P}[B \mid A_i]\,\mathbb{P}[A_i]$$

independence

chance of B <u>not</u> affected by whether or not A occurs!

independence

$$\mathbb{P}[B \mid A] = \mathbb{P}[B] \implies \mathbb{P}[A \cap B] = \mathbb{P}[A]\,\mathbb{P}[B]$$

$$\mathbb{P}[A \mid B] = \mathbb{P}[A]$$

pairwise independence

each pair is independent, i.e.:

$$\mathbb{P}[A \cap B] = \mathbb{P}[A]\,\mathbb{P}[B]$$

$$\mathbb{P}[B \cap C] = \mathbb{P}[B]\,\mathbb{P}[C]$$

$$\mathbb{P}[C \cap A] = \mathbb{P}[C]\,\mathbb{P}[A]$$

mutual independence

every subset is independent, i.e.:

given $A_1, \ldots, A_n$

$$\mathbb{P}\Big[\bigcap_{i \in I} A_i\Big] = \prod_{i \in I} \mathbb{P}[A_i] \quad \text{where } I \subseteq \{1, \ldots, n\}$$

3 Pairwise Independence

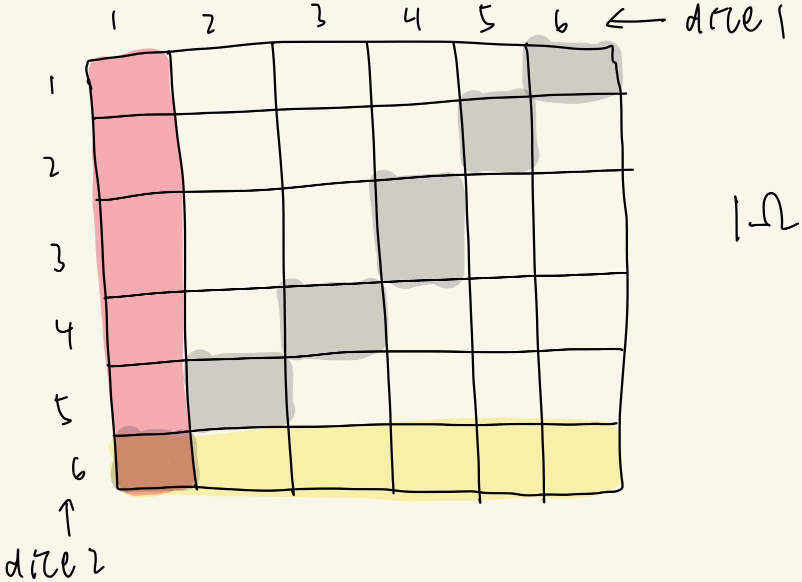
Recall that the events A_1, A_2, and A_3 are *pairwise independent* if for all $i \neq j$, A_i is independent of A_j. However, pairwise independence is a weaker statement than *mutual independence*, which requires the additional condition that $\mathbb{P}[A_1 \cap A_2 \cap A_3] = \mathbb{P}[A_1]\mathbb{P}[A_2]\mathbb{P}[A_3]$.

Suppose you roll two fair six-sided dice. Let A_1 be the event that the first die lands on 1, let A_2 be the event that the second die lands on 6, and let A_3 be the event that the two dice sum to 7.

(a) Compute $\mathbb{P}[A_1]$, $\mathbb{P}[A_2]$, and $\mathbb{P}[A_3]$.

(b) Are A_1 and A_2 independent?

(c) Are A_2 and A_3 independent?



$|\Omega| = 36$

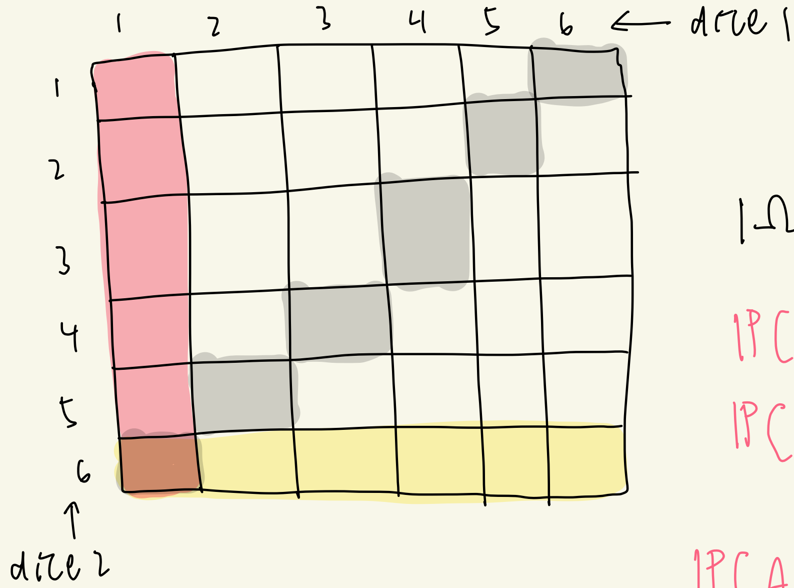
(a) $\mathbb{P}[A_1] = \frac{6}{36}$ $\mathbb{P}[A_2] = \frac{6}{36}$ $\mathbb{P}[A_3] = \frac{6}{36}$

(b) $\mathbb{P}[A_1 \cap A_2] = \frac{1}{36} = \mathbb{P}[A_1]\mathbb{P}[A_2]$ ✓

(c) $\mathbb{P}[A_2 \cap A_3] = \frac{1}{36} = \mathbb{P}[A_2]\mathbb{P}[A_3]$ ✓

(d) Are A_1, A_2, and A_3 pairwise independent?

(e) Are A_1, A_2, and A_3 mutually independent?



$|\Omega| = 36$

$\mathbb{P}[A_1 | A_2] = \mathbb{P}[A_1]$

$\mathbb{P}[A_2 | A_1] = \mathbb{P}[A_2]$

$\downarrow$

$\mathbb{P}[A_1 \cap A_2]$

$= \mathbb{P}[A_2 | A_1]\mathbb{P}[A_1]$

$= \mathbb{P}[A_2]\mathbb{P}[A_1]$

(d) pairwise independence:

$\mathbb{P}[A_1 \cap A_2] = \mathbb{P}[A_1]\mathbb{P}[A_2]$ ✓

$\mathbb{P}[A_2 \cap A_3] = \mathbb{P}[A_2]\mathbb{P}[A_3]$ ✓ → Yes!

$\mathbb{P}[A_3 \cap A_1] = \mathbb{P}[A_3]\mathbb{P}[A_1]$ ✓

(e) mutual independence:

$\mathbb{P}[A_1 \cap A_2 \cap A_3] \stackrel{?}{=} \mathbb{P}[A_1]\mathbb{P}[A_2]\mathbb{P}[A_3]$ → no!

$\frac{1}{36} \neq \left(\frac{1}{6}\right)\left(\frac{1}{6}\right)\left(\frac{1}{6}\right)$

DISC. 8B

Review: Conditional / Total Prob. / Independence

$$\mathbb{P}[B|A] = \frac{\mathbb{P}[B \cap A]}{\mathbb{P}[A]} = \frac{\mathbb{P}[A|B]\,\mathbb{P}[B]}{\mathbb{P}[A]}$$

partition Ω

$$\mathbb{P}[B] = \sum_i \mathbb{P}[B \cap A_i] = \sum_i \mathbb{P}[B|A_i]\,\mathbb{P}[A_i]$$

$$\mathbb{P}[B|A] = \mathbb{P}[B] \iff \mathbb{P}[A \cap B] = \mathbb{P}[A]\,\mathbb{P}[B] \iff A \text{ \& } B \text{ independ.}$$

FA'21 Final #11

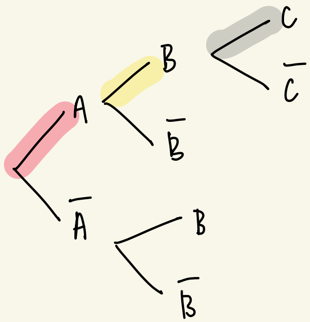
A bag contains a 4-sided die and a 6-sided die. Your friend Lucas pulls a die out of the bag uniformly at random, rolls it, and gets a 1. Conditional on this event, what is the probability they pulled the 4-sided die out of the bag? Show your work.

$\boxed{3/5}$

Week 8 Notes

- regrade requests open! due 3/18
- TA 1:1s open
- HW 8 due sat.
- Read Notes 13 & 14

Intersections of Events



$\mathbb{P}[A \cap B] = \mathbb{P}[B \mid A]\,\mathbb{P}[A]$

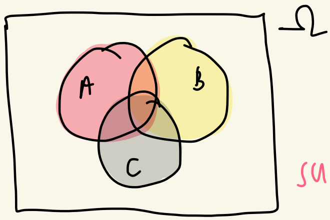
$\mathbb{P}[A \cap B \cap C] = \mathbb{P}[C \mid B \cap A]\,\mathbb{P}[B \mid A]\,\mathbb{P}[A]$

$\mathbb{P}[A_1] \times \mathbb{P}[A_2] \times \ldots \times \mathbb{P}[A_n]$ when independent events!

multiplication rule

$$\mathbb{P}\left[\bigcap_{i=1}^{n} A_i\right] = \mathbb{P}[A_1] \times \mathbb{P}[A_2 \mid A_1] \times \mathbb{P}[A_3 \mid A_1 \cap A_2] \times \ldots \times \mathbb{P}\left[A_n \,\middle|\, \bigcap_{i=1}^{n-1} A_i\right]$$

Unions of Events



$\mathbb{P}[A \cup B \cup C] =$

add! $\mathbb{P}[A] + \mathbb{P}[B] + \mathbb{P}[C]$

subtract $- \mathbb{P}[A \cap B] - \mathbb{P}[B \cap C] - \mathbb{P}[C \cap A]$

to avoid overcounting sample points → add back! $+ \mathbb{P}[A \cap B \cap C]$

Inclusion-Exclusion Rule

$$\mathbb{P}\left[\bigcup_{i=1}^{n} A_i\right] = \sum_{i=1}^{n} \mathbb{P}[A_i] - \sum_{i<j} \mathbb{P}[A_i \cap A_j] + \ldots + (-1)^{n-1}\,\mathbb{P}\left[\bigcap_{i=1}^{n} A_i\right]$$

↓ so we can conclude...

Union Bound

$$\mathbb{P}\left[\bigcup_{i=1}^{n} A_i\right] \le \sum_{i=1}^{n} \mathbb{P}[A_i]$$

← inequality becomes equality when mutually exclusive events

(no overlap!)

DISC. 9A

DISC. 9B

DISC. 11 B

Review: variance & covariance

$\text{var}(X) = \text{cov}(X,X) = \mathbb{E}[X^2] - (\mathbb{E}[X])^2$ = how spread out is X?

$\text{cov}(X,Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$ = how correlated are X & Y?

X & Y are independent $\Longrightarrow$ $\text{cov}(X,Y) = 0$

<u>but</u> not the other way around!

Review: Indicator Variables

$$X_i = \begin{cases} 1 & \text{if event occurs} \\ 0 & \text{otherwise} \end{cases}$$

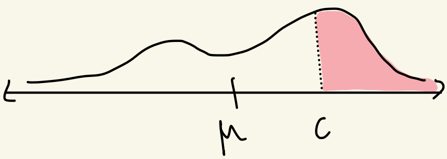
$$\boxed{\begin{array}{l} \mathbb{E}[X_i] = p \\ \text{var}(X_i) = p(1-p) \leq \frac{1}{4} \end{array}}$$

$X = \sum_{i=1}^{n} X_i$ = # occurences out of n, X_i are IID.

$$\mathbb{E}[X] = \mathbb{E}\left[\sum_{i=1}^{n} X_i\right] = n\mathbb{E}[X_1]$$

$$\mathbb{E}[X^2] = \mathbb{E}\left[\left(\sum_{i=1}^{n} X_i\right)^2\right] = \mathbb{E}\left[\sum_{i=1}^{n} X_i^2 + 2\sum_{i<j} X_iX_j\right]$$

concentration inequalities

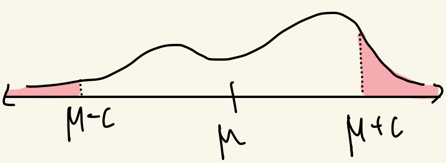


how likely is it for X to be c or greater?

Markov's Inequality

$$\mathbb{P}[X \geq c] \leq \frac{\mathbb{E}[X]}{c}$$

→ for nonnegative RVs only!



how likely is it for X to be c away from mean?

Chebyshev's Inequality

$$\mathbb{P}[|X - \mathbb{E}[X]| \geq c] \leq \frac{\text{var}(X)}{c^2}$$

Estimators

$\hat{p}$ estimates p if $\mathbb{E}[\hat{p}] = p$.

estimation error bound

$$\boxed{|\hat{p} - p| \le \varepsilon}$$

$$\mathbb{P}[|\hat{p} - p| \le \varepsilon] \ge \text{confidence}$$

↓ or

$$\mathbb{P}[|\hat{p} - p| > \varepsilon] < 1 - \text{confidence}$$

Sample Mean

$$\boxed{\bar{X}_n = \frac{X_1 + X_2 + \dots + X_n}{n}}$$ is an estimator of $\mathbb{E}[X_i]$.

Law of Large Numbers

$$\lim_{n \to \infty} \mathbb{P}[|\bar{X}_n - \mu| \ge \varepsilon] = 0$$

↓

probability of deviation goes to 0,

$\bar{X}$ converges to $\mathbb{E}[X_i]$

(estimator ⟶ true mean)

DISC. 12A

Review: Concentration Inequalities

Markov's: $\mathbb{P}[X \geq c] \leq \frac{\mathbb{E}[X]}{c}$ → one-sided, X is non-negative

Chebyshev's: $\mathbb{P}[|X - \mathbb{E}[X]| \geq c] \leq \frac{Var(X)}{c^2}$ → two-sided, X can be negative

Review: Variance

Discrete Uniform: $\frac{(b-a+1)^2 - 1}{12}$

Bernoulli: $p(1-p)$

Binomial: $np(1-p)$

geometric: $\frac{1-p}{p^2}$

Poisson: λ

Sp'23 #12

Suppose Shreyas stores some number S initialized to 0. Every time he flips a fair coin, if it lands heads he increments S by 1 and if it lands tails he decrements S by 1. He wishes to calculate $\mathbb{P}[S \geq 20]$ after flipping the coin 100 times.

2. (5 points) Provide an upper bound using Markov's inequality.

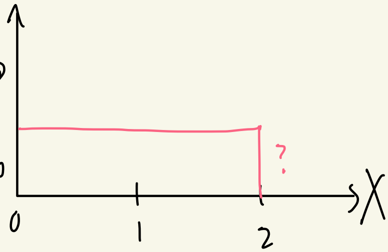
5/6

Week 12 Notes

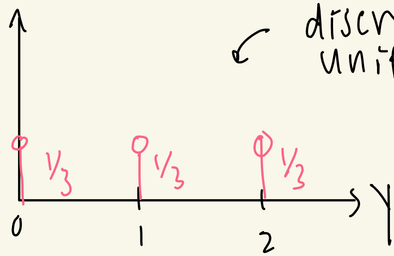
- HW 12 due Saturday
- read Note 21

continuous vs. discrete

continuous uniform



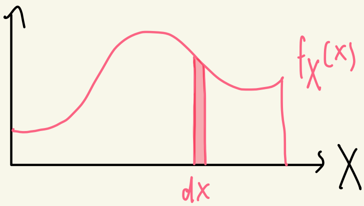
discrete uniform



$\mathbb{P}[X=1] = \frac{1}{\infty} = 0$

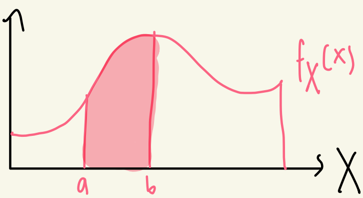
$\mathbb{P}[1 \le X \le 2] = \frac{1}{2}$ → we can determine probabilities of intervals!

probability density function



$f_X(x)$ = probability per unit length

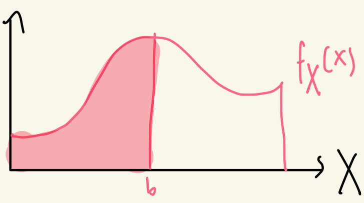
$\mathbb{P}[x \le X \le x+dx] \approx \underbrace{f_X(x)}_{\text{height}} \underbrace{dx}_{\text{width}}$



$$\boxed{\mathbb{P}[a \le X \le b] = \int_a^b f_X(x)\,dx}$$

cumulative distribution function

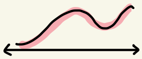
$$\mathbb{P}[X \le b] = \int_{-\infty}^{b} f_X(x)\,dx = F_X(b)$$



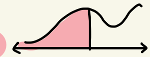
$$\boxed{\mathbb{P}[X \le x] = F_X(x) = \int_{-\infty}^{x} f_X(z)\,dz}$$

relating PDF & CDF

$F(x) = \int_{-\infty}^{x} f(z)\,dz$ (integrate!)

$f_X(x) = \text{PDF}$ 

- → $\underline{\text{not}}$ a probability
- → $f_X(x) \geq 0 \;\; \forall x$
- → $\int_{-\infty}^{\infty} f_X(x)\,dx = 1$
- → $\mathbb{P}[a \leq X \leq b] = \int_a^b f_X(x)\,dx$

$F_X(x) = \text{CDF}$ 

- → $\underline{\text{is}}$ a probability
- → $0 \leq F_X(x) \leq 1$
- → $\lim_{x \to \infty} F_X(x) = 1$
- → $\mathbb{P}[X \leq x] = F_X(x)$

$f(x) = \frac{d}{dx} F(x)$ (differentiate!)

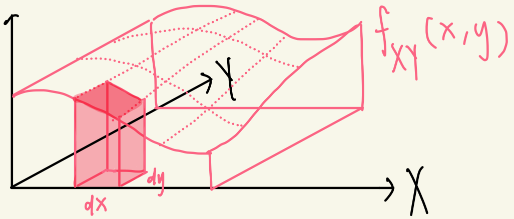
other ideas from discrete probability...

$$\left.\begin{aligned} \mathbb{E}[X] &= \int_{-\infty}^{\infty} x f(x)\,dx \\ \mathbb{E}[X^2] &= \int_{-\infty}^{\infty} x^2 f(x)\,dx \end{aligned}\right\} \text{ instead of sum} \rightarrow \underline{\text{integral}}!$$

$$\text{var}(X) = \mathbb{E}[X^2] - (\mathbb{E}[X])^2$$

X & Y are independent $\iff f_{XY}(x,y) = f_X(x) f_Y(y)$

continuous joint PDF



- → function of <u>two</u> variables
- → probability is a <u>double</u> integral
- → $f_{XY}(x,y) \geq 0 \;\; \forall x, y \in \mathbb{R}$
- → $\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_{XY}(x,y)\,dx\,dy = 1$

$f_{XY}(x,y)$ = probability per <u>unit area</u>

$$\mathbb{P}[x \leq X \leq x+dx,\; y \leq Y \leq y+dy] \approx \underbrace{f_{XY}(x,y)}_{\text{height}} \underbrace{dx\,dy}_{\text{area}}$$

joint PDF

$$\mathbb{P}[a \leq X \leq b,\; c \leq Y \leq d] = \int_c^d \int_a^b f_{XY}(x,y)\,dx\,dy$$

exponential random variable

↳ continuous version of <u>geometric</u>

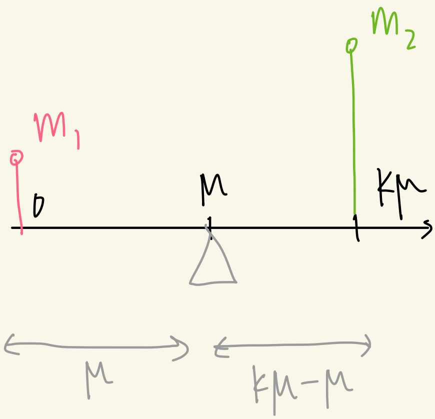
↳ $X \sim \text{Exp}(\lambda)$, where λ is <u>rate of occurence</u>

PDF: $f(x) = \begin{cases} \lambda e^{-\lambda x}, & x \geq 0 \\ 0 & \text{otherwise} \end{cases}$

$\mathbb{E}[X] = \frac{1}{\lambda}$

$\text{Var}(X) = \frac{1}{\lambda^2}$

DISC. 12B



$$\mathbb{P}[X \geq k\mu] \leq \frac{1}{k}$$

$$m_1 \cdot 0 + m_2 \cdot k\mu = \mu$$

$$m_2 \cdot k\mu = \mu$$

$$m_2 = \frac{1}{k}$$

$$\frac{0 \cdot m_1 + k\mu \cdot m_2}{m_1 + m_2} = \mu$$

$$k\mu \cdot m_2 = \mu(m_1 + m_2)$$

$$k m_2 = m_1 + m_2$$

$$m_1 + m_2 = 1$$

$$m_1 = 1 - m_2$$

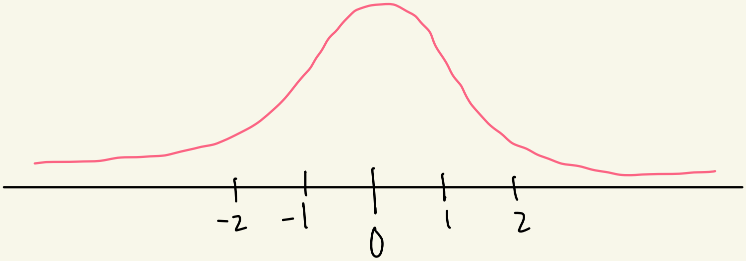
$$k m_2 = 1 - m_2 + m_2$$

$$m_2 = \frac{1}{k}$$

$\boxed{\text{DISC. 12B}}$

Review: Continuous vs. Discrete

Standard Normal Distribution



$\mathbb{E}[Z] = \underline{0}$

$\text{Var}(Z) = \underline{1}$

$Z \sim \underline{\mathcal{N}(0,1)}$

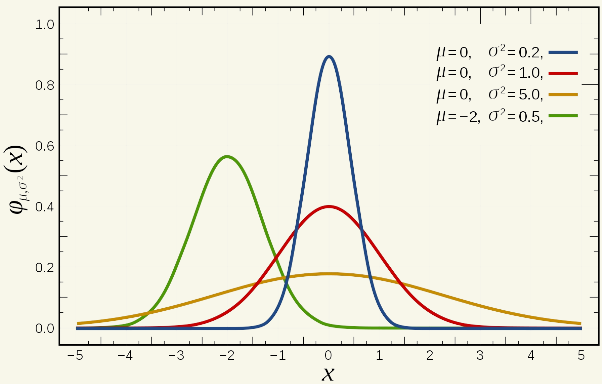
Standard normal PDF

$$f_Z(z) = \frac{1}{\sqrt{2\pi}} e^{-z^2/2}$$

standard norm. CDF

$$\Phi_Z(z) = \mathbb{P}[Z \le z] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{t^2}{2}} dt$$

general Normal Distribution



$X = \sigma Z + \mu$

scale by std.

shift by mean

$\mathbb{E}[X] = \underline{\mu}$, $\text{Var}(X) = \underline{\sigma}$

$X \sim \underline{\mathcal{N}(\mu,\sigma)}$

general norm. PDF

$$f_X(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-(x-\mu)^2/2\sigma^2}$$

adding Gaussians

if X, Y are independent,

$$aX + bY \sim \mathcal{N}(a\mu_X + b\mu_Y,\ a^2\sigma_X^2 + b^2\sigma_Y^2)$$

central limit theorem

$X_1, X_2, \ldots$ are IID, $\mathbb{E}[X_i] = \mu$, $\text{var}(X_i) = \sigma^2$.

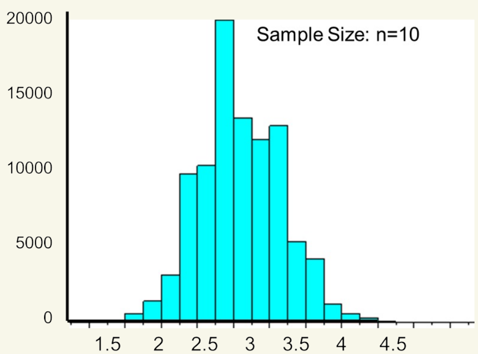
$$\frac{\sum_{i=1}^{n} X_i - n\mu}{\sigma\sqrt{n}} \quad \text{converges to } \mathcal{N}(0,1)$$

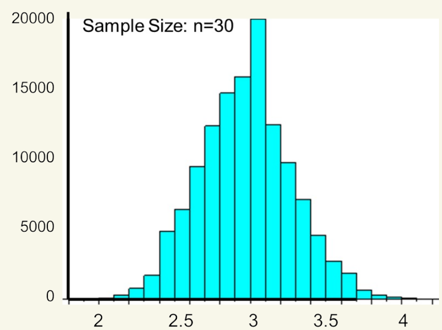
as $n \to \infty$.

another perspective...

$$\frac{S_n}{n} \longrightarrow \mathcal{N}\left(\mu, \frac{\sigma^2}{n}\right) \text{ as } n \to \infty.$$

Also, as $n \to \infty$, variance $\to 0$.





$\boxed{\text{DISC. 13 A}}$

Review: Gaussian R.V.

$$f_X(x) = \frac{1}{\sqrt{2\pi\sigma}} e^{-(x-\mu)^2/2\sigma^2}$$

SP'23 # 15

15. Just a moment or three.

Let $X \sim \mathcal{N}(\mu, \sigma^2)$.

1. Compute $\mathbb{E}[X]$.

2. Compute $\mathbb{E}[X^2]$.

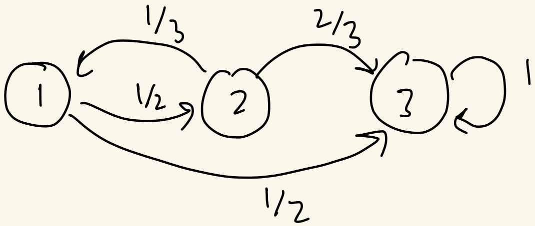
3. (5 points) Compute $\mathbb{E}[X^3]$. *Hint:* $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

$\boxed{1.\ \mu,\ 2.\ \mu^2+\sigma^2,\ 3.\ 3\sigma^2\mu+\mu^3}$

Week 13 Notes

- last time no HW option will be available
- RRR week: no required discussions
- read Note 22

markov chains



state space ($\mathcal{X}$) $= \{1, 2, 3\}$

X_n = position at time n

markov property

$$\mathbb{P}[X_{n+1} = j \mid X_n = i, X_{n-1}, \ldots, X_0] = \mathbb{P}[X_{n+1} = j \mid X_n = i]$$

probability transition matrix

$$P = \begin{bmatrix} 0 & 1/2 & 1/2 \\ 1/3 & 0 & 2/3 \\ 0 & 0 & 1 \end{bmatrix}$$

1. $P(i,j)$ is $\mathbb{P}[X_{n+1} = j \mid X_n = i]$
2. $\sum_{\text{row}} P(i,j) = 1$
3. $0 \leq P(i,j) \leq 1$

<u>ex:</u> start at $X_0 = 1 \rightarrow \pi_0 = [1 \quad 0 \quad 0] \rightarrow$

$\pi_1 = [0 \quad 1/2 \quad 1/2]$

$$[1 \quad 0 \quad 0] \begin{bmatrix} 0 & 1/2 & 1/2 \\ 1/3 & 0 & 2/3 \\ 0 & 0 & 1 \end{bmatrix} = [0 \quad 1/2 \quad 1/2]$$

in general...

$\pi_{n+1} = \pi_n P \quad , \quad \pi_n = \pi_0 P^n$

invariant distribution

$$\boxed{\pi = \pi P \longrightarrow \pi_n = \pi_0}$$

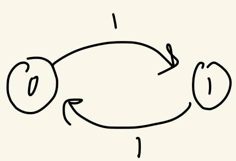
- if you start in π_0, distribution stays same!
- to solve for π:

1. $\pi = \pi P \longrightarrow$ AKA eigenvector of P^T with eigenvalue of 1
2. $\sum_{row} \pi(i) = 1 \rightarrow$ sum of entries $= 1$.

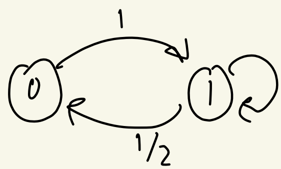
Fundamental Theorem

- irreducible = from state i, can go to any state j
- aperiodic = $\boxed{\gcd\{\#\text{ steps to return to } i\} = 1}$

↳ ex: self-loop ⇒ aperiodic



is periodic.



is aperiodic.

Fundamental thm.

finite, irreducible, aperiodic $\Rightarrow$ π_n converges to invariant distribution as $n \rightarrow \infty$

DISC. 13 B

Review: Markov chain properties

irreducible = path exists from every i to every j

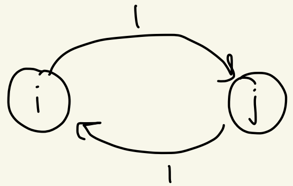
period = $\gcd\{\#$ steps to return to $i\}$

aperiodic = period of 1

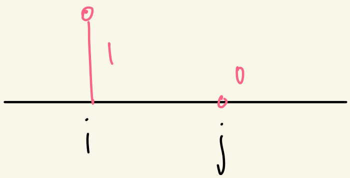
Week 13 Notes

- last time no HW option will be available
- RRR week: no required discussions
- read Note 22

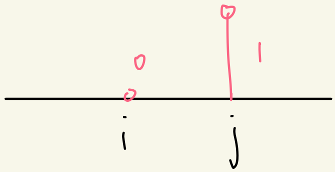
distributions at time n



$$P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

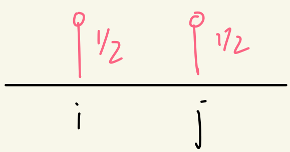
$\pi_0 =$ 

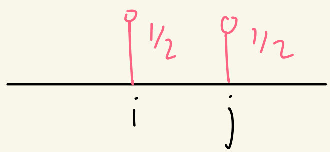
$=$ PMF of X_0

$\pi_1 = \pi_0 P =$ 

$=$ PMF of X_1

invariant distribution

$\pi_0 =$ 

$\pi_1 = \pi_0 P =$ 

$\pi = [\,1/2 \quad 1/2\,] =$ invariant distribution

solving for invariant distribution

① set up $\pi = \pi P$

$$\pi(i) = \sum_{\text{all } j} P_{ji}\, \pi(j) = \sum_{j} \begin{array}{c}\text{probability} \\ \text{of entering} \\ \text{(i) from (j)}\end{array} \times \pi(j)$$

② $\pi(1) + \pi(2) + \ldots + \pi(m) = 1$

③ solve system of equations for $\pi(1), \pi(2), \ldots, \pi(m)$

first-step equations

to solve for property $\alpha(1)$:

① write $\alpha(1)$ in terms of $\alpha(2), \alpha(3), \ldots \alpha(m)$

② write equations for each state

③ solve system of equations for $\alpha(1)$

ex: avg. # steps to state k

① $\beta(i) = 1 + \sum_{j} P(i,j)\, \beta(j)$

② $\beta(k) = 0$

③ solve for $\beta(1)$, if starting from 1

DISC. 14 A

review: calculating π

① $\pi(1) = \sum_{i=1}^{m} P_{i1}\, \pi(i)$

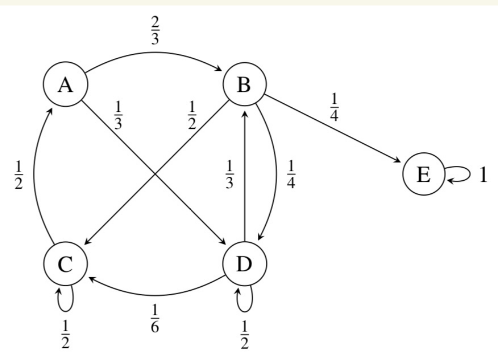
$\vdots$

(m) $\pi(m) = \sum_{i=1}^{m} P_{im}\, \pi(i)$

$\left.\begin{matrix} \\ \\ \end{matrix}\right\} \pi = \pi P$

(m+1) $\sum_{i=1}^{m} \pi(i) = 1$

sp '22 final #19



start from (A).
what is probability of reaching (E) before (C)?

4/15

week 14 Notes

- discussion today is <u>review</u> → lecture content is out of scope
- next week, discussions are drop-in OH
- fill out course evals!
- HW 14 due

DISC. 14 B

finals studying advice

what works for me, at least! ☺

1. make list of all topics
2. sort by least to most comfortable
3. for each topic:
   1. review concept until you can <u>explain</u> it to someone else.
   2. ask questions <u>on Ed</u> / <u>at OH</u>.
   3. do relevant exam/discussion problems until you <u>no longer make mistakes</u>.
4. do a full, timed practice exam.

week 14 Notes

- <u>last</u> discussion! next week, this time will be drop-in OH.
- HW 14 due on saturday.
- Fill out course evaluations → they help us a lot ♡♡