Discrete Math : Lecture 01 8.27.24

Prove. 1 is equal to 2

1. $a = b$ # given
2. $a \cdot a = a \cdot b$ # multiply by a
3. $a^2 - b^2 = ab - b^2$ # subtract b^2
4. $(a-b)(a+b) = b(a-b)$ # factoring
5. $a + b = b$ # cancel $a-b$
6. $b + b = b$ # sub a for b
7. $2b = b$

$2 = 1$

→ ERROR: cannot divide by zero!

Q: What is the minimum # of people s.t. there is a 50% chance that 2 people will have the same birthday?

- Given Uniform Distributions
- $P(A)$ = prob that people in a room share bday
- $P(A) = 1 - P(A')$ → not sharing a bday

- 1 person $\frac{365}{365} = 1$

2 people $\frac{365}{365} \cdot \frac{364}{365} = .997$ ~.3% sharing

3 people $\frac{365}{365} \cdot \frac{364}{365} \cdot \frac{363}{365}$ ~.8% sharing

⋮

23 people $\frac{365 \cdot 364 \cdot \ldots \cdot 343}{365^{23}}$ ~50.7% sharing

Q: Monty-Hall Problem: switching the doors is better!

Lecture 02:

8.29.24

Proposition: declarative statement that is either true or false

$2+2=4$ ✓ true
$2+2=5$ ✓ false
$x+4>0$ ✗ neither true or false

Proposition Variables: p, q, r, s, etc.

Compound Propositions:

Negation: $\neg$
Conjunction: $\wedge$ (and)
Disjunction: $\vee$ (or)
Implication: $\rightarrow$
Bi-conditional: $\leftrightarrow$

Negation: $\neg p$ OR $\overline{p}$ OR "not p"

p	$\neg p$
T	F
F	T

"it is not the case that p"

Ex. p: Mike can run 6-min miles
$\neg p$: It is not the case that Mike can run 6-min miles
$\neg p$: Mike cannot run 6-min miles

Conjunction: logic AND ($\wedge$)

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Ex. p: macbook has 16gb
q: macbook is 3GHz

$p \wedge q \rightarrow T$ if macbook has 16gb and 3GHz

Disjunction: logic OR ($\vee$)

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Exclusive OR: $\oplus$

"XOR"

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

Implications: conditional statement ($\to$)

"if p, then q"

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

p: "I am home. q: "it is raining"

$p \to q$: "If I am home it is reading

Ex: p: Mike learns discrete
q: Mike gets internship

$p \to q$ = if Mike learns discrete, mike gets internship

- Mike gets internship if Mike learns discrete
- Mike get internship unless Mike does not learn discrete

* lecture 2 slide goes over all the wordings *

Further Discussions:

- Proposition must have clear boolean value (T/F)
  - → its raining
  - → streets are wet
- Compound: p = its raining
  q = Hem and Brm are cats

$$p \vee q - T \text{ if } p = T \text{ or } q = T$$

- Implication: $p \to q$

→ if Brexit succeeds then Licester City will win Premier League

p → q

- Brexit failed, so Licester City won Premier League — T
- Brexit failed and Licester City lost... — T

Ex	P	Q	→
0	if its raining	then I wear rubber boots	
2	T	T	T
1	T	F	F
3	F	T	T
4	F	F	T

"nothing to prove I am a liar" so T

Ex-

P: Somebody born in Dallas
Q: Somebody who is a Texan

- P → Q: Someone born in Dallas is a Texan
- Someone born in Dallas is not a Texan
  P = T, Q = F T, F → F
- Someone not born in Dallas but is a Texan
  P = F, Q = T F, T → T
- Someone not born in Dallas is not a Texan
  P = F, Q = F F, F → T
- To be a Texan is a necessary cond for somebody to be born in Dallas
- To be born in Dallas is a sufficient cond to be a Texan

Converse, inverse, and contrapositive:

From p→q we can form new conditionals

- $q \to p$ is the converse of $p \to q$
- $\neg p \to \neg q$ is the inverse of $p \to q$
- $\neg q \to \neg p$ is the contrapositive of $p \to q$

- $p \to q \sim \neg q \to \neg p$ *
- $q \to p \sim \neg p \to \neg q$

Ex- proposition: All bats are mammals

"If $\underbrace{\text{something is a bat}}_{P}$ then $\underbrace{\text{it is a mammal}}_{Q}$"

→ identical to contrapositive: $(\neg Q \rightarrow \neg P)$

"if something is not a mammal then it is not a bat"

Inverse: $\neg P \rightarrow \neg Q$

"if something is not a bat then it is not a mammal"

→ not same as implication or contrapositive logically

ex. could be a rabbit

Converse: $Q \rightarrow P$

"if something is a mammal then it is a bat"

Ex- the $\underbrace{\text{home team wins}}_{Q}$ whenever $\underbrace{\text{it is raining}}_{P}$

contrapositive: $\neg Q \rightarrow \neg P$

inverse: $\neg P \rightarrow \neg Q$

converse: $Q \rightarrow P$

Implication: Contrapositive: Inverse: Converse:

p	q	$p \rightarrow q$	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$	q	p	$q \Rightarrow p$	$\neg p$	$\neg q$	$\neg p \Rightarrow \neg q$
T	T	T	F	F	T	T	T	T	F	F	T
T	F	F	T	F	F	F	T	T	F	T	T
F	T	T	F	T	T	T	F	F	T	F	F
F	F	T	T	T	T	F	F	T	T	T	T

Biconditionals: $p \leftrightarrow q$ "p if and only if q"

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Order of Operations:

$\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$

p: "I am home"

q: "It is raining"

$p \leftrightarrow q$: "I am home if and only if it is raining"

"p is necessary for q"

Lecture 03: 09.05.24

Homework 01 due 9.10.24 on Gradescope

Compound Proposition: new proposition made by combining one or more existing propositions

* Ways to express $p \to q$ in words slide *

* if P is false, there is no way to prove Q is T/F, so $P \to Q$ is automatically T

Bi-Conditional: $p \leftrightarrow q$ "p if and only if q"

Compound Propositions:

Order of Operations:

$\neg \to \wedge \to \vee \to \Rightarrow \to \Leftrightarrow$

Truth Tables:

rows: need a row for every combination of values for the propositions

columns:

- need a column for the compound proposition to the far right
- need a column for the truth value of each expression that occurs in the compound proposition

Ex. $p \vee q \to \neg r$

p	q	r	$p \vee q$	$\neg r$	$p \vee q \to \neg r$
T	T	T	T	F	F
T	T	F	T	T	T
T	F	T	T	F	F
T	F	F	T	T	T
F	T	T	T	F	F
F	T	F	T	T	T
F	F	T	F	F	T
F	F	F	F	T	T

6

Applications: • translate english statements into logical propositions

• logic circuits (logic design)
(AND, OR, NOT gates)
$\wedge, \vee, \neg$

Ex.

$$x = \underbrace{\overbrace{(a \text{ AND } inv(b))}^{i} \text{ OR } \overbrace{(inv(a) \text{ AND } b)}^{ii}}_{iii} \qquad y = (a \text{ AND } b)$$

a	b	i	ii	iii
0	0	0	0	0
0	1	0	1	1
1	0	1	0	1
1	1	0	0	0

a	b	y
0	0	0
0	1	0
1	0	0
1	1	1

<u>Tautology</u>: proposition which is always true
ex. $p \vee \neg p$

<u>Contradiction</u>: proposition which is always false
ex. $p \wedge \neg p$

<u>Contingency</u>: proposition that is neither a tautology or a contradiction
<u>ex.</u> p

<u>Logical Equivalence</u>:

: p and q are equivalent if $p \leftrightarrow$ is a tautology
· $p \leftrightarrow q \vee p \equiv q$

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

tautology

contradiction

Show $p \vee q \equiv \neg p \rightarrow q$

p	q	$\neg p$	q	$\neg p \rightarrow q$
T	T	F	T	T
T	F	F	F	T
F	T	T	T	T
F	F	T	F	F

Key Logical Equivalences:

Identity laws: $p \wedge T \equiv p$ $p \vee F \equiv p$

Domination laws: $p \vee T \equiv T$ $p \wedge F \equiv F$

Idempotent laws: $p \vee p \equiv p$ $p \wedge p \equiv p$

Double negation laws $\neg(\neg p) \equiv p$

Negation laws: $p \vee \neg p \equiv T$ $p \wedge \neg p \equiv F$

Commutative laws: $p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$

Associative laws ✓

Distributive ✓

Absorption $p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$

De Morgan's Laws:

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

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

* other important / useful logical equivalences slide

Ex. $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$. why?

* distribute disjunction over another disjunction

$(p \vee q) \vee (p \vee r)$

Ex. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$. why?

* distribute conjunction over disjunction

$(p \wedge q) \vee (p \wedge r)$

Ex. Is $\neg(p \vee q) \equiv \neg p \wedge \neg q$?

c Demorgan's Laws: $\neg p \wedge \neg q$ ∴ yes

Ex. $\neg(p_1 \wedge p_2 \wedge p_3 \wedge \ldots p_n)$

$\neg p_1 \vee \neg p_2 \vee \neg p_3 \ldots p_n$ DeMorgan Laws

Ex. Show $(p \wedge q) \Rightarrow (p \wedge q)$ is a ~~tautology~~?
→ Always True

$(p \wedge q) \Rightarrow (p \wedge q)$

$A \Rightarrow B \equiv \neg A \vee B$

Unfinished

DeMorgans Law

A	B	$\neg A$	$A \Rightarrow B$	$\neg A \vee B$
F	F	T	T	T
F	T	T	T	T
T	F	F	F	F
T	T	F	T	T

<u>Propositional Satisfiability</u>: a compound prop is satisfiable if there is an assignment of truth values to its variables that make it true

NP-Complete (SAT problem)

<u>Ex</u>. $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$

satisfiable. assign T to p, q, r

Ex. $(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$

satisfiable. assign T to p and F to q

Ex. $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$

<u>not</u> satisfiable

<u>Notation</u>:

$\bigvee_{j=1}^{n} p_j \equiv p_1 \vee p_2 \vee \dots \vee p_n$

$\bigwedge_{j=1}^{n} p_j \equiv p_1 \wedge p_2 \wedge \dots \wedge p_n$

SAT Problem:

<u>Ex</u>.
```
function MAX(a, b)
    if a ≥ b then
        return a
    else
        return b
    end if
end function
```

<u>Variables</u>:

r_is_A # returned value is input A

r_is_A ⟺ $(a \geq b)$

r_is_B # returned value is input B

r_is_B ⟺ $(a < b)$

<u>Correctness Conditions</u>:

$(r\_is\_A \rightarrow ((a \geq b \wedge (\underset{T}{a \geq a}))) \wedge (r\_is\_B \rightarrow (b \geq a) \wedge (\underset{T}{b \geq b}))$

$(r\_is\_A \rightarrow a \geq b) \wedge (r\_is\_B \rightarrow b \geq a)$.

Test -

Apply Negation

$\neg((r\text{-is-}A \Rightarrow a \geq b) \wedge (r\text{-is-}B \Rightarrow b \geq a))$

$\equiv$

$((r\text{-is-}A) \wedge (a < b)) \vee ((r\text{-is-}B \wedge (b < a))$

$a = 17,\ b = 24 \quad r\text{-is-}B = T \quad r\text{-is-}A = F$

$(F \wedge T) \vee (T \wedge F)$

$F \vee F \equiv F$ ✓

what if $r\text{-is-}B = T$ and $r\text{-is-}A = T$

$(T \wedge T) \vee (T \wedge F) \equiv T$ ✗

Quantifiers:

Application: Natural Language Processing (NLP)

Ex. How was the party after I left? Great! Everyone had a drink.

$\forall$ people p at the party, $\exists$ a drink p had

Ex. propositional logic is not enough

All men are mortal
Socrates is a man

Predicate Logic:

Variables: x, y, z
Predicates: P, M
Quantifiers: $\forall, \exists$

propositional functions:
$P(x), M(y)$
* can have ~~definitive~~ truth values

Ex.

$x > 3$ NOT a proposition
$x = y + 3$ NOT a proposition

instead: $P(x)$: $x > 3$ P: predicate: greater than 3
x: variable

↳ propositional function

Ex. Let $x + y = z$ be $R(x, y, z)$

$R(2, -1, 5)$ F
$R(3, 4, 7)$ T

* works with english phrases as well

Lecture 04 : 09.04.24

- Predicates
- Variables
- Quantifiers → Universal, Existential
- Majority Quantifiers → De Morgan's Laws
- Translating English to Logic (Applications)

Predicate : P, M, ...
Variables : x, y, z, ...
→ P(x), M(y) ...

* can use all logic / compound symbols from before

Quantifiers : are used to express English words like "all" & "some"

Universal Quantifier : "For all" symbol : ∀

Existential Quantifier : "There exists" symbol : ∃

ex. $\forall x P(x)$ and $\exists x P(x)$

↳ P(x) true for all x in domain
P(x) true for some x in domain

Q. How to create a proposition from a propositional function?

A. Assign a value to variable in propositional function

eg → $P(x): x < 7$; $P(1)$: T $P(10)$: F

B. Use quantifiers : Express extent to which predicate is true

→ Universal : ∀ - "for all"

→ existential : ∃ there is one or more element that makes function true

Domain : Always must specify
Indicates possible values of vars

Universal Quantifiers: $\forall x$

- $P(x)$ for all values x in the domain // $\forall x P(x)$ //

ex- $p(x) = x+1 > 1$ | domain: all positive real #'s

$\forall x P(x) = \text{True}$

ex- $P(x) = x^2 > 0$, domain: all integers

$\forall x P(x) = \text{False}$: b/c $P(0) < 0$

$\forall x P(x)$: n elements in domain:

$P(x_1) \wedge P(x_2) \wedge P(x_3) \wedge \ldots \wedge P(x_n) \equiv \forall x P(x)$

More About Domain:

$\forall x (x^2 \geq x)$

a) Domain is all real #'s

b) Domain is all integers

a) $x = \frac{1}{2} \Rightarrow (\frac{1}{2})^2 > \frac{1}{2} \sim \frac{1}{4} > \frac{1}{2}$ FALSE

b) $x = -2 \Rightarrow (-2)^2 \geq -2$ TRUE

Existential Quantifiers: $\exists x$

$\exists x P(x) \sim$ there is an x in our domain where $P(x) = T$

ex. $P(x): x > 3$ | domain is all real #'s

$P(4)$ - True

$\exists x Q(x)$: domain is n elements:

$Q(x_1) \vee Q(x_2) \vee \ldots \vee Q(x_n) \equiv \exists x Q(x)$

Truth values of $\exists x P(x)$ $\forall x P(x)$ - domain empty?

$\forall x P(x) = \text{TRUE}$ $\exists x P(x) = \text{FALSE}$

Uniqueness Quantifier:

- $\exists! x P(x)$: $P(x)$ is true for one and only one x in the domain

Ex. $P(x): x+1=0$ | domain is integers

$\exists! x P(x) = \text{TRUE}$

$\exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x))$

Restricted Domains:

$\boxed{\forall x < 0}\ (x^2 > 0)$: $U \in \mathbb{R}$ → domain

- $\forall x \in \mathbb{R} \Rightarrow x < 0, x^2 > 0$
- if $x < 0$, then $x^2 > 0$
  implies this language

→ $\forall x((x < 0) \rightarrow (x^2 > 0))$ write as implication

* Restriction of universal quantifier is the same of universal quantifier of a conditional statement (implies implication)

Ex- $\exists z > 0 (z^2 = 2) \equiv \exists (z > 0 \wedge z^2 = 2)$: $U \in \mathbb{R}$

CANNOT write the above as follows:

$\neq \exists z (z > 0 \rightarrow z^2 = 2)$ since this is true if $z \leq 0$

would be false: $F \rightarrow T$
$F \rightarrow F \rightarrow T$

Ex. Proposition: All lobsters go to heaven ~ implication

→ For every x if x is a lobster, then x goes to heaven

NOT: For every x (where x is a lobster) AND x goes to heaven
conjunction

* since if $F \rightarrow T \rightarrow F$ cannot interchangeably
$F \rightarrow F \rightarrow F$
use $\wedge$ and $\rightarrow$ in restricted domains even though language makes sense

Precedence of Quantifiers:

$\forall$ and $\exists$ have higher precedence than all logical operators

$\forall x P(x) \vee Q(x) \equiv (\forall x P(x)) \vee Q(x)$

$\forall x P(x) \vee Q(x) \not\equiv \forall x (P(x) \vee Q(x))$

Bound vs Free Vars:

Ex. $\exists x P(x,y)$ → x is bound, y is free

Ex. $\forall x\,[\exists y P(x,y) \vee Q(x,y)]$

- x, y are bound in $P(x,y)$
- y in $Q(x,y)$ is free
- scope of $\exists y$ is $P(x,y)$
- scope of $\forall x$ is $[\exists y P(x,y) \vee Q(x,y)]$

Bound Var: quantifier used on variable

Scope: part of logical expression where quantifiers applied

Equivalences in Predicate Logic:

$S \equiv T$ implies S and T has same truth value

ex: $\forall x \neg\neg S(x) \equiv \forall x S(x)$

Finite vs. Infinite Domain:

$\forall x P(x) : U \in [1,2,3] \equiv P(1) \wedge P(2) \wedge P(3)$

$\exists x P(x) : U \in [1,2,3] \equiv P(1) \vee P(2) \vee P(3)$

$\forall x P(x) : U \in \mathbb{R} \equiv P(1) \wedge P(2) \wedge \ldots$

$\exists x P(x) : U \in \mathbb{R} \equiv P(1) \vee P(2) \vee \ldots$

Negating Quantifiers:

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

De Morgan's Law:

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

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

Ex. what are the negations of $\forall x (x^2 > x)$ and $\exists x (x^2 = 2)$

$\neg(\forall x (x^2 > x)) \equiv \exists x (x^2 < x)$

$\neg(\exists x (x^2 = 2)) \equiv \forall x (x^2 \neq 2)$

Ex. Is $\neg(p \vee (\neg p \wedge q)) \equiv \neg p \wedge \neg q$?

1. $\neg p \wedge \neg(\neg p \wedge q)$ DeMorgan's Law
2. $\neg p \wedge (p \vee \neg q)$ DeMorgan's Law
3. $(\neg p \wedge p) \vee (\neg p \wedge \neg q)$ Distributive
4. FALSE $\vee \neg p \wedge \neg q$ Identity
5. $\neg p \wedge \neg q \equiv \neg p \wedge \neg q$ ✓

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

1. $\neg(p \wedge q) \vee (p \wedge q)$ identity $A \rightarrow B \sim \neg A \vee B$
2. $(\neg p \vee \neg q) \vee (p \wedge q)$ DeMorgan's Law
3. $((\neg p \vee \neg q) \vee p) \wedge ((\neg p \vee \neg q) \vee q)$ distributive
4. $(\neg p \vee \neg q \vee p) \wedge (\neg p \vee \neg q \vee q)$ associative
5. $(\neg p \vee p \vee \neg q) \wedge (\neg p \vee \neg q \vee q)$ reorder terms
6. $(T \vee \neg q) \wedge (\neg p \vee \neg q \vee q)$ negation law
7. $(T \vee \neg q) \wedge (\neg p \vee T)$ negation law
8. $T \wedge T$ so always true

Translation from English to Logic:

1. All lions are fierce
2. Some lions do not drink coffee
3. Some fierce creatures do not drink coffee

def $P(x)$, $Q(x)$, and $R(x)$ as x is a lion, x is fierce, and x drinks coffee

1. $\forall x (P(x) \rightarrow Q(x))$
2. $\exists x (P(x) \wedge \neg R(x))$
3. $\exists x (Q(x) \wedge \neg R(x))$

Ex. Why can't $\exists x (P(x) \wedge \neg R(x)) \equiv \exists x (P(x) \rightarrow \neg R(x))$

explicitly confirms x has to be a lion

x doesn't even have to be a lion for this to be true

Ex. Some student in this class have watched lecture videos on Panopto

$V(x)$: x has watched videos on Panopto

A: $U_1 \in$ all students in class

B: $U_2 \in$ all people

A. $\exists x V(x)$

B. $C(x) = x$ is a student in this class:

$\exists x (C(x) \wedge V(x))$

Lecture Notes 3 9.10.24

Remember that the restriction of a universal quantifier can be interpreted as the universal quantification of a conditional statement.

Ex. Express "All Hamsters are Awesome"

a) $U \in$ All breeds of hamsters

$H(x) = x$ is awesome

$\Rightarrow \forall x H(x)$

b) $U \in$ "All animals"

$D(x) = x$ is a Hamster

$H(x) = x$ is awesome

$\Rightarrow \forall x (D(x) \rightarrow H(x))$

Let $x =$ white hamsters

$D(x) = T$

$H(x) = T$ $T \rightarrow T = T$ ✓

Let $x =$ rabbit. Express "All Rabbits are Awesome"

$\Rightarrow \forall x (D(x) \rightarrow H(x))$

$D(x) = F$

$H(x) = T$ $F \rightarrow T = T$ ✓

Ex. Why can't we say $\forall x [D(x) \wedge H(x)]$?

$x =$ rabbit; $D(x) = x$ is a hamster

$H(x) = x$ is awesome

$\forall x [D(x) \wedge H(x)]$

$D(x) = F \longrightarrow F \wedge T = F$ ✗

Ex. Express "Some Animals are colorblind"

Let $A(x): x$ is animal & $U \in$ All creatures

$C(x): x$ is color blind

$\Rightarrow \exists x [A(x) \wedge C(x)]$

Let $x =$ goldfish

$A(x) = T$

$C(x) = F$

$T \wedge F = F$ ✓

Let $x =$ dog

$A(x) = T$

$C(x) = T$

$T \wedge T = T$ ✓

CANNOT use $\exists x\,[A(x) \to C(x)]$

Let x not be an animal

$A(x) = F$ $\quad F \to T/F = T$ ✗

$C(x) = T/F$

Ex.

$P(x)$: x is a lion

$Q(x)$: x is fierce

$R(x)$: x drinks coffee

$U \in$ all creatures

- All lions are fierce: $\forall x\,[P(x) \to Q(x)]$ ✓
  - → restricting domain to lions
- Some lions do not drink coffee:

  $\exists x\,[P(x) \land \neg R(x)]$ ✓

  $\exists x\,[P(x) \to \neg R(x)]$ ✗

  ← true even if x is not a lion

Ex. Express "There exists a meal x, such that if x is lunch, then x is not free"

$U \in$ all meals

$L(x)$: x is lunch $\quad \Rightarrow \exists x\,[L(x) \land \neg F(x)]$ ✓

$F(x)$: x is free

* Helps for system rules / logic *

→ predicates can have more than 1 var

→ can use multiple quantifiers in a statement

Nested Quantifiers

Ex. "Every real number has an inverse"

$\forall x \exists y (x + y = 0)$; $U \in \mathbb{R}$

** Quantification of two variables don't ...

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

$\forall y \forall x P(x, y)$ ...

nested for-loops

Think Nested Loops:

$\forall x \forall y P(x, y) \equiv$ For(x)
| For(y)
| | $P(x, y) = T$ for all x, y

$\forall x \exists y P(x, y) \equiv$ For(x)
| For(y)
| | $P(x, y) = T$ for $\exists$ y and all x

Order of Quantifiers:

Ex. Let $P(x, y) = x + y = y + x$

→ order does not matter

Ex. For every real number there is a number larger than it

$\forall x \exists y : y > x \Rightarrow T$ ✓

whats the difference b/w $\forall x \exists y$ vs. $\exists y \forall x$?

$\underbrace{\exists y \forall x}$: $y > x \Rightarrow F$ ✗

"there exists a y that is greater than all x"

Ex. $\forall x \forall y P(x, y) \equiv \forall y \forall x P(x, y)$

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

$Q(x, y) : x + y = 0$

$\exists y \forall x Q(x, y) = F$

$\forall x \exists y Q(x, y) = T$

Ex. For every real number x, if $x \neq 0$, there exists a real ~~x~~ y such that $xy = 1$

$\forall x[(x \neq 0) \rightarrow \exists y(xy = 1)]$

Ex. Everyone has exactly one best friend

Let $B(x,y)$: y is the best friend of x

$U \in$ all people

$\Rightarrow \forall x \exists! y \, B(x,y)$

Without Uniqueness Quantifier

Let z ...

$\Rightarrow \forall x \exists y [B(x,y) \land \forall z[(z \neq y) \rightarrow \neg B(x,z)]]$

Ex. There are 0 students who are Raiders fans

NOT a proposition, actually a tautology

$\exists x(x = x)$ $\forall x(x = x)$

Ex. There is at least 1 student who is a Bears fan

$\exists x B(x)$: $B(x)$ = student x who likes the Bears

Ex. There are at least 2 students who are Bears fans

I can find a student x and a student y and $x \neq y$ and both like the Bears

$B(x)$ = student x likes Bears

$\Rightarrow \exists x \exists y [(x \neq y) \land (B(x) \land B(y))]$

Ex. There are at most 0 students who are Raiders fan

$R(x)$ = x is a Raiders fan

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

Ex. There is at most one student that likes the Bears

* CANNOT directly express "at most"

$B(x)$: student x likes the Bears

$\forall x \forall y [\underbrace{(x \neq y)}_{\text{if } T} \rightarrow \underbrace{\neg(B(x) \land B(y))}_{\text{one has to be } F;\ T \rightarrow T \equiv T}]$

Remember: $A \to B \equiv \neg A \vee B$

$\therefore (x \neq y) \to \neg(B(x) \wedge B(y))$

$\Rightarrow \neg(x \neq y) \vee \neg(B(x) \wedge B(y))$

$\Rightarrow \forall x \forall y \left[(x = y) \vee \neg(B(x) \wedge B(y)) \right]$

$\equiv \forall x \forall y \left[(x \neq y) \to \neg(B(x) \wedge B(y)) \right]$

Ex: Translate into English -

- $\forall x \left[C(x) \vee \exists y (C(x) \wedge F(x, y)) \right]$

$C(x)$: x has a computer
$F(x,y)$: x and y are friends
$U_{x,y} \in$ all students at your university

"Every student at my university has a computer or has a friend that has a computer"

Ex: Let $F(x,y)$ be "x can fool y"
$U_{x,y} \in$ all people in the world

1. Everybody can fool Fred
$\forall x \, F(x, \text{Fred})$

2. There is nobody that can fool everybody
$\neg(\exists x \forall y \, F(x,y)) \equiv \forall x \exists y \neg F(x,y)$

3. Everybody can be fooled by somebody
$\forall y \exists x \, F(x,y)$

4. Tim can fool exactly two people
$\exists x \exists y \left[(x \neq y) \wedge [F(\text{Tim}, x) \wedge F(\text{Tim}, y)] \right]$

Lecture Notes: 9.12.24

Quiz 01: 9.19.24 (cover HW1)

- converse, inverse, implication, contrapositive
- equivalence proofs
- logical expressions ↔ english

* can use a table of information (a les created in next lectures slides *

Ex. Tim can fool exactly two people

Ex. There are at least 2 distinct people Tim can fool

$\exists x \exists y [(x \neq y) \wedge F(Tim, x) \wedge F(Tim, y)]$

* this is actually what we solved last class

Ex. Tim can fool exactly two people:

$\exists x \exists y [(x \neq y) \wedge F(Tim, x) \wedge F(Tim, y) \wedge$
$\forall z (F(Tim, z) \rightarrow (z = x \vee z = y))]$

Ex. $\neg(\forall x \exists y (xy = 1))$ $(x = 0)$

It is not the case, that for all values of x, there exists a y such that $xy = 1$ $(x = 0)$

$\equiv \exists x \neg \exists y (xy = 1) \equiv \exists x \forall y \neg (xy = 1)$

$\equiv \exists x \forall y (xy \neq 1)$

There exists an x for all y, where $xy \neq 1$ $(x = 0)$

Ex. $\neg \forall x (\exists y \forall z P(x,y,z) \wedge \exists z \forall y P(x,y,z))$

$\exists x \neg (\exists y \forall z P(x,y,z) \wedge \exists z \forall y P(x,y,z))$

$\exists x (\neg \exists y \forall z P(x,y,z) \vee \neg \exists z \forall y P(x,y,z))$

$\exists x (\forall y \neg \forall z P(x,y,z) \vee \forall z \neg \forall y P(x,y,z))$

$\exists x (\forall y \exists z \neg P(x,y,z) \vee \forall z \exists y \neg P(x,y,z))$

Ex.1 Everyone experiences some moments of doubt

Ex.2 I know someone who has never experienced a moment of doubt

$D(p,t)$ p = people t = time

1 = $\forall p \exists t\, D(p,t)$

2 = $\exists p \forall t\, \neg D(p,t)$

Logic and Proofs:

The Argument: we can express premises (above the line) and the conclusion (below the line) in predicate logic and arguments

$$\forall x (Man(x) \Rightarrow Mortal(x))$$
$$Man(Socrates)$$
$$\overline{\therefore Mortal(Socrates)}$$

Proofs: valid argument that establishes truth of mathematical statements

Argument: premise: sequence of statements
conclusion: last statement

Valid Argument: premise implies conclusion

$\bigwedge_{i=1}^{n} p_i \rightarrow q$ (which is true) becomes a tautology

Ex. 1. if you have a current password, you can log into the network

2. You have a current password

3. Therefore, you can log into the network

Argument Form:
$$p \rightarrow q$$
$$p \quad \leftarrow \text{p is TRUE}$$
$$\overline{\therefore q}$$

p, q are propositional variables —

$((p \rightarrow q) \wedge p) \rightarrow q \leftarrow$ T in all cases (tautology)

Ex How do we know this argument is valid

$((p \to q) \land p) \to q$

p	q	$p \to q$	$p \land (p \to q)$	q	$((p \to q) \land p) \to q$
T	T	T	T	T	T
T	F	F	F	F	T
F	T	T	F	T	T
F	F	T	F	F	T

tautology

OB:

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore p \end{array}$$

Modus Ponens
rule of inference

* if one of the argument premises is F, we cannot conclude the conclusion is T, even if the argument is valid

Ex

- If $\underbrace{\sqrt{2} > \frac{3}{2}}_{F}$ then $\underbrace{(\sqrt{2})^2 > \left(\frac{3}{2}\right)^2}_{F}$

$p: \sqrt{2} > \frac{3}{2}$ $\quad q: (\sqrt{2})^2 > \left(\frac{3}{2}\right)^2$

premise: $\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$ valid argument b/c in Modus Ponens form

→ Premise is F so cannot conclude conclusion is T!

P is false

$((p \to q) \land p) \to q$

* Modus Ponens form only allows us to infer q if we know p is T and $p \to q$ is T

↳ assume truth of p leads to truth of q

Ex: If today is Tuesday, I will go to CSE 2010
Today is Tuesday

∴ I will go to CSE 2010

Rules of Inference:

* table of all of these in notebook

Modus Ponens:

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array} \sim ((p \to q) \land p) \to q$$

Modus Tollens: derived from contrapositive

$$\begin{array}{l} p \to q \\ \neg q \\ \hline \therefore \neg p \end{array} \sim (\neg q \land (p \to q)) \to \neg p$$

Hypothetical Syllogism:

$$\begin{array}{l} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array} \sim ((p \to q) \land (q \to r)) \to (p \to r)$$

Disjunctive Syllogism:

$$\begin{array}{l} p \lor q \\ \neg p \\ \hline \therefore q \end{array} \sim (\neg p \land (p \lor q)) \to q$$

Addition:

$$\begin{array}{l} p \\ \hline \therefore p \lor q \end{array} \sim p \to (p \lor q)$$

Simplification:

$$\begin{array}{l} p \land q \\ \hline \therefore q \end{array} \sim (p \land q) \to p$$

Conjunction:

$$\begin{array}{l} p \\ q \\ \hline \therefore p \land q \end{array} \sim (p \land q) \to p \land q$$

Resolution:

$$\begin{array}{l} \neg p \lor r \\ p \lor q \\ \hline \therefore q \lor r \end{array} \quad ((\neg p \lor r) \land \ldots$$

* All of these are in table format and given on quizzes

24

Ex. If "pigs are pink" is T, then "pigs are pink or gray" is also true: p ... q

Rule: addition:
$$\frac{p}{\therefore p \lor q}$$

Ex. If "cats meow and hiss" is true, then "cats meow" is also true

Rule: Simplification:
$$\frac{p \land q}{\therefore p}$$

Ex. "If I am happy, then I smile" T
"I am happy" T
then "I smile" also T

Rule: Modus Ponens:
$$\frac{\begin{array}{l} p \to q \\ p \end{array}}{\therefore q}$$

Ex. "If I am happy, then I smile" T
"I am not happy" T
then "I am not happy" also T

Rule: Modus Tollens:
$$\frac{\begin{array}{l} p \to q \\ \neg q \end{array}}{\therefore \neg p}$$

Ex. If "it is sunny or rainy" is T and it is not sunny, it must be rainy

Rule: disjunctive syllogism
$$\frac{\begin{array}{l} p \lor q \\ \neg p \end{array}}{\therefore q}$$

Using Rules of Inference to Craft Valid Arguments:

Form:
$$\frac{\begin{array}{c} S_1 \\ S_2 \\ S_3 \\ \vdots \\ S_n \end{array}}{\therefore C}$$

Ex.
$$\frac{\begin{array}{l} \neg p \land q \\ r \to p \\ \neg r \to s \\ s \to t \end{array}}{\therefore t}$$

context on slides #x

$\neg p \land q$	premise
$\neg p$	(1)
$r \to p$	premise
$\neg r$	(2)
$\neg r \to s$	premise
s	(4)
$s \to t$	premise
$\therefore t$	

Ex - Assume the following are T, Prove r.

- $p \vee q$
- $\neg p \vee r$
- $\neg q \vee r$

step	statement	reason
1.	$p \vee q$	given
2.	$\neg p \vee r$	given
3.	$q \vee r$	resolution on lines 1, 2
4.	$\neg q \vee r$	given
5.	r	resolution on lines 3, 4

Ex Assume the following are T. Prove r

- $p \vee q$
- $p \to r$
- $q \to r$

step	statement	reason
1.	$p \vee q$	given
2.	$p \to r$	given
3.	$\neg p \vee r$	Logical equivalence on line 2
4.	$q \vee r$	resolution of lines 1, 3
5.	$q \to r$	given
6.	$\neg q \vee r$	Logical equivalence line 5
7.	r	resolution of lines 4, 6

Ex- Show that $\underbrace{((p \wedge q) \vee r)}$ and $\underbrace{r \to s}$ implies $p \vee s$

assume T

1. $(p \wedge q) \vee r$ — given
2. $(p \vee r) \wedge (q \vee r)$ — distributive law
3. $(p \vee r)$ — simplification
4. $r \to s$ — given
5. $\neg r \vee s$ — logical equivalence L.4
6. $p \vee s$ — resolution L. 3, 5

Lecture Notes:

9.17.24

Ex. given the following premises

- p
- $p \to q$
- $\neg q \vee r$
- $s \to \neg r$
- prove $\neg s$

step	statement	reason
1.	$p \to q$	given
2.	p	given
3.	q	modus ponens
4.	$\neg q \vee r$	given
5.	r	disjunctive syllogism
6.	$s \to \neg r$	given
7.	$\neg s \vee \neg r$	logical equivalent
8.	$\neg s$	disjunctive syllogism

Common Fallacies:

1. Fallacy Affirming Conclusion

Ex. if you do every problem in a book (p) then you'll learn discrete math (q)

$$\begin{array}{l} p \to q \\ \underline{q} \\ \therefore p \end{array}$$

I learned discrete math therefore I did every problem in the book

$((p \to q) \wedge q) \to p$ NOT a tautology

$((F \to T) \wedge T) \to F$

$(T \wedge T) \to F$ (F)

2. Fallacy of Denying the Hypothesis

$((p \to q) \wedge \neg p) \to \neg q$ NOT a tautology

p: it is raining
q: the ground is wet

Exs.

1. $\begin{array}{l} p \to q \\ \underline{\neg p} \\ \therefore \neg q \end{array}$ denying hypothesis

2. $\begin{array}{l} p \to q \\ \underline{\neg q} \\ \therefore \neg p \end{array}$ Modus Tollens

3. $\begin{array}{l} p \to q \\ \underline{p} \\ \therefore q \end{array}$ Modus Ponens

4. $\begin{array}{l} p \to q \\ \underline{q} \\ \therefore p \end{array}$ affirming conclusion

Handling Quantified Statements: sequence of statements

* 4 rules of inference for quantified expressions in slides/table

1. Unified instantiation:

$\forall x (P(x) \to Q(x)) \Rightarrow P(c) \to Q(c)$

2. Universal Generalization:

$\forall c \in U\, P(c) \Rightarrow \forall x P(x)$

3. Existential Instantiation:

$\exists x P(x) \Rightarrow \exists c \in U\, P(c)$

4. Existential Generalization:

$c \in U\, P(c) \Rightarrow \exists x P(x)$

Exs

1. UI: "All cats go to heaven" $\forall x P(x)$

Hemmingway is a cat

$$\frac{\forall x P(x)}{\therefore P(c) \text{ is T}}$$

2. UG: $\frac{P(c) \text{ for arbitrary } c}{\therefore \forall x P(x)}$

$\forall x \in \mathbb{R},\ x^2 > 0$

3. EI: $\frac{\exists x P(x)}{\therefore P(c)\ \exists c}$ There is somebody who got an A ∴ person x got an A

4. EG: $\frac{P(c) \text{ for particular } c}{\therefore \exists x P(x)}$

"Amy got A in the class"

∴ Somebody got an A in the class

Ex:

- Everyone in this class has taken a CS course. Alex is a student in this class. Alex has taken a CS course

  - $C(x)$: x is in this class
  - $S(x)$: x has taken a CS course
  - $U \in$ all people

premise: $\forall x (C(x) \to S(x))$ • $C(\text{Alex})$

conclusion: $S(\text{Alex})$

Prove $S(\text{Alex})$ OR craft argument:

Step	Statement	Reason
1.	$\forall x (C(x) \to S(x))$	given
2.	$C(\text{Alex}) \to S(\text{Alex})$	UG
3.	$C(\text{Alex})$	given
4.	$S(\text{Alex})$	Modus ponens

Ex:

... love ...

- $P(x)$: x is a runner in the Olympics
- $Q(x)$: x has participated in NCAA
- $R(x)$: x has won a race
- $U \in$ all runners

$$\exists x (P(x) \land \neg Q(x))$$
$$\bullet \quad \forall x (P(x) \to R(x))$$
$$\overline{\exists x (R(x) \land \neg Q(x))}$$

Step	Statement	Reason
1.	$\exists x (P(x) \land \neg Q(x))$	given
2.	$P(a) \land \neg Q(a)$	EI
3.	$P(a)$	simplification
4.	$\forall x (P(x) \to R(x))$	given
5.	$P(a) \to R(a)$	UI
6.	$R(a)$	Modus Ponens L. 3,5
7.	$\neg Q(a)$	simplification L. 2
8.	$R(a) \land \neg Q(a)$	conjunction
9.	$\exists x (R(x) \land \neg Q(x))$	EG

Ex: ... love ...

$$\underbrace{\forall x(S(x)\to C(x))}_{\text{every student likes crossword puzzles}} \wedge \underbrace{\exists x(S(x)\wedge I(x))}_{\text{some students like ice cream}} \to \underbrace{\exists x(S(x)\wedge C(x)\wedge I(x))}_{\text{there exists a student that likes crossword puzzles and ice cream}}$$

Step	Statement	reason
1.	$\forall x(S(x)\to C(x))$	premise
2.	$\exists x(S(x)\wedge I(x))$	premise
3.	$S(a)\wedge I(a)$	EI
4.	$S(a)\to C(a)$	UI

* be careful when using the same a in these sometimes will have to use a and b

Step	Statement	reason
5.	$C(a)$	Modus Ponens
6.	$S(a)\wedge I(a)\wedge C(a)$	Addition
7.	$\exists x(S(x)\wedge I(x)\wedge C(x))$	EG

Proofs of Mathematical Statements

proof: valid argument establishing truth of statement

Theorem: statement that can be shown to be true

- definitions
- other theorems
- axioms
- rules of inference

Conjecture: statement we are proposing to be true

- can be proven T / F

Forms: $\forall x \in U$ commonly omitted

$\forall x(P(x)\to Q(x))$

0

Ex- Direct proof : $p \to q$

If n is an odd integer, n^2 is odd

1- define : even integer as $2k$
odd integer as $2k+1$

prove : if n is an odd integer, n^2 is odd

assume : n is odd... (direct proof)

then $n = 2k+1$

$\Rightarrow n^2 = (2k+1)^2 = 4k^2+4k+1$

$\Rightarrow 2(2k^2+2k)+1$

Let $q = 2k^2+2k$

$\Rightarrow 2q+1 \Leftarrow$ odd

if n is odd, n^2 is odd

$\therefore \forall x$ (if n is odd $\Rightarrow x^2$ is odd)

Ex-

- $r \in \mathbb{R}$ is rational if integers p & q $(q \neq 0)$ such that $r = p/q$
- prove the sum of 2 rational numbers is rational

$r = \frac{p}{q}$, $s = \frac{t}{u}$ $\quad u \neq 0, q \neq 0$

$r+s = \frac{p}{q} + \frac{t}{u} = \frac{pu+tq}{qu}$

Let $v = pu+qt$
$w = qu$ $\Rightarrow \frac{v}{w}$

Lecture Notes: 9.19.24

Ex. int m, n
if m, n are perfect squares
then $m \cdot n$ is also a perfect sq

$m = s^2$
$n = t^2$
$m \cdot n = (s^2 t^2) = (st)^2 = y^2$
direct proof $y = st$

Thm. contraposition (proof by contraposition)
$p \to q \equiv \neg q \to \neg p$

Ex. for int n
if $\underbrace{n^2 \text{ is odd}}_{p}$ then $\underbrace{n \text{ is odd}}_{q}$ $p \to q$

By contraposition:
- Assume $\neg q$: n is even
$(n^2) = (2k)^2 = 4k^2 = 2(2k^2) = 2y$ $(\neg p)$
$y = 2k^2$

Ex. if n is an int and $\underbrace{3n+2 \text{ is odd}}_{p}$, then $\underbrace{n \text{ is odd}}_{q}$

- assume $\neg q$: n is even: $n = 2k$
$3(2k) + 2 = 6k + 2 = 2(3k+1) = 2y$: $\neg p$
$y = 3k+1$
$\neg q \to \neg p \therefore p \to q$

Proof by Contradiction:

to prove p, assume $\neg p$ and derive a contradiction
such as $p \land \neg p$
(indirect form of proofs)

Ex: prove $\sqrt{2}$ is irrational
(this is "famous")

proof by contradiction:

- assume $\sqrt{2}$ is rational
- 2 integers a, b: $b \neq 0$; $\underbrace{\gcd(a,b) = 1}$
- $\sqrt{2} = \frac{a}{b}$ (suggests $\sqrt{2}$ is rational) ⚠ fraction is in simplest form
- $\sqrt{2} = \frac{a}{b} \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow \underbrace{a^2 = 2b^2}$

→ suggests that: a^2 is even — $k = b^2 \sim 2k$

- can also say a is even: $[(2k)^2 = 4k^2 = 2(2k^2)]$

Rewrite: $\left.\begin{array}{l} a^2 = 2b^2 \\ a = 2k \end{array}\right\} \Rightarrow 2b^2 = (2k)^2$

$\Rightarrow 2b^2 = 4k^2 \Rightarrow b^2 = 2k^2$ (implies b^2 is an even #)

∴ b is also an even #

Contradiction: a is even # / b is even # | $\gcd(a,b) = 1$ not true

if a, b both even, $\gcd(a,b) \neq 1$ (lowest is 2)

Contradicts Assumption $\sqrt{2}$ is rational
assumption = F

Another Perspective:

$p \to q$ | p is hypothesis: $\sqrt{2}$ is a #
| q is conclusion: $\sqrt{2}$ is rational

Proof by Contradiction:

p: $\sqrt{2}$ is a rational #
q: $\sqrt{2}$ can be expressed as $\frac{a}{b}$ | $\gcd(a,b)=1$, $b \neq 0$

→ try to prove $\sqrt{2}$ is irrational by negating p

Contradiction:

Assume $\sqrt{2}$ is rational implies $\sqrt{2} = \frac{a}{b}$ ($\gcd(a,b)=1$)
- Work on previous page suggests: $\neg q$

Implies that p is F ($\neg p$ must be T)

Theorems that are Biconditional:

to show $p \leftrightarrow q$, must prove
$p \to q \land q \to p$

- * Proof by cases
- * Exhaustive proofs
- * Without Loss of Generality
- * Uniqueness proofs

In Slides

Lecture Notes:

Proof by Cases:

$m = 2k, 2k+1 >$ cases

Ex.
- Assume m is an integer. Show $2m^2 - 1$ is odd
- i.e. show that $2m^2 - 1 = 2k+1$ for some int k

Cases.

1. m is an even int:
$2(2k)^2 - 1 \Rightarrow 8k^2 - 1 \Rightarrow 8k^2 - 1 - 1 + 1$
$\Rightarrow 2(\underbrace{4k^2 - 1}_{4}) + 1 \Rightarrow 24 + 1 \therefore 2m^2 - 1$ is odd

k can also represent an odd integer as $2k-1$

2 - m is an odd integer
$2(2k+1)^2 - 1 \Rightarrow 2(4k^2 + 4k + 1) - 1$
$\Rightarrow 8k^2 + 8k + 2 - 1 \Rightarrow 8k^2 + 8k + 1$
$\Rightarrow 2(4k^2 + 4k) + 1 \Rightarrow 24 + 1 \therefore 2m^2 - 1$ is odd

Proof by Exhaustion:

Ex.
- Prove: if the name of a month has 5 or more characters, then a 4-letter word can be formed using those characters

$\exists$ January: Jury
February: Ruby
March: Arch
⋮
May: N/A
⋮

Without Loss of Generality:

Ex. x & y are integers

if (xy) and $(x+y)$ are even, then x, y are even

Proof by Contradiction:

p: x, y are integers AND (xy) & $(x+y)$ are even

q: x, y are even integers

$p \rightarrow q$

$\Rightarrow \neg q \rightarrow \neg p$ (to do so, show 1 int is odd)

- Assume x is odd : $2k$
- Assume y is even : $2m+1$

$\Rightarrow x+y = 2k+2m+1 \Rightarrow 2(k+m)+1$

$\Rightarrow a = \cancel{k+m} \Rightarrow 2m+1$. contradiction

- $y = \text{odd} = 2n+1$
- $x = 2m+1$

$\Rightarrow (2m+1)(2n+1) = 2(2mn+2m+2n)+1$

$q = 2mn+2m+2 \Rightarrow 2q+1$. contradiction

Proof by Cases:

to prove: $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$

Use tautology

$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow$ ——

slides

* Proof by Exhaustion
* Without Loss of Generality

Proof Strategies:

1. If statement is conditional
   - → try a direct proof
   - → try proof by contraposition
   - → try ... contradiction
2. If statement is disjunction
   - → proof by cases
3. To prove a statement false
   - → look for counter example
4. If proving existence of a property
   - → can form an existence proof

If way still so hard
   - → look for similar proof and adapt

Sets:

unordered collection of objects

elements/members: objects of a set

notation: $a \in A$: a is an element of A

$a \notin A$: a is not an element of A

Roster Method:

Given $S = \{a, b, c, d\}$

order doesn't matter

Repetition doesn't change the set:

$S = \{a, b, c, d\} = \{a, a, b, b, c, c, d, d\}$

Ellipses:

$S = \{a, b, c, \ldots, z\}$

Important Sets:

$\mathbb{N}$: natural numbers

$\mathbb{Z}$: integers

$\mathbb{Z}^+$: positive integers

$\mathbb{R}$: real numbers

$\mathbb{R}^+$: positive real #'s

$\mathbb{C}$: complex numbers

$\mathbb{Q}$: rational numbers

Set Builder Notation:

$S = \{x \mid x \in \mathbb{Z}^+ < 100\}$

(define properties all elements must satisfy

$S = \{x \mid P(x)\}$

Ex. Define S as set of living presidents

$S = \{$Carter, Clinton, W, Obama, Trump, Biden$\}$

$S = \{x \mid x =$ living presidents$\}$

Interval Notation:

$[a,b] = \{x \mid a \leq x \leq b\}$ closed

$(a,b) = \{x \mid a < x < b\}$ open

$(a,b]$, $[a,b)$ exist too

Universal and Empty set:

U : contains everything under consideration

$\emptyset$, $\{\}$: empty set (w/ notary)

Sets can be elements of sets:

ex. $\{\underbrace{\{1,2,3\}}_{\text{set}}, \underbrace{a}_{\text{element}}, \underbrace{\{s,t\}}_{\text{set}}\}$

set that contains 2 sets and an element

Note:

The empty set is different from the set that contains the empty set

$\emptyset \neq \{\emptyset\}$

Set Equality: $A = B$ if:

$\forall x (x \in A \leftrightarrow x \in B)$

Subsets:

$A \subseteq B$: A is a subset of B

$A \subseteq B$ holds if $\forall x (x \in A \rightarrow x \in B)$ is T

Proving Subsets:

$A \subseteq B$: show $\forall x (x \in A \rightarrow x \in B)$

$A \nsubseteq B$: find one example

Proper Subsets:

if $A \subseteq B$, but $A \neq B$

Notation: $A \subset B$

$\forall x (x \in A \rightarrow x \in B) \land \exists x$ . . .

Set Cardinality:

If n elements in set, set finite otherwise infinite

Ex. $|\emptyset| = 0$ $\quad |\mathbb{Z}| = \infty$

$|\{1,2,3\}| = 3$

$|\{\emptyset\}| = 1$

Ex. $A = \{1,2,3\}$

$B = \{2,3,4,5\}$

$C = \{A, B\} = \{\{1,2,3\},\{2,3,4,5\}\}$

$|A| = 3, \ |B| = 4, \ |C| = 2$

$A \in C$ T

$B \in C$ T

$1 \in A$ T

$1 \in C$ F

Power Sets:

$P(A)$: the set of all subsets of set A

if $A = \{a, b\}$, $\underbrace{P(A)}_{\text{power set}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

If $|A| = n$, $|P(A)| = 2^n$

Tuples:

ordered n-tuple: $(a_1, a_2, \ldots, a_n)$

tuples equal $\Leftrightarrow$ corresponding elements are equal

2-tuples are ordered pairs

Cartesian Product

$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$

set of ordered pairs where $a \in A$ and $b \in B$

Ex.

$U = \{a, b, c, d, e, f, g, h\}$ (the universe)

$A = \{a, b, c, d, e\}$

$B = \{c, d, e, f\}$

$A \times B$ = Cartesian product:

$\{(a,c), (a,d), (a,e), (a,f), (b,c),$
$(b,d), (b,e), (b,f), (c,c) \ldots \}$

$P(A): \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{e\},$
$\{a,b\}, \{a,c\}, \{a,d\}, \{a,e\},$
$\{b,c\} \ldots \}$

Why not $\{b,a\}$?

Because $\{a,b\} = \{b,a\}$

$\vdots$

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

$\vdots$

$\{a,b,c,d\}$

$\vdots$

$\{a,b,c,d,e\} \ldots \}$

$|P(A)| = 2^5 = 32$

Ex. $A = \{2,3,4\}, B = \{4,5\}$

$A \times B$, $B \times A$, B^2, B^3?

ordered pairs

$A \times B = \{(2,4), (2,5), (3,4), (3,5), (4,4), (4,5)\}$

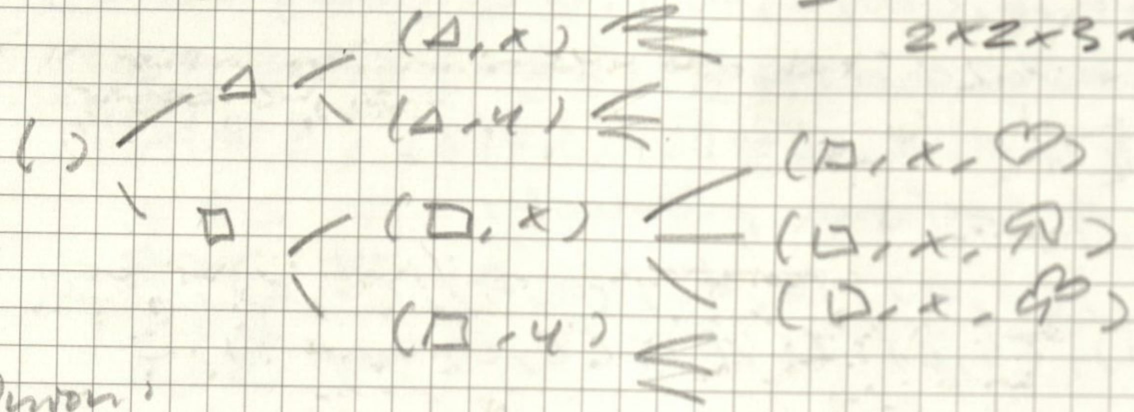
$B \times A = \{(4,2), (5,2), (4,3), (5,3), (4,4), (5,4)\}$

$B^2 = B \times B = \{(4,4), (4,5), (5,4), (5,5)\}$

$B^3 = B \times B \times B = \{(4,4,4), (4,4,5), (4,5,4) \ldots \}$

Ex. $\underbrace{\{\triangle, \square\}}_{2} \times \underbrace{\{x, y\}}_{2} \times \underbrace{\{\heartsuit, \spadesuit, \clubsuit\}}_{3}$

$2 \times 2 \times 3 = 12$



Union:

$A \cup B = \{x \mid x \in A \vee x \in B\}$

Intersection

$A \cap B = \{x \mid x \in A \wedge x \in B\}$

ex. $\{1, 2, 3\} \cap \{3, 4, 5\} = \{3\}$

Complement

$\overline{A} = \{x \in U \mid x \notin A\}$

$\overline{A}$ or A_c

Difference:

$A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \overline{B}$

Inclusion-Exclusion:

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

Ex. $U = \{a, b, c, d, e, f, g, h\}$

$A = \{a, b, c, d, e\}$; $B = \{c, d, e, f\}$

1. $A \cup B = \{a, b, c, d, e, f\}$
2. $A \cap B = \{c, d, e\}$
3. $\overline{A} = \{f, g, h\}$ 4. $\overline{B} = \{a, b, g, h\}$
5. $A - B = \{a, b\}$
6. $B - A = \{f\}$

Lecture Notes: 9.25.24

Why Sets?

Ex. many database operations on sets will produce subsets of the set generated when performing a Cartesian product operation

Consider:
- database columns (in tables) as sets
- database rows as n-tuples of the elements from each column or set
  → no 2 rows will be alike

* Not tested on this material *

Relations: subset of cartesian product

Relation R ⟨ create tuple that may be part of subset of interest

Table A, Table B:

$R \subseteq A \times B$

$xRy : x \in A, y \in B$

$x \not{R} y$?

* Tables A and B on handout *

Cartesian Product: every product sold × every sales location

Product

Product ID	prod name	cat	price
p001	laptop	electronic	$1000
p001	laptop	. . .	. . .
⋮			

Store

Store ID	name	loc
S001	techworld	NY
S002	gadgethub	SF
⋮		

columns in new table: $col_{T_1} + col_{T_2} = 4 + 3 = 7$
rows in new table: $\#row_{T_1} \times \#row_{T_2} = 4 \times 4 = 16$

Stock Availability:

$(P, S) \in R$
if a product P is available at store S

Subrelation: R' : stores that sell products below a certain price

$R' = \{(p002, s002), (p003, s003)\}$ discounts

Database Syntax:

SQL JOIN Operation: allows you to combine rows from 2 or more tables based on a related column b/w them

* subset of Cartesian product pairing rows from the joined tables where a condition is met

Ex. Same products/stores tables

SQL Query:

1. SELECT Prod.ProductID, Prod.ProductName, Stores.StoreID, Stores.StoreName
   # specify columns to retrieve
2. FROM Products
   # suggest primary table
   START w/ info Products
3. JOIN StockAvailability
4. ON Prod.ProductID = StockAvailability.ProductID
   # any products w/ availability included in subset of tuples extracted
5. JOIN Stores
6. ON Stores.StoreID = StockAvailability.StoreID

Ex- $C = \{CS101, CS102, CS201, CS301, CS401\}$

define R on C representing a "prerequisite" relationship

$R \subseteq C \times C$ — ordered pairs: (c_1, c_2) - suggests c_1 is a prereq for c_2

$R = \{(CS101, CS201), (CS102, CS201), \ldots\}$

more SQL query ex on handout for today

Set Operations:

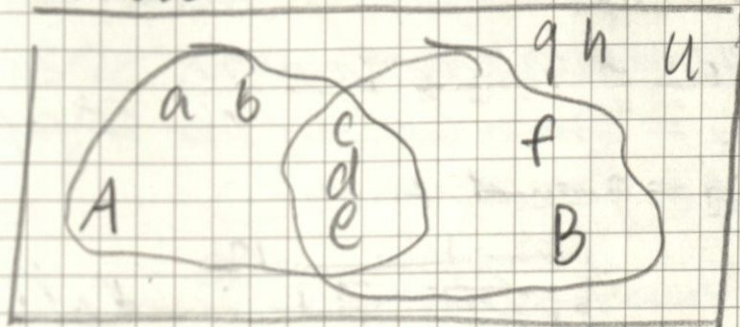
Union: $A \cup B$

Intersection: $A \cap B$

Complement: $\overline{A}$, B_c

Difference: $A - B$

Universe: U



$U = \{a, b, c, d, e, f, g, h\}$

$A = \{a, b, c, d, e\}$; $B = \{c, d, e, f\}$

Exclusive OR:

$A \oplus B: \{a, b, f\}$

elements in a OR b

* can nest operations as well *

Ex. $U = \mathbb{Z}^+$, P = set of all positive prime #'s

E = positive even integers

1. $P \cup E = \{n \in \mathbb{Z}^+ \mid n \in (P \vee E)\}$

2. $P \cap E = \{2\}$

3. ~~$\overline{P}$ = set of positive composite integers~~

4. $\overline{E} = \{2n+1 \mid n \in \mathbb{Z}^+\}$

5. $P - E = \{n \in P \mid n \notin E\}$?

6. $E - P = \{n \in E \mid n \notin P\}$?

7. $E \oplus P = \{n \in \mathbb{Z}^+ \mid (n \in P \vee n \in E) \wedge (n \neq 2)\}$

5. $P - E$ = all positive prime #'s except for 2

6. $E - P = \{2n \mid n \in \mathbb{Z}^+ \wedge n \geq 2\}$

7. $\underbrace{E}_{1/2} \oplus \underbrace{P}_{1/2} = \{n \in \mathbb{Z}^+ \mid n \text{ is prime or even} \wedge n \neq 2\}$

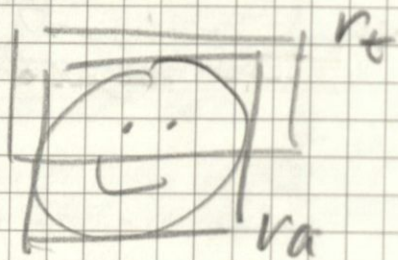
so must exclude

More Why?

Intersection over Union:

r_t = Drawn bounding box of target

r_a = ground truth



$$\frac{r_t \cap r_a}{r_t \cup r_a}$$

overlap is the r_t r_a

r_t overlap of r_a

Set Identities:

Identity Laws: $A \cup \emptyset = A$ $\quad A \cap U = A$

Domination Laws: $A \cup U = U$ $\quad A \cap \emptyset = \emptyset$

Idempotent Laws: $A \cup A = A$ $\quad A \cap A = A$

Complementation Law: $\overline{(\bar{A})} = A$

* more laws in sets slides *

→ a lot of the same from before

* Can also use same proof strategies

Ex: Prove $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

Suppose x is an arbitrary element of the universe

Proof 1:

	Assertion	Reason
1.	$x \in (A \cup B) \cap C$	given
2.	$[x \in (A \cup B)] \wedge [x \in C]$	definition of intersection
3.	$[(x \in A) \vee (x \in B)] \wedge [x \in C]$	def of union
4.	$[(x \in A) \wedge (x \in C)] \vee [(x \in B) \wedge (x \in C)]$	distributive law
5.	$[x \in (A \cap C)] \vee [x \in (B \cap C)]$	def of intersection
6.	$x \in [(A \cap C) \cup (B \cap C)]$	def of union

Proof #2: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$

A	B	C	$A \cup B$	$A \cap C$	$B \cap C$	$(A \cup B) \cap C$	$(A \cap C) \cup (B \cap C)$
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	0
1	0	1					
	⋮						

show columns are equivalent

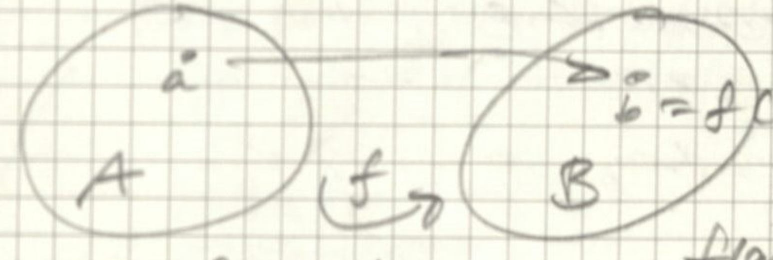
* won't see many of these
* lots of examples in slides

Functions:

Def. $f: A \to B$
assignment of each element of A to exactly one element of B

Notation: $f(a) = b$
b is a unique element of B assigned by f

* $f: A \to B \subseteq A \times B$ (a relation)
⇒ formal quantifier notation too



Injection:
$f(a) = f(b) \mid a = b \ \forall a, b \in U$

image: $f(a) = b$
a is preimage
b is image of a under f

Surjection:
$\forall x \in U \mid b \in B \Leftrightarrow a \in A$

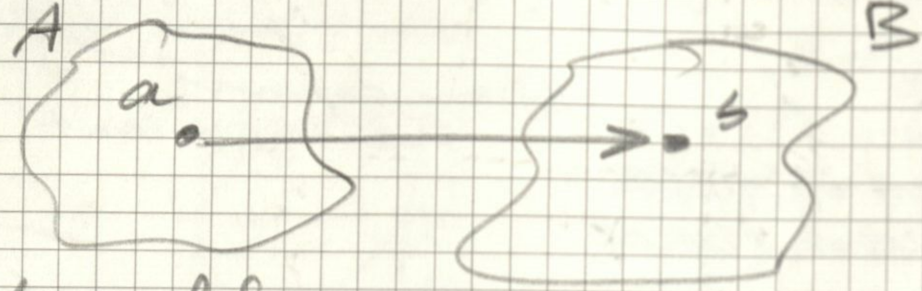
Can be defined in
- explicit statement
- expression
- computer program

Bijections:
Both

Injections: f is one-to-one
Surjection: f is onto
Bijection: f is both one-to-one and onto

Lecture Notes
Function Recap

function f = mapping from set A to set B

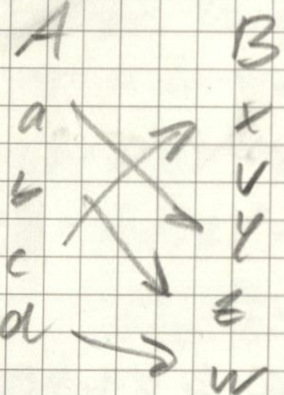


domain of f codomain of f

$f(a) = b$ | a, b elements of set A, B respectively

b = image of a under f
a = pre-image of b

"1-to-1" function: injection



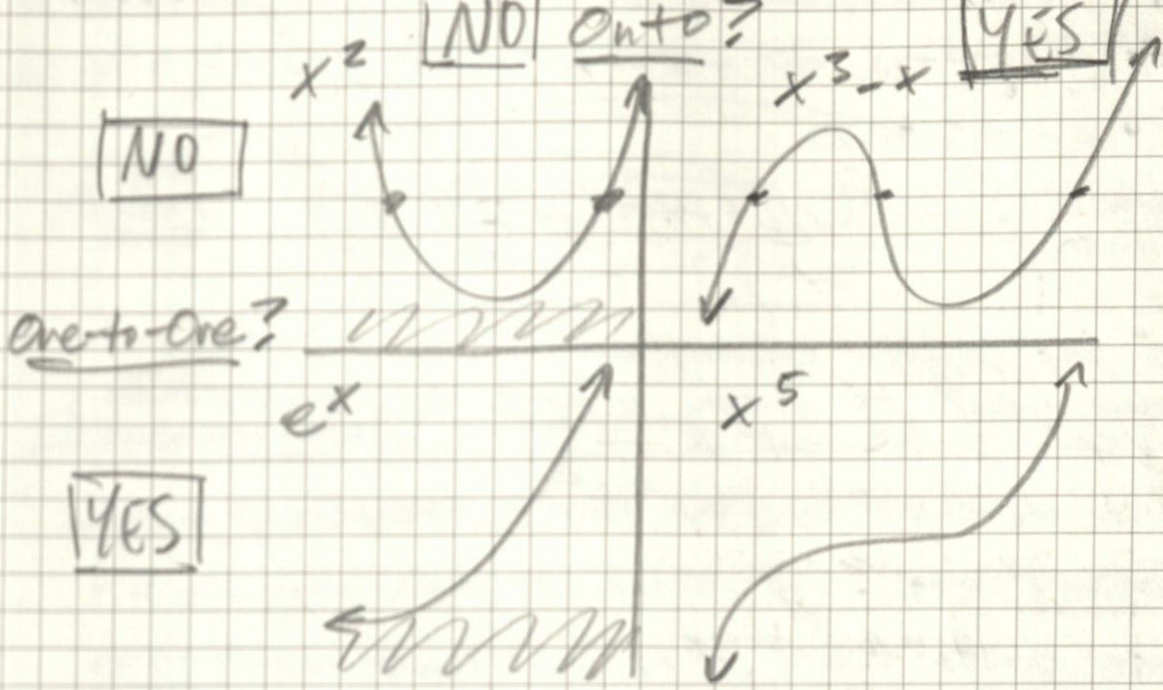
each element in A maps to only one element of B

"onto" function: surjection

$a \to x$
$b \to y$
$c \to z$
$d \to z$

all elements of B are mapped to be an element of A

Bijection: both an injection and a surjection



Ex - Show $f: \mathbb{N} \to \mathbb{N}$ defined by $f(n) = n^2$ is an injection (1-to-1 mapping)

- Lets use proof by contraposition
- Show: $m \neq n$, $f(m) \neq f(n)$
- Prove contrapositive: $f(m) = f(n) \Rightarrow m = n$

$p: m \neq n$ (Hypothesis)
$q: f(m) \neq f(n)$ (Conclusion)
$\neg q: f(m) = f(n)$
$\neg p: m = n$

$$f(m) = f(n) \Rightarrow m^2 = n^2$$
$$\Rightarrow m^2 - n^2 = 0$$
$$\Rightarrow (m-n)(m+n) = 0$$

$m = n$ or $\cancel{m = -n}$

must be $\in \mathbb{N}$

shown $\neg p$ ∎

Ex. Is $f: \mathbb{R} \to \mathbb{R}$ defined by x^2+2x a surjection

- What if $y = -2 \Rightarrow -2 = x^2+2x$

$\Rightarrow x^2+2x+2=0$

Quadratic Formula: $\frac{-b \pm \sqrt{b^2-4ac}}{2a} = \frac{-2 \pm \sqrt{-4}}{2}$ not real

proof by counter example

$\Rightarrow$ no way to map $y=-2$ to corresponding real value of x

*. Ex> of how to do all cases of this in slides of

Inverse Function:

* No inverse exists unless f is a bijection

$f^{-1}(y) = x \Leftrightarrow f(x) = y$

Ex. let $f: \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x+1$. Prove f is a bijective f'n

- Show $f(x) = 2x+1$ is BOTH 1-to-1 and onto
- Show injective / 1-to-1 property:

Consider arbitrary a, b

$f(a) = f(b)$ / $a = b$

$f(a) = f(b)$

$2a+1 = 2b+1$

$2a = 2b$

$a = b$ ⇐ Shown $f(x) = 2x+1$ is 1-to-1 ✓

- Show surjective/onto property:

Consider arbitrary element $b \in B$.

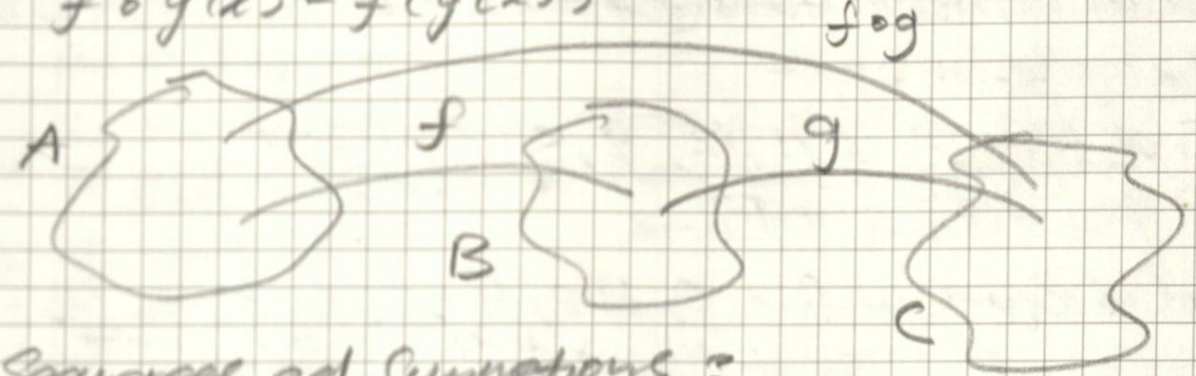
Find element $a \in A$ s.t. $f(a) = b$

— Let $b = f(a)$ Assume $b = 2a+1 \therefore a = \frac{b-1}{2}$

— If b is real in codomain, then a has to be real as well ✓

Composition:

$f \circ g(x) = f(g(x))$



Sequences and Summations:

Sequence: ordered list of elements

- a function from the subset of integers to a set S

notation: a_n

$a_n \equiv f(n)$; $f : \mathbb{Z} \to S$

Geometric Progression:

sequence in form $a, ar, ar^2, \ldots, ar^n$

- $a, r \in \mathbb{R}$

Arithmetic Progression:

form: $a_n = a, a+d, a+2d, \ldots, a+nd$

- $a, d \in \mathbb{R}$

Recurrence Relations:

- is a equation that expresses a_n in terms of one or more previous terms of the sequence
- A solution of a RR satisfys this formula
- need to satisfy initial conditions

Ex. Does a sequence satisfy a recurrence relation?

1. Find an expression for sequence 1, 1, 2, 3, 5, 8, 13, 21, ...

strategies:

diff. 0, 1, 1, 2, 3, 5

$F_n = F_{n-1} + F_{n-2}$

2. Find an expression for 0, 1, 2, 4, 5, 6, 8, 9, 10, ...

every 4th # skipped

$T_n = n + \lfloor n/3 \rfloor$ "floor" operation

n	$\lfloor n/3 \rfloor$	$\lfloor n/3 \rfloor + n$
0	0	0
1	0	1
2	0	2
3	1	4
4	1	5
5	1	6

Floor Function: $f(x) = \lfloor x \rfloor$ is largest integer $\leq x$

Ceiling Function: $f(x) = \lceil x \rceil$ is smallest integer $\geq x$

* Table with more properties of these symbols *

Ex- Determine whether $\{a_n\}$ where $a_n = 3n$ $\forall n \in Z^+$ is a solution to $a_n = 2a_{n-1} - a_{n-2}$ for $n = 2, 3, 4, \ldots$

i.e. Is $a_n = 3n$ going to give us $a_n = 2a_{n-1} - a_{n-2}$

1. $a_n = 3n$? 2. $a_n = 2^n$? 3. $a_n = 5$?

1> $a_{n-1} = 3(n-1)$

$a_{n-2} = 3(n-2)$

look at recurrence relation:

$a_n = 2a_{n-1} - a_{n-2}$

Sub expressions for a_{n-1} and a_{n-2}

$a_n = 2(3(n-1)) - (3(n-2))$

$= 6n - 6 - 3n + 6 = 3n$ & $a_n = 3n$ ✓

2. $a_n = 2^n$

$a_0 = 1,\ a_1 = 2,\ a_2 = 4, \ldots$

$a_n = 2a_{n-1} - a_{n-2}$

$a_2 = 2a_1 - a_0 = 4 - 1 = 3 \neq a_2 = 4$

$\therefore$ not a solution to recurrence relation

3. $a_n = 5$

$a_0 = 5,\ a_1 = 5,\ a_2 = 5, \ldots$

$a_2 = 2a_1 - a_0 = 10 - 5 = 5$ ✓ $\therefore$ solution

Ex. Is $a_n = (2 \cdot 3^n) + (-1)^n$ a solution for

$a_n = 2a_{n-1} + 3a_{n-2}$

$a_{n-1} = (2 \cdot 3^{n-1}) + (-1)^{n-1}$

$a_{n-2} = (2 \cdot 3^{n-2}) + (-1)^{n-2}$

Sub in a_{n-1} and a_{n-2} into recurrence relation:

$$a_n = 2\left[(2 \cdot 3^{n-1}) + (-1)^{n-1}\right] + 3\left[(2 \cdot 3^{n-2}) + (-1)^{n-2}\right]$$

$$= 2(2)(3^{n-1}) + 2(-1^{n-1}) + 3(2)(3^{n-2}) + 3(-1)^{n-2}$$

$$= (2)(2)(3^n)(3^{-1}) + 2(-1)^n(-1)^{-1} + (2)(3)(3^n)(3^{-2}) + 3(-1)^n(-1)^{-2}$$

$$= 3^n\left[\frac{4}{3} + \frac{6}{9}\right] + (-1)^n[-2+3]$$

$$= 3^n\left[\frac{4}{3} + \frac{2}{3}\right] + (-1)^n = (2 \cdot 3^n) + (-1)^n \checkmark$$

Solving Recurrence Relations: finding an a_n in terms of n called a closed formula

- Various Methods to do this
  - → forward substitution
  - → backward substitution

Ex. Let $\{a_n\}$ satisfy $a_n = a_{n-1} + 3$ for $n = 2, 3, 4, \ldots$
and suppose $a_1 = 2$

Forward Substitution:

$a_n = a_{n-1} + 3$ (For $a_1 = 2$, $n = 2, 3, 4, \ldots$)

$a_2 = a_{2-1} + 3 = a_1 + 3 = \underline{2 + 3} = 2 + 3(1)$

don't immediately
simplify to look for patterns

$a_3 = a_{3-1} + 3 = a_2 + 3 = (2+3) + 3 = 2 + 3(2)$

$a_4 = a_{4-1} + 3 = a_3 + 3 = ((2+3)+3) + 3 = 2 + 3(3)$

$a_n = 2 + 3(n-1)$ closed form ✓

Backward Substitution: $a_n = a_{n-1} + 3$

$a_n = (a_{n-2} + 3) + 3$

$= (a_{n-3} + 3) + 3 + 3$

$\vdots$

$a_n = 2 + 3(n-1)$ ✓

Ex. Consider $T_n = T_{n-1} + 2n - 1$. $T_0 = 0$

generate elements of sequence:

$T_1 = T_{1-1} + 2(1) - 1 = 0 + 2 - 1 = 1$ $(n, T_n) = (1, 1)$

$T_2 = T_{2-1} + 2(2) - 1 = 4$. $(2, 4)$

$T_3 = T_{3-1} + 2(3) - 1 = 9$. $(3, 9)$

Square of value of n to get T_n

$\Rightarrow$ Guess. $T_n = n^2$

check. $T_n = T_{n-1} + 2n - 1$

$T_n = (n-1)^2 + 2n - 1$

$= n^2 - 2n + 1 + 2n - 1 = n^2$ ✓

Ex. Find solution to $a_n = a_{n-1} - n$, $a_0 = 4$

$a_n = -n + a_{n-1}$

$a_{n-1} = -(n-1) + a_{n-1-1} = -(n-1) + a_{n-2}$

$a_{n-2} = -(n-1-1) + a_{n-3}$

$a_{n-3} = -(n-3) + a_{n-4}$

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

4

eqn to capture
sum of successive
#'s

$a_n = -(n + (n-1) + (n-2) + \ldots) + a_0$

Lecture Notes: 10.3.24

Ex. recurrence: $a_n = n \times a_{n-1}$; $a_0 = 1$

Use backwards substitution to find closed form

$a_n = n \times a_{n-1}$
$a_{n-1} = (n-1) \times a_{n-2}$
$a_{n-2} = (n-2) \times a_{n-3}$
⋮

$a_n = n \times (n-1) \times (n-2) \times \dots a_0$
$a_n = 1 \times 2 \times 3 \times \dots = n!$

*Ex. find formula for $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots$

utilize geometric progression; $a_n = \frac{1}{2^n}$

$a = 1, r = \frac{1}{2} \Rightarrow ar^n \rightarrow$

Ex. find formula for $1, 3, 5, 7, 9$

utilize arithmetic progression; $a_n = 2n+1$

$a = 1, d = 2 \Rightarrow nd + a_0 \rightarrow$

* useful sequences in slides *

Ex. What is the formula for $1, -3, 9, -27, \dots$

$a_0 = 1$

- look for differences → arithmetic
- look for ratios → geometric
- look for sign alternation

Use geometric progression: ar^n

$a = 1, r = -3 \Rightarrow (-3)^n$

Ex. $5, 3, 1, -1, -3$?

arithmetic: $a + nd \Rightarrow a_n = -2n + 5$
$5 - 2n$

Ex.

n:	0	1	2	3	4	...	19	20	21
a_n:	5	6	8	12	20		524292	1048580	2097156
ratios?		1.2	1.31	1.5	1.67			1.9999 ...	

* approaching 2 * $\Rightarrow 2^n + \dots$

a_n: $5-4=1$, $6-4=2$, $8-4=4$, $12-4=8$, $20-4=16$ ...

$a_n = 2^n + 4$

Summations:

Sum of terms $a_m, a_{m+1}, \dots, a_n$ from sequence $\{a_n\}$

Notations: j = index of summation

$$\sum_{j=m}^{n} a_j \quad \sum_{j=m}^{n} a_j \quad \sum_{m \le j \le n} a_j$$

For Sets:

$\sum_{j \in S} a_j$ ← sum all elements in set

* table of useful summation formulas in slides *

Geometric Series:

$$\sum_{j=0}^{n} ar^j = \begin{cases} \frac{ar^{n+1}-a}{r-1} & r \ne 1 \\ (n+1)a & r = 1 \end{cases}$$

Proof: Let $S_n = \sum_{j=0}^{n} ar^j$

$$\Rightarrow rS_n = r\sum_{j=0}^{n} ar^j = \sum_{j=0}^{n} ar^{j+1} = \sum_{k=0}^{n+1} ar^k$$

$$\Rightarrow \left(\sum_{k=0}^{n} ar^k\right) + (ar^{n+1} - a) = S_n + (ar^{n+1} - a)$$

$$\therefore rS_n = S_n + (ar^{n+1} - a) \Rightarrow rS_n - S_n = ar^{n+1} - a$$

$$\Rightarrow S_n(r-1) = ar^{n+1} - a \Rightarrow S_n = \frac{ar^{n+1}-a}{r-1} \text{ if } r \ne 1$$

$$\Rightarrow S_n = \sum_{j=0}^{n} ar^j = \sum_{j=0}^{n} a = (n+1)a \text{ if } r = 1$$

Product Notation :

Product of terms $a_m, a_{m+1}, \ldots, a_n$ from sequence $\{a_n\}$,

Notation

$$\prod_{j=m}^{n} a_j \qquad \prod_{j=m}^{n} a_j \qquad \prod_{m \le j \le n} a_j$$

Cardinality of Sets :

- Sets A, B : Have same cardinality iff bijective ie. $|A| = |B|$
- Consider cardinality / countability in context of finite and infinite sets

Finite : $S = \{1, 3, 5, 7, 9, 11\}$ $\quad |S| = 6$

$a_0 \; a_1 \; a_2 \; a_3 \; a_4 \; a_5$

Infinites CAN be countable if $|S| = |\mathbb{Z}^+|$

NOT COUNTABLE : Ex $|\mathbb{R}| = \cancel{\aleph}\ \aleph_0$

(aleph null)

How to show if set countable ?

* list elements of a set st. to be indexable by positive integers
→ establish one-to-one correspondence

$a_1, a_2, a_3, \ldots \quad a_1 = f(1), a_2 = f(2), a_3 = f(3), \ldots$

Ex. Show set of even integers is countable :

Show Bijectiveness :

$f(n) = 2n$; $f(\mathbb{Z}^+ \to \text{even}(\mathbb{Z}^+))$

Suppose $f(n) = f(m) \Rightarrow 2n = 2m \Rightarrow n = m$

injection / 1-to-1 ✓

Show onto : $\forall y\, \exists x\, (f(x) = y)$

- suppose arbitrary int t

t is one less than odd int : $2k+1-1 = 2k$

$\forall t\, \exists x\, (f(x) = 2k = t)$; $t = 2k$

∴ Countable

Exam 01 Review: 10.7.24

Proposition: statement that is either true or false

Negation: $\neg$
Conjunction: $\land$
Disjunction: $\lor$
Implication: $\rightarrow$
Biconditional: $\leftrightarrow$
Exclusive OR: $\oplus$

Implication: $p \rightarrow q$
Converse: $q \rightarrow p$
Inverse: $\neg p \rightarrow \neg q$
Contrapositive: $\neg q \rightarrow \neg p$

Order of Operations: $\neg, \land, \lor, \rightarrow, \leftrightarrow$

Tautology: always true
Contradiction: always false
Contingency: neither a Tautology or Contradiction

Key Logical Equivalences:

Identity Laws: $p \land T \equiv p \quad p \lor F \equiv p$

Domination Laws: $p \lor T \equiv T \quad p \land F \equiv F$

Idempotent Laws: $p \lor p \equiv p \quad p \land p \equiv p$

Double Negation Law: $\neg(\neg p) \equiv p$

Negation Laws: $p \lor \neg p \equiv T \quad p \land \neg p \equiv F$

Commutative Laws: $p \lor q \equiv q \lor p \quad p \land q \equiv q \land p$

Associative Laws: $(p \land q) \land r \equiv p \land (q \land r)$
$(p \lor q) \lor r \equiv p \lor (q \lor r)$

Distributive Laws: $(p \lor (q \land r)) \equiv (p \lor q) \land (p \lor r)$
$(p \land (q \lor r)) \equiv (p \land q) \lor (p \land r)$

Absorption Laws: $p \lor (p \land q) \equiv p \quad p \land (p \lor q) \equiv p$

DeMorgan's Laws: $\neg(p \land q) \equiv \neg p \lor \neg q$
$\neg(p \lor q) \equiv \neg p \land \neg q$

Other Useful Logical Equivalences:

$p \to q \equiv \neg p \vee q$

$p \to q \equiv \neg q \to \neg p$

$p \vee q \equiv \neg p \to q$

$p \wedge q \equiv \neg (p \to \neg q)$

$\neg (p \to q) \equiv p \wedge \neg q$

$(p \to q) \wedge (p \to r) \equiv p \to (q \wedge r)$

$(p \to r) \wedge (q \to r) \equiv (p \vee q) \to r$

$(p \to q) \vee (p \to r) \equiv p \to (q \vee r)$

$(p \to r) \vee (q \to r) \equiv (p \wedge q) \to r$

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

$\neg (p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

SAT Problems:

satisfiable: there exists an assignment of truth values to make the proposition true

unsatisfiable = no such assignment exists

$\bigvee_{j=1}^{n} p_j = p_1 \vee p_2 \vee \ldots \vee p_n$

$\bigwedge_{j=1}^{n} p_j = p_1 \wedge p_2 \wedge \ldots \wedge p_n$

Predicate:

Variables = x, y, z

Predicates: P, Q, M

Quantifiers: $\forall$, $\exists$, $\exists!$

Propositional Functions:

$\forall x P(x)$

$\exists y Q(y)$

Universal Quantifier ($\forall$) = "for all"

Existential Quantifier ($\exists$): "there exists"

Uniqueness Quantifier ($\exists!$): "there is one"

have higher precedence than all logical operators

$\forall x P(x) \equiv P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$

$\exists y Q(y) \equiv Q(y_1) \vee Q(y_2) \vee \ldots \vee Q(y_n)$

Bound vs Free Vars:

$\forall x P(x, y)$

- x is bound by quantifier
- y is free

Restricting Domain:

$\forall x\,(Q(x) \to P(x))$

- for all x, if $Q(x)$ holds, then $P(x)$ holds
- $Q(x)$ restricts the domain

$\exists x\,(Q(x) \land P(x))$

- there exists an x where $Q(x)$ and $P(x)$ hold
- $Q(x)$ restricts the domain

DeMorgan's Laws:

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

* quantifiers have scope and can be nested *

→ think for-loops

→ order matters!

Argument:

premise

premise

∴ conclusion

Proof: valid argument establishing truth of a statement

Valid Argument = premises imply conclusion

$\bigwedge_{i=1}^{n} p_i \to q$

Rules of Inference:

Modus Ponens:

$$\begin{array}{l} p \to q \\ \underline{p} \\ \therefore q \end{array}$$

Modus Tollens:

$$\begin{array}{l} p \to q \\ \underline{\neg q} \\ \therefore \neg p \end{array}$$

Disjunctive Addition:

$$\begin{array}{l} \underline{p} \\ \therefore p \lor q \end{array} \quad \text{or} \quad \begin{array}{l} \underline{q} \\ \therefore p \lor q \end{array}$$

Conjunctive Simplification:

$$\begin{array}{l} \underline{p \land q} \\ \therefore p \end{array} \quad \text{or} \quad \begin{array}{l} \underline{p \land q} \\ \therefore q \end{array}$$

Disjunctive Syllogism:

$$\begin{array}{l} p \lor q \\ \underline{\neg p} \\ \therefore q \end{array} \quad \text{or} \quad \begin{array}{l} p \lor q \\ \underline{\neg q} \\ \therefore p \end{array}$$

Conjunction:

$$\begin{array}{l} p \\ \underline{q} \\ \therefore p \land q \end{array}$$

Hypothetical Syllogism

$$\begin{array}{l} p \to q \\ \underline{q \to r} \\ \therefore p \to r \end{array}$$

Resolution:

$$\begin{array}{l} p \lor q \\ \underline{\neg p \lor r} \\ \therefore q \lor r \end{array}$$

Common Fallacies:

Affirming Conclusion:
$$\begin{array}{l} p \to q \\ q \\ \hline \therefore p \end{array}$$

Denying the Hypotheses:
$$\begin{array}{l} p \to q \\ \neg p \\ \hline \therefore \neg q \end{array}$$

Handling Quantified Statements:

Unified Instantiation:
$$\begin{array}{l} \forall x P(x) \\ \hline \therefore P(a) \end{array}$$

Unified Generalization:
$$\begin{array}{l} \forall a \in U\ P(a) \\ \hline \therefore \forall x P(x) \end{array}$$

Existential Instantiation:
$$\begin{array}{l} \exists x P(x) \\ \hline \therefore \exists a \in U\ P(a) \end{array}$$

Existential Generalization:
$$\begin{array}{l} \exists a \in U\ P(a) \\ \hline \therefore \exists x P(x) \end{array}$$

Proofs:

Theorem: statement that can be shown to be true
Lemma: helping theorem or result needed to prove a theorem
Corollary: result which follows directly from a theorem
Proposition: less important theorems
Conjecture: statement proposed to be true
Axiom: basic statement accepted as true

Proving Theorems:

common form: $\forall x (P(x) \to Q(x))$
show that: $P(c) \to Q(c)$
treat as: $p \to q$

Methods:

- trivial proof
- vacuous proof
- direct proof
- proof by contraposition
- proof by contradiction
- proof by cases
- exhaustive proofs
- without loss of generality
- uniqueness proofs

Trivial Proof: if q is true, $p \to q$ is also true

Vacuous Proof: if p is false, $p \to q$ is true

Direct Proof: assume p is true, show q must also be true

Proof by Contraposition: assume $\neg q$ is true, show $\neg p$ must also be true

Proof by Contradiction:

1. assume $\neg q$ is true
2. reach a contradiction
   a) violation of a theorem or axiom
   b) contradiction with a given assumption or fact
   c) situation where something is both T and F
4. conclude since $\neg q$ leads to a contradiction, q must be true

Biconditional Proofs: to proove $p \leftrightarrow q$ must prove $p \to q$ and $q \to p$

Proof by Cases:

to prove $\bigvee_{i=1}^{n} p_i \to q$ use:

$[(\bigvee_{i=1}^{n} p_i) \to q] \leftrightarrow [\bigwedge_{i=1}^{n} (p_i \to q)]$ where $p_i \to q$ is a case

Exhaustive Proof: special type of proof by case that examines all possible examples

Without Loss of Generality: by proving one case of a theorem, no additional argument is required to prove the other specified cases

Uniqueness Proof:

Existence: show x with desired property exists

Uniqueness: show if $x \neq y$, y does not have desired property
(or if both x and y have desired properties, then $x = y$)

Lecture Notes: 10.8.24

Algorithms: finite set of precise instructions to performing a computation or for solving a problem

Properties: input, output, correctness, finiteness, effectiveness, generality

Classes of Problems:

1. searching problems
2. sorting problems
3. optimization problems — not tested
   - the traveling salesman problem

Searching Problems:

- locate an element x in a list of distinct elements $a_1, a_2, \ldots, a_n$
- solution is index i where match is found

ex. linear search, binary search

Sorting Problems:

- puts elements in a list in increasing order

ex. bubble sort, insertion sort, merge sort

Ex. Determine if $S = \{11, 12, 13, \ldots\}$

$$\begin{array}{cccc} 11 & 12 & 13 & \\ \uparrow & \uparrow & \uparrow & \\ 1 & 2 & 3 & \ldots \quad n \leftrightarrow n+10 \end{array}$$

is finite, countably infinite, or uncountable

Ex. $S = \{-999, -998, \ldots, 998, 999\}$

finite.

Ex. $\{\pm 10, \pm 20, \pm 30, \ldots 0\}$

$\{0, -10, 10, -20, 20, -30, 30, \ldots\}$

countably infinite

Big-O Notation:

- measure of counting complexity of a function
  - → f(x) is "Big O" of g(x)
  - → f(x) is on the order of g(x)

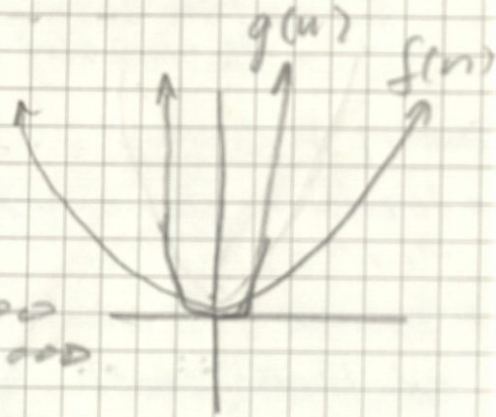
ex. $f(x) = 2x^3 + 2x^2 + \log x + 7x + 3$

$f(x) = O(x^3)$

Note. Big O notation — gives upper bound of growth rate of function

Ex. $f(n) = 100n^2 \quad g(n) = n^4$

n	f(n)	g(n)
1	100	1
5	2500	625
10	10000	10000
50	250,000	6,250,000
100	1,000,000	100,000,000



* $f(x)$ is $O(g(x))$
  - if $|f(x)| \leq \underline{c}\,|g(x)|$ when $x > \underline{k}$

c, k = witnesses

- $f(n)$ is $O(g(n))$ if positive constants c, k such that $f(n) \leq c(g(n))$ when $n > k$

$$\exists c \, \exists k \, \forall n \, [n > k \rightarrow f(n) \leq c g(n)]$$

- no formal method to find c, k...
  - → make a small table, look at ratios

Ex. $3n + 7 = f(n)$. show $O(n) = g(n) = n$

n	f(n)	g(n)	$\lceil f(n)/g(n) \rceil$
1	10	1	$\lceil 10/1 \rceil = 10$
10	37	10	$\lceil 37/10 \rceil = 4$
100	307	100	$\lceil 307/10 \rceil = 4$

Extract values of c, k:

$n > 1$ $(k = 1)$ | $c = 10$ (ratio)

$n > 10$ $k = 10$ | $c = 4$

$(k, c) = (1, 10) | (10, 4)$

$(k=1, c=10)$ $f(n) \le c(g(n))$ when $n > k$

$3n+7 \le 10 \quad n \quad\quad n>1$

$\Rightarrow 3n+7 \le 10$; $n > 1$

look @ constant 7 – show if I add value of 3n to 7 it shouldn't exceed 10. (when $n>1$)

to check:

$n > 1$ multiply both sides by 7 $\Rightarrow 7n > 7$

$\therefore \forall n > 1, \; 7n > 7$

Now, we can rewrite 10n term in original inequality:

$3n+7 \le 10n \equiv 3n+7 \le 3n+7n$

$3n \le 3n \quad 7 \le 7n$ ✓

Ex. 1 $k=10, c=4$

$f(n) \le c(g(n))$ when $n>k$

$3n+7 \le 4n$ when $n > 10$

$-3n \quad\quad -3n$

$7 \le n$ but est. $n > 10$

$10 > 7$ ✓

cont.

if $n>10$, implies $n>4$

implies $n^3 > 4n^2$

Substitute:

$n^3+3n^2+3n+1 \le n^3+n^3$

$n^3+3n^2+3n+1 \le 2n^3$

when $n > 10$

Ex. Show: $(n+1)^3$ is $O(n^3)$

1. make table of ratios

n	$f(n)$	$g(n)$	$\lceil f(n)/g(n) \rceil$
1	8	1	8
10	1331	1000	2
100	1030301	1000000	2

$k=10; c=2$

$(n+1)^3 \le c \cdot g(n)$ when $n>k$

$n^3+3n^2+3n+\underline{1} \le 2 \cdot n^3$ when $n > 10$

look at lowest order terms: if $n > 10$ implies $n > 1$

$n^3+3n^2+3n+\underline{1} \le n^3+3n^2+3n+\underline{n}$

$n^3+3n^2+3n+1 \le n^3+3n^2+4n$

if $n > 10$ implies $n > 4$ ⇒ lowest order term,

$n^2 > 4n$ ⇒ multiply each side w/ n

$n^3+3n^2+3n+1 \le n^3+3n^2+n^2$ ⇒ sub $4n$ w/ n^2

$n^3+3n^2+3n+1 \le n^3+\underline{4n^2}$

Lecture Notes: 10.10.24

Ex- Show n^2+2n+1 is $O(n^2)$

Identify constants c, k

$f(n) = n^2+2n+1$, $g(n) = n^2$

$f(n) \le \underline{\underline{c}} \cdot g(n) : n > \underline{\underline{k}}$

(1) Need 1 pair of c,k values

n	$f(n)$	$g(n)$	$\lceil f(n)/g(n) \rceil$
1	4	1	4
10	121	100	2
100	10201	10000	2
⋮			↑
k			c

Witness: $k=1$, $c=4$

- $f(n) \le c \cdot g(n) \Rightarrow n^2+2n+1 \le 4n^2$
- if $n>1 \Rightarrow n^2+2n+\underline{\underline{1}} \le n^2+2n+\underline{\underline{n}} : \underline{\underline{n}} > 1$

  $n^2+2n+1 \le n^2+3n : 3n \cdot n > 1 \cdot 3n$
- Replace $3n$ w/ $3n^2$: $n^2+2n+1 \le n^2+3n^2 : 3n^2 > 3n$

  $n^2+2n+1 \le \underline{\underline{4}}n^2$ ✓ c

Witness: $k=10$, $c=2$

$n^2+2n+1 < \underset{c}{2}n^2 : n > \underset{k}{10}$

- $n^2+2n+1 \le n^2+2n+n$

  $n^2+2n+1 \le n^2+3n : n>10 \Rightarrow n>3$

  $n \cdot n > 3 \cdot n$

  $n^2 > 3n$

$n^2+2n+1 \le n^2+n^2$

$n^2+2n+1 \le \underline{\underline{2}}n^2$ ✓ c

Intuition:

```
for (i=0; i<n; i++)          for (i=0; i<n; i++)
  for (j=0; j<n; j++)          for (j=0; j<n; j++)
    statement 1                  statement 1
              2                            :
              :                           10
              5
```

$n \cdot n \cdot 5 = 5n^2$ $n \cdot n \cdot 10 = 10n^2$

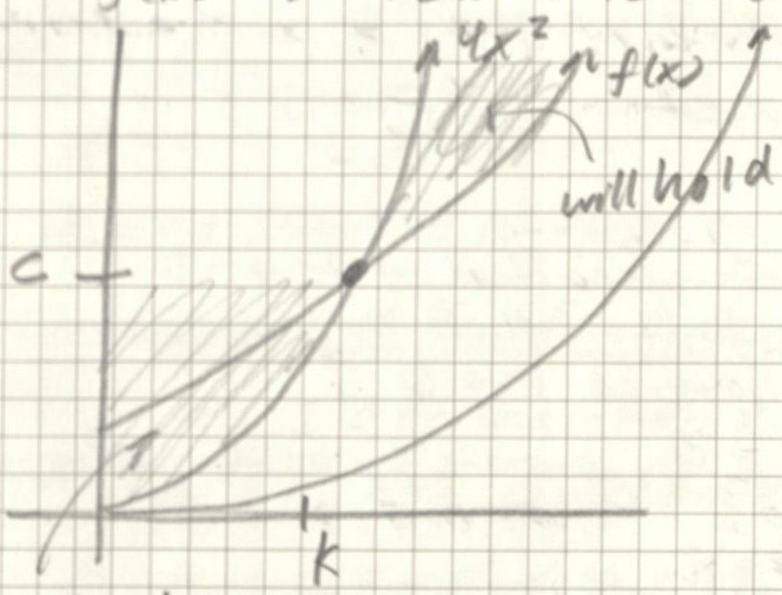
C   C

n	$f(n)$	$g(n)$	$\lceil f(n)/g(n) \rceil$
1	5	1	5
10	500	100	5
100	:	:	

$\underline{k}$: sense of input size — # of iterations $\underline{n}$
- intuition of size of input

Illustration of O Notation:

$f(x) = x^2 + 2x + 1$ is $O(x^2)$



will not hold

- if $f(x)$ is $O(g(x))$ and $h(x) > g(x) \in \mathbb{R}$
then $f(x)$ is $O(h(x))$
→ but want smallest complexity

Ex- Show $f(x) = 2x^3 + 10x$ is not $O(x^2)$

$f(x) = 2x^3 + 10x$: $\forall c \forall k \exists x ((x > k) \land (f(x) > c\,g(x)))$

— Show no values of c, k exist to meet this condition

$f(x) = 2x^3 + 10x$, $g(x) = x^2$

Ratio of $f(x)/g(x)$: $\frac{2x^3 + 10x}{x^2} = \frac{2x^3}{x^2} + \frac{10x}{x^2}$

$= 2x + \frac{10}{x}$

$\Rightarrow \lim_{x \to \infty} \left(2x + \frac{10}{x}\right) = 2x$

Note: Ratio of $f(x)/g(x) = 2x$ and grows w/o bound

$\therefore$ For any c, find x so $2x + \frac{10}{x} > c$

b/c 2x term grows linearly w/x

$\rightarrow 2x > c$

c constant

plug in value of x so $2x > c$

Ex- Show n^2 is not $O(n)$ via proof by contradiction

Recap: Proof by Contradiction : $(P \to Q)$

- Assume $\neg Q$
- Assume P is TRUE
- Derive a contradiction associated w/ $P \to \neg Q$
- if contradiction, assumption that Q is false has to be wrong, proves $P \to Q$

Ex: if $x \geq 3$, then $x^2 \geq 9$. prove by contradiction

1) STATE P, Q : P: $x \geq 3$ PROVE: $P \to Q$

Q : $x^2 \geq 9$

2) ASSUME $\neg Q$: $x^2 < 9$, 3) ASSUME P : $x \geq 3$

4) Derive a contradiction

- $x \geq 3$
- $x^2 < 9 \Rightarrow x < 3$ $\therefore$ contradiction

$\neg Q$ has to be false $\therefore P \to Q$

Show n^2 is not $O(n)$ by proof by contradiction

P: n^2 is $O(n)$ $\therefore$ $\exists c \exists k : f(n) \le c g(n) : n > k$
$\Rightarrow n^2 \le c \cdot n$

Q: Assumption that $n^2 \le cn$ – true for large n

Prove n^2 is not $O(n)$

- Assume $\neg Q$: $\exists c \exists k : n^2 > cn$
- Assume P: n^2 is $O(n)$
  $\exists c \exists k : n^2 \le cn : n > k$
- Contradiction: divide $n^2 \le cn$ by n
  $\Rightarrow n \le c \Rightarrow$ implies $\forall n > k, n \le c$
  $\therefore$ n can get large $\therefore$ proved

Big-O Estimates for Polynomials:

Let: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$
$: a_0, a_1, \ldots, a_n \in \mathbb{R} : a_n \ne 0$

$\Rightarrow$ Then: $f(x)$ is $O(x^n)$

$\therefore$ Leading term of polynomial dominates complexity

Big O Estimates:

$d > c > 1 \Rightarrow n^c$ is $O(n^d)$ but n^d not $O(n^c)$

* more examples of these in slides

Combinations of Functions:

if $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$
$\Rightarrow (f_1 + f_2)(x)$ is $O(\max(|g_1(x)|, |g_2(x)|))$

* other versions of this statement in slides

Ex. Give Big O estimate for:

$(n^2 \log(n) + n^2)(n^3 + 2)$

$\Rightarrow n^5 \log(n) + 2n^2 \log(n) + n^5 + 2n^2$

? Big O Notation for expression?

$\Rightarrow n^5 \log(n) \Rightarrow O(n^5 \log(n))$

Ex. Give Big O notation for:

$\underline{n!\, n^3} + n!\, n^2 + (n! \cdot \log(n)) + 2n^5 + 2n^4$
$+ 2n^2 \log(n)$

$\Rightarrow O(n!\, n^3)$

Big Omega Notation:

$f(x)$ is $\Omega(g(x))$ if $\exists c, k : |f(x)| \geq c|g(x)|$
for $x > k$

* "lower bound" of growth of function *

$\rightarrow$ Big O is "upper bound"

Ex. Show $n^2 - 2n + 1$ is $\Omega(n^2)$

$f(n)$ is $\Omega(g(n))$ if positive $c, k : f(n) \geq c \cdot g(n)$
for $n > k$

$\exists c \exists k \forall n (n > k \rightarrow f(n) \geq c g(n))$

Find c, k?

n	$f(n)$	$g(n)$	$\lceil g(n)/f(n) \rceil$
1	1	1	1
10	81	100	2
100	9801	10000	2

get c from $\frac{1}{c} = \lceil g(n)/f(n) \rceil$

$k = 10,\ c = \frac{1}{2}$

show $\underset{k}{n > 10} \rightarrow n^2 - 2n + 1 \geq \frac{n^2}{2} \leftarrow c$

- lowest term positive $\rightarrow n^2 - 2n + 1 \geq n^2 - 2n$
- $n > 10$ implies $-10 > -n \rightarrow$ implies $-2 > -0.2n$
- $-2 > -0.2n \Rightarrow n^2 - 2n > n^2 - 0.2n^2$

$n^2 - 2n + 1 > 0.8n^2$

$n > 10$ implies $0.8n^2 > \frac{1}{2} n^2$ ← c

By Theta Notation:

$f(x)$ is $\Theta(g(x))$ if $f(x)$ is $\Omega(g(x))$ and $f(x)$ is $O(g(x))$

$f(x)$ is $\Theta(g(x)) \leftrightarrow \exists c_1 \exists c_2 \exists k$:

: $c_1 g(x) < f(x) < c_2 g(x) : x > k$

* squeeze of $\Omega(g(x))$ and $O(g(x))$

Complexity of Algorithms:

- Time Complexity
- Space Complexity
- Best Case
- Worst Case
- Average Case

Lecture Notes: 10.15.24

Time Complexity:
- # of operations a program uses
- uses $O(N)$ and $\Theta(N)$

Basic operations:
- comparisons
- arithmetic operations → not all equal
- ignore minor details

* most interested in worst-case complexity *
→ also in average-case

* examples of algorithms in slides *
→ searching
→ sorting

* complexity terminology in slides *

P=NP? * probably not *

Modulo Arithmetic:

* make out cryptography exs in slides *

Divisibility and Modular Arithmetic:

Ex:
- $a, b \in \mathbb{Z} : a \neq 0$
- "a divides b" if $\exists c \in \mathbb{Z} : b = ac$
  $[b/a = c]$ $\Rightarrow \exists c(ac = b)$

Notations:

$a \mid b$ - "a divides b"
$a \nmid b$ - "a does not divide b

Properties:

Property	Intuition	Proof
1. if $a \mid b$, and $b \mid c$, then $a \mid b+c$	$\frac{b}{a} + \frac{c}{a} = \frac{b+c}{a}$	if $a \mid b$ & $a \mid c$, then $a \mid b+c$ • Assume integers s, t = $\frac{b}{a} = s$, $\frac{c}{a} = t$ $b = as$, $c = ta$ $b + c = as + ta$ $b + c = a(s+t)$ $\frac{b+c}{a} = \underbrace{s+t}_{\text{integer}}$
2. $a \mid b$, then $a \mid bc$ $\forall c \in \mathbb{Z}$	$\frac{b}{a} \sim \frac{b}{a} \cdot c$	$\frac{b}{a} = k \Rightarrow b = ak$ has same form of $\frac{b}{a} = c \Rightarrow b = ac$ • Multiply each side of $b = ak$ by $c \Rightarrow cb = cak$ • $\frac{cb}{a} = \underbrace{ck}_{\text{integer}}$

3. if $a|b$, $b|c$ then $a|c$ $\quad \frac{b}{a} = \frac{4}{2}$, $\frac{c}{b} = \frac{8}{4} \Rightarrow \frac{c}{a} = \frac{8}{2} = \underline{\underline{4}}$

__Proof.__ $\frac{b}{a} = t$, $\frac{c}{b} = s$

$b = at$, $c = bs$

substitute...

$c = ats \Rightarrow \frac{c}{a} = \underline{ts} \rightarrow$ integer

__Corollary.__ if a, b, c are integers, $a \neq 0$, so $a|b$ & $a|c$. Then, $a|mb+nc$ (m & n integers)

A. $\frac{b}{a} = k_1 \quad \frac{c}{a} = k_2 \mid k_1, k_2$ are integers

B. consider $mb+nc$. substitute...

$mb+nc = m(ak_1) + n(ak_2)$

C. $mb+nc = a(mk_1+nk_2)$

D. $\frac{mb+nc}{a} = mk_1 + nk_2 \leftarrow$ m, n, k_1, k_2 are all integers

__Properties of Divisibility:__

- integer divided by another integer results in a quotient and a remainder
- $a \in \mathbb{Z}$, $d = \mathbb{Z}^+$
- unique integers q, r, $0 \leq r < d$ so: $a = dq + r$
- d: divisor $\quad q$: quotient
  a: dividend $\quad r$: remainder

q: $\lfloor a/d \rfloor$

r: $a - d\lfloor a/d \rfloor$ # a mod d $\quad$? B3

__Ex.__ $31/4$ $\quad$ a = dividend, d = divisor

$$\begin{array}{r} 4\overline{)31} \\ -28 \\ \hline 3 \end{array}$$

q: $\lfloor 31/4 \rfloor = \lfloor 7.75 \rfloor = 7$

r: $a - d\lfloor a/d \rfloor = 31 - 4(7) = 3$

$a = dq + r$

Congruence Relations

def. if $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$ if $m \mid a-b \Rightarrow \frac{a-b}{m} = \text{integer}$

m: modulus

$a \equiv b \pmod{m}$: congruence

Ex. $17 \equiv 5 \pmod{6}$ since 6 divides $17-5 = 12$

$24 \not\equiv 14 \pmod{6}$ since 6 divides $24-14 = 10$ not divisible by 6

$a \equiv b \pmod{m}$ represents a function (different than $b \pmod{m} = a$)

Ex. Suppose $a, b \in \mathbb{Z}$: $a \equiv 4 \pmod{13}$ and $b \equiv 9 \pmod{13}$

Find an integer c with $0 \le c \le 12$; $c \equiv 9a \pmod{13}$

Note. $b \equiv 9 \pmod{13}$ chosen to serve as a multiplier for $c \equiv 9a \pmod{13}$ (9 comes from 1 of our 1st 2 congruences)

Soln. $p \equiv q \pmod{m}$

- $a \equiv 4 \pmod{13}$ → means a has a remainder of 4 when divided by 13
- $b \equiv 9 \pmod{13}$ → means b has a remainder of 9 when divided by 13
- multiply $4 \cdot 9 = 36$
  reduce: $36 \pmod{13} = 2$ R. 10
- possible value of $c = 10$
  $36 \equiv 10 \pmod{13}$

* congruences is preserved in multiplication

- $b \cdot a \equiv 9 \cdot 4 \pmod{13}$
  $10 \equiv 9a \pmod{13}$
  $10 \equiv 36 \pmod{13}$

then if $p \equiv q \pmod{13} \Rightarrow \frac{p-q}{m} = \frac{36-10}{13} = 2$ ✓

Lecture Notes: 10.17.24

Recap. $a \equiv b \pmod{m} \Rightarrow m \mid a-b \Rightarrow \frac{a-b}{m} = k \in \mathbb{Z}$

Note. NOT: $a \bmod m = b$

however: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

AND: Any # is congruent to its remainder mod m

Can replace original value w/ its remainder in any congruent expression

Ex: $23 \bmod 5$ | $5\overline{)23}^{4}$ R3 $23 \bmod 5 = 3$

$a = dq + r \Rightarrow 23 = 5(4) + 3$

$\Rightarrow 23 \equiv 3 \pmod{5}$

check: $\frac{23-3}{5} = 4$ integer ✓

Ex- $23+12 \equiv ? \pmod{5}$

$35 \equiv ? \pmod{5}$

Use $a \bmod m = b \bmod m$

$35 \bmod 5 = 0$

$23+12 \equiv 0 \pmod{5}$

Ex- $a \equiv 4 \pmod{13}$ $b \equiv 9 \pmod{13}$

$c \equiv 9a \pmod{13}$

$w \equiv x \pmod{m}$, $y \equiv z \pmod{m}$

$w = a$, $x = 4$, $y = c$, $z = 9a$

Preserve congruence across multiplication:

$wy \equiv xz \pmod{m}$

$ac \equiv 4 \cdot 9a \pmod{13}$

$c \equiv 36 \pmod{13}$ → $36 \bmod 13 = 10$

$10 \equiv 36 \pmod{13}$

OR

$\underline{10} \equiv 9a \pmod{13}$

← c

* can check this answer w/ both tests *

Ex: $a \equiv 4 \pmod{13}$ $b \equiv 9 \pmod{13}$

Find an integer c : $c \equiv a+b \pmod{13}$: $0 \le c \le 12$

$w \equiv x \pmod{m}$ $y \equiv z \pmod{m}$

* $w+y \equiv x+z \pmod{m}$ preserve congruence across addition

$a+b \equiv 4+9 \pmod{13} \Rightarrow a+b \equiv 13 \pmod{13}$

$13 \bmod 13 = 0 \Rightarrow 0 \equiv a+b \pmod{13}$

Check $a = 13k_1+4$ $b = 13k_2+9$

$k_1 = 2$ $k_2 = 4$

$a = 30$ $b = 61$

$91 \bmod 13 = 0$

any value of k here satisfies congruence

Ex. $a \equiv 4 \pmod{13}$ $b \equiv 9 \pmod{13}$

? c $0 \le c \le 12$: $c \equiv (2a+3b) \pmod{13}$

$w \equiv x \pmod{13}$ $y \equiv z \pmod{13}$

Find Form:

- Multiply $a \equiv 4 \pmod{13}$ by 2
  $b \equiv 9 \pmod{13}$ by 3

$2a \equiv 8 \pmod{13}$ $3b \equiv 27 \pmod{13}$

- Add $w+y \equiv x+z \pmod{13}$

$2a+3b \equiv 8+27 \pmod{13}$

$2a+3b \equiv 35 \pmod{13} \Rightarrow 35 \bmod 13 = 9$

$9 \equiv 2a+3b \pmod{13}$

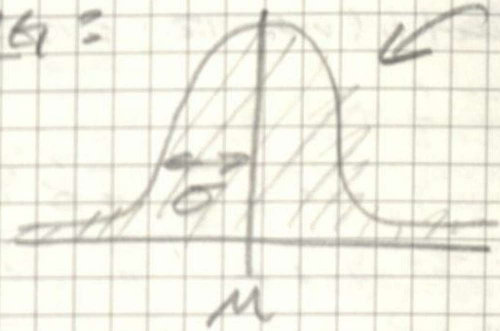
Check.

$\frac{9-(2a-3b)}{3}$ integer   The $a=30$, $b=61$

$\Rightarrow \frac{9-(2\cdot 30+3\cdot 61)}{13} = -18 \in \mathbb{Z}$ ✓

Applications:

PRNG:



w_1 neural network weights
w_2
w_3

Linear Congruential Recurrence Relation:

$$x_{n+1} = (a x_n + c) \bmod m$$

multiplier increment modulus

x_0 = seed $\quad 0 \le a \le m$

$x_0 < m \quad 0 \le c \le m$

* generates pseudo random numbers

Mersenne Twister

Lecture Notes: 8.29.24

Representation of Integers:

Typically use base 10 (decimal)

Also use base 2 (binary)
base 16 (hexadecimal)

* base 2 works/has worked very well with physical devices

Base Conversions:

Ex. convert 89 to base 2

$89 \div 2 = 44 \text{ r } 1 \leftarrow 2^0$
$44 \div 2 = 22 \text{ r } 0 \leftarrow 2^1$
$22 \div 2 = 11 \text{ r } 0 \leftarrow 2^2$
$11 \div 2 = 5 \text{ r } 1 \leftarrow 2^3$
$5 \div 2 = 2 \text{ r } 1 \leftarrow 2^4$
$2 \div 2 = 1 \text{ r } 0 \leftarrow 2^5$
$1 \div 2 = 0 \text{ r } 1 \leftarrow 2^6$

1011001

2^6 2^0

$1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + \dots$

<u>Ex.</u> 202_{10} in base 3?

$202 \div 3 = 67$ r 1

$67 \div 3 = 22$ r 1

$22 \div 3 = 7$ r 1

$7 \div 3 = 2$ r 1

$2 \div 3 = 0$ r 2

$21111_3 = 202_{10}$

$2 \cdot 3^4 + 1 \cdot 3^3 + 1 \cdot 3^2 + 1 \cdot 3^1 + 1 \cdot 3^0$

* Base b (arbitrary) representation in slides + written out algorithm

<u>Prime</u>:

$p \in \mathbb{Z}$ only divisible by 1 and p

<u>Fundamental Theorem of Arithmetic</u>:

every positive integer can be represented as a product of primes

<u>Ex.</u> prime factorization of 332?

$332 / 2 = 166$

$166 / 2 = 83$

$332 = 2 \cdot 2 \cdot 83$
$= 2^2 \cdot 83$

* there is one <u>one</u> unique prime factorization for any number *

* written in ascending order of primes *

<u>Ex.</u> Show n is prime:

if $n \in \mathbb{Z}$ is a composite integer then n is going to have a prime divisor that is $\leq \sqrt{n}$

$n = 18$; $\sqrt{18} \approx 4.24 \Rightarrow 2 \cdot 3 \cdot 3$ all $\leq \sqrt{n}$

<u>Proof</u>: composite # $n = a \cdot b$

$n = ab$ where $\begin{cases} 1 < a < n \\ 1 < b < n \end{cases}$

set up proof by contradiction (n has prime divisor $\leq \sqrt{n}$)

Assume: $a > \sqrt{n}$, $b > \sqrt{n}$

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

define as $n > n$ $\quad n > n$

contradiction (product should exceed n)

@ least a or b must be $\leq \sqrt{n}$

Proceed w/ trial divisor for all #'s $\le \sqrt{n}$
if none of prime #s $\le \sqrt{n}$ divide n,
<u>n is prime</u>

<u>Ex.</u> 2503 – is it prime
$\sqrt{2500} = 50$ – test #'s less than 50
is 2503 divisible by:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47
no — 2503 is prime
* prime number theorem in slides *
<u>Greatest Common Divisor</u>:
largest integer d where d/a and d/b
where $a, b \in \mathbb{Z}$ and not 0
<u>Relatively Prime</u>: $a, b \in \mathbb{Z}$ if $\gcd(a, b) = 1$
<u>Pairwise relatively prime</u>:
$a_1, a_2, \ldots a_n \in \mathbb{Z}$ if all combinations (tuples)
of $\gcd() = 1$
<u>Ex.</u> is 13, 33, 42 pairwise relatively prime
$\gcd(13, 33) = 1$
$\gcd(33, 42) = 3$ ✗ } <u>no</u>
$\gcd(13, 42) = 1$
<u>Using prime factorizations to find GCD:</u>
$\gcd(a, b)$: PF: $a: p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_n^{a_n}$
$b: p_1^{b_1} \cdot p_2^{b_2} \cdot p_3^{b_3} \cdots p_n^{b_n}$
$a.\ 1680: 2^4 \cdot 3 \cdot 5 \cdot 7$
$b.\ 11220: 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 17$ $\quad$ gcd: $2^2 \cdot 3^1 \cdot 5^1$
$= 60$
$\gcd(a, b)$: $p_1 = 2 \mid p_1^{\min(a_1, b_1)} = 2^2$
$p_2 = 3 \mid p_2^{\min(1,1)} = 3^1$
$= 5^1$

Using PF to find LCM:

same algorithm but take maximum exponent

$p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdot \ldots$

$1680: 2^4 \cdot 3 \cdot 5 \cdot 7 = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0 \cdot 17^0$

$11220: 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 17 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1 \cdot 17^1$

$\text{lcm}(1680, 11220) = 2^4 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1 \cdot 17^1$

$= 2199120$

* general algorithms of flows in slides *

$a, b \in \mathbb{Z}^+ \Rightarrow ab = \gcd(a,b) \cdot \text{lcm}(a,b)$

Euclidean Algorithm:

$\gcd(a, b) = \gcd(a, c)$ when $a > b$ and c is remainder of $a \div b$

ex $\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$

* can find $\gcd(a, b)$ without using PFs

$d \mid a$; $a = q \cdot d + r$; 287, 91

divisor dividend $q: \lfloor a/d \rfloor = \lfloor 287/91 \rfloor = 3$

$r: a - d\lfloor a/d \rfloor = 287 - 91(3) = 14$

$a, d, q, r \in \mathbb{Z}$

$\gcd(a, d) = \gcd(d, r)$

⋮ * more examples/generalizations in slides and written notes

once $r = \emptyset$ algorithm is done

Lecture Notes: 10.31.24

* Ex/Application of RSA Encryption in Wireless *

Recap. Euclidean Alg for GCD

$gcd(287, 91)$

$a = d \cdot q + r \Rightarrow 287 = 91 \cdot q + r$

$q = \lfloor a/d \rfloor = 3$

$r = a - d(q) = 287 - 91 \cdot 3 = 14$

idea. $gcd(a,d) = gcd(d,r)$

$gcd(91, 14)$

$91 = 14 \cdot q + r \Rightarrow q = 6, r = 7$

$gcd(91, 14) = gcd(14, 7)$

$a = qd + r \Rightarrow 14 = 7 \cdot q + r$

$q = 2, r = \emptyset$ (once $r = \emptyset$, done)

gcd = 'r' of previous step

$gcd(287, 91) = 7$

Why?

* Any divisor of 287, 91 must also be divisor of 14

$a = dq + r$

$287 - 91 \cdot 3 = 14 \Rightarrow 287 - 91 \cdot 3 = 14$

multiply each term by integer k:

$287k - 91(3)k = 14$ if $k = 1$

$287(2) - 91(3)(2) = \underline{28}$ if $k = 2$

multiples of 14

$ak - dqk = r$

$k(a - dq) = r$

$a - dq = r/k$ integer

* Any divisor of 91, 14 also divisor of 287

$a = dq + r$

$287 = 91q + r$

$287 = 91qk + rk$

$= k(91q + r)$

$\frac{287}{k} = 91qr$ integer

* $\gcd(287, 91) =$
$\gcd(91, 14) =$
$\gcd(14, 7) =$
$\vdots$

Aside: $\gcd(17, 10)$

$17 = 10 \cdot q + r$; $q = 1, r = 7$

$\gcd(10, 7)$

$10 = 7 \cdot q + r$; $q = 1, r = 3$

$\gcd(7, 3)$

$7 = 3 \cdot q + r$; $q = 2, r = \underline{1}$

$\gcd(3, 1)$

$3 = 3 \cdot q + r$; $q = 3$, $r = \emptyset$

$\gcd(17, 10) = 1$ ✓

* gcd of ints a, d can be expressed in

Form: $sa + td$ Bézout's Theorem

integer coefficients

s, t : Bézout Coefficients

Ex: $\gcd(6, 14) = 2$

$2 = (-2)(6) + (1)(14)$

Bézout Coefficients: $s = -2, t = 1$

* NOT unique *

How do we Systematically Find Be'zout Coeff?

Step 1. Apply Euclidean Alg to find GCD

Ex. gcd(252, 198) =

$a = dq + r \Rightarrow 252 = 198q + r \Rightarrow q = 1, r = 54$

gcd(198, 54) =

$a = dq + r \Rightarrow 198 = 54q + r \Rightarrow q = 3, r = 36$

gcd(54, 36) =

$a = dq + r \Rightarrow 54 = 36q + r \Rightarrow q = 1, r = 18$

gcd(36, 18) =

$a = dq + r \Rightarrow 36 = 18q + r \Rightarrow q = 2, r = 0$

gcd(252, 198) = 18

Step 2. Work Backwards to find Be'zout Coeff

goal: Express 18 as a linear combination of 252, 198

$18 = s(252) + t(198) \Rightarrow s, t = ?$

Recall. $54 = 36(1) + 18 \Rightarrow$ solve for 18

$18 = 54 - 36(1)$

Recall. $198 = 54(3) + 36 \Rightarrow$ solve for 36 substitute

$36 = 198 - 54(3)$

$18 = GCD = 54 - (198 - 54(3))(1)$

* do not express as single number! *

$18 = 54(4) - 198$

Recall, $252 = 198 \cdot 1 + 54 \Rightarrow$ solve for 54, substitute

$54 = 252 - 198(1)$

$18 = 4(252 - 198(1)) - 198$

$18 = \underset{s}{4}(252) - \underset{t}{5}(198)$

$s = 4 \qquad t = -5$

Ex. Express gcd(273, 94) as linear combo of 273, 94

gcd(273, 94) $\quad$ gcd(94, 85) $\quad$ gcd(85, 9)

$273 = 94(2) + 85 \quad 94 = 85(1) + 9 \quad 85 = 9(9) + 4$

gcd(9, 4) $\quad$ gcd(4, 1) $\quad$ relatively prime!

$9 = 4(2) + 1 \quad 4 = 4(1) + 0$

Start Here:

$9 = 4(2) - 1 \Rightarrow 1 = 9 - 4(2)$

$85 = 9(9) + 4 \Rightarrow 4 = 85 - 9(9)$

$1 = 9 - (85 - 9(9))(2)$

$= 19(94) - 21(83)$

$85 = 273 - 94(2)$

$1 = 19(94) - 21(273 - 94(2))$

$1 = 61(94) - 21(273)$

$s = 61 \qquad t = -21$

Solving Linear Congruences:

Form. $ax \equiv b \pmod{m}$; $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, $x \in$ variable

Goal. values of x that satisfy congruence

Theorem. a, m are relatively prime and $m > 1$,

- then inverse of a mod m exists
- unique integer $\bar{a}$ (inverse) $< m$ that is inverse of a mod m ...

... AND every inverse of a (mod m) is congruent to $\bar{a}$ (mod m)

How to find inverse $\bar{a}$?

1. Use Euclidean alg to show a, m are relatively prime
2. Find Bézout coeff s, t: $sa + tm = 1$
3. coefficient s is inverse of a mod m

Ex- inverse of 9 mod 23

1. $23 = 9(2) + 5$
   $9 = 5(1) + 4$
   $5 = 4(1) + 1$
   $4 = 4(1) + 0$
   $\gcd(23, 9) = 1$

$1 = 5(1) - 4(1)$
$1 = 5(1) - 9(1) + 5(1)$
$= 5(2) - 9(1)$
$1 = (23(1) - 9(2))(2) - 9(1)$
$= 23(2) - 9(3)$
$1 = \underbrace{-5}_{s}(9) + \underbrace{2}_{t}(23)$

inverse $\bar{a} = -5$

not complete solutions

$-5, -5 + 23, -5 + 23(2) \ldots$

$-5 + 23k \quad \forall k \in \mathbb{Z}$

Congruence:

$(9)(-5 + 23k) \equiv 1 \pmod{23}$

$k = 0: -45 \equiv 1 \pmod{23}$

$\frac{-45 - 1}{23} = -2 \rightarrow \in \mathbb{Z}$

$k = 2: \frac{369 - 1}{23} = 16$

$p \equiv q \pmod{n} \Rightarrow \frac{p - q}{n} \in \mathbb{Z}$ ✓

Solve lin congruence of form $ax \equiv b \pmod{m}$

$9x \equiv 15 \pmod{23}$

1. find inverse of congruence $9 \equiv 1 \pmod{23}$

$\bar{a} = -5$

2. $9 \cdot (-5) \equiv 1 \pmod{23}$

multiply each side by $b = 15$

$a \cdot \bar{a} \cdot b \equiv b \pmod{m}$

$a \cdot x \equiv b \pmod{m}$

solution of x : $x = \bar{a} \cdot b$

$x = -5 \cdot 15 = -75$ possible solution

$9 \cdot (-5)(15) \equiv 15 \pmod{23}$

$-675 \equiv 15 \pmod{23}$ $\Rightarrow \frac{-675 - 15}{23} = -30 \in \mathbb{Z}$

General Solution :

$\bar{a}b + km \Rightarrow -5(15) + 23k = -75 + 23k$

$\forall k \in \mathbb{Z}$

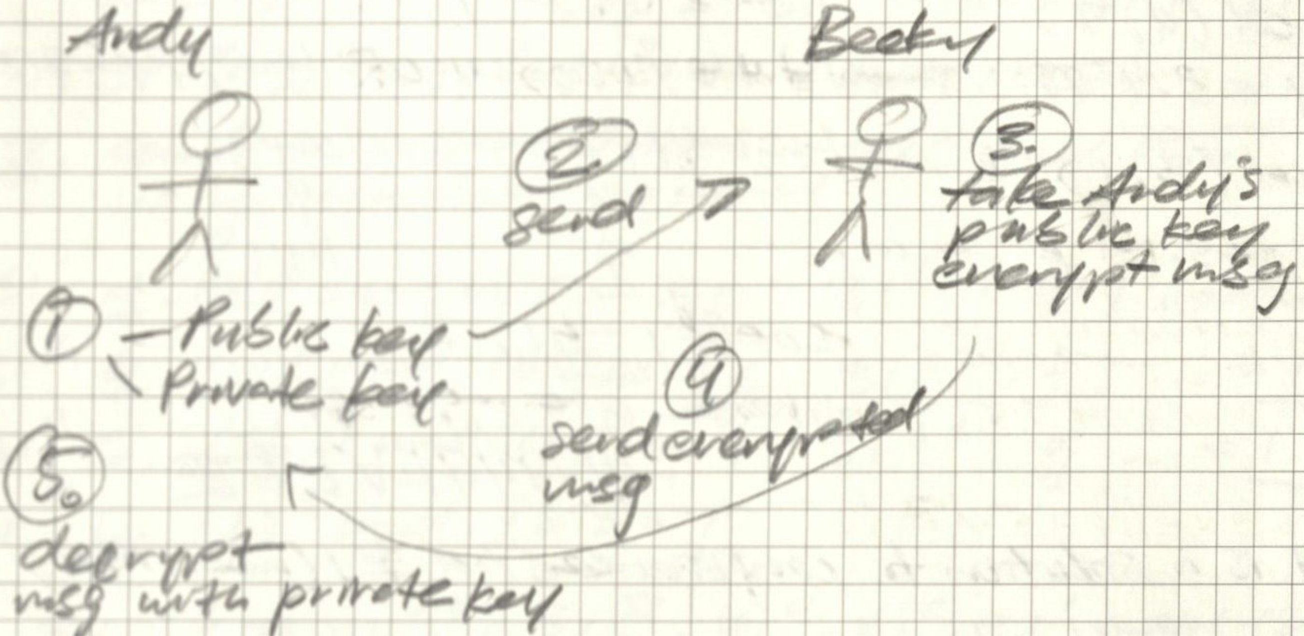
$9x \equiv 15 \pmod{23}$

Lecture Notes: 11.5.24

RSA Encryption:

Exploits — hard to factor the product of large prime numbers

exs. — ssh login



1. How do we generate public, private keys?
   - Start with 2 prime #s: $p = 5$, $q = 37$
   - Compute $p \cdot q$: $p \cdot q = 185$
   - Calculate $(p-1)(q-1)$: $(4)(36) = 144$
   - Choose #e b/w $1 < e < (p-1)(q-1)$
     ↳ e and 144 must be relatively prime

$e = 7$; Public key: e, $p \cdot q = N \Rightarrow 7, 185$

Generate Private Key: Solve Linear Congruence

$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$

public key

$7d \equiv 1 \pmod{144}$

private key

A. Find GCD(144, 7)

$144 = 7 \cdot q + r$

$144 = 7(20) + 4$

gcd(7, 4)

$7 = 4 \cdot q + 3$

gcd(4, 3)

$4 = 3 \cdot 1 + 1$

gcd(3, 1)

$3 = 3 \cdot 1 + \underline{0}$

B. Linear Combo

- $4 = (3)(1) + 1$ OR $1 = 4 - 3(1)$
- $7 = 4(1) + 3$ OR $3 = 7 - 4(1)$

$1 = 4 - [7 - 4(1)](1)$

$1 = 2(4) - 7$

$144 = 7(20) + 4$ OR $4 = 144 - 7(20)$

$1 = -41(7) + 2(144)$

$\uparrow$ 7 $\qquad \uparrow$ 144

coeff: $\underline{-41}$, 2

inverse $\bar{a} = -41$ OR

$-41 + 144k \ \forall k \in \mathbb{Z}$

-41 is a solution to congruence $7 \cdot d \equiv 1 \pmod{144}$

$\frac{7 \cdot (-41) - 1}{144} = -2 \in \mathbb{Z}$ (int) ✓

if $k = 1$, $-41 + 144(1) = 103$ ← private key

What if I could factor $p \cdot q$?

- calculate $p-1$, $q-1$
- reverse entire process

Encrypt Message M: $f(M) = M^e \pmod{N}$

$M = 6 \quad f(6) = 6^7 \pmod{185} = 31$

Decrypt: Message C: $f(C) = C^d \pmod{N}$

$C = 31 \quad f(31) = 31^{103} \pmod{185}$

$31^{103} \pmod{185}$

use fast modular exponentiation algorithm

1. Convert exponent 103_{10} to base 2

$103_{10} = \underset{64\ 32\ 16\ 8\ 4\ 2\ 1}{1100111}_2$

Tells us: $31^{103} = 31^{64} \cdot 31^{32} \cdot 31^{4} \cdot 31^{2} \cdot 31^{1}$

$31^{64} \cdot 31^{32} \cdot 31^{4} \cdot 31^{2} \cdot 31^{1} \pmod{185}$

2. compute relevant powers of 31^x mod 185 using repeated squaring

31^1 A. $(31)^1$ mod $185 = \underline{31}$ $\quad 31^{16}$: e 1^2 mod $\_ = 1$

31^2 B. $(31)^2$ mod $185 = \underline{36}$ $\quad 31^{32}$: f $\ldots = \underline{1}$

31^4 C. $(36)^2$ mod $185 = 1$ $\quad 31^{64}$: g $\ldots = \underline{1}$

31^8 D. $(1)^2$ mod $185 = \underline{1}$

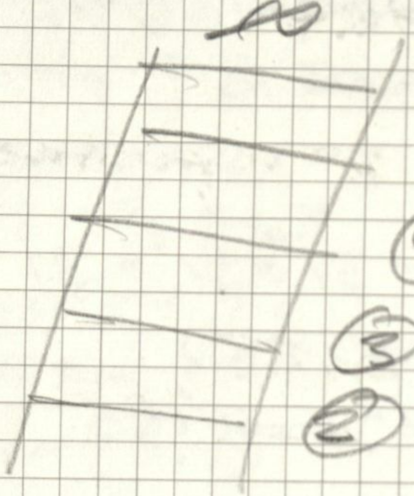
$31^{103} = 31^{64} \cdot 31^{32} \cdot 31^{4} \cdot 31^{2} \cdot 31^{1}$ mod 185

$= 1 \cdot 1 \cdot 1 \cdot 36 \cdot 31$ mod 185

$= 1116$ mod 185

$= 6$

Mathematical Induction:



① Infinitely long ladder

④ can reach an extra rung

③ Show, can reach next (kth) rung

② can reach rung 1 of ladder

⑤ Show, verify, $P(1)$ is TRUE

Show, $P(n)$ is TRUE for all pos integers n

⚠ only use to prove formulas obtained from other means...

$$1+2+3+4+\dots \quad n = \frac{n(n-1)}{2}$$

use induction to prove formula holds

MI

2-step proof process:

① Basis step

② Induction step

1. Basis step: prove $P(1)$ is TRUE
2. Induction step: show conditional $P(k) \Rightarrow P(k+1) \ \forall K$

- Assume $P(k)$ = TRUE for arbitrary int K
- Show $P(k+1)$ must also be TRUE
- Assume $P(K)$ = TRUE — Inductive Hypothesis (IH)
- Show $\forall k \in \mathbb{Z}^+ \left(P(k) \rightarrow P(k+1)\right)$
- Rule of inference: $\left(P(1) \land \left(P(k) \rightarrow P(k+1)\right)\right) \Rightarrow \forall n P(n)$

"if $P(k)$ is true, $P(k+1)$ also assumed true"...

Ex- show that if n is positive:

$$1+2+\dots+n = \frac{n(n+1)}{2} \leftarrow \text{given}$$

$P(n)$ is proposition that sum of 1^{st} n positive integers is $\frac{n(n+1)}{2}$

① Show $P(1)$ is TRUE

② Show conditional statement $P(k)$ implies $P(k+1)$ is TRUE $\forall k \in \mathbb{Z}^+$

1. $P(1)$ is TRUE b/c $P(1) = \frac{1(1+1)}{2} = 1$

2. IH: Assume $P(k)$ holds for arbitrary $k \in \mathbb{Z}^+$

$$\therefore 1+2+3+\dots+k = \frac{k(k+1)}{2}$$

w/ this assumption, show $P(k+1)$ is TRUE...

$$\therefore 1+2+\dots+k+(k+1) = \frac{(k+1)((k+1)+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

- Add $k+1$ to both sides of $P(k)$ equation:

$$1+2+3+\dots+k+(k+1) \overset{IH}{=} \frac{k(k+1)}{2}+\underline{(k+1)}$$

Show: $\frac{k(k+1)}{2}+(k+1) \overset{?}{=} \frac{(k+1)(k+2)}{2}$

$$\Rightarrow \frac{k(k+1)}{2}+\frac{2(k+1)}{2} \overset{\checkmark}{=} \frac{(k+1)(k+2)}{2}$$

$\therefore$ $P(k+1)$ is TRUE under assumption that $P(k)$ is TRUE $\Rightarrow$ completes induction step

$\therefore$ Proves $1+2+\dots+n = \frac{n(n+1)}{2}$ $\forall n$

Ex. Prove that

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

TRUE $\forall n \in \mathbb{Z}^+$

① $P(1) = 1^3 = \left(\frac{1(1+1)}{2}\right)^3 = \left(\frac{2}{2}\right)^3 = 1$ ✓

②

③ For some positive int k,

$1^3 + 2^3 + \dots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$

④ Show $P(k+1)$ holds

$1^3 + 2^3 + \dots + k^3 + (k+1)^3 = \left(\frac{(k+1)(k+2)}{2}\right)^2$

⑤ Add $(k+1)^3$ to both sides of (3)

Show $\left(\frac{(k)(k+1)}{2}\right)^2 + (k+1)^3 \stackrel{?}{=} \left(\frac{(k+1)(k+2)}{2}\right)^2$

$\Rightarrow \left(\frac{k(k+1)}{2}\right)\left(\frac{k(k+1)}{2}\right) + (k+1)(k+1)(k+1)$

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

$\Rightarrow \frac{(k+1)^2\left[k^2 + 2^2(k+1)\right]}{2^2} = \frac{(k+1)^2(k^2+4k+4)}{2^2}$

$= \frac{(k+1)^2(k+2)^2}{2^2} = \left(\frac{(k+1)(k+2)}{2}\right)^2$ ✓

Find a formula for:

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\dots+\frac{1}{n(n+1)}$$

$\frac{1}{n(n+1)}$ if $n=1$: $\frac{1}{1\cdot 2}=\frac{1}{2}$ ← $\frac{n}{n+1}$

if $n=2$: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}=\frac{1}{2}+\frac{1}{6}=\frac{2}{3}$ ← $\frac{n}{n+1}$

if $n=3$: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}=\frac{9}{12}=\frac{3}{4}$

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\dots+\frac{1}{n(n+1)}=\frac{n}{(n+1)}$$

Prove this holds:

Basis Step: $n=1$ $\frac{1}{n(n+1)}=\frac{1}{1\cdot 2}=\frac{1}{2}$ ✓

Assume for $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{n(n+1)}=\frac{n}{n+1}$

is TRUE if $n=k$

Add $\frac{1}{(k+1)(k+2)}$ to both sides of expression:

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\dots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}=\frac{k}{(k+1)}+\frac{1}{(k+1)(k+2)}$$

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

$$=\dots=\frac{(k+1)(k+1)}{(k+1)(k+2)}=\frac{k+1}{k+2}$$ ✓

Lecture Notes: 11-7-24

Ex. use MI to prove 3 divides n^3+2n $\forall n \in \mathbb{Z}^+$

Basis Step: $P(1) = (1)^3 + 2(1) = 3 \Rightarrow 3 \mid 3$

sub 1 for n

basis step works

Inductive Step: Assume 3 divides k^3+2k $\forall k \in \mathbb{Z}^+$

$\exists l \in \mathbb{Z} : 3l = k^3+2k \Rightarrow l = \frac{k^3+2k}{3} \in \mathbb{Z}$

$P(k+1) = (k+1)^3 + 2(k+1)$

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

$= k^3 + k^2 + 2k^2 + 2k + k + 1 + 2k + 2$

$= k^3 + 3k^2 + 3k + 2k + 3$

$= (k^3+2k) + 3k^2 + 3k + 3$

$= \underbrace{(k^3+2k)}_{\text{IH - Assumed divides by 3}} + \underbrace{3(k^2+k+1)}_{\text{Multiple of 3 is divisible by 3}}$

3 divides $(k+1)^3 + 2(k+1)$ by MI

Quasi-Proof why MI works:

- Suppose we know $P(1)$ is TRUE $\wedge$ $P(k) \to P(k+1)$ is TRUE $\forall k \in \mathbb{Z}^+$
- Show $P(n)$ is TRUE $\forall n \in \mathbb{Z}^+$
  $\to$ Assume for 1 pos int, $P(n)$ is FALSE
- $S = \mathbb{Z}^+ : P(n) = F \neq \emptyset$
- $m \in S$, $m \in \mathbb{Z}$: $P(m) = F$
- $m \neq 1$ b/c $P(1) = T$
- $m > 0 \Rightarrow m > 1 \Rightarrow m-1 \in \mathbb{Z}^+$ since $P(m-1) = T$

- $P(m-1) \Rightarrow P(m)$ is T
- $P(m)$ must be T $\Rightarrow$ arrived at contradiction

Recursively Defined Sets and Functions:

eg. powers of 2:

$a_0 = 1$

$a_{n+1} = 2 \cdot a_n \quad \forall n \in \mathbb{Z}$

Ex.

Recurrence Relation: $p_n = 2p_{n-1} + 3$: $p_1 = 2$

closed form: $p_n = 5n - 3$ ... is this valid?

$p_1 = 2$ | $p_1 = 2$

$p_2 = 2p_1 + 3 = 7$ | $p_2 = 5 \cdot 2 - 3 = 7$

$p_3 = 2p_2 + 3 = 17$ | $p_3 = 5 \cdot 3 - 3 = 12$

$p_4 = 37$ | $p_4 = 17$

does not match

Can use MI to see if it holds for all n

Basis case: if $n = 1$ recurrence relation: 2
closed form: 2 ✓

IH: $P_k = 5k - 3$

show it gives correct value for P_{k+1}

$P_n = 2P_{n-1} + 3$

$P_k = 2P_{k+1-1} + 3 = 2P_k + 3 \overset{IH}{=} 2(5k-3) + 3$

$= 10k - 3 \neq 5k - 2$

IH fails ... does not hold $\forall n \in \mathbb{Z}$

Recursively Defined Functions:

2 steps: to define recursive function for $\mathbb{Z}^+$

BASIS STEP: specify initial value

(ex. f_1, f_2 defined prior)

Recursive step: rule to find value of function at index n for smaller vals/indices

Ex. Give recursive def of a^n: $a \neq 0 \in \mathbb{R}$, $n \in \mathbb{Z}^+$

Base Case: $a_0 = 1$

Recursive case: $a \cdot a_0$

Ex. recursive def of $\sum_{k=0}^{n} a_k$

1. Basis: $\sum_{k=0}^{0} = a_0 = a_0$

2nd. $\sum_{k=0}^{n+1} a_k = \left(\sum_{k=0}^{n} a_k\right) + a_{n+1}$

Ex. $f(n) = -f(n-1)$: $n \geq 1$, $f(0) = 1$

Valid? - given $f(0)$

- each subsequent value defined by previous

$f(0) = 1$, $f(1) = -f(1-1) = -f(0) = -1$ ✓

$f(2) = -f(2-1) = -f(1) = -(-1) = 1$

Conjecture: $f(n) = (-1)^n$

TRUE: $n = 0 \Rightarrow (-1)^0 = 1$ ✓

TRUE: $n = k \Rightarrow f(k+1) = -f(k+1-1) = -f(k)$ ✓

$-f(k) = (-)(-1)^k$ by IH

$f(k+1) = (-1)^{k+1}$

OR

$(-1)^k(-1)^1 =$ ✓

Ex. $\underbrace{f(n) = 2f(n+1)}_{\text{not well formed/def}} : n \geq 2, \underbrace{f(0) = 0, f(1) = 1}_{\text{init cond}}$

$f(2) = 2f(2+1) = 2f(3)$

but no $f(3)$ so impossible to calculate

Ex. $f(n) = 2f(n-1) : n \geq 1, f(0) = 1, f(1) = 1$

$f(n) = 2f(n-1)$

$f(1) = 2f(1-1) = 2f(0) = 2 \cdot 1 = 2$ do not match

$\therefore$ not well formed

Recursively Defined Sets:

How? like functions → 2 steps:

Basis Step

Recursive Step

1. BS: specify initial elements of set
2. RS: rules to define set elements from known elements

include exclusion rules

Ex. Subset S defined by:

Basis: $3 \in S$

Recursive Step: if $x \in S$, $y \in S$, then $(x+y) \in S$

1st. $S = \{3\}$

$S = \{3, 6\}$

2nd: $S = \{3, 6, 9, 12\}$

Ex. recursively define set of pos ints powers of 5

Basis: $5 \in S$

Recursive: $n \in S \Rightarrow 5 \cdot n \in S$

1st. $\{5, 25\}$

2nd. $\{5, 25, 5 \cdot 5, 5 \cdot 25, \ldots\}$

Ex. recursively define set of pos ints not divisible by 5

Basis Step: $1 \in S, 2 \in S, 3 \in S, 4 \in S$

$S = \{1, 2, 3, 4\}$

Recursive Step: $x \in S \Rightarrow x + 5 \in S$

1st. $\{1, 2, 3, 4, 6, 7, 8, 9\}$

2nd. $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14\}$

Exam 2 Review: 11.11.24

Proof by Contraposition: $p \to q \equiv \neg q \to \neg p$

- Assume $\neg q$ is TRUE
- Show $\neg p$ must also be TRUE

Proof by Contradiction:

- Assume $\neg q$ is TRUE
- Reach a contradiction
  - violation of a theorem or axiom
  - contradiction w/ given assumption or fact
  - situation where something is both T & F
- Conclude since $\neg q$ leads to a contradiction, q must be TRUE

Proving Bi-Conditionals:

to show $p \leftrightarrow q$, prove $p \to q \wedge q \to p$

Proof by Cases, Proof by Exhaustion

Sets: unordered collections of objects

$a \in A \to$ set $\quad a \notin A$

↳ element/member ↳ not an element of

Roster Method:

$S = \{a, b, c, d\} = \{b, c, c, d, a\}$ ↳ order/repetition not counted

$S = \{a, b, c, \ldots, z\}$

↳ can use ellipses

$\mathbb{N}$: natural numbers $= \{0, 1, 2, 3, \ldots\}$

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

$\mathbb{Z}^+$: positive integers $= \{1, 2, 3, \ldots\}$

$\mathbb{R}$: real numbers

$\mathbb{R}^+$: positive real numbers

$\mathbb{C}$: complex numbers

$\mathbb{Q}$: rational numbers

Set-Builder Notation:

$S = \{x \mid x \in \mathbb{Z}^+ \wedge x < 100\}$

$S = \{x \mid P(x)\}$

↳ previously defined predicate

Interval Notation: $[a,b], [a,b), (a,b], (a,b)$

Universal Set: $U = \{\text{everything under observation}\}$

Empty Set: $\emptyset = \{\}$

* Sets can be elements of sets *

$\emptyset \neq \{\emptyset\}$

Set Equality: $A = B \leftrightarrow \forall x (x \in A \leftrightarrow x \in B)$

* does not have to be in the same order

Subsets: $A \subseteq B \leftrightarrow \forall x (x \in A \rightarrow x \in B)$

Proper Subsets: $A \subset B \leftrightarrow A \subseteq B \wedge A \neq B$

Set Cardinality: $|A|$

amount of elements in set A

finite, countably infinite, or uncountably infinite

Power Sets: $P(A)$

set of all subsets of A

$A = \{a, b\} \rightarrow P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

$|A| = n \rightarrow |P(A)| = 2^n$

Tuples: (a, b)

ordered n-tuple: $(a_1, a_2, a_3, \dots, a_n)$

* two n-tuples are equal iff all their corresponding elements are equal

Cartesian Product

$A \times B = \{(a,b) \mid a \in A \land b \in B\}$

* set of all ordered pairs of elements in A and B *

$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n \mid a_i \in A_i \text{ for } i = 1, 2, \ldots n\}$

Union: $A \cup B = \{x \mid x \in A \lor x \in B\}$

Intersection: $A \cap B = \{x \mid x \in A \land x \in B\}$

Compliment: $\overline{A} = \{x \in U \mid x \notin A\}$

Difference: $A - B = \{x \mid x \in A \land x \notin B\}$

* set operations are communicative, associative, and distributive *

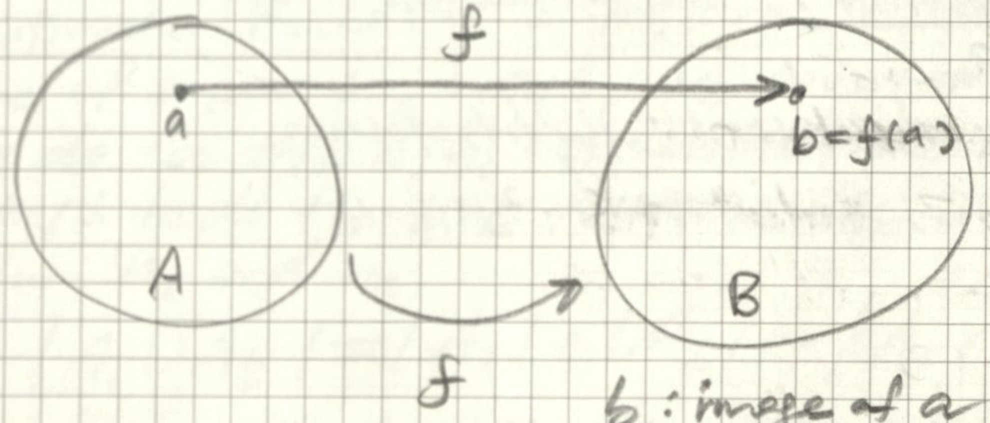
De Morgans: $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$

Absorbtion: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$

Complementation: $A \cup \overline{A} = U$, $A \cap \overline{A} = \emptyset$

Functions: $f : A \to B$

maps elements from set A to set B



b: image of a under f

A: domain of f   a: preimage of b

B: codomain of f   range: set of all images

* 2 functions are equal when they have the same domain, codomain, and map each element of the domain to the same element of the codomain *

<u>injection</u>: '1-to-1' function
each element of A maps to <u>only</u> one element of B
$f(a) = f(b) \rightarrow a = b \ \forall a, b \in U(f)$

<u>surjection</u>: 'onto' function
all elements of B are mapped to an element of A
$\forall x \in U(f) \rightarrow b \in B \leftrightarrow a \in A$

<u>bijection</u>: both an injection and a surjection

* inverse functions only exist for bijections! *

* function composition *
$f \circ g(x) = f(g(x))$

<u>Sequence</u>: ordered list of elements

<u>Geometric</u>: $a, ar, ar^2, \ldots, ar^n$

<u>Arithmetic</u>: $a, a+d, a+2d, \ldots, a+nd$

<u>Recurrence Relation</u>: sequence a_n in terms of some a_{n-m}

- forward vs. backward substitution
- closed-form solutions

Lecture Notes: 11.12.24

Idea: Assume set of objects w/ certain properties
→ Counting is used to determine the number of these objects

ex. poker - Flop: 5H, 8H, 7H
You: 8c, 8s
Me: ?

Product Rule: procedure w/ 2 tasks solved in n_1 and n_2 ways respectively
→ possible combos: $n_1 n_2$ ways

sets: $|A_1 \times A_2 \times \dots \times A_n| = |A_1| \times |A_2| \times \dots \times |A_n|$

ex. seats in theatre: $\frac{\text{letter}}{A-Z} \cdot \frac{\#}{1-50} = 26 \times 50 = 1300$

Sum Rule: Task can be done in 1 of n_1 ways or 1 of n_2 ways (none of the n_1 ways are the same as n_2 ways)
→ there are $n_1 + n_2$ ways to do the task

set: $|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$

Subtraction Rule: if a task can be done in one of n_1 or n_2 ways, the total # of ways to do the task is $n_1 + n_2$ minus the # of ways to do the task that are the same b/w n_1 and n_2

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

⚠ consider overlapping elements

Ex- # of bitstrings of length 8 that start with 1 or end w/ 00

- Start w/ 1?

$$\underline{1}\ \underbrace{\_\ \_\ \_\ \_\ \_\ \_\ \_}_{7 \text{ slots} \sim 2^7 \text{ possible combinations}}$$

- end w/ 00?

$$\underbrace{\_\ \_\ \_\ \_\ \_\ \_}_{6 \text{ slots} \sim 2^6 \text{ possible combinations}}\ \underline{0}\ \underline{0}$$

- catch overlap

$$\underline{1}\ \underbrace{\_\ \_\ \_\ \_\ \_}_{5 \text{ slots} \sim 2^5 \text{ duplicates}}\ \underline{0}\ \underline{0}$$

$\Rightarrow 2^7 + 2^6 - 2^5 = 128 + 64 - 32 = 160$

Ex- How many bit strings are there of length 6 or less, not counting the bit string

↳ Solve w/ empty string

$2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6$

Use geo progression formula

↳ $2^7 - 1$ ← subtract empty string

How many positive ints b/w [1000, 9999]

1. Are divisible by 9?
2. Are even?
3. Have distinct digits?

Figure out total #'s:

$9999 - 1000 + 1 = 9000$ #'s to consider

1. $9000/9 = 1000$
2. $9000/2 = 4500$
3. _ _ _ _   8   7 $9 \cdot 9 \cdot 8 \cdot 7 = 4536$

9 choices (can't be 0)   9 choices (can't be same as 1st digit — can be 0)

Ex: how many ways can a photographer arrange 6 people in a row from a group of 10 ppl if:

1. bride must be in picture
2. bride and groom must be in picture
3. bride or groom is in picture

1. bride can be in 6 slots:
but 10 people in picture:

$$\underbrace{(9 \cdot 8 \cdot 7 \cdot 6 \cdot 5)}_{\text{5 other pple}} \cdot 6 = 90720$$

↓ positions for bride

2. bride in 1 of 6 slots
groom in 1 of 5 remaining slots

$$(8 \cdot 7 \cdot 6 \cdot 5) \cdot 6 \cdot 5 = 50400$$

40320 //

3. # of ways for just bride: $90720 - 50400$
true for groom as well - by symmetry
$\therefore 40320 + 40320$ for 1 of either

Pigeonhole Principle:

Ex. What is the minimum # of students, each coming from 1 of the 50 states, to guarantee that are at least 100 from the same state

- minimum objects N s.t. @ least r of those objects must be in @ least 1 of k boxes

$$N = k(r-1)+1$$

$k = 50$, $r = 100$, $N = ?$

$$N = 50(100-1)+1 = 4951$$

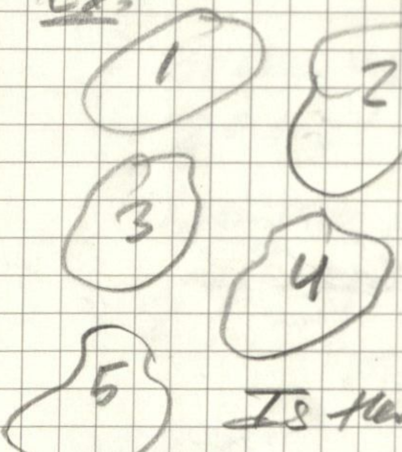
Lecture Notes: 11.14.24

Pigeonhole Principle:

given N objects placed into k boxes, at least 1 box has $\lceil N/k \rceil$ objects

- Interested In: minimum # of objects N so at least r objects can fit into 1 of k boxes
- w/ N objects, there must be at least r objects in 1 of k boxes if $\lceil N/k \rceil \geq r$

Ex.



$K = 5$ (boxes)

$N = 16$ (objects)

$r = 2$ (at least 2 objects in 1 of the boxes)

Check. $\lceil 16/5 \rceil = 4 \geq 2$ ✓

Is there a formula for N?

$$N = k(r-1)+1$$

* derivation in typed notes *

Ex- Show that if 7 ints were selected from the first 10 positive ints, there must exist two pairs of ints that sum to 11

Boxes: (1,10), (2,9), (3,8), (4,7), (5,6)
$k=5$ pigeonholes...

Expression: $N = k(r-1)+1$

What if $N=6$?
eg {10, 9, 8, 7, 6, 5}
{1, 2, 3, 4, 5, 6}

$6 = 5(r-1)+1 \Rightarrow r = 2$

What if $N=7$?
$7 = 5(r-1)+1$
$r = \frac{6}{5}+1 > 2$
implies more than one

at least 1 box will have $r=2$ pairs met

What if $N=5$
$r = \frac{4}{5}+1 = 1.8 < 2$

Permutations and Combinations:

Ex. How many ways are there for 10 women and 6 men are standing in line and no men stand next to each other?

. place W, no M next to another M { M at end / M b/w 2 W

1st insight: 11 possible places to put a M

_ W _ W _ W _ W _ W _ W _ W _ W _ W _ W _
1 2 3 4 5 6 7 8 9 10 11

2nd. # of ways to place the W?
place $W_1 \to (n-1)$ left
place $W_2 \to (n-2)$ left ...
place $W_3 \to (n-3)$ left

unique combos?
n! women
10!

Express as permutation: $P(n, r) \Rightarrow P(10, 10)$
n # of items to arrange; r # positions to fill

$P(n,r) = \frac{n!}{(n-r)!} = \frac{10!}{0!} = 10!$

3rd. place M in gaps – use Combinations

Combinations: unordered selections of objects from a set

- 11 gaps that could be filled
- 6 men to fill gaps

possible combos: $C(n,r) = \frac{n!}{r!(n-r)!}$ $n=11$, $r=6$

$\Rightarrow \frac{11!}{6!\,5!} = 462$

combos to arrange W: $10! = 3{,}628{,}800$ × # combos to put M in gaps: 462

$\Rightarrow$ 3,628,800 × 462 combos for both

$P(6,6) = 6! = 720$ (# of arrangements of M w/ gaps)

$\Rightarrow P(10,10) \cdot C(11,6) \cdot P(6,6)$ = huge!

1. Why C() for M? order of filling gaps does not matter — we have already established the gap positions!
2. Why P() for W? the arrangement of W determines the position of the gaps!

Ex. A department contains 10M and 15W. How many ways are there to form a committee w/ 6 members where there are more W than M

1st: identify possible combos for M & W

6 W , 0 M → C(15, 6) = 5005
5 W ; 1 M → C(15, 5) • C(10, 1) = 30030
4 W ; 2 M → C(15, 4) • C(10, 2) = 61425

Total Combos : 5005 + 30030 + 61425 = 96,460
(or) (or)

Ex. How many ways is there for a horse race to finish with four horses to finish if ties are possible?
(Note any # of 4 horses may tie)

1st Case. No ties : P(4, 4) = 4! = 24

2nd Case. only 2 horses tie :
C(4, 2) : # of ways 2 horses tie
P(3, 3) : remaining 3 positions
⇒ C(4, 2) × P(3, 3) = 36

3rd Case : 2 sets of horses tie
C(4, 2) = 6

4th Case : 3 horses tie, 1 place
C(4, 3) × 2 = 8

5th Case : All horses tie : 1

24 + 36 + 6 + 8 + 1 = 75

* more examples in written / typed notes *

Lecture Notes: 11-19-24

Women/Men Problem cont.

to change ordering of W → unique set of gaps

$$\left.\begin{array}{l} \_\ w_1\ \_\ w_2\ \_\ \cdots \\ \_\ w_4\ \_\ w_7\ \_\ \cdots \end{array}\right\}\ \text{gaps treated differently}$$

* Gaps are dependent on order of women *

Permutation/Combination Summary: for distinct items

	Order Matters	Order does not matter
Repetition Not Allowed:	$P(n,r) = \frac{n!}{(n-r)!}$	$C(n,r) = \frac{n!}{r!(n-r)!}$
Repetition Allowed:	$P(n,r) = n^r$	$C(n+r-1,r) = \frac{(n+r-1)}{r!(n-1)!}$

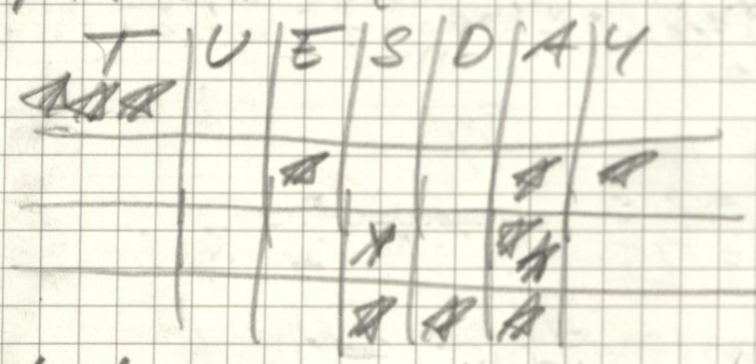
Note. indistinguishable objects, no repetition $\rightarrow \frac{n!}{n_1!\cdot n_2!\cdot\ldots\cdot n_k!}$

Ex. # of different strings of length 7 comprised of the letters in TUESDAY

Repetition Allowed: TTTTTTY, YYYYYYT } valid

$P(7,7) = n^r = 7^7$

# of ways of 3 char strings w/ letters from TUESDAY, repetition allowed



all valid ways

select 3 ★s + 6 bars in a row

→ Total of 9 "positions" to choose from

$C(9,3)$ $n=7$ $r=3$

C things to choose from

$C(n+r-1,r) = C(9,3) = \frac{9!}{3!6!}$

Ex. # of distinct strings that can be created from ABRACADABRA (11 chars)

NOT $P(11, 11) \to$ A could be formed by 5 different A's ...

Use $C(11, 5) \to$ # of ways to place the A's
— leaves 6 positions free

$C(6, 2) \to$ # of B's
$\to$ # open positions

$C(4, 2) \to$ # of R's
$\to$ # open positions

$C(2, 1) \to$ C's
$C(1, 1) \to$ D's

Answer $= C(11,5) \cdot C(6,2) \cdot C(4,2) \cdot C(2,1) \cdot C(1,1)$

* can be done in any order *

Ex. # of ways to distribute n distinguishable objects into k distinguishable boxes and want n_i objects in each boxes?

Sidebar. # of ways to distribute 5 cards to 4 players?
- 52 card deck, 4 boxes, 5 objects.
- 1 additional box $\to$ cards not dealt

$$C(52,5) \cdot C(47,5) \cdot C(42,5) \cdot C(37,5)$$

1st player gets 5 cards, 2nd, 3rd, last player

Or can be expressed as $= \dfrac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$

$$= \frac{52!}{5!\,47!} \cdot \frac{47!}{5!\,42!} \cdot \frac{42!}{5!\,37!} \cdot \frac{37!}{5!\,32!}$$

$$= \frac{52!}{5!\,5!\,5!\,5!\,\underline{32!}}$$

undealt deck

Discrete Probability:

- **Experiment**: procedure that gives 1 out of some # of possible outcomes (ex. coin toss)
- **Sample Space**: set of all possible outcomes of experiment

Ex. {heads, tails}, {1, 2, 3, 4, 5, 6}
coin toss — roll a dice

- **Event**: some subset of the sample space

$$P(E) = \frac{|E|}{|S|}$$

$|E|$ → subset of S
$|S|$ → finite, nonempty sample space

Ex. Assume deck of 52 cards, and you draw 5 cards from deck. What is probability that exactly 3 are queens?

1st: # of ways to choose N queens (N=3)

$$C(4,3) = \frac{4!}{3!\,1!} = 4$$ unique combos of 3 queens

4 → total queens

2nd: Figure out # of combos of remaining cards

$C(48, 2)$ – why 48? why not 49? must account for the fact that we do not want the 4th queen

$$C(48,2) = \frac{48!}{46!\,2!} = 1128$$

3rd: total # of ways to get 5 cards where 3 are queens

$$= 4 \cdot 1128 = 4512$$

4th: # of unique 5 hands of cards?

$$C(52,5) = 2{,}598{,}960$$

5th: Probability? $4512/2598960 = 0.17$

Lecture Notes: 11.21.24

Ex. consider urn w/ 20 balls, each of different colors. What is the prob. of drawing a blue ball, then red, then green?

$b = 7; r = 6; g = 7$ ← # of each color of ball

w/o Replacement:

$P(20,3) = \frac{20!}{(20-3)!} = 20 \cdot 19 \cdot 18 = 6840$

# of ways to choose color of balls in order:

$C(7,1) \cdot C(6,1) \cdot C(7,1) = 294$
blue red green

Prob. $294/6840 = 4.3\%$

Corollary - Blue ball first: $7/20$
Red ball 2nd: $6/19$
Green ball 3rd: $7/18$

Prob. $\frac{7 \cdot 6 \cdot 7}{20 \cdot 19 \cdot 18} = .043$

W/ Replacement:

# of possible outcomes:

$P(20,3) = n^r = 20^3 = 8000$ possible outcomes

allowing for repetition

# of favorable outcomes:

$C(7,1) \cdot C(6,1) \cdot C(7,1) = 294$

Prob. $294/8000 = 3.7\%$ ← should be lower

Complement of an Event:

E = event, S = sample space

$\overline{E} = S - E \Rightarrow P(\overline{E}) = 1 - P(E)$

Ex. n-bit string. Prob that @ least 1 of n bits is 0? $n=10$

The ONLY answer that does not satisfy this:

1 1 1 1 1 1 1 1 1 1

Prob. $1/2^{10}$

So compliment: $1-\frac{1}{2^{10}}$

Ex. Prob of $x \in \mathbb{Z}^+ : x \le 1000$ divisible by either 7 or 11 or both

$P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)$

E_1: random int divisible by 7

E_2: random int divisible by 11

$E_1 \cup E_2$: " " by 77

Recall. $\lfloor n/d \rfloor$ — # ints that don't exceed n and are divisible by d

$|E_1| = \lfloor 1000/7 \rfloor$, $|E_2| = \lfloor 1000/11 \rfloor$,

$|E_1 \cup E_2| = \lfloor 1000/77 \rfloor$

$P(|E_1 \cup E_2|) = \lfloor 1000/7 \rfloor + \lfloor 1000/11 \rfloor - \lfloor 1000/77 \rfloor = \frac{220}{1000}$

Prob. 22%

makes sure numbers are not double counted

Experiments where All Outcomes are not Equally Likely:

$0 \le p(S_i) \le 1$ for $i = 1, 2, \ldots, n$

$\sum_{i=1}^{n} p(S_i) = 1$

Ex. A pair of dice where $P(4) = \frac{2}{7}$ for 1st die

$P(1) = P(2) = P(3) = P(5) = P(6) = \frac{1}{7}$

and $P(3) = \frac{2}{7}$ for second die

"

~

Prob of P(7)?

1st. possible ways to get 7?

(1,6); (2,5); (3,4); (4,3); (5,2); (6,1)

$P(1,6) = \frac{1}{7} \cdot \frac{1}{7} = \frac{1}{49}$

$P(2,5) = P(3,4) = P(1,1) = P(5,2) = \frac{1}{49}$

$P(4,3) = \frac{2}{7} \cdot \frac{2}{7} = \frac{4}{49}$

$P(7) = 5\left(\frac{1}{49}\right) + \frac{4}{49} = \frac{9}{49}$

Conditional Probability:

Events E, F: $\underset{\text{given}}{P(E|F)} = \frac{P(E \cap F)}{P(F)}$; $P(F) \neq 0$

Ex. what is cond. prob. that 4 heads appear when a fair coin is flipped 5 times and the 1st flip is a tail?

1st. flip is a Tail = F

2nd: # of outcomes if 1st flip is tail

$\underbrace{T \_\_ \ \_\_ \ \_\_ \ \_\_}_{\text{4 more events}} - 2^4 = 16$

(permutation w/ replacement)

Note. 2^5 possible outcomes for 5 flips

$P(F) = \frac{16}{32} = \frac{1}{2}$

3rd. consider $|E \cap F|$ or $P(E \cap F)$

$= P(E) \cdot P(F) = \frac{1}{2^4} \cdot \frac{1}{2^1} = \frac{1}{32}$

4th. $P(E|F) = \frac{P(E \cap F)}{P(F)} = \frac{\frac{1}{32}}{\frac{1}{16}} = \frac{1}{16}$

* what if first flip is heads? $F = \{H \_ \_ \_ \_\}$; $P(H) = \frac{2^4}{2^5} = \frac{1}{2}$

$E \cap F = \{HHHHT, HHHTH, HHTHH, HTHHH\}$

$P(E \cap F) = 2^2 / 2^5 = \frac{1}{8}$ ...

Conditional Probability for Independent Events:

if $P(E|F) = P(E)$, then E, F are independent

$P(E|F) = \frac{P(E \cap F)}{P(F)} \Rightarrow E, F$ are independent if
$P(E) \cdot P(F) = P(E \cap F)$

since $P(E|F) \underset{\uparrow}{=} \frac{P(E) \cdot P(F)}{P(F)} = P(E)$
would equal

Ex. E: RNG bit string of length 3 has odd # of 1s
F: String starts with a 1
Are E, F independent?

odd # of 1s: $\{001, 010, 100, 111\}$ E

start w/ 1: $\{100, 101, 110, 111\}$ F

$P(E) = 4/8 = 1/2$ $P(F) = 4/8 = 1/2$

$E \cap F$: $\{100, 111\}$. $P(E \cap F) = 2/8 = 1/4$

E, F are independent iff $P(E) \cdot P(F) = P(E \cap F)$
$\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ ✓

$\therefore E, F$ are independent

Ex. Assume family of 4 kids, all equally likely
E: Family of 4 kids, 2 boys
F: Family of 4 " " @ least 1 boy
Are E, F independent?

$|S| = 16 = \{BBBB, BBBG, \ldots, GGGG\}$
$|E| = \{BBGG, BGBG, BGGB, GGBB, GBBG, GBGB\}$
$P(E) = 6/16 = 3/8$
$|F|$: $P(F) = 1 - P(\overline{F}) = 1 - 1/16 = 15/16$
$E \cap F = E$. $P(E \cap F) = P(E) = 3/8$
E already satisfies F $\therefore$ not independent
do the check!

Lecture Notes: 11.20.24

Using Recurrence Relations to solve Counting problems:

Ex. How many bit strings of length n do not contain consecutive 0's?

$n=1$: 0, 1 ; 2 strings don't have consecutive 0s

$n=2$: 00, 01, 10, 11 ; 3 " "

$n=3$: 000, 001, 010, 011, 100, 101, 110, 111 ; 5 " "

a_n = # of n-bit strings " "

$a_{n+1} = a_n + a_{n-1}$

Ex. A password has letters and #'s w/ at least 1 letter and number. How many combinations of length 8 are there?

?. cases: Letters: 8 7 6 5 4 3 2 1 0

Numbers: 0 1 2 3 4 5 6 7 8

Allowed: N Y Y Y Y Y Y Y N

Use permutations, not combinations:

123456 ~~7~~ 463521

$P(26,7) \times P(10,1) \times \underbrace{C(8,1)}$

think: XXXXXXX#

accounts for all combinations of X's and #'s here

$+ P(26,6) \times P(10,2) \times C(8,2)$

$+ \vdots$

$+ P(26,1) \times P(10,7) \times C(8,7)$

$= 2,612,182,842,880$

Can express as a recurrence relation:

password of length n is formed as follows:

- Any letter or # followed by $n-1$ character pswd
- Any letter followed by $n-1$ #'s
- Any # followed by $n-1$ letters

$a_n = (26+10)a_{n-1} + (10 \cdot 26^{n-1}) + (26 \cdot 10^{n-1});$

$a_1 = 0$

$n=2: a_2 = 36a_1 + 10 \cdot 26 + 26 \cdot 10^1 = 520$

or $P(26,1) * P(10,1) * C(2,1) = 520$

$a_8 = \text{''} = 2,612,182,842,880$

1-more way: $P(36,8) - \underbrace{P(26,8) - P(10,8)}$

subtracting 8 char pswds that are either all letters or numbers

& 3 ways to solve these counting problems &

NOTE if using recurrence relations try to find a closed form solution

3 ways to express a sequence:

- $\{3,5,6,7,9,\ldots\}$ define elements ago
- closed form: $a_n = \frac{(-1)^n}{n+1}; n \geq 0$
- recurrence relation: $a_n = 3a_{n-1} + a_{n-2} + 1; n \geq 2$

implies 2 initial conditions needed

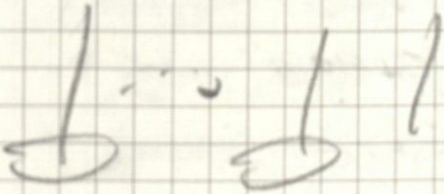
Ex: Towers of Hanoi

- move disks from one peg to another, but never put a larger disk on top of a smaller one
- how many moves are required

find a recurrence relation $\{H_n\}$

H_n: number of moves w/ n-disks

1 disc:



1 move

$H_1 = 1$

$H_2 = 2H_1 + 1$

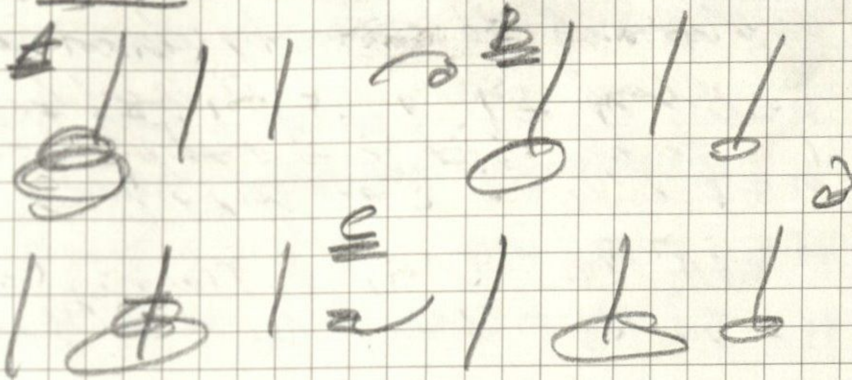
$H_2 = 3 = 2 \cdot 1 + 1 = 2^1 + 1$

$H_3 = 2(2^1+1)+1 = 2^2+2^1+1$

$H_4 = 2(2^2+2^1+1)+1$

$\quad = 2^3+2^2+2^1+1$

2 discs:



3 moves

B moved n-1 disks to peg #3

C transferred larger disc to peg #2

D transferred n-1 disc to peg #2

$H_n = (H_{n-1}) + 1 + (H_{n-1})$

smallest   larger   small

$H_n = 2(H_{n-1}) + 1$

$H_n = 2H_{n-1} + 1 = 2^{n-1} + 2^{n-2} + 2^{n-3} + \dots + 2^2 + 2^1 + 1$

geometric series: $a + ar + ar^2 + \dots$ $a = 1, r = 2$

closed form: $\frac{ar^{n+1} - a}{r-1} = \frac{2^n - 1}{r-1} = 2^n - 1$

$H_n = 2^n - 1$

can prove closed form solutions via MI #

Ex: How many ways can you deposit n dollars w/ a \$1 bronze, \$1 silver, and \$3 gold, order matters, $n \geq 3$

To deposit n dollars

1. 1st deposit n-1 dollars then insert bronze
2. 1st deposit n-1 dollars then silver
3. 1st deposit $\underline{n-3}$ dollars then gold

$\Rightarrow V_n = 2V_{n-1} + V_{n-3}$

degree 3, need 3 initial conditions

Context: find recurrence relation v_n and initial conditions to satisfy equations

$n=0: v_0 = 1$ (only 1 way to deposit \$0...)

$n=1: v_1 = 2$ (bronze, silver)

$n=2: v_2 = 4$

$n=3: v_3 = 2v_2 + v_0 = 2(4)+1 = 9$

Ex: How many elements are in the union of 2 finite sets?

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

Find the # of positive ints not exceeding 1000 that are the square or the cube of an integer

$|A|$ = # of integers, ≤ 1000, square of an integer

$|B|$ = # of " , " , " , " cube " "

$\Rightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$

$1^3 = 1$ $\quad$ $10^3 = 1000$

For set A: $k \cdot k \leq n = 1000$

$k^2 \leq n \Rightarrow k \leq \sqrt{n}$

$|A| = \lfloor \sqrt[3]{n} \rfloor$ ... $|B| = \lfloor \sqrt[3]{n} \rfloor$

$|A \cap B|$ ~ implies 6th root of n. $\sqrt[6]{n}$

$n=2: 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64$

$4^3 = 64 \quad 8^2 = 64$

$|A \cup B| = |A| + |B| - |A \cap B| = 31 + 10 - 3 = 21$

$\lbrack 1, 2, 3$

$1, 64, 729$

Lecture Notes: 12.3.24

Relation Graphs:

- given sets A, B
- binary relation b/w $A, B \to$ subset of $A \times B$

Ex. $A = \{1, 2\}$, $B = \{x, y\}$

$A \times B = \{(1,x), (1,y), (2,x), (2,y)\}$

$R = \{(1,x), (2,y)\}$

Notation.

$a R b \in R \sim (a,b)$ is in R

$a \not R b \in R \sim (a,b)$ is not in R

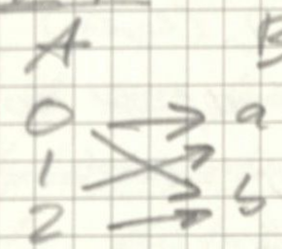
Ex. $A = \{0, 1, 2\}$, $B = \{a, b\}$

$R = \{(0,a), (0,b), (1,a), (2,b)\}$

Is $0 R a$? yes b/c $(0,a) \in R$

Is $1 R b$? no b/c $(1,b) \notin R$

Graph.



Matrix.

R	a	b
0	X	X
1	X	
2		X

Ex. $(s_1, c_1) \in R$, $(s_1, c_3) \in R$, $(s_2, c_3) \in R$,
$(s_2, c_m) \in R$, $(s_3, c_1) \in R$

R	c_1	c_2	c_3	...	c_j	...	c_m
s_1	X		X				
s_2			X				X
s_3	X	Y					
⋮							
s_i					Y		
s_m							

Add Elements to Relation?

— Y

(s_3, c_2); (s_i, c_j)

Ex. List ordered pairs of relation R from $A = \{0, 1, 2, 3, 4\}$ to $B = \{0, 1, 2, 3\}$ where $(a, b) \in R$ if and only if:

$a = b \Rightarrow R = \{(0,0), (1,1), (2,2), (3,3)\}$

$a + b = 4 \Rightarrow R = \{(1,3), (2,2), (3,1), (4,0)\}$

no $(0, 4)$ b/c $4 \notin B$

$a / b \Rightarrow R = \{(1,0), (1,1), (1,2), (1,3), (2,0), (2,2), (3,0), (3,3), (4,0)\}$

Reflexive Relation: relation R where $(a, a) \in R \ \forall a \in A$ w/ respect to set A

Ex. $A = \{a, b\} \Rightarrow R = \{(a,a), (b,b)\}$

Note. $R = \{(a,a), (b,b), (c,d)\}$ R w/ respect to set A is still reflexive

Symmetric Relation: relation R where

$\forall a \in A \land \forall b \in B \, ((a,b) \in R \rightarrow (b,a) \in R)$

Ex. $A = \{a, b\}$, $R = \{(a,b), (b,a), (c,d)\}$ is symmetric w/ respect to A

* Note, can have extra elements in relation R

Antisymmetric Relation: relation R where

$\forall a \in A \land \forall b \in B \, [((a,b) \in R \land (b,a) \in R) \rightarrow (a == b)]$

"if $(a,b) \in R$ and $(b,a) \in R$ then $a == b$"
↳ equal to

Transitive Relation:

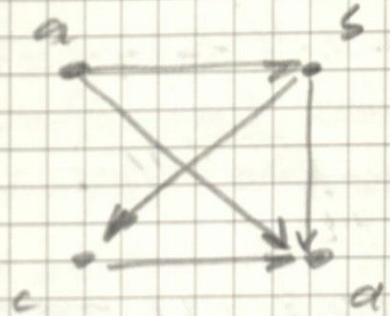
A relation R on set A is transitive if

$\forall a \in A \ \forall b \in B \ \forall c \in C \, [((a,b) \in R \land (b,c) \in R) \rightarrow (a,c) \in R]$

Representing relations using digraphs 3

digraph — directed graphs

Ex.



$R = \{(a,b), (a,d), (b,c), (b,d), (c,d)\}$

Notation:

V = set of nodes (vertices)

E = set of edges (arcs)

(a, b) = initial vertex : a
terminal vertex : b

* a node can loop back on itself * ↗ (edge back to itself)

Def.

Reflexive: loop at every node

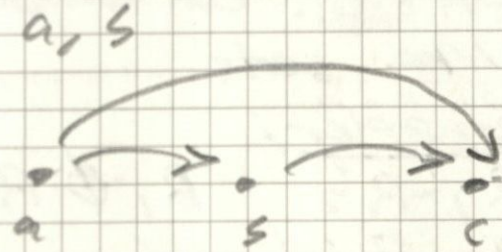
Symmetric: for two nodes a and b :

- there is a directed arc from a to b
- " " b to a

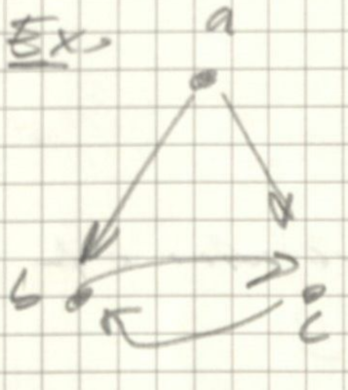
* can be distinct or not *

Antisymmetric: iff never two arcs above for distinct a, b

Transitive:



Ex.



Reflexive: No

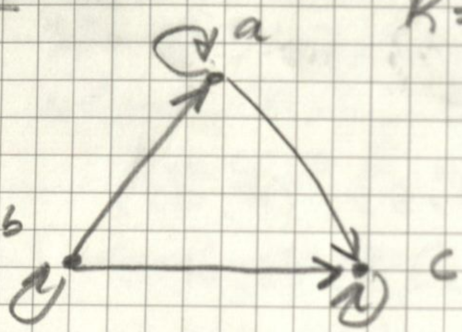
Symmetric: No

Antisymmetric: No

Transitive: No

$R = \{(a,b), (a,c), (b,c), (c,b)\}$

Ex.



$R = \{(a,a), (b,b), (c,c), (b,a), (a,c), (b,c)\}$

Reflexive: Yes

Symmetric: No

Antisymmetric: Yes

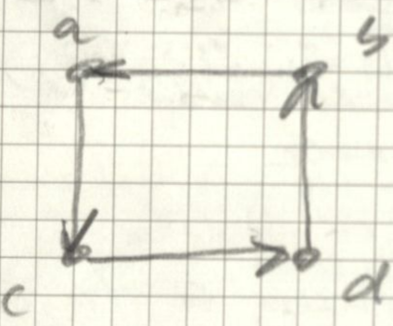
Transitive: Yes

& only need a single example to disprove any of these

Note. Elements can be transitive w/ themselves

$(b,a)(a,c) \Rightarrow (b,c)$ ✓
$(a,a)(a,c) \Rightarrow (a,c)$ ✓
$(b,b)(b,a) \Rightarrow (b,a)$ ✓
$(b,b)(b,c) \Rightarrow (b,c)$ ✓

Ex.



$R = \{(a,c), (c,d), (d,b), (b,a)\}$

Reflexive: No

Symmetric: No

Antisymmetric: Yes

Transitive: No

$(a,c)(c,d) \rightarrow (a,d)$ ✗

Combining Relations:

set A, B, $R \subseteq A \times B$. Can combine/operate relations just like sets

Ex. R_1, R_2. consider:

$R_1 \cup R_2$ $R_1 - R_2$ $R_1 \oplus R_2$
$R_1 \cap R_2$ $R_2 - R_1$ ⋮

Ex. R relates from A to B
S relates from B to C

The composite of R & S ($S \circ R$) is relation of (a, c) $\forall a \in A$, $\forall c \in C$, ... where $\exists b \in B$ s.t. $(a,b) \in R \wedge (b,c) \in S$

Relation Closure: add the correct elements to satisfy a particular property of a relation

"symmetric closure"
"reflexive closure"
"transitive closure"

How to determine what to add to satisfy a particular property P?
(P = symmetry, reflexivity, transitivity, ...)

Let R be a relation on set A that may or may not have a property P
If there's a relation S w/ property P containing R such that S is a subset of every relation w/ property P containing R, then S is the closure of R with respect to P

Ex: $R = \{(1,1), (1,2), (2,1), (3,2)\}$ on set $A = \{1,2,3\}$. How to make R reflexive?

Add $(2,2)$ & $(3,3)$ to R

$S = \{(1,1), (1,2), (2,1), \underline{(2,2)}, (3,2), \underline{(3,3)}\}$

$R \subseteq S$

Lecture Notes: 12.5.24

Ex. $R = \{(a,b) \mid a \equiv b \pmod{m}\}$ is an equivalence relation

* Show reflexivity, symmetry, transitivity *

Reflex. $a \equiv b \pmod{m}$, $(a,a) \in R$

$\hookrightarrow \frac{a-b}{m} = k \Rightarrow a-b = km \Rightarrow a-a = km$

$\uparrow$ $\Rightarrow 0 = km$

$a \equiv a \pmod{m}$ $b = a$ $k = 0$ ✓

Symmetry: $(a,b) \in R \rightarrow (b,a) \in R$

$a \equiv b \pmod{m}$

$\frac{a-b}{m} = k \Rightarrow a-b = km$

$b-a = -km$ ✓

$\frac{b-a}{m} = -k$ ✓ $b \equiv a \pmod{m}$

Transitivity: $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m}$

$\rightarrow a \equiv c \pmod{m}$

$a-b = km$ $b-c = lm$

$(a-b) + (b-c) = km + lm$

$a-c = (k+l)m$ ✓

equivalence relation: relation that is reflexive, symmetric, and transitive

Q. is the "divides" operation an equivalence relation? $(a|b)$

Reflexive: $a|a = 1$ ✓

Transitive: $a|b \wedge b|c \rightarrow a|c$

$b = ak$, $c = bl$, $a|c$: $c = akl$ ✓

Symmetric: find a single counter ex

$4|2$ ✓

$2|4$ ✗ not an integer

Equivalence Classes

- Assume R is an equivalence relation on set A
- The set of all elements related w/ respect to R to $a \in A$ is the equivalence class of a, $[a]_R$, or $[a]$

  i.e. $[a]_R = \{s \mid (a,s) \in R\}$

  i.e. equivalence class $[a]_R$ is the set of all elements s s.t. $(a,s) \in R$
- $b \in [a]_R$ is a representative of the class (any element of the class can be the representative)
- Each element of set A would belong to one and only one equivalence class, which means equivalence relation partitions the set A into distinct subsets

Ex. What is the equivalence class of 0 for congruence mod 4

want to identify all ints so $a \equiv 0 \pmod 4$ is satisfied

$[0] = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$

$\frac{-8-0}{4} = -2$ ✓ integer

Ex: $A = \{2, 4, 6, 8, 10\}$

R is a binary relation on A:

$(m, n) \in R$ iff $\underline{m \equiv n \pmod 4}$ $\forall m, n \in A$

ie: 4 divides $m - n$

OR $(m-n)$ is an integer multiple of 4

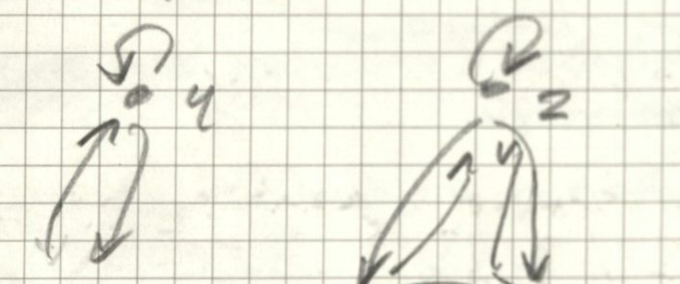
(m, n)	$m-n$	is $\in R$?	is mult. of 4?
$(2,2)$	0	yes	0 is a mult of 4
$(2,4)$	-2	no	-2 not mult of 4
$(2,6)$	-4	yes	-4 mult of 4
⋮			
$(4,2)$	2	no	2 not mult
$(4,4)$	0	yes	yes
⋮			

$R = \{(2,2), (2,6), (2,10), (4,4), (4,8),$
$(6,6), (6,10), (8,8), (6,2), (10,2),$
$(8,4), (8,8), (10,10)\}$

Show R is a equivalence relation:

- show reflexivity, sym, trans

Use a graph: use ordered pairs as (source, destination)



reflex ✓

sym ✓

trans ✓

2 connected components: graphically represent 2 distinct equivalence classes w/ respect to R

$[2] = \{2, 6, 10\}$ $\quad [4] = \{4, 8\}$

$[2] = [6] = [10] = \{2, 6, 10\}$

Ex. What is the equivalence class of 2 for congruence mod 5?

$[a]_4 = \{ \ldots, \quad , \ldots \}$

ie. want all integers st $a \equiv 2 \pmod 5$

ie. $5 \mid (a-2)$ or $\frac{a-2}{5} \in \mathbb{Z}$

$\ldots, -13, -8, -3, 2, 7, 12, \ldots$

$[a]_m = \{ \ldots, a-2m, a-m, a, a+m, a+2m, \ldots \}$

Ex. Suppose A is a nonempty set and f is a function that has A as its domain. Let R be a relation on A

$R = \{ (x,y) : f(x) = f(y) \}$

Show R is equivalence relation on A

1. $(x,x) \in R$ b/c $f(x) = f(y)$ $\therefore R$ reflexive
2. $(x,y) \in R$ iff $f(x) = f(y)$
   will hold only if $f(y) = f(x)$
   $(y,x) \in R$ $\therefore R$ symmetric
3. if $(x,y) \in R$ and $(y,z) \in R$
   then $f(x) = f(y) \wedge f(y) = f(z) \rightarrow f(x) = f(z)$
   $\therefore R$ transitive

* qualitative exs of equivalence relations in written notes *

How does an equivalence relation partition a set?

Context: Histogram - Buckets: 90-100, 80-90, 70-80, ⋮

$\Rightarrow$ each student will only be in one bucket

S = set of all students in classes

$A_{i,j,k,\ldots}$ = bins

Each $A_{i,j,k,\ldots}$ has at least 1 student

(a bin/graph node will only exist if it has at least 1 student to represent)

A_i's disjoint $A_i \cap A_j = \emptyset$ if $i \neq j$

$A_i \cup A_j \ldots \cup A_n \sim \bigcup A_n = S$

More Formally:

R = relation on set S - consists of pairs (x, y) where x, y are students who received the same range (grade) (in the same bin)

Reflex: $(x, x) \in R \ \forall x \in S$
should be in same bin as himself

Sym: $(x, y) \in R \rightarrow (y, x) \in R$

Trans: $(x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$
all in same bin

Ex: List the ordered pairs in equiv relation R produced by partitions of S (A_1 and A_2)

$S = \{a, b, c, d, e\}$

$A_1 = \{a, b\}$

$A_2 = \{c, d, e\}$

$A_1 = \{(a, a), (a, b), (b, a), (b, b)\}$

$A_2 = \{(c, c), (d, d), (e, e), (c, d), (d, c), (e, d), (d, e), (e, c), (c, e)\}$

has to satisfy R, S, T

Lecture Notes :

2.10.24

Graph Theory :

- $G(V, E)$

set of vertices: $V(G)$ or V_G

set of edges: $E(G)$ or E_G

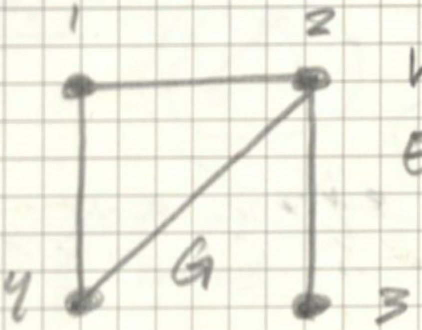
cartesian product

- $E \subseteq V \times V$

i.e. # of edges $\leq$ vertices^2

- edge e connects u, v : $\{u, v\}$

Ex.

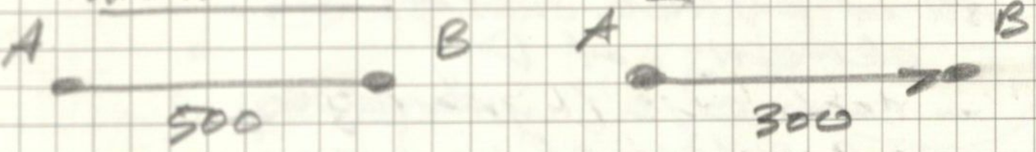


$V(G) = \{1, 2, 3, 4\}$

$E(G) = \{\{1,2\}, \{2,3\}, \{2,4\}, \{1,4\}\}$

Edge Types:

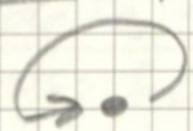
undirected: directed:



edge weight

* digraph applications in slides

Loops : path back to itself

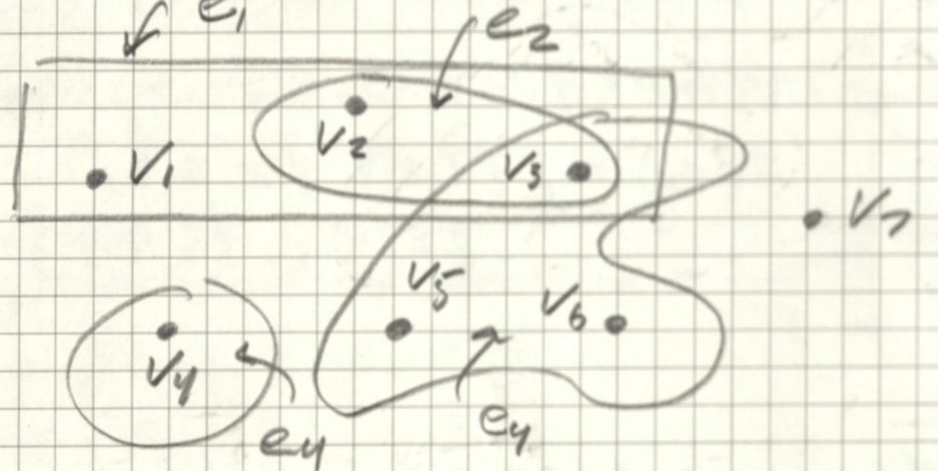


Graph Types: undirected, directed (digraphs)
mixed (both directed / undirected edges)

Multi-Graphs: multiple edges

Simple Graphs: no directed edges
no loops
no multiple edges

Hypergraphs: shapes as global edges



$E \subseteq 2^V$ all of possible subsets on elements of V
— each edge (hyperedge) is a subset of vertices

$E \subset V \times V \times V \ldots$

$V = \{1, 2, 3, 4, 5\}$

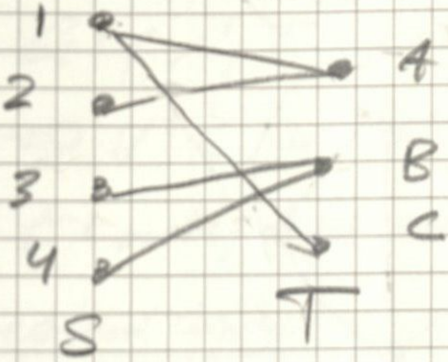
$E = \{\{1, 2, 3\}, \{5, 6, 3\}, \{2, 3\}, \ldots\}$

(the graph above):

$V = \{1, 2, 3, 4, 5, 6, 7\}$

$E = \{\{v_1, v_2, v_3\}, \{v_2, v_3\}, \{v_3, v_5, v_6\}, \{v_4\}\}$

Bipartite Graphs:



$V = S \cup T$

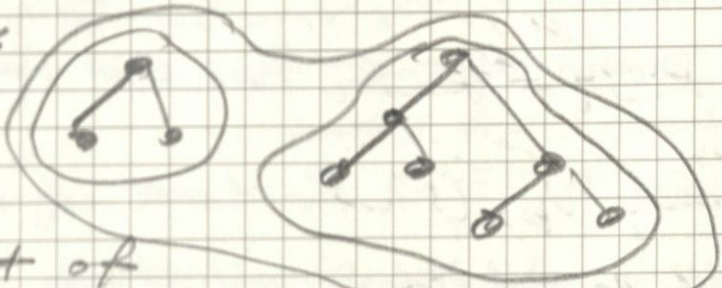
each edge in E has exactly one end vertex in S and one in T

agents $\rightarrow$ tasks

Trees: undirected, connected, acyclic graphs

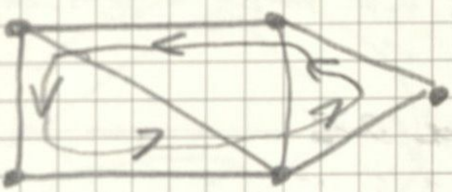
no loops/cycles

Forest:

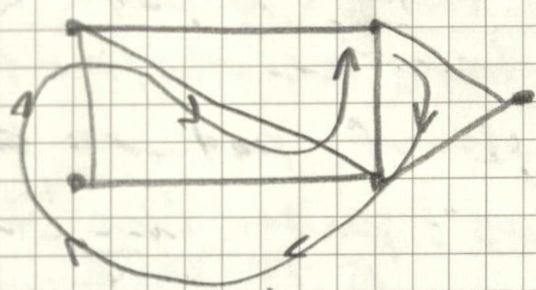


set of trees

Ex.



simple cycle

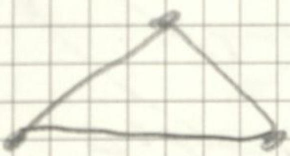


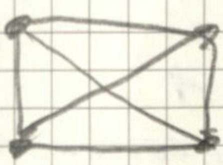
not a cycle

C_4:

C_K : # of nodes in cycle

Complete Graphs: have an edge between every possible set of vertices





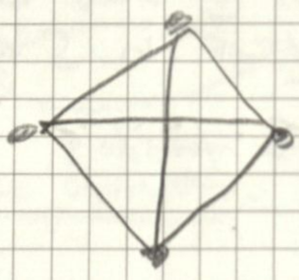
Clique – K_n : graph w/ n nodes

Planar Graph:

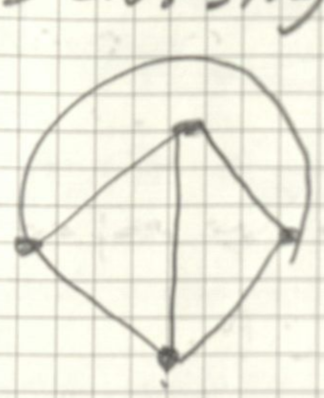
- graph w/o any edges crossing

ex. trees

ex.



not planar



planar

Walk: A sequence $(v_0, e_1, v_2, e_2, \ldots, v_{k-1}, e_{k-1}, e_k, v_k)$ of V and E s.t. every edge e_i has end vertices v_{i-1} and v_i

connects v_0 and v_k (start and end of walk)

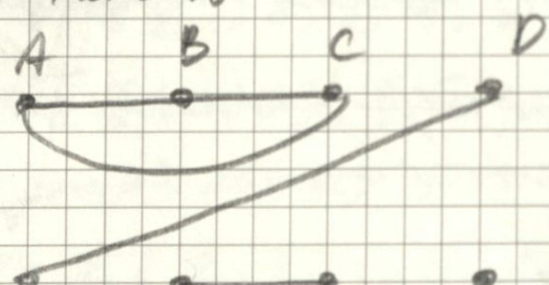
Paths: A walk in which all edges are distinct

Simple Paths: A path where all edges and all vertices are distinct

length of path = # edges

Cycles: path where start and edge vertex is the same

Connected Components: two vertices are connected if there is a walk between them



4 connected components

$\{A, B, C\}$, $\{D, E\}$, $\{F, G\}$, $\{H\}$

↳ subgraph

no overlap between connected subgraphs

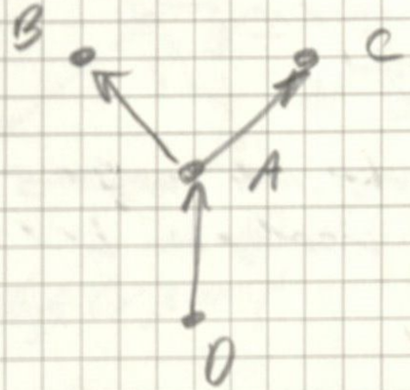
Connected component of graph G — maximally connected subgraph of G

$G'(V', E')$ of $G(V, E)$

$\Rightarrow V' \subseteq V,\ E' \subseteq E$

E' only has edges w/ vertices in V'

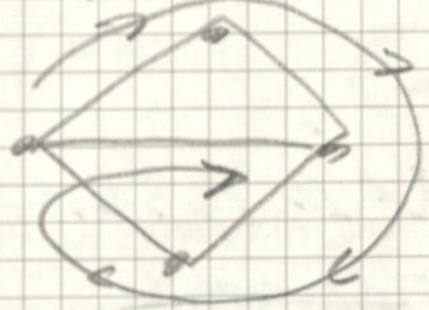
<u>Directed Graphs</u>:



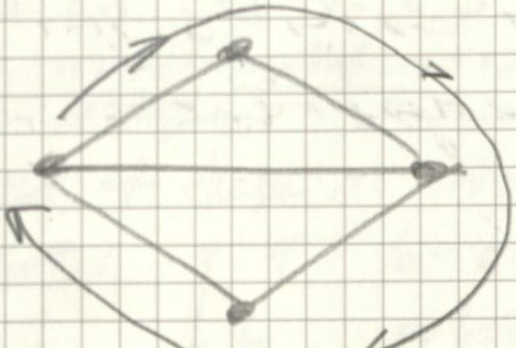
<u>Out-Component</u>: nodes that can be reached from node A via directed path

<u>In-component</u>: set of nodes for which there is a path to A

<u>Eulerian Path</u>: a graph traversal where each <u>edge</u> is traversed <u>exactly</u> 1 time



<u>Hamiltonian Path</u>: graph traversal where each <u>vertex</u> is traversed 1 time



Lecture Notes: 12.12.24

Shortest Path: path b/w 2 vertices of minimum length

Distance: between vertex u, v is the length of the shortest path b/w them
$\Rightarrow \infty$ if this path does not exist

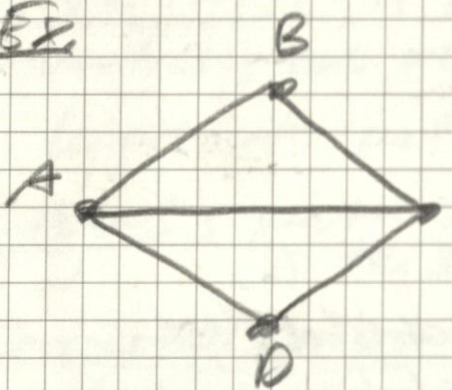
Subgraphs: consider $G'(V', E')$ s.t. $V' \subseteq V$ and $E' \subset E$

Note. E' only has edges from E to V'

Induced Subgraph: E' contains all edges from E that exist between nodes in V' ie. both endpoints in V'

Partial subgraph: E' contains some of the edges in E that have both endpoints in V'

Ex.



$V' = \{A, B, C\}$

$E' = \{\{A, B\}, \{B, C\}\}$

partial subgraph: b/c no edge $\{A, C\}$

$V' = \{A, B, C\}$, $E' = \{\{A, C\}, \{C, D\}, \{A, D\}\}$

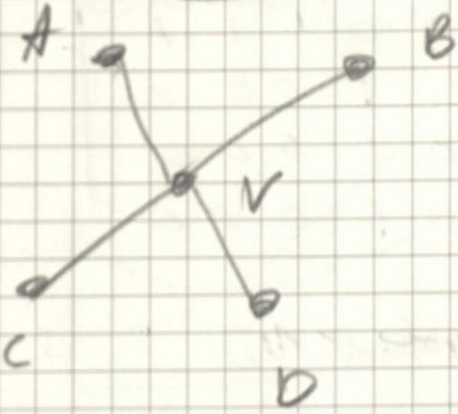
Induced Subgraph: all edges that exist in E'

Degree of a vertex:

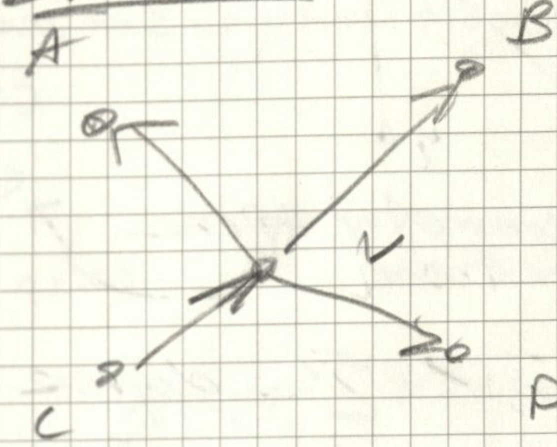
undirected: # of edges incident to vertex

directed: degree in and degree out

Ex — Undirected



Directed



$\deg(v) = 4$

in_deg(V) = 1

out_deg(V) = 3

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

$|V| = n$

$|E| = m$

$$\sum_{v \in V} \deg(v) = m$$

$$= \sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v)$$

terminal vertices

initial vertices

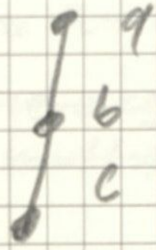
Graph Isomorphisms:

an isomorphism from graphs G to H is a bijection $f: V(G) \to V(H)$ such that xy is an edge of G iff $f(x)f(y)$ is an edge of H

an automorphism is an isomorphism on to itself

ex of these in written notes

Orbit:



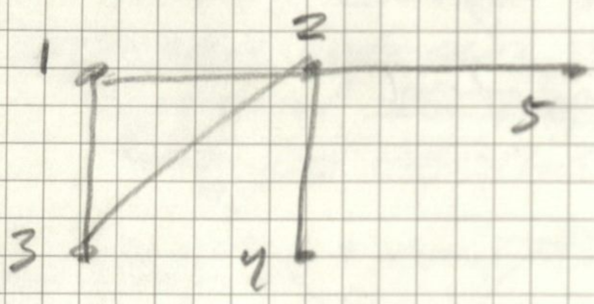
b - only mapped to itself

orbit(a) = {a, c}

orbit(b) = {b}

Graph Representations:

Adjacency Matrix:



$$\begin{array}{c|c} v_i / v_j & \begin{matrix} 1 & 2 & 3 & 4 & 5 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{matrix} & \begin{bmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

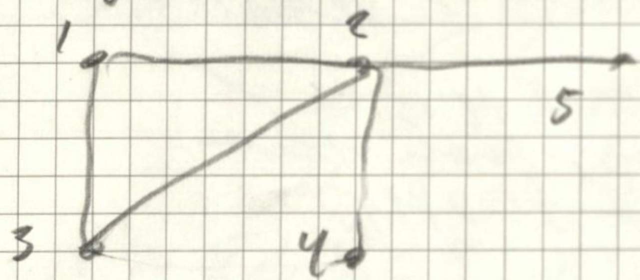
symmetric undir. matrix

$\rightarrow \Sigma$ = degree of vertex v_i

$\downarrow \Sigma$ = degree of vertex v_j

* $A_{ij} = 1$ if edge b/w v_i and v_j ; 0 otherwise
# can be done w/ directed graphs as well
# n^2 space complexity — big! #

Adjacency List:



1 : 2, 3
2 : 1, 3, 4, 5
3 : 1, 2
4 : 2
5 : 2

vertex

vertices w/ connection to node

Space : $O(m+n)$

edges # vertices

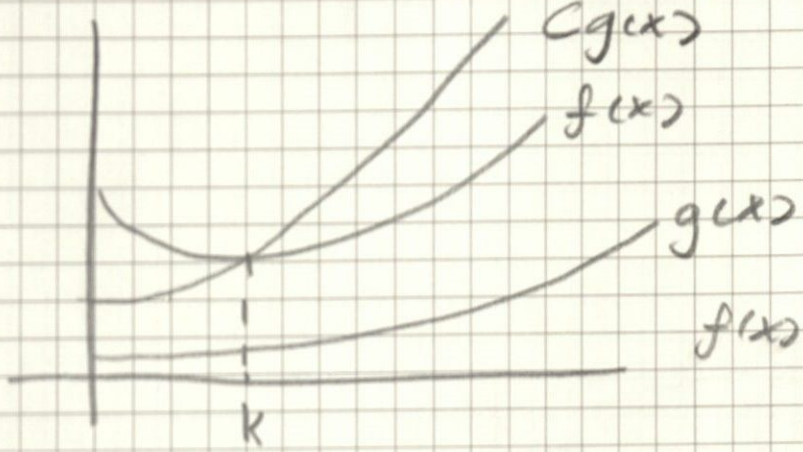
Final Exam Review: 12.15.24

Big-O Notation:

$f(n)$ is $O(g(n))$ if $|f(n)| \leq c|g(n)|$ when $n > k$

ie. $\exists c \exists k \forall n [n > k \rightarrow f(n) \leq cg(n)]$

c, k are witnesses - positive constraint constants



$f(x) < Cg(x) \ \forall x < k$

To find c, k:

n	f(n)	g(n)	$\lceil f(n)/g(n) \rceil$
1	⋮	⋮	⋮
10			
100			
⋮			

k c

* find smallest c, k from table that satisfy def. *

Solving Congruences

if $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$
if $m \mid a-b \Leftrightarrow \frac{a-b}{m} \in \mathbb{Z}$

Congruence: $a \equiv b \pmod{m}$

Linear Congruence: $ax \equiv b \pmod{m}$

Properties of Divisibility: $a = dq + r$

$q = \lfloor a/d \rfloor$

$r = a - d \lfloor a/d \rfloor$

* congruences are preserved across addition and multiplication *