MAT 1348

01-12-2015

mysite.science.uottawa.ca/msajna//MAT 1348

Lecture 1.

Introduction to logic.

⇒ logic of proof.

logic = science of correct math reasoning

Proof = Correct mathematical arg

applications of proof. program verification, algorithm correctness, system security.

1.1 Preposition of logic

$\forall x : 1+x=3.$

For all → Quantifier

Ex

Let $x=1$
$1+x=5$ } preposition

Proposition: a claim (declarative sentence) that is either true (T) or false (F), but not both

Ex on web

Proposition ⇒ we can tell true or false

1. P T 3. PF

2. PT 4. N.P unless we know the val x

5. P. T

$\exists x (1 + x = 3)$

6. P. F 7. N.P. 8. N.P. 9. N.P (M_{OV} = unknown) Yes: if it is clear who gov. are.

10. Yes if it is clear what the time period is.

11. Not logical proposition

12. Yes if it is clear who alice and bob are.

Now make complicated proposition using proposition connectives.

Truth values : T, F.

p, q, r, s, p_1, s_1, ... symbols for propositions.

Compound propositions: new propositions from old using logical connectives

$(\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \oplus)$

1. Negation: $\neg p$ "not p"

"it is not the case that p is T"

p	$\neg p$
T	F
F	T

e.g: p: "It snowed yesterday"

$\neg p$: "It did not snow yesterday"

2. Conjunction: $p \wedge q$ "p and q" / "p but q"

together

Truth table

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

e.g: p: "It snowed yesterday"

q: "It is raining today"

$p \wedge q$: "It snowed yesterday and/but it is raining today".

∴ The compound proposition is false.

3. Disjunction: $p \vee q$ "p or q" ("or both") (inclusive or)

"p unless q"

"p or else q"

part

Truth table:

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

e.g. p: "I sing"

q: "I play the piano."

$p \vee q$: "I sing or I play the piano". do not

If $p \vee q$ is F, then: I don't sing & don't play piano

Warning: In natural languages "or" often means "either ... or"

4. Exclusive or: $p \oplus q$ "either p or q (but not both)"

trt:

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

e.g: "The meal includes either a salad or a soup."

5. Implication: $p \to q$ "p implies q", "if p, then q"

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

e.g. p: "I will get elected"

q: "I will lower taxes"

$p \to q$: "If I get elected, then I'll lower taxes."

note: the only case when I can be accused of lying is if I get elected (p is T) but did not lower taxes (q is F)

Other ways to interpret $p \to q$

"p only if q" → "q is necessary for p" "q follows from p"

"q, if p" ← "q whenever p" "q unless not p" ↓

"p is sufficient for q"

logic cannot distinguish b/t if and when

"q or else not p"

q should be true unless p false

Given an implication $p \to q$, we define:

- converse of $p \to q$: $q \to p$
- contrapositive of $p \to q$: $\neg q \to \neg p$ ($\equiv p \to q$)
- inverse of $p \to q$: $\neg p \to \neg q$

equivalent!

Ex. p: "It is sunny on Sat"

q: "I go skiing on Sat"

$p \to q$: "I'll go skiing on Sat if it is sunny"

p → 2 → conclusion

hypothesis

(i.e. $p \to q$ and $q \to p$)

↘ not the same as if then

"if and only if"

Note: in natural lang, "if then" often means (bi conditional)

Lecture 2

01-15-2015

Biconditional

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

iff

"p is necessary & sufficient for q"

"if p, then q, and conversely"

Truth table

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

Confusion.

In everyday lang, "if p, then q" often means "p iff q"

Eg. "If you finish vegetables, then you may have desert"

p → T

But perhaps we really mean $p \leftrightarrow q$

Precedence of logical operators:

operator precedence.

$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Eg: $p \rightarrow \neg q \wedge r$ means $p \rightarrow ((\neg q) \wedge r)$

∴ we'll write $p \rightarrow (\neg q \wedge r)$

- $p \vee q \wedge r$ means $p \vee (q \wedge r)$ we'll write.
- $p \leftrightarrow q \rightarrow \neg r$ means $p \leftrightarrow (q \rightarrow (\neg r)) \equiv p \leftrightarrow (q \rightarrow \neg r)$

2. S: System software being updated.

V: user can access the file system

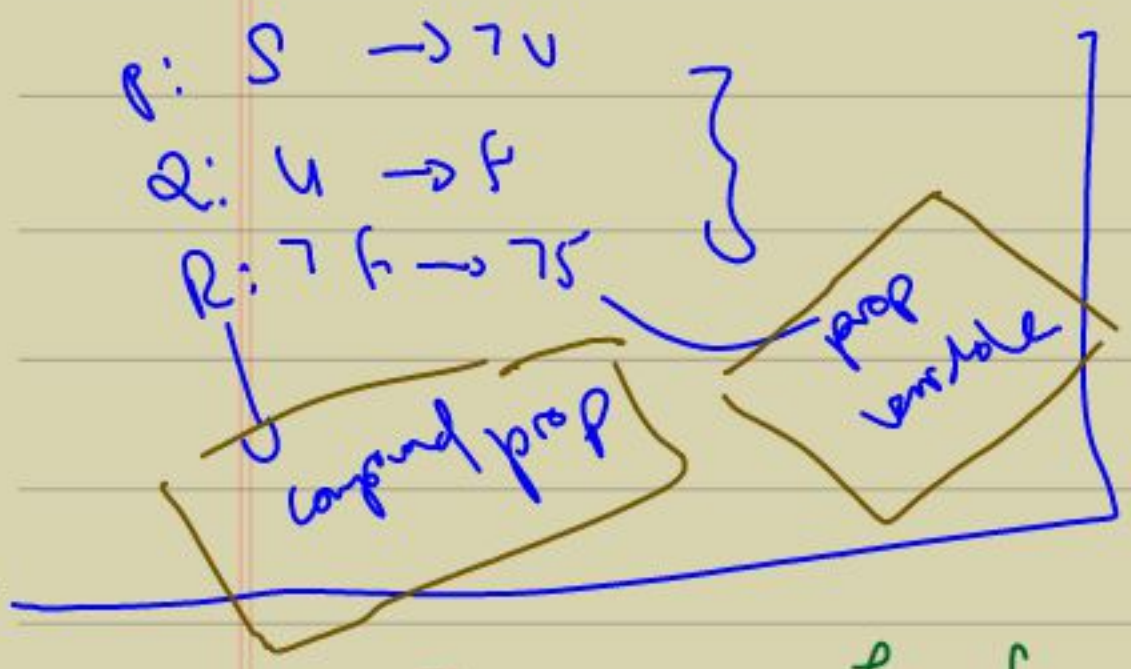
f: user can save new files

error translation

$P: S \to \neg V$

$Q: V \to f$

$R: \neg f \to \neg S$



Is the set $\{S \to \neg V, V \to f, \neg f \to \neg S\}$ consistent?

S	V	f	$S \to \neg V$	$V \to f$	$\neg f \to \neg S$
T	T	T	F	T	T
T	T	F	F	F	F
T	F	T	T	T	T ←
T	F	F	T	T	F
F	T	T	T	T	T ←
F	T	F	T	F	T
F	F	T	T	T	T ←
F	F	F	T	T	T ←

When 1 row T, the propositions is consistent

(not find out the set!!).

Ex Knights & Knaves prob

truth — lie

1. U met 2 ppl, A say "Am a knave but B isn't."
what are A and B?

Step 1: Define prop variable.

p: "A is a knight."

q: "B is a knight"

comp A: $\neg p \wedge q$ Step 2: Write statement compound prop)

Step 3: Construct truth table.

p	q	$\neg p \wedge q$	
T	T	F X	
T	F	F X	
T	T	T X	knaves lies →
F	F	F ✓	

looking 4 a row(s) in which columns 1 (p) and 3 ($\neg p \wedge q$) match. p is F, q is F.

Conclude: A & B are both knaves

(34). A say: "We are both knights"

B say: "Either A is a knight or I am a knight but not both"

A: $p \wedge q$

B: $p \oplus q$

A: p	B: q	A: $p \wedge q$	B: $p \oplus q$	∴
T	T	T ✓	F X	X
T	F	F X	T X	X
F	T	F ✓	T ✓	both match.
F	F	F ✓	F ✓	

map

∴ A is a knave, B could be either.

Lecture3

01-19-2015

Propositional equivalence

A proposition is called:

→ a tautology if it is always T

→ a contradiction ——— F

→ → a contingency if it can assume both T and F values

Satisfiable

E.g. contingency = $\neg p$, $p \wedge q$, ...

contradiction = $p \wedge \neg p$

tautology = $p \vee \neg p$

($p \vee q$ $\neg p \rightarrow q$ logically equivalent)

Def Propositions P and Q are called logically equivalent ($P \equiv Q$) if they always assume the same truth value.

ie. $P \leftrightarrow Q$ is a tautology

E.x. Show that $p \rightarrow q$ and $\neg p \vee q$ are logically equivalent

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

identical cols

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

Ex. Show that $\neg(p \wedge q) \leftrightarrow \neg p \vee \neg q$ is a tautology.

p	q	$\neg(p \wedge q)$	$\neg p \vee \neg q$	
T	T	F	F	identical rows
T	F	T	T	
F	T	T	T	
F	F	T	T	

TABLE 5 Logical Equivalences.

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

TABLE 6 Logical Equivalences Involving Implications.

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

TABLE 7 Logical Equivalences Involving Biconditionals.

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

Ex. Use the table of logical equivalences to show $(p \to q) \wedge (p \to r)$ and $p \to (q \wedge r)$ are log. eq.

$$(p \to q) \wedge (p \to r) \equiv (\neg p \vee q) \wedge (\neg p \vee r) \quad \text{(impli)}$$
$$\equiv \neg p \vee (q \wedge r) \quad \text{(distributive)}$$
$$\equiv p \to (q \wedge r) \quad \text{(impli)}$$

Ex. Show that $(p \vee q) \wedge (\neg p \vee r) \to (q \vee r)$ is a tautology.

$$\neg\big((p \vee q) \wedge (\neg p \vee r)\big) \vee (q \vee r) \quad \text{(impli)}$$

$$\equiv \neg(p \vee q) \vee \neg(\neg p \vee r) \vee (q \vee r) \quad \text{(De Morgan Law)}$$

$$\equiv \big[(\neg p \wedge \neg q) \vee (\neg(\neg p) \wedge \neg r)\big] \vee (q \vee r) \quad \text{" + double neg law}$$

$$\equiv \big((\neg p \wedge \neg q) \vee q\big) \vee \big((p \wedge \neg r) \vee r\big) \quad \text{commutative \& associative}$$

→ absorption law?

$$\equiv \big((\neg p \vee q) \wedge (\neg q \vee q)\big) \vee \big((p \vee r) \wedge (\neg r \vee r)\big) \quad \text{dist law.}$$

$$\equiv \big((\neg p \vee q) \wedge \mathbf{T}\big) \vee \big((p \vee r) \wedge \mathbf{T}\big) \quad \text{(Negation)}$$

R/L diff! — do need!

$$\equiv (\neg p \vee q) \vee (p \vee r) \quad \text{(Identity law)}$$

$$\equiv (\neg p \vee p) \vee (q \vee r) \quad \text{(comm \& assoc laws)}$$

$$\equiv \mathbf{T} \vee q \vee r \equiv \mathbf{T} \quad \text{(Neg. Law \& Dominance L)}$$

Lecture 4

01-22-2015

e.g Write the following propositions in DNF.

$P: (a \to b) \leftrightarrow (a \wedge b)$

(a) Write a truth table for P:

a	b	$a \to b$	$a \wedge b$	$(a \to b) \leftrightarrow (a \wedge b)$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	F
F	F	T	F	T

(b) Find a DNF for P:

a	b	P	
T	T	T	←
T	F	T	←
F	T	F	
F	F	F	

$(a \wedge b) \vee (a \wedge \neg b) \equiv P$

$\Leftarrow$

Observe: $(a \wedge b) \vee (a \wedge \neg b) \equiv a$

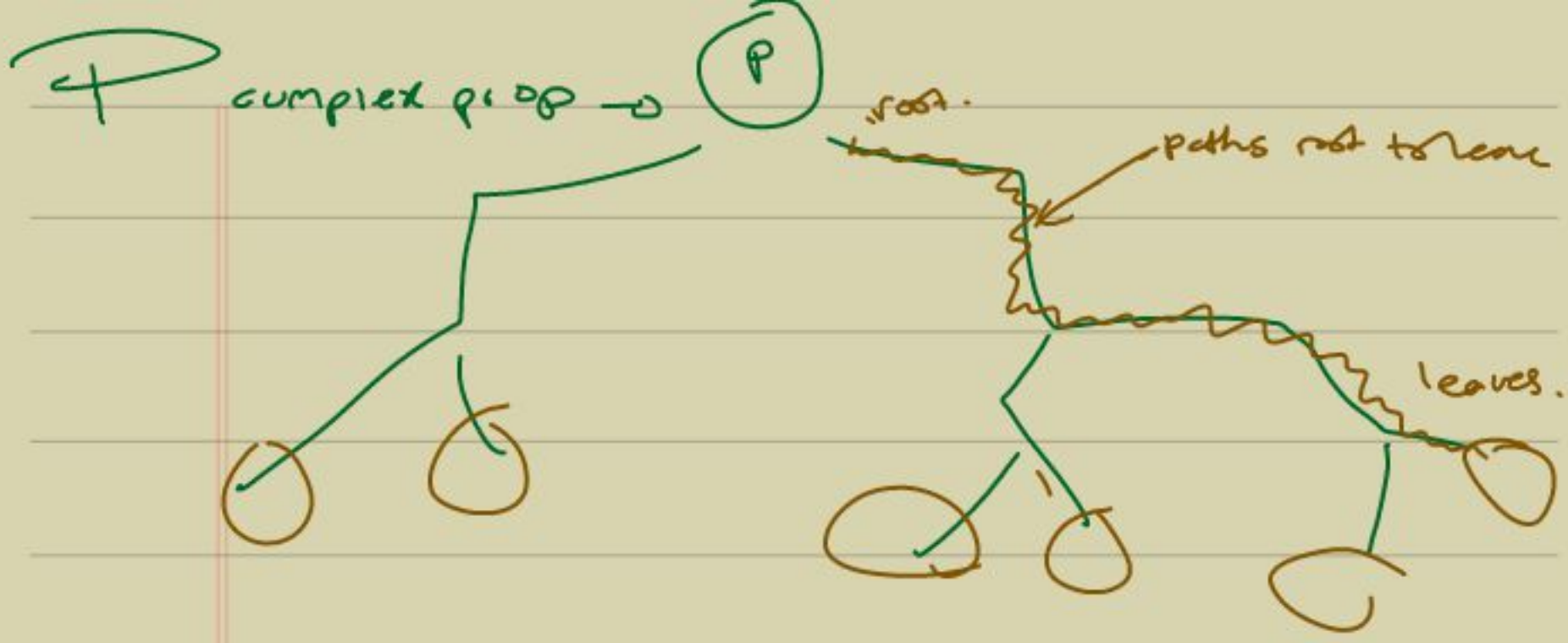
$a \wedge (b \vee \neg b) \equiv a \wedge T \equiv a$

$\therefore$ DNF is not unique

---

everything that is not literals are called (compled propostion.)

Contains logicall connectives other that just $\neg$



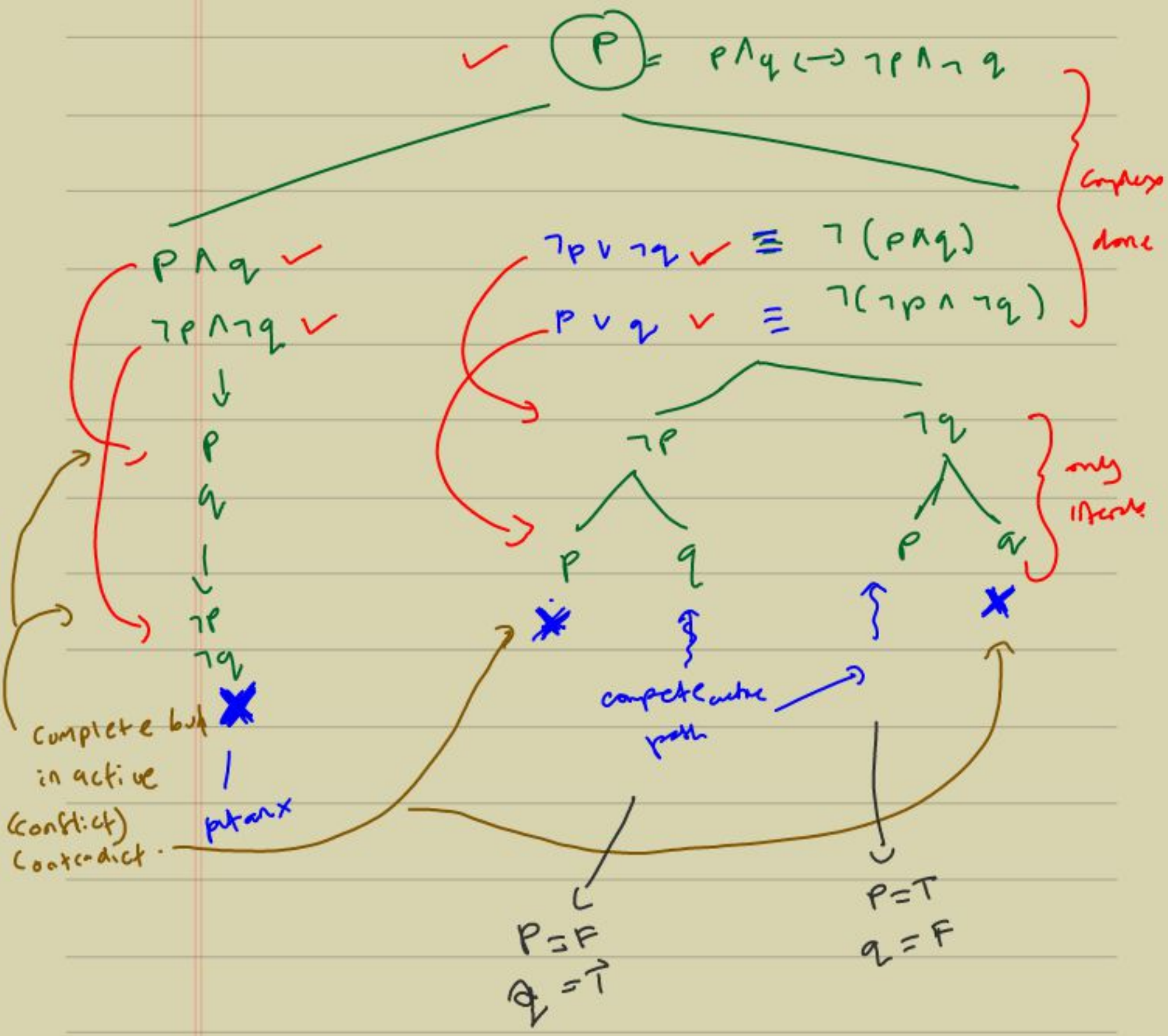
2 path ≤ active → no contradictions. (no P&¬P arising atomic)
inactive.

X at the end. ⇒ e.g P & ¬P in a path

when drawing ⇒ there's branching rules

do is complete if it contains no
unchecked complex prop

Let $P \equiv p \wedge q \leftrightarrow \neg p \wedge \neg q$



∴ We see P is T iff $P=T, q=F$ or $P=F, q=T$

∴ P is not a contradiction b/c there are truth assignments that make it T (we have complete active path)

∴ P is not a tautology b/c there are truth assignments for which P is F (the ones not covered by the complete active path)

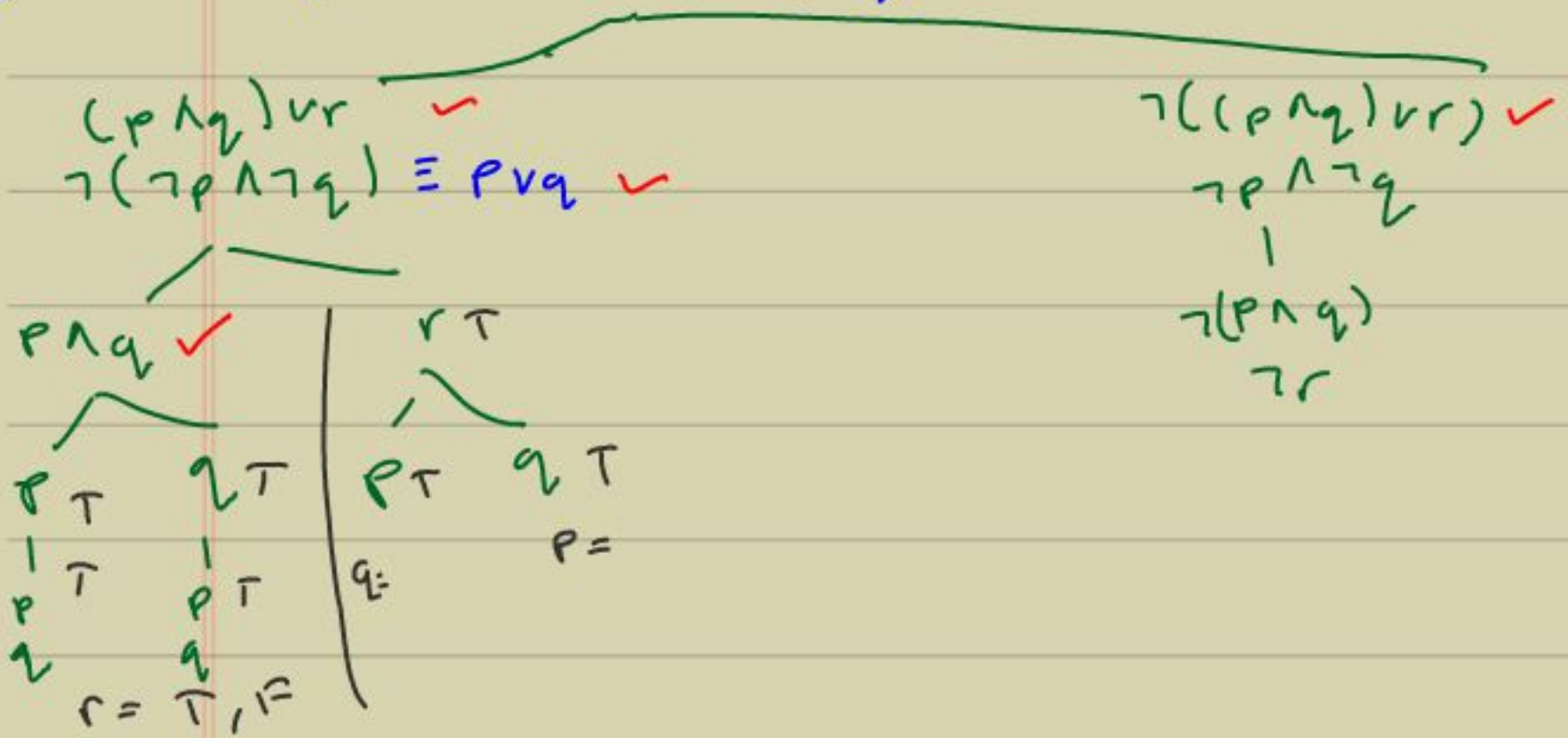
$\Longrightarrow$ Therefore it is contingency.

from previous ● DNF : $(p \wedge \neg q) \vee (\neg p \wedge q)$

From the complete active paths, we read the conjunctive clauses for the DNF for P.

---

(2) Construct a TT's for $\neg((p \wedge q) \vee r \longleftrightarrow \neg p \wedge \neg q)$



Lecture 5

01-26-2015

Examples on Truth Trees

MAT1348

1. Construct a complete truth tree for the proposition

$$P_1: \quad (p \wedge q) \vee r \leftrightarrow (\neg p \wedge \neg q).$$

   Find a DNF for P_1.

2. Construct a complete truth tree for the proposition

$$P_2: \quad \neg\left((p \wedge q) \vee r \leftrightarrow (\neg p \wedge \neg q)\right).$$

   Find a DNF for P_2.

3. Use truth trees to determine whether

$$P_3: \quad p \wedge q \leftrightarrow \neg p \wedge \neg q$$

   is a contradiction. If the answer is no, give a counterexample.

4. Use truth trees to determine whether

$$P_4: \quad (p \vee q) \wedge (\neg p \vee r) \rightarrow q \vee r$$

   is a tautology. If the answer is no, give a counterexample.

5. Use truth trees to determine whether the set of propositions

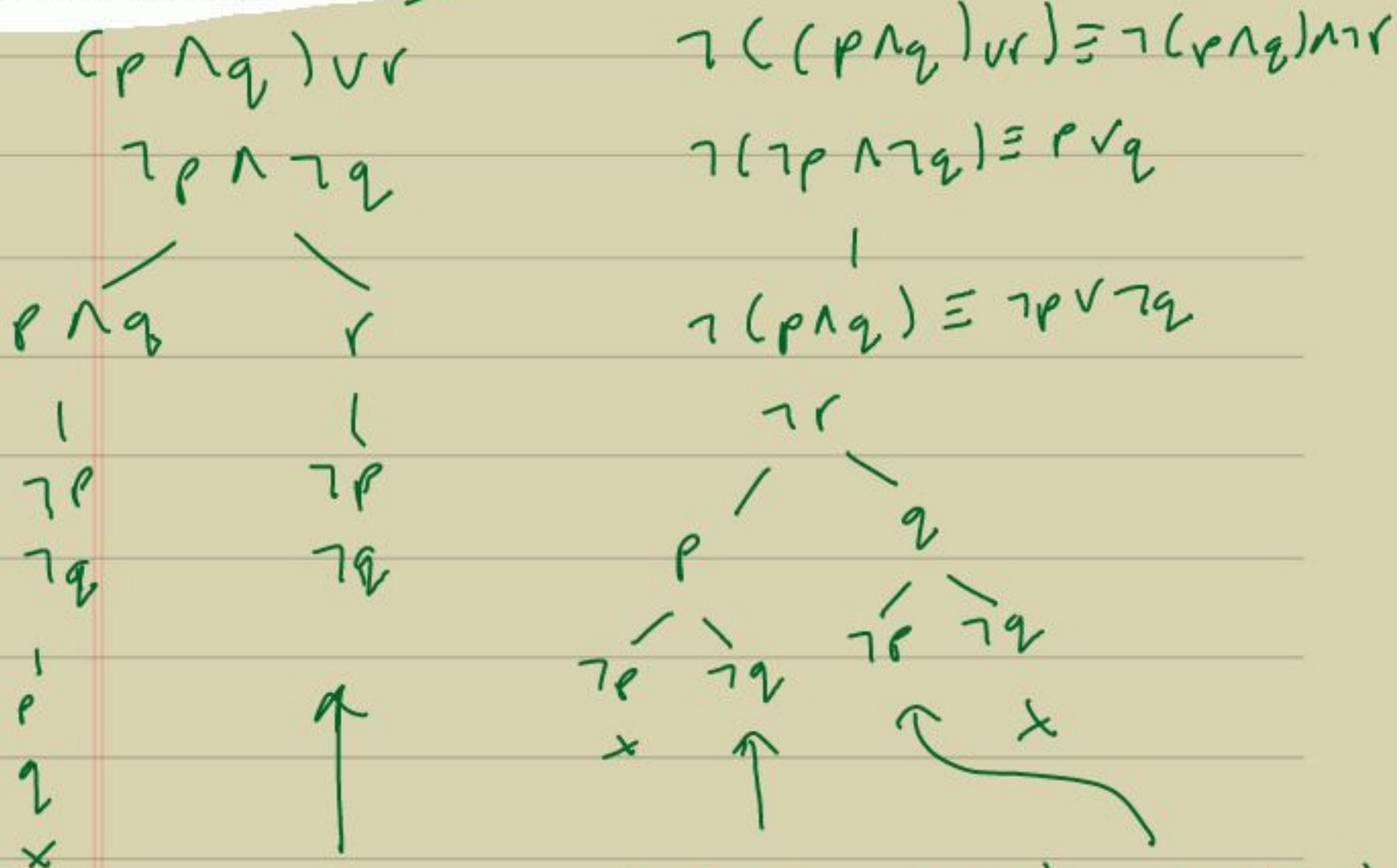
$$\{p \rightarrow (\neg r \vee q), p \leftrightarrow (q \wedge r), p \rightarrow r\}$$

   is consistent.

1. Construct a complete truth tree for the proposition

$$P_1: \quad (p \wedge q) \vee r \leftrightarrow (\neg p \wedge \neg q).$$

Find a DNF for P_1.



DNF: $(\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \; (\neg p \wedge q \wedge \neg r)$

P_1 is true iff

p = F	or	p = T		or	p = F		
q = F		q = F			q = T		
r = T		r = F			r = T		

is P_1 a contradiction

NO as it is true for certain truth assignment. we have three (counter examples)

if P_1 a tautology

NO it is not always T. there are $2^3 - 3 = 5$ counterexamples, e.g

p = T
q = T
r = T

4. Use truth trees to determine whether

$$P_4 : \neg\big((p \vee q) \wedge (\neg p \vee r) \rightarrow q \vee r\big)$$

is a tautology. If the answer is no, give a counterexample.

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

Is $P_4 \Rightarrow$ a tautology $\rightsquigarrow$ P_4 true iff $\neg P_4$ is a cont.

$\neg P_4$

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

↓

$(p \vee q) \wedge (\neg p \vee r)$ ✓

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

↓

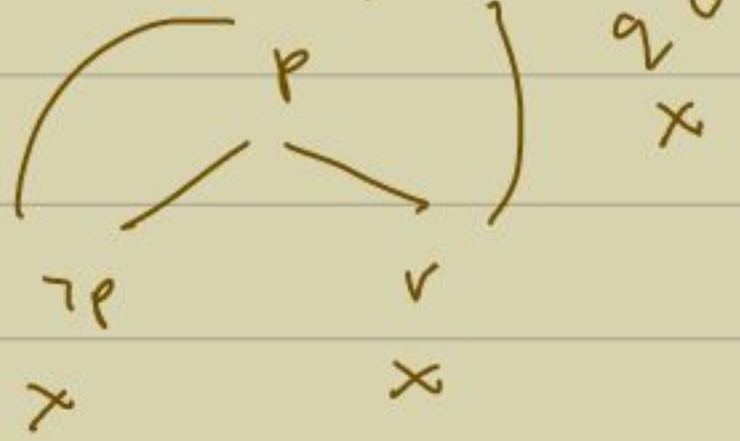
$p \vee q$ —

$\neg p \vee r$ —

↓

$\neg q$

$\neg r$



$\Rightarrow$ no complete active path

$\therefore$ no truth assignments make the prop T

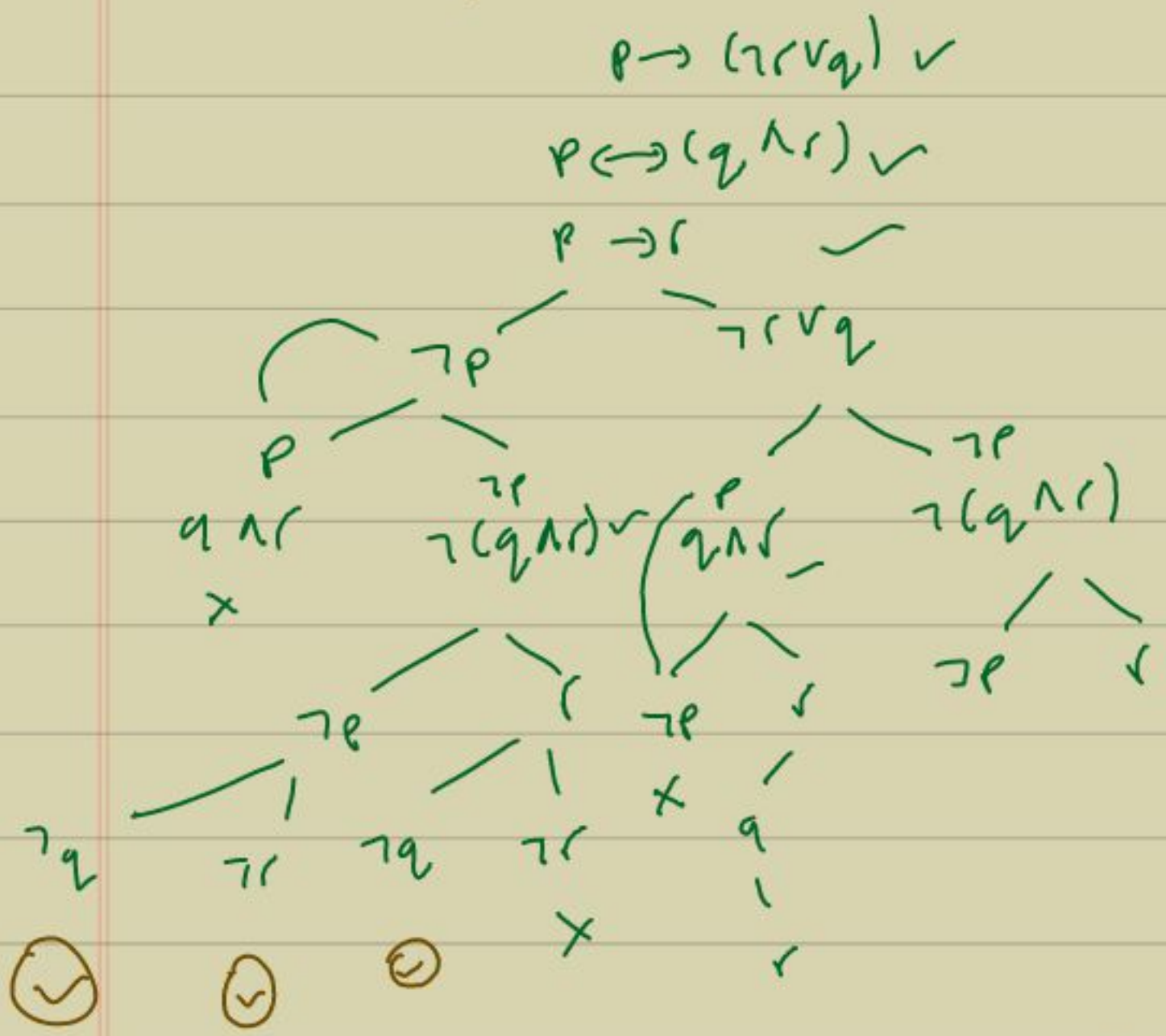
↓

$\neg P_4$

so P_4 is always T

$\therefore P_4$ is a tautology.

5. Is the set $\{p \to (\neg r \vee q),\ p \leftrightarrow q \wedge r,\ p \to r\}$ consistent.



$p = f$
$q = f$
$r = T/F$

} truth assignment that make all true.

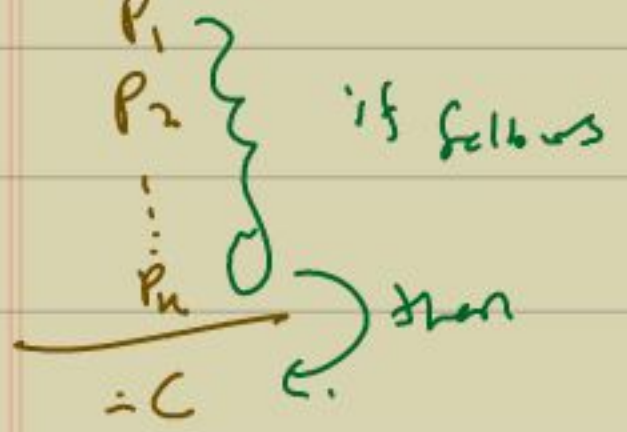
∴ so the set is indeed consistent

Arguments

$(P_1 \wedge P_2 \wedge \dots \wedge P_n) \rightarrow C$

$P_1, P_2, \dots, P_n$ — premises or hypotheses

C — conclusion



- Any valid argument's complex prop ($\rightarrow$) is a tautology
- Arg is valid if $(P_1 \wedge \dots \wedge P_n) \rightarrow C$ is a tautology

Lecture 6

01-29-2015

Q.4. arg example lectures:

(ii) using truth tables.

l	S	m	l ∨ ¬S	m → ¬l	S → ¬m	(P1 ∧ P2) → C1
T	T	T	T	F	F	
T	T	F	T	T ✓	T ✓	all T.
T	F	T	T	T	T	
T	F	F	T	T ✓	T ✓	
F	T	T	F	T	F	
F	T	F	F	T	T	
F	F	T	T	T	T	
F	F	F	T	T	T	

∴ In all rows where P1 & P2 are T, C1 is also T.

Hence P1 ∧ P2 → C1 is a tautology - and the arg is valid.

(iii) Using truth trees. a: is P1 ∧ P2 → C1 a tautology?
ie ¬(P1 ∧ P2 → C1) is a contradiction?

¬((P1 ∧ P2) → C1)

≡ ¬(¬(P1 ∧ P2) ∨ C1)

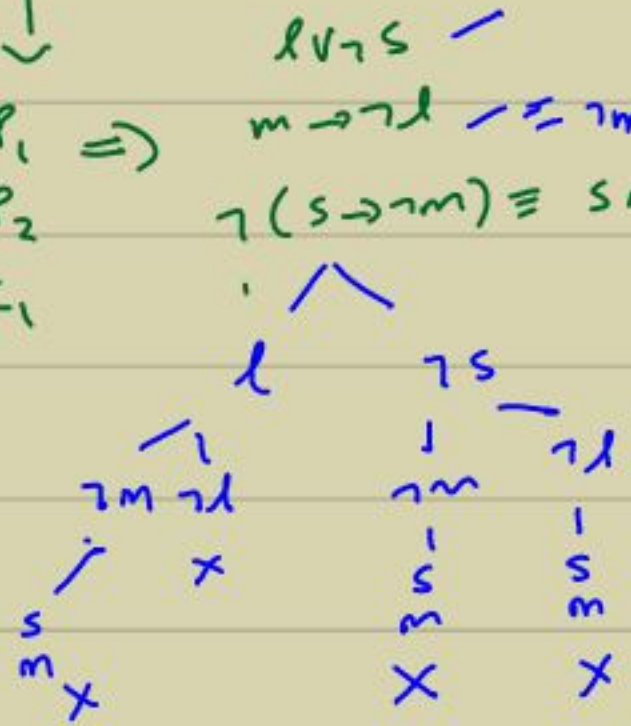
≡ (P1 ∧ P2) ∧ ¬C1

∴ no complete open path.
∴ the negation of the arg is a contradiction, and the arg is a tautology. Hence its valid.

P1 ⇒ l ∨ ¬S / m → ¬l / ≡ ¬m ∨ ¬l / ¬(S → ¬m) ≡ S ∧ m /

P2

¬C1



Question 2. $l \vee s$, $m \to l$ valid?

$\therefore \neg m \to s l$

There are rows where P_1 & P_2 are both T, but C_2 is F.

Hence $P_1 \wedge P_2 \to C_2$, is not always T. and it is invalid.

$P_1 \wedge P_2 \to C_1$

T $\quad$ F $\Rightarrow$ F.

counter ex.

(if) truth assignments that make all premises T and cond F): (1) $l = s = T$, $m = F$

(2) $l = T$, $s = m = F$

T. Table

We have complete active path: neg of arg is not a contr. So arg is not a tautology. So arg is invalid

9

Lecture 7

02-02-2015

Examples of proofs-by-type

Direct proof

Thm. Let n be an integer. **If n is odd, then n^2 is odd.**

Proof strategy: The statement to prove is of the form $p \to q$, where

p: "n is odd"

q: "n^2 is odd"

∴ using a direct proof, we assume p, and show q follows.

Proof: Assume n is odd. Hence $n = 2m+1$ for some integer m.

Then: $n^2 = (2m+1)^2 = 4m^2+4m+1 = 2(2m^2+2m)+1$

Since m is an integer, $2m^2+2m$ is an integer, say $k = 2m^2+2m$. Thus $n^2 = 2k+1$, so n^2 is odd (q). □ QED

Indirect proof

Thm: Let n be an integer. If $5n+4$ is odd, then n is odd.

Proof strategy: The statement is of the form $p \to q$, where

p: "$5n+4$ is odd"

q: "n is odd"

Using indirect proof (by contrapositive), we prove the contrapositive $\neg q \to \neg p$ using a direct proof. Hence assume $\neg q$ and show $\neg p$ follows.

Note: $\neg q$: "n is even"

$\neg p$: "$5n+4$ is even"

Proof: Assume n is even. Then $n = 2k$ for some integer k

Then, $5n+4 = 5(2k)+4 = 2(5k+2)$

Since k is integer, so is $m = 5k+2$ is integer.

Hence, $5n+4 = 2m$, where m is an integer.

So $5n+4$ is even $\square$

Definitions

Def An integer n is called:

- **even** if $n = 2k$ for some integer k.
- **odd** if $n = 2m+1$ for some integer m

Proof by contradiction (Paul Erdos)

Thm: $\sqrt{2}$ is irrational.

Proof strategy: The statements of the form P where

P: "$\sqrt{2}$ is irrational"

For a proof by contradiction, assume $\neg P$, and derive a contradiction Note $\neg P$: "$\sqrt{2}$ is rational"

Proof: Assume $\sqrt{2}$ is rational. Then, there exist integers a and $, b \neq 0$ s.t. $\sqrt{2} = \frac{a}{b}$. claim we may assume that a and b have no common divisor >1. If not: $a = da'$, $b = db'$, and $\frac{a}{b} = \frac{da'}{db'} = \frac{a'}{b'}$. and we take a', b' instead. So: we may assume that a/b is a reduced fraction. $\sqrt{2} = \frac{a}{b}$ / $2 = \frac{a^2}{b^2}$ / $2b^2 = a^2$

Now: a^2 is even, so a must be even. Hence $a = 2k$ for some integer k. Then: $2b^2 = (2k)^2 = 4k^2$. $\therefore b^2 = 2k^2$ and b is even. We have that 2 divides both a & b, $\rightarrow\leftarrow$ since a/b is a reduced fraction. Conclud $\sqrt{2}$ is irrational $\square$

Def: Let m, n be positive integers If $n = km$ for some integer k, then we say:

- m divides n (or is divisor of n)
- n is a multiple of m
- write $m \mid n$ "m divides n"

Def. A real number r is rational if $r = \frac{p}{q}$ for some int

For p & q, $q \neq 0$.

A real number that is not rational is irrational (π, i) (real but not rational)

Proof by cases

We are proving $P \to q$ where $P = P_1 \vee P_2 \vee \dots \vee P_k$

$$P \to q \equiv P_1 \vee P_2 \vee \dots \vee P_k \to q \equiv \neg(P_1 \vee P_2 \vee \dots \vee P_k) \vee q$$

$$\equiv (\neg P_1 \wedge \neg P_2 \wedge \dots \wedge \neg P_k) \vee q$$

$$\equiv (\neg P_1 \vee q) \wedge (\neg P_2 \vee q) \wedge (\neg P_3 \dots \wedge (\neg P_k \vee q)$$

$$\equiv (P_1 \to q) \wedge (P_2 \to q) \wedge \dots \wedge (P_k \to q)$$

Thm: On the Island of Kkk, we have natives A, B, C.

A: "All of us are knaves."

B: "Exactly one of us is a knave"

Then C is a knight

Proof strategy: Define the following propositions.

a: "A is a knight."

b: "B is a knight."

c: "C is a knight."

We must prove c is T

identical.	
Def $P_1 = a$	$a \wedge b$
$P_2 = \neg a \wedge b$	$a \wedge \neg b$
$P_3 = \neg a \wedge \neg b$	

we need to prove $c \equiv (P_1 \vee P_2 \vee P_3) \to c \equiv (P_1 \to c) \wedge (P_2 \to c) \wedge (P_3 \to c)$

$P_1 \vee P_2 \vee P_3 \equiv T$

Case 1: to prove $P_1 \to c$ (example of vacuous proof)

Assume $P_1 = a$. Hence a is T and A is a knight.

So A is telling the truth, and A, B, C are all knaves, a contradiction

Hence, a is F, and $P_1 \to C$ is T

Case 2: to prove $P_2 \to c$

Assume P_2 is T, ie. a is F and b is T. So A is a knaves and B is a knight. Since B is telling the truth exactly 1 (A) is a knave. Hence C is a knight. ie c is T.

Case 3: To prove $P_3 \to C$

Assume P_3 is T, so a and b are F, and A & B are both knaves. Since A is lying, not all of A, B, C are knaves, and C is a knight. Thus, C is T □

Vacuous proof

Thm If $0 > 1$, then $\sqrt{2}$ is rational

($0 > 1$: $p \equiv F$; $\sqrt{2}$: q)

Proof Since p is F, $P \to q$ is T □

Trivial proof

Thm: If $0 < 1$, then $\sqrt{4}$ is rational.

($0 < 1$: p; $\to$; $\sqrt{4}$: q)

Proof Since q is T, $p \to q$ is T.

Lecture 8

02-05-2015

Proof by Equivalence

Thm Let m, n be +ve integers. Then; $m=n$ if and only if $m \mid n$ and $n \mid m$

Proof strategy The proposition to prove is in the form $p \leftrightarrow q$ where:

p: "$m=n$"

q: "$m \mid n$ and $n \mid m$"

We need to prove $p \to q$ and $q \to p$.

Proof To prove $p \to q$:

Assume $m=n$. We have $n = 1 \cdot m$ so $m \mid n$ and also $m = 1 \cdot m$ so $n \mid m$. Hence $m \mid n$ and $n \mid m$, and q follows.

$n = km$
$m = ln$

To prove $q \to p$:

Assume $m \mid n$ and $n \mid m$. Hence $n = km$ and $m = ln$ for some integers k and l. Then:

$n = km = k(ln) = (kl)n$

$n - (kl)n = 0$

$n(1 - kl) = 0$

$1 - kl = 0$

$kl = 1$

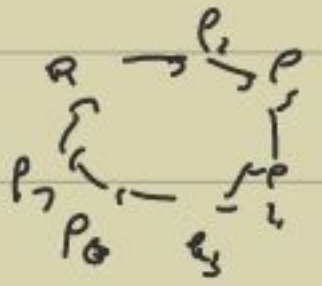
* Since $m, n > 0$, $k, l > 0$.

So, $k = l = 1$. Hence $n = 1 \cdot m = m$

Thus p follows

Note: To prove that propositions P_1, P_2, P_k are mutually equivalent, it suffices to prove:

$P_1 \to P_2$, $P_2 \to P_3$, ..., $P_k \to P_1$



Thm Let a and b be real numbers. Then the following are equivalent:

(i) $a<b$ (ii) $\frac{a+b}{2} > a$ (iii) $\frac{a+b}{2} < b$

Proof. To prove (i) → (ii)

Assume $a<b$. Then $a<b$ $\}+a$

$2a<b+a$

$a<\frac{a+b}{2}$ so (iii) follows

To prove (ii) → (iii)

Assume $\frac{a+b}{2} > a$. then:

$a+b>2a$

$b>a$

$2b>a+b$

$b>\frac{a+b}{2}$ so (iii) follows

To prove (iii) → (i): exercise □

Bonus proof (mixed types)

Thm The equation $x^3+x+1=0$ has no rational roots.

Proof (By contradiction, then by cases)

Suppose $x^3+x+1=0$ has a rational root $r=\frac{a}{b}$ where a, b are integers, $b\neq 0$, and $\frac{a}{b}$ is reduced.

Hence $\left(\frac{a}{b}\right)^3+\frac{a}{b}+1=0 \quad \} \cdot b^3$

$$a^3+ab^2+b^3=0$$

Case 1: a is even: then a^3+ab^2 is even. So b^3 is even.

Suppose b is odd, $b=2k+1$ for an integer k.
Then $b^3=(2k+1)^3=8k^3+12k^2+2k+1$.
$=2(4k^3+6k^2+k)+1$, so b^3 is odd, $\Rightarrow\Leftarrow$

Hence b is even. Hence $\frac{a}{b}$ is not reduced, contradiction.

Case 2: a is odd. Then $a^3+ab^2+b^3=0$. If b is odd,

odd + [odd + odd] = odd + [even + even] = odd + even

Then ab^2 and b^3 are both odd; if b is even then ab^2 and b^3 are both even. In any case, ab^2+b^3 is even.

Hence $a^3+ab^2+b^3$ is odd, and hence $\neq 0$, a contradiction.

Conclusion: There is no rational number $\frac{a}{b}$ that is a root of $x^3+x+1=0$

2.1 Sets

Def: A set is a well-defined unordered collection of objects (elements or members)

E.g.: {students in this classroom}
{classes that you are taking this term}

$A = \{1, 2, a, \text{Ottawa}\}$

$1 \in A$ "1 is an element of set A"

$3 \notin A$ "3 is not an element of set A"

$S = \{a, b, c\}$, $T = \{b, c, a\}$, $U = \{a, a, b, c\}$

we have $S = T = U$.

Def. Two sets are equal if they have the same elements (regardless of the order listed, and multiplicity).

Well defined?

$S = \{A : A \text{ is a set that does not contain itself}\}$

This a self-referred definition. – there is no set like this

Barber's paradox.

Describing a set - A.

(1) by listing its elements (using ellipses if needed)

e.g $A = \{a, e, i, o, u\}$

$B = \{3, 6, 9, \cdots, 36\}$

$C = \{3, 4, 5, 6, \cdots\}$

(2) Using a self-builder notation

e.g $A = \{l : l$ is a lower-case vowel of the Eng alphabet$\}$

$B = \{3n : n$ is an integer, $1 \leq i \leq 12\}$

$C = \{n : n$ is an integer, $n \geq 3\}$

Important standard. Sets of numbers.

$\mathbb{N} = \{0, 1, 2, 3, \cdots\}$ the sets of natural numbers.

$\mathbb{Z} = \{\cdots, -1, 0, -1, \cdots\}$ the set of integers / whole numbers

$\mathbb{Q} = \{\frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N}, b \neq 0\}$ the set of rational numbers

$\mathbb{R} = \{r : $ real number is $r\}$

$\mathbb{C} =$ set of complex numbers

$\mathbb{Z}^+ = \{n \in \mathbb{Z} : n > 0\} = \{1, 2, 3, \cdots\}$ ... set of +ve $\mathbb{Z}$

similarly we define $\mathbb{Z}^-$, $\mathbb{Q}^+$, $\mathbb{Q}^-$, $\mathbb{R}^+$, $\mathbb{R}^-$, ...

The emptyset: either $\{\}$ or $\emptyset$

Note: $\{\emptyset\}$ is not an empty set

The universal set; $\mathcal{U}$ (set of all objects under consideration)

Lecture9

02-09-2015

Def: A set A is a subset of a set B (denoted $A \subseteq B$) if every elt. of A is also an elt of B. That is if the implication

$x \in A \Rightarrow x \in B$ is $\top$ for all $x \in U$.

e.g. $A = \{a, b, c\}$, $B = \{a, c\}$, $C = \{a, \{b\}, c\}$

$B \subseteq A$, $B \subseteq C$, $A \not\subseteq B$, $A \not\subseteq C$ (b/c $b \notin C$)

also $A \neq C$

E.g. $\emptyset \subseteq \mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

Trivial subsets For any set S: (1) $S \subseteq S$

(2) $\emptyset \subseteq S$ (example of a vacuous proof)

Def. A set A is called a proper subset of a set B if $A \subseteq B$ and $A \neq B$

(Written $A \subset B$, or $A \subsetneq B$)

Ex. $S \subseteq S$ but $S \not\subset S$

thm $A=B$ iff $A \subseteq B$ and $B \subseteq A$

To prove that $A=B$, we must prove $A \subseteq B$ and $B \subseteq A$.

Cardinality

Def: If a set A has exactly n (distinct) elements where $n \in \mathbb{N}$ then A is called finite set n is its cardinality (or size); denoted $|A|=n$.

Ex. $A = \{a, b, c\}$, $|A|=3$

$B = \{a, b, a\}$, $|B|=2$

$C = \{3n : n \in \mathbb{Z}, 1 \le n \le 12\}$ $|C|=12$

$D = \{a, \{a\}, \{a, \{a\}\}\}$ $|D|=3$

Ex. $A = \{a, b, c\}$

All subsets of A:

0-elt subsets: $\emptyset$

1-elt subsets: $\{a\}, \{b\}, \{c\}$ "singletons"

2-elt subsets: $\{b, c\}, \{a, c\}, \{a, b\}$

3-elt subsets: $\{a, b, c\}$

$P(A) = \{\phi, \{a\}, \{b\}, \{c\}, \{a,B\}, \{q,(\}, \ldots\}$

Power set of A

Def: The power set of a set A is the set containing all subsets of A (denoted $P(A)$ or 2^A)

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

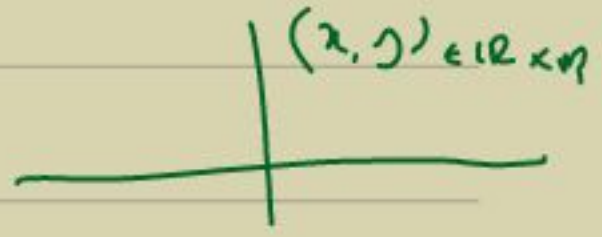
Cartesian products

Eg: $S = \{w,b,g\}$, $P = \{B,G\}$

$S \times P = \{(w,B), (w,G), (b,G), (b,B), (g,B), (g,G)\}$

Def. The Cartesian product of sets A & B is the set of all ordered pairs (a,b) for $a \in A$, $b \in B$ That is,

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



(E.g) ~~$S \times B$~~ $(G,w) \notin S \times P$
$(w,G) \in S \times P$

Notes: * In general, $A \times B \neq B \times A$

So cartesian product is not commutative

e.g. $\{a,b\} = \{b,a\}$ but $(a,b) \neq (b,a)$

unordered pairs — ordered pairs.

Def cartesian product of sets $A_1, A_2, \dots, A_n$:

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$$

↑ n-tuple, n-dim vector.

Notation: $A^n = \underbrace{A \times A \times \dots \times A}_{n \text{ times}} = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in A\}$

e.g. $\mathbb{R}^n$

Thm $|A \times B| = |A| \cdot |B|$

Proof $A \times B = \{(a, b) : a \in A, b \in B\}$

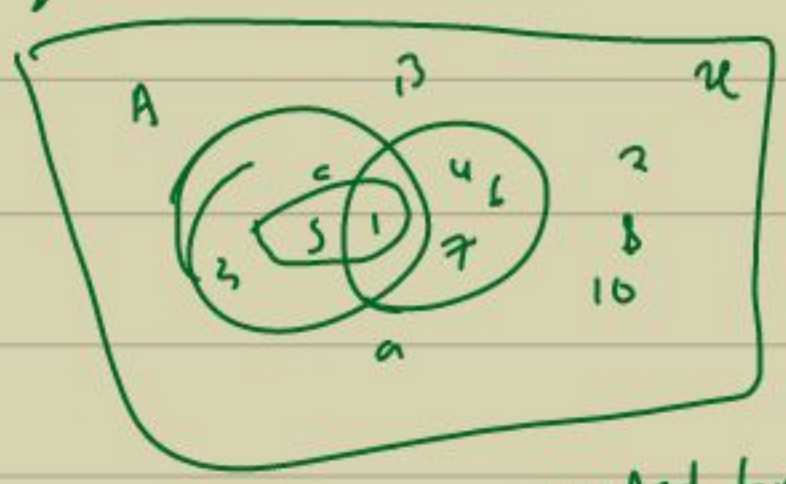
↑ $|A|$ options. ↖ $|B|$ options.

So $|A \times B| \le |A| \cdot |B|$

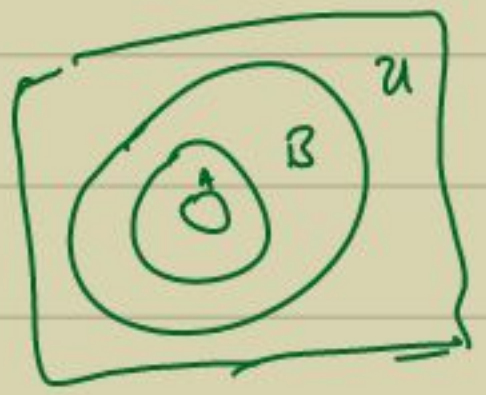
2.2. Set operations.

Venn diagrams.

e.g. $U = \{1, 2, \dots, 10\}$, $A = \{1, 3, 5\}$, $B = \{1, 4, 6, 7\}$, $C = \{1, 5\}$.



e.g. $A \subseteq B$ is represented by



Intersection and union of sets

A, B sets

Union $A \cup B =$

$\{x : x \in A \vee x \in B\}$

e.g. $A = \{1, 2, 3\}$, $B = \{1, 3, 5, 7\}$,

$C = \{5, 7\}$, $A \cup B = \{1, 2, 3, 5, 7\}$

Intersection: $A \cap B = \{x : x \in A \wedge x \in B\}$

$A \cap B = \{1, 3\}$ $A \cap C = \emptyset$

$B \cap C = \{5, 7\} = C$

In general: if $C \subseteq B$, then $B \cap C = C$

$B \cup C = \{1, 3, 5, 7\} = B$

In general: if $C \subseteq B$, then $B \cup C = B$

Def

Sets A and B are disjoint if $A \cap B = \emptyset$

Difference, complement, symmetric difference

Difference $A - B = \{x : x \in A \wedge x \notin B\}$

complement: $\bar{A} = \{x : x \in U \wedge x \notin A\}$

Symmetric difference

$A \oplus B = \{x : x \in A - B \vee x \in B - A\}$

$= (A - B) \cup (B - A)$

$= (A \cup B) - (A \cap B)$

Eg. $A=\{1,2,3\}$, $B=\{1,3,5,7\}$, $C=\{5,7\}$, $U=\{1,\dots,10\}$

$A-B=\{2\}$ $\quad \bar{B}=\{2,4,6,8,10\}$

$B-A=\{5,7\}$ $\quad A\cap\bar{B}=\{2\}$

Observe: $A-B=A\cap\bar{B}$

$A\oplus B=\{2,5,7\}$

$=(A-B)\cup(B-A)$

$(A\cup B)-(A\cap B)=\{1,2,3,5,7\}\cup\{1,3\}=\{2,5,7\}=A\oplus B$

Lecture 10

02-12-2015

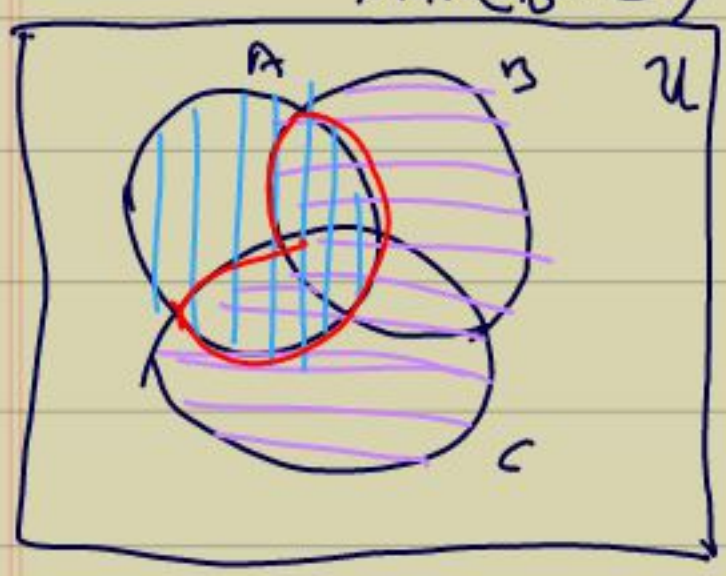
Set identities.

to

1) Using Venn diagrams.
2) Proving using membership tables.
3) Proving rigorously using definitions of set operations and the rules of logic.

Eg. (1) show $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

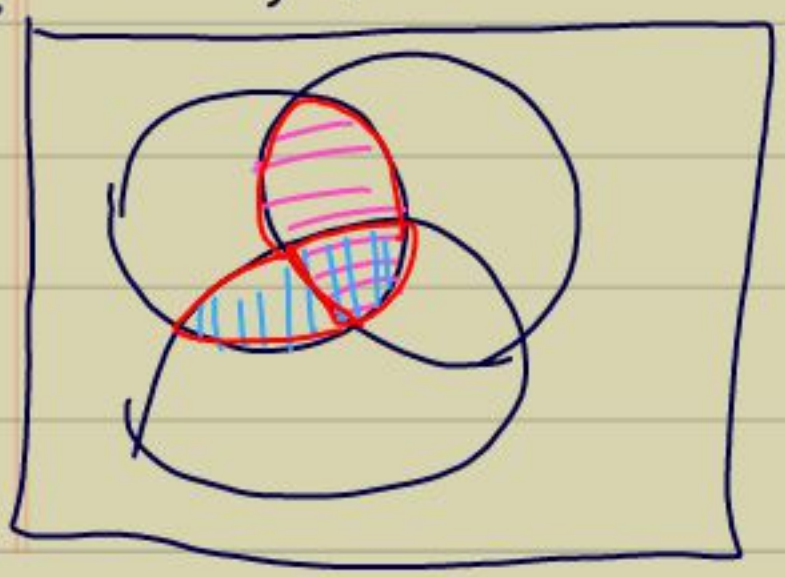
$A \cap (B \cup C)$



$B \cup C$:≡

A :≡ ||||

$(A \cap B) \cup (A \cap C)$



$A \cap B$:≡

$A \cap C$:≡ ||||

(2) Prove $\overline{A \cup B} = \bar{A} \cap \bar{B}$

A	B	$A \cup B$	$\overline{A \cup B}$	$\bar{A}$	$\bar{B}$	$\bar{A} \cap \bar{B}$
1	1	1	0	0	0	0
1	0	1	0	0	1	0
0	1	1	0	1	0	0
0	0	0	1	1	1	1

identical columns

(3) Prove $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Let $S_1 = \overline{A \cap B}$ and $S_2 = \bar{A} \cup \bar{B}$

We must prove $S_1 = S_2$. This is done by proving $S_1 \subseteq S_2$ and $S_2 \subseteq S_1$

To show $S_1 \subseteq S_2$:

Take any $x \in S_1$. Then $x \in \overline{A \cap B}$. Hence $x \notin A \cap B$, and so (*) $x \notin A$ or $x \notin B$. Therefore $x \notin \bar{A}$ or $x \notin \bar{B}$. $\therefore x \in \bar{A}$ or $x \in \bar{B}$.

Hence $x \in \bar{A} \cup \bar{B}$, so $x \in S_2$. That shows $S_1 \subseteq S_2$.

(*) That is, it is not the case that $x \in A$ and $x \in B$

$x \in A \cap B$, so it is not

To

To show $S_2 \subseteq S_1$

Take any $x \in S_2$. So $x \in \bar{A} \cup \bar{B}$, therefore $x \in \bar{A}$ or $x \in \bar{B}$.

Hence, $x \notin A$ or $x \notin B$, so $x \notin A \cap B$, which means, $x \in \overline{A \cap B}$. Thus $x \in S_1$. This shows $S_2 \subseteq S_1$ □

Using basic set identities to prove others

e.g. Show $\overline{A \cup B \cup C} = \bar{A} \cap \bar{B} \cap \bar{C}$

$\overline{A \cup B \cup C} = \overline{A \cup (B \cup C)}$ (Assoc Law)

$= \bar{A} \cap \overline{(B \cup C)}$ (De Morgan's Law)

$= \bar{A} \cap (\bar{B} \cap \bar{C})$ (De Morgan's)

$= \bar{A} \cap \bar{B} \cap \bar{C}$ (Assoc Law)

---

e.g. Prove $C - (\bar{A} \cap B) = (C \cap A) \cup (C - B)$

$C - (\bar{A} \cap B) = C \cap \overline{(\bar{A} \cap B)}$

$= C \cap (\bar{\bar{A}} \cup \bar{B})$

$= C \cap (A \cup \bar{B})$

$= (C \cap A) \cup (C \cap \bar{B})$

$= (C \cap A) \cup (C - B)$

Note:
$A - B = A \cap \bar{B}$

$A - B =$
$= \{x \in A : x \notin B\}$

Def A function f from a set A to a set B is an assignment that assigns to each $a \in A$ exactly one $b \in B$ (written $b = f(a)$)

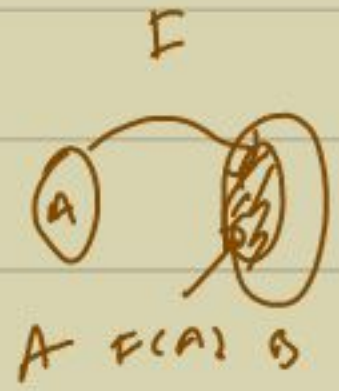
We write $f : A \to B$

A ... domain of F

B ... codomain of F

$f(a)$ ... image of $a \in A$

$f(A) = \{f(a) : a \in A\}$ ... image of set A.



$f^{-1}(b) = \{a \in A : f(a) = b\}$ .. preimage of $b \in B$.

(that is, $f(a) = b \leftrightarrow a \in f^{-1}(b)$)

$f(S) = \{f(a) : a \in S\}$ ... image of $S \subseteq A$.

e.g. We have $f : A \to B$, $A = \{a, b, c, d, e\}$,

$B = \{1, 2, 3, 4\}$,

defined by $f(a) = 1$, $f(b) = 4$, $f(c) = 1$, $f(d) = 2$,

$f(e) = 2$.

for example

Determine: $f(A) = \{1, 2, 4\}$

$f^{-1}(2) = \{d, e\} \subseteq A$

$f^{-1}(3) = \emptyset$

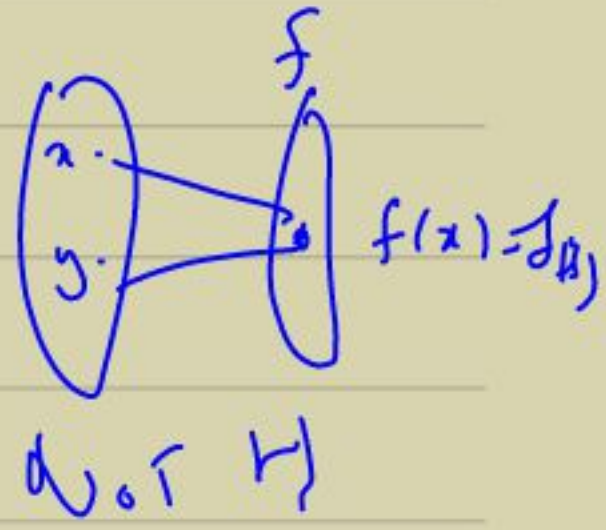
$f^{-1}(4) = \{b\}$

$f^{-1}(\{c, d, e\}) = \{1, 2\}$

One-to-one functions

Def A function $f: A \to B$ is 1-1 (or injective) if for all $x, y \in A$:

$f(x) = f(y) \rightarrow x = y$



Not 1-1

Lecture 11

02-23-2015

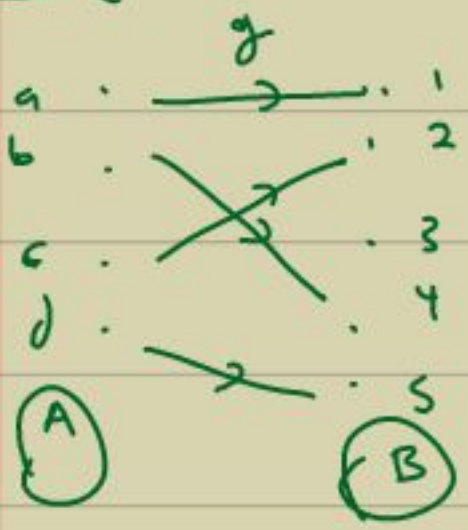
1 Def: $f: A \to B$ is <u>one-to-one</u> if for all $x, y \in A$: $f(x) = f(y) \to x = y$

E.g: From transparency.

F is not 1-1 b/c $\boxed{F(a) = f(c) = 1}$

Counterexample.

<u>E.g.</u> Example of a 1-1 function.



If $f: A \to B$ is 1-1, and A & B are finite sets, then $|A| \leq |B|$

<u>E.g</u> Is $f: \mathbb{R}^+ \to \mathbb{R}$, defined by $f(x) = x^2$, 1-1?

Take any $x, y \in \mathbb{R}^+$ and suppose $f(x) = f(y)$

$F(x) = f(y)$

$x^2 = y^2$

$x^2 - y^2 = 0$

$(x-y)(x+y) = 0$

$x - y = 0$ $\quad x + y = 0$

$\therefore x = y, \; x = -y$

But $x = -y$ is not possible b/c $x, y \in \mathbb{R}^+$. Hence $x = y$.

Conclude f is 1-1.

E.g. Is $g: \mathbb{R} \to \mathbb{R}$, def by $g(x) = x^2$, 1-1?

No. : Counterexample; $g(2) = g(-2) = 4$
(x, y)

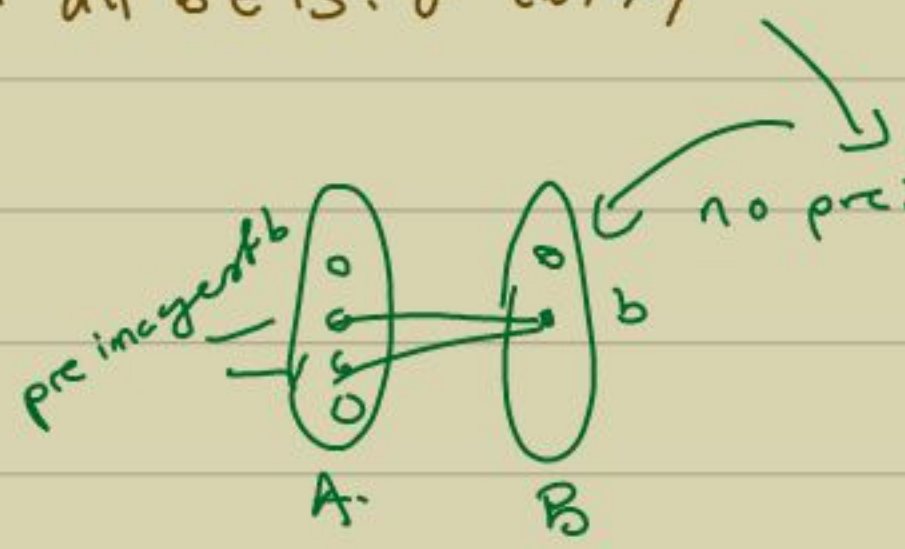
(We have $x \neq y$ with $g(x) = g(y)$.)

Def $f: A \to B$ is onto (or surjective) if (equivalently):

- for all $b \in B$, there exist $a \in A$ s.t. $f(a) = b$

(no lonely element in codomain)

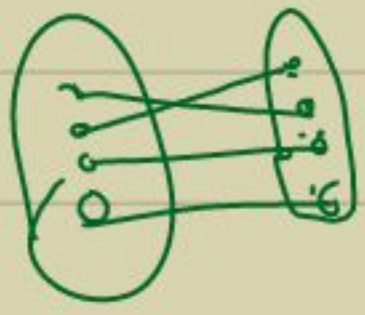
- $f(A) = B$
- for all $b \in B$: $f^{-1}(b) \neq \emptyset$



E.g. Example from transparency:

Not onto b/c there is no $x \in A$ s.t. $f(x) = 3$

onto function:



If $f: A \to B$ is onto and A & B are finite sets, then $|A| \geq |B|$

Ex. Is $f: \mathbb{R} \to \mathbb{R}^+$, defined by $f(x) = x^2$, onto?

Take any $b \in \mathbb{R}^+$. To show f is onto,
(codomain)

we must find $a \in \mathbb{R}$ s.t $f(a) = b$.

That is: $a^2 = b$

Then $a = \sqrt{a}$ or $a = -\sqrt{b}$

and $\sqrt{b}, -\sqrt{b} \in \mathbb{R}$ (in the codomain)

Conclusion: For all $b \in \mathbb{R}^+$, there exists an $a \in \mathbb{R}$ s.t $f(a) = b$; namely, $a = \sqrt{b}$ or $a = -\sqrt{b}$

Hence f is onto.

E.g. Is $g: \mathbb{R} \to \mathbb{R}$, def. by $g(x) = x^2$, onto?

No: counterexample, there is no $a \in \mathbb{R}$ s.t $g(a) = -1$

E.g. Is $f: \mathbb{Z}^2 \to \mathbb{Z}^2$, defined by

$f(x,y) = (x+2y, -x)$

one-to-one? onto?

Notes: $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(x,y) : x, y \in \mathbb{Z}\}$

$f((x_1,y_1) = f(x,y)$

$f(0,3) = (0+2\cdot 3, -0) = (6,0)$

Show f is 1-1: Take any $(x,y), (x',y') \in \mathbb{Z}^2$

Suppose $f(x,y) = f(x',y')$

Then: $(x+2y, -x) = (x'+2y', -x')$

So $x+2y = x'+2y'$ $\quad\quad$ $x - x' + 2y - y' = 0$

$-x = -x'$ $\quad\quad$ $-x - x' \quad\quad = 0$

Hence $x = x'$ and $y = y'$

and $(x,y) = (x',y')$

Conclude: f is 1-1

To prove f is (?) onto:

Take any $(a,b) \in \mathbb{Z}^2$ (domain). Can we find $(x,y) \in \mathbb{Z}^2$ (domain) s.t. $f(x,y) = (a,b)$?

If so, then $(x+2y, -x) = (a,b)$

So $x+2y = a$

$-x = b$

Then $x = -b$ and $y = \frac{a+b}{2}$

Note: if $a+b$ is odd, then $\frac{a+b}{2} \notin \mathbb{Z}$

Hence f is not onto

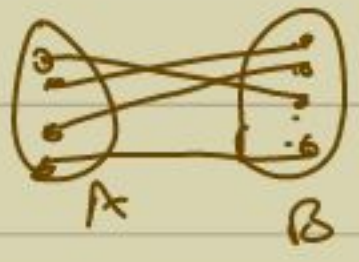
Alternatively, here is a counterexample there is no $(x,y) \in \mathbb{Z}^2$ s.t. $f(x,y) = (0,1)$

If there exist $(x,y) \in \mathbb{Z}^2$ s.t. $f(x,y) = (0,1)$,

then $\left.\begin{matrix} x+2y = 0 \\ -x = 1 \end{matrix}\right\}$ so $y = \frac{1}{2} \notin \mathbb{Z}$

Def A function $f: A \to B$ is a <u>bijection</u> (or <u>one-to-one correspondence</u>) if it is both one-to-one and onto

E.g. Example of a bijection:



If $f: A \to B$ is a bijection, and A, B are finite, then $|A| = |B|$.

Cardinality of infinite sets

Def If finite sets A and B have the same cardinality (i.e. $|A| = |B|$) if there exists a bijection $f: A \to B$.

E.g. $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| \neq |\mathbb{R}|$

E.g Is $f: \mathbb{R} \to \mathbb{R}$, def by $f(x) = 5x - 7$, a bijection?

To prove that it is 1-1:

Take any $x, y \in \mathbb{R}$ (domain) and suppose

$f(x) = f(y)$

$5x - 7 = 5y - 7$

$x = y$

Hence f is 1-1

To show f is onto:

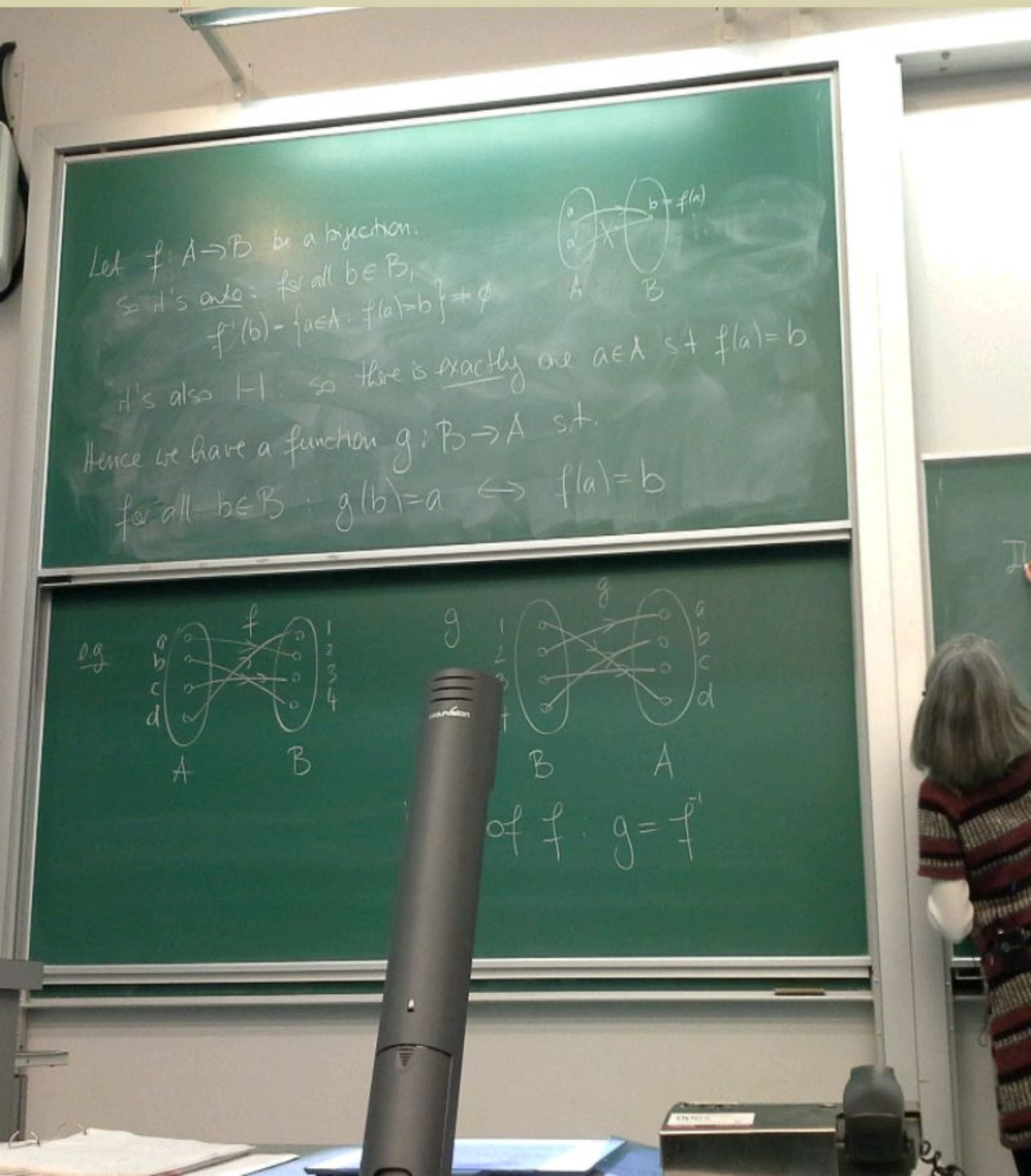
Take any $b \in \mathbb{R}$ (codomain), find $a \in \mathbb{R}$ (dom) s.t. $f(a) = b$; $5a - 7 = b$; $a = \frac{b+7}{5}$.

Since $b \in \mathbb{R}$, we have $a \in \mathbb{R}$ $\therefore f$ is onto

since it is 1-1 & onto, it is bijection.

Lecture 12

02-26-2015



Inverse functions

Def The inverse f^{-1} of $f: A \to B$ (if it exists) is a function $f^{-1}: B \to A$ defined by

$$f^{-1}(b) = a \iff f(a) = b$$

f is invertible if f^{-1} exists

Thm f is invertible $\iff$ it is a bijection. ←

eg Find f^{-1} for $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 5x - 7$

We have seen that f is a bijection, so it is invertible.

Take any $b \in \mathbb{R}$ (codomain). Find the unique $a \in \mathbb{R}$ (domain) s.t. $f(a) = b$.

(one & only one)

$f(a) = b$

$5a - 7 = b$

$a = \frac{b+7}{5}$ $(\in \mathbb{R}, \text{domain})$

So $f : \mathbb{R} \to \mathbb{R}$, $f^{-1}(b) = \frac{b+7}{5}$

unique = one and only one = exactly one

↑

distinct

e.g. What is wrong with this "def" of a 1-1 function?

"$f : A \to B$ is 1-1 if for each $a \in A$ there is a unique $b \in B$ s.t. $f(a) = b$."

a distinct, or different

The identity function

A any set

$1_A : A \to A$, def. $1_A(x) = x$ ... identity f. on A

It is a bijection, and hence invertible

$1_A^{-1} : A \to A$, $1_A^{-1}(x) = x$ so $1_A^{-1} = 1_A$

Composite functions

Def. Let $f : A \to B$ and $g : B \to C$ be functions

The composition $g \circ f$ [illegible] and g is the function $g \circ f : A \to C$ def by

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

Eg $f, g : \mathbb{R} \to \mathbb{R}$, $f(x) = 5x - 7$, $g(x) = x^2$

Find $g \circ f$ and $f \circ g$, if they exist

$g \circ f : \mathbb{R} \to \mathbb{R}$

$(g \circ f)(x) = g(f(x)) = g(5x-7) = (5x-7)^2$

$f \circ g \quad \mathbb{R} \to \mathbb{R}$

$(f \circ g)(x) = f(g(x)) = f(x^2) = 5x^2 - 7$

Conclude in general, $f \circ g \neq g \circ f$ (composition is not commutative)

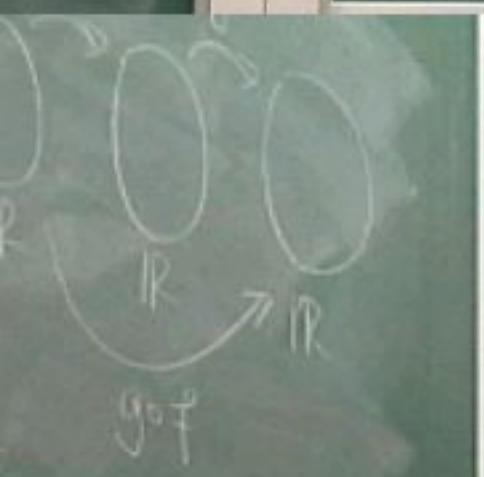
$f(a) = b$

$5a - 7 = b$

$a = \frac{b+7}{5}$

So f^{-1}, $\mathbb{R}$

unique = 1 distinct



Even if both ...ing are ...fined

...position is ...mutative)

Eg Let $f : A \to B$ be a bijection

Hence f has an inverse, $f^{-1} : B \to A$

Find $f \circ f^{-1}$ and $f^{-1} \circ f$

$f \circ f^{-1} \quad B \to B$

$f^{-1} \circ f \quad A \to A$

for any $b \in B$:

$(f \circ f^{-1})(b) = f(\underbrace{f^{-1}(b)}_{a}) = f(a)$ where $a = f^{-1}(b)$

$= b$

so $f \circ f^{-1} = 1_B$

so $f(a) = b$

Similarly, $f^{-1} \circ f = 1_A$

Eg $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 5x - 7$

$g: \mathbb{R} \to \mathbb{R}^+ \cup \{0\}$, $g(x) = x^2$

$g \circ f : \mathbb{R} \to \mathbb{R}^+$

$f \circ g$ does not exist

① Do the following assignment define functions? If so, are they one-to-one, onto?

(a) $f: \mathbb{R} \to [0, \infty)$, $f(x) = 5e^x$

Yes, a function

Is it 1-1?

Suppose $f(x) = f(y)$ for some $x, y \in \mathbb{R}$

Then $5e^x = 5e^y$

$e^x = e^y$

$\ln(e^x) = \ln(e^y)$

$x \ln(e) = y \ln(e)$

$x = y$

Ans: f is 1-1.

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

$\mathbb{Z} \times (\mathbb{Z} - \{0\}) = \{(m, n) : m \in \mathbb{Z}, n \in \mathbb{Z} - \{0\}\}$

(c) $h: \mathbb{Z} \times (\mathbb{Z} - \{0\}) \to \mathbb{Q}$, $h(m, n) = \frac{m}{n}$

Is a function

Is h 1-1?

Suppose $h(m_1, n_1) = h(m_2, n_2)$ for

$\frac{m_1}{n_1} = \frac{m_2}{n_2}$

Counterexample $\frac{1}{1} = \frac{2}{2}$

So $h(1,1) = 1 = h(2,2)$

Thus we have

≤ 1 $h(1,1) = h(2,2)$

Ans: not 1-1

Is h onto?

Take any $q \in \mathbb{Q}$. By the defn of rationals,
there exist $a, b \in \mathbb{Z}$, $b \neq 0$, s.t. $q = \frac{a}{b}$

Then $q = h(a,b)$ and $(a,b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$

Ans: h is onto.

Then $q = h(a,b)$ and $(a,b) \in \mathbb{Z} \times (\mathbb{Z} - \{0\})$

Ans: h is onto.

(b) $g: \mathbb{R}^2 \to \mathbb{R} \times \mathbb{Z}$, $g(r$ $,5)$

$\mathbb{R} \times \mathbb{R}$ Yes, a

Is it 1-1?

Supp $g(x,y) =$

$(x+2y, 5)$

$f: A \to B$

Not 1-1. Counterex

$g(0,1) = g(2,0)$

Onto? no!

03-09-2015

Relation R from A to B^{-A}: $R \subseteq A \times B^{-A}$

$(a,b) \in R$

Def. A binary relation R on a set A is called an equivalence relation if it is: reflexive, symmetric, and transitive.

e.g. ≈ equality of any objects
≈ equivalence of propositions.

Def A binary (bit) string of length n ($n \geq 0$) is a sequence of n symbols, each a 0 or 1. $l(s)$ = length of string s

e.g. 0110101 bit string of length 7

$l(0110101) = 7$.

$B = \{\text{bit strings}\}$

e.g bit strings of length 1: 0, 1

2: 00, 01, 10, 11

3: 000, 001, 010, ...

0: ε

Ex. Define a relation L on B by

$(s,t) \in L \iff l(s) = l(t)$

(a) show L is an equiv. relation

≈ to show that L is reflexive.

take any $s \in B$. Then $l(s) = l(s)$ and so $(s,s) \in L$. Hence L is reflexive.

Pay attn to correct reasoning!.

- To show $\mathcal{L}$ is symmetric.

  take any $s, t \in B$.

  If $(s,t) \in L$, then $l(s) = l(t)$, so $l(t) = l(s)$,

  yielding $(t,s) \in L$. Hence $\mathcal{L}$ is sym.

- To show L is transitive:

  Take any $s, t, r \in B$

  Assume $(s,t), (t,r) \in L$

  Hence $l(s) = l(t)$ and $l(t) = l(r)$

  Hence $l(s) = l(r)$, and so $(s,r) \in L$

  Therefore, L is transitive

since $\mathcal{L}$ is refl, sym & transitive, it is an equiv relation

b) Find the set of all $t \in B$ s.t. $t \, L \, 011$ (or $(t, 011) \in L$)

By defn of L

$(t, 011) \in L \iff l(t) = l(011) = 2$

so $S = \{t \in B : (t, 011) \in L\} =$

$= \{t \in B \cdot l(t) = 2\} = \{000, 001, \ldots, 111\} = [011]_L$

equivalence class of 011 wrt L

Def Let R be an equivalence relation on a set A, and $a \in A$. Then.

$$[a]_R = \{b \in A : (a,b) \in R\} = \{b \in A : aRb\}$$

is called the equivalence class of a wrt R

Eg. $A = \{1, 2, \ldots, 16\}$

$R = \{(a,b) : \frac{a}{b} = 2^k \text{ for some } k \in \mathbb{Z}\}$

e.g. $a=2$, $b=6$ $\quad \frac{a}{b} = \frac{2}{6} = \frac{1}{3} \neq 2^k$ for any $k \in \mathbb{Z}$ so $(a,b) \notin R$

$c=8$ $\quad \frac{a}{c} = \frac{2}{8} = \frac{1}{4} = 2^{-2} \in \mathbb{Z}$, so $(a,c) \in R$

(a) Show R is an equiv relation

$\Rightarrow$ to show R is reflective:

Take any $a \in A$

$\top$

03-12-2015

E.g. Define a rln R on $\mathbb{R}^2$ as:

$(x_1, y_1) R (x_2, y_2) \iff x_1^2 - y_1 = x_2^2 - y_2$.

(a) Prove that R is an eq. rln on $\mathbb{R}^2$ ~

(b) Determine the eq. class of $(0,0)$ w.r.t R.

Give a geometric description

(c) Determine the partition of $\mathbb{R}^2$ into eq classes w.r.t R.

(b) $[(0,0)]_R = \{(x,y) \in \mathbb{R}^2 : (0,0) R (x,y)\}$

$= \{(x,y) \in \mathbb{R}^2 : 0^2 - 0 = x^2 - y\}$

$= \{(x,y) \in \mathbb{R}^2 : x^2 - y = 0\}$

$= \{(x,y) \in \mathbb{R}^2 : y = x^2\}$

= parabola with equation $y = x^2$

(c) Take any $(a,b) \in \mathbb{R}^2$

$[(a,b)]_R = \{(x,y) \in \mathbb{R}^2 : a^2 - b = x^2 - y\}$

$= \{(x,y) \in \mathbb{R}^2 : y = x^2 - (a^2 - b)\}$

= Parabola with equation $y = x^2 - (a^2 - b)$

For any $c \in \mathbb{R}$, we have $y = x^2 - c$ is the eq. class of $(0, -c)$. So the partition of $\mathbb{R}^2$ into eq. classes is $\{y = x^2 + c : c \in \mathbb{R}\}$

Congruences

$14 = 2 \cdot 5 + 4$
$24 = 5 \cdot 5 + 4$
$\Big\} \; 14 \equiv 24 \pmod 5$

remainder in $\{0, 1, 2, 3, 4\}$

$-14 = (-3)\,5 + 1$

$14 \not\equiv -14 \pmod 5$

Let $m \in \mathbb{Z}$, $m \geq 2$ (modulus), let $a, b \in \mathbb{Z}$

Def a is said to be congruent to b modulo m, written as $a \equiv b \pmod m$, iff $a - b = k \cdot m$ for some $k \in \mathbb{Z}$.

iff $m \mid (a-b)$ iff a and b give the same remainder in $\{0, 1, \ldots, m-1\}$ when divided by m.

e.g T or F?

$1 \equiv 3 \pmod 2$ T $\quad 1 - 3 = -2 = (1) \cdot 2$

$1 = 0 \cdot 2 + 1$

$3 = 1 \cdot 2 + 1$

$1 \equiv 4 \pmod 2$ F $\quad 1 - 4 = -3 = (-2) \cdot 2 + 1$

$1 \equiv 4 \pmod 3$ T $\quad 1 - 4 = -3 = (-1) \cdot 3$

e.g $49 \equiv 13 \pmod 6$ T $\quad 49 - 13 = 36 = 6 \cdot 6$

$49 \equiv 13 \pmod 8$ F $\quad 49 - 13 = 36 = 7 \cdot 5 + 1$

$3 \equiv -3 \pmod 5$ F $\quad 3 - (-3) = 6 = 1 \cdot 5 + 1$

$3 \equiv -3 \pmod 6$ T

Ex Prove that $\equiv \pmod m$ is an eq. relation on $\mathbb{Z}$

* To show $\equiv \pmod m$ is reflexive:

Take any $a \in \mathbb{Z}$. Then $a-a = 0 = 0 \cdot m$, so $a \equiv a \pmod m$

* To show $\equiv \pmod m$ is symmetric:

Take any $a, b \in \mathbb{Z}$.

Assume $a \equiv b \pmod m$. Hence $a-b = km$ for some

$k \in \mathbb{Z}$. Now $b-a = -(a-b) = (-k)m$, and $-k \in \mathbb{Z}$

Hence $b \equiv a \pmod m$

* To show $\equiv \pmod m$ is transitive:

Take any $a, b, c \in \mathbb{Z}$ a-

assume $a \equiv b \pmod m$ and $b \equiv c \pmod m$

Hence $a-b = km$ and $b-c = lm$ for $k, l \in \mathbb{Z}$

Now $a-c = (a-b)+(b-c) = km + lm = (k+l)m$

and $k+l \in \mathbb{Z}$. Therefore, $a \equiv c \pmod m$

E.g. Determine the partition of $\mathbb{Z}$ into congruency classes (= eq. classes) modulo 3

$[0] = \{b \in \mathbb{Z} : 0 \equiv b \pmod 3\}$

$= \{b \in \mathbb{Z} : 0-b = k \cdot 3$ for some $k \in \mathbb{Z}\}$

$= \{b \in \mathbb{Z} : b = 3l$ for some $l \in \mathbb{Z}\}$

$[1] = \{b \in \mathbb{Z} : 1 \equiv b \pmod 3\} =$

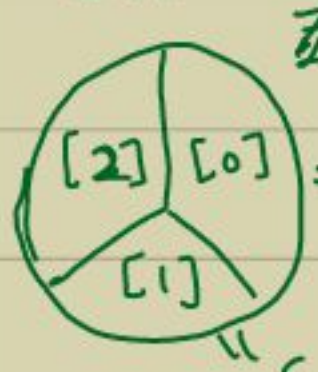
$= \{b \in \mathbb{Z} : b - 1 = k \cdot 3 \text{ for } k \in \mathbb{Z}\}$

$= \{b \in \mathbb{Z} : b = 3k + 1 \text{ for } k \in \mathbb{Z}\}$

Sim $[2] = \{b \in \mathbb{Z} : b = 3k + 2 \text{ for some } k \in \mathbb{Z}\}$

$\mathbb{Z}$

$\{\ldots, -1, 2, 5, \ldots\}$



$= \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$

$\{\ldots, -2, 1, 4, 7, \ldots\}$

Partition of $\mathbb{Z}$

$\{[0], [1], [2]\}$

The basics of counting

The product rule

A, B sets, $|A| = m$, $|B| = n$

$|A \times B| = mn$

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

$m \cdot n = mn$

E.g. How many strings of length 2 s.t 1st symbol is a lowercase letter and the 2nd a digit?

$A = \{a, b, \ldots, z\}$ $B = \{0, 1, \ldots, 9\}$

$A \times B = \{(\alpha, \beta) : \alpha \in A, \beta \in B\}$

Ans: $|A \times B| = 26 \cdot 10 = 260$.

Using tasks.

T_1 ... choosing 1st symbol ... 26 ways

T_2 ... " 2nd " .... 10 ways.

ways to perform (T_1, T_2) ... $26 \cdot 10 = 260$ (Product Rule)

Product Rule for k sets

$A_1 \times A_2 \times \dots \times A_k = \{(a_1, a_2, \dots, a_k) : a_i \in A_i, i = 1, \dots, k\}$

$|A_1 \times A_2 \times \dots \times A_k| = |A_1| \cdot |A_2| \cdots |A_k|$

e.g. How many Ontario license plates?

U U U U U U U U U U

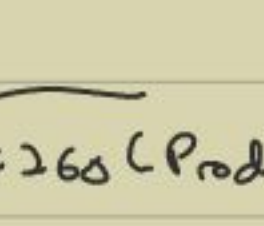
letter letter letter letter digits digits digits 10

26 26 26 26 $\Rightarrow 26^4 \cdot 10^3$ #

=

Eg. How many functions $f : A \to B$, where $|A| = m$, $|B| = n$

Let $A = \{a_1, a_2, \dots, a_m\}$



Procedure: to choose $f(a_1), f(a_2), \dots, f(a_m) \in B$

T_1: choose $f(a_1) \in B$ ... n ways

T_2: choose $f(a_2) \in B$ (after $f(a_1)$ has been chosen) ... n ways

T_m: " $f(a_m) \in B$ (after $f(a_1), \dots, f(a_{m-1})$ have been chosen) ... n ways.

ways to perform $(T_1, T_2, \dots, T_m)$ $\underbrace{n \cdot n \cdot \dots \cdot n}_{m} = n^m$

So: $|\{f: A \to B\}| = |B|^{|A|}$

$\{f: A \to B\} = B^A$

03-16-2015

E.g. How many 1-1 functions $f: A \to B$ if $|A|=m, |B|=n$?

Procedure: choosing

03-23-2015

exactly 2 vowels.

(b) exactly 2 vowels!

T_1: Construct a string of 4 consonants 21^4 ways.

T_2: " " 4 " 2 vowels 5^2 ways.

U _ U _ U _

choose 2.

T_3: choose 2 out of 6 spots for the vowel $\binom{6}{2}$ ways.

(c) at least 1 vowel?

strings of length 6 with ≥ 1 vowel =

(# strings of len 6) − (# strings of len 6 with 0 vowels).

$= 26^6 - 21^6$

(d) at least 2 vowels?

$= 26^6 - (21^6 + 30 \cdot 21^5)$

└ from (c)

/

0 vowels

1 vowel.

6.4. Binomial coefficient & Binomial Theorem.

Recall: $c(n,r)$ = # r-combinations from an n-set.

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

↑ binomial coefficient

Simple observations:

$$\binom{n}{0} = \frac{n!}{0!\,n!} = 1 = \binom{n}{n}$$

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

$$\binom{n}{r} = \binom{n}{n-r}$$

Binomial = sum of 2 terms (summands)

e.g. $x+y$, $1+x$, $2a+3b^2$, $5-3xy^3$, $\frac{1}{x^2}-3y$ ....

Q: What is the coefficient of $x^i y^j$ in the expansion of $(x+y)^n$?

Binomial Theorem: x, y variables, $n \in \mathbb{N}$

$$(x+y)^n = \binom{n}{0}x^n y^0 + \binom{n}{1}x^{n-1}y^1 + \binom{n}{2}x^{n-2}y^2 + \dots$$
$$\binom{n}{n-2}x^2 y^{n-2} + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}x^0 y^n$$

$$= \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

e.g Expand $(x+y)^5 = \sum_{i=0}^{5} \binom{5}{i} x^{5-i} y^i$

$= \binom{5}{0}x^5 + \binom{5}{1} x^4y + \binom{5}{2}x^3y^2 + \binom{5}{3}x^2y^3 + \binom{5}{4}xy^4$

$+ \binom{5}{5}x^0y^5$

$= x^5 + 5x + 10x^3y^2 + 10^2y^3 + 5xy^4 + 1y^5$

1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

E.g. Determine the coefficient of $x^{12}y^{17}$ in the expansion of

$(3x^2 - 5y)^{23} = \sum_{i=0}^{23} \binom{23}{i} (3x^2)^{23-i} (-5y)^i$

$= \binom{23}{i} 3^{23-i} x^{2(23-i)} (-5)^i y^i$

$= \binom{23}{i} 3^{23-i} (-5)^i x^{46-2i} y^i$ ✱

We need $46-2i = 12$ and $i = 17$

$i = 17$

From ✱ The coeff of $x^{12}y^{17}$: (from (✱))

$\binom{23}{17} 3^{23-17} (-5)^{17} = -\binom{23}{6} \cdot 3^6 \cdot 5^{17}$

What about the coefficient of x^6y^{19}?

Need $6 = 46 - 2\cdot 19$

not true!

Ans: 0

Identities involving binomial coefficients.

(1) $\sum_{i=0}^{n} \binom{n}{i} = 2^n = (1+1)^n$

(2) $\sum_{i=0}^{n} (-1)^i \binom{n}{i} = (1-1)^n = 0$

(3)

03-26-2015

Binomial coefficient:

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

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

(i)

5.1 Math Induction.

Let $P(n)$ be a proposition about an integer n.

e.g. $P(n)$: "$1+2+3+\dots+n=\frac{1}{2}n(n+1)$"

Is $P(n)$ T for all $n \geq 1$?
(integers)

PMI

IF — (1) $P(1)$ is T and

(2) $P(k) \to P(k+1)$ is T for all $k \geq 1$,

then $P(n)$ is T for all integers $n \geq 1$.

Terminology: (1) is called the basis of induction (BI)

(2) is called the induction step (IS)

* $P(k)$ in the implication $P(k) \to P(k+1)$ is called the induction hypothesis (IH)

Note that $P(k) \to P(k+1)$ being T does not mean $P(k) \to T$!

Eg. Prove $P(n)$ for all integers $n \geq 1$ where

$P(n)$: "$\sum_{i=1}^{n} i = \frac{1}{2} n(n+1)$"

Proof BI: Prove $P(1)$: "$\sum_{i=1}^{1} i = \frac{1}{2} 1\cdot(1+1)$"

LHS of $P(1)$: $\sum_{i=1}^{1} i = 1$

RHS of $P(1)$: $\frac{1}{2}\cdot 1(1+1) = 1$

So LHS = RHS and $P(1)$ is T

IS: To prove $P(k) \to P(k+1)$ for all $k \geq 1$.

Fix any $k \geq 1$. Assume $P(k)$ is T (IH)

i.e. assume $\sum_{i=1}^{k} i = \frac{1}{2}k(k+1)$

Examine $P(k+1)$: "$\sum_{i=1}^{k+1} i = \frac{1}{2}(k+1)((k+1)+1)$"

LHS of $P(k+1)$: $\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1)$

$$IH = \frac{1}{2}k(k+1) + \frac{2}{2}(k+1)$$

$$= \frac{1}{2}(k+1)(k+2)$$

RHS of $P(k+1)$: $\frac{1}{2}(k+1)((k+1)+1) = \frac{1}{2}(k+1)(k+2)$

LHS = RHS in $P(k+1)$,

So indeed, $P(k) \to P(k+1)$ is T

Conclusion. Since $P(1)$ is T and $P(k) \to P(k+1)$ is T for all $k \geq 1$, by PMF, $P(n)$ is T for all $n \geq 1$. □.

E.g. Show that $n^2 - 7n + 12 \geq 0$ for all $n \in \mathbb{Z}$, $n \geq 3$

Proof.

Let $P(n)$: "$n^2 - 7n + 12 \geq 0$"

We must prove $P(n)$ is T for all $n \geq 3$.

BI: To prove $P(3)$: "$3^2 - 7 \cdot 3 + 12 \geq 0$"

LHS of $P(3)$: $3^2 - 7 \cdot 3 + 12 = 9 - 21 + 12 = 0$

RHS of $P(3)$: 0

So LHS $\geq$ RHS, and $P(3)$ is T.

IS: to prove $P(k) \to P(k+1)$ is T for all $k \geq 3$

Fix any $k \geq 3$ ~~Assume~~ Assume IH, $P(k)$: "$k^2 - 7k + 12 \geq 0$"

Examine $P(k+1)$: "$(k+1)^2 - 7(k+1) + 12 \geq 0$".

LHS of $P(k+1)$: $(k+1)^2 - 7(k+1) + 12 =$

$= k^2 + 2k + 1 - 7k - 7 + 12.$

$= (k^2 - 7k + 12) + (2k - 6)$

$\overset{IH}{\geq} 0 + (2k - 6) = 2(k - 3) \geq 0$ (bc $k \geq 3$)

$=$ RHS

We have LHS $\geq$ RHS in $P(k+1)$, so $P(k) \to P(k+1)$ is T

Conclusion: since $P(3)$ is T, and $P(k) \to P(k+1)$ is T for all $k \geq 3$, by PMI, $P(n)$ is T for all $n \geq 3$

($n_0 = 3$)

03-30-2015

Strong Induction: For $n_0 \in \mathbb{Z}$

IF (1) $P(n_0)$ is T and

(2) $P(n_0) \wedge P(n_0+1) \wedge \dots \wedge P(k)) \to P(k+1)$

is T for all $k \geq n_0$

THEN $P(n)$ is T for all $n \geq n_0$

E.g. Let $(a_0, a_1, a_2, \dots)$ be a sequence defined by

$a_0 = 1$

$a_1 = 0$

$a_n = 5a_{n-1} - 6a_{n-2}$ for $n \geq 2$

Show that $a_n = 3 \cdot 2^n - 2 \cdot 3^n$ for all $n \geq 0$

Proof let $P(n)$: "$a_n = 3 \cdot 2^n - 2 \cdot 3^n$"

BI: to prove $P(0)$: "$a_0 = 3 \cdot 2^0 - 2 \cdot 3^0$"

LHS of $P(0)$: $a_0 = 1$

RHS " " : $3 \cdot 2^0 - 2 \cdot 3^0 = 1$ ∴ LHS = RHS & $P(0)$ is T

IS: Prove $(P(0) \wedge P(1) \wedge \dots \wedge P(k)) \to P(k+1)$ is T for all $k \geq 0$

Fix k: assume $P(0) \wedge P(1) \wedge \dots \wedge P(k)$ is T.

That is $P(0), P(1), \dots, P(k)$ are all T

That is, $P(i)$: "$a_i = 3 \cdot 2^i - 2 \cdot 3^i$" is T for all $i = 0, 1, \dots, k$.

Examine $P(k+1)$: "$a_{k+1} = 3\cdot 2^{k+1} - 2\cdot 3^{k+1}$"

LHS of $P(k+1)$: $a_{k+1} = 5\cdot a_k - 6a_{k-1}$

$= 5(3\cdot 2^k - 2\cdot 3^k) - 6(3\cdot 2^{k-1} - 2\cdot 3^{k-1})$ ← IH

$= 15\cdot 2^k - 10\cdot 3^k - 18\cdot 2^{k-1} + 12\cdot 3^{k-1}$.

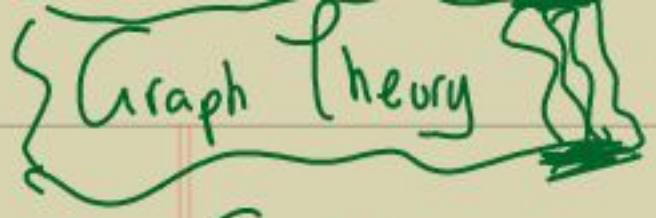
$= 30\cdot 2^{k-1} - 30\cdot 3^{k-1} - 18\cdot 2^{k-1} + 12\cdot 3^{k-1}$

$= 12\cdot 2^{k-1} - 18\cdot 3^{k-1}$

$= 3\cdot 2^{k+1} - 2\cdot 3^{k+1}$

RHS of $P(k+1)$: $3\cdot 2^{k+1} - 2\cdot 3^{k+1}$.

Conclusion: Since $P(0)$ is T and $P(0) \wedge \dots \wedge P(k) \to P(k+1)$ is T for all $k \geq 0$, by strong Ind, $P(n)$ is T for all $n \geq 0$.



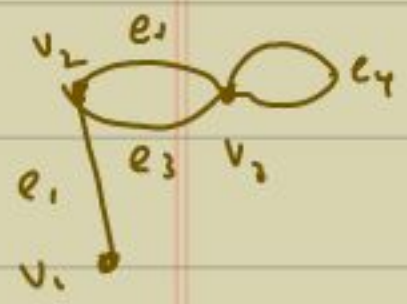
1.1 Graphs

1 Def: Graph: $G = (V, E)$ with $\Psi : E \to \{\{u,v\} : u,v \in V\}$

(Ψ: each edge e is sent to a set $\{u,v\}$)

V ... vertex set $(V \neq \emptyset)$

E ... Edge set



$\Psi(e_1) = \{v_1, v_2\}$

$\Psi(e_2) = \{v_2, v_3\} = \Psi(e_3)$

$\Psi(e_4) = \{v_3\}$

Ψ is the incidence function

$\Psi(e_4) = \{v_3\}$

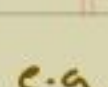
For a graph G: $V(G)$, $E(G)$, Ψ_G

Def $e \in E(G)$ is called:

* a loop if $\Psi(e) = \{u\}$ for some $u \in V(G)$
* a link, otherwise (i.e. if $\Psi(e) = \{u,v\}$ for $u,v \in V(G)$, $u \neq v$)

Def $l_1, l_2 \in E(G)$ are called parallel or multiple if $\Psi(e_1) = \Psi(e_2)$ and $e_1 \neq e_2$

Def G is simple if it has no loops & no parallel edges

e.g. 

for a simple graph, ψ can be omitted, we write $e_1 = \{v_1, v_2\}$

$= v_1 v_2 \neq v_3 v_4$

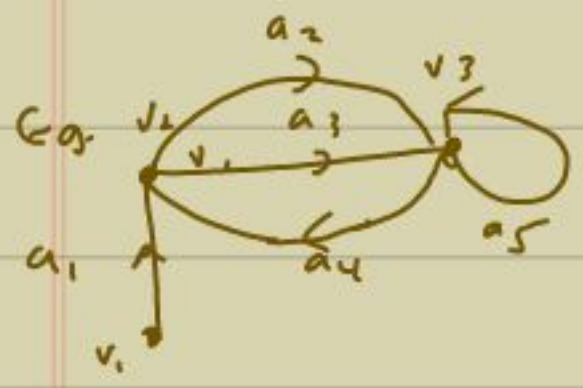
1.2 Directed graphs

Def Directed graph (digraph): $D = (V, A)$

with $\psi: A \to \{(u,v) : u, v \in V\}$

V ... vertex set

A ... arc set (set of arcs or directed edges)



$\psi(a_1) = (v_1, v_3)$

$\psi(a_2) = (v_2, v_3) = \psi(a_3)$

$\psi(a_4) = (v_3, v_2)$

$\psi(a_5) = (v_3, v_3)$

↑ directed loop

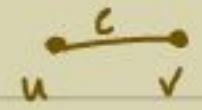
a_2, a_3 are parallel, but a_2 and a_4 are not.

2.1 Terminology - degrees

Def. Let $G = (V, E)$ be a graph.

* $u, v \in V$ are adjacent or neighbours in G if $uv \in E$

(write $u \sim_G v$)



* edge uv is incident with its endpts. u & v.

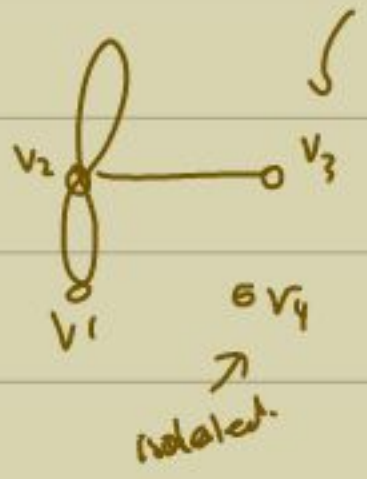
* $u \in V$: $\deg_G(v) = \#$ edges incident with u in G, each loop counting twice.

* u is isolated if $\deg(u) = 0$

" pendant if $\deg(u) = 1$

Eg.

G:



$\deg(v_1) = 3$

$\deg(v_2) = 6$

$\deg(v_3) = 1$

$\deg(v_4) = 0$

deg seq. $\Rightarrow (3, 6, 1, 0)$ or $(0, 1, 6, 3)$.

Def: if $V(G) = \{v_1, \ldots, v_n\}$, then $(\deg(v_1), \deg(v_2), \ldots, \deg(v_n))$ is called the degree sequence of G.

Neighbour of $v_2 = v_1, v_2, v_3$

$v_4 = —$

Thm. [Handshaking thm]

In any graph $G = (V, E)$.

$$\sum_{u \in V} \deg_G(u) = 2|E| \quad \square$$

Eg Let $G = (V, E)$ be a graph with deg seq, $(2, 2, 3, 3, 4, 6)$.

vertices $\supset$ no of ver.

$|E| = ?$

(First, $|V| = 6$)

By the H. Thm: $\sum_{u \in V} \text{degree}(u) = 2 + 2 + 3 + 3 + 4 + 6$

$= 20 = 2|E|$

$= |E| = 10$

Subject 04-02-2015

Cor Any graph has an even # of odd-degree vertices.

Ex* Let $G = (V, E)$ be a graph, $|V| = 14$, $|E| = 29$,
$\deg(u) \in \{3, 5, 7\}$ for all $u \in V$.
Also, (# vertices of deg 3) = 2(# vertices of deg 5)
How many vertices of each degree does G have?

Solution: Let x = # vertices of deg 3
y = 5
z = 7

Then: $x + y + z = 14$

By handshaking thm:

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

$$3x + 5y + 7z = 2 \cdot 29 = 58$$

$$x + y + z = 14$$

$$x - 2y = 6$$

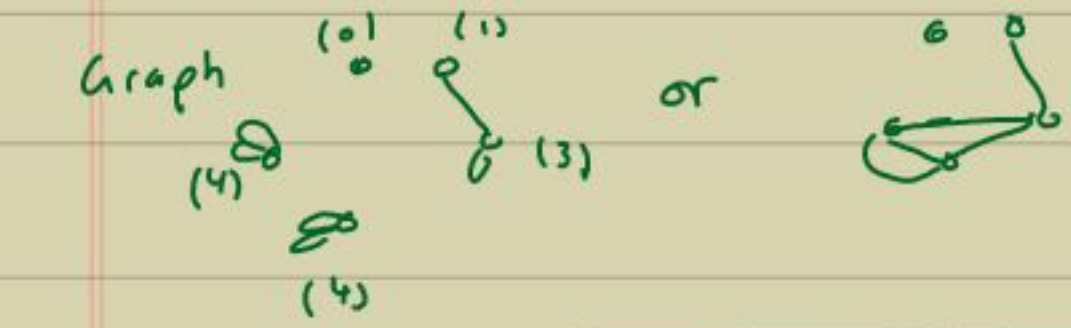
unique soln to this SLE: $x = 8$, $y = 4$, $z = 2$

∴ G has 8 vertices of deg 3, 4 of deg 5, 2 of deg 7.

Ex Does there exist a graph / simple graph with the following degree sequence:

(1) (1,2,3,3,4,4). This sequence contains an odd # of odd entries and every graph has an even # of odd-degree vertices.

(2) (0,1,3,4,4)

Graph 

or

There is no simple graph with deg sequence (0,1,3,4,4)

Suppose $G=(V,E)$ is a simple graph with deg seq. (0,1,3,4,4) Hence $\exists$ (there exist) $u, v \in V$ s.t. $\deg(u)\neq 0$ and $\deg(v)=4$ 
Hence $u \sim x$ for all $x \in V$, and $v \sim x$ for all $x \in V$, $x \neq v$, $\rightarrow\leftarrow$

(2.2) some special graphs

* complete graph K_n $(n \geq 1)$: simple graphs with

$$V(K_n) = \{v_1, v_2, \ldots, v_n\}$$

$$E(K_n) = \{ xy : x, y \in V, x \neq y \}$$

observe: $|V(K_n)| = n$

$\deg_{K_n}(n) = n-1$

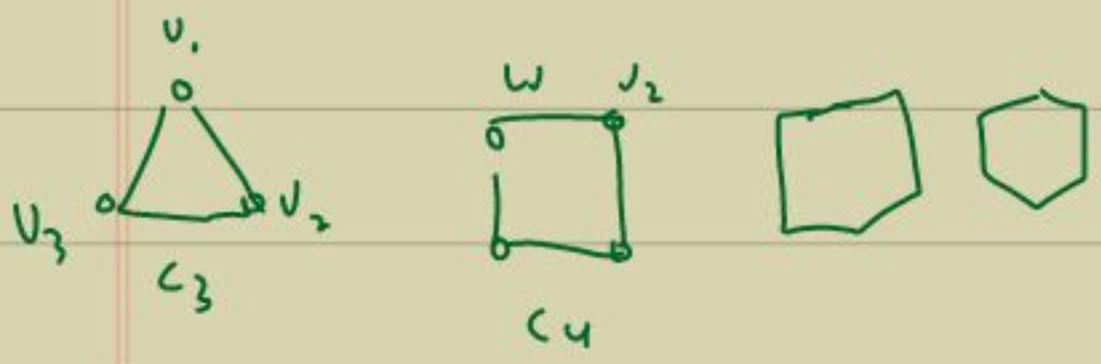
$$|E(K_n)| = \frac{1}{2} \sum_{n \in V(K_n)} \deg(n)$$

$$= \frac{1}{2}\, n(n-1) = \binom{n}{2}$$

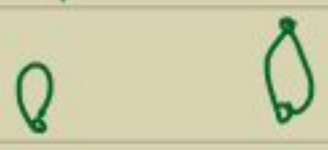
* Cycle C_n $(n \geq 3)$ - simple graphs with $(n =$ length of $C_n)$

$V(C_n) = \{v_1, v_2, \ldots, v_n\}$

$E(C_n) = \{v_1v_2, v_2v_3, v_3v_4, \ldots, v_{n-1}v_n, v_nv_1\}$



Cycles C_1 and C_2 Non-simple.



Observe $|V(C_n)| = n$ $\deg(v) = 2$ for all $v \in V(C_n)$

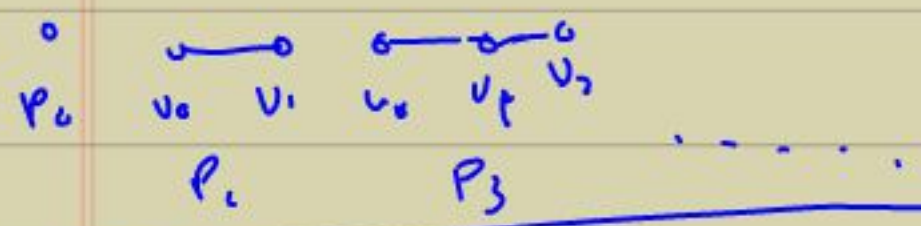
$|E(C_n)| = n$

---

* Path P_n $(n \geq 0)$ - simple graph with

$V(P_n) = \{v_0, v_1, v_2, \ldots, v_n\}$

$E(P_n) = \{v_0v_1, v_1v_2, \ldots, v_{n-1}v_n\}$



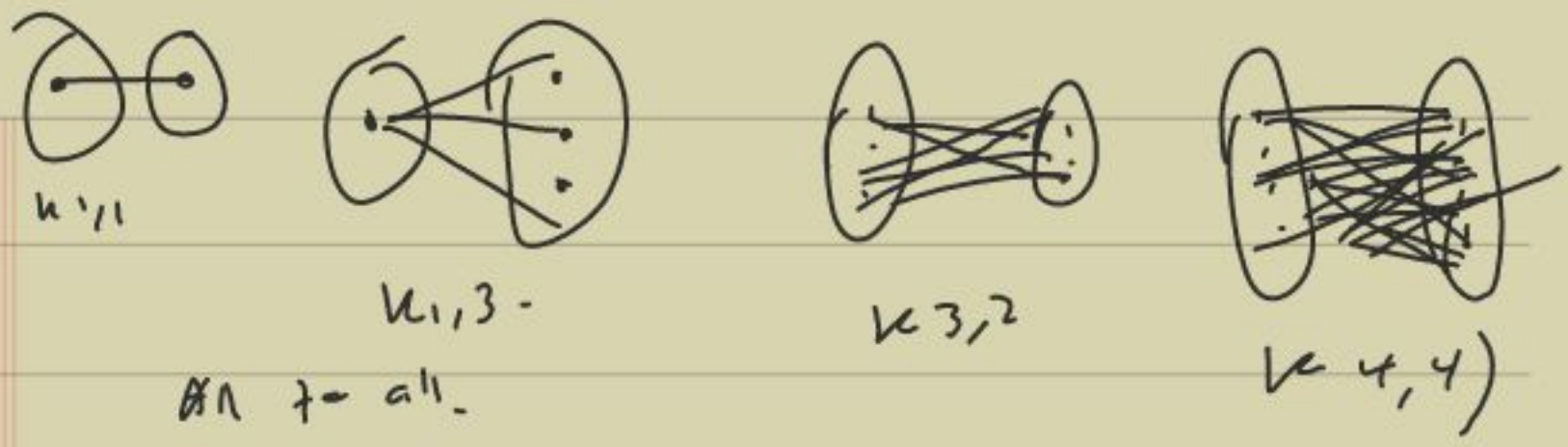
---

* Complete bipartite graphs $K_{m,n}$ $(m, n \geq 1)$

$V(K_{m,n}) = X \cup Y$ For $X = \{x_1, x_2, \ldots, x_m\}$, $Y = \{y_1, y_2, \ldots, y_n\}$

$X \cap Y = \emptyset$ $E(K_{m,n}) = \{xy : x \in X, y \in Y\}$

e.g



Not all.

Observe: $|V(K_{m,n})| = m+n$

$|E(K_{m,n})| = mn$

$$\deg(u) = \begin{cases} n & \text{if } u \in X \\ m & \text{if } u \in Y \end{cases}$$

2.3 subgraphs

E.g

observe

$\{a,b,c\} = V(H) \subseteq V(G) = \{a,b,c,d\}$

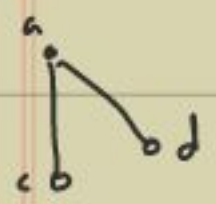
$\{ab, bc\} = E(H) \subseteq E(G) = \{ab, ac, ad, bc\}$

Def If G and H are simple graphs with $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$, then H is said to be a subgraph of G.

Ex Find all subgraphs of G with exactly 3 vertices and 2 edges

soln Possible Vx sets for such a subgraph

$V_1 = \{a,b,c\}$, $V_2 = \{a,b,d\}$, $V_3 = \{a,c,d\}$, $V_4 = \{b,c,d\}$

i	subgraphs of G with V_2 set V_i and ex 2 edges
1	
2	
3	
4	None

2.4. Bipartite graphs

Def $G=(V,E)$ is **bipartite** if V has a partition $\{X,Y\}$ s.t. every edge of G has 1 endpt. in X and the other in Y.

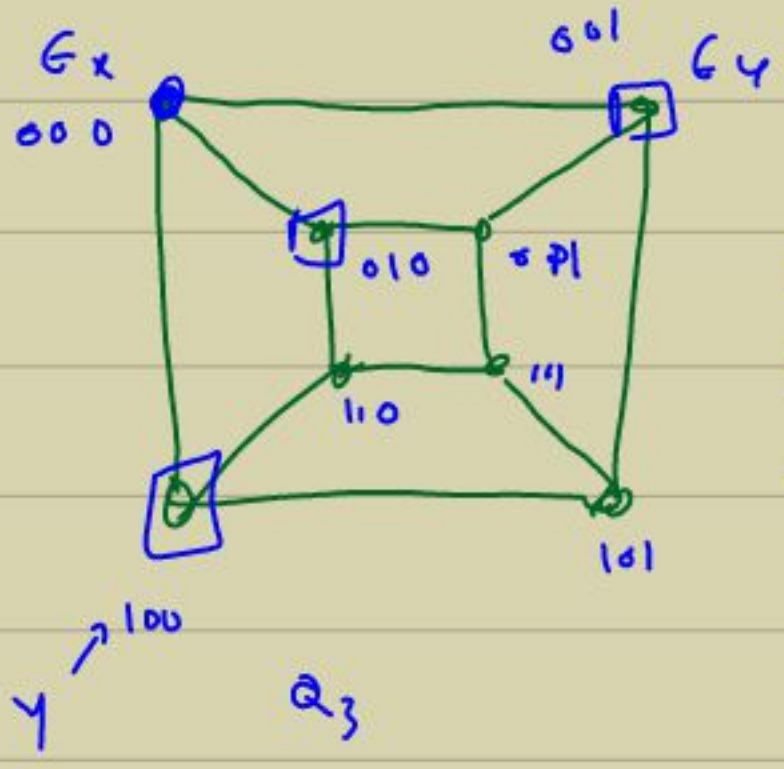
$\{X,Y\}$ = bipartition of G; X,Y = parts of G.

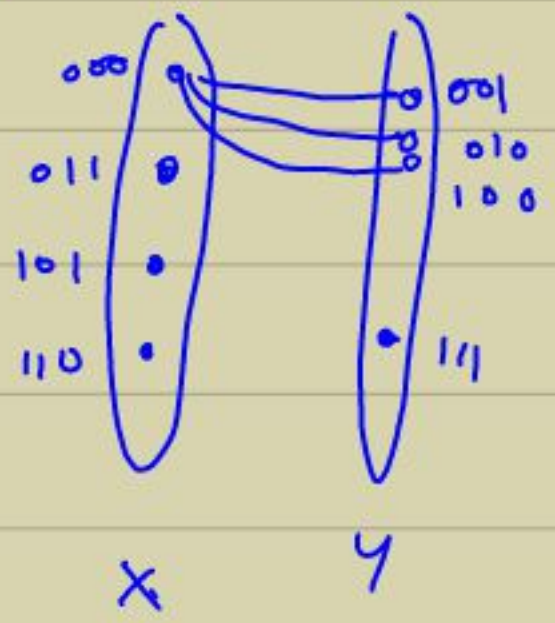
E.g. Are these graphs bipartite? Justify.

G: 

Yes, bipartite with the indicated bipartition

G_2:





like Grey code
change 1 bit.

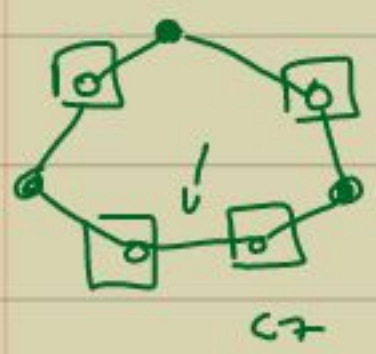
Grey code

000
001
011
010

04-09-2015

Bipartite graphs

Is C_7 bipartite?



C_7

we cannot properly 2-vertex colour C_7

so C_7 is not bipartite.

Thm: TFAE:

(1) G is bipartite

(2) G has a proper 2-vertex colouring i.e. the vertices of G can be coloured with 2 colours s.t. the endpts of each edge receive distinct colours.

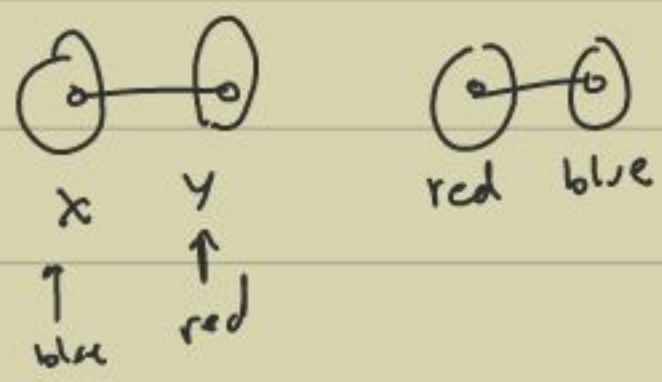
(3) G has no subgraph that is an odd-length cycle

Proof (1) $\Rightarrow$ (2)

(2) $\Rightarrow$ (1)

(2) $\Rightarrow$ (3) ✓

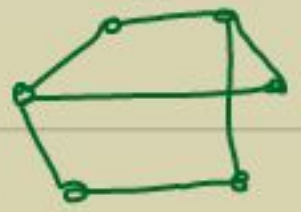
(3) $\Rightarrow$ (2)

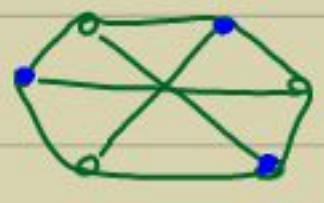


To show G : s:

* bipartite: give a proper 2-vx colouring
* not bipartite: find an odd-length cycle

E.g. Is G bipartite? Justify.

G:  No: it has a subgraph C_5

G:  ✓  ✓

Ex for what values of the parameters are the following bipartite.

K_n: $n \in \{2, 1\}$

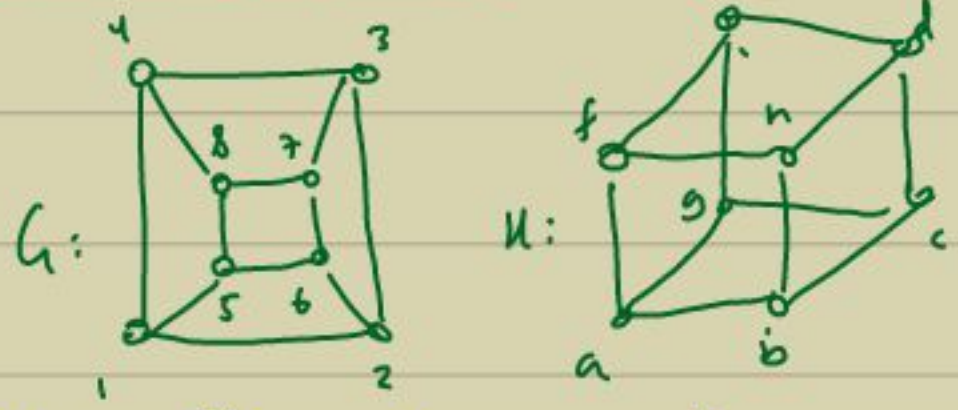
C_n: n even

P_n: all n

$K_{m,n}$: all m, n.

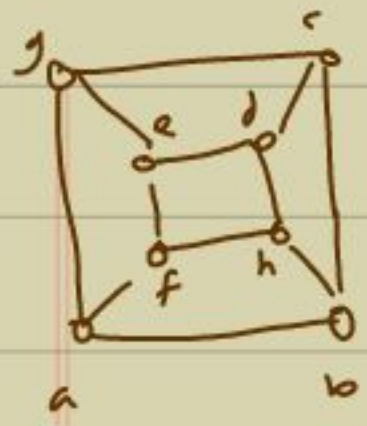
3.2 Graph Isomorphism (relabelling)

E.g.



G & H are "essentially the same; same structure.

"Relabelling" H: (redraw H so it "looks-like" G)



x	1	2	3	4	5	6	7	8
phi: $\varphi(x)$	a	b	c	g	f	h	d	e

observe: for all $x, y \in V(G)$

$$x \sim_G y \iff \varphi(x) \sim_H \varphi(y)$$

Def let G and H be simple graph. An isomorphism from G to H is a bijection $\varphi: V(G) \to V(H)$

s.t. for all $x, y \in V(G)$

$$x \sim_G y \iff \varphi(x) \sim_H \varphi(y)$$

G and H are isomorphic if there exists an isomorphism from G to H; denote $G \cong H$

Graph invariants (properties preserved by isom):

* # vertices
* # edges
* degree sequence
* being bipartite
* having specific subgraphs (e.g. C_7, P_{15}...)
* any purely structural property.

Not invariants

* vertex/edge labels * drawing * vertex/edge colours/weights

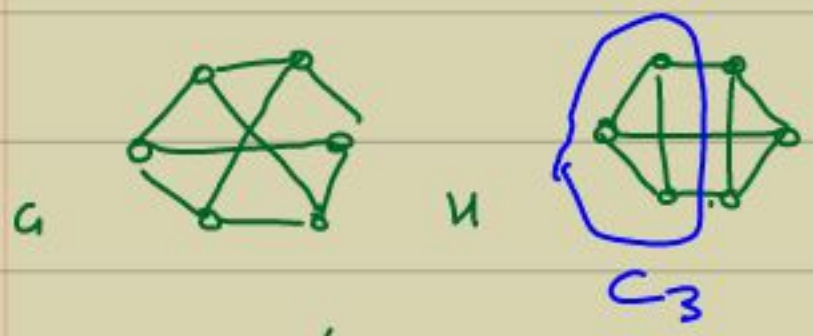
How to prove:

* $G \cong H$: give an isomorphism $\varphi: G \to H$

* $G \ncong H$: give an invariant in which G and H differ.

E.g. Are G and H isomorphic? justify.

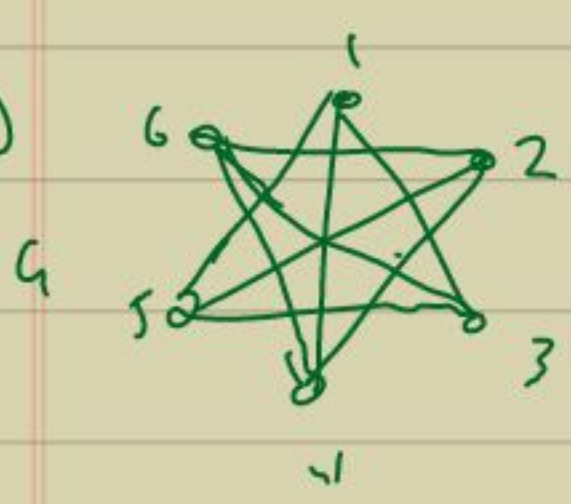
(a)

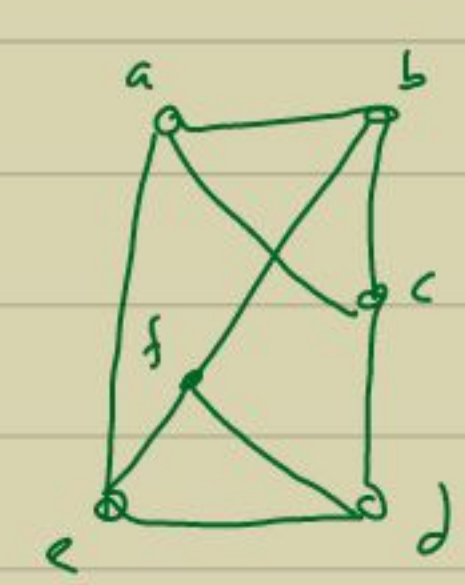


Same # vertices, same degree seq.

$G \ncong H$: G is bipartite ($G \cong K_{3,3}$)
H is not (it has a subgraph $\cong C_3$)

(b)





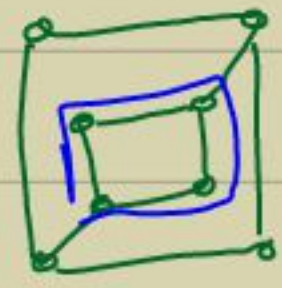
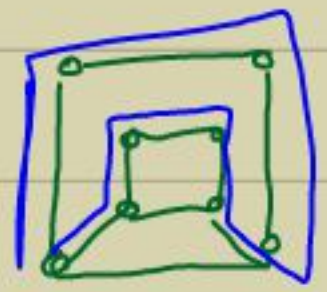
Same #vertices
same deg seq

Redraw H so it looks like G.

$\varphi: V(G) \longrightarrow V(H)$

x	1	2	3	4	5	6
$\varphi(x)$	a	d	b	e	c	f

is an isomorphism $G \to H$, so $G \cong H$

(c) G:  H: 

H has a subgraph $\cong C_8$

G has no subgr $\cong C_8$

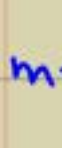
$\therefore G \ncong H$.

Ex List all pairwise non-isomorphic simple graphs with 4 vertices

Let m = # edges Then $m \in \{0, 1, \dots, 6\}$

↳ simple graph.

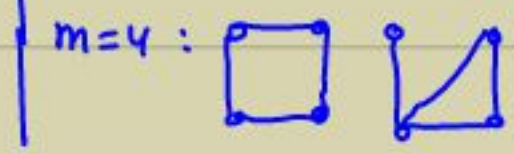
$m=0$: 

$m=1$: 

$m=2$: 

$\binom{4}{2} = \binom{6}{2}$

$m=3$ 



$m=4$:

$m=5$ 

$m=6$ 

1.1 Walks, trails, paths, cycles

Def Let $G = (V, E)$ be graph with inc. function ψ

Let $x, y \in V$, $k \in \mathbb{N}$

an (x,y)-walk of length k in G is a sequence.

$W = v_0 e_1 v_1 e_2 v_2 \dots v_{k-1} e_k v_k$

s.t:

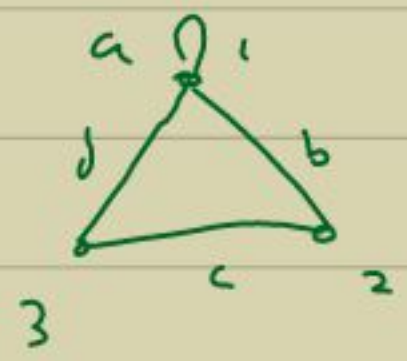
Def: ✱ $v_0, v_1, \dots, v_k \in V$ (may be repeated)

✱ $e_1, e_2, \dots, \dots, e_k \in E$ $\quad v_{i-1}\ e\ v_i$

✱ $v_0 = x,\ v_k = y$

✱ $\gamma(e_i) = \{v_{i-1}, v_i\}$ for all $i = 1, 2, \dots, k$.

<u>e.g</u>



$w = 1\,b\,2\,b\,1\,a\,1\,d\,3$

(1, 3)-walk of len 4

<u>Def</u> A walk $w = v_0\, e_1\, v_1\, e_2\, v_2 \dots v_{k-1}\, e_k\, v_k$ is called.

✱ <u>closed</u> if $v_0 = v_k$, otherwise, open.

✱ <u>trail</u> if $e_1, e_2, \dots, e_k$ are distinct

✱ a <u>path</u> if $v_0, v_1, \dots, v_k$ are all distinct.

✱ <u>cycle</u> if $v_0 = v_k$ and $v_1, \dots, v_k$ are distinct.