Set Theory

Set theory branch of maths deals with the properties of well defined collections of objects.

It forms the bases of several other branches of maths such as counting theory, relations, graph theory and finite state machines.

SET DEFINITION

= a set is a well defined collection of any kind of objects, it could be numbers, colours, vowels.

It is unordered and each member of the set is unique.

NOTATION example

All vowels in english language = $\{a, e, i, o, u\}$

Empty set = $\{\}$ or $\emptyset$

$\in$ = elements in a set, $\notin$ elements not in a set

$Z \notin$ set of all vowels

SET CARDINALITY → number of elements in a set

$E = \{2, 4, 6, 8\}$ then $|E| = 4$

SUBSET OF A SET $\subseteq$ → if B contains all the elements of A then A is a subset of B.

example $A = \{1, 2, 3\}$ $B = \{1, 2, 3, 4, 5\}$ then $A \subseteq B$

SPECIAL SETS

$\mathbb{N}$ = set of all natural numbers (positive integers)

$\mathbb{Z}$ = set of all integers positive and negative

$\mathbb{Q}$ = set of rational numbers (includes fractions)

$\mathbb{R}$ = set of all real numbers (all numbers, but not ∞)

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

LISTING METHOD

is one of two ways of representing a set. It is the most straightforward and simply involves listing all the items in the set

example 1

$S_1 = \{2, 4, 6, 8\}$

RULE OF INCLUSION

is the second method of representing a set. It involves writing a rule such that when it is true the element is a member of the set

example 1

all odd integers $\{2n+1 \mid n \in \mathbb{Z}\}$

all even integers $\{2n \mid n \in \mathbb{Z}\}$

In certain cases using the rule of inclusion (set building notation) is the only way to really describe a set. For example all numbers in the set of rational numbers. It is much easier to write this as

$$\mathbb{Q} = \{n/m \mid n, m \in \mathbb{Z} \text{ and } m \neq n\}$$

POWER SET

is where a set contains sets ~~for example~~ of all the subsets.

$A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$B = \{\{1, 2, 3, 4\}, \{5, 6\}, \{7, 8, 9\}\}$

note $\{1, 2, 3, 4\}$ is a subset of A, but an element of B

"Given an set S, the powerset of S, P(S) is the set containing all the subsets of S."

example 1 $S = \{1, 2, 3\}$

$P(S) = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 2, 3\}\}$ (includes $\emptyset$

example 2 $S = \{a, b\}$

$P(S) = \{\{\emptyset\}, \{a\}, \{b\}, \{a, b\}\}$

The powerset of an empty set is $S = \{\emptyset\}$ $P(S) = \{\emptyset\}$

CARDINALITY of a powerset

$$\boxed{\text{Given set } S \text{ then } |P(S)| = 2^{|S|}}$$

for example $S = \{a, b, c\}$ then $|S| = 3$ and $|P(S)| = 2^3 = 8$

example 1

Given a set A, if $|A| = n$, find $|P(P(P(A)))|$

$|P(A)| = 2^{|A|} = 2^n$

$|P(P(A))| = 2^{|P(A)|} = 2^{2^n}$

$|P(P(P(A)))| = 2^{|P(P(A))|} = 2^{2^{2^n}}$

Set Operations

UNION $\cup$ given two sets A and B the union or $A \cup B$ contains all the elements in A **OR** B

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

example 1

$A = \{1, 2, 3\}$
$B = \{4, 5, 6\}$
$A \cup B = \{1, 2, 3, 4, 5, 6\}$

or

A	B	A ∪ B
0	0	0
0	1	1
1	0	1
1	1	1

INTERSECTION $\cap$ given two sets A and B the intersection or $A \cap B$ contains all the elements in both A **AND** B

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

example 2

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

SYMMETRIC DIFFERENCE given 2 sets A and B, the symmetric difference or $A \oplus B$ are all the elements in A and B but not in both

$$A \oplus B = \{x \mid (x \in A \text{ or } B) \text{ and } x \notin A \cap B\}$$

example 3

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

DIFFERENCE given 2 sets A and B the difference or $A - B$ are all the elements that are in A but not in B

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

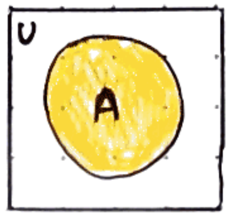
example 4

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

VENN DIAGRAMS

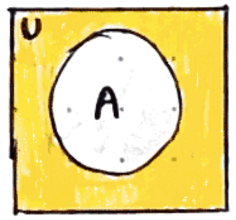
Venn diagrams can be used to represent sets and help us visualise various operations

THE UNIVERSAL SET - is a set containing everything $A \subseteq U$



THE COMPLIMENT OF A SET - given a set A the complement is written as $\bar{A}$ and is all the elements in U that are not in A

AKA $\bar{A} = U - A$



example 1 - the complement of a set

$U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $A = \{2, 4, 6, 8, 10\}$

$\bar{A} = U - A$ or $\{1, \boxed{2}, 3, \boxed{4}, 5, \boxed{6}, 7, \boxed{8}, 9, \boxed{10}\} - \{\boxed{2}, \boxed{4}, \boxed{6}, \boxed{8}, \boxed{10}\}$
$= \{1, 3, 5, 7, 9\}$

CARDINALITY of a powerset

$\boxed{\text{Given set } S \text{ then } |P(S)| = 2^{|S|}}$

for example $S = \{a, b, c\}$ then $|S| = 3$ and $|P(S)| = 2^3 = 8$

example 1

Given a set A, if $|A| = n$, find $|P(P(P(A)))|$

$$|P(A)| = 2^{|A|} = 2^n$$

$$|P(P(A))| = 2^{|P(A)|} = 2^{2^n}$$

$$|P(P(P(A)))| = 2^{|P(P(A))|} = 2^{2^{2^n}}$$

Set Operations

UNION $\cup$ given two sets A and B the union or $A \cup B$ contains all the elements in A **OR** B

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

example 1

$A = \{1, 2, 3\}$
$B = \{4, 5, 6\}$
$A \cup B = \{1, 2, 3, 4, 5, 6\}$

or

A	B	A ∪ B
0	0	0
0	1	1
1	0	1
1	1	1

INTERSECTION $\cap$ given two sets A and B the intersection or $A \cap B$ contains all the elements in both A **AND** B

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

example 2

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

SYMMETRIC DIFFERENCE given 2 sets A and B, the symmetric difference or $A \oplus B$ are all the elements in A and B but not in both.

$$A \oplus B = \{x \mid (x \in A \text{ or } B) \text{ and } x \notin A \cap B\}$$

example 3

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

DIFFERENCE given 2 sets A and B the difference or $A - B$ are all the elements that are in A but not in B

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

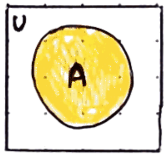
example 4

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

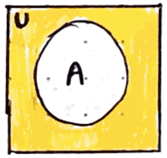
VENN DIAGRAMS

Venn diagrams can be used to represent sets and help us visualise various operations

THE UNIVERSAL SET – is a set containing everything $A \subseteq U$



THE COMPLIMENT OF A SET – given a set A the complement is written as $\overline{A}$ and is all the elements in U that are not in A
AKA $\overline{A} = U - A$



example 1 – the complement of a set

$U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ $A = \{2, 4, 6, 8, 10\}$

$\overline{A} = U - A$ or $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} - \{2, 4, 6, 8, 10\}$
$= \{1, 3, 5, 7, 9\}$

De morgans Laws

FIRST LAW → the compliment of the union of two sets A and B is equal to the intersection of their complements.

$$\overline{A \cup B} = \bar{A} \cap \bar{B}$$

SECOND LAW → the compliment of the intersection of two sets A and B is equal to the union of their complements.

$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

PROOF →

example 1
$\overline{A \cup B} = \bar{A} \cap \bar{B}$

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

EQUAL

example 2
$\overline{A \cap B} = \bar{A} \cup \bar{B}$

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

equal

LAWS OF SETS

COMMUTATIVITY is when the order of the elements does not affect the outcome eg $2+3 = 3+2$ or $3 \times 2 = 2 \times 3$ BUT NOT $2-3 \neq 3-2$

$\cup$ union $\cap$ intersection $\oplus$ symmetric difference are all commutative

ASSOCIATIVITY → where grouping the elements doesn't change the result eg
$2+3+4 = (2+3)+4 = 2+(3+4)$

$\cup$ union $\cap$ intersection $\oplus$ symmetric difference are all associative operations

DISTRIBUTIVITY → states the multiplying the sum of two numbers is the same as multiplying each number together and adding them

$$a(b+c) = (a \times b) + (a \times c)$$

for the union of sets this looks like

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

for the intersection of sets this looks like

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

union	intersection	name
$A \cup B = B \cup A$	$A \cap B = B \cap A$	commutative
$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$	associative
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	distributive
$\overline{A \cup B} = \bar{A} \cap \bar{B}$	$\overline{A \cap B} = \bar{A} \cup \bar{B}$	de morgans
$A \cup \emptyset = A$	$A \cap \emptyset = \emptyset$	identities
$A \cup U = U$	$A \cap U = A$	
$A \cup \bar{A} = U$	$A \cap \bar{A} = \emptyset$	compliment
$\bar{U} = \emptyset$	$\bar{\emptyset} = U$	
$\bar{\bar{A}} = A$		double complement
$A \cup (B \cap A) = A$	$A \cap (B \cup A) = A$	absorption
$A - B = A \cap \bar{B}$		set difference

EMPTY SET → an empty set is denoted by $\{\}$ or $\emptyset$ not to be confused by $\{\emptyset\}$ which is a set with a single empty element. Think of computer folders, where an empty folder within a folder, the main folder contains something

PARTITION

Partitioning an object into parts such that the elements are completely seperated from each other, yet together they form the whole object.

"A partition of set A is a set of subsets such that all subsets are disjointed and the union of all subsets is equal to A"

Disjoint where $A \cap B = \emptyset$

Subsets

A is a subset of B only if every element of A is also an element of B. We use the notation $A \subseteq B$ to show this.

To prove A is not a subset of B we only need to show one element where $x \in A$ with $x \notin B$

FOR EVERY SET S

$\rightarrow \emptyset \subseteq S$

$\rightarrow S \subseteq S$

Proof for $\emptyset \subseteq S$

We must show $\forall x (x \in \emptyset \rightarrow x \in S)$ is true. Aka if x is in the empty set then it must be in S. Since no ~~set is~~ element is in the empty set ($x \in \emptyset$ is FALSE) then this is always true.

If A is a subset of B but $A \neq B$ then we use $A \subset B$

functions

A function is a rule that relates how one quantity relates to another quantity.

Aka speed = distance / time

A function input must map to $\boxed{\text{exactly 1}}$ output

We can consider this using sets in which the function maps elements in set A to elements in set B.

It is well-behaved as given a starting point we will always know how to get to the end point.

Example 1

$S_1 = \{sea, land, sky\}$

$S_2 = \{1, 2, 3, 4, 5, 6\}$

$f(x)$ = maps the number of letters in S_1 to S_2

Sea $\rightarrow$ 3

Land $\rightarrow$ 4

Sky $\rightarrow$ 3

FORMALLY $x \in A \rightarrow f(x) = y \ (y \in B)$

"x is an element of A, when passed through $f(x)$ becomes y where y is an element of B"

DOMAIN, CO-DOMAIN, RANGE

Given a function $f: A \rightarrow B$ and $x \in A \rightarrow f(x) = y \in B$

A is the set of all inputs and is the $\boxed{\text{domain}}$ also known as $Df = A$

B is the set of all outputs and is known as the $\boxed{\text{co-domain}}$ also written as $co\text{-}D_f = B$.

The set containing all outputs is the $\boxed{\text{range}}$ and is written as Rf.

IMAGE AND PRE-IMAGE

The input x when run through the function produces output y. x is the preimage with y being the image (pre-image is also known as the anticedent.

Using the earlier example where

$A = \{on, sea, land, sky\}$
$B = \{1, 2, 3, 4, 5, 6\}$
f = the length of each string

DOMAIN = Df = A {on, sea, land, sky}
CO-DOMAIN = co-Df = B {1, 2, 3, 4, 5, 6}
RANGE = {2, 3, 4}

We can also say 'land' is the image of 4 and we can write the pre-image of 3 as pre-image (3) = {sea, sky}

PLOTTING FUNCTIONS

A linear function is of the form $ax+b$ with b being the y intercept and a being the gradient.

A quadratic equation is of the form ax^2+bx+c and may have multiple x intercepts and is shaped like a parabola.

An exponential function is b^x, the variable b is the base. Exponentials have some important properties such as:

$$b^x \times b^y = b^{x+y} \qquad (b^x)^y = b^{x \times y} \qquad (a/b)^x = a^x/b^x$$

$$b^x \div b^y = b^{x-y} \qquad (a \times b)^x = a^x \times b^x \qquad b^{-x} = 1/b^x$$

Injective and Surjective functions

An injective function is one where given two different ~~outputs~~ inputs a, b you will get two different outputs.
Aka image of $a \neq$ image B

Formally this is written ~~of~~ as $\forall a, b \in A$ if $a \neq b$ then $f(a) \neq f(b)$.

PROOF → show $f: \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x + 3$ is an injection

first assume that $a = b$

$f(a) = 2a + 3$ and $f(b) = 2b + 3$

$$2a + 3 = 2b + 3$$
$$2a = 2b$$
$$a = b$$

then assume $a \neq b$
if $f(a) \neq f(b)$ then

$$2a + 3 \neq 2b + 3$$
$$2a \neq 2b$$
$$a \neq b$$

$\therefore f$ is injective

To show it is not injective we only need to find one example of 2 inputs mapping to the same output. In a quadratic equation $f(x) = x^2$

x^2 where $x = 5$ or -5 produces the same output
$5^2 = 25$ $(-5)^2 = 25$
$5 \neq -5$

$\therefore f$ is not injective

A surjective function is very similar in that every element in the co-domain has at least one pre image in the domain of f. aka the range = co-domain.

Proof let $y \in \mathbb{R}$ show that $\exists x \in \mathbb{R} \mid f(x) = y$

$$f(x) = y \to 2x + 3 = y$$
$$2x = y - 3$$
$$x = \frac{y-3}{2}$$

$\therefore \forall y \in \mathbb{R} \; \exists x = \frac{y-3}{2} \in \mathbb{R} \mid f(x)$

$\therefore f$ is surjective as $\frac{y-3}{2}$ is always $\mathbb{R}$

Function Composition

Given a function $f(x)$ and $g(x)$ the composition of f and g is written as $f \circ g = f(g(x))$

example 1

Given $f(x) = 2x$ and $g(x) = x^2$ find $(f \circ g)(x)$

$$f(g(x)) = f(x^2) = 2(x^2) \qquad (f \circ g)(1) = f(1^2) = 2 \times 1^2 = 2$$

If $g: A \to B$ and $f: B \to C$ the $(f \circ g): A \to C$

$\boxed{\text{NOTE: Function composition is NOT commutative}}$

Bijective Functions

A bijective function (also known as invertible) is one that is both injective and surjective. Aka each element of the co-domain has exactley one pre-image

example 1, show $f: \mathbb{R} \to \mathbb{R}$ with $f(x) = 2x+3$ is bijective

Let $a, b \in \mathbb{R}$ show $f(a) = f(b)$ then $a = b$

$$f(a) = f(b) \to 2a+3 = 2b+3$$
$$2a = 2b$$
$$a = b \quad \therefore \text{ IS INJECTIVE}$$

let $y \in \mathbb{R}$ show $\forall y \in \mathbb{R}\ \exists x \in \mathbb{R}$

$$f(x) = y \to 2x+3 = y$$
$$2x = y-3$$
$$x = \frac{y-3}{2} \in \mathbb{R} \quad \therefore \text{ IS SURJECTIVE}$$

INVERSE FUNCTION

If the function is bijective then the inverse of the function exists.

If $f: A \to B$ then $f^{-1}: B \to A$

example 1, we have already established $f(x) = 2x+3$ is a bijection. to find the inverse we solve for y when $f(x) = y$

$$f(x) = y$$
$$2x+3 = y$$
$$2x = y-3$$
$$x = \frac{y-3}{2}$$

$$\therefore f^{-1}(x) = \frac{x-3}{2}$$

IDENTITY FUNCTION

The composition of the f and f^{-1} is equal to $x \to (f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = x$

example 1

If $f = 2x+3 \quad f^{-1} = \frac{x-3}{2}$

then $(f^{-1} \circ f)(x) = \frac{2x+3-3}{2} = \frac{2x}{2} = x$

PLOTTING THE INVERSE → the inverse of the function will always be symetric to the straight line $y = x$.

logarithmic functions

Exponential functions and logarithmic functions are closely related

If $f(y) = \log_b x$ then $f^{-1}(x) = b^y$

LOGARITHMIC RULES

$\log_b m \times n = \log_b m + \log_b n$ $\qquad \log_b 1 = 0$

$\log_b \frac{m}{n} = \log_b m - \log_b n$ $\qquad \log_b b = 1$

$\log_b m^n = n \times \log_b m$

NOTE $\ln(x)$

FLOOR AND CEILING FUNCTIONS

Floor and ceiling functions map $\mathbb{R}$ real numbers $\rightarrow$ $\mathbb{Z}$ to integers

FLOOR takes a real number x and rounds it down to the nearest integer n

$n \leq x < n+1$ or $\text{floor}(x) = \lfloor x \rfloor = n$

CEILING takes a real number x and rounds it up to the nearest integer $n+1$

$n < x \leq n+1$ or $\text{ceiling}(x) = \lceil x \rceil = n+1$

Proof let m be an integer such that $m = \lfloor x \rfloor$. Show that $\lfloor x+n \rfloor = \lfloor x \rfloor + n$

$m \leq x < m+1$ or $m+n \leq x+n \leq m+n+1$

This implies $\lfloor x+n \rfloor = m+n$, and $m = \lfloor x \rfloor$ therefore $\lfloor x+n \rfloor = \lfloor x \rfloor + n$

PROPOSITIONAL LOGIC

Propositional logic can be used in logic circuit design, as well as applying to programming languages such as prolog.

Many computer systems (theorem provers, program verifiers, AI) use logic based programming languages. They expand on propositional logic to use predicates.

"A proposition is a declarative statement that is either true or false but not both"

TRUTH TABLES - are tabular representations of all the possible combinations of truth values for a set of propositional variables. eg

p	q	$p \wedge q$	$p \vee q$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	0

a truth table will contain 2^n rows where n is the number of variables

TRUTH SET is the set of all elements of set S for which the proposition p is true

example 1

let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

let P and Q be two propositions

$P \rightarrow n$ is even

$Q \rightarrow n$ is odd

Therefore the truth set of p is $P = \{2, 4, 6, 8, 10\}$ and q is $Q = \{1, 3, 5, 7, 9\}$

PRECEDENCE OF LOGICAL OPERATORS $\neg \ \wedge \ \vee \ \rightarrow \ \leftrightarrow$

CONVERSE the converse of the statement $p \rightarrow q$ is $q \rightarrow p$

Let p: it's sunny q: John goes to the park

$p \rightarrow q$ ~~is~~ if it is sunny then john goes to the park

$q \rightarrow p$ if john goes to the park it is sunny

CONTRAPOSITIVE has the same truth table as the original statement so $p \rightarrow q$ becomes $\neg q \rightarrow \neg p$

$\neg q \rightarrow \neg p$ if john does not go to the park then it is not sunny

INVERSE and converse are equivalent $p \rightarrow q$ becomes $\neg p \rightarrow \neg q$

$\neg p \rightarrow \neg q$ if it is not sunny then john does not go to the park

Biconditional $\leftrightarrow$

the biconditional $p \leftrightarrow q$ is the equivalent of $(p \to q) \land (q \to p)$. They are interpreted as <u>if and only if</u>

LAWS of PROPOSITIONAL logic

	Disjunction	Conjunction
Idempotent Laws	$p \lor p \equiv p$	$p \land p \equiv p$
Commutative Laws	$p \lor q \equiv q \lor p$	$p \land q \equiv q \land p$
Associative Laws	$(p \lor q) \lor r \equiv p \lor (q \lor r)$	$(p \land q) \land r \equiv p \land (q \land r)$
Distributive Laws	$p \lor (q \land r) \equiv (p \lor q) \land (p \lor r)$	$p \land (q \lor r) \equiv (p \land q) \lor (p \land r)$
Identity Laws	$p \lor F \equiv p$	$p \land T \equiv p$
Domination Laws	$p \lor T \equiv T$	$p \land F \equiv F$
De Morgans Laws	$\neg(p \lor q) \equiv \neg p \land \neg q$	$\neg(p \land q) \equiv \neg p \lor \neg q$
Absorption Laws	$p \lor (p \land q) \equiv p$	$p \land (p \lor q) \equiv p$
Negation Laws	$p \lor \neg p \equiv T$	$p \land \neg p \equiv F$
Double Negation Laws	$\neg\neg p \equiv p$	$\neg\neg p \equiv p$

Predicate Logic

Predicate logic seeks to resolve limitations of propositional laws. Such statements it helps us to resolve are

→ All men are mortal
→ Socrates is a man
∴ Socrates is mortal

A question such as $x^2 = 4$ is not a proposition and it has no truth table until x is given a value.
In such an instance the variable is 'x' and the predicate is 'equal to 4'

We represent this as $P(x)$, where as soon as we give x the value it can be evaluated aka $P(2) = TRUE$, $P(3) = FALSE$

You can also use multiple values aka $P(x, y)$ denotes $x^2 > y$ therefore $P(-2, 3) = TRUE$ $P(2, 4) = FALSE$

QUANTIFIERS

they express the extent to which the statement is true over a range of variables

UNIVERSAL QUANTIFIERS $\forall$ → $P(x)$ is true for elements in the range. $\forall x\, P(x)$ = 'for all x'

EXISTENTIAL QUANTIFIERS $\exists$ → There exists an x in the range where $P(x)$ is true. $\exists x\, P(x)$ = 'for some of x'

UNIQUENESS QUANTIFIERS $\exists!$ → there exists a unique value x in the range such that $P(x)$ is true
$\exists! x\, P(x)$ = 'there exists a unique x'

nested quantifiers

$\forall x \forall y\, P(x, y)$ → $P(x, y)$ is true for every pair (x, y)
$\exists x \exists y\, P(x, y)$ → There is a pair (x, y) for which $P(x, y)$ is true
$\forall x \exists y\, P(x, y)$ → For all of x, there is a y for which $P(x, y)$ is true
$\exists x \forall y\, P(x, y)$ → There is an x for which $P(x, y)$ is true for all y

Binding Variables

are those that are bound by the quantifier for example $\exists x\, P(x, y)$ x is bound but y is free.

ORDER OF OPERATIONS

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

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

Quantifiers have precedence over all other operators

De Morgans Laws for Quantifiers

Negating quantified expressions is fairly common for universal $\forall$ quantified statements we simply need to prove only one instance is incorrect.

Let S be "All university computers are connected to the network"
Let P be "There is at least one computer in the university operating on linux"

In the instance of S we need to show only one computer is not connected to the network so:

$$\forall x P(x) \text{ becomes } \exists x \neg P(x)$$

For P we need that all of the university computers do not operate on linux so:

$$\exists x P(x) \text{ becomes } \forall x \neg P(x)$$

$\boxed{\text{example}}$ 1. Let S be "Every student of computer science has taken a course in neural networks" formally this is written as

$$\forall x P(x)$$

The negation is to show that "some students have not taken a course in neural networks" or formallay

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

when we have nested quantifiers we apply this from left to right:

$$\begin{aligned} \forall x \exists y \forall z P(x,y,z) &\equiv \exists x \neg P(x) \exists y \forall z P(x,y,z) \\ &\equiv \exists x \forall y \neg \forall z P(x,y,z) \\ &\equiv \exists x \forall y \exists z \neg P(x,y,z) \end{aligned}$$

RULES OF INFERENCE

In propositional logic an argument is defined as a sequence of propositions. The final proposition is the $\boxed{\text{conclusion}}$ the preceeding proposition are the $\boxed{\text{premise or hypothesis}}$

example 1 → if you have access to the internet, you can order a book on machine learning.

→ you have access to the internet $\boxed{\text{VALID}}$

→ ∴ You can order a book on machine learning

example 2 → if you have access to the internet, you can order a book on machine learning

→ you can order a book on machine learning

→ ∴ You have access to the internet

$\boxed{\text{INVALID}}$ you can order a book through avenues other than the internet

These rules can be used to build up complex valid arguments while avoiding producing large complex truth tables.

MODUS PONENS

$(p \wedge (p \to q)) \to q$ a tautology

and the rules of inference

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

Let P = "It is snowing"
Let Q = "I will study discrete maths"

If it is snowing then I will study discrete maths $P \to Q$
It is snowing P
Therefore I will study discrete maths $\therefore Q$

MODUS TOLLENS $(\neg q \land (p \to q)) \to \neg p$

And the rules of inference

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

let p = "It is snowing"
let q = "I will study discrete maths"

Becomes → I will not study discrete maths
→ If it is snowing I will study discrete maths
→ ∴ It is not ~~sted~~ snowing

CONJUNCTION $p \land q \to p \land q$

And the rules of inference

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

Let p = "I will study discrete maths"
Let q = "I will study programing

Becomes → I will study discrete maths
→ I will study programming
→ ∴ I will study discrete maths and I will study programming

SIMPLIFICATION $p \land q \to p$

And the rules of inference

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

Becomes → I will study discrete maths and I will study programming
→ ∴ Therefore I will study discrete maths

ADDITION $p \to (p \lor q)$

And the rules of inference

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

I will study discrete maths
∴ I will study discrete maths or I will study programming

HYPOTHETICAL SYLLOGISM $(p \to q) \land (q \to r) \to (p \to r)$

And the rules of inference:

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

let p: It is snowing
let q: I will study discrete maths
let r: I will get good grades

Becomes: → If it is snowing then I will study discrete maths
→ If I study discrete maths then I will get good grades
→ ∴ If it is snowing I will get good grades

RESOLUTION $((p \lor q) \land (\neg p \lor r)) \to (q \lor r)$

And the rules of inference:

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

let P: It is raining
let Q: It is cold
let R: It is snowing

Becomes → It is raining or it is cold
→ It isn't raining or It is snowing
→ Therefore it is cold or it is snowing

DISJUNCTIVE SYLLOGISM $((p \lor q) \land \neg p) \to q$

And the rules of inference

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

let p : I will study programming
let q : I will study discrete maths

Becomes → I will study programming or discrete maths
→ I will not study programming
→ ∴ I will discover discrete maths.

Building Valid Arguments

1. Assign variables to each proposition
2. Start with the hypothesis
3. Build up the logical steps
4. Add in the conclusion

example 1

We have the following statements:

- ☆ It is not cold tonight.
- ☆ We will go to the theatre only if it is cold
- ☆ If we do not go to the theatre we will watch a movie at home.
- ☆ If we watch a movie at home we will need to make popcorn

we define our variables:

- p : it is cold tonight
- q : We will go to the theatre
- r : We will watch a movie at home
- s : We will need to make popcorn

We then build the logical statements

- ☆ $\neg p$
- ☆ $q \to p$
- ☆ $\neg q \to r$
- ☆ $r \to s$

We can then build this as follows

$q \to p$	hypothesis
$\neg p$	hypothesis
$\therefore \neg q$	Modus Tollens
$\neg q \to r$	hypothesis
$\therefore r$	Modus Tollens
$r \to s$	hypothesis
$\therefore s$	CONCLUSION

FALLACIES

a fallacy is the use of an incorrect argument when reasoning. Common formal fallacies are

AFFIRMING THE CONSEQUENT is taking $P \to Q$ and assuming ~~$Q \to P$~~ $Q \to P$ is also correct.

- ➡ If an animal is a dog, then it has 4 legs
- ➡ My cat has 4 legs
- ∴ Therefore my cat is a dog.

A CONCLUSION THAT DENIES THE PREMISE is taking $P \to Q$ and assuming $\neg P \to \neg Q$ is also correct

- ➡ If you are a ski instructor then you have a job
- ➡ You are not a ski instructor
- ∴ You have no job

CONTRADICTORY PREMISE is where the two premises are inconsistent or incompatible.

- ➡ God is omnipowerful
- ➡ God creates a stone he cannot lift
- ∴ God can lift the stone

DENYING THE ANTECEDENT same as a conclusion that denies the premise

EXISTENTIAL FALLACY is when your initial statement may not have happened

- ➡ All trespassers will be prosecuted
- ➡∴ Some of those prosecuted have trespassed

FALLACY OF EXCLUSIVE PREMISES invalid categorical syllogism that is invalid because both premises are negative

- No cats are dogs
- Some dogs are not pets
- ∴ some pets are not cats

Rules of Inference w/ Quantifiers

UNIVERSAL INSTANTIATION

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

All computer science students study discrete maths
John is computer science student ∴ will study discrete maths

EXISTENTIAL INSTATIATION

$$\frac{\exists x P(x)}{\therefore P(c)}$$

There exists ~~a~~ data science student who uses python
Therefore there is a student using Python

UNIVERSAL GENERALISATION

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

C is a data science student, studying machine learning
∴ for all data science students, they study machine learning

EXISTENTIAL GENERALISATION

$$\frac{P(c)}{\therefore \exists x P(x)}$$

John a data science student got an A in machine learning
Therefore there exists a data science student that got an A

UNIVERSAL MODUS PONENS

$$\frac{\forall x P(x) \rightarrow Q(x) \quad P(a)}{\therefore Q(a)}$$

Every computer science student studying data science will study machine learning / John is doing data science
∴ John will study machine learning

UNIVERSAL MODUS TOLLENS

$$\frac{\forall x P(x) \rightarrow Q(x) \quad \neg Q(a)}{\therefore \neg P(a)}$$

Every computer science student studying data science will do machine learning / John isn't studying ~~ES~~ ML
∴ John is not a data science student

EXPRESSING complex statements

1. determine the universe of discourse of the variables
2. Reformulate the statement by making FOR ALL and THERE EXISTS explicit
3. define the variables and the predicates
4. Add in quantifiers and logical operators

EXAMPLE 1: There exists a real number between any two not equal real numbers.

1. the universe is the set $\mathbb{R}$
2. For all real numbers THERE EXISTS a real number between 2 other real numbers
3. For all real numbers x, y there exists a real number z between x and y
4. $\forall x, y \in \mathbb{R}\ \exists z \in \mathbb{R}\ x < z < y$

BOOLEAN ALGEBRA

Boolean algebra forms the basic building blocks of computer circuit analysis. We can represent "when the system is activated a fire sprinkler should spread water if high heat is detected" becomes:

$w = h \text{ AND } a$ where h = high heat detected
a = system is activated
w = water is sprayed

AND $\rightarrow x \cdot y,\ x \cap y,\ x \wedge y$

OR $\rightarrow x + y,\ x \cup y,\ x \vee y$

NOT $\rightarrow x',\ \overline{x},\ \neg x$

HUNTINGTONS POSTULATES

There are six criteria that must be satisfied by any boolean algebra.

- → **CLOSURE**, all results must be binary $\{0, 1\}$
- → **IDENTITY**, $x + 0 = x$ and $x \cdot 1 = x$
- → **COMMUTATIVITY**, $x + y = y + x$ and $x \cdot y = y \cdot x$
- → **DISTRIBUTIVITY**, $x \cdot (z + y) = (x \cdot z) + (x \cdot y)$

  $x + (z \cdot y) = (x + z) \cdot (x + y)$
- → **COMPLEMENT**, complements exist for all elements. $x + \overline{x} = 1$ $\quad x \cdot \overline{x} = 0$
- → **DISTINCT ELEMENTS**, the elements are distinct. $0 \neq 1$

Application of De Morgans Theorums

$\overline{x \cdot y} = \overline{x} + \overline{y}$ THEORUM 1

$\overline{x + y} = \overline{x} \cdot \overline{y}$ THEORUM 2

To build equivalent boolean relations you take the first then reverse all the signs and variables.

- $+$ becomes $\cdot$ and vice versa
- 0 becomes 1 and vice versa

example $A + B \cdot C \equiv A \cdot (B + C)$ this is **DUALITY PRINCIPLE**

There are several ways you can go about proving that this is true

PERFECT INDUCTION prove using truth tables (tedious as the tables become large as the variables grow).

AXIOMATIC PROOF you use huntingtons postulates to substitute values until identical expressions are found.

DUALITY PRINCIPLE apply the duality principle and then check every theorem remains valid.

CONTRADICTION assume the hypothesis is false to show the conclusion is false.

example, $x + (x \cdot y) \equiv x$

This can be proved via a truth table

x	y	$x \cdot y$	$x + (x \cdot y)$
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	1

We can also prove it using huntingtons postulates

$$\begin{aligned} x + (x \cdot y) &\equiv (x \cdot 1) + (x \cdot y) \\ &\equiv x \cdot (y + 1) \\ &\equiv x \cdot 1 \\ &\equiv x \end{aligned}$$

Boolean Functions

A boolean function maps from 1 or more boolean inputs to a boolean output

For n input values there are 2^n possible combinations, eg with 3 variables you will a table with 8 rows.

While there is a single way of representing a boolean function in a truth table there are multiple ways of representing the function algebraically.

For example $x + \overline{x} \cdot y = x + y$

Standardised boolean functions are represented as either 'sum of all products' or 'product of all sums'.

SUM OF PRODUCTS is of the form $f(x, y, z) = xy + xz + yz$

PRODUCT OF SUMS is of the form $f(x, y, z) = (x + y) \cdot (x + z) \cdot (y + z)$

The sum of products is usually the prefered form as it is usually easier to use and simplify

BUILD A SUM OF PRODUCTS FORM

1. Look at the values of the variables that make the function evaluate to 1.

2. If an input is 1, it appears uncomplemented in the expression

3. If an input is 0, it appears complemented in the expression

4. The function is then represented as a sum-of-products of all the terms for which the function is 1.

x	y	$f(x,y)$	
0	0	0	→ ignore per step 1
0	1	1	→ x is complemented y is not $\bar{x}y$
1	0	1	→ x is uncomplemented y is $x\bar{y}$
1	1	1	→ x and y are uncomplemented xy

$$\therefore f(x,y) = \bar{x}y + x\bar{y} + xy$$

Useful functions:

EXCLUSIVE OR

x	y	$f(x,y)$	
0	0	0	→ ignore
0	1	1	→ $\bar{x}y$
1	0	1	→ $x\bar{y}$
1	1	0	→ ignore

$\therefore f(x,y) = \bar{x}y + x\bar{y}$

IMPLIES

x	y	$f(x,y)$	
0	0	1	$\bar{x}\bar{y}$
0	1	1	$\bar{x}y$
1	0	0	→ ignore
1	1	1	xy

$\therefore f(x,y) = \bar{x}\bar{y} + \bar{x}y + yx$ or $\bar{x} + y$

Logic Gates

A logic gate is the basic element of circuits implement a boolean operation.

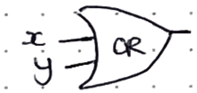
All boolean functions can be written in terms of these three logic gates

AND

an and gate produces a HIGH output (value 1) only when all its inputs are high. Otherwise its output is LOW

OR

The or gate produces a HIGH (value 1) output only when at least 1 input is HIGH. Otherwise its outputs are low.



NOT

Not (inverter) gate produces HIGH output when the input is LOW; And LOW when the input is HIGH

XOR

The XOR gate produces a HIGH output if its inputs have different values. If they are the same then the output is low.

$\boxed{\text{NAND}}$ is an inversion of an and gate

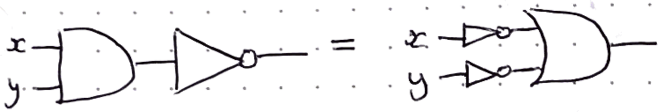
$\boxed{\text{NOR}}$ is an inversion of an or gate

$\boxed{\text{XNOR}}$ is an inversion of an XOR gate

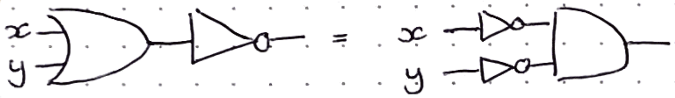
AND, OR, XOR and XNOR are commutative and associative, all can be extended beyond 2 input

NAND and NOR are commutative but not associative, extension beyond 2 inputs is less obvious, use parentheses!

De morgans laws in logic gates can be represented as follows:



or $\overline{x \cdot y} = \overline{x} + \overline{y}$



or $\overline{x + y} = \overline{x} \cdot \overline{y}$

Combinational Circuits

A combinational circuit is a way a representing a boolean function using logic gates.

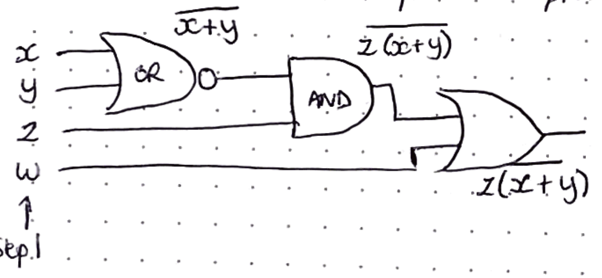
We can use this circuit to represent all states of the function, and intuitively we want to minimise the number of gates used in order to reduce the cost of the circuit.

WRITING FUNCTION FROM A CIRCUIT

LABEL all gates outputs that are a function of the input variables

EXPRESS the boolean functions for each gate in the first level

REPEAT until all outputs are expressed



BUILD A CIRCUIT FOR A PROBLEM

The steps to build a circuit to address a specific problem are:

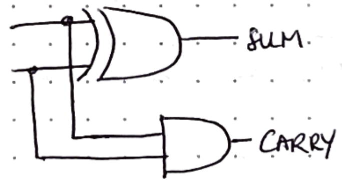
LABELLING the inputs and output variables

MODELLING the problem as a boolean expression

REPLACING each operation by the equivalent logic gate

A function that adds binary bits is as follows.

x	y	sum (OR)	carry (AND)
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1



Simplify Circuits

Every function can be written as a sum-of-products but this may not be the most efficient solution in terms of the number of gates.

Simplifying has the following benefits:

- Reduces the costs of circuits by reducing the number of gates
- May reduce computation time
- Allows more logic for the same area.

To simplify expressions we can use the following:

Theorem	Logical Sum	Logical Product
Idempotent Laws	$x + x = x$	$x \cdot x = x$
Tautology/contradiction	$x + 1 = 1$	$x \cdot 0 = 0$
Involution	$\bar{\bar{x}} = x$	
Associative Laws	$(x+y)+z = x+(y+z)$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
Absorption Laws	$x + (x \cdot y) = x$	$x \cdot (x+y) = z$
Uniqueness of Complement	If $x+y=1$ & $y \cdot x = 0$ then $x = \bar{y}$	
Inversion Law		

$\boxed{\text{Example 1}}$ Simplify $E = \overline{\overline{(xy)}z} \; \overline{((\bar{x}+z)(\bar{y}+\bar{z}))}$

$= \overline{\overline{(xy)}} + \bar{z} \; \overline{((\bar{x}+z)(\bar{y}+\bar{z}))}$ de morgans $\overline{x \cdot y} = \bar{x} + \bar{y}$

$= (xy + \bar{z})(\overline{(\bar{x}+z)} + \overline{(\bar{y}+\bar{z})})$ involution $\bar{\bar{x}} = x$ and de morgans

$= (xy + \bar{z})(\bar{\bar{x}}\bar{z} + \bar{\bar{y}}\bar{\bar{z}})$ de morgans

$= (xy + \bar{z})(x\bar{z} + yz)$ involution

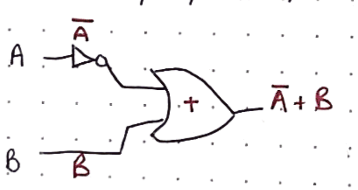
$= xyx\bar{z} + xyyz + \bar{z}x\bar{z} + yz\bar{z}$ multiply out

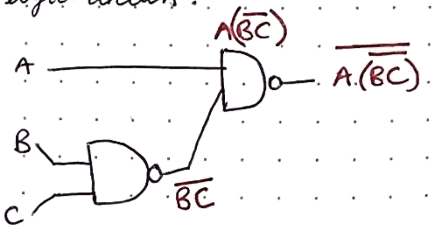
$= xy\bar{z} + xyz + x\bar{z} + 0$ idempotent, contradiction $z \cdot \bar{z} = 0$, $y \cdot 0 = 0$

$= xy + x\bar{z}$ using absorption law

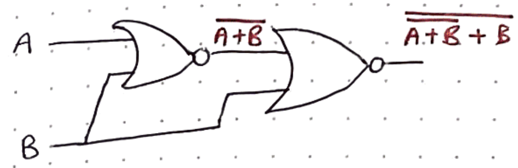
Boolean Algebra Questions

What is the output for the following logic circuit:





Write down the truth table for the following circuit



A	B	$A+B$	$\overline{A+B}$	$\overline{A+B}+B$	$\overline{\overline{A+B}+B}$
0	0	0	1	1	0
0	1	1	0	1	0
1	0	1	0	0	1
1	1	1	0	1	0

Simplify each of the following expressions to $0, 1, A, B, AB, A+B, \overline{AB}, \bar{A}+\bar{B}, \bar{A}B, A\bar{B}$:

1. $\overline{\bar{A}+\bar{B}}$
   $\bar{\bar{A}}\bar{\bar{B}}$ using de morgans
   AB

2. $A(A+\bar{A})+B$
   $A(1)+B$ as $A+\bar{A}=1$
   $A+B$ as $A.1 = A$

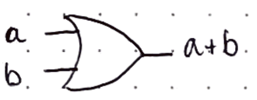
3. $(A+B)(\bar{A}+B)\bar{B}$
   $(A+B)(\bar{A}\bar{B}+B\bar{B})$ distributivity
   $(A+B)(\bar{A}\bar{B}+0)$ $B.\bar{B}=0$
   $A\bar{A}\bar{B} + \bar{A}B\bar{B}$ $A.\bar{A}=0$ commutativity
   $0B + 0A$
   0 ∴ A contradiction

Use the laws of boolean algebra to simplify $a + \bar{a}b = a + b$

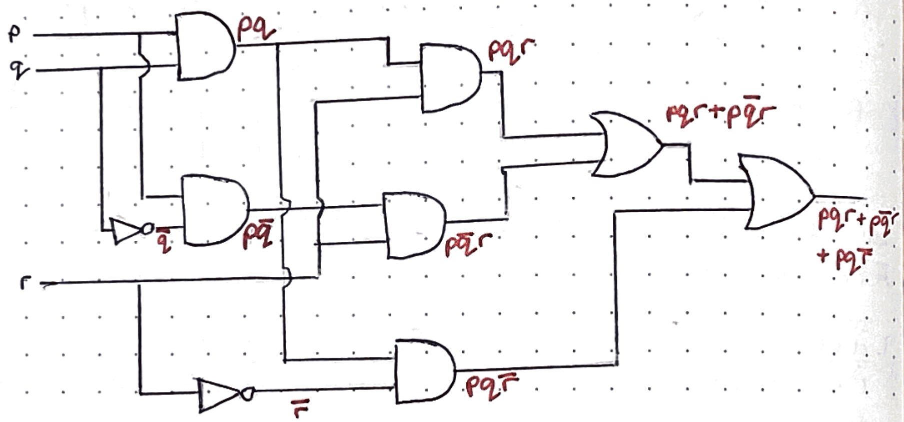
$a + \bar{a}b = a.1 + \bar{a}b$ Identity Law
$= a(1+b) + \bar{a}b$ ~~Identity Law~~ Domination Law
$= a.1 + ab + \bar{a}b$ Distributive
$= a.1 + b(a\bar{a})$ Distributive
$= a + b$

Use the truth table to show the above, and then find a simplified ~~target~~ circuit:

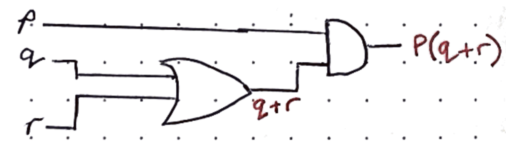
a	b	$\bar{a}b$	$a+\bar{a}b$	$a+b$
0	0	0	0	0
0	1	1	1	1
1	0	0	1	1
1	1	0	1	1



What is the output of the following logic circuit?



Simplify the above circuit $pqr + p\bar{q}r + pq\bar{r}$



PROOFS

A proof is a valid argument used to ~~produce~~ prove the truth of a mathematical statement

THEORUM a formal statement that can be shown to be true

AXIOM a statement assumed true to serve as a premise for future arguments

LEMMA a proven statement used as a step to a larger result

COROLLARY a theorem that can be established by a short proof from a theorem.

To formally write the theorem "there exists a real number between any two non equal real numbers" can be written as

$\forall x, y \in \mathbb{R}$ if $x<y$ then $\exists z \in \mathbb{R}$ where $x<z<y$

DIRECT PROOF

a direct proof is showing $p \to q$ is true. Using the above theory we would show this as follows

PROOF let x and y be elements in $\mathbb{R}$ where $x<y$
let $z = \frac{x+y}{2}$, $z \in \mathbb{R}$ therefore $x<z<y$ is true

CONTRAPOSITIVE PROOF

a contrapositive proof is using $\neg q \to \neg p$ to show $p \to q$ is true.

PROOF If n^2 is even then n is even, contrapositive becomes
If n is odd then n^2 is odd

let $n = 2k+1$ (anything multiplied by 2 is even, +1 is odd)

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= (2k+1)(2k+1) \\ &= 4k^2+2k+2k+1 \\ &= 2(2k^2+2k)+1 \end{aligned}$$
(anything multiplied by 2 is even, +1 is odd)

$\therefore$ if n^2 is odd then n is odd

CONTRADICTION

relies on assuming the premise $p \to q$ to be false and showing it leads to a contradiction.

PROOF There are infinitely many prime numbers assume
there are finite amount of prime numbers

lets make c the product of all prime numbers +1
c has at least one prime divisor

mathmatical Induction

is showing that if $P(1)$ is true then we can see it as a drop in dominos. showing $P(k) \rightarrow P(k+1)$ is true means all is true. using inference

$$\frac{P(1) \quad \forall k\,(P(k) \rightarrow P(k+1))}{\therefore \forall n\, P(n)}$$

→ The base case is to work out $P(1)$

→ The inductive step is to show $P(k) \rightarrow P(k+1)$ is true

(EXAMPLE 1) Show $P(n)$: $1+2+3+4\ldots+n = \frac{n(n+1)}{2}$

BASE CASE $1 = \frac{1(1+1)}{2}$ ∴ True

INDUCTIVE STEP

$$1+2+3+4\ldots k = \frac{k(k+1)}{2}$$

$$1+2+3+4\ldots+(k)+(k+1) = \frac{(k+1)(k+2)}{2}$$

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

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

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

Example 2 Prove $3^n < n!$ if $n \geq 7$

BASE CASE $3^7 < 7!$ or $2187 < 5040$

INDUCTIVE STEP $3^k < k!$

$3^{k+1} < (k+1)!$

$$3 \times 3^k < (k+1) \times k!$$

STRONG INDUCTION

makes the inductive step easier to prove by assuming it is true for all k less than $k+1$

example 3. where $n \geq 2$ show it is divisible by a prime number

BASE CASE 2 is a prime number. 2/2, aka 2 divides itself

INDUCTIVE STEP let m be a prime number where $2 \leq m \leq k+1$
We consider 2 cases
→ either k is prime, in which case it is divisible by itself
→ or it is not prime, in which case it is the product of ab

WELL ORDERING PROPERTY

The axioms about $\mathbb{N}$ that we assume to be true are

1. The number 1 is a positive number
2. If $n \in \mathbb{N}$ is a positive integer then $n+1$ is also positive
3. Every positive integer except for one is proceeded by a positive integer
4. WELL ORDERING property is every non empty subset of the set of positive integers has at least 1 element.

example 4. Let S be the set of positive integers > 1 without a prime divisor.
Suppose S is non-empty, it is not a prime since it would be it's own prime divisor.
Therefore it must have another divisor d where $1 < d < n$ then d must have a prime divisor

RECURSION

Defining a mathematical object in terms of itself is called recursion

RECURSIVE FUNCTION

consists of the $\boxed{\text{basis step}}$ the initial value

and the $\boxed{\text{recursive step}}$ a rule for finding the value from its previous values

example 1 The fibbonacci function can be defined as

$$f(0) = 1$$
$$f(1) = 1$$
$$f(n) = f(n-1) + f(n-2)$$

RECURSIVE SETS

$\boxed{\text{Basis step}}$ initial contents of the set

and the $\boxed{\text{recursive step}}$ is a rule for generating new elements for the set

for example

$(2, 3) \in S$ BASIS STEP

RECURSIVE STEP $x \in S \wedge y \in S \rightarrow x + y \in S$

$(2, 3, 5, 7, 8 \ldots)$

RECURSIVE ~~RELATI~~ ALGORITHMS

A recursive algorithm solves a problem by reducing it to a smaller instance of the same problem.

example for computing $n!$

```
function Factorial(n)
    if n=0 then
        return 1
    return n x Factorial (n-1)
```


Recurrence Relations

A recurrence relation is an equation that defines a sequence based on a rule that produces the next term as a function of the previous terms.

In many cases it is useful to formulate the problem sequence and then try and solve it

Linear Recurrence

A relation in which each term of the sequence is a linear function of the earlier terms.

LINEAR HOMOGENOUS

$\rightarrow a_n = C_1 a_{n-1} + C_2 a_{n-2} + C_3 a_{n-3} \ldots + C_k a_{n-k} \quad C_1 \ldots C_k \in \mathbb{R}$

LINEAR NON-HOMOGENOUS

$\rightarrow a_n = C_1 a_{n-1} + C_2 a_{n-2} \ldots C_k a_{n-k} + f(n).$

Linear homogenous relations have constant coefficients with every output being divisible by those co-efficients.

We call the oldest value in the sequence the degree for example $f(n) = f_{n-1} + f_{n-3}$ is a linear homogenous relation to the third degree

Solving Linear Homo Lines

The basic approach to solving linear homogenous recurrence relations is to look for solutions of the form $a_n = r^n$

NOTE $a_n = r^n$ is only a solution if if and only if:

$$r^n = C_1 r^{n-1} + C_2 r^{n-2} \ldots + C_k r^{n-k} \quad \text{when}$$
$$a_n = C_1 a_{n-1} + C_2 a_{n-2} \ldots + C_k a_{n-k}$$

We then divide both sides by r^{n-k} and subtract right from the left to get

$$r^k - C_1 r^{k-1} - C_2 r^{k-2} - \ldots C_{k-1} r - C_k = 0$$ CHARACTERISTIC EQUATION

Solving the characteristic equation is the first step towards finding a solution to the linear homogenous recurrance

example 1 → solve $a_n = a_{n-1} + 2a_{n-2}$ where $a_0 = 2$ and $a_1 = 7$

→ let $a_n = r^n$ to get

$$r^n = r^{n-1} - 2r^{n-2}$$

→ divide both sides by r^{n-2}

$$r^{(n)-(n-2)} = r^{(n-1)-(n-2)} - 2r^{(n-2)-(n-2)}$$

$$r^2 = r + 2$$

→ rearrange to get a quadratic equation

$$0 = r^2 - r - 2$$

→ substitute into the quadratic equation

$$= \frac{-(-1) \pm \sqrt{-1^2 - 4\times1\times-2}}{2\times1}$$

$$= \frac{1 \pm \sqrt{9}}{2} = \frac{1 \pm 3}{2}$$ ∴ roots are 2 and -1

→ If $a_n = \alpha_1 r_1^n + \alpha r_2^n$ then the sequence $\{a_n\}$ is a recurrance relation

$$= \alpha_1 2^n + \alpha_2 (-1)^n$$

→ then we substitute in the known values for a_0 and a_1

$$a_0 = 2 = \alpha_1 2^0 + \alpha_2 (-1)^n = \alpha_1 + \alpha_2$$

$$a_1 = 7 = \alpha_1 2^1 + \alpha_2 (-1)^1 = \alpha_1 2 + \alpha_2$$

→ then ~~now~~ solve the equations

$2 = \alpha_1 + \alpha_2$ rewrite this to get $\alpha_1 = 2 - \alpha_2$

$7 = 2\alpha_1 - \alpha_2$ substitute in new value α_1

→ $7 = 2(2 - \alpha_2) - \alpha_2$ or $7 = 4 - 2\alpha_2 - \alpha_2$

Therefore $\alpha_2 = -1$ then substitute this back in to get α_1

$2 = \alpha_1 + -1$ or $3 = \alpha_1$

∴ the solution is $3 \times 2^n - 1(-1)^n$

TEST $a_0 = 2$, $a_1 = 7$, $a_2 = 7 + 2\times2 = 11$

$$a_2 = 3\times2^2 - 1(-1)^2 = 12 - 1(1) = 11$$

GOOD

NOTE when quadratic equation doesn't work then factorise; steps are the same but root 1 and root 2 will have same value

example 2 what is the solution for $a_n = 6a_{n-1} - 9a_{n-2}$, $a_0 = 1$ and $a_1 = 6$

→ assume $a_n = r^n$

$$r^n = 6r^{n-1} - 9r^{n-2}$$

→ divide both sides by r^{n-2}

$$r^2 = 6r - 9$$

→ rearrange to a quadratic and factorise

$$0 = r^2 - 6r + 9 \to (r-3)(r-3)$$

∴ one solution 3

→ If $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n$ then $\{a_n\}$ is a recurrence relation

$\alpha_1 3^n + \alpha_2 n 3^n$ ∴ $r_2^n = n r^n$

→ Solve using initial given values

$a_0 = 1 = \alpha_1$, $\alpha_1 = 1 - \alpha_2$

$a_0 = 1 = \alpha_1$ ∴ $\alpha_1 = 1$

substitute into a_1

$a_1 = 6 = 3 + \alpha_2 \times 3$

$6 = 3(1 - \alpha_2) + 3\alpha_2$

$6 = 3 - 3\alpha_2$

$3 = 3\alpha_2$ or $\alpha_2 = 1$

∴ $\alpha_1 = 1$ and $\alpha_2 = 1$

∴ Solution is $a_n = 3^n + n3^n$

If you have 2 roots

$$a_n = \alpha_1 r_1^n + \alpha r_2^n$$

If you have 1 root

$$a_n = \alpha_1 r_0^n + \alpha_2 n r_0^n$$

GRAPH THEORY

Graphs are discrete structures (aka not continuous) consisting of vertices and edges connecting them.

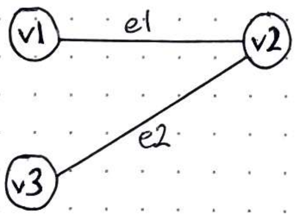
Graph theory is a branch of mathematics that studies these structures.

APPLICATIONS

→ modelling computer networks
→ modelling road maps
→ solving shortest path problems
→ Assigning jobs to employees
→ distinguishing chemical compound structures

A graph is an ordered triple $G = \{V, E\}$ where V is the set of vertices and E is the set of edges.

VERTEX



The basic element of a graph and is drawn as a node or a dot. The set of vertices of G is usually written as V(G) or just V

← In this figure:

$$V(G) = \{v1, v2, v3\}$$

EDGE

an edge is a link between the vertices the set of edges is usually written as E(G) or just E.

In the above graph:

$$E(G) = \{e1, e2\} = \{\{v1, v2\}, \{v2, v3\}\}$$

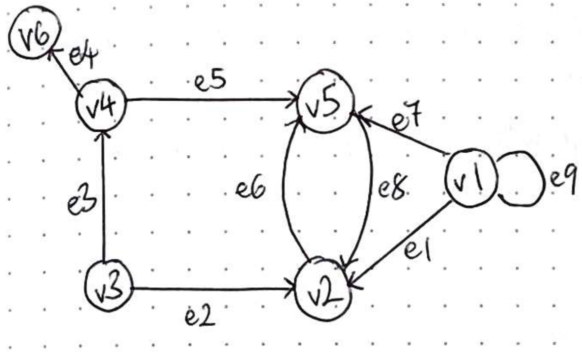
ADJACENCY

→ two vertices are adjacent if they are endpoints on the same edge

→ Two edges are adjacent if they share the same vertex

→ If the vertex V, is the endpoint of edge e, then v and e are said to be incident.

LOOP + PARALLEL EDGES

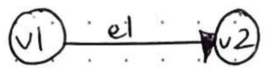


v2 and v5 are linked by e6 and e8, e6 and e8 are said

The vertex v1 is linked to itself by e9, e9 is referred to as a loop.

DIRECTED GRAPHS

a directed graph is one where the edges have a direction.



e1 is a connection for v1 to v2
it is NOT a connection for v2 to v1.

WALKS and PATHS

WALK

is a sequence of vertices and edges, where the edge or vertices can be repeated.

It is usually of the form uv, vw, wx, ... yz

Using the above graph we can do a walk of length 4 we can go from v1 to 6 by v1v2, v2v3, v3v4, v4v6 = e1, e2, e3, e4 = v1v2v3v4v6

TRAIL

is a walk in which no edge is repeated. A vertices can be repeated

CIRCUIT is where the start and ending vertices are the same, but only vertices can be repeated

PATH is where neither a vertices or edge is repeated

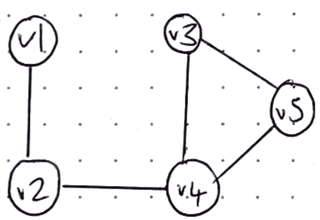
CYCLE is a closed path where the vertex is reachable from itself

EULERIAN is a path that uses every edge once. If such a path exists then it is TRAVERSABLE.

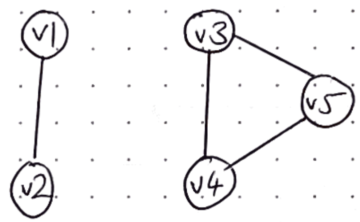
HAMMILTONIAN PATH uses every vertex only once. If a path exists then the graph is TRACEABLE

HAMMILTONIAN CYCLE uses every vertex only once except for the starting vertex which gets used twice at the start and end. If that exists it is a HAMMILTONIAN GRAPH

CONNECTIVITY an undirected graph is connected if you can get from one vertex to another by ~~p~~ following a sequence of edges. This means any two random nodes are connected by a path.



CONNECTED



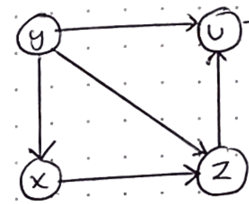
NOT CONNECTED

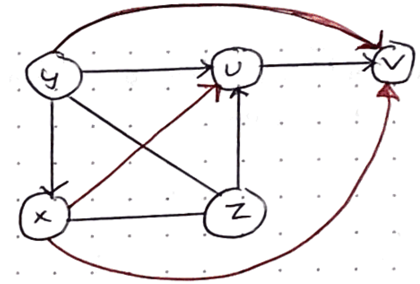
STRONG CONNECTIVITY a strongly connected graph is one where there is a path from any node to another node. Pay attention to directed path arrows.

TRANSITIVE CLOSURE given a directed graph G, the transitive graph G^* is such that

→ it has all the same vertices as G

→ if G has a directed path from u to v then g^* has an edge u to v





The Degre Sequence

UNDIRECTED graph it is the number of edges attached to the vertex (a loop counts as two).

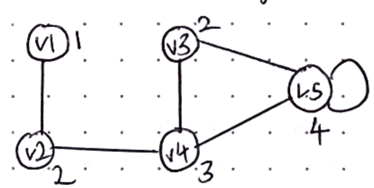
DIRECTED GRAPH

IN-DEGREE → number of edges going in

OUT-DEGREE → number of edges going out

DEGREE → the sum of in-degree and out-degree

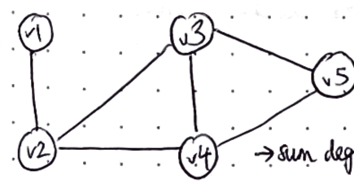
Given an undirected graph the degree sequence is the set of degrees for each vertex reducing eg



⇐ the degree sequence is 4, 3, 2, 1

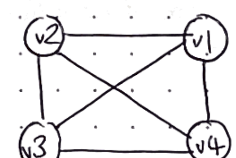
NOTE The sum of the degree sequence is always even
It is always the count of all the edges x 2

SIMPLE GRAPHS
contain no loops and no parallel edges

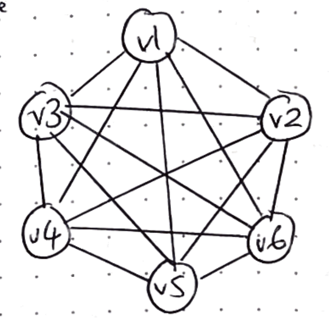


→ vertices have degrees higher or equal to vertex count = NO

REGULAR GRAPHS
all local degrees are the same



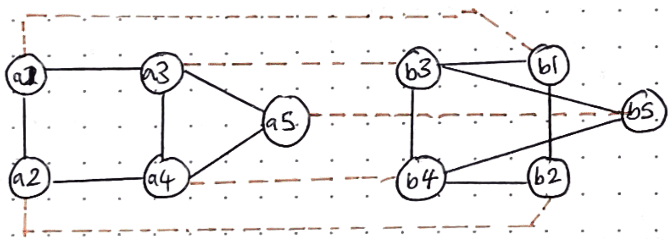
COMPLETE GRAPH where every edge is adjacent.



Every vertex has a degree $n-1$
Sum of degree sequences $n(n-1)$
number of edges $\frac{n(n-1)}{2}$

Isomorphic Graphs

Two graphs are isomorphic if there is a bijection that preserves adjacency and non-adjacency.



G_1	a_1	a_2	a_3	a_4	a_5
$f(G_1)=G_2$	b_1	b_2	b_3	b_4	b_5

Step 1 is to map each function, it is bijective as each element in G_1 maps to exactly 1 in G_2 and vice versa

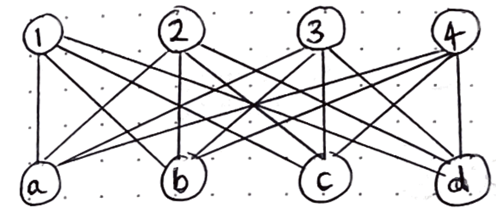
Step 2 ➔ if an edge uv exists in G_1 then it also exists in G_2 as $f(u)\,f(v)$

NOTE 2 graphs of different degree sequences cannot be isomorphic
2 graphs with the same degree sequence aren't automatically isomorphic

Imagine, can you rearrange the graphs to look like one another without breaking the connections

Bipartite Graphs

A graph $G(V,E)$ is bipartite if the set of vertices V can be partitioned into two disjoint sets such that each edge has a start and end in V_1 or V_2.



each edge starts in the top and ends in the bottom.

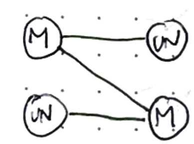
MATCHING a matching is a set of pairwise non-adjacent edges, none of which are loops. Meaning no two edges share the same endpoint.
A vertex is matched (or saturated) if it is an endpoint of one of the edges in the matching. Otherwise, the vertex is unmatched.

MAXIMUM MATCHING a maximum matching size such that if any edge is added, it is no longer a matching. In a single bipartite graph there may be many possible maximal matchings.

Hopcroft-Karp Algo

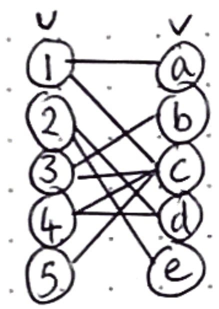
1. INITIALISE $M = \{\}$
2. WHILE AUGMENTING PATH EXISTS
   - → USE BFS to build layers that terminate at free vertices
   - → START AT FREE vertices in C, use DFS
3. RETURN M

An augmenting path connects two unmatched vertices



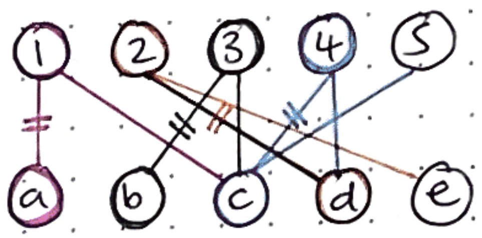
UN - unmatched
M - matched
— - path

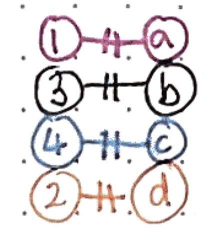
example



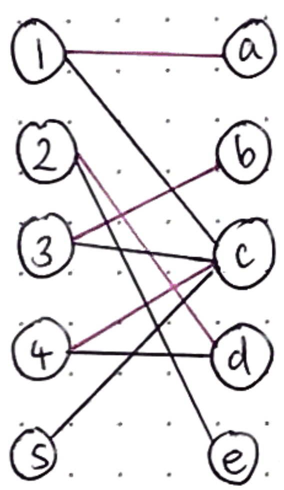
$\boxed{\text{STEP 1}}$ → lets start with an empty M. No matched pairs

$\boxed{\text{STEP 2}}$ → look at each vertex in U and match it to a vertex in V. when matched remove all the ~~vertex~~ edges attached to each vertex.

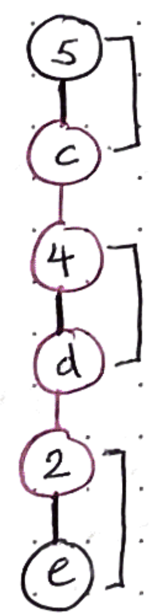




Once we have done the first pass our graph looks like this



$\boxed{\text{STEP 3}}$ we then start from an unmatched vertex and find a path to another unmatched vertex. So starting on 5

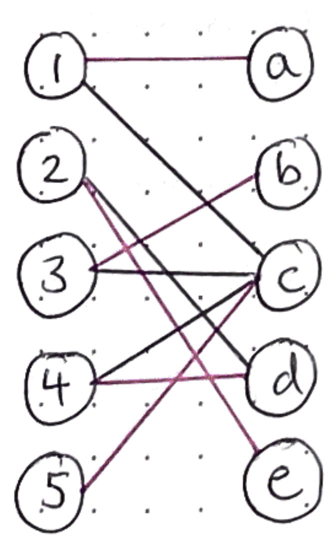


$\boxed{\text{STEP 4}}$ This path contains 2 edges that are currently matching c-4 and d-2 so we remove these from M

$\boxed{\text{STEP 5}}$ we then add back the newly matched 5-c, 4-d and 2-e back into M. To get

1 — a
3 — b
5 — c
4 — d
2 — e

all nodes are now matched and so we stop this is our final result



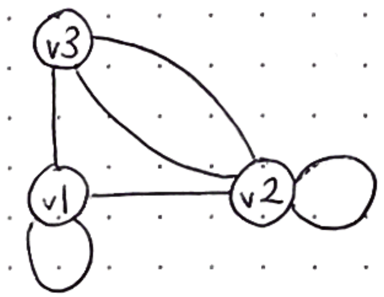
Adjacency Matrix of a graph

The adjacency list is simply a list of all the vertices and what is adjacent to them for example

Vertex	Adjacent Vertices
A	B, C
B	A, C, D
C	A, B, D, E
D	B, C, E
E	C, D

NOTE we can draw a graph from its adjacency list alone.

A graph can also be represented by an adjacency matrix. Using the graph below

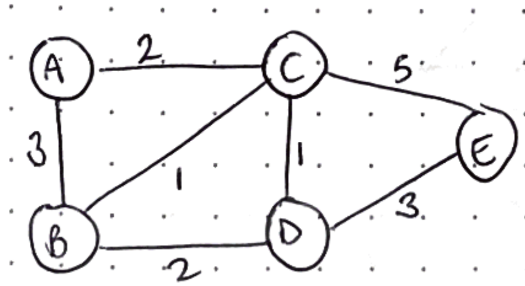


$$M(G) = \begin{bmatrix} v1v1 & v1v2 & v1v3 \\ v2v1 & v2v2 & v2v3 \\ v3v1 & v3v2 & v3v3 \end{bmatrix}$$

$$M(G) = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 0 \end{bmatrix}$$

The adjacency matrix can also be produced for directed graphs. But it is important to note that $V1$ being adjacent to V_2 does not imply V_2 being adjacent to $v1$

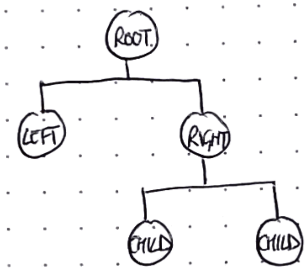
Dijkstra Algo is used to compute the shortest distance between ~~alg~~ vertexs. It is done on a weighted graph (where an edge is given a value)



VERTEX	SHORTEST DISTANCE FROM A	PRIOR VERTEX
A		
B		
C		
D		
E		

TREES

An ACYCLIC graph is one that has no cycles (a loop where no edge or vertex is repeated). A tree is a connected acyclic undirected graph. It cannot have loops or parallel edges.



A FOREST is a cycle free disconnected graph

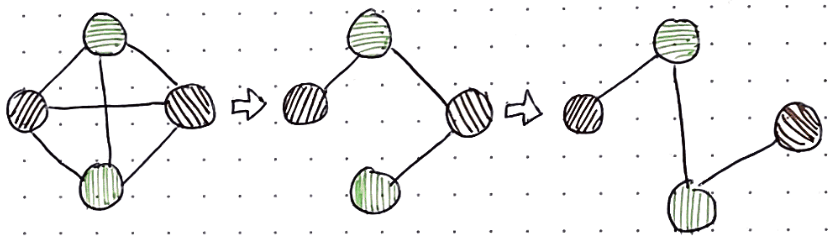
In a undirected path you must be careful not to create a cycle otherwise it ceases to become a tree

A tree with n vertices has n-1 edges.

ROOTED TREE is where you have defined a vertex to be the root. Every edge is directed away from the edge

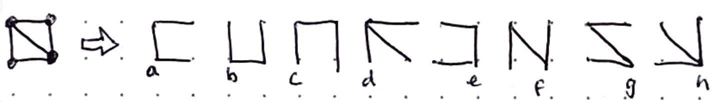
SPANNING TREES

is a subgraph of G in a tree format. It contains all vertices of G but no cycles



etc

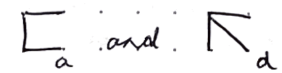
All possible combinations should be considered for example:



NON-ISOMORPHIC spanning trees are said to be isomorphic if there is a bijection preserving adjacency between the two trees

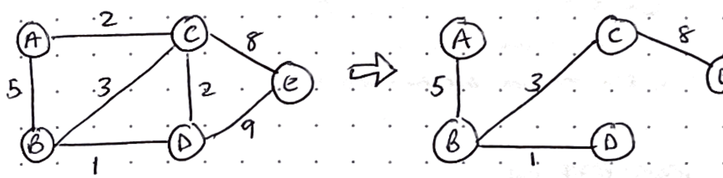
In the above examp. a, b, c, e, f, g are all isomorphic to each other and d, h are also isomorphic to each other.

If we were asked to show the non-isomorphic trees, we would only need to pick one from each set eg



MINIMUM SPANNING TREE

If we have a connected undirected graph with a weight (or cost). The cost of the spanning tree would be the sum of all its edges



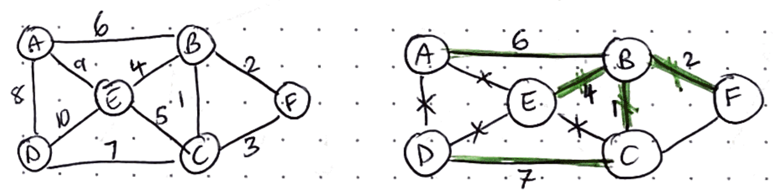
$5+3+1+8$
$= 17$

MINIMUM COST SPANNING TREE is the spanning tree for G that has the minimum cost.

There are two basic algorithms for finding this tree

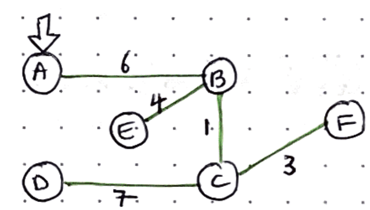
KRUSKAL ALGO

- → Start with the cheapest edge
- → Repeatedly add the cheapest edge that does not create a cycle



PRIMS ALGO

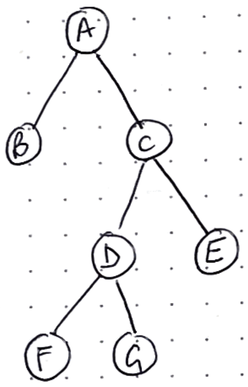
- → Pick a node at random
- → branch out selecting the smallest cost



Rooted Trees

A rooted tree is a directed tree with one vertex distinguished as a root and every vertex has a directed path to that root

Only one vertex must have IN-DEGREE of 0 and all others must have an indegree of 1



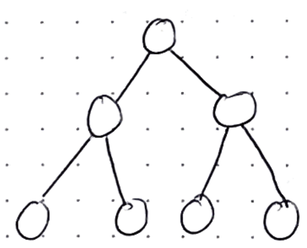
A → Root of the tree
C → is the parent of D & E
F & G → are the children of D
C & A → are ancestors of F & G
F & G → are siblings
C & D → are internal nodes

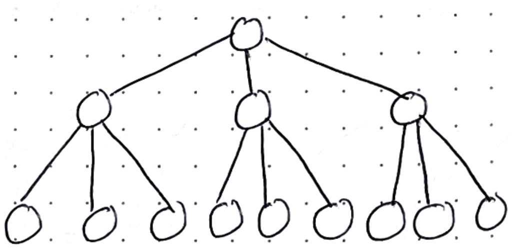
DEPTH or height is the number of edges to the specified node. G = depth of 3. The height is the same but from the bottom
eg. B = height 0, C = height 2.

The depth or height of the tree is the longest path across all its nodes.

BINARY TREE
Every vertex has 2 or fewer children.

TERNARY TREE
Every vertex has 3 or fewer children





M-ARY TREE has m or fewer children per node. It is regular if all internal nodes have exactly m children

Two trees with different degree sequences are not isomorphic

$T_1 \cong T_2$ is the notation for showing T_1 and T_2 are isomorphic.

Binary Search Trees

A binary search tree is a rooted binary tree whose internal nodes stores keys and sometimes an associated value. It also satisfies the requirements of each key in each node must be less than or equal to the node on the right of the subtree and vice versa for the left.

APPLICATIONS → binary search trees are good data stores for modifiable data. It allows for fast insertion, deletion and searching

HEIGHT OF A TREE → can be found two ways

$$\log_2 \text{ inequality} \Rightarrow 2^{h-1} < n+1 \leq 2^h$$
$$h-1 < \log_2(n+1) \leq h$$

$$\text{or ceiling function} \Rightarrow h = \lceil \log_2(n+1) \rceil$$

Both will give the same result and are equivalent.

BINARY SEARCH ALGO. → works by splitting the list into 2 and discarding the bit that isn't relevant and repeat until list is empty or item is found.

RELATIONS

A binary relation over two sets A and B is a subset of the cartesian product $A \times B$. We say $a \in A$ is related to $b \in B$ if and only if (a, b) belongs to the set $A \times B$.

In maths we study relationships such as
→ the relationship of a positive integer and the one it divides.
→ Relation between real number and one larger than it

Relation vs Function

A relation can be defined between elements of a set and elements of another set. We also refer to a relation using R.

example, we have set A and set B, $x \in A$ and $y \in B$, then we would write the relation as xRy

If x is a SON OF person y, then SON OF is the relationship that links them
xRy = x is a SON OF y $x \not R x$ = x is NOT the SON OF x

If we have two sets of the below:

$$A = \{3, 2, 1\} \text{ and } B = \{6, 4, 2\}$$

Then the cartesian product $A \times B$ becomes:

$$A \times B = \{(1,2), (1,4), (1,6), (2,6), (2,4), (2,2), (3,2), (3,4), (3,6)\}$$

Formally: $R \subseteq A \times B$ where R is the set of ordered pairs (a,b) where $a \in A$ and $b \in B$. $(a,b) \in R$ means aRb

When $A = B$, we get a relation $R \subseteq A \times A$

EXAMPLE $A = \{1, 2, 3, 4\}$ Let R be a relation on A.

$$x, y \in A, \ xRy \text{ if and only if } x < y$$

$$R = \{(1,2), (1,3), (1,4), (2,3), (2,4), (3,4)\}$$

Matrix and Graphs for relations

A matrix representation is fairly straightforward:

$A = \{$Sofia, Samir, sarah$\}$
$B = \{$maths, art, english, PE$\}$

	maths	art	english	PE
Sofia	X	X		
Samir		X	X	
Sarah	X		X	

$$\Rightarrow \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

COMBINING RELATIONS → The union of two relations is the same as the union of two sets:

$$M_R \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \quad M_S \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad M_{R \cup S} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$$

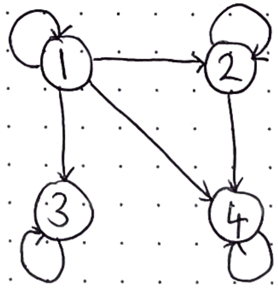
The intersection is also the same as for two sets, using M_R and M_S above, you get:

$$M_{R \cap S} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

When doing the process for graphs you follow these steps

→ list all the elements of A
→ if $(a, b) \in R$ a directed edge is drawn

example. $A = \{1, 2, 3, 4\}$, let $R = \{(x, y) \mid x \mid y\}$



Relation Properties

A realion R in a set S is said to be reflexive if and only if $x R x, \forall x \in S$. Or (x, x) is an element of R.

Example $R = \{(a,b) \in \mathbb{Z}^2 \mid a \leq b\}$

This is easy to show as if we take any element in $\mathbb{Z}$ we can show that $x \leq x$, which means $x R x$, hence $(x, x) \in R$.

This IMPLIES the relation R is refexeve however we can also say it is not refleswe seice $x \nless x$ hence $x \not R x$

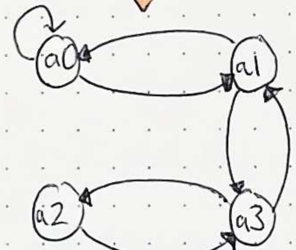
MATRIX OF A REFLEXIVER RELATION

→ all elemenb of the diagonal will be 1

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

A relation R is symmetric if and only if $\forall a, b \in S$, $aRb \rightarrow bRa$

Digraph of a symmetric relation

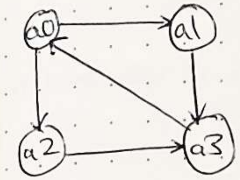


The matrix in hun is also symetric

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

Anti-symetric relations are if and only if $\forall a, b \in S$, $(aRb \land bRa) \rightarrow a = b$

The digraph of an anti symetric relation will have no parallel edges between vertices



The matrix will show that if $i \neq j$ and $m_{ij} \neq 0$ then $m_{ji} = 0$

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

Relation Properties

TRANSIVITY if and only if $\forall a, b, c \in S$ $(aRb \land bRc) \rightarrow aRc$

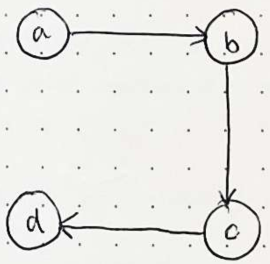
for example $R = \{(x,y) \in \mathbb{N}^2 \mid x \leq y\}$

Transcotive as if $x \leq y$ and $y \leq z$ the $x \leq z$

$R = \{(2,3), (3,2), (2,2)\}$

Not transestive $3R2$ and $2R3$ but not $3 \not R 3$

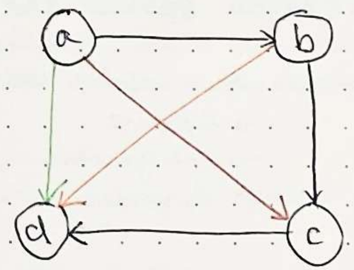
TRANSISTIVE CLOSURE OF A RELATION, what is the minimum number to make the below transitive.



if aRb and bRc then aRc

if bRc and cRd the bRd

if aRb and bRc and cRd then aRd



Equivalence Relations and Classes

Equivalence relations are relations that are reflexive, symmetric and transistive.

Example $R = \{(a,b) \in \mathbb{Z}^2 \mid a \bmod 2 = b \bmod 2\}$

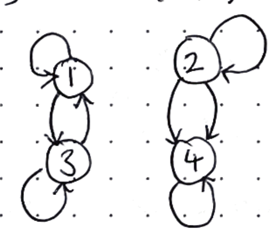
REFLEXIVE $aRa,\ \forall a \in \mathbb{Z}$
SYMMETRIC $\forall a,b \in \mathbb{Z}\ aRb \rightarrow bRa$
TRANSISTIVE $\forall a,b,c \in \mathbb{Z}\ (aRb \wedge bRc) \rightarrow aRc$

$\therefore$ R is an equivalence relation.

EQUIVALENCE CLASS an equivalence class is a subset of a set S such that equivalent elements are part of that subset
In other words if the elements of S have an equivalence relation between them then we can split S into classes in which a and b belong to the same subset only if a and b are equivalent

Example $S = \{1,2,3,4\}$ and $R = \{(a,b) \in S^2 \mid a \bmod 2 = b \bmod 2\}$

Matrix $R = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$



The two equivalence classes are

$\{1,3\}$ and $\{2,4\}$

PARTIAL AND TOTAL ORDER

A partial order is a relation that is

→ Reflexive
→ Antisymmetric
→ Transistive

For example $R = \{(a,b) \in \mathbb{Z}^2 \mid a \leq b\}$ this relation is

REFLEXIVE $\forall a \in \mathbb{Z}\ a \leq a$
TRANSISTIVE $\forall a,b,c \in \mathbb{Z}\ (a \leq b \wedge b \leq c) \rightarrow a \leq c$
ANTISYMMETRIC $\forall a,b \in \mathbb{Z}\ (a \leq b \wedge b \leq a) \rightarrow a = b$

$\therefore$ R is a partial order

A total order is a relation that is
→ a partial order
→ $\forall (a,b) \in S\ (aRb \vee bRa)$
↳ all elements that are pairs must be comparable in respect to R

For example $R = \{(a,b) \in \mathbb{Z}^2 \mid a \leq b\}$

PARTIAL ORDER as shown above
$\forall (a,b) \in S\ (aRb \vee bRa)$

BASICS OF COUNTING

Combinatorics is a branch of discrete maths concerned with the study of finite or countable discrete structures, it studies collections or arrangements of objects.

PRODUCT RULE where the tasks are indendent of each other and task 1 has n possible ways of doing it and task 2 has m possible ways of doing it. This means there are $n \times m$ ways of completing both tasks

ADDITION RULE the total number of ways each task can be completed (NOTE not total number of combinations) assuming both tasks are independent is $n + m$

Example a university must choose a student or faculty to represent them

There are 77 students and 10 faculty = 87 ways to choose a representative.

Example 2 - a label in a programming language can be either a single letter or a letter followed by 2 digits

A single letter can be selected from 26 letters of the alphabet

A letter 26 followed by 2 digits 10×10 has $26 \times 10 \times 10$ combinations

$\therefore$ The total is $26 \times 10 \times 10 + 26 = 2626$

SUBTRACTION RULE
If there are n number of ways to do task 1 and m number of ways to do task 2, and they share o common ways; Then the total number of combinations is $n \times m - o$. $|A \cup B| = |A| + |B| - |A \cap B|$

DIVISION RULE
If a task can be done n ways, and for every way n can be done there is another way that is the same the the task can be done in n/d ways

Example you have 4 red bricks and 2 white. How many ways can you arrange these bricks.

There are $6!$ combinations, but of those there are $4!$ ways to arrange a red brick an $2!$ a white. eg. white white red is the same as white white red. Therefore there are $6!/(4!2!)$ combinations

COMBINATION - R unordered selection or r elements

PERMUTATION - R ordered selection of r elements

	Ordered Permutations	Unordered Combo
Repetition Not	$n!/(n-k)!$	$n!/k!(n-k)!$
Repetition allow	n^k	$(n+k-1)!/(k!(n-1)!)$

Binomial Coefficients

A binomial expression is one that consists of two terms connected by + or − for example $x + a$ or $3x - 2y$

The complexity of expanded binomial expressions grows with the power:

$$(x+y)^1 = x+y$$
$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$
$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

The binomial theorem states if x and y are variables and n a non negative integer, the expansion of $(x+y)^n$ can be formalised as

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

Example, what is the coefficent of x^8y^7 in the expansion of $(3x-y)^{15}$?

We can rewrite this to become $(3x+(-y))^{15}$ and then substitute it in:

$$(3x+(-y))^n = \sum_{k=0}^{15} \binom{15}{k} (3x)^k (-y)^{15-k}$$

We set k to 8 (so x^8) and get

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

$$= \binom{15}{8} 3^8 (-1)^{15-8} \qquad [-1^7 = -1]$$

$$= \binom{15}{8} (-3)^8$$

$$= \frac{15!}{8!7!} \times -3^8$$

Pascals Identity

Pascals identity helps us simplify complicated binomial coefficients. It states that for positive natural numbers n and k

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

Proof, let $|T| = n+1$, $a \in T$ and $S = T - \{a\}$

There are $\binom{n+1}{k}$ subsets of T containing k elements. Each subset either

- ★ contains a with another k-1 elements
- ★ contains k elements of S and not a

Hence there are $\binom{n}{k-1}$ subsets of k elements containing a and $\binom{n}{k}$ subsets of k elements of T that don't contain a.

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

PASCALS TRIANGLE

using pascals identity, we can organise binomial coefficients in a triangular shape called Pascals Triangle.

In this triangle the element $a_{n,r}$ is the binomial coefficient $\binom{n}{r}$

(0, 0) ← n = 0

(1, 0) (1, 1) ← n = 1

(2, 0) (2, 1) (2, 2) ← n = 2

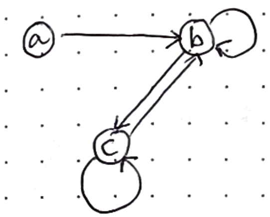
(3, 0) (3, 1) (3, 2) (3, 3) ← n = 3

PROBLEM SHEETS

RELATIONS

Let $S = \{a, b, c\}$ and $A = \{(c, c), (a, b), (b, b), (b, c), (c, b)\}$

Draw the relationship digraph:



The relation is not reflexive, what pair needs to be added.

For the relation to be reflexive it needs each element to have a relation to itself. (aka each element in S needs to have a loop

$\boxed{(a, a)}$

The relation is not symmetric what needs to be added so it is?

For the relation to be symmetric if there exists a relation aRb then there exists a relationship bRa.

$\boxed{(b, a)}$

The relation is not transitive what must be added so it is?

A relation is transitive if aRb and bRc then there must be aRc

$\boxed{(a, c)}$

The relation is not anti-symmetric what should be removed so it is.

A relation is anti-symmetric if there are no parallel lines on the digraph. Aka if aRb and bRa then a = b.

$\boxed{(b, c) \text{ or } (c, b)}$

The following relations are defined on a set $S = \{a, b, c\}$

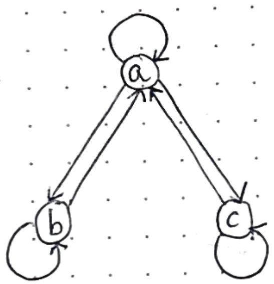
$R_1 = \{(a,a), (a,b), (a,c), (b,a), (b,b), (c,a), (c,c)\}$

$R_2 = \{(a,a), (a,b), (b,a), (b,b), (c,c)\}$

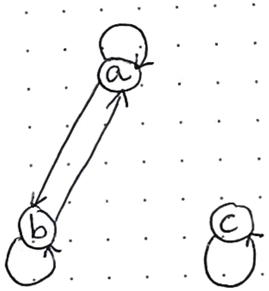
$R_3 = \{(a,b), (a,c), (b,a), (b,c), (c,a), (c,b)\}$

$R_4 = \{(a,a), (a,b), (a,c), (b,b), (b,c), (c,c)\}$

$R_1 =$

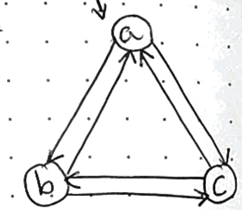


$R_2 =$

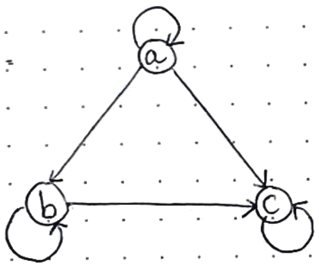


$R_3 =$

It must have loops to be transitive



$R_4 =$



	Reflexive	Symmetric	AntiSym	Trans	Equiv
R_1	1	1	0	0	0
R_2	1	1	0	1	1
R_3	0	1	0	0	0
R_4	1	0	1	1	0

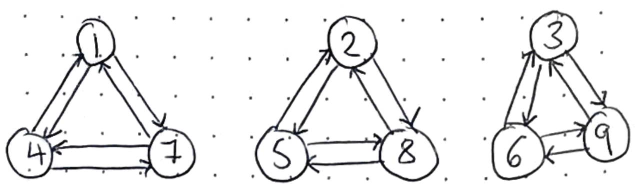
Let $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and let P be the partition on S given by

$\{\{1,4,7\}, \{2,5,8\}, \{3,6,9\}\}$

What two conditions are needed for P to be a partition?

- ★ All elements in S must be present
- ★ Each element must only appear once

Draw the digraphs



Write down the equivalence class $[5]$ as a set $= \{2, 5, 8\}$

Let $S = \mathbb{Z} \times \mathbb{N}^+$ and let R be relation on S defined as follows:
$(a,b) \, R \, (c,d)$ whenever $ad = bc$

Show the R is an equivalence relation →

An equivalence relation is one that is reflexive, symmetric and transitive.

⇨ A relation is reflexive if $(a,b) R (a,b)$ this is clearly true as $ab = ba$

⇨ the relation is symmetric as if a path exists for $(a,b) R (c,d)$ then there must equal a path for $(c,d) R (a,b)$ once:

$(ad = bc) \Rightarrow (cb = da) \Rightarrow (c,d) R (a,b)$

⇨ the relation is transitive as $\forall (a,b), (c,d) (e,f) \in S$. $(a,b) R (c,d)$ and $(c,d) R (e,f)$

List the ordered pairs in the 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) $a = b$ ANSWER ~~$\{0,1,2,3\}$~~ $\{(0,0), (1,1), (2,2), (3,3)\}$

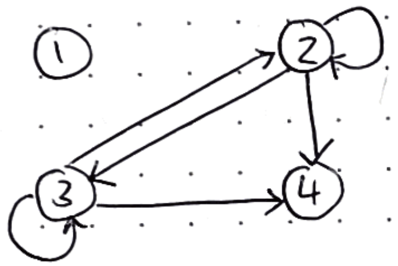
b) $a + b = 4$ ANSWER $\{(1,3), (2,2), (3,1), (4,0)\}$

c) $a > b$ ANSWER $\{(1,0), (2,0), (2,1), (3,2), (3,1), (3,0), (4,3), (4,2), (4,1), (4,0)\}$

d) $a \mid b$ ANSWER $\{(1,0), (1,1), (1,2), (1,3), (2,2), (3,3)\}$

Let $S = \{1,2,3,4\}$, state if the following are reflexive, symmetric, antisymmetric or transitive.

$a = \{(2,2), (2,3), (2,4), (3,2), (3,3), (3,4)\}$



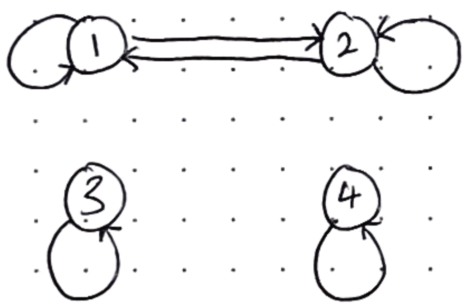
★ For reflexivity all must have a loop 1, 4 do not. 4R4 NOT REFLEXIVE

★ For it to be symmetric if there exists aRb there must also be bRa. you have (3,4) but not (4,3) NOT SYMETRIC

★ To be antisymmetric you cannot have aRb + here is bRa, (3,2)(2,3) means it is not antisymmetric.

★ If there exists aRb and bRc you must have aRc for it to be transitive this graph satisfies that

$b = \{(1,1), (2,2), (1,2), (2,1), (3,3), (4,4)\}$



★ It is reflexive as $\forall b$. bRb (aka all elements in S have a loop.

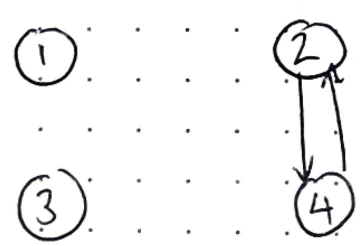
★ It is symmetric as if aRb exists there must also be bRa.

★ It is not antisymmetric as (1,2)(2,1)

★ It is transitive as if aRb and bRc there must be aRc eg

$\{(1,2), (2,1), (1,1)\}$

c) $= \{(2,4), (4,2)\}$



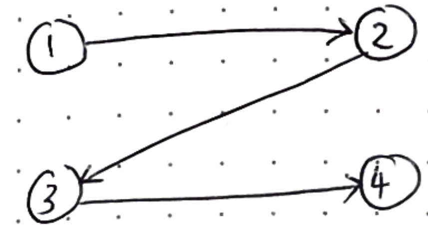
⇨ Not Reflexive

⇨ It is symmetric

⇨ Not Antisymmetric

⇨ Not transitive

$d = \{(1,2), (2,3), (3,4)\}$



⇨ Not symmetric

⇨ Not reflexive

⇨ Is anti symmetric

⇨ Not transitive