MATH255: Mathematics for Computing

Dr Chayne Planiden

School of Mathematics and Statistics
University of Wollongong

April 3, 2024

Definition

*A **linear function** has the form*

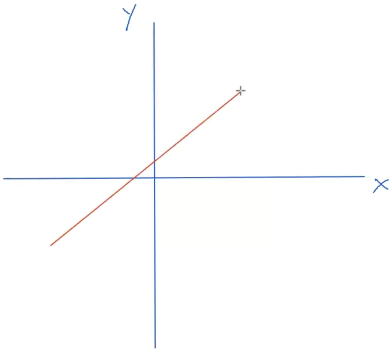
$$f(x) = mx + b,$$

where $m, b \in \mathbb{R}$.

There are several forms of a linear function

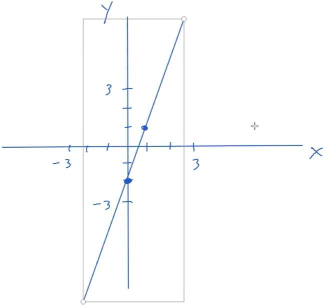
- Standard form: $Ax + By = C$
- Slope-intercept form: $y = mx + b$
- Point-slope form: $y - y_1 = m(x - x_1)$
- Two-point form: $y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$

The graph of a linear function is a straight line.



A common Statistics question is that of the best-fit line through a set of data points; we will see that in later weeks. Linear interpolation and linear programming are other common practical uses.

The slope-intercept form tells you what the slope and the y-intercept of the function are. For example $y = 3x - 2$ has slope 3 and intercept -2, so to draw the graph, put a point at $(0, -2)$ and another at slope 3 (rise/run = 3) from there.



Or you can use a table of values and get points on the same line. Plug in x-values to the function and record the y-values:

x	0	1	10	-5
y	-2	1	28	-17

- The point-slope form uses one point (x_1, y_1) and the slope, so draw the point and find another point using the slope formula rise/run (see video).
- The two-point form gives you the slope indirectly: the rise over the run is $m = \frac{y_2 - y_1}{x_2 - x_1}$.

Solving a system of linear equations means finding the points where all the straight lines intersect.

$$
\begin{aligned}
2x + 3y &= 6 \\
4x + 9y &= 15
\end{aligned}
$$

Elimination method: multiply one equation as needed so that one coefficient matches the other equation, then subtract the equations to cancel that variable.

$$
\begin{array}{r}
-4x - 6y = -12 \\
4x + 9y = 15 \\
\hline
3y = 3
\end{array}
$$

So $y = 1$ and then we find x by substituting that into either of the two equations:

$$2x + 3 \cdot 1 = 6 \rightarrow x = \frac{3}{2}$$

Substitution method: solve one equation for a variable and substitute that into the other equation.

$$2x + 3y = 6 \rightarrow x = \frac{6 - 3y}{2} = 3 - \frac{3}{2}y$$

$$4x + 9y = 15 \rightarrow 4\left(3 - \frac{3}{2}y\right) + 9y = 15 \rightarrow y = 1$$

Definition

A ***polynomial function*** *has the form*

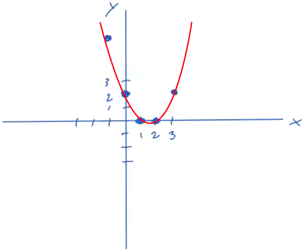
$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0,$$

where $a_i \in \mathbb{R}$.

- $n = 0$: constant function. Eg. $f(x) = 2$
- $n = 1$: linear function. Eg. $g(x) = 4x - 3$
- $n = 2$: quadratic function. Eg. $h(x) = -x^2 + 2x - 1$

The **degree** of a polynomial is the highest power of x (the value of n). Quadratic functions are degree 2, linear functions are degree 1, constant functions are degree 0.

To graph a polynomial function, make a. table of values and plot the points, then join them with a smooth curve.



$$f(x) = x^2 - 3x + 2$$

x	y
0	2
1	0
−1	6
2	0
3	2

Definition

*The **roots** of a function are the points at which the value of the function is zero. Graphically, they are the points at which the graph crosses the x-axis.*

A polynomial of degree n has at most n roots.

Linear: $y = mx + b = 0 \rightarrow mx = -b \rightarrow x = -\frac{b}{m}$ is the root.

Quadratic: $y = ax^2 + bx + c$ has 0, 1 or 2 roots depending on the discriminant $D = b^2 - 4ac$.
$D > 0$: 2 roots.
$D = 0$: 1 root.
$D < 0$: 0 roots.

If a quadratic can be factorised, the linear factors tell you the roots.

$f(x) = 2x^2 - 5x + 3 = (2x - 3)(x - 1) = 0 \to x = \frac{3}{2}; x = 1$ are the roots.

The quadratic formula $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$, which uses the discriminant, tells you the same thing:

$$x = \frac{5 \pm \sqrt{25 - 4 \cdot 2 \cdot 3}}{2 \cdot 2} = \frac{5 \pm \sqrt{1}}{4} = \frac{5 \pm 1}{4} \to x = \frac{3}{2}, x = 1$$

With any degree polynomial, if factorisable, you see the roots from each linear factor.

$$f(x) = (x + 1)(x - 3)(3x + 2) = 0 \to x = -1, x = 3, x = -\frac{2}{3}$$

To answer the question of where a polynomial is positive or negative, use the roots. Between each pair of roots, the function will have the same sign throughout.

$$f(x) = (x+1)(x-3)(3x+2) = 0 \to x = -1, x = 3, x = -\frac{2}{3}$$

Here, you have four regions to test: $(-\infty, -1)$, $\left(-1, -\frac{2}{3}\right)$, $\left(-\frac{2}{3}, 3\right)$ and $(3, \infty)$. Use any test point you want in each region.

$f(-2) = (-2+1)(-2-3)(3(-2)+2) < 0$, so the function is negative on all of $(-\infty, -1)$.

$f\left(-\frac{3}{4}\right) > 0$, so the function is positive on all of $\left(-1, -\frac{2}{3}\right)$.

$f(0) < 0$, so the function is negative on all of $\left(-\frac{2}{3}, 3\right)$.

$f(4) > 0$, so the function is positive on all of $(3, \infty)$.

Factorisation.

$f(x) = 5x^2 - 10x + 25$ Factor out any common terms, such as the 5 here since all coefficients are multiples of 5..

$f(x) = 5(x^2 - 2x + 5)$

$g(x) = x^3 - 3x^2 + 2x$ Factor out an x here.

$g(x) = x(x^2 - 3x + 2)$

If there aren't any common factors, then separate into two linear factors.

$h(x) = x^2 - 5x + 6 = (x - 2)(x - 3)$

See video for details; check your work by FOILing.

Example. $f(x) = 3x^2 - 2x - 1$ The linear factors of x must be $3x$ and x. The factors of the constant -1 must be 1 and -1. So which combination gives the product $-2x$ in the middle?

$$(3x+1)(x-1)$$
$$(3x-1)(x+1)$$

These are the only two possibilities; the first one is correct. Verify this by multiplying the RHS to get the LHS. Example. $f(x) = 3x^2 - 2x - 2$

$$(3x-2)(x+1)$$
$$(3x+1)(x-2)$$
$$(3x+2)(x-1)$$
$$(3x-1)(x+2)$$

These are the only four possibilities; none of them is correct. This function does not factor into integer factors.

Example. $4x^2 - x - 3$ has possible $4x, x$ or $2x, 2x$ factors, so four possibilities. The correct one is $f(x) = (4x + 3)(x - 1)$.

For higher-degree functions, we can't efficiently use this method, so we use long division instead.

Example. Find the factors of $f(x) = x^3 + 4x^2 + x - 6$.

Possible factors are $(x \pm 1), (x \pm 2), (x \pm 3, (x \pm 6)$. Let's try $(x - 1)$.

$$
\begin{array}{r}
x^2 + 5x + 6 \\
x - 1 \overline{\smash{\big)}\, x^3 + 4x^2 \quad + x - 6} \\
\underline{- x^3 \quad + x^2} \qquad\qquad \\
5x^2 \quad + x \quad \\
\underline{- 5x^2 + 5x} \quad \\
6x - 6 \\
\underline{- 6x + 6} \\
0
\end{array}
$$

Since the remainder is zero, $x - 1$ is a factor and the other factor is the top part, $x^2 + 5x + 6$.

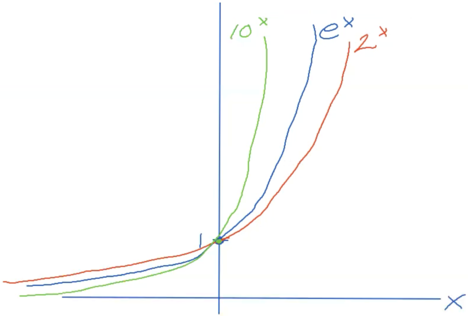
$f(x) = (x - 1)(x^2 + 5x + 6)$

Now factor the quadratic and find the final answer.

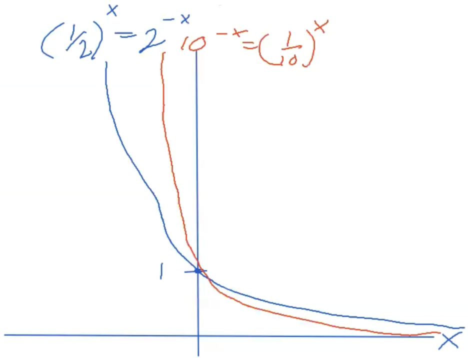
$f(x) = (x - 1)(x + 2)(x + 3)$

Exponential Functions. $f(x) = ab^x, a \in \mathbb{R}, b > 0.$

- Exponential functions grow faster than polynomial functions.
- They are commonly used in questions of growth/decay of a substance or a population and in financial applications.
- If $a > 0$, then $ab^x > 0 \; \forall \; x$.



If $b < 1$, then the curve faces the other way.



Example. The population of a town grows at rate $P(t) = 12500(1.02)^t$, t in years. What is the starting population and what will it be in six years?

Answer. The starting population is at $t = 0$.

$P(0) = 12500(1.02)^0 = 12500$

After 6 years ($t = 6$):

$P(6) = 12500(1.02)^6 \approx 14077$

Example. A bacterial culture grows 9% per day. Today there are 23900 bacteria. What is the equation that describes the growth? What will be the population a week from now?

Answer. $P(t) = 23900(1.09)^t$, t in days.

$P(7) = 23900(1.09)^7 \approx 43690$

Example. A car worth \$38,000 5 years ago is worth \$11,000 now. What will it be worth 4 years from now?

Answer. $V(t) = 38000b^t$, t in years and we have to find b.

$$V(0) = 38000$$
$$V(5) = 38000b^5 = 11000$$
$$\rightarrow b^5 = \frac{11000}{38000} \rightarrow b = \sqrt[5]{\frac{11}{38}} \approx 0.78$$

$V(9) = 38000(0.78)^9 \approx 4061$

Example. You deposit \$6500 in an investment account that pays 3.6% compounded semiannually. What is it worth in 20 years? Compounded weekly, what would it be worth in 20 years?

Answer. The compound interest formula is $A(t) = P\left(1 + \frac{r}{n}\right)^{nt}$, where A is the new amount, P is the principal (initial investment), r is the interest rate, t is the total investment time in years and n is the number of times compounded per year.

$$A(20) = 6500\left(1 + \frac{0.036}{2}\right)^{2\cdot 20} \approx 13268.58 \qquad \text{(semiannually)}$$

$$A(20) = 6500\left(1 + \frac{0.036}{52}\right)^{52\cdot 20} \approx 13350.49 \qquad \text{(weekly)}$$

MATH255: Mathematics for Computing

Dr Chayne Planiden

School of Mathematics and Statistics
University of Wollongong

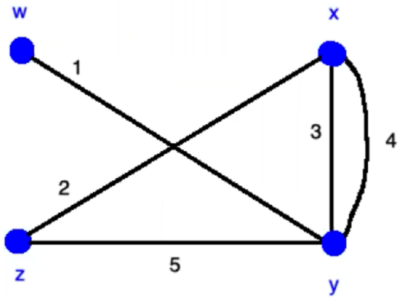
March 1, 2024

Definition

*A **graph** consists of two finite sets: a nonempty set V of vertices and a set E of edges, where each edge is associated to a subset of V of either 1 or 2 vertices, called the endpoints of the edge.*

- An edge with only one endpoint is a **loop**.
- Two or more edges with the same endpoints are **parallel edges**.
- An edge is said to *connect* its endpoints and be *incident* on each endpoint.
- A vertex on which no edge is incident is *isolated*.
- Two vertices connected by an edge are *adjacent*.

Example. Write down V and E for the following graph. List any loops and parallel edges.



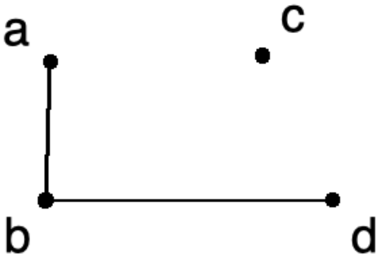
$$V = \{w, x, y, z\}$$
$$E = \{1, 2, 3, 4, 5\} = \{wy, xz, xy_1, xy_2, yz\}$$

Exercise. Draw a graph that has 5 vertices including 1 isolated, 1 loop and 1 pair of parallel edges. Write down V and E.

Definition

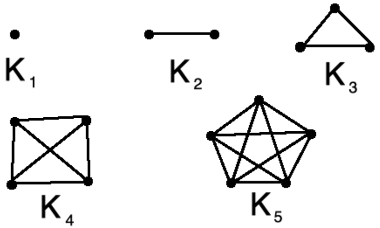
*A **simple graph** is a graph that does not have loops nor parallel edges.*

Example. Draw a simple graph with $V = \{a, b, c, d\}$ and 2 edges, one of which has endpoints b and d.



Definition

*A **complete graph** of n vertices, denoted by K_n, is a simple graph with n vertices, whose edge set contains one edge for every pair of distinct vertices.*



Definition

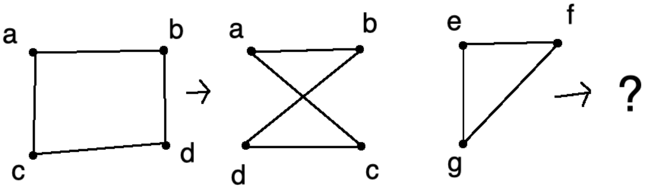
A simple graph is ***bipartite*** *if there exist* $U \subseteq V$ *and* $W \subseteq V$ *such that*

(a) $U \cup W = V$ *and* $U \cap W = \varnothing$;

(b) *every edge connects a vertex of* U *with a vertex of* W.

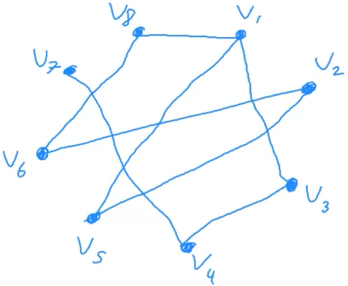
A bipartite graph can be rearranged if necessary so that every edge goes from one subset of V to the other; there can be no edge incident one two vertices in the same subset.

Example. Which are bipartite?



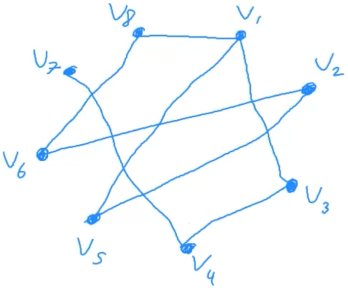
The square in original form doesn't appear to be bipartite, but with $U = \{a, d\}$ and $V = \{b, c\}$, it becomes apparent. However, the triangle is not bipartite, as there is no way to subdivide V appropriately.

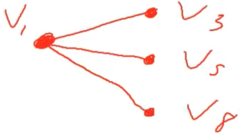
To determine if a graph is bipartite, put one vertex in U and all adjacent ones in V, then all adjacent to those ones in U, etc. If successful with all vertices, the graph is bipartite.



Graph Theory

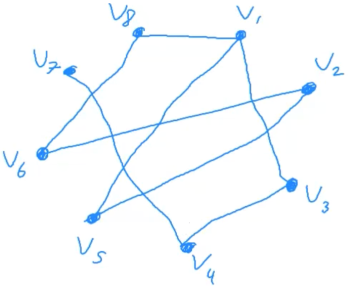
To determine if a graph is bipartite, put one vertex in U and all adjacent ones in V, then all adjacent to those ones in U, etc. If successful with all vertices, the graph is bipartite.

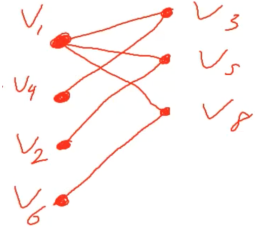




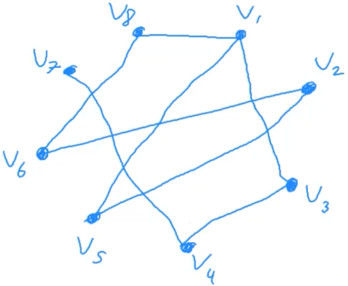
Graph Theory

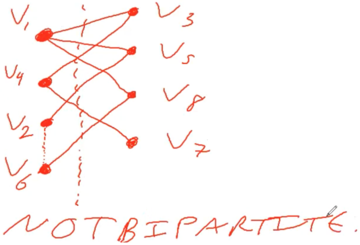
To determine if a graph is bipartite, put one vertex in U and all adjacent ones in V, then all adjacent to those ones in U, etc. If successful with all vertices, the graph is bipartite.





To determine if a graph is bipartite, put one vertex in U and all adjacent ones in V, then all adjacent to those ones in U, etc. If successful with all vertices, the graph is bipartite.



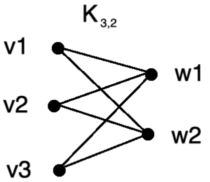


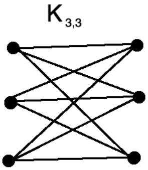
Definition

*A **complete bipartite graph** on (m, n) vertices, denoted by $K_{m,n}$, is a simple graph with $V = \{v_1, \ldots, v_m, w_1, \ldots, w_n\}$ such that for all $1 \leq i, k \leq m$ and all $1 \leq j, l \leq n$ we have*

1. *an edge from each v_i to each w_j;*
2. *no edge from any v_i to any v_k;*
3. *no edge from any w_j to any w_l.*

Example. Draw $K_{3,2}$ and $K_{3,3}$.

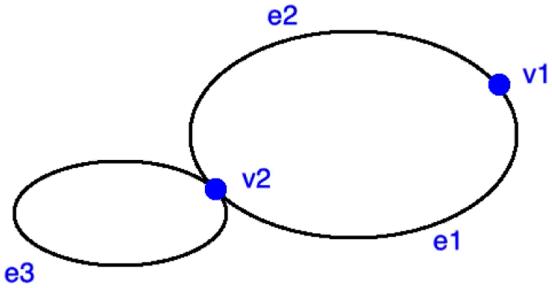




Definition

A graph H is a ***subgraph*** *of a graph G if every vertex in H is in G and every edge in H is in G.*

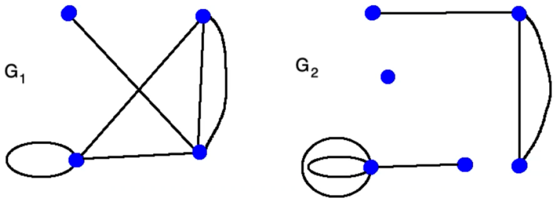
Exercise. Draw all the subgraphs of the graph below. There are 3 subgraphs with just one vertex and 8 subgraphs with both vertices.



Definition

Let $G = (V, E)$ be a graph, $v \in V$. The ***degree*** *of v, denoted by $\delta(v)$, is the number of edges incident on v (with loops counted twice). The degree of G is the sum of degrees of all $v \in V$.*

Example. Find the degrees of G_1 and G_2.



Note G_1 has vertices of degrees $\delta(v_1) = 1, \delta(v_2) = 3, \delta(v_3) = 4$ and $\delta(v_4) = 4$, so $\delta(G_1) = 12$.

Exercise. Draw graphs with $|V| = 4$ and vertices of degrees

- $1, 1, 3, 3$;
- $1, 1, 2, 3$.

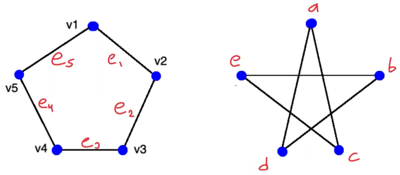
Theorem (The Handshake Theorem)

The degree of a graph is twice the number of its edges.

This holds because each edge has 2 endpoints. So the degree of a graph is always even. A graph with 4 vertices of degrees $1, 1, 2, 3$ is impossible.

Isomorphism

Is there a difference between these two graphs?

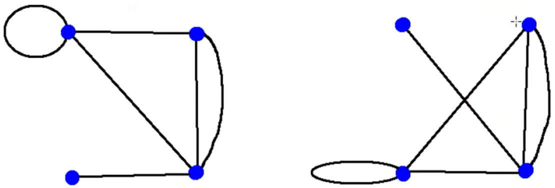


Definition

*Let $G = (V, E), G' = (V', E')$ be graphs. If there exist bijective functions $f : V \to V', h : E \to E'$ that preserve adjacency, then G and G' are **isomorphic** to each other.*

We can see that with the bijections
$f : \{(v1, a), (v2, c), (v3, e), (v4, b), (v5, d)\}$ and
$h : \{(e_1, ac), (e_2, ce), (e_3, eb), (e_4, bd), (e_5, da)\}$, the two graphs above are isomorphic.

Exercise. Show that the two graphs below are isomorphic by labelling edges and vertices appropriately.

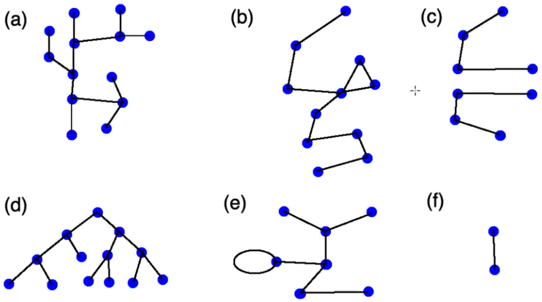


Exercise. Draw all possible graphs (up to isomorphism) with $|V| = |E| = 2$. Hint: there are four of them.

Definition

*A graph is a **tree** if it is connected and has no simple circuits nor loops.*

Exercise. Which are trees?



Theorem

For any $n \in \mathbb{N}$, a tree with n vertices has $n-1$ edges.

Theorem

For any $n \in \mathbb{N}$, if G is a connected graph with $|V| = n$ and $|E| = n-1$, then G is a tree.

Exercise.

(a) Draw a tree with 5 vertices and 4 edges.

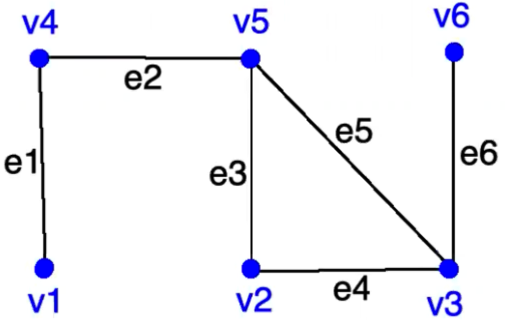
(b) Draw a graph with 5 vertices and 4 edges that is not a tree.

Definition

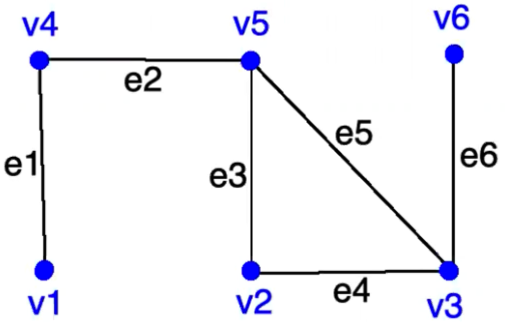
*A **spanning tree** of G is a subgraph that contains every vertex of G and is a tree.*

- Every connected graph has a spanning tree.
- Any two spanning trees of a graph have the same number of edges.

Exercise. Find all spanning trees of the graph below.



Exercise. Let the edges represent telephone lines, the numbers represent the cost of installation in thousands of dollars. Determine the minimum cost of installing the network.



Definition

*A **weighted graph** is a graph in which each edge has an associated positive weight. The sum of all edge weights is the **weight** of the graph.*

Definition

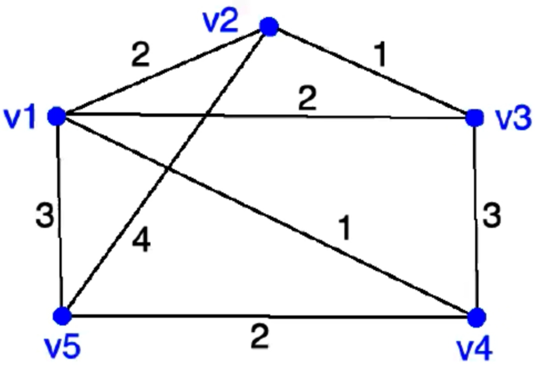
*A **minimum spanning tree (MST)** of a connected, weighted graph is a spanning tree that has the least possible weight.*

Minimum spanning trees are not necessarily unique, but all MSTs of a graph have the same number of edges and the same weight. We use $w(e)$ and $w(G)$ for the weights of edge e and graph G.

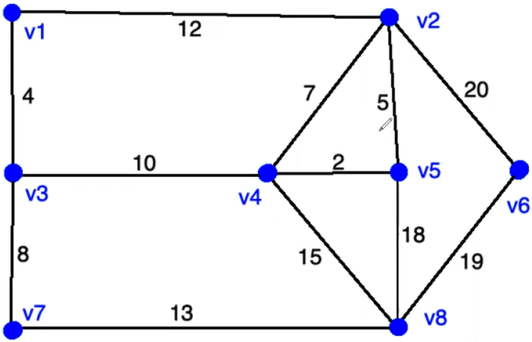
Kruskal's Algorithm

One method of finding an MST is to insert edges one-by-one into the subgraph in increasing order of weight, not allowing any circuits to form. This is Kruskal's algorithm.

Exercise. Use Kruskal's algorithm to find an MST.



Exercise. Use Kruskal's algorithm to find an MST.



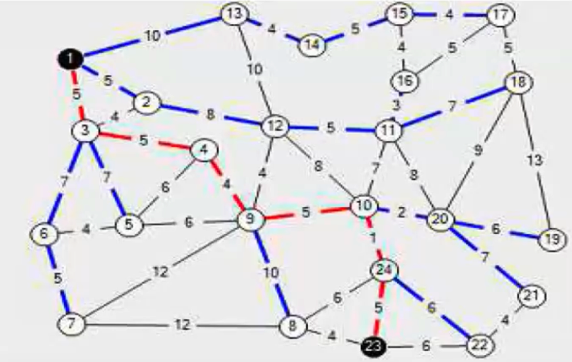
Prim's Algorithm

Another manner of building an MST is by inserting vertices one-by-one and then adding the edge to each new vertex that (1) increases the subgraph weight minimally and (2) does not create a circuit.

Exercise. Repeat the previous two exercises using Prim's algorithm.

Dijkstra's Algorithm

Finding the shortest path through a graph is an important aspect of graph theory. There are many methods; we will learn Dijkstra's method.



We keep track of the following at every iteration.

- The set of nodes not yet processed: U.
- The sets of predecessor nodes and successor nodes of Node k: $P(k)$ and $S(k)$.
- The length of the (partial) shortest path from the source node to the current Node k: $F(k)$.
- The distance between Nodes k and j: $D(k, j)$.

Initialise. $k = 1$; $F(1) = 0$; $F(j) = \infty, j = 2, \ldots, n$; $U = \{1, \ldots, n\}$; $P(k) = \varnothing$.

WHILE $k \neq n$ AND $F(k) < \infty$

$U = U \setminus \{k\}$

FORALL $j \in U \cap S(k)$

IF $F(j) > D(k,j) + F(k)$

$F(j) = D(k,j) + F(k)$

$P(j) = k$

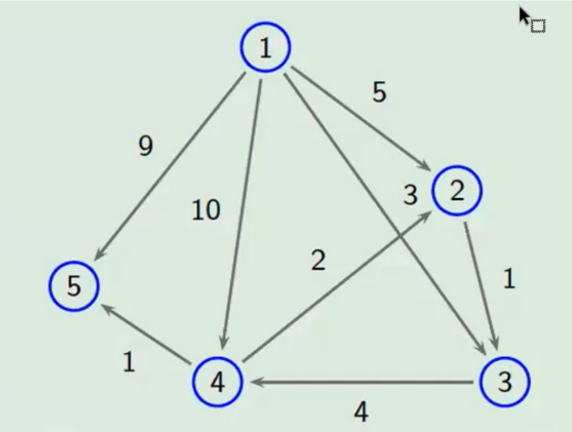
END

END

$k =$ index of $\min\{F(j) : j \in U\}$

END

Consider the following directed network with source node 1 and sink node 5. Determine the shortest path using Dijkstra's algorithm.



First iteration: the source node goes in the first row and all the weights from there to the other nodes go in the row, with subscript '1' to say that the predecessor is Node 1. If you can't get to a node from Node 1, that weight is infinite.

	1	2	3	4	5
1	0_1	5_1	3_1	10_1	9_1

Every iteration, there will be a node whose weight will no longer change; that's the one you put in the first column of each row. Mark that weight with a different colour, underline, etc.

Now look at the non-permanent weights; what is the smallest one? It's weight 3, Node 3. So Node 3 is the next permanent one and it goes in the header of Row 2.

Then look where you can go from the new node that would be an improvement over the current path to all other nodes. From 3, we can get to 4 at an overall lower cost, so we replace the weight of 4: 10_1 changes to 7_3 because going $1 \to 3 \to 4$ only weight 7 in total, rather than $1 \to 4$ with weight 10.

	1	2	3	4	5
1	0_1	5_1	3_1	10_1	9_1
3	0_1	5_1	3_1	7_3	9_1

Then repeat; what is the lowest non-permanent weight now? It's 5, Node 2. Node 2 is the head of the next row. Note. If there are more than one with the same weight, you can choose any one.

	1	2	3	4	5
1	0_1	5_1	3_1	10_1	9_1
3	0_1	5_1	3_1	7_3	9_1
2	0_1	5_1	3_1	7_3	9_1

From 2, we cannot get to anywhere else more efficiently than we already have, so no other weights changed that time. Now repeat; the next lowest weight is 7, so Node 4 forms the next row.

	1	2	3	4	5
1	0_1	5_1	3_1	10_1	9_1
3	0_1	5_1	3_1	7_3	9_1
2	0_1	5_1	3_1	7_3	9_1
4	0_1	5_1	3_1	7_3	8_4

Weight 8 through Node 4 is better than 9 through Node 1, so change it. Finally, Node 5 is last and forms the last row.

	1	2	3	4	5
1	0_1	5_1	3_1	10_1	9_1
3	0_1	5_1	3_1	7_3	9_1
2	0_1	5_1	3_1	7_3	9_1
4	0_1	5_1	3_1	7_3	8_4

Backtrack through the subindices to find the path: to get to 5 we went through 4 (8_4), to get to 4 we went through 3 (7_3) and to get to 3 we went through 1 (3_1), so the shortest path is

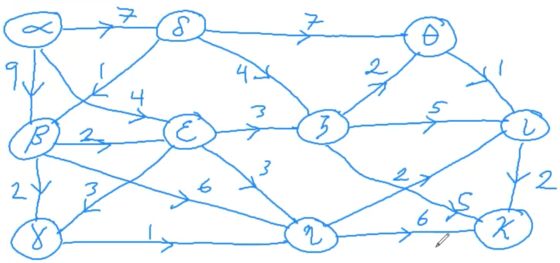
$$1 \to 3 \to 4 \to 5$$

with total cost 8.

Note. The algorithm actually gives you all the shortest paths from the source node to ALL other nodes. The bottom row gives:

Sink	Path	Weight
1	$1 \to 1$	0
2	$1 \to 2$	5
3	$1 \to 3$	3
4	$1 \to 3 \to 4$	7
5	$1 \to 3 \to 4 \to 5$	8

Here is a bigger example, ten nodes alpha through kappa.



Graph Theory

If α is the source, then α heads Row 1.

	α	β	γ	δ	ε	ζ	η	θ	ι	κ
α	0	9_α	∞	7_α	4_α	∞	∞	∞	∞	∞

The smallest weight is 4, Node ε, so Row 2:

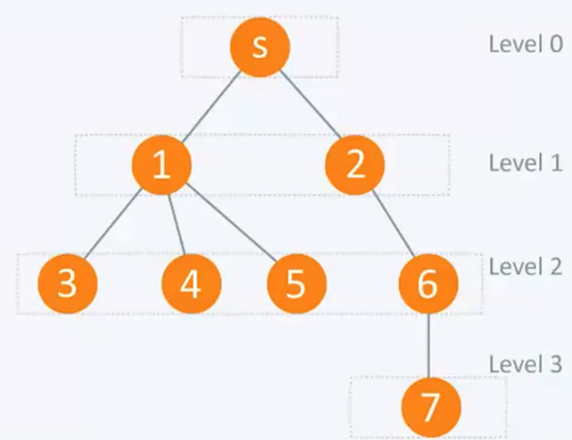
	α	β	γ	δ	ε	ζ	η	θ	ι	κ
α	0	9_α	∞	7_α	4_α	∞	∞	∞	∞	∞
ε	0	9_α	7_ε	7_α	4_α	7_ε	7_ε	∞	∞	∞

Continuing in this manner (do it yourself!) we get the answer:

	α	β	γ	δ	ε	ζ	η	θ	ι	κ
α	0	9_α	∞	7_α	4_α	∞	∞	∞	∞	∞
ε	0	9_α	7_ε	7_α	4_α	7_ε	7_ε	∞	∞	∞
γ	0	9_α	7_ε	7_α	4_α	7_ε	7_ε	∞	∞	∞
δ	0	8_δ	7_ε	7_α	4_α	7_ε	7_ε	14_δ	∞	∞
ζ	0	8_δ	7_ε	7_α	4_α	7_ε	7_ε	9_ζ	12_ζ	12_ζ
η	0	8_δ	7_ε	7_α	4_α	7_ε	7_ε	9_ζ	9_η	12_ζ
β	0	8_δ	7_ε	7_α	4_α	7_ε	7_ε	9_ζ	9_η	12_ζ
θ	0	8_δ	7_ε	7_α	4_α	7_ε	7_ε	9_ζ	9_η	12_ζ
ι	0	8_δ	7_ε	7_α	4_α	7_ε	7_ε	9_ζ	9_η	11_ι
κ	"	"	"	"	"	"	"	"	"	11_ι

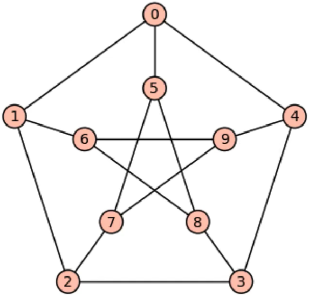
Shortest path is $\alpha \to \varepsilon \to \eta \to \iota \to \kappa$, weight 11.

Breadth-first Search. To find a particular node of a graph, there are two algorithms we will study. The breadth-first search (BFS) searches through the graph level by level, making a tree and scanning it from the top down.



The source node is the root of the tree and all adjacent nodes form the first level. Then each of those are searched and their adjacent nodes form the second level, and so on until the node of interest is found or until the whole graph is searched. The algorithm is 'push and pop', adding unvisited nodes into a queue (pushing) and removing them as they are visited (popping).

```
Input:  s as the source node.
BFS(G,s):  define Q as a queue.
Q.enqueue(s)
Mark s as visited.
While (Q is not empty)
    v = Q.dequeue( )
    For all neighbours w of v in G
        If w is not visited
            Q.enqueue(w)
            Mark w as visited.
```



Let 0 be the source, so push 0.

0									

If it's not what you want, pop it and push all its unvisited neighbours: 1,5 and 4.

0	1	5	4						

Then repeat. If 1 isn't what you want, pop it and push its unvisited neighbours: 6 and 2.

0	1	5	4	6	2				

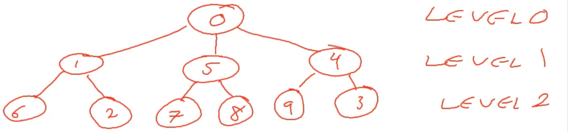
Then 5.

0	1	5	4	6	2	7	8		

Then 4.

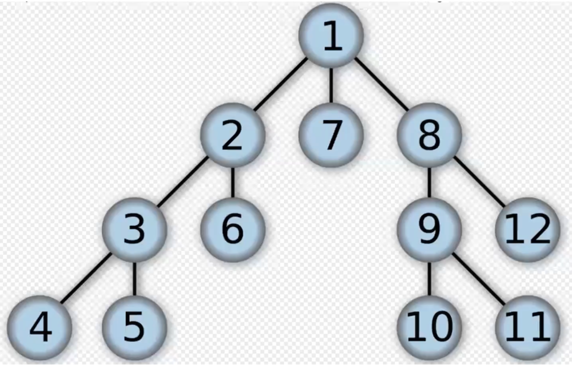
0	1	5	4	6	2	7	8	9	3

Continue from left to right until you find the objective. The inspection tree formed is:



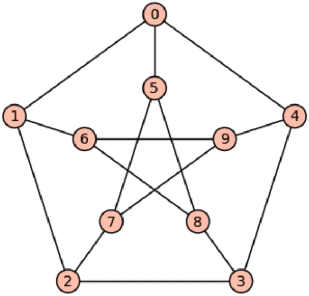
and it is inspected level by level from the top down.

Depth-first Search. The other method we will see is the depth-first search (DFS). It searches from source node to a leaf, then backtracks and goes to the next leaf, etc.



DFS also used push and pop, but it always pops the last node to be pushed.

```
DFS(G,v)
Stack S := { };
Set all nodes as unvisited.
push S, v;
While (S is not empty)
    u := pop S;
    If u is not visited
        Mark u visited;
        Push all unvisited neighbours of u.
```



Let's use source node 8. Push 8.

8									

Then pop it and push its neighbours 5, 6 and 3.

8	5	6	3						

Then 3 is popped next, since it was last to be pushed. Push its unvisited neighbours.

8	5	6	3	4	2				

Continue by popping 2 and pushing its unvisited neighbours.

8	5	6	3	4	2	1	7		

Then pop 7 and push its unvisited neighbours.

8	5	6	3	4	2	1	7	9	

Pop 9. It has no unvisited neighbours, so it's a leaf.

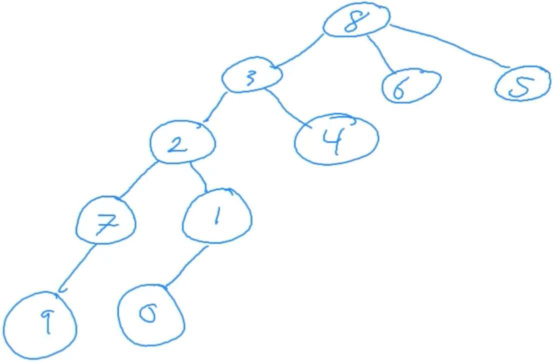
8	5	6	3	4	2	1	7	9	

Backtrack and pop 1, and push neighbour 0.

8	5	6	3	4	2	1	7	9	0

Pop 0, it's another leaf. Backtrack to 4, another leaf. Then 6, leaf. Then 5, leaf and you're done.

The inspection tree is:



and it's inspected one whole branch completely first, root to leaf, then backs up to the next branch and continues until success.

MATH255: Mathematics for Computing

Dr Chayne Planiden

School of Mathematics and Statistics
University of Wollongong

January 17, 2024

Definition

A pair (a, b) *is an* ***ordered pair*** *if it has the property*

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

Definition

The ***Cartesian product*** $A \times B$ *is the set of all ordered pairs with first element from* A *and second element from* B.

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

Example. Let $A = B = \mathbb{R}$. Then $A \times B = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the set of all points in the Cartesian plane.

Example. Let $A = \{3\}, B = \{2, 3\}$. Then $A \times B = \{(3, 2), (3, 3)\}$.

Example. Let $A = \{x, y\}, B = \{1, 2, 3\}, C = \{\alpha, \beta\}$. Then

$A \times B = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$ and

$(A \times B) \times C = \{((x, 1, \alpha), (x, 2, \alpha), (x, 3, \alpha), (y, 1, \alpha), (y, 2, \alpha), (y, 3, \alpha), (x, 1, \beta), (x, 2, \beta), (x, 3, \beta), (y, 1, \beta), (y, 2, \beta), (y, 3, \beta)\}$.

Definition

*A **relation** R from A to B is a subset of $A \times B$ that is defined by some rule that relates elements of A with elements of B. We say that a is related to b, denoted by aRb, if $(a, b) \in R$.*

Example. Let $S = \{0, 1, 2, 3\}, R \subseteq S \times S$:

$R = \{(x, y) : \exists z \in \mathbb{N} \texttt{ s.t. } x + z = y\}$.

(a) What is a simpler description of R?

(b) List all the elements of R.

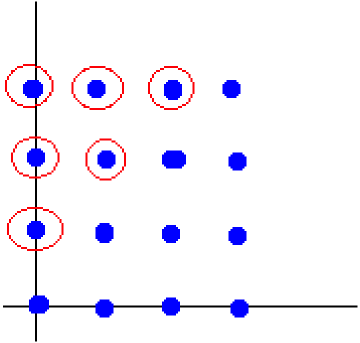
(c) Sketch $S \times S$ and circle the members of R.

(a) Since $x, y \in S$ and $x + z = y$ for some $z \in \mathbb{N}$, R is all pairs (x, y) such that $x < y$.

$$R = \{(x, y) : x < y\}$$

(b) $R = \{(0,1),(0,2),(0,3),(1,2),(1,3),(2,3)\}$

(c)



Example. On $\mathbb{Z}\setminus\{0\}, R = \{(x, y) : \exists\, z \in \mathbb{Z} \text{ s.t. } xz = y\}$

(a) Describe R. (What if $x = \pm 1, x = \pm 2, \ldots$)

(b) True or false: $(2, -4) \in R$, $-3R0, (3, 5) \in R$.

(a) If $x = 1$, then $1 \cdot z = y$, so $(1, \pm 1), (1, \pm 2), \cdots \in R$.
If $x = -1$, then $-1 \cdot z = y$, so $(-1, \pm 1), (-1, \pm 2), \cdots \in R$.
If $x = 2$, then $2 \cdot z = y$, so $(2, \pm 2), (2, \pm 4), \cdots \in R$.
This pattern continues with all choices of x, so
$R = \{(x, y) : y$ is a nonzero multiple of $x\}$.

(b) Since -4 is a nonzero multiple of 2, we have $(2, -4) \in \mathbb{R}$.
Since 0 is not a nonzero multiple of -3, we have
$(-3, 0) \notin R$.
Since 5 is not a nonzero multiple of 3, we have $(3, 5) \notin \mathbb{R}$.

Example. On $\mathbb{Z}$, $R = \{(m, n) : m - n \text{ is even}\}$.

(a) Which are in R? $(0, 3), (-5, -6), (2, -11), (17, 1)$

(b) Prove that n odd $\rightarrow nR1$.

(a) $0 - 3 = -3 \rightarrow (0, 3) \notin R$
$-5 - (-6) = 1 \rightarrow (-5, -6) \notin R$
$2 - (-11) = 13 \rightarrow (2, -11) \notin R$
$17 - 1 = 16 \rightarrow (17, 1) \in R$

(b) Let n be odd. Then $\exists\, k \in \mathbb{Z}$ $\texttt{s.t.}$ $n = 2k + 1$. Is $nR1$?

$$n - 1 = (2k + 1) - 1 = 2k, k \in \mathbb{Z} \rightarrow nR1.$$

Relations are sets, so all the set operators seen so far can be applied to relations.

Example. On $\mathbb{R}$, $R_1 = \{(x, y) : x = y\}, R_2 = \{(x, y) : x = -y\}$. What are $R_1 \cup R_2$ and $R_1 \cap R_2$?

$R_1 \cup R_2 = \{(x, y) : x = \pm y\}, R_2 = \{(0, 0)\}$.

Definition

*Let R be a relation from A to B. The **domain** and **range** of R are the following.*

$$\operatorname{dom} R = \{x \in A : \exists\, y \in B \text{ s.t. } xRy\}$$

$$\operatorname{ran} R = \{y \in B : \exists\, x \in A \text{ s.t. } xRy\}$$

Note. $\operatorname{dom} R \subseteq A$ and $\operatorname{ran} R \subseteq B$.

Example. Let $A = \{0, 1, 2, 3\}$, $R = \{(0, 0), (0, 1), (0, 2), (3, 0)\}$. Find $\operatorname{dom} R$, $\operatorname{ran} R$.

$\operatorname{dom} R = \{0, 3\}$, $\operatorname{ran} R = \{0, 1, 2\}$

Example. On $\mathbb{Z}$, let $R = \{(x, y) : xy \neq 0\}$. Find $\operatorname{dom} R, \operatorname{ran} R$.

$\operatorname{dom} R = \mathbb{Z} \setminus \{0\}, \operatorname{ran} R = \mathbb{Z} \setminus \{0\}$

Example. On $\mathbb{Z} \times \mathbb{Q}$, let $R = \left\{(x, y) : x \neq 0 \wedge y = \frac{1}{x}\right\}$. Find $\operatorname{dom} R, \operatorname{ran} R$.

$R = \left\{(1, 1), \left(2, \frac{1}{2}\right), \left(3, \frac{1}{3}\right), \ldots, (-1, -1), \left(-2, -\frac{1}{2}\right), \left(-3, -\frac{1}{3}\right), \ldots\right\}$

$\operatorname{dom} R = \mathbb{Z} \setminus \{0\}, \operatorname{ran} R = \left\{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{3}, \ldots\right\}$

Definition

*Let R be a relation from A to B. The **inverse relation** R^{-1} from B to A is define*

$$R^{-1} = \{(y, x) : (x, y) \in R\}.$$

Note. dom R^{-1} = ran R, ran R^{-1} = dom R.

Example. Let $A = \{a, b, c\}, B = \{1, 2, 3, 4\}$,
$R = \{(a, 1), (b, 2), (c, 3), (a, 4)\}$. Find R^{-1}.

$$R^{-1} = \{(1, a), (2, b), (3, c), (4, a)\}$$

Example. On $\mathbb{N}$, let $R = \{(x, y) : y = 2x\}$. Write 3 elements of R and 3 elements of R^{-1}. Define R^{-1}.

$(1, 2), (5, 10), (36, 72) \in R$
$(2, 1), (10, 5), (72, 36) \in R^{-1}$
$R^{-1} = \{(x, y) : x = 2y\}$

Definition

Let R be a relation on A. Then R is

1. ***reflexive*** *if $\forall\ x \in A, xRx$;*
2. ***symmetric*** *if $\forall\ x, y \in A, xRy \to yRx$;*
3. ***transitive*** *if $\forall\ x, y, z \in A, xRy \wedge yRz \to xRz$.*

Example. On $\mathbb{N}$, $R = \{(x, y) : x \text{ is a factor of } y\}$ $(y = kx, k \in \mathbb{N})$.

$\forall\ x \in \mathbb{N}, xRx?$ $x = 1 \cdot x, 1 \in \mathbb{N}$ TRUE. Thus, R is reflexive.

$\forall\ x, y \in \mathbb{N}, xRy \to yRx?$
$2R6$ since $6 = 3 \cdot 2$, but $2 = 6k \to k = \frac{1}{3} \notin \mathbb{N}$, so $(6, 2) \notin R$.
Thus, R is not symmetric.

$\forall\ x, y, z \in \mathbb{N}, xRy \wedge yRz \to xRz?$
$xRy \wedge yRz \to y = kx, z = py, k, p \in \mathbb{N}$.
$z = py = p(kx) = (pk)x, pk \in \mathbb{N} \to xRz$. Thus, R is transitive.

Example. On $\mathbb{R}$, $R = \{(x, x) : x \in \mathbb{R}\}$ is the identity relation.

Since $(x, x) \in \mathbb{R}\ \forall\ x \in \mathbb{R}$, we have that R is reflexive.

Since $(x, y) \in R \to x = y \to (y, x) \in R$, we have that R is symmetric.

Since $(x, y), (y, z) \in R \to x = y = z \to (x, z) \in R$, we have that R is transitive.

Example. On $\mathbb{Z}$, $R = \{(x, y) : x < y\}$.

Since $x \not< x$ for any $x \in \mathbb{Z}$, we have that $(x, x) \notin R \; \forall \; x \in \mathbb{Z}$ and R is not reflexive.

For instance $3 < 5$ so $(3, 5) \in R$, but $5 \not< 3$ so $(5, 3) \notin R$ and R is not symmetric.

If $x < y$ and $y < z$, then for sure $x < z$. So $(x, y), (y, z) \in R \rightarrow (x, z) \in R \; \forall \; x, y, z \in \mathbb{Z}$ and R is transitive.

Example. On the set P of people in the world, $R = \{(x, y) : x \text{ is in the family of } y\}$.

$\forall\ x \in P$, x is in the family of x. So R is reflexive.

$\forall\ x, y \in P$, i x is in the family of y, then y is in the family of x. So R is symmetric.

$\forall\ x, y, z \in P$, if x is in the family of y and y is in the family of z, then x is in the family of z. So R is transitive.

Exercise. Determine reflexive, symmetric, transitive for the following relations.

1. On $\mathbb{R}$, $R = \{(x, y) : y = x^2\}$.
2. On P, $R = \{(x, y) : x \text{ loves } y\}$.

Definition

Let R be a relation on A. Then R is an ***equivalence relation*** *on A iff R is reflexive, symmetric and transitive.*

Example. On Z, prove that $R = \{(a,b) : ab = 0\}$ is not an equivalence relation.

This is a symmetric relation, since $ab = 0 \to ba = 0$. But it is not reflexive nor transitive. One counterexample is enough, bet here is one for each.

If $(1,1) \in R$, then $1 \cdot 1 = 0$ FALSE. Thus, $(1,1) \notin R$ and R is not reflexive. Therefore, R is not an equivalence relation.

$(1,0) \in R$ and $(0,3) \in R$, but $(1,3) \notin R$, so R is not transitive. Therefore, R is not an equivalence relation.

Exercise. Prove that for any given $n \in \mathbb{Z}$, $R = \{(a,b) : (b-a)/n \in \mathbb{Z}\}$ is an equivalence relation on $\mathbb{Z}$.

Example. Let $A = \{0,1,2,3\}$, $R = \{(0,0),(0,2),(1,1),(2,0),(2,2),(3,3)\}$. Prove R is an equivalence relation.

Since $(0,0),(1,1),(2,2),(3,3) \in R$, we have that R is reflexive.

$(0,2) \in R \to (2,0) \in R$ and vice versa, and trivially $(0,0) \in R \to (0,0) \in R$, etc., so we have that R is symmetric.

$(0,0),(0,2) \in R \to (0,2) \in R; (1,1),(1,1) \in R \to (1,1) \in R$
$(2,0),(0,0) \in R \to (2,0) \in R; (2,0),(0,2) \in R \to (2,2) \in R$
$(2,2),(2,0) \in R \to (2,0) \in R; (2,2),(2,2) \in R \to (2,2) \in R$
$(3,3),(3,3) \in R \to (3,3) \in R; (0,0),(0,0) \in R \to (0,0) \in R$
So we have that R is transitive.

Therefore, R is an equivalence relation.

Definition

Let R be an equivalence relation on A. For each $a \in A$, the ***equivalence class*** *of a, denoted by $[a]$, is the set of all elements of A that are related to a.*

$$[a] = \{x \in A : xRa\}$$

- For any $a, b \in A$, either $[a] = [b]$ or $[a] \cap [b] = \varnothing$.
- All equivalence classes of A form a **partition** of A: their union is A and their pairwise intersection is empty.

Example. Let $A = \{0, 1, 2\}$, $R = \{(0, 0), (1, 1), (2, 2), (0, 1), (1, 0)\}$. Find $[0], [1], [2]$.

$[0] = \{x \in A : xR0\} = \{0, 1\}$
$[1] = \{x \in A : xR1\} = \{0, 1\}$
$[2] = \{x \in A : xR2\} = \{2\}$

Example. What do the equivalence classes of the identity relation on $\mathbb{R}$ look like? $R = \{(x, x) : x \in \mathbb{R}\}$

$\left[\frac{1}{2}\right] = \left\{x \in \mathbb{R} : xR\frac{1}{2}\right\} = \left\{\frac{1}{2}\right\}$
$[0] = \{0\}$
$[-2.4] = \{-2.4\} \ldots$

Every equivalence class is just one element.

Example. On $\mathbb{Z}$, let $R = \{(a, b) : a \equiv b \pmod 3\}$. Find $[0], [1], [2]$.

$$[0] = \{x \in \mathbb{Z} : xR0\} = \left\{x \in \mathbb{Z} : \frac{0-x}{3} \in \mathbb{Z}\right\} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$
$$[1] = \left\{x \in \mathbb{Z} : \frac{1-x}{3} \in \mathbb{Z}\right\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$[2] = \left\{x \in \mathbb{Z} : \frac{2-x}{3} \in \mathbb{Z}\right\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

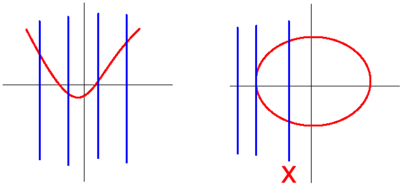
Note. $[0] = [3] = [-3] = [6] = \cdots$, etc.,
$[0] \cap [1] = \varnothing$, $[0] \cap [2] = \varnothing$, $[1] \cap [2] = \varnothing$ and
$[0] \cup [1] \cup [2] = \mathbb{Z}$.

Definition

*A relation f from A to B is a **function** iff for each $x \in A$ there is at most <u>one</u> $y \in B$ such that $(x, y) \in f$.*

A function f from A to B is denoted by $f : A \to B$. The equation $y = f(x)$ means that $(x, y) \in f$, in which case y is the *image* of x under f.

Relations on $\mathbb{R}$ can be plotted by drawing all the points. A graphical way to see if a relation is a function or not is the vertical line test: every vertical line cuts through the curve of the relation at most once. This is not a proof, but it is a good way to visualise functions.



The relation on the left is a function, as every possible vertical line intersects the curve only once. The relation on the right is not a function; while there are some vertical lines that intersect at most once, there are others that intersect twice.

Exercise. Sketch the relations below and convince yourself which ones are functions via the vertical line test.

1. On $\mathbb{R}$, $R = \{(x, y) : y = x^2\}$
2. On $\mathbb{R}$, $R = \{(x, y) : x = y^2\}$
3. On $\mathbb{R}^+$, $R = \{(x, y) : x = y^2\}$
4. On $\mathbb{R}$, $R = \{(x, y) : y = \sqrt{x}\}$

Exercise. Which are functions?

1. The identity relation on $A = \{1, 5, 10\}$
2. $A = \{0, 2, 4\}$, $B = \{1, 3, 5\}$, R on $A \times B$,
   $R = \{(x, y) : x + 1 = y\}$
3. On $\mathbb{Z}$, $F = \{(x, y) : x + 1 = y\}$
4. On $\mathbb{R}$, $R = \{(x, y) : y = 1\}$

Definition

*Let $f : A \to B$ be a function. Then f is **injective (one-to-one)** iff for all $x_1, x_2 \in A$,*

$$f(x_1) = f(x_2) \Leftrightarrow x_1 = x_2.$$

That is, each element of the range is the image of only one element of the domain.

Note. An injective function satisfies the horizontal line test.

Example. Let $A = \{0, 1, 2, 3\}, f : P(A) \to \mathbb{N} \cup \{0\}$, $f(A_i) = |A_i|$, so f outputs the number of elements in A_i. Prove or disprove that f is injective.

$$f(\{1, 2\}) = 2$$
$$f(\{1, 3\}) = 2$$

So this is not a $1 - 1$ function; f is not injective.

Example. Which are injective?

- On $A = \{1, 2, 3\}, F = \{(1, 2), (2, 3), (3, 1)\}$.
- On A, $G = \{(1, 2), (2, 1), (3, 1)\}$.
- On $\mathbb{Z}$, $F = \{(x, y) : y = 2x\}$.
- On $\mathbb{Z} \setminus \{0\} \times \mathbb{R}$, $F = \{(x, y) : y\sqrt{x^2 - 1}\}$.

Functions

1. By direct inspection, every output comes from one distinct input. Therefore, F is injective.
2. By direct inspection, the 1 is an output for two different inputs: the 2 and the 3. Therefore, G is not injective.
3. Let $F(x_1) = F(x_2)$. Then

$$2x_1 = 2x_2 \rightarrow \frac{2x_1}{2} = \frac{2x_2}{2} \rightarrow x_1 = x_2.$$

   Therefore, F is 1-1.
4. Let $F(x_1) = F(x_2)$. Then

$$\sqrt{x_1^2 - 1} = \sqrt{x_2^2 - 1} \rightarrow \sqrt{x_1^2 - 1}^2 = \sqrt{x_2^2 - 1}^2$$
$$\rightarrow x_1^2 - 1 = x_2^2 - 1 \rightarrow x_1^2 = x_2^2 \rightarrow x_1 = \pm x_2$$

   For instance, $F(1) = 0$ and $F(-1) = 0$. Therefore, F is not 1-1.

Definition

A function $f : A \to B$ is ***surjective (onto)*** *iff* $\operatorname{ran} f = B$. *That is,*

$$\forall\, y \in B\, \exists\, x \in A \text{ s.t. } f(x) = y.$$

Example. Let $A = \{1, 2, 3, 4, 5\}, B = \{a, b, c, d\}$. Which are surjective?

1. $f : A \to B, f = \{(1, a), (2, c), (3, c), (4, d), (5, d)\}$
2. $f : A \to B, f = \{(1, a), (2, b), (3, c), (4, d), (5, a)\}$
3. $f : \mathbb{R} \to \mathbb{R}, f(x) = 4x - 1$
4. $f : \mathbb{Z} \to \mathbb{Z}, f(x) = 4x - 1$

Functions

1. Since $b \in B$ & there is no $x \in A$ s.t. $f(x) = b$, f is not onto.
2. Since every $y \in B$ is output for at least one $x \in A$, f is onto.
3. Let $y \in \mathbb{R}$. Is there $x \in \mathbb{R}$ s.t. $f(x) = y$?

   $$y = 4x - 1 \rightarrow x = \frac{y+1}{4} \in \mathbb{R} \qquad \text{YES}$$

   Therefore, f is surjective.
4. For instance, let $y = 2$. Then

   $$2 = 4x - 1 \rightarrow x = \frac{2+1}{4} = \frac{3}{4} \notin \mathbb{Z}\,.$$

   Therefore, f is not surjective.

Definition

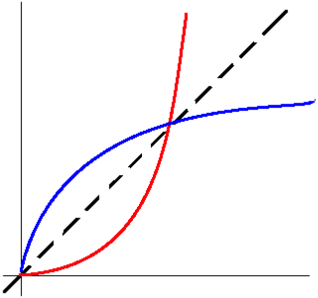
*The **inverse** of a function f, denoted by f^{-1}, is also a function iff f is **bijective**, i.e. injective and surjective.*

In the case that f^{-1} is a function, the following properties are satisfied.

- $\operatorname{dom} f^{-1} = \operatorname{ran} f$
- $\operatorname{ran} f^{-1} = \operatorname{dom} f$
- $f(f^{-1}(x)) = x \ \forall\ x \in \operatorname{ran} f$
- $f^{-1}(f(x)) = x \ \forall\ x \in \operatorname{dom} f$

Graphically, f^{-1} is the reflection of f about the line $y = x$.

Example. Sketch $f : \mathbb{R}^+ \to \mathbb{R}^+, f(x) = x^2$. Find and sketch f^{-1}. Is f^{-1} a function?



The red curve is $y = x^2$. Reflecting on $y = x$ (black dashed), we obtain the function $y = \sqrt{x}$ in blue, the inverse function of x^2.

Example. Find and test the inverse function of $f : \mathbb{R} \to \mathbb{R}, f(x) = 3x - 2$.

$$f^{-1} : x = 3y - 2 \to x + 2 = 3y \to y = \frac{1}{3}(x+2)$$

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

$$f^{-1}(f(x)) = f^{-1}(3x-2) = \frac{1}{3}[(3x-2)+2] = \frac{1}{3} \cdot 3x = x$$

Example. Let $f : \mathbb{R} \to \mathbb{R}, f(x) = \frac{x-2}{x+1}$. Find the domain and range of f, prove f is bijective and find f^{-1}.

The domain is the set of all allowable inputs, so only the -1 causes a problem (division by zero): $\operatorname{dom} f = \mathbb{R} \setminus \{-1\}$. The range of f is the domain of f^{-1}, so let's wait on that.

Injective. Let $f(x_1) = f(x_2)$. Then

$$\frac{x_1 - 2}{x_1 + 1} = \frac{x_2 - 2}{x_2 + 1} \Leftrightarrow (x_1 - 2)(x_2 + 1) = (x_1 + 1)(x_2 - 2)$$
$$\Leftrightarrow x_1 x_2 - 2x_2 + x_1 - 2 = x_1 x_2 + x_2 - 2x_1 - 2$$
$$\Leftrightarrow -2x_2 + x_1 = x_2 - 2x_1 \Leftrightarrow 3x_1 = 3x_2 \Leftrightarrow x_1 = x_2$$

Therefore, f is injective.

Surjective. Let $y \in \mathbb{R}$. If $\exists\, x \in \mathbb{R}$ $\texttt{s.t.}$ $f(x) = y$, then

$$y = \frac{x-2}{x+1} \Leftrightarrow y(x+1) = x-2 \Leftrightarrow xy + y = x - 2$$
$$\Leftrightarrow x(1-y) = 2 + y \Leftrightarrow x = \frac{2+y}{1-y} \in \mathbb{R},$$

as long as $y \neq 1$. Therefore, f is surjective. Also, this gives $f^{-1}(x) = \frac{2+x}{1-x}$ and thus $\operatorname{ran} f = \operatorname{dom} f^{-1} = \mathbb{R} \setminus \{1\}$.

MATH255: Mathematics for Computing

Dr Chayne Planiden

School of Mathematics and Statistics
University of Wollongong

April 5, 2024

A **set** is a collection of elements. The elements are commonly numbers, but can be anything. The elements of a set have no order and no repetition.

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

Sets can be finite or infinite and the Universe is a pre-defined set of all possible elements and denoted by U.

$$\begin{aligned}
\mathbb{N} &= \{1, 2, 3, \ldots\} && \text{(Natural Numbers)}\\
\mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} && \text{(Integers)}\\
\mathbb{Q} &= \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\} && \text{(Rational Numbers)}\\
\mathbb{I} &= \{\pi, e, \sqrt{2}, \ldots\} && \text{(Irrational Numbers)}\\
\mathbb{R} &= \mathbb{Q} \cup \mathbb{I} && \text{(Real Numbers)}
\end{aligned}$$

A set can be defined by a property: $T = \{x \in S : p(x)\}$.

Example

$\{x \in \mathbb{R} : -2 < x \leq 5\} = (-2, 5]$ *is an* ***interval*** *of the real number line and is an infinite set. A parenthesis indicates the endpoint is not in the interval; a bracket indicates that the endpoint is in the interval.*

$\{x \in \mathbb{Z} : -2 < x \leq 5\} = \{-1, 0, 1, 2, 3, 4, 5\}$ *is a finite set of integers.*

Example

What is $\{x \in \mathbb{R} : x^3 = x\}$*?*

$$
\begin{aligned}
x^3 &= x \\
x \cdot x^2 &= x \\
x \cdot x^2 - x &= 0 \\
x(x^2 - 1) &= 0 \\
x(x+1)(x-1) &= 0 \\
x &= -1, 0, 1
\end{aligned}
$$

Therefore, $\{x \in \mathbb{R} : x^3 = x\} = \{-1, 0, 1\}$.

The **empty set** $\varnothing$ is a set with no elements in it.

$$\varnothing = \{\} = \{x \in \mathbb{N} : x \neq x\} = \{x \in \mathbb{R} : 3 < x < 2\}$$

The **cardinality** of a finite set is the number of elements in the set: $|S| = n$ means that S has cardinality n, so it contains n elements. Note that $|\varnothing| = 0$.

Definition

*Set A is a **subset** of set B, and B is a **superset** of A, if every element of A is also in B.*

$$A \subseteq B \Leftrightarrow \forall x \in U, x \in A \rightarrow x \in B$$

If $\exists x \in A$ s.t. $x \notin B$, then $A \not\subseteq B$.

Example

1. $\{1, 2\} \subseteq \{1, 2, 3\}$	*TRUE*
2. $\{0, 2\} \subseteq \{1, 2, 3\}$	*FALSE*
3. $-1 \in \{x \in \mathbb{N} : x^2 = 1\}$	*FALSE*
4. $\{1\} \in \{x \in \mathbb{N} : x^2 = 1\}$	*FALSE*
5. $A \subseteq A \; \forall \; A$	*TRUE*
6. $\varnothing \subseteq A \; \forall \; A$	*TRUE*

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

Example

Let $A = \{1, 2, 3\}$. *True or false?*

(a) $a \subseteq A$	*FALSE*
(b) $\varnothing \in A$	*FALSE*
(c) $\varnothing \subseteq A$	*TRUE*
(d) $\{\varnothing\} \subseteq A$	*FALSE*
(e) $1 \in A$	*TRUE*
(f) $\{1\} \in A$	*FALSE*
(g) $3 \subseteq A$	*FALSE*
(h) $\{1, 2, 3\} \subseteq A$	*TRUE*

Equality of Sets

Definition

*Two sets A and B are **equal** if $A \subseteq B$ and $B \subseteq A$.*

To prove equality of sets, prove that each is a subset of the other.

Example

Prove $A = \{n \in \mathbb{N} : n \text{ is even}\} = B = \{n \in \mathbb{N} : n^2 \text{ is even}\}$.

Proof.

($\subseteq$) Let $n \in A$. Then $n = 2k, k \in \mathbb{N}$.
$n^2 = (2k)^2 = 4k^2 = 2(2k^2) \rightarrow n \in B$.
Thus, $A \subseteq B$.

($\supseteq$) Let $n \in B$. Then n^2 is even. Suppose n is odd, so that
$n = 2k + 1, k \in \mathbb{N}$.
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ is odd, a contradiction. So n is even and we have that $B \subseteq A$.

Therefore, $A = B$. $\square$

Homework. Let
$A = \{n \in \mathbb{Z} : n = 2p, p \in \mathbb{Z}\}$,
$B = \{n \in \mathbb{Z}, n \text{ is even}\}$,
$C = \{n \in \mathbb{Z} : n = 2q - 2, q \in \mathbb{Z}\}$,
$D = \{n \in \mathbb{Z} : n = 3r + 1, r \in \mathbb{Z}\}$.

(a) Is $A = B$?

(b) Is $A = C$?

(c) Is $A = D$?

Set Algebra.

- An *operation* on a set S is a rule for combining elements of S.
- A *binary operation* combines pairs of elements to produce another.
- A binary operation $*$ is *closed* if $x, y \in S \rightarrow x * y \in S$.
- Four common operations on numbers are $+, -, \cdot$ and $/$.

Example

Are $+, -, \cdot, /$ *closed on* $\mathbb{N}$*?*

Proof.

$+$: Let $x, y \in \mathbb{N}$. Then $x + y \in \mathbb{N}$ TRUE. Therefore, $+$ is closed on $\mathbb{N}$.

$-$: Let $x = 1, y = 2$. Then $x - y = -1 \in \mathbb{N}$ FALSE. Therefore, $-$ is not closed on $\mathbb{N}$.

$\cdot$: Let $x, y \in \mathbb{N}$. Then $xy \in \mathbb{N}$ TRUE. Therefore, $\cdot$ is closed on $\mathbb{N}$.

$/$: Let $x = 2, y = 5$. Then $\frac{x}{y} = \frac{2}{5} \in \mathbb{N}$ FALSE. Therefore, $/$ is not closed on $\mathbb{N}$. $\square$

Definition

*An element $e \in S$ is called an **identity** under operation $*$ if*

$$e * x = x * e = x \;\forall\; x \in S.$$

Example

Does $\mathbb{N}$ have an identity under $+$? Under $\cdot$?

Proof.

$+$: $e + x = x \rightarrow e = x - x \rightarrow e = 0$, but $0 \notin \mathbb{N}$. So there is no additive identity in $\mathbb{N}$.

$\cdot$: $ex = x \rightarrow e = \frac{x}{x} \rightarrow e = 1$; $xe = x \rightarrow e = \frac{x}{x} \rightarrow e = 1$. Since $1 \in \mathbb{N}$, the (unique) multiplicative identity in $\mathbb{N}$ is 1. $\square$

Definition

*If $\exists$ e identity of S, an element $x \in S$ is called **invertible** under $*$ if $\exists\, y \in S$ s.t.*

$$x * y = y * x = e.$$

Then y is called the inverse of x and vice versa.

Example

What are the invertible elements of $\mathbb{N}$ under $+$? Under $\cdot$?

Proof.

$+$: There is no identity under $+$ in $\mathbb{N}$. Therefore, there are no invertible elements.

Proof.

$\cdot$: The identity is 1. Let $x \in \mathbb{N}$.

$$x \cdot y = 1 \rightarrow y = \frac{1}{x}$$

So if there are invertible elements x, the inverse $\frac{1}{x}$ has to be in $\mathbb{N}$. The only natural number that qualifies is $x = 1 \rightarrow y = 1$, so that is the only invertible element. $\square$

Example

Which of $+, -, \cdot, /$ are closed on $\mathbb{R}$?

Proof.

Let $x, y \in \mathbb{R}$. Then

$x + y \in \mathbb{R}$,

$x - y \in \mathbb{R}$ and

$xy \in \mathbb{R}$.

Therefore, $+, -, \cdot$ are closed. But $\frac{x}{y}$ is not always a real number; if $y = 0$, then $\frac{x}{y} \notin \mathbb{R}$. Therefore, $/$ is not closed. $\square$

Example

Does $\mathbb{R}$ have identities under $+, \cdot$?

Proof.

$$e + x = x \to e = 0, x + e = x \to e = 0, 0 \in \mathbb{R}$$
(additive identity)

$$e \cdot x = x \to e = 1, x \cdot e = x \to e = 1, 1 \in \mathbb{R}$$
(multiplicative identity)

$\square$

Example

What are the invertible elements of $\mathbb{R}$ under $+$? Under $\cdot$?

Proof.

$+$: Let $x, y \in \mathbb{R}$ be such that $x + y = 0$. Then $y = -x$, so the invertible pairs are $\{(x, -x) : x \in \mathbb{R}\}$.

$(3, -3), (-\pi, \pi), (0, 0), \left(\frac{2}{3}, -\frac{2}{3}\right), \ldots$

$\cdot$: Let $x, y \in \mathbb{R}$ be such that $xy = 1$. Then $y = \frac{1}{x}$, so the invertible pairs are $\left\{\left(x, \frac{1}{x}\right) : x \in \mathbb{R} \setminus \{0\}\right\}$.

$\left(2, \frac{1}{2}\right), \left(7\pi, \frac{1}{7\pi}\right), \left(-8.37, \frac{1}{-8.37}\right), \left(\frac{3}{5}, \frac{5}{3}\right) \ldots$ $\square$

Definition

- *A binary operation $*$ on S is **commutative** if*

$$x * y = y * x \ \forall \ x, y \in \S.$$

- *A binary operation $*$ on S is **associative** if*

$$(x * y) * z = x * (y * z) \ \forall \ x, y, z \in S.$$

Example

The operations $+$ and $\cdot$ are commutative and associative on $\mathbb{N}$.

$$x + y = y + x \ \forall \ x, y \in \mathbb{N}$$
$$x + (y + z) = (x + y) + z \ \forall \ x, y, z \in \mathbb{N}$$
$$xy = yx \ \forall \ x, y \in \mathbb{N}$$
$$x(yz) = (xy)z \ \forall \ x, y, z \in \mathbb{N}$$

Homework. Prove by counterexample that $-$ and $/$ are not commutative and not associative on $\mathbb{N}$.

Example (Rock – Paper – Scissors)

Let $M = \{r, p, s\}$ and consider the binary operation $*$ that gives the winner of the game.

$$r * p = p * r = p \qquad \text{(paper beats rock)}$$
$$r * s = s * r = r \qquad \text{(rock beats scissors)}$$
$$p * s = s * p = s \qquad \text{(scissors beats paper)}$$
$$p * p = p, r * r = r, s * s = s \qquad \text{(ties)}$$

We see by the above that $*$ is commutative. Is it associative?

$$(r * p) * s = p * s = s$$
$$r * (p * s) = r * s = r$$

Therefore no, $*$ is not associative.

Definition

A binary operation $\cdot$ on a set S is ***distributive*** *over another binary operation $+$ if for all $a, b, c \in S$ we have*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \text{ and}$$
$$(b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

For example, multiplication is distributive over addition on $\mathbb{N}$.

Exercise. Prove that addition is not distributive over multiplication on $\mathbb{N}$: $a + (bc) \neq (a + b)(a + c)$ for at least one choice of $a, b, c \in \mathbb{N}$.

Example

Let $a, b \in \mathbb{N}$. Simplify the expression $8[(a+b)] + 2a$.

$$\begin{aligned}
[8(a+b)] + 2a &= (8a+8b) + 2a && \text{(distributive)} \\
&= (8b+8a) + 2a && \text{(commutative)} \\
&= 8b + (8a+20) && \text{(associative)} \\
&= 8b + [(8+2)a] && \text{(distributive)} \\
&= 8b + 10a
\end{aligned}$$

Definition

*A set S with order $\leq$ is called **well-ordered** if every nonempty subset of S has at least one smallest element. That is,*

$$\varnothing \neq T \subseteq S \to \exists\, s_0 \in T \text{ s.t. } s_0 \leq s \;\forall\, s \in T.$$

Example. The set $\mathbb{N}$ with the usual order $\leq$ is well-ordered, since every subset of $\mathbb{N}$ has a least element.

Example. Is $\mathbb{Z}$ well-ordered?

For instance, the set of all odd numbers $\{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$ is a subset of $\mathbb{Z}$ and it does not have a smallest element. So no, $\mathbb{Z}$ is not well-ordered.

Algebra of Sets

Operations on Sets

- Union: $A \cup B = \{x : x \in A \vee x \in B\}$
- Intersection: $A \cap B = \{x : x \in A \wedge x \in B\}$
- Complement: $\overline{A}, A', A^c = \{x : x \notin A\}$
- Difference: $A - B, A \setminus B = \{x : x \in A \wedge x \notin B\}$
- Power Set: P(A)={all subsets of A}

Example. Let $U = \mathbb{R}$. Write $A \cup B$ and $A \cap B$.

(a) $A = \{1\}, B = \{2\}$
$A \cup B = \{1, 2\}$
$A \cap B = \{\} = \varnothing$

(b) $A = \{\text{even numbers}\}, B = \{\text{odd numbers}\}$
$A \cup B = \mathbb{Z}$
$A \cap B = \varnothing$

(c) $A = \{x \in \mathbb{R} : 0 \leq x \leq 2\}, B = \{x \in \mathbb{R} : 1 \leq x \leq 3\}$
$A \cup B = \{x \in \mathbb{R} : 0 \leq x \leq 3\} = [0, 3]$
$A \cap B = \{x \in \mathbb{R} : 1 \leq x \leq 2\} = [1, 2]$

Example. Let $U = \mathbb{Z}$. Write $\overline{A}$.

(a) $A = \{1, 2, 3\}$
$\overline{A} = \{\ldots, -2, -1, 0, 4, 5, 6, \ldots\}$

(b) $A = \{x \in \mathbb{Z} : x \text{ is even}\}$
$\overline{A} = \{\ldots, -3, -1, 1, 3, \ldots\} = \{x \in \mathbb{Z} : x \text{ is odd}\}$

(c) $A = \{x \in \mathbb{Z} : x > 0 \vee x < 0\}$
$\overline{A} = \{0\}$

Example. Let $U \in \mathbb{R}$, $A = \{1, 2, 3\}$, $B = \{2\}$, $C = \{2, 3, 4\}$, $D = [0, 1]$.

(a) $A - C = \{1\}$

(b) $B - C = \varnothing$

(c) $D - B = D$

(d) $D - A = [0, 1)$

(e) $A - D = \{2, 3\}$

Example. Let $A = \{1, 2, 3\}$. Find $P(A)$.

$P(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$

Note. $|A| = n \to |P(A)| = 2^n$

Algebra of Sets

Example. Prove $(A \subseteq C) \wedge (B \subseteq C) \to [(A \cup B) \subseteq C]$

$$[(A \to C) \wedge (B \to C)] \underset{\color{blue}F}{\to} [(A \vee B) \to C]$$

$$[(A \to C) \underset{\color{blue}T}{\wedge} (B \to C)] \to [(A \underset{\color{blue}F}{\vee} B) \to C]$$

$$[(A \underset{\color{blue}T}{\to} C) \wedge (B \underset{\color{blue}T}{\to} C)] \to [(A \underset{\color{blue}T}{\vee} B) \to \underset{\color{blue}F}{C}]$$

$$[(\underset{\color{blue}F}{A} \to \underset{\color{blue}F}{C}) \wedge (\underset{\color{blue}F}{B} \to \underset{\color{blue}F}{C})] \to [(A \vee B) \to C]$$

All the variables being FALSE contradicts that fact that the AND is TRUE, so this statement cannot be false; it is a tautology. Therefore, the original expression of sets is always true.

Definition

Two sets A and B are ***disjoint*** *if $A \cap B = \varnothing$.*

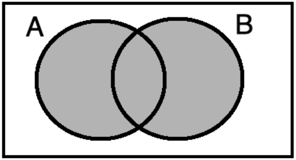
Example. Let $U = \mathbb{R}$. Write two disjoint sets to each of the sets below.

(a) $\{x \in \mathbb{Z} : x \text{ is even}\}$
$\{x \in \mathbb{Z} : x \text{ is odd}\}$; $\{1, \frac{2}{3}, \pi\}$

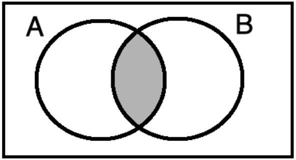
(b) $\{x \in \mathbb{R} : x^2 - 5x + 6 \geq 0\}$
$(x-2)(x-3) \geq 0 \to x \in (-\infty, 2] \cup [3, \infty)$
$\{2.1, 2.2, \ldots, 2.9\}$; $\{\frac{9}{4}, \frac{5}{2}, \frac{11}{4}\}$

Algebra of Sets

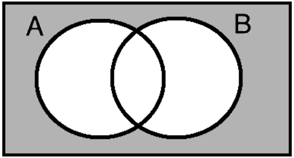
A **Venn diagram** is a graphical representation of sets. It is a good way to visualise union, intersection, complement and difference of sets.



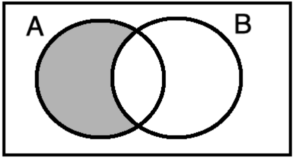
$A \cup B$



$A \cap B$



$\overline{A}$



$A - B$

Algebra of Sets

1.
   (a) $(A \subseteq B \wedge B \subseteq C) \rightarrow A \subseteq C$
   (b) $A \subseteq A \cup B$; $B \subseteq A \cup B$
   (c) $A \cap B \subseteq A$; $A \cap B \subseteq B$
2.
   (a) $A = B \leftrightarrow (A \subseteq B \wedge B \subseteq A)$
   (b) $A \subseteq B \leftrightarrow A \cup B = B$; $A \subseteq B \leftrightarrow A \cap B = A$
3.
   - $A \subseteq B \rightarrow A \cup C \subseteq B \cup C$; $A \subseteq B \rightarrow A \cap C \subseteq B \cap C$
4.
   - $A \cup B = B \cup A$; $A \cap B = B \cap A$
5.
   - $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$
6.
   - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$; $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

7.

- $\overline{A \cup B} = \overline{A} \cap \overline{B}$; $\overline{A \cap B} = \overline{A} \cup \overline{B}$

8.

(a) $\overline{\overline{A}} = A$

(b) $A \subseteq B \leftrightarrow \overline{B} \subseteq \overline{A}$; $A - B = A \cap \overline{B}$

(c) $\overline{U} = \varnothing$; $\overline{\varnothing} = U$

9.

(a) $A \cap U = A$; $A \cup \varnothing = A$; $A \cap \varnothing = \varnothing$

(b) $A \cup U = U$; $A \cap \overline{A} = \varnothing$; $A \cup \overline{A} = U$

10.

(a) $(A \subseteq C \wedge B \subseteq C) \leftrightarrow (A \cup B) \subseteq C$

(b) $(A \subseteq B \wedge A \subseteq C) \leftrightarrow A \subseteq (B \cap C)$

Example

Prove De Morgan's law $\overline{A \cup B} = \overline{A} \cap \overline{B}$*.*

Proof.

$(\subseteq)$: Let $x \in \overline{A \cup B}$. Then $x \notin A \cup B \rightarrow x \notin A \wedge x \notin B$
$\rightarrow x \in \overline{A} \wedge x \in \overline{B} \rightarrow x \in \overline{A} \cap \overline{B}$. Thus, $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

$(\supseteq)$: Let $x \in \overline{A} \cap \overline{B}$. Then $x \in \overline{A} \wedge x \in \overline{B} \rightarrow x \notin A \wedge x \notin B$
$\rightarrow x \notin A \cup B \rightarrow x \in \overline{A \cup B}$. Thus, $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$.

Therefore, $\overline{A \cup B} = \overline{A} \cap \overline{B}$. □

Exercise. Prove that $A \subseteq B \leftrightarrow A \cup B = B$.

MATH255: Mathematics for Computing

Dr Chayne Planiden

School of Mathematics and Statistics
University of Wollongong

March 4, 2024

Definition

*The **universal quantifier** is denoted by $\forall$ and indicates "for all".*

*The **existential quantifier** is denoted by $\exists$ and indicates "there exists".*

Definition

*A **predicate** is an expression that becomes T or F when values are substituted for the variables.*

*The **domain** of a predicate is the set of all possible values it can take on.*

*The **truth set** of a predicate is the subset of the domain that makes the predicate true.*

Example

What is the truth set of $p(x)$: x *is an integer less than 5,* $\operatorname{dom} p = \mathbb{Z}$*?*

Answer. Truth set: $\{\ldots, -2, -1, 0, 1, 2, 3, 4\}$

Example

What is the truth set of $q(x) : x^2 > x, \operatorname{dom} q = \mathbb{R}$*?*

Answer. Truth set: $(-\infty, 0) \cup (1, \infty)$

Definition

The general form of a ***universal statement*** *is as follows.*

$$\forall\, x \in D, p(x)$$

"For all x in the domain of predicate p, $p(x)$."

- All humans are mortal.
- Every real number has a nonnegative square: $\forall\, x \in \mathbb{R}, x^2 \geq 0$.

To prove a universal statement, you must show that the statement is true for every element in the domain. To disprove a universal statement, you need to find one counterexample, i.e. a member of the domain that makes the statement false.

Example

Prove or disprove: $\forall\ x \in \mathbb{R}, x^2 > x.$

This is false; there are many counterexamples. For instance, $x = \frac{1}{2}$ gives $\left(\frac{1}{2}\right)^2 > \frac{1}{2} \rightarrow \frac{1}{4} > \frac{1}{2}$, which is false.

Example

Prove or disprove: every integer greater than zero has a prime factor.

False: let $x = 1$. Then x does not have a prime factor, since the primes start at 2.

Example

Let $D = \{1, 2, 3, 4, 5\}$. Show that

(a) $\forall\ x \in D, x^2 \geq x$ *is TRUE, and*

(b) $\forall\ x \in D, \frac{1}{x^2} < \frac{1}{x}$ *is FALSE.*

(a) $1^2 \geq 1 \leftrightarrow 1 \geq 1$ T
$2^2 \geq 2 \leftrightarrow 4 \geq 2$ T
$3^2 \geq 3 \leftrightarrow 9 \geq 3$ T
$4^2 \geq 4 \leftrightarrow 16 \geq 4$ T
$5^2 \geq 5 \leftrightarrow 25 \geq 5$ T: therefore, $\forall\ x \in D, x^2 \geq x$ is TRUE.

(b) $\frac{1}{1^2} < 1 \leftrightarrow 1 < 1$ F: therefore, $\forall\ x \in D, \frac{1}{x^2} < \frac{1}{x}$ is FALSE.

Definition

The general form of an ***existential statement*** *is as follows.*

$$\exists\ x \in D \text{ such that } p(x)$$

"There exists x in the domain of predicate p such that $p(x)$."

- There is a cat in my house.
- There exist integers m, n such that $m + n = mn$.

To prove an existential statement, you must find one element of the domain that makes the statement true. To disprove an existential statement, you need to prove the statement false for every element of the domain.

Example

Show that the statement $\exists\ m \in \mathbb{Z}\ \texttt{s.t.}\ m^2 = m$ *is TRUE.*

$1^2 = 1$, or $0^2 = 0$: therefore, $\exists\ m \in \mathbb{Z}\ \texttt{s.t.}\ m^2 = m$ is TRUE.

Example

Let $E = \{5, 6, 7, 8, 9, 10\}$. *Show that the statement* $\exists\ m \in E\ \texttt{s.t.}\ m^2 = m$ *is FALSE.*

$5^2 = 25 \neq 5$
$6^2 = 36 \neq 6$
$7^2 = 49 \neq 7$
$8^2 = 64 \neq 8$
$9^2 = 81 \neq 9$
$10^2 = 100 \neq 10$: therefore, $\exists\ m \in E\ \texttt{s.t.}\ m^2 = m$ is FALSE.

Negation of Universal Statement

What is the negation of, "all mathematicians wear glasses"?

Negation of Universal Statement

What is the negation of, "all mathematicians wear glasses"?

"There exists a mathematician who does not wear glasses."

Negation of Universal Statement

What is the negation of, "all mathematicians wear glasses"?

"There exists a mathematician who does not wear glasses."

Definition

The negation of the universal statement

$$\forall\, x \in D, p(x)$$

is the existential statement

$$\exists\, x \in D \text{ s.t. } \sim p(x).$$

Example

No computer hacker is over 40 years old.

There is a computer hacker over 40 years old.

All prime numbers are odd.

There exists an even prime number.

Every blonde person has blue eyes.

There is a blonde person who does not have blue eyes.

$\forall\ x \in \mathbb{R}, \frac{1}{x} > 1$

$\exists\ x \in \mathbb{R}\ \texttt{s.t.}\ x \leq 1$

Negation of Existential Statement

What is the negation of, "some fish breathe air"?

Negation of Existential Statement

What is the negation of, "some fish breathe air"?

"No fish breathes air."

Negation of Existential Statement

What is the negation of, "some fish breathe air"?

"No fish breathes air."

Definition

The negation of the existential statement

$$\exists\, x \in D \text{ s.t. } p(x)$$

is the universal statement

$$\forall\, x \in D, \sim p(x).$$

Negation of Existential Statement

Example

There is a triangle whose sum of angles is 200 degrees.

All triangles have sum of angles not equal to 200 degrees.

There is a 120-year-old woman in Australia.

All women in Australia are not 120 years old.

$\exists\, x \in \mathbb{R} \texttt{ s.t. } x^2 = -1$

$\forall\, x \in \mathbb{R}, x^2 \neq -1$

Proof of Valid Argument

Definition

*An **argument** is a sequence of statements, all of which are assumptions except the last one, which is the conclusion. If the conclusion is true whenever all assumptions are true, then the argument is valid.*

Example

If x is a pig, then x is pink. (assumption)

Peppa is a pig. (assumption)

Therefore, Peppa is pink. (conclusion)

Proof of Valid Argument

Definition

*A **proof** is a valid argument used to establish a result.*

Example

Prove that if $x \in \mathbb{R}$ and n is even, then $x^n \geq 0$.

Proof.

Since n is even, we know that $n = 2m$ for some $m \in \mathbb{Z}$. Then

$$x^n = x^{2m} = (x^m)^2 \geq 0$$

$\square$

To test an argument for validity, use a truth table. Identify all the rows in which all assumptions are true and verify that the conclusion is also true in those rows.

Example

$p \to (q \vee \sim r)$
$q \to (p \wedge r)$
$\therefore p \to r$

p	q	r	$q \vee \sim r$	$p \wedge r$	$p \to (q \vee \sim r)$	$q \to (p \wedge r)$	$p \to r$
T	T	T	T	T	T	T	T
T	T	F	T	F	T	F	F
T	F	T	F	T	F	T	T
T	F	F	T	F	T	T	F
F	T	T	T	F	T	F	T
F	T	F	T	F	T	F	T
F	F	T	F	F	T	T	T
F	F	F	T	F	T	T	T

Since there is a row that has true assumptions and false conclusion, the argument is **invalid.**

Homework. Test the validity.

(a) $p \vee (q \vee r)$
$\sim r$
$\therefore p \vee r$

(b) $p \rightarrow q$
p
$\therefore q$

Definition

An argument that has two assumptions is called a ***syllogism****. The most basic form of syllogism is the* ***modus ponens*** *form:*

$p \to q$
p
$\therefore q$

Definition

The ***law of syllogism*** *is as follows.*

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

Homework. Prove it, either by quick method or by truth table.

Proof of Existential Statement

To prove a statement of the form

$$\exists\, x \in D \text{ s.t. } p(x),$$

one must find at least one $x \in D$ that makes $p(x)$ true.

Example

Prove there is an even number that can be written in two different ways as the sum of two primes.

Proof.

$$\begin{aligned} 2 &= 2 \\ 4 &= 2+2 \\ 6 &= 3+3 \\ 8 &= 3+5 \\ 10 &= 5+5 = 3+7 \end{aligned}$$

$\square$

Proof of Existential Statement

Example

Prove that there exist $m, n \in \mathbb{N}$ whose sum of reciprocals is an integer: $\frac{1}{m} + \frac{1}{n} \in \mathbb{Z}$.

Proof.

Let $m = n = 1$. Then

$$\frac{1}{m} + \frac{1}{n} = \frac{1}{1} + \frac{1}{1} = 1 + 1 = 2.$$

$\square$

Proof of Universal Statement

To prove a statement of the form

$$\forall\, x \in D, p(x),$$

one must prove that $p(x)$ is true for every possible choice of $x \in D$. If the domain is reasonably small, the method of exhaustion involves substituting each $x \in D$ into p and verifying the $p(x)$ is true for each one.

Example

Prove that every number that is even between 4 and 18 is the sum of two prime numbers.

Proof.

$$\begin{aligned} 4 &= 2 + 2 \\ 6 &= 3 + 3 \\ 8 &= 3 + 5 \\ 10 &= 3 + 7 \\ 12 &= 5 + 7 \\ 14 &= 7 + 7 \\ 16 &= 5 + 11 \end{aligned}$$

$\square$

Homework. Investigate proofs (not by exhaustion!) that every even number can be written as the sum of two prime numbers.

Another proving method is called the generalised proof, in which arbitrary (unspecified) elements of the domain are used to shoe validity for all elements.

Example

Prove that if $a, b \in \mathbb{Z}$, then $10a + 8b$ is even.

Proof.

Let $a, b \in \mathbb{Z}$. Then

$10a + 8b = 2(5a + 4b)$.
Since $a, b \in \mathbb{Z}$, $5a$ and $4b$ are also in $\mathbb{Z}$, as is the sum $5a + 4b$. Therefore,

$2(5a + 4b)$ is even. $\square$

Disproof of Existential Statement

To disprove a statement, prove its negation. In the case of an existential statement, the negation is universal.

$$\sim (\exists\, x \in D \text{ s.t. } p(x)) \equiv \forall\, x \in D, \sim p(x)$$

Example

Disprove: there exists an even prime number greater than 2.

Proof.

The negation is: all prime numbers greater than 2 are odd. Let $x > 2$ be prime. Suppose that x is even. Then $x = 2m, m \in \mathbb{Z}$ and

$$\frac{x}{2} = \frac{2m}{2} = m \in \mathbb{Z},$$

which means that x is divisible by 2, thus not a prime number. This is a contradiction, since we started out with, 'let x be prime'. So our supposition that x is even is false, therefore, x is odd. $\square$

Disproof of Universal Statement

In the case of a universal statement, the negation is existential.

$$\sim (\forall\, x \in D, p(x)) \equiv\ \exists\, x \in D \texttt{ s.t. } \sim p(x)$$

Example

Disprove: $\forall\, x \in \mathbb{R}, x < 0\ \vee\ x > 0$.

Proof.

The negation is $\exists\, x \in \mathbb{R} \texttt{ s.t. } x \geq 0\ \wedge\ x \leq 0$. Let $x = 0$. Then $x \geq 0$ and $x \leq 0$. □

Example

Disprove: $\forall\ a, b \in \mathbb{R}, a^2 = b^2 \rightarrow a = b$.

Proof.

Let $a = -1, b = 1$. Then $a^2 = (-1)^2 = 1$ and $b^2 = 1^2 = 1$, so $a^2 = b^2$, but $a \neq b$. $\square$

Homework. Prove or disprove: $\forall\ x \in \mathbb{R},\ \exists\ y \in \mathbb{R}\ \texttt{s.t.}\ x + y = 0$.

A **direct proof** of a statement begins with supposing that the assumptions are true and using them to prove that the conclusion must also be true.

Example

Prove that if $3x - 9 = 15$*, then* $x = 8$*.*

Proof.

$$
\begin{aligned}
3x - 9 &= 15 \\
3x - 9 + 9 &= 15 + 9 \\
3x &= 24 \\
\frac{3x}{3} &= \frac{24}{3} \\
x &= 8
\end{aligned}
$$

$\square$

Example

Prove that the sum of any two even numbers is even.

Proof.

Let a, b be even numbers. Then $\exists\ c, d \in \mathbb{Z}$ s.t. $a = 2c, b = 2d$.

$$\begin{aligned} a + b &= 2c + 2d \\ &= 2(c + d) \end{aligned}$$

Since $c, d \in \mathbb{Z}$, $c + d \in \mathbb{Z}$. So $a + b$ is an integer times two, therefore, it's an even number. $\square$

Example

Prove that if a, b are perfect squares, then ab is a perfect square.

Proof.

We have $a = c^2, b = d^2$ for some $c, d \in \mathbb{Z}$.

$$\begin{aligned} ab &= c^2 d^2 \\ &= (cd)^2 \end{aligned}$$

Since $c, d \in \mathbb{Z}$, $cd \in \mathbb{Z}$. Therefore, ab is a perfect square. $\square$

Example

Prove that $\forall\ x \in \mathbb{R}, -x^2 + 2x + 1 \leq 2.$

Proof.

Let $x \in \mathbb{R}$.

$$\begin{aligned} -x^2 + 2x + 1 \leq 2 &\Leftrightarrow -x^2 + 2x + 1 - 2 \leq 0 \\ &\Leftrightarrow (-1)(-x^2 + 2x - 1) \geq (-1)0 \\ &\Leftrightarrow x^2 - 2x + 1 \geq 0 \\ &\Leftrightarrow (x-1)^2 \geq 0 \ \ \text{TRUE} \end{aligned}$$

□

Proof by Contradiction

To prove a statement **by contradiction**, suppose that the conclusion is false and show that an assumption also must be false. This means that if all assumptions are true, the conclusion must be true.

Homework. Prove by truth table that $p \to q \equiv \sim q \to \sim p$.

Example

Prove that $\forall\ n \in \mathbb{N}$*, if* n^2 *is even, then* n *is even.*

Proof.

Suppose that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} n^2 &= (2k+1)^2 = 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 = \quad \text{ODD} \end{aligned}$$

Therefore, if n^2 is even, then n is even. □

Proof by Contradiction

Example

Prove that $y \in \mathbb{R} \setminus \mathbb{Q} \to y + 7 \in \mathbb{R} \setminus \mathbb{Q}$.

Proof.

Suppose $y + 7 \in \mathbb{Q}$. Then $\exists\ a, b \in \mathbb{Z}$ $\texttt{s.t.}$ $y + 7 = \frac{a}{b}$.

$$y + 7a = \frac{a}{b} \Leftrightarrow y = \frac{a}{b} - 7$$
$$\Leftrightarrow y = \frac{a - 7b}{b} \in \mathbb{Q}$$

Therefore, $y \in \mathbb{R} \setminus \mathbb{Q} \to y + 7 \in \mathbb{R} \setminus \mathbb{Q}$. $\square$

Example

Prove that there is an infinite number of prime numbers.

Proof.

Suppose there is a finite number of prime numbers: $\{p_1, p_2, \ldots, p_n\}$. Define $p = p_1 p_2 \cdots p_n + 1$ and note that $p > p_n$. Now for any prime number p_i, we have

$$\frac{p}{p_i} = \frac{p_1 p_2 \cdots p_n + 1}{p_i} = \frac{p_1 p_2 \cdots p_n}{p_i} + \frac{1}{p_i}$$
$$= p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n + \frac{1}{p_i} \notin \mathbb{Z}$$

Since p is not divisible by any prime number p_i, p is prime. This is a contradiction, since $\{p_1, \ldots, p_n\}$ is the list of all primes. Therefore, there is an infinite number of prime numbers. $\square$

MATH255: Mathematics for Computing

Dr Chayne Planiden

School of Mathematics and Statistics
University of Wollongong

April 10, 2024

Week 1:
Logic

Definition

A statement is an expression that is either true or false, never both.

Example

Are the following statements?

1. *There are 10 people in this classroom.* — *Yes.*
2. *Is it lunchtime?* — *No.*
3. $3 + 4 = 7$ — *Yes.*
4. $x > 2$ — *No.*
5. *There exists x such that $x < 2$.* — *Yes.*
6. *This sentence is false.* — *No.*

Note. We are not saying whether the expression is true or false, only whether it is a statement.

Example

1. *If $x^2 = 9$, then $x = \pm 1$.* *False.*
2. *If $x^2 = 9$, then $x = \pm 3$.* *True.*

Proof of both.

Let $x^2 = 9$. Then take the square root of both sides:

$$\sqrt{x^2} = \pm\sqrt{9}$$
$$x = \pm 3$$

□

Connectives. There are five basic connectives for forming compound statements by connecting simple statements. Let p and q be statements.

Negation	$\sim p$	"Not p"
Conjunction	$p \wedge q$	"p and q"
Disjunction	$p \vee q$	"p or q"
Conditional	$p \rightarrow q$	"If p, then q"; "p implies q"
Biconditional	$p \leftrightarrow q$	"p if and only if q"

Week 1: Negation

Negation. p true $\rightarrow \sim p$ false. p false $\rightarrow \sim p$ true.

Example

- *p: It is raining now. $\sim p$: It is not raining now.*
- *q: Video games are not fun. $\sim q$: Video games are fun.*
- *$r: x > 2$ or $x < 2$. $\sim r: x \leq 2$ and $x \geq 2$ (i.e. $x = 2$).*

A truth table identifies all possibilities of a compound statement being true or false. The truth table for the negation is the simplest one, since it involves only one simple statement.

p	$\sim p$
T	F
F	T

Conjunction. The conjunction is the 'and' connective and connects two statements.

Example

1. *p: It is hot. q: It is sunny.*
   $p \wedge q$*: It is hot and sunny.*
2. $p : x < 2$. $q : x > -1$.
   $p \wedge q : -1 < x < 2$ *or* $x \in (-1, 2)$.

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

Disjunction. The disjunction is the ‘or’ connective and connects two statements.

Example

1. *p: I take the bus to school. q: I take the train to school.*
   $p \vee q$*: I take the bus or the train to school.*
2. $p : x < -1,\ q : x > 1$
   $p \vee q : x < -1$ *or* $x > 1;\ |x| > 1;\ x \in (-\infty, -1) \cup (1, \infty)$

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

Note. The preceding is the inclusive or, which is true when both statements are true. There is also an exclusive or $\oplus$, which is true only when one statement or the other is true, but not both.

Do you want coffee or tea? This is an exclusive or, because you would not want both, only one or the other.
Do you want milk or sugar? This is an inclusive or, since you might want one or the other or both.

We don't normally use $\oplus$, since we can write it equivalently as follows.

$$p \oplus q \equiv (p \vee q) \wedge \sim (p \wedge q)$$

A compound statement that involves n simple statements will have a truth table of 2^n rows, in order to cover all possible combinations of T/F of each simple statement. The number of columns is your choice, but you need one for each simple statement and one for the final statement at least. Add as many intermediate columns as you wish.

Example

1. $p \vee \sim p$
2. $\sim p \wedge q$
3. $(p \wedge q) \vee \sim r$

Week 1: Truth Tables

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

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

Week 1: Truth Tables

p	q	r	$p \wedge q$	$\sim r$	$(p \wedge q) \vee \sim r$
T	T	T	T	F	T
T	T	F	T	T	T
T	F	T	F	F	F
T	F	F	F	T	T
F	T	T	F	F	F
F	T	F	F	T	T
F	F	T	F	F	F
F	F	F	F	T	T

Conditional. The conditional is the implication connective and connects two statements.

Example

1. *p: I work hard. q: I do well.*
   $p \to q$: *If I work hard, then I do well.*
2. $p : x = 2$, $q : x^2 = 4$
   $p \to q$: *if* $x = 2$, *then* $x^2 = 4$.

Note. In Example 2 we have a true statement: if $x = 2$, then $x^2 = 4$. But the reverse is not true.
$q \to p$ (if $x^2 = 4$, then $x = 2$) is false, since $x = -2$ also yields $x^2 = 4$.

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

Why is $p \to q$ true when p is false?

Example

p: It rains. q: I will go home. Consider all possibilities.

- *If it rains and I go home, then $p \to q$ happened (it's true).*
- *If it rains and I don't go home, then $p \to q$ didn't happen (it's false).*
- *If it doesn't rain, then whether I go home or not, $p \to q$ is still true by default.*

Biconditional. The biconditional is the double implication connective and connects two statements.

Example

1. $p : x^3 = -8$, $q : x = -2$
   $p \leftrightarrow q : x^3 = -8 \leftrightarrow x = -2$ *(true)*
2. *p: Michael is a bachelor. q: Michael is male. r: Michael has never been married.*
   $p \leftrightarrow (q \wedge r)$*: Michael is a bachelor if and only if he is male and has never been married.*

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

Example

Write the truth value.

1. $x^2 = 1 \leftrightarrow x = 1 \vee x = -1$

Example

Write the truth value.

1. $x^2 = 1 \leftrightarrow x = 1 \vee x = -1$ T

Example

Write the truth value.

1. $x^2 = 1 \leftrightarrow x = 1 \vee x = -1$ T
2. *I get wet if and only if it's raining.*

Example

Write the truth value.

1. $x^2 = 1 \leftrightarrow x = 1 \vee x = -1$ T
2. *I get wet if and only if it's raining.* *F*

Example

Write the truth value.

1. $x^2 = 1 \leftrightarrow x = 1 \vee x = -1$ *T*
2. *I get wet if and only if it's raining.* *F*

Note. $p \leftrightarrow q$ is equivalent to $p \rightarrow q \wedge q \rightarrow p$.

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow p)$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Main Connective. The main connective is the one that binds the whole statement together. It is applied last, after all delimited pieces. If there are no delimiters, connectives are applied in left-to-right order.

( ) - parentheses
[ ] - brackets
{ } - braces

Example

The main connectives below are indicated in red.

- $(p \vee \sim q) \rightarrow (p \vee r)$
- $p \rightarrow [q \rightarrow (r \vee \sim r)]$
- $\sim [(p \wedge q) \vee (\sim p \wedge q)]$

Week 1: Tautology/Fallacy/Contingency

- A **tautology** is a statement whose truth value is always true.
- A **fallacy** is a statement whose truth value is always false.
- A **contingency** is a statement whose truth value is sometimes true, sometimes false.

- A **tautology** is a statement whose truth value is always true.
- A **fallacy** is a statement whose truth value is always false.
- A **contingency** is a statement whose truth value is sometimes true, sometimes false.

$p \vee \sim p$ is a tautology, $p \wedge \sim p$ is a fallacy. This can be seem with truth table: if the statement is true (false) in every row, it is a tautology (fallacy).

p	$\sim p$	$p \vee \sim p$
T	F	T
F	T	T

p	$\sim p$	$p \wedge \sim p$
T	F	F
F	T	F

Example

Is the statement $\sim [(\sim p \wedge q) \wedge p]$ *a tautology, fallacy or contingency?*

Example

Is the statement $\sim [(\sim p \wedge q) \wedge p]$ a tautology, fallacy or contingency?

p	q	$\sim p$	$\sim p \wedge q$	$(\sim p \wedge q) \wedge p$	$\sim [(\sim p \wedge q) \wedge p]$
T	T	F	F	F	T
T	F	F	F	F	T
F	T	T	T	F	T
F	F	T	F	F	T

The statement is a tautology.

The **quick method** to prove a tautology sets the main connective FALSE and works backwards to see if there is some combination of simple variable truth values that indeed makes the compound statement false. If not, then it is a tautology. If there is some combination, then the statement is not a tautology, since you have found a way to make it false. The same is true for fallacies, setting the main connective TRUE.

Week 1: Tautology/Fallacy via Quick Method

Example

Is the following a tautology?

$$(p \wedge q) \rightarrow (t \wedge s)$$

$$\begin{array}{ccccccccccc}
(& p & \wedge & q &) & \rightarrow & (& r & \wedge & s &) \\
 & & & & & \mathrm{F} & & & & & \\
(& p & \wedge & q &) & \rightarrow & (& r & \wedge & s &) \\
 & & \mathrm{T} & & & & & & \mathrm{F} & & \\
(& p & \wedge & q &) & \rightarrow & (& r & \wedge & s &) \\
 & \mathrm{T} & & \mathrm{T} & & & & \mathrm{F} & & \mathrm{T} &
\end{array}$$

This is one choice of p, q, r, s that does make the statement false, so no it is not a tautology.

Week 1: Tautology/Fallacy via Quick Method

Example

Is the following a tautology?

$$[(p \to q) \wedge (q \to r)] \to (p \to r)$$

$$
\begin{array}{ccccccccccccccccccc}
[& (& p & \to & q &) & \wedge & (& q & \to & r &) &] & \to & (& p & \to & r &) \\
 & & & & & & & & & & & & & \color{blue}{F} & & & & & \\
[& (& p & \to & q &) & \wedge & (& q & \to & r &) &] & \to & (& p & \to & r &) \\
 & & & & & & \color{blue}{T} & & & & & & & & & & \color{blue}{F} & & \\
[& (& p & \to & q &) & \wedge & (& q & \to & r &) &] & \to & (& p & \to & r &) \\
 & & & \color{blue}{T} & & & & & & \color{blue}{T} & & & & & & \color{blue}{T} & & \color{blue}{F} & \\
[& (& p & \to & q &) & \wedge & (& q & \to & r &) &] & \to & (& p & \to & r &) \\
 & & \color{blue}{T} & & \color{red}{T} & & & & \color{red}{F} & & \color{blue}{F} & & & & & & & &
\end{array}
$$

For the statement to be false, q must be both true and false, a contradiction. Therefore, the statement is always true (tautology).

Homework. Make a truth table for this statement.

Example

Is the following a fallacy?

$$\sim [(p \to q) \to (\sim p \vee q)]$$

$\sim$	[	(	p	$\to$	q	)	$\to$	(	$\sim$	p	$\vee$	q	)	]
T														
$\sim$	[	(	p	$\to$	q	)	$\to$	(	$\sim$	p	$\vee$	q	)	]
							F							
$\sim$	[	(	p	$\to$	q	)	$\to$	(	$\sim$	p	$\vee$	q	)	]
				T							F			
$\sim$	[	(	p	$\to$	q	)	$\to$	(	$\sim$	p	$\vee$	q	)	]
				T					F			F		
$\sim$	[	(	p	$\to$	q	)	$\to$	(	$\sim$	p	$\vee$	q	)	]
			T		F					T				

The statement cannot be true, therefore, it is a fallacy.

- **Substitution Rule.** If in a tautology all instances of a variable are replaced by the same statement, it is still a tautology.

Example

$p \vee \sim p = T$, *so* $q \vee \sim q = T$ *and*
$[(p \vee q) \rightarrow r] \vee \sim [(p \vee q) \rightarrow r] = T$

- **Substitution of Equivalence.** If in a tautology we replace a statement with an equivalent statement, it is still a tautology.

Example

$p \equiv \sim (\sim p)$, *so* $(p \wedge q) \rightarrow r \equiv [\sim (\sim p) \wedge q] \rightarrow r$.

Two statements are **logically equivalent** if they have identical truth table values in every row.

Example

p	$\sim p$	$\sim(\sim p)$
T	F	T
F	T	F

The columns for p and $\sim(\sim p)$ are identical, so they are equivalent: $p \equiv \sim(\sim p)$.

Example

Simplify $\frac{1-\sin^2 x}{\cos x}$.

Using the identity $\sin^2 x + \cos^2 x = 1$, we get the following.

$$\cos^2 x = 1 - \sin^2 x$$

$$\frac{1-\sin^2 x}{\cos x} = \frac{\cos^2 x}{\cos x} = \cos x$$

Example

Given that $p \to q \equiv \sim p \vee q$ *and that* $q \to (p \to q) = T$*, prove that*

$$s \to (\sim r \vee s) = T.$$

$$\begin{aligned}
q &\to (p \to q) = T && \\
q &\to (r \to q) = T && \text{(Sub } r \text{ for } p\text{)} \\
s &\to (r \to s) = T && \text{(Sub } s \text{ for } q\text{)} \\
s &\to (\sim r \vee s) = T && \text{(Sub of equiv)}
\end{aligned}$$

Week 1: Equivalence Laws

1. Commutative

$$p \vee q \equiv q \vee p$$
$$p \wedge q \equiv q \wedge p$$
$$p \leftrightarrow q \equiv q \leftrightarrow p$$

2. Associative

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

3. Distributive

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

1. Double Negation

$$\sim\sim p \equiv p$$

2. De Morgan's Laws

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

3. Implication Laws

$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$
$$p \rightarrow q \equiv \sim p \vee q$$
$$p \rightarrow q \equiv \sim q \rightarrow \sim p$$
$$\sim(p \rightarrow q) \equiv p \wedge \sim q$$

Homework. Prove one example of each of the six categories of laws by truth table.

Example

Is $(p \wedge \sim q) \wedge (\sim p \vee q)$ a tautology or fallacy?

$$(p \wedge \sim q) \wedge (\sim p \vee q) \equiv (p \wedge \sim q) \wedge \sim (p \wedge \sim q) \quad \text{(De Morgan)}$$

This is of the form $r \wedge \sim r$, which we know is always false. Therefore, the statement is a fallacy.

Example

Is $(p \leftrightarrow q) \leftrightarrow (\sim p \leftrightarrow q)$ a tautology or fallacy?

$$\begin{aligned} (p \leftrightarrow q) \leftrightarrow (\sim p \leftrightarrow q) \equiv & (p \leftrightarrow \sim p) \leftrightarrow (q \leftrightarrow q) \quad \text{(Associative)} \\ & F \leftrightarrow T \\ & F \end{aligned}$$

The statement is a fallacy.

Example

Prove that $(p \to q) \to r \equiv [(\sim p \to r) \wedge (q \to r)]$.

Use the equivalence $s \to t \equiv \sim s \vee t$ (1).

$$\begin{aligned}
(p \to q) \to r &\equiv (\sim p \vee q) \to r && (1)\\
&\equiv \sim (\sim p \vee q) \vee r && (1)\\
&\equiv (\sim\sim p \wedge \sim q) \vee r && \text{(De Morgan)}\\
&\equiv (p \wedge \sim q) \vee r && \text{(Double Neg)}\\
&\equiv (p \vee r) \wedge (\sim q \vee r) && \text{(Distribution)}\\
&\equiv (\sim\sim p \vee r) \wedge (\sim q \vee r) && \text{(Double Neg)}\\
&\equiv (\sim p \to r) \wedge (q \to r) && \text{(1) twice}
\end{aligned}$$