



Proof by Induction

This topic is demonstrated mainly by example:

Example 1.1

Prove that $\forall x \forall y \forall z . x+(y+z) = (x+y)+z$

assuming only: i) $\forall x . 0 + x = x$

ii) $\forall x \forall y . (x+1) + y = (x+y) + 1$

iii) $\forall x . x = x$

iv) $\forall x \forall y . x + 1 = y + 1 \Rightarrow x = y$

Base case:

$$0+(y+z) = (0+y)+z$$

By rule i), $(y+z) = (y) + z$

$$y+z = y+z$$

True by rule iii)

Step case:

$$n+(y+z) = (n+y)+z \quad |-$$

$$(n+1)+(y+z) = ((n+1)+y)+z$$

By rule ii), $n+(y+z)+1 = ((n+y)+1)+z$

By rule ii), $n+(y+z)+1 = ((n+y)+z)+1$

By rule iv), $n+(y+z) = (n+y)+z$

True by hypothesis

Example 1.2

Prove that $\forall m \forall n . f(m + n, n) = m$

assuming usual facts about additions and:

i) $f(m, 0) = m$

ii) $f(m, n + 1) = p(f(m,n))$

iii) $p(0) = 0$

iv) $p(n + 1) = n$

Base Case:

$$f(m+0, 0) = m$$

By addition, $f(m,0) = m$

True by rule i)

Step case:

$$f(m+n, n) = m \quad |-$$

$$f(m+(n+1),n+1) = m$$

$$f(m+(n+1),n+1) = p(f(m+n+1, n)) = m$$

Work out what the function does! It returns the difference, as long as it is positive.

$$\text{So, } p(f(m+n+1, n)) = p(m+n+1-n) = p(m+1) = m$$

True.

Example 1.3

Prove that $2^0 + 2^1 + \dots + 2^{n-1} + 2^n = 2^{n+1} - 1$

Base case:

$$2^0 = 2^{0+1} - 1 = 1$$

True.

Step case:

$$2^0 + \dots + 2^n = 2^{n+1} - 1 \quad |-$$

$$2^0 + \dots + 2^n + 2^{n+1} = 2^{n+2} - 1$$

Using induction hypothesis:

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

$$2^{n+1} + 2^{n+1} = 2^{n+2}$$

$$2^{n+2} = 2^{n+2}$$

True.



Example 1.4

Prove that $\forall n . 3 \mid (n^3 - n)$ (\mid means "divides")

Base case:

$$3 \mid 0^3 - 0$$

$$3 \mid 0$$

True by definition.

Step case:

$$3 \mid (n^3 - n) \quad \mid-$$

$$3 \mid (n+1)^3 - (n+1)$$

$$\exists j . 3j = n^3 - n \quad \mid-$$

$$\exists k . 3k = (n+1)^3 - (n+1)$$

$$\exists k . 3k = n^3 + n^2 + 2n^2 + 2n + n + 1 - n - 1$$

$$\exists k . 3k = 3j + 3n^2 + 3n$$

$$\exists k . k = j + n^2 + n \text{ which is always an integer}$$

Example 1.5

Prove that $a^{m+n} = a^m \cdot a^n$

Base case:

$$a^{m+0} = a^m \cdot a^0$$

$$a^m = a^m$$

Step case:

$$a^{m+(n+1)} = a^m \cdot a^{n+1}$$

$$a^{(m+n)+1} = a^m \cdot a^n \cdot a$$

$$a \cdot a^{(m+n)} = a^m \cdot a^n \cdot a$$

$$a^{(m+n)} = a^m \cdot a^n$$

True by induction hypothesis

Example 1.6

Given the sequence given by $a_0 = 0$; $a_{n+1} = 2a_n + 1$, find a formula for a_n and prove it is correct.

n = 0	1	2	3	4	5
$a_n = 0$	1	3	7	15	31

$$a_n = 2^n - 1$$

Base case:

$$a_0 = 2^0 - 1 = 1 - 1 = 0$$

QED

Step Case:

$$a_n = 2^n - 1 \quad \mid-$$

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

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

Substitute in the sequence definition:

$$2a_n + 1 = 2 \cdot 2^n - 1$$

$$2a_n = 2 \cdot 2^n - 2$$

$$a_n = 2^n - 1$$

QED



Vectors

Equality

Vectors are equal if they are the same length, and each corresponding component is the same, i.e. $v = u \Leftrightarrow \forall i. v_i = u_i$, e.g. $(1, 3, 5) = (1, 3, 5)$ but $(2, 4, 6) \neq (4, 2, 6)$ and $(2, 4) \neq (2, 4, 6)$

Addition

Add corresponding components:

$$(u_i) + (v_i) = (u_i + v_i), \text{ e.g. } (2, 3, 5) + (5, 2, 6) = (8, 5, 11) \text{ and } ((1,2), (2,3)) + ((1,1), (3,2)) = ((2,3), (5,5))$$

Vector addition is commutative:

$$\begin{array}{ll} (u_i) + (v_i) & \\ (u_i + v_i) & \text{by vector addition} \\ (v_i + u_i) & \text{by vector equality} \\ (v_i) + (u_i) & \text{by vector addition, backwards.} \end{array}$$

and associative.

Unary Minus and Subtraction

$$-(u_i) = (-u_i), \text{ e.g., } -(2,4,5) = (-2, -4, -5)$$

Vector subtraction is defined as $(u_i - v_i) = (u_i) + (-v_i)$ or $(u_i) - (v_i) = (u_i - v_i)$

Vector subtraction is *not* commutative or associative.

Scalar Product

$$k(v_i) = (kv_i), \text{ e.g. } 2(1,2,5) = (2,4,10)$$

It follows, therefore, that scalar multiplication by -1 is equivalent to unary minus.

$$\text{Scalar multiplication distributes across addition, e.g. } 3((2, 1) + (7, -2)) = 3(2, 1) + 3(7, -2) = (6, 3) + (21, -6) = (27, -3)$$

Delta Vectors and Coordinate Systems

A vector, δ_i , is vector with 1 in the i th position, and 0s everywhere else.

Hence, any vector can be expressed as a *linear combination* - a sum of scalar multiples of δ vectors, e.g., $(3, 4, 5) = 3(1, 0, 0) + 4(0, 1, 0) + 5(0, 0, 1) = 3\delta_1 + 4\delta_2 + 5\delta_3$

This is called a *co-ordinate system*. Such a system can be constructed with vectors other than δ vectors, e.g., $(3, 4, 5) = -3(1, -1, 0) + 6(1, 0, -1) + 1(0, 1, -1)$

Example 2.1

Prove that $(1, -1, 0)$, $(1, 0, 1)$ and $(0, 1, -1)$ form a co-ordinate system:

$$(x, y, z) = a(1, -1, 0) + b(1, 0, 1) + c(0, 1, -1)$$

$$1: \quad x = a + b$$

$$2: \quad y = c - a$$

$$3: \quad z = b - c$$

$$\text{Adding 1, 2 and 3:} \quad x + y + z = 2b \quad b = (x+y+z)/2$$

$$\text{Adding 2 and 3: } y + z = b - a \quad \text{then subtract 1 } y + z - x = -2a \quad a = (x - y - z)/2$$

$$\text{From 2:} \quad c = y + a \quad c = y + (x-y-z)/2 \quad 2c = 2y + (x-y-z) \quad c = (x+y-z)/2$$

Inner ('Dot') Product

Is defined as $(u_i) \cdot (v_i) = \sum_i u_i v_i$, e.g., $(2, 3) \cdot (3, -1) = 2 \cdot 3 + 3 \cdot -1 = 6 - 3 = 3$

Inner product is commutative, $u \cdot v = v \cdot u$

Scalar multiplication commutes with inner product, $(ku) \cdot v = k(u \cdot v)$

Inner product distributes over vector addition, $u \cdot (v + w) = (u \cdot v) + (u \cdot w)$

$$0 \cdot v = v \cdot 0 = 0$$

$$v_i = v \cdot \delta_i, \text{ e.g., } 3 = (1, 3, 5) \cdot (0, 1, 0) = 3$$

Magnitude

The magnitude of a vector, $v = |v| = \sqrt{(v \cdot v)}$, e.g. $|(1,2,3)| = \sqrt{(1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3)} = \sqrt{14}$

$|ku| = k|u|$ if k is positive

Vectors with magnitude 1, are called *unit vectors*.



Matrices

Equality

Matrices are equal if they are the same size and each corresponding element is the same.

Addition

Add together the corresponding elements, e.g.,

$$\begin{matrix} 1, 2, 4 \\ 3, 6, 2 \end{matrix} + \begin{matrix} 4, 2, 5 \\ 5, 2, 3 \end{matrix} = \begin{matrix} 5, 4, 9 \\ 8, 8, 5 \end{matrix}$$

Scalar Multiplication

Multiply each element by the scalar factor, e.g.,

$$2 \begin{matrix} 1, 3, 2 \\ 2, 4, 1 \end{matrix} = \begin{matrix} 2, 6, 4 \\ 4, 8, 2 \end{matrix}$$

Matrix Multiplication

Let A be an m×n matrix and B be an n×p matrix. Then the product of A and B is the m×p matrix C whose (i,j)th entry is given by:

$$C_{ij} = \sum_{k=1}^n a_{ik} b_{kj} \quad \text{for } i = 1..m \text{ and } j = 1..p.$$

The product AB is only defined if the number of columns of A is the same as the number of rows of B. AB and BA may not both be defined. If they both do exist, they are not necessarily equal and might not even be of the same size.

Eg.,

$$\begin{matrix} a, b \\ c, d \end{matrix} * \begin{matrix} e, f \\ g, h \end{matrix} = \begin{matrix} ae+bg, af+bh \\ ce+dg, cf+dh \end{matrix}$$

So,

$$\begin{matrix} 2, 3 \\ -1, 3 \end{matrix} * \begin{matrix} 0, 1 \\ 2, 3 \end{matrix} = \begin{matrix} 2*0+3*2, & 2*1+3*3 \\ -1*0+3*2, & -1*1+3*3 \end{matrix} = \begin{matrix} 6, 11 \\ 6, 8 \end{matrix}$$

Second matrix must have same number of columns as the first matrix has rows.

Matrix multiplication is associative = A(BC) = (AB)C

Matrix multiplication commutes with scalar multiplication = (kA)B = k(AB)

Matrix multiplication distributes over addition = A(B+C) = AB + AC

Note that AB does not always equal BA.

Multiplication by the zero matrix results in the zero matrix.

Square Matrices

The sum of n×n matrices is an n×n matrix.

The scalar multiple of an n×n matrix is an n×n matrix.

The multiplication of two n×n matrices is an n×n matrix.

Diagonal Matrices

The diagonal of an n×n matrix is the vector A_{ii} (length n), i.e. the diagonal of 1, 4, 3 is (1, 4, 2).

$$\begin{matrix} 2, 4, 2 \\ 4, 5, 2 \end{matrix}$$

A *diagonal matrix* is one where the diagonal values are the only non-zero elements.

The sum of diagonal n×n matrices is a diagonal n×n matrix.

A scalar multiple of a diagonal n×n matrix is a diagonal n×n matrix

The multiple of two n×n matrices is an n×n matrix.

Identity Matrices

An *identity matrix* is a diagonal matrix with a the diagonal elements all set to 1. Often represented by I.



Revision Notes

Invertible Matrices

A matrix, A, is *invertible* if there exists a matrix, B, such that $AB = BA = I$.

B is called the *inverse* of A, and is written A^{-1}

Any matrix has only *one* inverse.

There is a formula for working out the inverse of a matrix:
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{(ad-bc)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Determinants

The determinant of a 2x2 matrix, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is written $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ and defined as $ad - bc$.

Determinants of larger matrices can be defined:

$$\begin{vmatrix} a & b & c \\ d & e & f \\ g & h & i \end{vmatrix} = a \cdot \begin{vmatrix} e & f \\ h & i \end{vmatrix} - b \cdot \begin{vmatrix} d & f \\ g & i \end{vmatrix} + c \cdot \begin{vmatrix} d & e \\ g & h \end{vmatrix}$$

Note: alternating + and -, and each top row component is multiplied by the determinant of the matrix given by the elements not in the same row or column as the top row element.

$$|I| = 1$$

$$|AB| = |A| |B|$$

$|A| = 0$ iff A is not invertible.

If A is invertible, $|AA^{-1}| = 1$.

Transposition

The *transpose* of a matrix is the matrix produced by switching around the rows and columns so the first row becomes the first column, the second row becomes the second column, etc., e.g.,

$$\begin{pmatrix} 0 & 1 \\ 4 & 2 \\ 3 & 2 \end{pmatrix}^T = \begin{pmatrix} 0 & 4 & 3 \\ 1 & 2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 4 & 2 \\ 3 & 2 \end{pmatrix}^T = \begin{pmatrix} 4 & 3 \\ 2 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 2 \end{pmatrix}^T = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

Formally, $(A^T)_{ij} = A_{ji}$

Properties:

$$(A+B)^T = A^T + B^T$$

$$(AB)^T = B^T A^T$$

For a diagonal matrix, D, $D^T = D$

$$(A^T)^T = A$$

Transposition commutes with inverse: $(A^{-1})^T = (A^T)^{-1}$

Triangular Form

A matrix is *upper triangular* if all elements below the main diagonal are 0.

Formally, $i > j$ implies that $A_{ij} = 0$.

The sum of two upper triangular matrices is an upper triangular matrix.

The scalar multiple of an upper triangular matrix is an upper triangular matrix.

The product of two upper triangular matrices is an upper triangular matrix.



Solving Simultaneous Equations with Matrices

Taking the example, $2x + 3y = 1$
 $-x + 2y = 3$

These can be re-written in matrix form as $\begin{pmatrix} 2 & 3 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$

Multiplying both sides by $\begin{pmatrix} 2 & 3 \\ -1 & 2 \end{pmatrix}^{-1}$ gives

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ -1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Using the formula for finding the inverse of a matrix:

$$\begin{pmatrix} 2 & 3 \\ -1 & 2 \end{pmatrix}^{-1} = \frac{1}{\det} \begin{pmatrix} 2 & -3 \\ 1 & 2 \end{pmatrix}$$

$$\text{So, } \begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 2 & -3 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{7} \begin{pmatrix} 2+(-9) \\ 1+6 \end{pmatrix} = \frac{1}{7} \begin{pmatrix} -7 \\ 7 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

So $x = -1, y = 1$.

A More General Technique - Gaussian Elimination

If the determinant of the matrix representing the coefficients is 0, the pair of equations either have infinitely many solutions or none at all. If it is 1, there is a single solution, if it is anything else, there are several solutions.

Often, equations such as the ones above are represented not by two separate matrices - one for the coefficients and one for the rhs of the equation, but in a single *augmented* matrix:

$$\begin{pmatrix} 2 & 3 & 1 \\ -1 & 2 & 3 \end{pmatrix}$$

It would be much easier if the lhs of the augmented matrix was in upper triangular form, i.e.

$$\begin{aligned} x + 2y - z &= 8 \\ 3y + z &= 5 \\ 3z &= 6 \end{aligned}$$

Gaussian elimination involves reducing an augmented matrix into upper triangular form. Just like in normal equation manipulation, you may i) multiply a row by a non-zero factor, ii) add/subtract two rows and iii) swap two rows.



Revision Notes

Illustrated by example:

$$\begin{aligned} x + 2y - z &= 8 \\ 2x + 3y + z &= 5 \\ x - 2y - 3z &= 6 \end{aligned}$$

$$\begin{array}{cccc} 1 & 2 & -1 & 8 \\ 2 & 3 & 1 & 5 \\ 1 & -2 & -3 & 6 \end{array}$$

Swap A and B:

$$\begin{array}{cccc} 2 & 3 & 1 & 5 \\ 1 & 2 & -1 & 8 \\ 1 & -2 & -3 & 6 \end{array}$$

Multiply B and C by 2:

$$\begin{array}{cccc} 2 & 3 & 1 & 5 \\ 2 & 4 & -2 & 16 \\ 2 & -4 & -6 & 12 \end{array}$$

Subtract 1 from B and C:

$$\begin{array}{cccc} 2 & 3 & 1 & 5 \\ 0 & 1 & -3 & 11 \\ 0 & -7 & -7 & 7 \end{array}$$

Divide C by 7:

$$\begin{array}{cccc} 2 & 3 & 1 & 5 \\ 0 & 1 & -3 & 11 \end{array}$$

Add B to C:

$$\begin{array}{cccc} 2 & 3 & 1 & 5 \\ 0 & 1 & -3 & 11 \\ 0 & 0 & -4 & 12 \end{array}$$

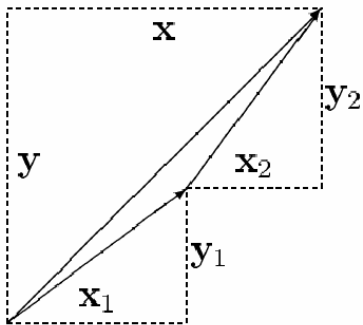
It is possible to divide C by 4:

$$\begin{array}{cccc} 2 & 3 & 1 & 5 \\ 0 & 1 & -3 & 11 \\ 0 & 0 & -1 & 3 \end{array}$$

And that's it!

$$\begin{array}{cccc} 0 & -1 & -1 & 1 \end{array}$$

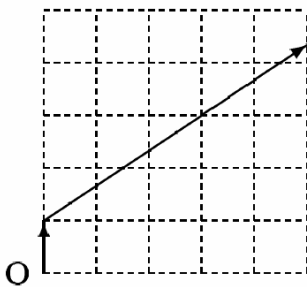
Vectors and Geometry



Adding two vectors, $(x_1 \ y_1)$ and $(x_2 \ y_2)$:

Scalar product simply increases the length, but not the direction, of a vector.

Parametric equation of a vector:



This vector can be represented by the equation
$$\begin{matrix} x & = & 0 & + & t & 3 \\ y & & 1 & & & 2 \end{matrix}$$

This is related to the standard $y = mx + c$ equation in that the y-intercept, c is 1 and the gradient, m is $2/3$: $y = 2x/3 + 1$

Inner Product:

$a \cdot b = |a| |b| \cos \theta$ where θ is the angle between the two vectors.

N.B. $a \cdot b = 0$ means a and b are at right angles.

A Circle is represented by the equation $|p - c| = r$ where p is a vector whose magnitude is the radius of the circle and c is the centre of the circle.

Transformations

A mapping of the form $T: v \rightarrow v + c$ for a fixed vector c is a *translation*.

A mapping of the form $L: v \rightarrow Av$ for a fixed vector A is a *linear mapping*.

Linear mappings have the following properties:

Distribution over addition: $L(u+v) = A(u+v) = Au + Av = L(u) + L(v)$

Distribution over scalar multiplication: $L(ku) = A(ku) = k(Au) = kL(u)$

Preservation of the origin: $L(0) = A(0) = 0$

Preservation of lines - if the entire line is not preserve, the mapping is not linear.



Revision Notes

Matrices for various transformations can be evolved from looking at the effects of a translation on unit points, i.e., to find a matrix for reflection in the y-axis: the image produced by performing this translation on the x unit vector, 1 is -1 and the image for the y unit vector 0 is 0 hence the matrix is

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

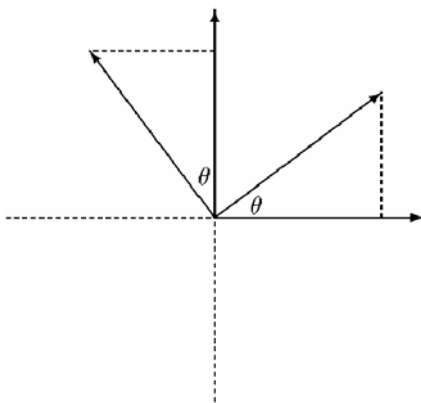
Rotation: Again, by looking at the effect of rotation on the unit vectors, the matrix for a 90° clockwise rotation is

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

180° is accordingly

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

To find the matrix for a general anti-clockwise rotation of θ :



The vector 1 would be moved to $\cos \theta$ and 0 to $-\sin \theta$

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

Hence for any anticlockwise rotation, θ , the matrix is:

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

What about a rotation about a point other than the origin? E.g., 90° anticlockwise about (1, 1): Break the operation into the following steps: First perform a translation of $-(1, 1)$. Then perform the rotation, then translate back using (1, 1):

$$T(u) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (u - \begin{pmatrix} 1 \\ 1 \end{pmatrix}) + \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Similarly, a reflection in the line $x + y = 0$ can be seen as a clockwise rotation of 45° about the origin (to map the reflecting line onto the y axis), followed by a reflection in the y axis and then an anticlockwise rotation 45° about the origin.



Graph Theory

A Graph, G , is a pair (V, E) where V is a set of vertices (nodes) and E is a set of unordered pairs of distinct edges.

If a edge joins two vertices, these vertices are *adjacent*.

The *endpoints* of an edge are the two nodes it connects.

An endpoint of an edge is said to be *incident* on that edge.

The *degree* of a vertex is the number of edges incident on it. As every edge has two endpoints, it makes sense that $\sum \text{deg}(v) = 2 |E|$.

A *walk* is a sequence of alternating vertices and edges such that $e_i = \{v_{i-1}, v_i\}$

There are several special types of walk:

- A *closed walk* is one where the first vertex is the same as the last.
- A *path* is one where every vertex is distinct
- A *trail* is one where every edge is distinct
- A *cycle* is a closed walk where every vertex (except the first/last) is distinct. A k -cycle is a cycle of length k (n.b. that the first and last vertex count as one).

Any walk can be made into a path - just remove any cycles.

A *subgraph*, g , of a graph $G = (V, E)$, is a pair (v, e) such that every vertex of g is also a vertex of G and every edge of g is also an edge of G . The endpoints of every edge in e must be members of v .

This last condition ensures that a subgraph is itself a graph.

A subgraph generated by a set of vertices (i.e. those vertices and all edges joining them) is represented by $G \setminus v$ - the graph G once the vertex v and all edges involving v have been removed.

A graph is *connected* if there is a path between any two vertices.

Any graph can be viewed as a collection of connected subgraphs. Looking at all pairs of vertices, u and v such that there is a path from u to v , we can define an equivalence relation on these vertices:

Reflexivity: There is a path, length 0, from every vertex to itself.

Symmetry: If there is a path from u to v , there is a path from v to u .

Transitivity: If there is a path from u to w and from w to v then there is a path from u to v .

A vertex, v , is a *cut point* if $G \setminus v$ is disconnected.

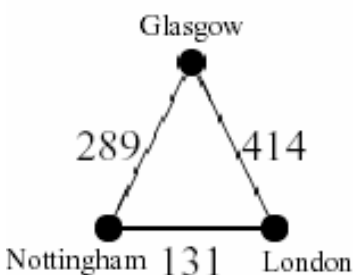
A *Complete Graph* is every vertex is connected to every other by a single edge.

A *Regular Graph* is one where every vertex has the same degree.

A *Bipartite Graph* is one where the set of vertices can be seen as the disjoint union of two sets, L and R , such that every edge connects a vertex in L to one in R .

Labelled Graphs

The nodes and edges of graphs can be labelled to provide extra information.





For example,

n → "Nottingham" {n,l} → 131

l → "London" {l,g} → 414

g → "Glasgow" {g,n} → 298

denotes this graph:

Tree Graphs

A *Forest* is a graph with no cycles (acyclic). A *Tree* is a connected acyclic graph. Hence, the connected components of a forest, is a tree.

A *Spanning Tree* of a graph, G, is both a tree and a sub-graph of G.

Rooted Trees have a single nodes specified as the root. The length of the unique path from the root to another node, v, is called the *level* of v. The *depth* of the tree is length of the longest path starting at the root.

Directed graphs are those where the edges are given a direction (or orientation). They are represented by *ordered pairs* of vertices. The *indegree* of a vertex is the number of edges that end with that vertex (how many edges go into that vertex). The *outdegree* of a vertex is the number of edges that start with that vertex. A vertex with an indegree of 0 is called a *source*. A vertex with a zero outdegree is called a *sink*.

As every edge has one start and one end, $\sum_v \text{indegree}(v) = |E| = \sum_v \text{outdegree}(v)$.

Directed Walks

A directed walk from a vertex v_0 to v_n consists of alternating vertices and edges, such that $e_i = (v_{i-1}, v_i)$.

A directed semiwalk between the same vertices consists of alternating vertices and edges, such that $e_i = (v_{i-1}, v_i)$ OR $e_i = (v_i, v_{i-1})$.

For any graph, if, for any pair of vertices, u and v, there is a semipath from u to v then the graph is *weakly-connected*. If there is a path from u to v OR a path from v to u, the graph is *unilaterally-connected*. If there is a path from u to v AND v to u, the graph is *strongly-connected*.



Combinatorial Analysis and Probability

- If one event can result in *either* n ways *or* m ways, the total ways it can occur is $n+m$
- If one event can result in n ways and a subsequent event can happen in m ways, there are $m.n$ ways in which they can both occur.

Factorials

How many 8 letter anagrams are there of the word 'computer'?

There are 8 possible choices for the first letter, 7 for the second, 6 for the third, etc., so the answer is $8*7*6*5*4*3*2*1 = 8! = 40,320$

Permutations - ordered combinations

How many four letter words can be constructed from the word 'computer'?

Again, 8 choices for the first letter, 7 for the second, etc., so the answer is $8*7*6*5 = 8!/4! = {}_8P_4 = 1,680$.

nPr is also used when considering a group of object when some are identical, e.g., anagrams of the word 'banana' - a six letter word but only 3 are distinct. Hence, the number of 6 letter anagrams of 'banana' is ${}_6P_3 = 60$

Combinations

When the order of elements do not matter, use nCr .

Each national lottery ticket has six numbers taken from [1..49]. Total number of tickets is:

$${}_{49}P_6 / 6! = {}_{49}C_6 = 13,983,816.$$

$${}_nC_r = {}_nC_{n-r}$$

Binomial Coefficients

The expansion of terms of the form $(a + b)^n$ can be expressed using nCr .

First write down a sequence of $a^x b^y$ with x starting at n at decreasing one by one, while simultaneously, y starts at 0 and increases by one each time. Then multiply each term by nCy .

$$\text{E.g., } (a+b)^4 = {}_4C_0 a^4 b^0 + {}_4C_1 a^3 b^1 + {}_4C_2 a^2 b^2 + {}_4C_3 a^1 b^3 + {}_4C_4 a^0 b^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

Probability

The ratio s/n where n is the number of times an experiment is performed and s is the number of times a result occurred. It is called the *Relative Frequency*. $P(X) = \lim_{n \rightarrow \infty} s/n$

The set S of all possible outcome from a particular experiment is called the *sample space* of the experiment. Subsets of S are called events.

The empty set, \emptyset , is called the *impossible event*.

A singleton, $\{x\} \subseteq S$ is called an *atomic* or *elementary* event.

If A and B are events, $A \cup B$ is the event that occurs when the outcome appears in *either* A or B .

If A and B are events, $A \cap B$ is the event that occurs when the outcome appears in both A and B .

If $A \cap B = \emptyset$, A and B are *mutually exclusive*.

If $S_1 \dots S_n$ are events and $S_1 \cup \dots \cup S_n = S$ then the events $S_1 \dots S_n$ are *exhaustive*.

A *Probability Space* is a sample space and a function P mapping each element to a corresponding probability. If P of each element is the same, the space is said to be *equiprobable*.

$P(A \setminus B)$ is the probability of an event that is in A but not in B . $P(A \setminus B) = P(A) - P(A \cap B)$.

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Hence, if the events A and B are mutually exclusive, $P(A \cup B) = P(A) + P(B)$

$P(A|E)$ means the probability of A happening given that E has already happened.

$$P(A|E) = \frac{P(A \cap B)}{P(E)}$$

If $P(A|E) = P(A)$ then the events, A and E are mutually exclusive. Hence, $P(A \cap B) = P(A) \cdot P(B)$



Program Correctness

Partial Correctness

- correspondence between implementation and specifications
- if the program ends normally, we know certain properties of the final state.

Termination

- Program must end normally for input states for which the initial properties hold.

Partial Correctness + Termination = Total Correctness

Hoare Triples

{Preconditions} Statements {Postconditions}

A triple is valid if, for inputs that hold for the preconditions, after the statements are executed, the postconditions hold

Inference Systems

Consists of axioms and rules of inference. A proof is a sequence of formulae where each formula is either an axiom or can be derived from axioms or previous formulae by application by rules of inference.

The Assignment Axiom

$\{e = 12\} x := e \{x=12\}$

Whatever is true about a e before we do an assignment is true about x afterwards.

Rule of Composition

If the postconditions of one triple are the same as the preconditions of a following triple, the two can be glued together:

$\{P\}S_1\{Q\}, \{Q\}S_2\{R\}$ gives $\{P\}S_1S_2\{R\}$

Rule of Consequence - Strengthening

Given $\{Q\}S\{R\}$ and $P \Rightarrow Q$ we can infer $\{P\}S\{R\}$

We know that $y > 5 \Rightarrow y + 5 > 10$ so

from $\{y+5 > 10\} x := y + 5 \{x > 10\}$

we can infer $\{y > 5\} x := y + 5 \{x > 10\}$

Rule of Consequence - Weakening

Given $\{P\}S\{Q\}$ and $Q \Rightarrow R$ we can infer $\{P\}S\{R\}$

Since $x > 112 \Rightarrow x > 0$

from $\{x > 100\} x := x + 12 \{x > 112\}$

we can infer $\{x > 100\} x := x + 12 \{x > 0\}$

Ghost Variables

Used to 'remember' intermediate values, i.e.:

$\{x = X \ \& \ y = Y\}$

$x := x + x$

$\{x = 2X\}$

Rule for if-then-else

Given $\{P \ \& \ B\}S_1\{Q\}$ and $\{P \ \& \ \neg B\}S_2\{Q\}$ we can infer $\{P\}$ if B then S_1 else $S_2 \{Q\}$

Rule for while

Given $\{P \ \& \ B\}S\{P\}$ we can infer $\{P\}$ while B do S $\{P \ \& \ \neg B\}$