mathcentre

For the help you need to support your course

Mathematics for Computer Science Facts & Formulae

mathcentre is a project offering students and staff free resources to support the transition from school mathematics to university mathematics in a range of disciplines.

www.mathcentre.ac.uk

This leaflet has been produced in conjunction with the Higher Education Academy Maths, Stats & OR Network, and sigma.

For more copies contact the Network at **info@mathstore.ac.uk**

sigma — centre for excellence in mathematics & statistics support

The Higher Education Academy — Maths, Stats & OR Network

Truth tables

not P

P	$\sim P$
T	F
F	T

P **and** Q

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P **or** Q

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P **xor** Q

P	Q	$P \underline{\vee} Q$
T	T	F
T	F	T
F	T	T
F	F	F

if P **then** Q

P	Q	$P \Longrightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P **if and only if** Q

P	Q	$P \Longleftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Propositions and predicates: A **proposition**, P, is a statement that has a truth value, i.e. it is either true (T) or false (F). Thus, for example, the statement P: *the earth is flat* is a proposition with truth value F. A **compound proposition** is one constructed from elementary propositions and logical operators, e.g. $P \wedge (Q \vee R)$ is a compound proposition constructed from the propositions P, Q and R.
A compound proposition which is always true is called a **tautology**. A compound proposition which is always false is called a **contradiction**. Two compound propositions which are constructed from the same set of elementary propositions are said to be **logically equivalent** if they have identical truth tables.

A **predicate**, $P(x)$, is a statement, the truth value of which depends on the value assigned to the variable x. Thus, for example $P(x): x^2 - 3 > 0$ is a predicate.

Quantifiers: $\forall$, for all (sometimes called the **universal quantifier**). $\exists$, there exists (sometimes called the **existential quantifier**). Quantifiers convert predicates to propositions. The proposition $\exists x\, P(x)$ is true if there exists at least one value of x for which $P(x)$ is true. The proposition $\forall x\, P(x)$ is true if $P(x)$ is true for every value of x.

Algorithms

Suppose we have two positive integers m, n, with m greater than n. When m is divided by n, the result is a whole number part plus a remainder. For example given 16 and 5, then $\frac{16}{5} = 3$, remainder 1. The number 3 is called the **quotient**, 1 is called the **remainder**, and 5 is called the **divisor**.

Algorithm to convert decimal to binary
Step 1: Divide the number by 2. Retain the quotient and record the remainder.
Step 2: If the quotient in Step 1 is 0 then stop.
Step 3: If the quotient in Step 1 is not 0 go to Step 1 using the quotient as the number which is divided by 2.
The binary representation of the initial decimal number is given by the remainders in the reverse order to that in which they were obtained.

Euclid's Algorithm for the Greatest Common Divisor of two positive integers a **and** b**, GCD**(a, b)
Step 1: Divide the larger of the two integers by the smaller.
Step 2: If the remainder is zero then stop, the GCD(a, b) is the divisor.
Step 3: If the remainder is not zero then divide the divisor by the remainder and go to Step 2.

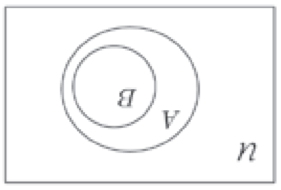
Prim's Algorithm for the minimum spanning tree in a network of n **vertices.**
Step 1: Choose any vertex. Choose the edge of shortest length incident on this vertex. Call this graph P.
Step 2: Choose the edge (i, j) with the shortest length amongst all the edges (i, k) where i is in P and k is not in P. Add this edge to P. (If there are multiple edges of the same shortest length then choose one of them arbitrarily.)
Step 3: If P has $n - 1$ edges then stop - it is a minimal spanning tree, otherwise go to Step 2.

Binary Search Algorithm to find an element x **in an ordered list** L **made up of** n **elements** $a_1 < a_2 < \ldots < a_n$.
Step 1: Check if x is greater than the middle element of the list L. If this is true then set this upper half of the list to be the new search list L. If false set the lower half of the list to be the new search list.
Step 2: If there is only one element a_L remaining in the list then stop. If $x = a_L$ the element is found. If $x \neq a_L$ the element is not in the list.
Step 3: If there is more than one element in the list then go to step 1.

Bubble Sort Algorithm to arrange an unordered list of n **numbers** $a_1, a_2, \ldots a_n$ **in ascending order.**
Step 1: Set counter $j = 2$.
Step 2: From $i = n$ to j , if $a_i < a_{i-1}$ swap a_i and a_{i-1}.
Step 3: Increase counter value j by 1.
Step 4: If $j = n$ stop, the list is sorted, otherwise go to step 2.

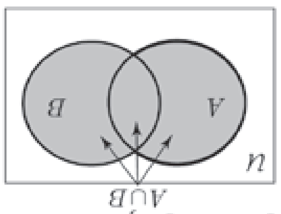
Sets and Venn Diagrams

Empty & Universal Sets
The **empty** or **null** set: $\emptyset$ is the set that contains no elements.
The **universal** set, $\mathcal{U}$ or $\mathcal{E}$: the set that contains all the elements being considered in a particular problem.
Set membership
If an element x is a member of the set X we write $x \in X$.
Subsets
Set B is a subset of A (written $B \subseteq A$) if every element of B is an element of A, i.e. if $x \in B$ then $x \in A$. If $B \subseteq A$ and $B \neq A$ then we write $B \subset A$ and B is said to be a **proper subset** of A. The empty set is a subset of every set.



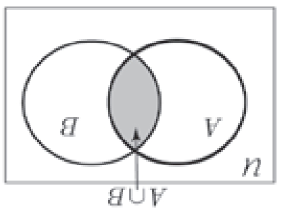
Equality of sets
$A = B$ if and only if $A \subseteq B$ and $B \subseteq A$.
Union
$A \cup B = \{x : x \in A \text{ or } x \in B\}$.

$A \cup B$



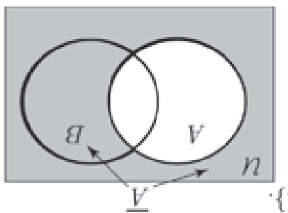
Intersection
$A \cap B = \{x : x \in A \text{ and } x \in B\}$.

$A \cap B$



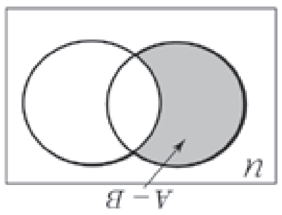
Complement
$\overline{A} = \{x : x \notin A\}$.

$\overline{A}$



Set difference (or complement of B **relative to** A**)**
$A - B$ (or $A \backslash B$) $= \{x : x \in A \text{ and } x \notin B\}$.

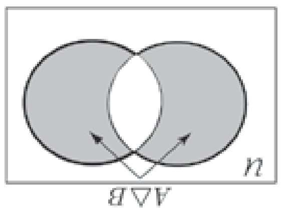
$A - B$



Symmetric difference

$$A \triangle B = (A \cup B) - (A \cap B)$$
$$= \{x : (x \in A \text{ and } x \notin B) \text{ or } (x \notin A \text{ and } x \in B)\}$$

$A \triangle B$



Cartesian Product
$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$

Union and intersection of an arbitrary number of sets

$$\cup_{i=1}^{n} A_i = A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n$$

$$\cap_{i=1}^{n} A_i = A_1 \cap A_2 \cap A_3 \cap \ldots \cap A_n$$

Power set
The **power set**, $P(X)$, of a set X is the set of all subsets (including the empty set) of X. For example, if $X = \{a, b, c\}$ then
$P(X) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}, \emptyset\}$.
Set cardinality
$|A|$ = the **cardinality** of the set A, that is, the number of distinct elements of the set. So if $A = \{1, 2, 3, 3, 8\}$ then $|A| = 4$.

For any sets A, B, C and X,
$|A \cup B| = |A| + |B| - |A \cap B|$.
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B|$
$\qquad - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.
$|A \times B| = |A||B|$
$|P(X)| = 2^n$ where $n = |X|$.

v1. June 2008
primary content by Mark McCartney. Series edited and typeset by Tony Croft.

Commonly used sets

$\mathbb{N}$ - the set of natural numbers $\{1, 2, 3, \ldots\}$.
$\mathbb{Z}$ - the set of integers, $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
$\mathbb{Q}$ - the set of rational numbers, $\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$.
Examples of rational numbers are:
$-\frac{3}{4}$, $7 = \frac{7}{1}$, $0.21 = \frac{21}{100}$, $\frac{22}{7}$.
$\mathbb{R}$ - the set of real numbers, i.e. {all numbers expressible as finite or infinite decimal expansions}.
Examples of real numbers are:
$-\frac{3}{4}$, 7, 0.21, $\frac{22}{7}$, π, $\sqrt{2}$.
$\mathbb{C}$ - the set of complex numbers $\{x + \sqrt{-1}\, y \ : x, y \in \mathbb{R}\}$.

Set Algebra

$A \cup B = B \cup A$ $A \cap B = B \cap A$	commutativity
$A \cup (B \cup C) = (A \cup B) \cup C$ $A \cap (B \cap C) = (A \cap B) \cap C$	associativity
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	distributivity
$A \cup \emptyset = A$ $A \cap \mathcal{U} = A$	identity
$A \cup \overline{A} = \mathcal{U}$ $A \cap \overline{A} = \emptyset$ $\overline{\overline{A}} = A$	complementarity
$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$	absorption
$(A \cap B) \cup (A \cap \overline{B}) = A$ $(A \cup B) \cap (A \cup \overline{B}) = A$	minimization
$\overline{A \cup B} = \overline{A} \cap \overline{B}$ $\overline{A \cap B} = \overline{A} \cup \overline{B}$	de Morgan's laws
$A \cup A = A$ $A \cap A = A$	idempotency

Logic

$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	commutativity
$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	associativity
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	distributivity
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	absorption
$\sim (p \vee q) \equiv (\sim p) \wedge (\sim q)$ $\sim (p \wedge q) \equiv (\sim p) \vee (\sim q)$	de Morgan's laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	idempotency

Alternative notations for negation: $\neg p$, $\overline{p}$

Algebra

$$(x+k)(x-k) = x^2 - k^2$$

$$(x+k)^2 = x^2 + 2kx + k^2, \quad (x-k)^2 = x^2 - 2kx + k^2$$

$$x^3 \pm k^3 = (x \pm k)(x^2 \mp kx + k^2)$$

Formula for solving a quadratic equation:

$$\text{if } ax^2 + bx + c = 0 \text{ then } x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Laws of Indices:

$$a^m a^n = a^{m+n} \qquad \frac{a^m}{a^n} = a^{m-n} \qquad (a^m)^n = a^{mn}$$

$$a^0 = 1 \qquad a^{-m} = \frac{1}{a^m} \qquad a^{1/n} = \sqrt[n]{a} \qquad a^{\frac{m}{n}} = (\sqrt[n]{a})^m$$

Laws of Logarithms:

For any positive base b (with $b \neq 1$)

$$\log_b A = c \quad \text{means} \quad A = b^c$$

$$\log_b A + \log_b B = \log_b AB, \qquad \log_b A - \log_b B = \log_b \frac{A}{B},$$

$$n \log_b A = \log_b A^n, \qquad \log_b 1 = 0, \qquad \log_b b = 1$$

Formula for change of base: $\log_a x = \dfrac{\log_b x}{\log_b a}$

Logarithms to base e, denoted $\log_e$ or alternatively ln are called *natural logarithms*. The letter e stands for the exponential constant which is approximately 2.718.

Useful Symbols and Notations

$a \mid b$	a divides b
$a \not\mid b$	a does not divide b
$a \bmod b$	remainder when a is divided by b
$\lfloor x \rfloor$	floor of x; the greatest integer less than or equal to x
$\lceil x \rceil$	ceiling of x; the smallest integer greater than or equal to x
$\gcd(a,b)$	greatest common divisor of a and b
$\operatorname{lcm}(a,b)$	least common multiple of a and b
$P \equiv Q$	P and Q are logically equivalent
$\sum_{i=1}^{n} a_i$	$= a_1 + a_2 + \ldots + a_{n-1} + a_n$
$\prod_{i=1}^{n} a_i$	$= a_1 \times a_2 \times \ldots \times a_{n-1} \times a_n$
$\sum_{i \in S} a_i$	the sum of the elements in the set $\{a_i : i \in S\}$
$\prod_{i \in S} a_i$	the product of the elements in the set $\{a_i : i \in S\}$

For example, if S is the set of odd integers between 0 and 10, and $a_i = i$ then $\sum_{i \in S} a_i = 1+3+5+7+9 = 25$ and

$$\prod_{i \in S} a_i = 1 \times 3 \times 5 \times 7 \times 9 = 945.$$

Sequences and Series

Arithmetic progression:

$$a, a+d, a+2d, \ldots$$

a = first term, d = common difference,
kth term $= a + (k-1)d$.
Sum of n terms,

$$S_n = \frac{n}{2}(2a + (n-1)d)$$

Sum of the first n integers:

$1 + 2 + 3 + \ldots + n =$

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

Sum of the squares of the first n integers:

$1^2 + 2^2 + 3^2 + \ldots + n^2 =$

$$\sum_{k=1}^{n} k^2 = \frac{1}{6}n(n+1)(2n+1)$$

Geometric progression:

$$a, ar, ar^2, \ldots$$

a = first term, r = common ratio,
kth term $= ar^{k-1}$
Sum of n terms,

$$S_n = \frac{a(1-r^n)}{1-r}, \text{ provided } r \neq 1$$

Sum of an infinite geometric series:

$$S_\infty = \frac{a}{1-r}, \quad -1 < r < 1$$

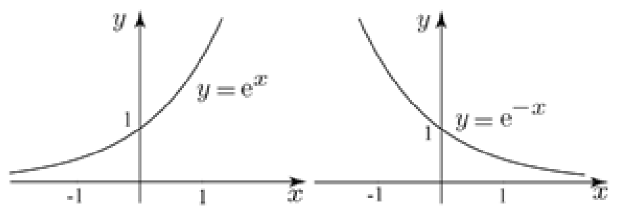
Proof by Induction

Let $P(n)$ be a statement defined for all integers $n \geq 1$.
Then if
1. P(1) is true, and
2. for all $k \geq 1$, $P(k) \Rightarrow P(k+1)$ is true,
then $P(n)$ is true for all $n \geq 1$.

This can be compactly written in symbolic form as $P(1) \wedge (\forall k (P(k) \Rightarrow P(k+1))) \Rightarrow \forall n\ P(n)$.

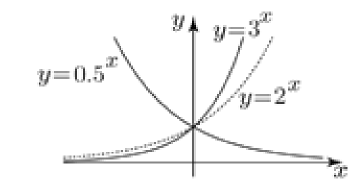
Graphs of common functions

Exponential functions



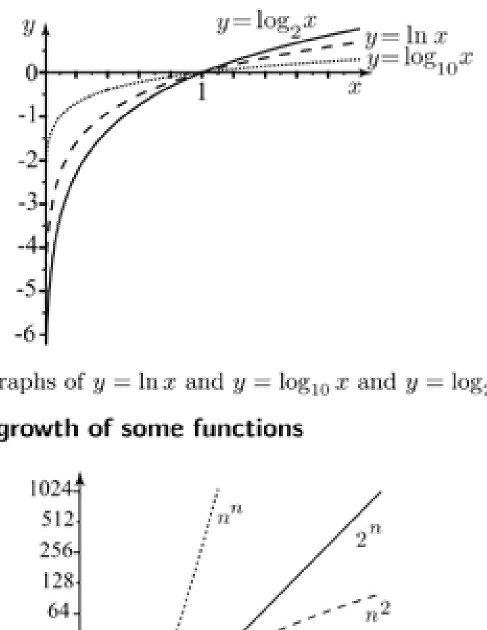
Graph of $y = e^x$ showing exponential growth

Graph of $y = e^{-x}$ showing exponential decay



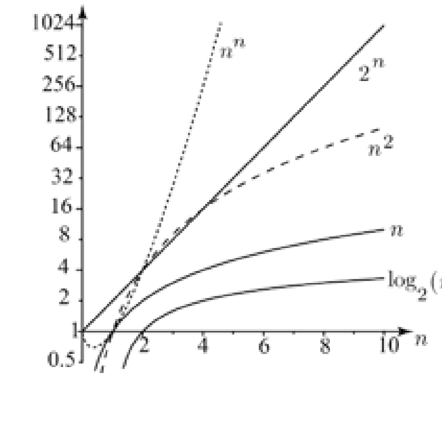
Graphs of $y = 0.5^x$, $y = 3^x$, and $y = 2^x$

Logarithmic functions



Graphs of $y = \ln x$ and $y = \log_{10} x$ and $y = \log_2 x$

The growth of some functions



Probability

Events & probabilities:

The **intersection** of two events A and B is $A \cap B$.
The **union** of A and B is $A \cup B$.
Events A and B are **mutually exclusive** if they cannot both occur, denoted $A \cap B = \emptyset$ where $\emptyset$ is called the **null event**.
For any event A, $0 \leq P(A) \leq 1$.
For two events A and B

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

If A and B are mutually exclusive then

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

Equally likely outcomes:

If a complete set of n elementary outcomes are all equally likely to occur, then the probability of each elementary outcome is $\frac{1}{n}$. If an event A consists of m of these n elements, then $P(A) = \frac{m}{n}$.

Independent events:

A, B are *independent* if and only if

$$P(A \cap B) = P(A)P(B).$$

Conditional Probability of A given B:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \qquad \text{if} \quad P(B) \neq 0.$$

Bayes' Theorem:

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

Theorem of Total Probability:

The k events $B_1, B_2, \ldots B_k$ form a *partition* of the sample space S if $B_1 \cup B_2 \cup B_3 \ldots \cup B_k = S$ and no two of the B_i's can occur together. Then $P(A) = \sum_i P(A|B_i)P(B_i)$. In this case Bayes' Theorem generalizes to

$$P(B_i|A) = \frac{P(A|B_i)P(B_i)}{\sum_j P(A|B_j)P(B_j)} \qquad (i = 1, 2, \ldots k)$$

If B' is the *complement* of the event B,

$$P(B') = 1 - P(B)$$

and

$$P(A) = P(A|B)P(B) + P(A|B')P(B')$$

This is a special case of the theorem of total probability. The complement of the event B is commonly denoted $\overline{B}$.

Matrices and Determinants

The 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant

$$|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$$

The 3×3 matrix $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ has determinant

$$|A| = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

The inverse of a 2×2 matrix

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then $A^{-1} = \dfrac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ provided that $ad - bc \neq 0$.

Matrix multiplication: for 2×2 matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta & a\gamma + b\delta \\ c\alpha + d\beta & c\gamma + d\delta \end{pmatrix}$$

Remember that $AB \neq BA$ except in special cases.

Binary Relations

A **binary relation**, R, from set A to set B is a subset of the Cartesian Product, $A \times B$. If $(a,b) \in R$ we write aRb.
A binary relation on a set A is a subset of $A \times A$.
For a relation R on a set A:
R is **reflexive** when $aRa\ \forall a \in A$.
R is **antireflexive** when $aRb \Longrightarrow a \neq b,\ a, b \in A$.
R is **symmetric** when $aRb \Longrightarrow bRa,\ a, b \in A$.
R is **antisymmetric** when aRb and $bRa \Longrightarrow a = b, a, b \in A$.
R is **transitive** when aRb and $bRc \Longrightarrow aRc,\ a, b, c \in A$.
An **equivalence relation** is reflexive, symmetric and transitive.
A **partial order** is reflexive, antisymmetric and transitive.

Functions

A binary relation, f, on $A \times B$ is a **function** from A to B, written $f : A \to B$, if for every $a \in A$ there is one and only one $b \in B$ such that $(a,b) \in f$. We write $b = f(a)$.
We call A the **domain** of f and B the **codomain** of f.
The **range** of f is denoted by $f(A)$ where $f(A) = \{f(a) : a \in A\}$.
A function $f : A \to B$ is **one-to-one** or **injective** if $f(a_1) = f(a_2) \Longrightarrow a_1 = a_2$.
A function $f : A \to B$ is **onto** or **surjective** if for every $b \in B$ there exists an $a \in A$ so that $b = f(a)$.
A function is **bijective** if it is both injective and surjective.

Complexity Functions

A function $f(n) = O(g(n))$ if there exists a positive real number c such that $|f(n)| \leq c|g(n)|$ for sufficiently large n. More informally, we say that $f(n) = O(g(n))$ if $f(n)$ grows no faster than $g(n)$ does with increasing n. Writing $f(n) \prec g(n)$ indicates that $g(n)$ has greater order than $f(n)$ and hence grows more quickly. The hierarchy of common functions is

$$1 \prec \log(n) \prec n \prec n^k \prec c^n \prec n! \prec n^n$$

where $c, k > 1$.

Combinatorics

The number of ways of selecting k objects out of a total of n where the order of selection is important is the number of permutations:

$${}^nP_k = \frac{n!}{(n-k)!}$$

The number of ways in which k objects can be selected from n when the order of selection is not important is the number of combinations:

$${}^nC_k = \frac{n!}{(n-k)!k!}$$

where $0! = 1, n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (n-1) \cdot n$.

$${}^nC_k = {}^nC_{n-k}$$

$${}^{n+1}C_k = {}^nC_k + {}^nC_{k-1}$$

$${}^nC_0 + {}^nC_1 + \ldots {}^nC_{n-1} + {}^nC_n = 2^n$$

$$(1+x)^n = {}^nC_0 + {}^nC_1 x + {}^nC_2 x^2 + \ldots + {}^nC_{n-1} x^{n-1} + {}^nC_n x^n$$

Thus the value of ${}^nC_k$ is given by the kth entry in the nth row of Pascal's triangle:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

where elements are generated as the sum of the two adjacent elements in the preceding line, the top row is designated row 0, and the left-most entry is labelled 0. For example, the 6 in the final row above is in row 4 and is entry 2, since both row and entry counting start at 0, i.e. ${}^4C_2 = 6$.