
Glossary

AECL	Atomic Energy Canada Ltd.
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AMN	Abstract Machine Notation
BCH	BoseChauduri and Hocquenghem
BNF	Backus Naur Form
CCS	Calculus Communicating Systems
CICS	Customer Information Control System
CMM	Capability Maturity Model
CMMI[®]	Capability Maturity Model Integration
CPO	Complete Partial Order
CSP	Communicating Sequential Processes
CTL	Computational Tree Logic
DAG	Directed Acyclic Graph
DES	Data Encryption Standard
DOD	Department of Defence
DPDA	Deterministic Pushdown automata
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FCFS	First Come, First Served
FSM	Finite State Machine
GCD	Greatest Common Divisor
GCHQ	General Communications Headquarters

GSM	Global System Mobile
HOL	Higher Order Logic
IBM	International Business Machines
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standards Organization
LCM	Least Common Multiple
LD	Limited Domain
LEM	Law Excluded Middle
LIFO	Last In, First Out
LPF	Logic of Partial Partial Functions
LT	Logic Theorist
LTL	Linear Temporal Logic
MIT	Massachusetts Institute of Technology
MTBF	Mean time between failure
MTTF	Mean time to failure
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
NBS	National Bureau of Standards
NFA	Non Deterministic Finite State Automaton
NIST	National Institute of Standards & Technology
NP	Non-deterministic polynomial
OM	Object Modelling Technique
PDA	Pushdown Automata
PMP	Project Management Professional
RDBM	Relational Database Management System
RSA	RivestShamir and Adleman
SCAMPI	Standard CMM Appraisal Method for Process Improvement
SECD	StackEnvironmentCode, Dump
SEI	Software Engineering Institute

SQL	Structured Query Language
TM	Turing Machine
UML	Unified Modelling Language
UMTS	Universal Mobile Telecommunications System
VDM	Vienna Development Method
VDM*	Irish School of VDM
VDM-SL	VDM specification language
WFF	Well-formed formula
YACC	Yet Another Compiler Compiler

Index

A

Abstract algebra, 109
Abuse of statistics, 342
Abu Simbel, 2
Agile development, 288
Alexander the Great, 9
Algebra, 99
Algorithm, 213
Al-Khwarizmi, 20
Alphabets and words, 186
Annuity, 91
Antikythera, 17
Application of functions, 46
Applications of relations, 40
Aquinas, 16
Archimedes, 14
Aristotle, 16
Arithmetic sequence, 87
Arithmetic series, 88
Artificial intelligence, 274
Athenian democracy, 9
Augustus, 19
Automata theory, 117
Axiomatic approach, 305
Axiomatic semantics, 193

B

Babylonians, 4, 5
Backus Naur Form, 189
Bags, 327
Bijective, 44
Binary relation, 25, 26, 34, 40, 50
Binary system, 71
Binary trees, 149
Binomial distribution, 340
Bletchey park, 158
Block codes, 174
B method, 311
Brouwer, L. E. J., 267
Bombe, 159, 161, 165

Boole's symbolic logic, 225

Boole, 225

Bush, Vannevar, 229

C

Caesar, Julius, 156

Caesar cipher, 156

Capability Maturity Model Integration (CMMI), 285, 287, 289, 295–297

Cayley–Hamilton theorem, 135

CCS, 313

Central limit theorem, 346

Chinese remainder theorem, 23

Chomsky hierarchy, 189

Church, Alonzo, 46, 212

Church–Turing thesis, 213

CICS, 303

Classical engineers, 286

Classical mathematics, 293

Cleanroom methodology, 353

Codd, Edgar, 40

Coding theory, 171

Combination, 95

Commuting diagram property, 332

Competence set, 40

Completeness, 212

Complete partial orders, 202

Compound interest, 85

Computability, 212

Computability and decidability, 207

Computable function, 47, 197

Computer representation of numbers, 71

Computer representation of sets, 33

Conditional probability, 338

Correlation, 340

Covariance, 339

Cramer's rule, 135

Cryptographic systems, 160

Cryptography, 155

CSP, 313

D

Darlington nuclear power plant, 303
 Data reification, 331
 Decidability, 210, 211
 Decomposition, 331
 Deduction theorem, 248
 Def Stan 00-55, 302
 Deming, 295
 Denotational semantics, 196
 Determinants, 133
 Digital signatures, 168
 Dijkstra, 272
 Diphantine equations, 70
 Distribution of primes, 65

E

Egyptians, 6
 Enigma codes, 157
 Equivalence relation, 37
 Eratosthenes, 12
 Error correcting code, 171
 Error detection and correction, 176
 Euclid, 10
 Euclid's algorithm, 63
 Euclidean algorithm, 11
 Euler's theorem, 70
 Euler Euclid theorem, 66
 Existential quantifier, 235, 236, 252

F

Fermat's Little theorem, 70
 Field, 112
 Finite-state machines, 118, 119
 Flowcharts, 290
 Floyd, 290
 Formalism, 208, 209
 Formal specification, 299
 Four-Colour theorem, 151
 Frege, Gottlob, 208, 230
 Frequency table, 347
 Functional programming, 46
 Functional programming languages, 46
 Functions, 41
 Fundamental theorem of arithmetic, 61
 Fuzzy logic, 264

G

Garmisch conference, 283
 Gaussian distribution, 345
 Gaussian elimination, 136
 Geometric sequence, 87
 Geometric series, 88
 Grammar, 187
 Graph, 142, 143, 152

Greatest common divisor, 61, 62
 Greek, 1, 8
 Group, 109

H

Halting problem, 215, 256
 Hamiltonian paths, 147
 Hamming code, 180
 Hellenistic age, 10
 Hilbert's programme, 210
 Histogram, 347
 Hoare logic, 292
 HOL system, 279
 Horner's method, 108
 Humphries, Watt, 295
 Hypothesis testing, 348

I

Indices and logarithms, 106
 Information hiding, 314
 Injective, 44
 Input assertion, 194
 Interpretation, 255
 Intuitionist logic, 267
 Irish School of VDM, 309
 Isabelle, 279
 Islamic mathematics, 19

J

Juran, 295

K

Karnak, 2
 Königsberg seven bridges problem, 142

L

Lambda calculus, 197
 Lattices and order, 199
 Laws of probability, 337
 Least common multiple, 62
 Leibniz, 71
 Limited domain relation, 39
 Linear block codes, 177
 Logic and AI, 274
 Logic of partial functions, 269
 Logic programming languages, 275
 Logic Theorist, 278

M

Mathematical induction, 75
 Mathematical proof, 306, 332
 Mathematics in software engineering, 293
 Matrix, 130
 Matrix operations, 131

- Matrix theory, 127
Mersenne, 57
Mersenne primes, 57
Miranda, 47
Model-oriented approach, 305
Modular arithmetic, 69
Monoids, 109
- N**
Natural deduction, 246
Normal distribution, 345
Number theory, 53
- O**
Omar Khayman, 22
Operational semantics, 193, 195
Output assertion, 194
- P**
Paradoxes and fallacies, 222
Parallel postulate, 10
Parity, 56
Parnas, 286, 313
Parnas logic, 271
Parse trees and derivations, 191
Partial correctness, 312
Partial function, 43, 325
Partially ordered sets, 199
Perfect numbers, 57
Permutation, 93
Permutations and combinations, 92
Pidgeonhole principle, 93
Plaintext, 156, 162
Plato, 15
Plimpton 322 tablet, 5
Poisson distribution, 340
Postcondition, 194, 310
Precondition, 310, 312
Predicate, 251
Predicate logic, ix, 235, 236, 250
Predicate transformer, 312
Principia mathematica, 210
Probability mass function, 339
Probability theory, 336, 359
Process calculi, 312
Process maturity models, 295
Professional engineers, 287
Programming language semantics, 192
Prolog, 276
Proof in propositional calculus, 242
Proof in Z, 332
Propositional logic, ix, 235, 236
Public key cryptosystem, 160
Public key systems, 165
Pushdown automata, 121
Pythagoras, 9
- Q**
Quadratic equations, 103
Queuing theory, 356
- R**
Random sample, 343
Random variable, 338, 339
Rectangular number, 55
Recursion, 80, 203
Refinement, 300
Reflexive, 35
Reification, 331
Relational database management system, 40
Relations, 34
Requirements validation, 300
Rhind Papyrus, 7
Ring, 111
RSA public key cryptographic system, 53, 54
RSA public key cryptosystem, 167
Russell, Bertrand, 208
Russell's paradox, 32, 209
- S**
Schema calculus, 310
Schema composition, 328, 330
Schema inclusion, 329
Schemas, 328
Secret key cryptosystem, 160
Semantics, 185, 205
Semantic tableaux, 244, 257
Sequence, 86, 326
Set theory, 26
Shannon, Claude, 227
Sieve of Eratosthenes algorithm, 60
Simple channel code, 173
Simple equation, 100
Simple interest, 89
Simultaneous equations, 100
Software crisis, 283
Software engineering, 283, 285, 289
Software inspections, 294
Software reliability, 350, 351, 356
Software reliability and defects, 351
Software reliability models, 353
Software testing, 294
Spiral model, 287
Square number, 55
Standard deviation, 339, 344
Standish group, 284, 289
Statistical sampling, 342
Statistical usage testing, 353

Statistics, 342
Stoic logic, 223
Story, 289
Strong induction, 76, 78
Structural induction, 82
Structured query language, 40
Surjective, 44
Syllogistic logic, 16, 220, 221
Symmetric, 35
Symmetric key systems, 161
Syntax, 185, 205

T

Tautology, 248
Temporal logic, 265
Theorem provers, 278
Theory of congruences, 67
Time value of money, 91
Transition function, 119
Transitive, 35
Trees, 148
Triangular number, 55
Truth table, 237, 238
Turing machine, 123, 213
Tutankhamun, 2
Two \times Two matrices, 129

U

Undefined values, 269
Undirected graphs, 143
Universal quantifier, 235, 236, 252
Usability of formal methods, 314

V

Valuation functions, 255
Variance, 339, 344
VDM^{*}, 310
VDM, 301, 308
Vector space, 113
VIPER, 306
Waterfall model, 287

W

Weakest precondition, 312
Weak induction, 76
Wilson's theorem, 70

Z

Z, 301
Zermelo set theory, 311
Z specification, 310, 320
Z specification language, 310