

Index

- 3x + 1 conjecture, 128–129
- Absorption laws
 - for Boolean algebra, 902, 903
 - for propositions, 34
 - for sets, 157
- Academic collaboration graph, 709
- Academic paper, 710
- Ackermann's function, 448
- Acquaintanceship graph, 709, 750
- Ada, Augusta (Countess of Lovelace), 36, 37
- Adapting, existing proofs, 122
- Adders, 914–915
 - full, 915, 932
 - half, 914, 915, 932
- Addition
 - algorithm, 321–322
 - associative laws for, A–1
 - Boolean, 900, 932
 - closure laws for, A–1
 - commutative laws for, A–1
 - finite-state machine for, 1016–1017
 - inverse laws for, A–2
 - of matrices, 239, 247
 - of multisets, 180
 - rules of inference, 84
 - of subsets, 879
- Additive compatibility law, A–2
- Additive inverses, for integers modulo m , 314
- Additively homomorphic, 384
- Adjacency lists, 737
- Adjacency matrix, 738–739, 814
 - counting paths between vertices by, 758–759
- Adjacent cells, 918
- Adjacent vertices, 718, 814
- Adjective, 1000, 1001
- Adleman, Leonard, 378
- Advanced counting techniques, 542–613
 - recurrence relations.
- See* Recurrence relations
- Advanced Encryption Standard (AES), 377
- Adverb, 1000, 1001
- Affine cipher, 375, 376, 388
- Affine transformation, 375
- Affirming the conclusion, fallacies of, 92
- Airline routes, 711
- Aleph null, 226, 247
- Algebraic axioms, A–1–A–2
- Algebraic number theory, 128
- ALGOL, 1007, 1008
- Algorithmic paradigm, 291–293, 301
 - brute-force, 292–293, 301
- Algorithms, 253–266
 - addition, 321–322
 - approximation, 305, 789
 - binary search, 257–258, 301
 - binary search tree, 839–841
 - Boolean product of zero-one matrices, 290
 - Boyer-Moore majority vote, 269
 - breadth-first search, 876
 - brute-force, 292–293, 301
 - bubble sort, 259–260
 - c -approximation, 305
 - cashier's, 262–263
 - complexity of. *See* Complexity, of algorithms
 - computer time used by, 296
 - constructing base b expansion, 318
 - correctness of, 255
 - deferred acceptance, 269
 - definiteness of, 255
 - definition of, 253, 300, 317
 - depth-first search, 874
 - Dijkstra's, 783–787, 815
 - for **div** function, 324
 - divide-and-conquer, 572, 615
 - division, 309–310, 387
 - effectiveness of, 255
 - Euclidean, 342–343, 388, 435–436
 - Euler circuits, 768
 - finding maximum element, 255
 - finiteness of, 255
 - Fleury's, 769, 778
 - Floyd's, 791
 - Gale-Shapley, 269
 - generality of, 255
 - for graph isomorphism, 744
 - greedy, 262–265, 301, 410–411, 846
 - Hamilton circuit, 772–773
 - Huffman coding, 845–846
 - input, 255
 - insertion sort, 260
 - for integer operations, 321–325
 - Kruskal's, 886–888, 892
 - linear/sequential, 256, 301
 - merge sort, 456–457
 - for minimum spanning trees, 884–889
 - for **mod** function, 324
 - modular exponentiation, 326
 - multiplication, 323–324
 - naive string matcher, 261–262
 - optimal, 299
 - origin of term, 253
 - output, 255
 - parallel, 729
 - preorder traversal, 862
 - Prim's, 885–886, 892
 - properties of, 255–256

- pseudocode, 254–255
- and recurrence relations, 549–553
 - recursive. *See* Recursive algorithms
- reverse-delete, 891
- searching. *See* Search algorithms
- serial, 728
- shortest-path, 783–787
- Sollin's, 890
- sorting. *See* Sorting algorithms
- string matching, 261–262
- topological sorting, 690
- traversal, 856–863
- Warshall's, 660–663
- Alice in Wonderland*, 60
- Al-Khowarizmi, Abu Ja'far
 - Mohammed ibn Musa, 253
- Alphabet, 1001, 1063
- Alpha-beta pruning, 851
- Alphanumeric character, 477
- Ambiguous grammars, 1065
- Anagrams, 267
- Analytic Engine, 37
- Analytische Zahlentheorie*, 273
- Ancestors, of vertex, 828, 891
- AND gate, 25, 911, 932
- AND operator, 14
- Antecedent, of conditional statement, 7
- Antichain, 701
- Antisymmetric relation, 627–628, 696
- Appel, Kenneth, 804
- Applications
 - of backtracking, 877–879
 - of congruences, 365–370
 - of Euler circuits, 770
 - of Euler paths, 770
 - of graphs colorings, 809–810
 - of pigeonhole principle, 492–494
 - of propositional logic, 20–26
 - of satisfiability, 38–39
 - of trees, 839–851
- Approximation algorithm, 305,
- Arborescence, 896
- Archimedean property, A–4
- Archimedes, A–5
- Archimedes' screw, A–5
- Argument, 81, 149
 - building, rules of inference and, 85–86
 - Cantor diagonalization, 229, 247
 - premises of, 60, 81, 82, 149
 - in propositional logic, 83
 - valid, 81–82
- Argument form, 82, 149
 - valid, 82
- Aristotle, 3
- Arithmetic
 - fundamental theorem of, 330
 - modulo m , 314–315
- Arithmetic mean, 121, 418
- Arithmeticonum Libri Duo*, 398
- Arithmetic progression, 210,
 - primes and, 337
- Array
 - linear, 729
 - two-dimensional, 729
- Art gallery problem, 813
- Art gallery theorem, 813
- Article, 1000, 1001
- Articulation points, 753
- The Art of Computer Programming*, 258, 275
- Assignments, frequency, 810
- Assignment statements, A–10–A–11
- Associated homogenous recurrence relations, 564
- Association rules, 696
 - from data mining, 641–644
 - lift of, 646
 - strong, 644
- Associative laws for addition, A–1
 - for Boolean algebra, 902
 - for disjunction, 34
 - for lattices, 701
 - for multiplication, A–1
 - for propositions, 34
 - for sets, 157
- Associativity, for integers modulo m , 314
- Asymmetric relations, 633
- Asymptotic functions, 285
- Asynchronous transfer mode (ATM), 197
- Atomic propositions, 3
- Atomic sets, 173
- Autokey ciphers, 391
- Automation
 - deterministic, 1030
 - finite-state. *See* Finite-state automata
 - linear bounded automata, 1049
 - nondeterministic, 1030, 1041
 - pushdown, 1049
- quotient, 1037
- Average-case complexity, 288
 - time, 288, 301
- Axioms, 99, 150, 246
 - field/algebraic, A–1–A–2
 - mathematical induction, A–5
 - order, A–1, A–2
 - for real numbers, A–1–A–2
 - for set of positive integers, A–5
 - used to prove basic facts, A–3–A–4
 - Zermelo-Fraenkel, 235
- Bachmann, Paul Gustav Heinrich, 273
- Back edges, 873, 883
- Back substitution, 356
- Backtracking, 873–874
 - applications of, 877–879
- Backus, John, 1008
- Backus–Naur form (BNF), 1007–1009, 1064
- Backward differences, 556
- Backward reasoning, 121
- Backward substitution, 213
- Bacon, Kevin, 751
- Bacon number, 751
- Balanced m -ary trees, 834–835, 891
- Balanced strings of parentheses, 467
- Balanced ternary expansions, 328
- Bandwidth, of graph, 821
- Base b
 - expansions, 318, 320
 - Miller's test for, 364
 - pseudoprimes to, 360
 - strong pseudoprime to, 364
- Base conversion, 318–320
- Bases, of DNA molecules, 475
- Basis step, 397, 399, 436, 462
 - proof by strong induction, 419
- Basket, 642
- Begging the question, 109, 149
- Bell, E. T., 677
- Bellman, Richard, 549, 552
- Bell numbers, 677
- Bernoulli family tree, 826
- Bernoulli's inequality, 416
- Bézout, Étienne, 345
- Bézout's coefficients, 345, 388
- Bézout's identity, 345
- Bézout's theorem, 345–346, 388
- Bhaskaracharya, 181
- Biconditional statement, 11, 149
 - logical equivalences involving, 34

- Biconnected graphs, 754
- Bidirectional bubble sort, 303
- Big- O estimates, 275–278
 - for combinations of functions, 278–280
 - for exponential functions, 278
 - for functions, 275–277
 - for logarithms, 278
 - for polynomials, 275
- Big-Omega (big- Ω) notation, 280–282, 300
- Big- O notation, 271–275
 - definition of, 271–275, 300
 - history of, 271
- Big-Theta (big- Θ) notation, 280–282, 300
- Bi-implications, 11
- Bijection, 191, 247
- Bijective function, 191
- Bijective proofs, 503
- Binary coded decimal expansion, 925
- Binary coded decimal form, 329
- Binary expansions, 318
 - conversion between octal/hexadecimal expansions and, 320
- Binary insertion sort, 268
- Binary relation, 623, 696
- Binary representation, 320, 388
- Binary search algorithm, 257–258, 300, 301, 573
 - recursive, 452–453
 - worst-case complexity, 287–288
- Binary search trees, 839–841, 891
- Binary trees, 440–441, 829, 830, 891
 - extended, 440
 - full, 440–441
 - with prefix codes, 844–846
- Binomial coefficients, 500, 507, 534
 - extended, 585
 - identities involving, 512–513
- Binomial expression, 507
- Binomial theorem, 507–510, 535
 - extended, 586
- Binomial trees, 894
- Bipartite graphs, 722–724, 814
 - coloring of, 723
 - complete, 724
 - and matchings, 725–728
- Bit operations, 14, 149
- Bits, 13, 149
 - parity check, 368
- Bit string, 14, 149
 - encoding, 844
- Bitwise operations, 14, 149
- Bitwise operators, 14, 149
- Block ciphers, 376, 388
- Block of statements, A–13
- Blocks, Sudoku, 40
- Board, 124
- Boole, George, 3, 6, 898
- Boolean algebra, 6, 42, 898–929, 932
 - abstract definition of, 904
 - Boolean functions. *See* Boolean functions
 - identities of, 902–904
- Boolean expressions, 900–902, 932
 - dual of, 904, 907, 932
- Boolean function of degree n , 900, 902, 932
- Boolean functions, 898–904
 - Boolean expressions and, 900–902
 - complement of, 901
 - dual of, 904
 - functionally complete set of operators for, 909
 - implicant of, 920, 932
 - minimization of, 917–929, 932
 - representing, 901–902, 907–909
 - self-dual, 933
 - threshold, 934
 - values of, 901
- Boolean power, of square zero–one matrix, 243
- Boolean product, 899, 901, 931
- Boolean product of zero–one matrix, 242–243, 247, 290
- Boolean ring, 973
- Boolean searches, 22–23
- Boolean sum, 899, 931
- Boolean variable, 13, 149, 900, 908, 931
- Boruvka, Otakar, 888
- Bottom-up parsing, 1006
- Bound
 - greatest lower, 686
 - least upper, 686
 - lower. *See* Lower bound
 - for number of leaves in m -ary tree, 835–836
 - upper. *See* Upper bound
- Bounded lattices, 701
- Bound variable, 54, 149
- Boxes, distributing objects into, 522–525
 - distinguishable, 522–523
 - indistinguishable, 522, 523–525
- Boyer-Moore majority vote algorithm, 269
- Breadth-first search, 875–877, 892
 - depth-first search vs., 876–877
- Breaking codes, 375
- Bridge, in graphs, 753
- Brute-force algorithm, 292–291, 301
- B-tree of degree k , 893
- Bubble sort, 259–260, 301
 - bidirectional, 303
 - worst-case complexity of, 288–289
- Buoyancy, principle of, A–5
- Busy beaver function, 1059
- Busy beaver problem, 1063
- Butane, 831
- Bytes, 318
- Cactus, 894
- Caesar, Julius, 373
- Calculus, predicate, 50
- Call graphs, 709
 - connected components of, 753
- The Canterbury Puzzles* (Dudeney), 546
- Cantor, Georg, 159, 160, 229
- Cantor diagonalization argument, 229, 247
- Cantor digits, 533
- Cantor expansion, 329
- c -approximation algorithm, 305
- Cardinality, 163, 225–235, 247, 247
 - of multisets, 180
- Cardinal numbers, 163
- Carmichael, Robert Daniel, 361
- Carmichael number, 360, 388
- Carroll, Lewis (C. L. Dodgson), 60
- Carry, 321
- Cartesian products, 164–167
- Cases, proof by, 112, 113–116, 150
 - errors with, 116
- Cashier's algorithm, 262–263
- Catalan, Eugène Charles, 550
- Catalan conjecture, 550
- Catalan numbers, 549
- Caterpillar, 895
- Cayley, Arthur, 825, 831
- Ceiling function, 196–198, 247
 - properties of, 197
- Celebrity problem, 418
- Cells, adjacent, 918

- Center vertex, 838
- Chain, 679, 701
- Character cipher, 376, 388
- Characteristic equation, 558
- Characteristic function, 203
- Characteristic roots, 558, 615
- Check digits, 368–370
 - ISBNs, 369–370
 - ISSN, 372
 - parity check bits, 368
 - Universal Product Code, 369
- Checkerboards
 - definition of, 124
 - standard, 124
 - tilings of, 124–127, 412–413
- Chessboard
 - knight's tour on, 779
 - n -queens problem on, 878
- Child, of vertex, 828, 891
- Chinese postman problem, 770
- Chinese remainder theorem, 354–356, 389
- Chomp, 117–118, 429
- Chomsky, linguist Noam, 999, 1006
- Chromatically k -critical graphs, 812
- Chromatic number, 815
 - of graph, 804
- Chung-Wu Ho, 426
- Church, Alonzo, 1060
- Church-Turing thesis, 1057
- Ciphers
 - affine, 375, 388
 - autokey, 391
 - block, 376, 388
 - character, 376, 388
 - monoalphabetic, 376
 - shift, 373, 374, 376, 388
 - transposition, 376
 - Vigenère, 386
- Circuits, 815
 - combinational. *See* Combinational circuits
 - combinatorial, 26
 - in directed graph, 655, 696
 - Euler, 765–770, 815
 - in graphs, 749
 - Hamilton, 764, 770–775
- Circular reasoning, 109, 149
- Circular relation, 699
- Circular r -permutation of n , 506
- Citation graphs, 710
- Class
 - congruence, 312
 - equivalence. *See* Equivalence classes
 - NP, 294, 1060–1061, 1064
 - P, 294, 1060–1061, 1064
- Class A addresses, 478
- Class B addresses, 478
- Class C addresses, 478
- Classical cryptography, 373–377
- Clique, 808
- Closed form, 597
- Closed formula, 212
- Closed interval, 159
- Closed walk, 750
- Closest-pair problem, 578–580
- Closure laws
 - for addition, A-1
 - for multiplication, A-1
- Closures
 - for integers modulo m , 314
 - Kleene, 1021, 1064
- Closures, of relations, 654–663, 696
 - reflexive, 654–655
 - symmetric, 655
 - transitive, 654, 657–660
- Cloud, 383
- Clustering coefficient, 818
- COBOL, 1008
- Cocks, Clifford, 378, 379
- Codeword enumeration, 548–549
- Codomain
 - of functions, 186, 247
 - of partial function, 199
- Coefficients
 - Bézout's, 345, 388
- binomial, 500, 507, 534
 - clustering, 818
 - constant. *See* Constant coefficients
 - multinomial, 529
- Collaboration graphs, 709, 751
- Collatz problem, 128
- Collision
 - in hashing, 366
- Coloring
 - of bipartite graphs, 723
 - edge, 812
 - of graphs, 803–810, 815, 877–878
 - k -tuple, 812
 - of maps of regions, 803
 - of simple graphs, 804
- Combinational circuits, 911–912
- depth of, 917
- examples of, 913–914
- minimization of, 917–929
- Combinations, 500–504
 - generalized, 516–525
 - generating, 531–533
 - with repetition, 516–521
- Combinatorial circuit, 26
- Combinatorial game theory, 851
- Combinatorial proof, 503, 534
- Combinatorics, 470, 534
- Comments, in pseudocode, A-11
- Common difference, 210
- Common ratio, 210
- Communication networks, 709
- Commutative group, 315
- Commutative laws
 - for addition, A-1
 - for Boolean algebra, 902
 - for lattices, 701
 - for multiplication, A-1
 - for propositions, 34
 - for sets, 157
- Commutative ring, 315
- Commutativity, for integers modulo m , 314
- Comparable elements, 678, 697
- Compatibility laws, A-2
- Compatible talks, 550
- Compatible total ordering, 690, 697
- Complement
 - of Boolean function, 901, 932
 - of elements, 702, 899
 - of fuzzy sets, 185
 - of sets, 156, 157, 247
- Complementary graph, 736
- Complementary relations, 633
- Complementation law, 174
- Complemented lattices, 702, 905
- Complement laws, 174
- Complete bipartite graphs, 724, 814
- Complete graphs, 721, 814
- Complete induction, 420
- Complete m -ary tree, 837
- Complete matching, 726, 814
- Complete m -partite graph, 817
- Completeness property, A-3
- Complexity, of algorithms, 285–296
 - average-case, 288
 - computational. *See* Computational complexity of algorithms
 - constant, 293

- Dijkstra's, 787
- exponential, 293, 293
- factorial, 293
- linear, 293
- linearithmic, 293
- logarithmic, 293
- merge sort, 577
- polynomial, 293, 293
- practical considerations, 295–296
- space, 286, 301
- time, 286, 300
- worst-case, 287–288, 301
- Complex numbers, sets of, 158
- Composite, 330, 387, 1062
 - of relations, 629–630
- Composite key, 637, 696
- Compositions, of functions, 192–195, 247
- Compound interest, 213
- Compound propositions, 3, 31, 148
 - consistent, 149
 - equivalences, in Boolean algebra, 899
 - equivalent, 10
 - logically equivalent, 31, 149
 - satisfiable, 38, 149
 - truth tables of, 12
 - unsatisfiable, 38
- Computable functions, 235, 247, 1059, 1064
- Computational complexity, 286, 1057–1061
- Computational complexity of algorithms
 - of depth-first search algorithms, 875
 - Dijkstra's algorithm, 787
- Computational geometry, strong induction in, 424–426
- Computation models, 999–1061
 - finite-state machines, 999, 1012–1018, 1020–1034
 - language. *See* Language pushdown automaton, 1049
 - Turing machine, 999, 1048, 1049
- Computer arithmetic with large integers, 356–358
- Computer file systems, 831
- Computer networks, 704–705
 - local area networks, 728
 - multicasting over, 872
- Computer representation, of sets, 179–180
- Concatenation, 438, 1020, 1064
- Conclusion, 60, 82, 149
 - of conditional statement, 7
- Concurrent processing, 711
- Conditional constructions, A–11–A–12
- Conditional-disjunction equivalence, 32
- Conditional statements, 7–11
 - contrapositive of, 10
 - converse of, 10
 - definition of, 7
 - direct proof of, 100
 - inverse of, 10
 - logical equivalences involving, 34
 - truth table for, 7
- Conditions, don't care, 924–926
- Confidence, 642, 696
- Congruence class, 312
- Congruence classes modulo m , 669, 697
- Congruence modulo m , 666–667
- Congruences, 311
 - applications of, 365–370
 - linear, solving, 351–362
- Congruent to b modulo m , 311
- Conjectures, 99, 149
 - $3x + 1$, 128–129
 - Catalan, 550
 - Frame's, 556
 - Goldbach's, 338
 - twin primes, 339
- Conjunction, 4
 - definition of, 149
 - distributive law of disjunction over, 33
 - rules of inference, 84
 - truth table for, 4
- Conjunctive normal form, 909, 910
- Connected components, of graphs, 752–753, 815
- Connected graphs, 749–759, 815
 - directed, 756–757
 - strongly, 756
 - undirected, 752–753
 - weakly, 756
- Connecting vertices, 718
- Connectives, 4
- Connectivity relation, 657, 697
- Consequence, of conditional statement, 7
- Consistent compound propositions, 149
- Consistent system specifications, 21–22
- Constant coefficients
 - linear homogenous recurrent relations with, 558–564, 615
 - linear nonhomogenous recurrent relations with, 564–567, 615
- Constant complexity, 293
- Constants, 558
- Constructions
 - conditional, A–11–A–12
 - loop, A–12–A–13
- Constructive existence proofs, 117, 150
- Context-free grammars, 1004, 1063
- Context-free language, 1004
- Context-sensitive grammars, 1004
- Context-sensitive language, 1004
- Contingency, 31, 149
- Continuum hypothesis, 235, 247
- Contradiction, 31, 149
 - proofs by, 105–108, 150
- Contraposition, proof by, 101–105, 150
- Contrapositive, of conditional statements, 10, 149
- Converse
 - of conditional statements, 10, 149
 - of directed graphs, 735
- Conversion base, 318–320
 - between binary and hexadecimal expansions, 320
 - between binary and octal expansions, 320
- Convex polygon, 424
- Cook, Stephen, 295
- Cook-Levin theorem, 294
- Corollary, 99, 150
- Correctness
 - of algorithm, 255
 - program. *See* Program correctness
 - of recursive algorithms, 453–454
- Correspondence, one-to-one, 191, 193, 247
- Countable sets, 226–228, 247
- Counterexamples, 50, 107, 123, 150

- Countess of Lovelace (Augusta Ada), 36, 37
- Counting, 470–534
 - advanced techniques. *See* Advanced counting techniques
 - bit strings, 474
 - by distributing objects into boxes, 522–525
 - functions, 472
 - generating functions and, 587–589
 - Internet addresses, 478
 - one-to-one functions, 472
 - passwords, 477
 - paths between vertices, 758–759
 - permutations, 497–500
 - pigeonhole principle and, 488–494
 - principles, 471–477
 - problems, 470, 477–478
 - subsets of finite sets, 408–410, 474
- Count of an itemset, 642, 696
 - A Course of Pure Mathematics*, 118
- Covering relation, 682
- Covers, 682, 813, 927
- C programming language, 669–670
- Crawl frontier, 880
- Cross edge, 883
- Crossing number, 803
- Cryptanalysis, 375–376, 388
- Cryptographic protocols, 382–383
- Cryptography, 372–384
 - classical, 373–377
 - public key, 372, 377–378
- Cryptosystems, 376, 388
 - fully homomorphic, 384, 388
 - Paillier, 387
 - private key, 377–378
 - public key, 378
 - RSA system, 378–379, 388
- Curse of dimensionality, 552
- Cut edge, 753, 815
- Cut set, 894
- Cut vertices, 753, 815
- Cycle, 814
 - in directed graph, 655, 696, 721
- Cyclic monoid, 948
- Czekanowski, Jan, 888
- Databases
 - attribute of, 636
 - composite key, 637
 - fields, 636
 - intension, 637
 - primary key, 636–637
 - records, 636
 - and relations, 636–637
- Data compression, 845
- Datagrams, 487
- Datalogy, 1008
- Data mining, association rules from, 642–644
- Datatype, 159
- Decidable problem, 1058–1059
- Decimal expansions, 318
- Decision problem, 1058, 1064
- Decision trees, 842–844, 891
- Decreasing functions, 189
- Decryption, 374
 - RSA system, 380
- Deductive reasoning, 397
- de Fermat, Pierre, 359
- Deferred acceptance algorithm, 269
- Deficiency, 735
- Definiteness, of algorithm, 255
 - Degree
 - of linear homogenous recurrence relations, 557
 - n -ary relations, 635
 - of region, 795
 - of vertex in niche overlap graph, 719
 - of vertex in undirected graph, 718, 814
- Degree-constrained spanning tree, 895
- Degree of membership, of universal set, 185
- De La Vallée-Poussin, Charles-Jean-Gustave-Nicholas, 336
- Delay machine, 1016
- De Morgan, Augustus, 31, 36, 807
- De Morgan's laws, 31
 - for Boolean algebra, 902, 907
 - for propositions, 34, 35
 - proving by mathematical induction, 408–410
 - for quantifiers, 57–58
 - for sets, 157
- Dense
 - graph, 740, 745
 - partially ordered set, 695
- Density, of undirected graphs, 745
- Denying the hypothesis, fallacies of, 92
- Depth-first search, 872–875, 892
 - breadth-first search vs., 876–877
 - in directed graphs, 879–880
- Depth of combinational circuits, 917
- Derangements, 611–613, 615
- Derivable from, 1002
- Derivation, 1002
- Derivation trees, 1005–1007, 1063
- Descartes, René, 166
- Descendants, of vertex, 828, 891
- Deterministic finite-state automata, 1030, 1064
- Devil's pair, 749
- Diagonal, of simple polygon, 424
- Diagonal matrix, 245
- Diagonal relation, 654
- Diagrams
 - Hasse, 682–684, 697
 - state, 1014
 - Venn, 160–161
- Diameter, of graphs, 821
- Dictionary ordering, 529
- Difference, A–6
- Difference equation, 556
- Differences backward, 556
 - common, 210
 - first, 556
 - first forward, 618
 - forward, 618
 - of multisets, 180
 - of sets, 156, 157, 247
 - $(k + 1)$ st, 556, 618
 - symmetric, 183, 247
- Diffie-Hellman key agreement protocol, 382
- Digital circuits, 25–26
- Digital signatures, 383, 388
- Digraphs/directed graphs, 696, 707, 814
 - circuit/cycle in, 656, 697, 721
 - connectedness in, 756–757
 - converse of, 736
 - dense, 740
 - depth-first search in, 879–880
 - edges of, 650, 720–721
 - Euler circuit of, 765
 - loops in, 650, 696
 - paths in, 655–656, 696
 - representing relations using, 650–651
 - self-converse, 819
 - simple, 707
 - strong components of, 756–757, 815

- vertices, 650
- Dijkstra, Edsger Wybe, 783, 784
- Dijkstra's algorithm, 783–787, 815
- Diophantus, 128, 359
- Dirac, Gabriel A., 772, 774
- Dirac's theorem, 773
- Directed edges, 707, 720–721, 814
- Directed graphs. *See* Digraphs/
 - directed graphs
- Directed multigraphs, 707, 707, 814
- Directly derivable, 1002
- Direct proof, 100–101, 150
- Dirichlet, G. Lejeune, 489
- Dirichlet drawer principle, 488
- Discrete logarithm, 361, 388
- Discrete logarithm problem, 361
- Disjoint sets, 171
- Disjunction, 5–6
 - associative law for, 34
 - definition of, 5, 149
 - distributive law over conjunction, 33
 - truth table for, 4
- Disjunctive normal form, 908
- Disquisitiones Arithmeticae*, 312
- Distance, 883
- Distinguishable boxes
 - distinguishable objects in, 522–523
 - indistinguishable objects in, 523
- Distributive lattice, 701, 905
- Distributive laws, 902–903
 - for Boolean algebra, 902
 - for propositions, 34
 - for real numbers, A–2
 - for sets, 157
- Distributivity, for integers modulo m , 314
- div** function, 310
- Divide-and-conquer algorithms, 572, 615
- Divide-and-conquer recurrence
 - relations, 573–580
- Dividend, 310
- Divisibility, results, proving by
 - mathematical induction, 406–408
- Divisibility relation, 678
- Division
 - of integers, 308, 308–311, 387
 - trial, 331–332
- Division algorithm, 309–310, 388
- Division rule, 481, 535
- Divisor, 308, 310
 - greatest common, 340–342
- DNA (deoxyribonucleic acid), 474
- Dodgson, Charles Lutwidge (Lewis Carroll), 60
- Domain of definition, of partial function, 199
- Domains, 50, 52
 - of discourse, 50, 149
 - finite, 53–62
 - of function, 186, 247
 - n -ary relations, 635
 - of partial function, 199
 - restricted, quantifiers with, 54
- Dominating set, of vertices, 818
- Domination laws
 - for Boolean algebra, 902
 - for propositions, 34
 - for sets, 157
- Dominos, 124, 398
- Don't care conditions, 924–926, 932
- Double counting proofs, 503
- Double hashing, 371
- Double negation law, 33
- Dual
 - of Boolean expression, 904, 907, 932
 - of partially ordered set, 693
- Dual graph, 804
- Duality principle, 904
- Dudeney, Henry, 546
- Dynamic programming, 549, 615
 - example of, 549–550
- Ear, 429
- Eccentricity, of vertex, 838
- Edge chromatic number, 812
- Edge coloring, 812
- Edge contraction, 731
- Edge cut, 755, 815
- Edges, 705
 - adding from graph, 730
 - back, 873, 883
 - connectivity, 755–756, 815
 - cross, 883
 - cut, 753, 815
 - of digraphs, 650, 720–721
 - directed, 707, 815
 - endpoints of, 705
 - forward, 883
 - incident, 718
 - matched, 726
 - of multigraphs., 706
 - multiple, 706, 814
 - multiple directed, 707, 814
 - of multiplicity, 707
 - noncomplete, 721
 - removing from graph, 730
 - tree, 873
 - undirected, 709, 814
 - unmatched, 726
- Effectiveness, of algorithm, 255
- Egyptian fraction, 465
- Elementary subdivision, 797, 815
- Elements
 - comparable, 678, 697
 - complement of, 702, 899
 - equivalent, 666
 - identity, for integers modulo m , 314
 - incomparable, 678, 697
 - majority, 269
 - maximal, in partially ordered set, 684–686
 - maximum, finding in finite sequence, 255
 - minimal, in partially ordered set, 684–686
 - of partially ordered set, 677
 - relationships between. *See* Relations
 - of sets, 157, 246
- The Elements*, 342
- Ellipses (...), 158
- Empty set, 160, 246
- Empty string, 210, 247, 1001
- Encryption, 373, 388
 - homomorphic, 373, 383–384
 - private key, 388
 - public key, 388
 - RSA, 379–380
- Encryption key, 366, 388
- Endpoints, of edges, 705
- Enumeration, 470, 534. *See also* Counting
 - codeword, 548–549
- Equality
 - of functions, 186
 - of sets, 158, 246
- Equal matrices, 238
- Equation
 - characteristic, 558
 - difference, 556
- Equivalence
 - logical. *See* Logical equivalences
 - proof of, 106–107

- Equivalence classes, 668–672
 - definition of, 668, 697
 - and partitions, 670–673
 - representative of, 668
- Equivalence relations, 665–673, 697
- *-equivalent, 1037
- Equivalent, 697
 - compound propositions, 10
- Equivalent Boolean expressions, 900
- Equivalent elements, 666
- Eratosthenes, 332
- Erdős, Paul, 700
- Erdős number, 699, 751
- Errors
 - with exhaustive proof, 116
 - with proof by cases, 116
 - in proofs, 108–109
 - single, 370
 - transposition, 370
- Essential prime implicant, 920, 932
- Euclid, 342
- Euclidean algorithm, 342–345, 388, 435–436
- Euler, Leonhard, 765, 767
- Euler circuit, 764–770, 815
- Euler paths, 764–770, 815
- Euler's criterion, 365
- Euler's formula, 794–797, 815
- Evaluation functions, 851
- Even integer, 101
- Exams, scheduling, 809–810
- Exclusion rule, 436
- Exclusive or
 - definition of, 6, 149
 - truth table for, 7
- Exhaustive proofs, 112–113, 150
 - errors with, 116
- Existence proofs
 - constructive, 117, 150
 - definition of, 117
 - nonconstructive, 117–119, 150
- Existential generalization, 93
- Existential instantiation, 93
- Existential quantification, 49, 52, 149
- Existential quantifier, 52–53
- Expansions
 - balanced ternary, 328
 - base- b , 318, 320
 - binary, 318
 - binary coded decimal, 925
 - Cantor, 329
 - decimal, 318
 - hexadecimal, 318
 - octal, 318
 - sum-of-products, 907–909, 932
- Exponential complexity, 293
- Exponential functions, A–7
 - big- O estimates for, 278
- Exponential generating function, 600
- Expressions
 - Boolean, 900–902, 932
 - infix form of, 864
 - logically equivalent, 149
 - prefix form of, 865
 - regular, 1038, 1064
- Extended Backus–Naur form (EBNF), 1012
- Extended binary trees, 440
- Extended binomial coefficients, 585
- Extended binomial theorem, 586
- Extended Euclidean algorithm, 346
- Extension, of relations, 637
- Exterior, of simple polygon, 424
- Factor, 308
- Factorial complexity, 293
- Factorial function, 198
- Facts, 99
- Fallacies, 81, 92, 149
 - of affirming the conclusion, 92
 - of denying the hypothesis, 92
- Family trees, 826
- Fefferman, Charles, 337
- Female pessimal, 303
- Fermat's last theorem, 128, 273
- Fermat's little theorem, 358–359, 389
- Fibonacci, 436
- Fibonacci numbers formula for, 561
 - iterative algorithm for, 456
 - rabbits and, 544
 - recursive algorithm for, 455
- Fibonacci sequence, 211–212
- Field axioms, A–1–A–2
- Fields, databases, 636
- Final exams, scheduling, 809–810
- Final state, finite-state automaton, 1021
- Final value, A–12
- Finite domain, quantifiers, 53–62
- Finite graph, 705
- Finiteness, of algorithms, 255
- Finite sets, 163, 246
 - Jaccard similarity of, 185
 - number of subsets of, 408–410, 474
- union of, 602
- Finite-state automata, 1021–1030
 - designing, 1024–1025
 - deterministic, 1026–1030, 1064
 - equivalent, 1026–1030
 - nondeterministic, 1030–1033, 1064
 - set not recognized by, 1047
- Finite-state machine, 999, 1012–1018, 1064
 - for addition, 1016
 - language recognition by, 1022–1027
 - with no output, 1020–1034
 - with outputs, 1014–1017
 - types of, 1017
- First difference, 556
- First forward difference, 618
- Fleury's algorithm, 769, 778
- Floor function, 196–198, 247
 - properties of, 197
- Floyd's algorithm, 791
- Forests, 838, 891
 - minimum spanning, 890
 - spanning, 882
- Formal language, 1000
- Formal power series, 584
- Formulas
 - closed, 212
 - Euler's, 794–797, 815
 - for Fibonacci numbers, 561–562
 - Stirling's, 199
 - summations, 221, 401–404
 - well-formed, 438–440, 870
- FORTRAN, 1008
- Forward differences, 618
- Forward edge, 883
- Forward reasoning, 121
- Forward substitution, 213
- Four color theorem, 804–808, 815
- Frame's conjecture, 556
- Free group 946
- Free monoid 944
- Free semigroup 944
- Free variable, 54, 149
- Freud, Sophia, 36
- Frequency assignments, 810
- Frequent, 642
- Frequent itemset, 642, 696
- Friendship graph, 708
- Frisbee, rocket-powered, 900
- Full adder, 915, 932
- Full binary trees, 439–440

- Full m -ary trees, 829, 891
 - counting vertices in, 833–834
- Full subtractor, 916
- Fully homomorphic cryptosystem, 384, 388
- Functional completeness, 909, 932
- Functionally complete set of
 - operators, for Boolean functions, 909, 932
- Functions, 156, 185–200, 247
 - Ackermann's, 448
 - asymptotic, 285
 - big- O estimates for, 275–277
 - bijective, 191, 247
 - Boolean. *See* Boolean functions
 - busy beaver, 1059
 - ceiling, 196–198, 247
 - characteristic, 203
 - codomain of, 186, 247
 - compositions of, 192–195, 247
 - computable, 235, 247, 1064
 - counting, 472
 - decreasing, 189
 - definition of, 185
 - div**, 310, 324
 - domain of, 186, 247
 - equality of, 186
 - Euler Φ -function, 349
 - evaluation, 851
 - exponential, A–7
 - factorial, 198
 - floor, 196–198, 247 generating. *See* Generating functions
 - graphs of, 195
 - greatest integer, 196
 - growth of, 270–276
 - hashing, 366–367
 - increasing, 189
 - integer-valued, 188
 - inverse, 192–195, 247
 - invertible, 192
 - iterated, 449
 - linear probing, 367
 - logarithmic, A–7–A–9
 - McCarthy 465
 - mod**, 310, 324, 387
 - not invertible, 192
 - number-theoretic, 1055
 - one-to-one, 188–192, 247, 472
 - one-to-one correspondence, 191, 247
 - onto, 188–192, 247, 610–611
 - output, 1014
 - partial, 199, 247
 - propositional, 47, 48, 148
 - range of, 186, 247
 - real-valued, 188
 - recursive/inductive definitions, 433–436, 462
 - as relations, 624
 - strictly decreasing, 189
 - strictly increasing, 189
 - surjective, 190
 - total, 199
 - transition, 1014, 1021, 1022
 - uncomputable, 235, 247, 1059, 1064
- Fundamental theorem of arithmetic, 330, 388, 422
- Fuzzy sets, 185
 - complement of, 185
 - intersection of, 185
 - union of, 185
- Gale-Shapley algorithm, 269
- Game trees, 846–851, 891
- Gates, logic, 25, 149, 910–915
 - AND, 25, 911, 932
 - NOT, 25
 - OR, 25, 911, 932
 - threshold, 934
 - XOR, 934
- Gating networks, 911
 - examples of, 913–914
- Gauss, Karl Friedrich, 312
- Gene, 475
- Generality, of algorithm, 255
- Generalization
 - existential, 93
 - universal, 93
- Generalized combinations, 516–525
- Generalized induction, 444–445
- Generalized permutations, 516–525
- Generalized pigeonhole principle, 490–494, 535
- Generating functions, 583–596, 615
 - and counting problems, 587–589
 - exponential, 600
 - ordinary, 583
 - probability, 602
 - proving identities via, 596
 - for recurrence relations, 594–596
- Gene sequencing, 475
- Genome, 475
- Gentry, Craig B., 384
- Geometric mean, 121, 418
- Geometric progression, 210
 - definition of, 247
 - sums of, 404
 - sums of terms, 218
- Geometric series, 218
- Giant strongly connected component (GSCC), 757
- Givens, Sudoku, 40
- Goldbach, Christian, 338
- Goldbach's conjecture, 338
- Golomb's self-generating sequence, 468
- Gossip problem, 418
- Graceful tree, 895
- Grammars, 1000. *See also* Language
 - ambiguous, 1065
 - Backus–Naur form, 1007–1009
 - context-free, 1004, 1063
 - context-sensitive, 1004
 - language generated by, 1002
 - monotonic, 1004
 - noncontracting, 1004
 - phrase-structure, 1001–1004
 - productions of, 1001
 - regular, 1004, 1046–1047, 1064
 - type 0, 1004, 1005, 1063
 - type 1, 1004, 1005, 1063
 - type 2, 1004, 1005, 1063
 - type 3, 1004, 1005, 1063
 - use of, 1000
- Grand Hotel, Hilbert's, 227–228
- Graphic sequence, 735
- Graphs, 814–815
 - academic collaboration, 709
 - acquaintanceship, 708, 750
 - airline routes, 711
 - bandwidth of, 821
 - biconnected, 754
 - bipartite, 722–724, 814
 - call, 709
 - chromatically k -critical, 812
 - chromatic number of, 804
 - circuits in, 749
 - citation, 710
 - collaboration, 709, 751
 - coloring of, 803–810, 815, 877–878
 - complementary, 736
 - complete, 721
 - complete m -partite, 817
 - connected component of, 752–753

- connectivity. *See* Connected graphs
- cut set of, 894
- definition of, 705
- degree sequence of, 735
- with diagnostic lines, 706
- diameter of, 821
- directed. *See* Digraphs dual, 804
- edges. *See* Edges
- Euler circuit in, 764–770
- Euler paths in, 764–770
- finite, 705
- friendship, 708
- Hollywood, 709
- homeomorphic, 797–798
- infinite, 705
- influence, 709
- intersection, 715
- isomorphic, 737, 741–744
- k -connected, 754, 815
- k -tuple coloring, 812
- mixed, 707, 707
- models, 708–714
- module dependency, 711
- monotone decreasing property of, 822
- monotone increasing property of, 822
- multigraphs. *See* Multigraphs with multiple lines, 706
- with multiple one-way lines, 707
- neighbors in, 718
- niche overlap, 712
- nonisomorphic, 741
- nonplanar, 796
- nonseparable, 753, 815
- paths in, 750–751
- Petersen, 778
- planar, 792–798, 815
- precedence, 711
- protein interaction, 712, 713
- pseudographs, 706, 707, 814
- radius of, 821
- regular, 736, 814
- representation of, 737–745
- simple. *See* Simple graphs simple directed, 707, 814
- spanning forest of, 882
- sparse, 739, 745
- strongly connected, 756
- subgraph of, 730, 814
- terminology, 707, 718–721
- underlying undirected, 721
- undirected. *See* Undirected graphs union of, 732, 814
- vertices. *See* Vertex (vertices) weakly connected, 756
- web, 710, 757
- weighted. *See* Weighted graphs
- Graphs of functions, 195
- Gray, Frank, 775
- Gray codes, 773–774
- “Greater than or equal” relation, 678
- Greatest common divisor (gcd), 340–342, 387
- as linear combinations, 345–348
- recursive algorithm for computing, 451
- Greatest element, of partially ordered set, 684, 697
- Greatest integer function, 196
- Greatest lower bound, 686, 697
- Great Internet Mersenne Prime Links Search (GIMPS), 335
- Greedy algorithms, 262–265, 301, 410–411, 846
- Growth of functions, 270–276
- big- O notation, 271–275
- Guarding set, 813
- Guthrie, Francis, 807
- Hadamard, Jacques, 336
- Haken, Wolfgang, 804
- Half adder, 914, 915, 932
- Half subtractor, 916
- Hall, Philip, 727
- Hall’s marriage theorem, 726–728, 815
- Halting problem, 265–266, 1059
- Hamilton, William Rowan, 770, 772, 807
- Hamilton circuits, 764, 770–775, 815
- Hamilton paths, 770–775, 815
- Handle vertex, 894
- Handshaking theorem, 719–720, 815
- Hardy, Godfrey Harold, 118
- Hardy–Weinberg law, 118
- Harmonic mean, 132
- Harmonic number, 285
- inequality of, 406
- Harmonic series, 406
- Hashing/hashing function, 366–367
- collision in, 366
- double, 371
- Hasse, Helmut, 683
- Hasse diagrams, 682–684, 697
- Hasse’s algorithm, 128
- Hatcheck problem, 611–613
- Header length field, 487
- Heawood, Percy, 804
- Height, of rooted trees, 834, 891
- Hexadecimal expansions, 318
- conversion between binary expansion and, 320
- Hexadecimal representation, 320, 388
- Hexagon identity, 514
- Hilbert, David, 228, 235
- Hilbert’s Grand Hotel, 227–228
- Hilbert’s Tenth Problem, 1059
- Hoare triple, 393
- Hockeystick identity, 515
- Hollywood graphs, 709
- Homeomorphic graphs, 797–798, 815
- Homomorphic encryption, 373, 383–384
- Hopper, Grace Brewster Murray, 1031
- Hops, 729
- Horner’s method, 298
- Host number (hostid), 478
- Houses-and-utilities problem, 792
- Huffman, David A., 845
- Huffman coding, 845–846, 892
- Hydrocarbons, trees modeling, 830
- Hypothesis
- of conditional statement, 7
- continuum, 235, 247
- inductive, 397, 400, 412, 414, 727
- Hypothetical syllogism, 84
- Icosian puzzle, 770
- Idempotent laws
- for Boolean algebra, 902, 907
- for lattices, 701
- for propositions, 34
- for sets, 157
- Identification numbers single error in, 370
- Identifiers, in C Programming Language, 669–670
- Identity
- Bézout’s, 345
- elements, for integers modulo m , 314
- elements axiom, A–2
- hexagon, 514
- hockeystick, 515

- involving binomial coefficients, 512–513
- Pascal's, 510–512, 535
- proving, generating functions for, 596
- Vandermonde's, 512–513
- Identity laws
 - additive, A–2
 - for Boolean algebra, 902
 - multiplicative, A–2
 - for propositions, 34
 - for sets, 157
- Identity matrix, 241, 247
- if then statement, 48, A–11–A–12
- Image
 - of element, 186, 247
 - inverse, 202
 - of subsets, 188
- Implicant, 932
 - essential prime, 920, 932
 - prime, 920, 932
- Implication, 7, 149
- Incidence matrices, 740, 814
- Incident edge, 718, 814
- Inclusion–exclusion principle. *See* Principle of inclusion–exclusion
- Inclusive or, 5
- Incomparable elements, 678, 697
- Incomplete induction, 420
- Increasing functions, 189
- Increment, for linear congruential method, 367
- In-degree of vertex, 720, 814
- Independence number, 821
- Independent vertices, 821
- Index of summation, 217–218
- Index registers, 810
- Indirect proofs, 102
- Indistinguishable boxes
 - distinguishable objects in, 523–525
 - indistinguishable objects and, 525
- Induction
 - complete, 420
 - generalized, 444–445
 - incomplete, 420
 - mathematical. *See* Mathematical induction
 - strong induction. *See* Strong induction
 - structural, 433, 441–444, 462
- Inductive definitions, 433
 - of functions, 433–436
 - of sets, 436–441, 462
 - of strings, 437
 - of structures, 436–441
- Inductive hypothesis, 397, 400, 412, 414, 727
- Inductive loading, 418
- Inductive reasoning, 397
- Inductive step, 397, 462
- Inequality
 - Bernoulli's, 416
 - harmonic numbers, 406
 - proving by mathematical induction, 405–406
 - triangle, 132, 185
- Infinite graph, 705
- Infinite ladder, 396
 - strong induction and, 420–421
- Infinite series, 221
- Infinite set, 157, 164, 247
- Infinity of primes, 333–335
- Infix form, 864
- Infix notation, 863–867, 892
- Influence graph, 709
- Informal proofs, 99
- Information flow, lattice model of, 687
- Information networks, 710
- Information retrieval (IR), 713
- Initial conditions, 211, 615
- Initial state, 1014, 1021
- Initial term, 210
- Initial value, A–12
- Initial vertex, 650
- Injection, 188
- Inorder traversal, 856, 857–860, 863–864, 892
- Input, algorithms, 255
- Input alphabet, 1014, 1021
- Insertion sort, 260, 301
 - binary, 268
 - worst-case complexity of, 288–289
- Instantiation existential, 93
 - universal, 92, 93
- Integers, 308, 317
 - binary coded decimal form, 329
 - composite, 330
 - division of, 308, 308–311
 - even, 101
 - fast multiplication of, 574
 - large, computer arithmetic with, 356–358
 - least common multiple, 341
 - nondecreasing, 266
 - odd, 101
 - one's complement representations, 328
 - pairwise relatively prime, 341, 387
 - positive, 158, 308, 348, 395
 - primes, 330–331
 - relatively prime, 341, 387
 - representations of, 317–320
 - sequences, 215–216
 - sets of, 158
 - signed, 1009
 - squarefree, 614
 - two's complement representations, 329
 - unary representations, 1055
- Integer sequences, 214–217
- Integers mod m , 314–315
 - additive inverses, 314
 - associativity, 314
 - closure, 314
 - commutativity, 314
 - distributivity, 314
 - identity elements, 314
- Integer-valued functions, 188
- Intension, of database, 637
- Interest, compound, 213
- Interior, of simple polygon, 424
- Interior diagonal, of simple polygon, 424
- Interior vertices, 660
- Internal vertices, 828, 891
- International Standard Book Number (ISBN-10), 369–370
- International Standard Serial Number (ISSN), 372
- Internet, search engines on, 880
- Internet addresses, counting, 478
- Internet Protocol (IP) multicasting, 872
- Intersection
 - of fuzzy sets, 185
 - of multisets, 180
 - of sets, 171, 177–179, 247
- Intersection graph, 715
- Intervals, 158
 - closed, 159
 - open, 159
- Intractable problem, 294, 301
- Intractable problems, 1061
- Invariant for graph isomorphism, 741, 815

- Inverse, 352, 388
 - of conditional statements, 10, 149
 - multiplicative, 71
- Inverse functions, 192–195, 247
- Inverse laws
 - for addition, A–2
 - for multiplication, A–2
- Inverse relations, 633
- Inverter, 25, 911, 932
- Invertible function, 192
- IP multicasting, 872
- IR. *See* Information retrieval (IR)
- Irrational numbers, 104
- Irreflexive relations, 632
- Isobutane, 831
- Isolated vertex, 719, 814
- Isomorphic graphs, 737, 741–744, 814
 - paths and, 757–758
- Items, 642
- Itemset, 642, 696
- Iterated function, 449
- Iterated logarithm, 449
- Iteration, 209, 213, 455–456, 462
- Iterative, 455
- Iterative algorithm, for Fibonacci numbers, 456
- Jaccard distance, 185
- Jaccard similarity, of finite sets, 185
- James, William, 48
- Jealous husbands problem, 764
- Jigsaw puzzle, 429
- Jobs
 - lateness of, 304
 - slackness of, 304
- Join, 696
 - in lattice, 701
 - n -ary relations, 639
 - of zero–one matrices, 242, 247
 - Josephus problem, 555
- Kakutani's problem, 128
- Karnaugh, Maurice, 919
- Karnaugh maps, 918, 918–924, 932
- k -connected graphs, 754, 815
- Kempe, Alfred, 804
- Kempe, Alfred Bray, 805
- k -equivalent, 1037
- Key, 366, 388
 - composite, 637, 696
 - primary, 636–637, 696
- Key exchange, 382, 388
- Key exchange protocol, 386, 388
- Keyspace, 377
- Kissing problem, 216
- Kitab al-jabr w'al muquabala*, 253
- k -itemset, 642
- $(k + 1)$ st difference, 556, 618
- Kleene, Stephen, 1022, 1038
- Kleene closure, 1021, 1064
- Kleene's theorem, 1040–1041, 1064
- K-map, 918, 918–924, 932
- Knapsack problem, 304, 617
- Knight, 779
- Knight's tour, 779
- Knuth, Donald E., 258, 271, 275, 280
- Kronecker delta, 241
- Kruskal, Joseph Bernard, 887, 888
- Kruskal's algorithm, 886–888, 892
- k -tuple coloring, 812
- Kuratowski, Kazimierz, 797
- Kuratowski's theorem, 797–798, 815
- k -vertex-connected, 754
- Labeled tree, 838
- Lady Byron, 37
- Lagarias, Jeffrey, 128
- Lamè, Gabriel, 437
- Landau, Edmund, 271
- Landau symbol, 271
- Language, 1000–1009, 1063. *See also* Grammars
 - context-free, 1004
 - context-sensitive, 1004
 - formal, 1000
 - generated by grammar, 1002
 - natural, 1000
 - recognition by finite-state machines, 1022–1027, 1064
 - recognized/accepted, 1023, 1032
 - regular, 1004
 - syntax, 1000
- Language over, 1001
- Large integers, computer arithmetic with, 356–358
- Lateness, of job, 304
- Lattice point, 464
- Lattices, 686–687, 697
 - associative laws for, 702
 - bounded, 702
 - commutative laws for, 702
 - complemented, 702
 - distributive, 702
 - idempotent laws for, 702
- join in, 701
- lower bound of, 702
- meet in, 701
- upper bound of, 701
- Law of detachment, 83
- Law of double complement, in Boolean algebra, 902, 907
- Laws
 - commutative. *See* Commutative laws
 - complement, 174
 - complementation, 174
 - De Morgan's. *See* De Morgan's laws
 - distributive. *See* Distributive laws
 - domination. *See* Domination laws
 - of double complement, in Boolean algebra, 902, 907
 - double negation, 33
 - Hardy–Weinberg, 118
 - idempotent. *See* Idempotent laws
 - identity. *See* Identity laws
 - inverse, A–2
 - negation, 33
 - transitivity, A–2
 - trichotomy, A–2
 - used to prove basic facts, A–3–A–4
- Laws of Thought* (Boole), 3, 898
- Leaf, 828, 891
- Least common multiple, 341, 387
- Least element, of partially ordered set, 684, 697
- Least upper bound, 686, 697, A–3
- Left child, of vertex, 830
- Left subtree, 830
- Legendre symbol, 365
- Lemma, 99, 150
- Length of path, 749
 - in directed graphs, 655
 - in weighted graph, 782
- Length of string, 210, 437
- Le problème de rencontres, 612
- Level, of vertex, 834, 891
- Level order of vertex, 894
- Lexicographic ordering, 444, 529, 680–682, 697
- Liber Abaci, 436
- Lift, of association rules, 646
- Limits, definition of, 72
- Linear array, 729
- Linear bounded automata, 1049

- Linear combinations, greatest common divisor as, 345–348, 387
- Linear complexity, 293
- Linear congruences, solving, 351–362, 388
 - Chinese remainder theorem, 354–356
 - Linear congruential method, 367
- Linear homogenous recurrence relations, 558–564, 615
- Linearithmic complexity, 293
- Linearly ordered sets, 679
- Linear nonhomogenous recurrence relations, 564–567
- Linear probing function, 367
- Linear search algorithm, 256, 300, 301
 - average-case complexity of, 288
 - recursive, 452
- List coloring, 813
- Lists, merging, 458–459
- Literal, 908, 932
- Load balancing problem, 305
- Local area networks, 728
- Logarithmic complexity, 293
- Logarithmic functions, A–7–A–9
- Logarithms
 - big- O estimates for, 278
 - discrete, 361, 388
 - iterated, 449
- Logical equivalences, 31–35, 903
 - constructing, 35–37
 - quantifiers, 55
- Logical expressions
 - translating from English into, 20–21, 58–60, 72–74
 - translating mathematical statements into, 71–72
- Logically equivalent compound propositions, 31, 148
- Logically equivalent expressions, 149
- Logical operators, 3, 148
 - precedence of, 12
- Logic circuits, 25–26, 149
- Logic puzzles, 23–25
- Longest path problem, 792
- Loop constructions, A–12–A–13
- Loops/looping, 696, 814
 - in digraphs, 650, 706
 - within loops, A–14
 - nested, 67
- quantification and, 54, 68
- Lord Byron, 37
- Lower bound, 697
 - greatest, 686, 697
 - of lattices, 701
 - of partially ordered set, 686
- Lower limit, of summation, 217
- Lucas, Édouard, 545
- Lucas, François Édouard, 215
- Lucas numbers, 464, 569
- Lucas sequence, 215
- Lukasiewicz, Jan, 866
- Machine minimization, 1027
- Machines
 - finite-state, 999, 1012–1018, 1020–1034, 1064
 - Mealy, 1017, 1064
 - Moore, 1017, 1019
 - Turing, 999, 1048, 1049, 1051–1061
 - unit-delay, 1016
- Majority element, 269
- Makespan, 305
- Male optimal, 303
- Mappings, 186. *See also* Functions
- Maps, coloring of, 804
- m -ary trees, 829, 891
 - balanced, 834–835
 - complete, 837
 - full, 829, 833–834, 891
 - number of leaves in, bound for, 835–836
- Master theorem, 577
- Matched edges, 726
- Matchings, 814
 - bipartite graphs and, 725–728
 - complete, 726, 814
 - maximum, 726, 814
- Mathematical Analysis of Logic* (Boole), 6
- Mathematical induction, 36, 396–419
 - axiom, A–5
 - bad of, 400
 - creative uses of, 411
 - definition of, 396
 - good of, 400
 - proofs by. *See* Proofs, by
 - mathematical induction validity of, 419–420
 - as valid proof technique, 398–399
- Mathematical statements, translated into logical expressions, 71–72
- A Mathematician's Apology*, 118
- Matrix-chain multiplication, 291
- Matrix/matrices, 238–243
 - addition of, 239, 247
 - adjacency, 738–739, 759, 814
 - arithmetic, 239–240
 - Boolean product of, 242
 - definition of, 238
 - diagonal, 245
 - equal, 238
 - identity, 241, 247
 - incidence, 740, 814
 - multiplication, 290–291, 574–577
 - powers of, 241–242
 - product of, 239–240, 247
 - representing relations using, 647–650
 - sparse, 739
 - square, 238, 241
 - symmetric, 242, 247
 - transpose of, 241–242, 247
 - upper triangular, 300
 - zero-one, 242–243, 247
- Maurolico, Francesco, 398
- Maximal elements, 684–686
- Maximum matching, 726, 814
- Maximum spanning tree, 890
- Maxterm, 910
- McCarthy, John, 466
- McCarthy 465 function, 465
- McCluskey, Edward, 926
- Mealy, G. H., 1017
- Mealy machines, 1017, 1064
- Mean, 267
 - arithmetic, 121, 418
 - geometric, 121, 418
 - harmonic, 132
 - quadratic, 132
- Median, 267
- Meet
 - in lattice, 701
 - of zero-one matrix, 242, 247
- Members, of sets, 157, 246
- Membership tables, 176, 247
- Memoization, 551
- Merge sort, 456–460, 462, 574
 - complexity of, 577
 - recursive, 457
- Mersenne, Marin, 334

- Mersenne primes, 334, 335, 387
- Mesh network, 729
- Metacharacters, 1012
- Methods
 - middle-square, 371
 - Quine-McCluskey, 918, 918, 926–929
 - roster, 157, 246
- Methods of proof, 100
 - by cases, 112, 113–116
 - by contradiction, 105–108
 - by contraposition, 101–105
 - direct, 100–101
 - by exhaustion, 112–113
 - proofs of equivalence, 106–107
 - trivial, 103
 - vacuous, 102
- Methodus Differentialis*, 199
- Metrics, 185
- Middle-square method, 371
- Millbanke, Annabella, 37
- Miller's test for base b , 364
- Minimal elements, 684–686
- Minimization of combinational circuits, 917–929
- Minimum dominating set, 818
- Minimum spanning forest, 890
- Minimum spanning trees, 884–889
 - algorithms for, 884–889
 - definition of, 884, 892
- Minmax strategy, 850, 891
- Minterm, 908, 932
- Mistakes, in proofs, 108–109
- Mixed graph, 707
- Mode, 267
- Modeling
 - computation. *See* Computation
 - models
 - with graphs, 708–714
 - with recurrence relations, 543–549
 - with trees, 830–833
- modfunction, 310, 324
- Modular arithmetic, 308–309, 311–315, 387
- Modular exponentiation, 325–326
 - algorithm, 326
 - recursive algorithm for, 452
- Modular properties, in Boolean algebra, 907
- Module dependency graph, 711
- Modulus, 311
 - for linear congruential method, 367
- Modus ponens, 83, 84
 - universal, 94
- Modus tollens, 84
 - universal, 95
- Mohammed's scimitars, 768
- Molecules, trees modeling, 830
- Monoalphabetic ciphers, 376
- Monotone decreasing, 822
- Monotone increasing, 822
- Monotonic grammars, 1004
- Moore, E. F., 1017
- Moore machine, 1017, 1019
- Muddy children puzzle, 24
- Multicasting, Internet Protocol, 872
- Multigraphs, 706, 707, 814
 - directed, 707, 814
 - Euler path of, 767–768
- Multilevel security policy, 687
- Multinomial coefficient, 529
- Multinomial theorem, 529
- Multiple directed edges, 707, 814
- Multiple edges, 706, 814
- Multiple output circuit, 914
- Multiples, 308
- Multiplexer, 917
- Multiplication algorithm, 323–324
 - associative laws for, A–1
 - closure laws for, A–1
 - commutative laws for, A–1
 - integers, 574
 - inverse laws for, A–2
 - matrix, 290–291, 574–577
 - matrix-chain, 291
- Multiplicative compatibility law, A–2
- Multiplicative inverse, 71
- Multiplicatively homomorphic, 384
- Multiplicity
 - edges of, 707
 - of multisets elements, 180
- Multiplier, for linear congruential method, 367
- Multisets, 180–181
 - cardinality of, 181
 - definition of, 180, 246
 - difference of, 181
 - intersection of, 181
 - multiplicities of elements, 181
 - sum of, 181
 - union of, 181
- Mutually reachable vertices, 761
- Mutually relatively prime, 391
- Naive set theory, 160
- Naive string matcher, 261–262
- NAND operator, 909, 932
- n -ary predicate, 48
- n -ary relations, 635–644, 696
 - degree, 635
 - domains, 635
 - operations on, 638–639
- Natural language, 1000
- Natural language understanding (NLU), 713
- Natural numbers, 159
 - sets of, 156
- Naur, Peter, 1008
- NAUTY (software for isomorphism testing), 744
- n -cube, 722, 814
- n -dimensional hypercube, 722
- Negation, 148
 - of nested quantifiers, 74–75
 - of propositions, 3, 4
 - of quantified expression, 56–57
 - truth table for, 4
- Negation laws, 33
- Negation operator, 4
- Neighbors, in graphs, 718
- Nested loops, 68
- Nested quantifiers, 67
 - negation of, 74–75
 - statements involving, 67–68
 - translating into English, 72
 - translating mathematical statements into statements involving, 71–72
- Network number (netid), 478
- Networks
 - communication, 709
 - computer. *See* Computer network
 - gating, 911
 - information, 710
 - mesh, 729
 - semantic, 713
 - social, 708
 - tree-connected, 832–833
- Niche overlap graph, 712
- Nim, 848
- NLU. *See* Natural language understanding (NLU)
- Nodes. *See* Vertex (vertices)
- Noncomplete edges, 721
- Nonconstructive existence proofs, 117–119, 150

- Noncontracting grammars, 1004
- Nonconvex polygon, 424
- Nondecreasing integers, 266
- Nondeterministic finite-state automata, 1030–1033, 1064
- Nondeterministic Turing machine, 1056–1057, 1064
- Nonisomorphic graphs, 741
- Nonoverlapping, 429
- Nonplanar graphs, 797
- Nonseparable graphs, 753, 815
- Nonterminals, 1001
- Nonterminal symbols, 1001
- NOR operator, 909, 932
- Notation
 - big- O , 271–275
 - big- Ω (big- Ω), 280–282, 300
 - big- Θ (big- Θ), 280–282, 300
 - infix, 863–867, 892
 - Polish, 864, 892
 - postfix, 864–867, 892
 - prefix, 864–867, 892
 - reverse Polish, 865, 892
 - sequence, 209
 - set builder, 158
 - summation, 217
- NOT gate, 25
- Not invertible function, 192
- Noun, 1000, 1001
- Noun phrase, 1000, 1001
- NP (class of nondeterministic polynomial-time problems), 294, 1060–1061, 1064
- NP-complete problems, 294–295
- n -place predicate, 48
- n -queens problem, 38–40, 878
- n -tuples, 636
 - ordered, 164
- Null quantification, 66
- Null set, 160, 246
- Null string, 1001
- Numbering plan, 473–474
- Numbers
 - Bacon, 751
 - Bell, 677
 - cardinal, 163
 - Carmichael, 360, 388
 - Catalan, 549
 - chromatic, 804, 815
 - complex, 158
 - crossing, 803
 - edge chromatic, 812
 - Erdős, 699, 751
 - Fibonacci. *See* Fibonacci numbers
 - harmonic, 285, 406
 - independence, 821
 - Lucas, 464, 569
 - natural, 158
 - pseudorandom, 367–368
 - Ramsey, 493
 - rational, 158
 - real, 158
 - routing transit, 391
 - Ulam, 250
- Number-theoretic functions, 1055
- Number theory, 307, 372
- Objects, 160
 - distinguishable, 522–523
 - indistinguishable, 523–525
- Obligato game, 152
- Octal expansions, 318
 - conversion between binary expansion and, 320
- Octal representation, 320, 388
- Odd integer, 101
- Odd pie fights, 411–412
- Odlyzko, Andrew, 216
- One's complement, 328
- One-to-one correspondence, 191, 193, 247
- One-to-one function, 188–192, 247, 472
- On-Line Encyclopedia of Integer Sequences (OEIS), 216
- Onto functions, 188–192, 247, 610–611
- Open interval, 159, 418
- Open problems, 127–129
 - about primes, 337–339
- Operands, well-formed formula of, 438–440
- Operators
 - bitwise, 13, 14, 149
 - logical. *See* Logical operators
 - negation, 4
 - selection, 638, 696
 - well-formed formulae of, 438–440
- Opposite parity, 101
- Optimal algorithm, 299
- Optimal connectivity, 820
- Optimal for suitors, 430
- Optimization problems, 262
- Order, of quantifiers, 68–70
- Order axioms, A–1, A–2
- Ordered n -tuples, 164
- Ordered pairs, 165
- Ordered rooted tree, 829, 891
- Ordering
 - lexicographic, 444, 529, 680–682, 697
 - partial, 677–692, 697
 - quasi-ordering, 701
 - total, 679, 690, 697
- Ordinary generating function, 583
- Ore, Øystein, 772, 774
- Ore's theorem, 773
- Organizational tree, 831–832
- OR gate, 25, 911, 932
- Orientation of undirected graph, 820
- OR operator, 14, 22
- Out-degree of vertex, 720, 814
- Output, algorithms, 255
- Output alphabet, 1014
- Output function, 1014
- P (class of polynomial-time problems), 294, 1060–1061, 1064
- Paillier cryptosystem, 387
- Pairwise relatively prime integers, 341, 387
- Palindrome, 266, 485, 1010
- Paradoxes, 160, 246
 - Russell's, 170, 235
- Parallel algorithms, 729
- Parallel processing, 296, 729
 - tree-connected, 832–833
- Parent, of vertex, 828, 891
- Parent relations, 631–632
- Parity
 - opposite, 101
 - same, 101
- Parity check bits, 368
- Parse trees, 1005–1007, 1064
- Parsing
 - bottom-up, 1006
 - top-down, 1006
- Partial functions, 199, 247
 - codomain of, 199
 - domain of, 199
 - domain of definition, 199
 - undefined values of, 199
- Partially homomorphic, 384
- Partially ordered set, 677, 697
 - comparable elements of, 678

- dense, 695
- dual of, 693
- elements of, 677
- greatest element of, 684
- Hasse diagram of, 682–684
- least element of, 684
- maximal elements in, 684–686
- minimal elements in, 684–686
- well-founded, 695
- Partial orderings, 677–692, 697
- Partitions
 - of positive integers, 448, 525, 602
 - refinement of, 676
 - of sets, 670–673, 697
- Pascal, Blaise, 441
- Pascal's identity, 510–512, 535
- Pascal's triangle, 510–512, 534
- Passwords, 477
- Paths, 750–751
 - in acquaintanceship graphs, 750
 - in collaboration graphs, 751
 - counting between vertices, 758–759
 - in directed graphs, 655–656, 696
 - Euler, 765–770, 815
 - Hamilton, 770–775, 815
 - and isomorphism, 757–758
 - length of. *See* Length of path
 - in undirected graph, 815
- Pattern, strings, 261
- Payoff, 848
- Pecking order, 820
- Peirce, Charles Sanders, 48
- Pendant vertex, 719, 814
- Perfect graphs, 808
- Perfect power, 113
- Perfect square, 101
- Permutations, 497–500, 534
 - generalized, 516–525
 - generating, 529–531
 - with indistinguishable objects, 521–522
 - with repetition, 516
- Petersen, Julius Peter Christian, 780
- Petersen graph, 778
- Phrase-structure grammars, 1001–1004, 1063
 - types of, 1004–1005
- Pick's theorem, 429
- Pigeonhole principle, 105, 488–494, 535
 - applications of, 492–494
 - generalized, 490–492, 535
- Planar graphs, 792–798, 815
 - applications of, 793
 - Euler's formula and, 794–797
- Polish notation, 864, 892
- Polygon
 - convex, 424
 - definition of, 424
 - nonconvex, 424
 - sides, 424
 - simple, 424
 - triangulations, 425
 - vertex, 424
- Polynomial complexity, 293, 294
- Polynomials, big- O estimates for, 275
- Polyominoes, 126
- Poset. *See* Partially ordered set
- Positive integers, 158, 308, 395
 - partition of, 448, 525, 602
 - prime factorization of, 348
- Positive real numbers, 158
- Postconditions, 49
- Postfix form, 865
- Postfix notation, 864–867, 892
- Postorder traversal, 856, 860–862, 863–864, 892
- Postulates, 99
- Power generator, 371
- Powers, of matrices, 241–242
- Power series, 584–587
 - formal, 584
- Power sets, 164, 247
- Precedence
 - of logical operators, 12
 - of quantifiers, 54
- Precedence graphs, 711
- Preconditions, 49
- Predicate calculus, 50
- Predicate logic, 46
- Predicates, 46–49, 149
 - logically equivalent, 55
 - n -ary, 48
 - n -place, 48
 - truth set of, 167
- Prefix codes, 844–846
- Prefix form, 864
- Prefix notation, 864–867, 892
- Preimage, of element, 186, 247
- Premises
 - of argument, 60, 81, 82, 149
 - of conditional statement, 7
- Preorder traversal, 856–857, 862, 863–864, 892
- Prim, Robert Clay, 887, 888
- Primary key, 636–637, 696
- Prime implicant, 920, 932
- Prime number theorem, 335–336
- Primes, 330–331, 387
 - and arithmetic progressions, 337
 - conjectures about, 337–339
 - distribution of, 335–336
 - factorization, 332
 - infinitude of, 333–335
 - mutually relatively, 391
 - open problems about, 337–339
 - primitive root of, 361, 388
- Primitive root, of primes, 361, 388
- Prim-Jarník algorithm, 885–886
- Prim's algorithm, 885–886, 892
- Principia Mathematica*, 42, 161
- Principle of buoyancy, A–5
- Principle of inclusion–exclusion, 172, 479, 602–606, 615
 - alternative form of, 608–609
 - applications of, 608–613
- Principle of mathematical induction, 397
- Principles
 - counting, 471–477
 - Dirichlet drawer, 488
 - duality, 904
 - pigeonhole, 105, 488–494, 535
 - of well-ordered induction, 679
- Private key cryptosystems, 377–378
- Private key encryption, 388
- Probability generating function, 602
- Problems
 - art gallery, 813
 - busy beaver, 1063
 - celebrity, 418
 - Chinese postman, 770
 - closest-pair, 578–580
 - Collatz, 128
 - counting, 470, 477–478
 - decidable, 1058–1059
 - decision, 1058, 1064
 - discrete logarithm, 361
 - gossip, 418
 - halting, 265–266, 1059
 - hatcheck, 611–613
 - Hilbert's Tenth, 1059
 - houses-and-utilities, 792
 - intractable, 294, 301, 1061

- jealous husbands, 764
- Josephus, 555
- Kakutani's, 128
- kissing, 216
- knapsack, 304, 617
- longest path, 792
- NP-complete, 294–295
- n -queens, 878
- open, 127–129, 337–339
- optimization, 262
- P versus NP, 294–295
- satisfiability, 41
- searching, 256
- shortest-path, 781–789, 815
- solvable, 294, 301, 1058–1059, 1064
- Syracuse, 128
- tractable, 293, 301, 1061
- traveling salesperson, 773, 783, 787–789, 815
- Ulam's, 128
- undecidable, 1058
- unsolvable, 294, 301, 1058, 1064
- Procedure statements, A–10
- Product
 - Boolean, 899, 901, 931
 - of matrix, 239–240
- Productions, of grammars, 1001
- Product-of-sums expansion, 910
- Product rule, 471, 534
 - for sets, 535
 - partial, 393
- Projection, 614, 696
- Proofs, 99
 - bijective, 503
 - by cases, 112, 113–116, 150
 - combinatorial, 503, 534
 - by contradiction, 105–107, 150
 - by contraposition, 101–105, 150
 - definition of, 99, 150
 - direct, 100–101, 150
 - double counting, 503
 - of equivalence, 106–107
 - exhaustive, 112–113, 150
 - existence. *See* Existence proofs
 - existing, adapting, 122
 - indirect, 102
 - informal, 99
 - by mathematical induction. *See* Proofs, by mathematical induction
 - methods of. *See* Methods of proof
 - mistakes in, 108–109
 - trivial, 103, 150
 - uniqueness, 119–120, 150
 - using strong induction, 421–424
 - vacuous, 102, 150
- Proofs, by mathematical induction, 399–414
 - of divisibility results, 406–408
 - examples of, 400–414
 - guidelines for, 399–400
 - of inequalities, 404–406
 - mistaken, 412–414
 - of results about algorithms, 410–411
 - of results about sets, 408–410
 - summation formulae, 401–404
- Proof strategy, 103–105, 120–123
- Proper subgraph, 730
- Proper subset, 162, 246
- Properties
 - Archimedean, A–4
 - relations, 624–629
 - of trees, 833–836
 - well-ordering, 427–428, 462, A–5
- Propositional calculus, 3
- Propositional equivalences, 30–41, 173
- Propositional function, 47, 48, 149
- Propositional logic, 1–14, 46
 - applications of, 20–26
 - argument in, 82
 - rules of inference for, 83–85
 - valid arguments in, 81–82
 - well-formed formulae in, 438
- Propositional variables, 3, 148
- Propositions, 2–7
 - atomic, 3
 - compound. *See* Compound propositions
 - conjunction of, 4
 - definition of, 2, 99, 149
 - disjunction of, 5–6
 - negation of, 3, 4
 - truth value of, 3
- Protein interaction graphs, 712, 713
- Protocols
 - cryptographic, 382–383
 - Diffie-Hellman key agreement, 382
 - key exchange, 388
- Pseudocode, 254–255, A–10
- Pseudographs, 706, 707, 814
- Pseudoprimes, 359–361, 388
 - to base b , 360
- Pseudorandom numbers, 367–368
 - generated by linear congruential method, 367
 - middle-square generator, 371
 - power generator for, 371
 - pure multiplicative generator, 368
- Public key cryptography, 373, 377–378
- Public key cryptosystems, 378
- Public key encryption, 388
- Pumping lemma, 1051
- Pure multiplicative generator, 368
- Pushdown automaton, 1049
- Puzzles
 - Icosian, 770
 - jigsaw, 429
 - logic, 23–25
 - muddy children, 24
 - Reve's, 546
 - Sudoku, 40–41
 - Tower of Hanoi, 545–548
- P versus NP problem, 294–295
- Pythagorean triples, 128
- Quadratic mean, 132
- Quadratic nonresidue, 365
- Quadratic residue, 364
- Quantification, 49
 - existential, 49, 52, 149
 - and looping, 54, 68
 - null, 66
 - universal, 49, 50, 55–56, 149
- Quantified expression, negation of, 56–57
- Quantified statements restricted domain, 167
 - rules of inference for, 93–94
- Quantifiers, 49–53
 - De Morgan's laws for, 57–58
 - existential, 52–53
 - finite domain, 53–62
 - logical equivalences, 55
 - nested. *See* Nested quantifiers
 - order of, 68–70
 - precedence of, 54
 - with restricted domains, 54
 - scope of, 55
 - in system specifications, 60
 - truth sets and, 167

- universal, 50–51
- Quasi-ordering, 701
- Quick sort, 461
- Quine, Willard Van Orman, 928
- Quine–McCluskey method, 918, 926–929
- Quotient, 310, A–6
- Quotient automaton, 1037

- Radius, of graphs, 821
- Ramanujan, Srinivasa, 118, 120
- Ramsey, Frank Plumpton, 494
- Ramsey number, 493
- Ramsey theory, 494
- Range, of function, 186, 247
- Ratio, common, 210
- Rational numbers, 104, 150, 158
- r -combinations, 500, 521, 534
- Reachable vertex, 761, 896
- Real numbers, 158
 - axioms for, A–1–A–2
 - positive, 158
 - upper bound, A–3
- Real-valued functions, 188
- Reasoning
 - backward, 121
 - circular, 109, 149
 - deductive, 397
 - forward, 121
 - inductive, 397
- Recognizes, by finite-state machine, 1017
- Records, databases, 636
- Recurrence relations, 211–213, 615
 - algorithms and, 549–553
 - applications of, 543–553
 - associated homogenous, 564
 - definition of, 247
 - divide-and-conquer, 573–580
 - linear, solving, 557–567
 - linear homogeneous, 558–564
 - linear nonhomogeneous, 564–567
 - modeling with, 543–549
 - simultaneous, 571
 - solution of, 211, 543
- Recursion, 432, 455–456
- Recursive algorithms, 450–460, 462
 - binary search, 453
 - for computing a^n , 450
 - for computing greatest common divisor, 451
 - for computing $n!$, 450
 - correctness of, 453–454
 - for Fibonacci numbers, 455
 - linear search, 453
 - for modular exponentiation, 452
 - trace of, 450
- Recursive definitions, 395, 433
 - of extended binary trees, 439
 - of functions, 433–436, 462
 - of sets, 436–441, 462
 - of strings, 437
 - of structures, 436–441
- Recursive merge sort, 457
- Recursive modular exponentiation, 452
- Recursive step, 436
- Reentrant knight's tour, 779
- Refinement, of partitions, 676
- Reflexive closures, 654–655
- Reflexive relation, 626, 629, 696
- Regions, of planar representation
 - graphs, 794, 815
- Regular expressions, 1039, 1064
- Regular grammars, 1004, 1063
- Regular graph, 736, 814
- Regular language, 1004
- Regular sets, 1038, 1039, 1046–1047, 1064
- Relational data model, 636, 696
- Relations, 696
 - antisymmetric, 627–628, 696
 - asymmetric, 633
 - binary, 623
 - circular, 699
 - closures of. *See* Closures, of relations
 - combining, 629–632
 - complementary, 633
 - composite of, 629–630
 - connectivity, 657, 697
 - covering, 682
 - databases and, 636–637
 - diagonal, 654
 - divisibility, 678
 - equivalence, 665–673, 697
 - extension of, 637
 - functions as, 624
 - “greater than or equal,” 678
 - inverse, 633
 - irreflexive, 632
 - n -ary. *See* n -ary relations parent, 631–632
 - properties of, 625–629
 - recurrence. *See* Recurrence relations
 - reflexive, 626, 629, 696
 - representing. *See* Relations, representation of on set, 624–625
 - representation of on set, 624–625
 - of sets, 167
 - symmetric, 627–628, 696
 - transitive, 628–629, 631, 696
- Relations, representation of, 646–650
 - using digraphs, 650–651
 - using matrices, 646–650
- Relatively prime integers, 341, 387
- Remainder, 310
- Rencontres*, 612
- Repetition
 - combinations with, 517–521
 - permutations with, 516
- Representative, of equivalence class, 668
- Resolution (rules of inference), 84,
- Restricted domains, quantifiers with, 54, 167
- Results, 99
- return** statement, A–14
- Reverse-delete algorithm, 891
- Reverse Polish notation, 865, 892
- Reve's puzzle, 546
- Right child, of vertex, 830
- Right triominoes, 126, 413
- Ring topology, 728
- Rivest, Ronald, 378
- RNA (ribonucleic acid), 474
- Rocket-powered Frisbee, 900
- Root, 439, 828
- Rooted Fibonacci trees, 838
- Rooted spanning tree, 884
- Rooted trees, 439, 828–830
 - decision trees, 842–844
 - definition of, 828, 891
 - height of, 834, 891
 - ordered, 829, 891
- Roster method, 157, 246
- Round-robin tournament, 427, 725
- Routing transit number (RTN), 391
- Roy, Bernard, 660
- Roy–Warshall algorithm, 660–663
- r -permutation, 498, 521, 534
- RSA cryptosystem, 373, 388
- RSA system, 378
 - cryptosystem, 378–379
 - decryption, 380

- digital signatures, 383
- encryption, 379–380
- as public key system, 381–382
- Rule
 - division, 481, 534
 - product, 471, 534
 - sum, 471, 475
- Rules of inference, 81–95, 149
 - addition, 84
 - and argument building, 85–86
 - conjunction, 84
 - disjunctive syllogism, 84
 - hypothetical syllogism, 84
 - modus ponens, 83, 84
 - modus tollens, 84
 - for propositional logic, 83–85
 - for quantified statements, 93–94,
 - resolution, 84
 - simplification, 84
- Rules of syntax, 1000
- Russell, Bertrand, 160
- Russell's paradox, 170, 235
- Same order, big-*O* relationships, 272
- Same parity, 101
- Satisfiability, 38
 - applications of, 38
 - problems, solving, 41
- Satisfiable compound propositions, 38, 149
- Saturated hydrocarbons, trees
 - modeling, 830
- Scheduling problems final exams, 809–810
 - greedy algorithm for, 410–411
- Schröder–Bernstein theorem, 230–231
- Scope, of quantifiers, 54
- Search algorithms, 256–258, 300
 - binary, 257–258, 301
 - breadth-first, 875–877
 - depth-first, 872–875
 - linear, 256, 301
 - ternary, 267
- Search engines, 880
- Searches
 - Boolean, 22–23
 - Web page, 22–23
- Searching problems, 256
- Second principle of mathematical induction, 420
- Seeds, 880
 - for linear congruential method, 367
- Sees, 813
- Selection operator, 638, 696
- Selection sort, 268
- Self-complementary graph, 747
- Self-converse directed graph, 819
- Self-dual Boolean function, 933
- Self-generating sequences, 468
- Semantic networks, 713
- Semantic relation, 713
- Semantics, 1000
- Sentence, 1000, 1001
- Sentential variables, 3
- Separating set, 753
- Sequences, 156, 209–217
 - definition of, 209, 247
 - Fibonacci, 211–212
 - finding maximum and minimum of, 573
 - generating functions for. *See* Generating functions
 - Golomb's self-generating, 468
 - graphic, 735
 - integer, 214–217
 - Lucas, 215
 - notation, 209
 - recurrence relations. *See* Recurrence relations
 - self-generating, 468
 - strictly decreasing, 493
 - strictly increasing, 493
 - unimodal, 618
- Sequential search algorithm, 256
- Serial algorithms, 728
- Series
 - geometric, 218
 - harmonic, 406
 - infinite, 221
 - power, 584–587
- Set builder notation, 158, 246
- Set equality, 246
- Set identities, 173–176
 - absorption laws for, 174
 - associative laws for, 174
 - commutative laws for, 174
 - complementation law for, 174
 - complement laws for, 174
 - De Morgan's laws for, 174
 - distributive laws for, 174
 - domination laws for, 174
 - idempotent laws for, 174
 - identity laws for, 174
 - methods of proving, 177
- Sets, 156–168, 246
 - atomic, 173
 - cardinality of, 163, 225–235, 247
 - Cartesian products of, 164–167
 - complement of, 173, 174, 247
 - of complex numbers, 158
 - computer representation of, 179–180
 - countable, 226–228, 247
 - definition of, 157
 - difference of, 173, 174, 247
 - disjoint, 171
 - elements/members of, 157
 - empty, 160, 246
 - equality of, 159, 246
 - finite. *See* Finite sets
 - fuzzy, 185
 - guarding, 813
 - identities. *See* Set identities
 - infinite, 156, 164, 247
 - of integers, 158
 - intersection of, 171, 177–179, 247
 - language of, 157–158
 - linearly ordered, 679
 - naive theory, 160
 - of natural numbers, 157
 - not recognized by finite-state automaton, 1047
 - null, 160, 246
 - operations, 170–181
 - partially ordered. *See* Partially ordered set
 - partition of, 670–673
 - power, 164, 247
 - product rule for, 534
 - recognition, Turing machine and, 1054–1055
 - recursive/inductive definitions of, 436–341, 462
 - regular, 1038, 1039, 1046–1047, 1064
 - relation of, 167
 - relation on, 624–625
 - roster method, 157
 - separating, 753
 - singleton, 160
 - size of, 163
 - of strings, 1020–1021
 - successor of, 184
 - totally ordered, 679
 - uncountable, 225, 229–235, 247
 - union of, 170–171, 177–179, 247

- universal, 160, 246
- well-ordered, 466, 679, 697
- Shaker sort, 303
- Shamir, Adi, 378
- Shannon, Claude Elwood, 900
- Sheffer, Henry Maurice, 42
- Sheffer stroke, 42
- Shift ciphers, 373, 375, 376, 388
- Shortest-path algorithm, 783–787
- Shortest-path problems, 782–789, 815
- Siblings, of vertex, 828, 891
- Sides, of polygon, 424
- Sieve of Eratosthenes, 332–337, 388, 609–610, 615
- Signatures, digital, 383, 388
- Signed integer, 1011
- Signless Stirling numbers of the first kind, 524, 539
- Simple directed graph, 707, 814
- Simple graphs, 705, 707, 721–722, 814
 - coloring of, 804
 - crossing number of, 803
 - dense, 740
 - isomorphic graphs, 741–744
 - orientation of, 820
 - paths in, 750
 - self-complementary, 747
 - with spanning trees, 870–872
 - sparse, 739, 745, 889
 - thickness of, 803
 - union of, 732
 - vertices of, 731, 737
- Simple path, 750, 815
- Simple polygon, 424
- Simplification (rules of inference), 84
- Single-elimination tournament, 714
- Singleton set, 160
- Sink, 1066
- Size, of sets, 163
- S_k -tree, 894
- Slackness, of job, 304
- Sloane, Neil, 216
- Smullyan, Raymond, 23–24
- Social networks, 708
- Sollin's algorithm, 890
- Solution, 38
 - of recurrence relations, 211, 543
- Solvable problem, 294, 301, 1058–1059, 1064
- Sorting
 - definition of, 258, 300
 - topological, 690–692, 697
- Sorting algorithms, 258–260
 - bidirectional bubble sort, 303
 - bubble sort, 259–260, 301
 - insertion sort, 260, 301
 - merge sort, 456–460, 462, 574
 - quick sort, 461
 - selection sort, 268
 - shaker sort, 303
- Space complexity, 286, 301
- Spanning forest, of graph, 882
- Spanning trees, 870–880, 892
 - breadth-first search and, 875–877
 - definition of, 870
 - degree-constrained, 895
 - depth-first search and, 872–875
 - in IP multicasting, 872
 - maximum, 890
 - minimum, 884–889, 892
 - rooted, 884
- Sparse graphs, 739, 745, 889
- Sparse matrix, 739
- Specifications system, 21–22
- SQL (Structured Query Language), 640
- Squarefree integer, 614
- Square matrix, 238, 241
- Stable matching, 269
- Standard checkerboard, 124
- Star height, 1066
- Star topology, 728
- Start state, 1021
- State diagram, 1014
- Statements, A–10
 - assignment, A–10–A–11
 - biconditional, 11, 34, 149
 - block of, A–13
 - conditional. *See* Conditional statements
 - if then**, 48, A–11–A–12
 - involving nested quantifiers, 67–68
 - procedure, A–10
 - return**, A–14
- States, 1014, 1021
- State table, 1014
- Stirling, James, 199
- Stirling numbers of the second kind, 524
- Stirling's formula, 198
- Straight triomino, 126
- Strategy
 - minmax, 850, 891
 - proofs, 103–105, 120–124
- Strictly decreasing functions, 189
- Strictly decreasing sequence, 493
- Strictly increasing functions, 189
- Strictly increasing sequence, 493
- String matching, 261–262
- Strings, 210, 247
 - bit, 13
 - counting, 474
 - distinguishable, 1051
 - empty, 210, 247, 1001
 - indistinguishable, 1051
 - length of, 210, 437
 - lexicographic ordering of, 680
 - null, 1001
 - pattern, 261
 - recognized/accepted, 1023
 - set of, 1020–1021
 - ternary, 554
- String searching, 300
- Stroke, Sheffer, 42
- Strong association rules, 644
- Strong induction, 419–426, 462
 - in computational geometry, 424–426
 - and infinite ladder, 420–421
 - proofs using, 421–424
 - validity of, 419–420
- Strongly connected components
 - of directed graph, 756–757, 815
 - of web graph, 757
- Strongly connected graphs, 757
- Strong pseudoprime to base b , 364
- Structural induction, 433, 441–444, 462
 - examples of proofs using, 442–444
- Structured Query Language (SQL), 640
- Structures, recursive/inductive
 - definitions of, 436–441
- Subgraph, 730, 814
- Subgraph induced, 730
- Subsequence, 493
- Subsets, 161–163, 246
 - counting number, of finite set, 408–410, 474
 - image of, 188
 - inverse image of, 202
 - proper, 162, 246
 - sums of, 879
- Subtraction rule, 479–481, 534

- Subtractors
 - full, 916
 - half, 916
- Subtree, 828, 891
- Successor, of sets, 184
- Sudoku, 40–41
- Suites, 269
- Suitors, 269
- Summations, 217–221
 - formulae, 221, 401–404
 - index of, 217–218
 - lower limit, 217
 - notation, 217
 - upper limit, 217
- Sum-of-products expansions, 907–909, 932
- Sum rule, 471, 475, 534
- Sums
 - Boolean, 901, 932
 - of geometric progressions, 404
 - of matrices, 239
 - of multisets, 180
 - of subsets, 879
- Sun-Tsu, 354
- Superset, 161
- Support, 642, 696
 - of association rule, 643–644, 696
- Surjection, 190, 247
- Surjective functions, 190
- Symbolic Logic, 163
- Symbols, 1001
- Symmetric closure, 655
- Symmetric difference, 183, 247
- Symmetric matrix, 242, 247
- Symmetric relations, 627–628, 696
- Syntax, 1000
- Syracuse problem, 128
- System of distinct representatives (SDR), 818
- System specifications, 21–22
 - quantifiers in, 60
- Tables, 636
- state, 1014
- Tao, Terence, 337
- Tautology, 31, 41, 83, 149
- Telephone calls, 709
- Telephone numbering plan, 473–474
- Terminals, 1001
- Terminal vertex, 650
- Ternary search algorithm, 267
- Ternary string, 554
- Test/testing
 - Miller's, 364
- Text, 261
- Theorems
 - art gallery, 813
 - Bézout's, 345–347, 388
 - binomial, 507–510, 535
 - Chinese remainder, 354–356, 389
 - Cook-Levin, 294
 - definition of, 100, 149
 - Dirac's, 773
 - extended binomial, 586
 - Fermat's last, 128, 273
 - Fermat's little, 358–359, 389
 - four color, 804, 815
 - fundamental theorem of arithmetic, 330, 388, 422
 - Hall's marriage, 726–728, 815
 - handshaking, 719–720, 815
 - Kleene's, 1040–1041, 1064
 - Kuratowski's, 797–798, 815
 - master, 577
 - methods of proof, 100
 - multinomial, 529
 - Ore's, 773
 - Pick's, 429
 - prime number, 335–336
 - Schröder-Bernstein, 230–231
 - stating, 100
 - Wilson's, 363
- Thickness, of simple graphs, 803
- Threshold function, 934
- Threshold gate, 934
- Threshold value, 934
- Tic-tac-toe, 849–850
- Tilings, of checkerboards, 124–127, 412–413
- Time complexity, 286–289, 300
 - average-case, 288, 301
 - worst-case, 287–288, 301
- Top-down parsing, 1006
- Topological sorting, 690–692, 697
- Topology
 - ring, 728
 - star, 728
- Total function, 199
- Total length field, 487
- Totally ordered sets, 679, 697
- Total ordering, 679, 697
 - compatible, 690, 697
- Tournament
 - round-robin, 427, 714
 - single-elimination, 714
- Tournament sort, 852
- Tower of Hanoi, 545–548
- Trace, algorithm, 255, 450
- Tractable problem, 293, 301
- Tractable problems, 1061
- Trail, 750
- Transaction, 642
- Transformations, 186. *See also*
 - Functions
 - affine, 375
- Transition function, 1014, 1021, 1022
- Transition rules, 1052
- Transitive closures, 654, 657–660
 - computing procedure, 660
- Transitive relations, 628–629, 631, 696
- Transitivity law, A–2
- Translation
 - English sentences to logical expressions, 20–21, 58–60, 72–72
 - mathematical statements to logical expressions, 71–72
 - nested quantifiers into English, 72
- Transpose, of matrix, 241–242, 247
- Transposition cipher, 376
- Transposition error, 370
- Traveling salesperson problem (TSP), 773, 783, 787–789, 815
- Traversal algorithms. *See* Tree traversal
- Tree-connected network, 832–833
- Tree diagrams, 482–483, 534
- Tree edges, 873
- Trees, 826–889
 - applications of, 839–851
 - binary. *See* Binary trees
 - binary search, 839–841, 891
 - caterpillar, 895
 - decision, 842–844, 891
 - definition of, 826, 826, 891
 - derivation/parse, 1005–1007, 1063
 - family, 826
 - game, 846–851, 891
 - graceful, 895
 - labeled, 838
 - m*-ary, 829
 - as models, 830–833
 - properties of, 833–836
 - rooted. *See* Rooted trees rooted
 - Fibonacci, 838
 - spanning. *See* Spanning trees

- terminology for, 828
- value of, 850
- Tree traversal, 891
 - inorder, 856, 857–860, 863–864, 892
 - postorder, 856, 860–862, 863–864, 892
 - preorder, 856, 862, 863–864, 892
 - universal address system, 855–856
- Trial division, 331–332
- Triangle inequality, 132, 185
- Triangulations, of polygon, 425
- Trichotomy law, A–2
- Triomino
 - right, 126, 413
 - straight, 126
- Trivial proof, 103, 150
- Truth set, of predicate, 167
- Truth tables
 - for biconditional statement, 11
 - of compound propositions, 12
 - for conditional statements, 7
 - for conjunction, 4
 - definition of, 149
 - for disjunction, 5
 - for exclusive or, 7
 - for negation, 4
- Truth value, 3, 149
- Tukey, John Wilder, 13
- Turing, Alan Mathison, 1048
- Turing machine, 999, 1048, 1049, 1051–1061, 1064
 - computing functions with, 1055
 - definition of, 1052–1054
 - nondeterministic, 1056–1057, 1064
 - representation of, 1052
 - and sets recognition, 1054–1055
 - transition rules, 1052
 - types of, 1056–1057
 - universal, 1057
- Twin primes conjecture, 339
- Two's complement, 329
- Type (datatype), 159
- Type 0 grammar, 1004, 1005, 1063
- Type 1 grammar, 1004, 1005, 1063
- Type 2 grammar, 1004, 1005, 1063
- Type 3 grammar, 1004, 1005, 1063
- Ulam numbers, 250
- Ulam's problem, 128
- Unary representations, of integers, 1055
- Uncomputable functions, 235, 247, 1059, 1064
- Uncountable sets, 225, 229–235, 247
- Undecidable problem, 1058
- Undefined values, of partial function, 199
- Underlying undirected graph, 721
- Undirected edge, 707, 814
- Undirected graphs, 707, 718, 720, 814
 - connectedness in, 752–753
 - density of, 745
 - Euler circuit of, 765
 - orientation of, 820
 - underlying, 721
- Unicasting, 872
- Unicycle, 900
- Unimodal sequence, 618
- Union
 - of finite sets, 602
 - of fuzzy sets, 185
 - of graphs, 732–733, 814
 - of multisets, 180
 - of sets, 170–171, 177–179, 247
- Uniqueness proof, 119–120, 150
- Unit-delay machine, 1016
- Unit (Egyptian) fraction, 465
- Unit property, in Boolean algebra, 902
- Universal address system, 855–856
- Universal generalization, 93
- Universal instantiation, 93
- Universal modus ponens, 94
- Universal modus tollens, 95
- Universal Product Code (UPC), 369
- Universal quantification, 49, 50, 55–56, 149
- Universal quantifier, 50–51
- Universal set, 160, 246
 - degree of membership, 185
- Universal transitivity, 98
- Universal Turing machine, 1057
- Universe of discourse, 50, 149
- Unmatched edges, 726
- Unsatisfiable compound propositions, 38
- Unsolvable problem, 294, 301, 1058, 1064
- UPC check digit, 369
 - Upper bound, 697
 - of lattice, 702
 - least, 686, 697, A–3
 - of partially ordered set, 686
 - of real numbers, A–2
- Upper limit, of summation, 217
- Upper triangular matrix, 300
- U.S. Coast Survey, 48
- Vacuous proof, 102, 150
- Valid argument, 81–82, 149
- Valid argument form, 82, 149
- Valid partner, 303
- Values
 - of Boolean function, 901
 - final, A–12
 - initial, A–12
 - threshold, 934
 - of trees, 850
 - truth, 3, 149
 - of vertex in game tree, 849–851, 891
- Vandermonde, Alexandre-Théophile, 512–513
- Vandermonde's identity, 512–513
- Variables, A–12
 - binding, 54–55,
 - Boolean, 13, 149, 900, 908, 931
 - free, 54, 149
 - propositional, 3, 148
 - random. *See* Random variables
 - sentential, 3
- Veitch, E. W., 918
- Vending machine, 1012–1013
- Venn, John, 163
- Venn diagrams, 160–161, 246
 - complement of sets, 173
 - difference of sets, 173
 - intersection of sets, 171
 - union of sets, 170
- Verb, 1000, 1001
- Verb phrase, 1000, 1001
- Vertex (vertices), 650
 - adjacent, 718
 - ancestors of, 828, 891
 - bipartition of, 722
 - child of, 828, 891
 - in collaboration graph, 709
 - connecting, 718
 - connectivity, 753–754, 755–756
 - counting in full m -ary trees, 833–834
 - counting paths between, 758–759
 - cut, 753, 815
 - degree, in undirected graph, 718
 - descendants of, 828, 891
 - distance between, 821

- dominating set of, 818
- eccentricity of, 838
- handle, 894
- in-degree of, 720, 814
- independent, 821
- in influence graph, 709
- initial, 650
- interior, 660
- internal, 828, 891
- isolated, 719, 814
- left child, 830
- left subtree, 830
- level of, 834, 891
- level order of, 894
- mutually reachable, 761
- out-degree of, 720, 814
- parent of, 828, 891
- pendant, 719, 814
- of polygon, 424
- reachable, 761, 896
- removing from graph, 731
- right child, 830
- right subtree, 830
- siblings of, 828, 891
- of simple graphs, 732, 737
- terminal, 650
- value in game tree, 849–851, 891
- Vertex basis, 763
- Vertex cut, 753
- Vigenère cipher, 386
- Vocabulary, 1001, 1063
- Walk, 749
- Warshall, Stephen, 660, 662
- Warshall's algorithm, 660–663
- Weakly connected graphs, 756
- Web crawlers, 880
- Web graphs, 710
 - strongly connected components of, 757
- Web pages, searching, 22–23
- Weighted graphs, 815
 - shortest path between, 781–789
- Weights, 934
- Well defined, 433
- Well-formed formulae, 438–440, 870
- Well-founded partially ordered set, 695
- Well-ordered induction, principle of, 679
- Well-ordered set, 466, 679, 697
- Well-ordering property, 427–428, 462, A–5
- Wheels, 721, 814
- Wiles, Andrew, 128
- Wilson's theorem, 363
- Without loss of generality (WLOG), 115, 150
- Witnesses
 - big- O notation, 271, 300
 - and existence proof, 117
- WLOG (without loss of generality), 115, 150
- Word, 1001
- Word and Object, 928
- Worst-case complexity, 287–288, 301
 - of binary search, 287–288
 - of bubble sort, 288–289
 - of insertion sort, 288–289
- XOR gate, 934
- XOR operator, 14
- Zermelo-Fraenkel axioms, 235
- Zero-one matrix, 242–243, 247
 - Boolean product of, 242–243, 247, 290
 - join of, 242, 247
 - meet of, 242, 247
 - representing relations using, 646–650
 - of transitive closure, 659–660
 - Warshall's algorithm and, 660–663
- Zero property, in Boolean algebra, 902
- Zhang, Yitang, 340

Mc
Graw
Hill