

- Antisymmetric relation, 577–578, 633
  - representing
  - using digraphs, 595
  - using matrices, 591–592
- Appel, Kenneth, 728
- Application(s)
  - of backtracking, 791–793
  - of Bayes’ theorem, 471–472
  - of congruences, 287
  - of graphs colorings, 731–732
  - of graph theory, 644–649, 658–663, 680–681, 687, 698, 702, 731–732
  - of inclusion–exclusion, 558–564
  - of pigeonhole principle, 403–405
  - of propositional logic, 16–22
  - of satisfiability, 32–34
  - of trees, 757–769
- Approximation algorithm, 235, 715
- Arborescence, 807
- Archimedean property, A-5
- Archimedes, A-4
- Archimedes’ screw, A-4
- Argument, 69, 110
  - Cantor diagonalization, 173, 186
  - premises of, 69
  - propositional logic, 70
  - valid, 69, 110
- Argument form, 70, 110
  - valid, 70, 110
- Aristotle, 2, 3
- Arithmetic
  - fundamental theorem of, 306, 336–337
  - modular, 240–306
  - modulo  $m$ , 243
- Arithmetic mean, 100, 332
- Arithmeticonum Libri Duo* (Maurolico), 313
- Arithmetic progression, 186
  - of primes, 262, 263
- Array linear, 662
  - two-dimensional, 662
- Arrow, Peirce, 36
- Ars Conjectandi* (Bernoulli), 459
- Art Gallery
  - problem, 735
  - theorem, 735
- Article, 848
- Articulation points, 683
- Artificial intelligence, 138, 380
  - fuzzy logic in, 16
- Assertion
  - final, 372, 378
  - initial, 372, 378
- Assignment, stable, 343
  - optimal, 343
- Assignment of jobs, 565
- Assignments, frequency, 732
- Assignment statements, A-11–A-12
- Associated homogenous recurrence relations, 520
- Associative laws, 27
  - for addition, A-1
  - for Boolean algebra, 815, 818
  - for lattices, 637
  - for multiplication, A-1
  - for propositions, 27
  - for sets, 129
- Associativity
  - for integers modulo  $m$ , 243
- Asymmetric relation, 582
- Asymptotic functions, 218
- Asynchronous transfer mode (ATM), 149
- AT&T network, 682
- Autokey cipher
  - keystream, 309
- Autokey ciphers, 309
- Automated theorem proving, 114
- Automaton
  - deterministic, 872, 873
  - deterministic finite-state, 899
  - finite-state, 866–872
    - nondeterministic, 873
  - linear bounded, 886
  - nondeterministic, 873
  - nondeterministic finite-state, 899
  - pushdown, 886
  - quotient, 878
  - set not recognized by, 885
- Average-case complexity of algorithms, 482–484
- Average-case time complexity, 220, 232
  - of linear search, 221
- Avian influenza, 476
- AVL-trees, 808
- Award
  - Turing, 854
- Axiom(s), 185, A-1–A-5
  - Completeness, A-2
  - field, A-1
  - for real numbers, A-1–A-2
  - for set of positive integers, A-5
  - in proving basic facts, A-3–A-5
  - of Mathematical Induction, A-5
  - order, A-2
  - Zermelo–Fraenkel, 176
- B-tree of degree  $k$ , 805
- Bézout coefficients, 270, 306
- Bézout’s identity, 270
- Bézout’s theorem, 269, 306
- Bézout, Étienne, 269
- Bachmann, Paul, 206
- Bachmann, Paul Gustav Heinrich, 207
- Back edges, 788
- Back substitution
  - solving systems of linear congruences using, 279
- Backtracking, 787–789, 804
  - applications of, 791–793
  - in directed graphs, 793
- Backus, John, 854
- Backus–Naur form, 899
- Backus–Naur form (BNF), 854
- Backward differences, 513
- Backward substitution
  - iteration using, 160
- Bacon, Kevin, 680–681
- Bacon number, 680
- Bacteria, 168, 501
- Balanced rooted trees, 753, 804
- Balanced strings of parentheses, 382
- Balanced ternary expansions, 256
- Bandwidth of graph, 741
- Bar
  - chocolate, 342
- Barber paradox, 16
- Base  $b$ 
  - expansions, 246, 306
    - algorithm for constructing, 248
    - Miller’s test for, 286
    - pseudoprime to the, 282
    - strong pseudoprime to, 286
- Base-10 expansions, 246
- Base conversion, 247
- Bases of DNA molecules, 389
- BASIC, 391
- Basis, vertex, 691
- Basis step, 313, 333, 349, 377, 752, 767
- Basketball, 434
- Bayes’ theorem, 468–475
  - generalized, 472
- Bayes, Thomas, 470, 472
- Bayesian spam filters, 472–475
- Begging the question, 90, 110
- Bell, E. T., 618
- Bellman, Richard, 508
- Bell numbers, 618
- Bernoulli’s inequality, 330
- Bernoulli, James, 458, 459
- Bernoulli family tree, 745
- Bernoulli trial, 479, 494
  - and binomial distribution, 458–460
- Bernstein, Felix, 175
- Bi-implication, 9
- Biconditional, 9–10, 110
  - implicit use of, 10
  - statement, 9
  - truth tables for, 9
- Biconnected graph, 684
- Bicycle racers, 475
- Bidirectional bubble sort, 233
- Bienaymé’s formula, 489
- Bienaymé, Irenée-Jules, 489
- big- $O$  estimates
  - for combinations of functions, 212
  - for exponential functions, 212
  - of important functions, 209
  - of  $n!$ , 210
  - for polynomials, 209, 212
  - for products of functions, 213
  - for sums of functions, 212
  - of logarithms, 212
- Big- $O$  notation, 205–232
  - careless use of, 216
  - origin of, 206
- Big- $O$  relationship
  - witnesses to, 205
- big-Omega ( $\Omega$ ) notation, 214, 232
- big-Theta ( $\Theta$ ) notation, 215, 232
- Big-Theta estimates for polynomials, 216
- Bit, 11
- Bijection, 144, 186
- Bijective proofs, 412
- Binary coded decimal expansion, 836
- Binary digit, 11
- Binary expansions, 246
- Binary insertion sort, 196, 203
- Binary relation, 573, 633
- Binary representation, 306
- Binary search
  - worst-case complexity, 220
- Binary search algorithm, 194, 232, 528
  - recursive, 363
- Binary search trees, 757–759, 804
- Binary trees, 352–353, 748, 749
  - definition of, 804
  - extended, 352
    - full, 352–353
    - height of, 355
  - number of vertices of, 355
  - with prefix code, 762–763
- Binit, 11
- Binomial coefficients, 410, 415–421, 439
  - extended, 539
- Binomial distribution, 458–460
- Binomial expression, 415
- Binomial theorem, 415–418, 439
  - extended, 540
- Binomial trees, 805
- Bipartite graphs, 656–658, 736
  - coloring of, 657
- Bird flu, 476
- Birthday problem, 461–463

I-4 Index

Bit, 11, 110  
    origin of term, 11  
    parity check, 290  
Bit operation(s), 11, 110  
Bits, 149  
Bit string, 12, 110 subitem representing set with, 134  
Bit strings  
    counting, 388  
        without consecutive 0s, 505  
    decoding, 762–763  
    generating next largest, 437  
    in interstellar communication, 476  
    length of, 505  
Bitwise operation, 110  
Bitwise operators, 12  
Block  
    Sudoku, 32  
Block cipher, 297, 306  
Blocks of statements, A-14–A-15  
BNF (Backus–Naur form), 854  
Boat, 692  
Bob, 302, 305  
Bonferroni’s inequality, 467  
Book number of graph, 744  
Boole’s inequality, 467  
Boole, George, 3, 5, 472, 811  
Boolean algebra, 811–846  
    abstract definition of, 815  
    definition of, 843  
    identities, 27  
    identities of, 814–816  
Boolean expressions, 812–814, 843  
    dual of, 816, 843  
Boolean functions, 811–819, 843  
    dual of, 816, 843  
    functionally complete set of operators for, 821  
    implicant of, 832  
    minimization of, 828–840, 843  
    representing, 813–821  
    self–dual, 844  
    threshold, 845  
Boolean power of a square zero–one matrix, 183  
Boolean product, 811–812, 821, 843  
    of two zero–one matrices, 182  
Boolean product of zero–one matrices  
    algorithm for, 223  
Boolean searches, 18  
Boolean sum, 811–812, 821, 843  
Boolean variable, 11, 110, 814, 820, 843  
Boruvka, Otakar, 800  
Bots, 794  
Bottom-up parsing, 853  
Bound  
    greatest lower, 634  
    least upper, 634, A-2  
        of poset, 625  
    of lattice, 637  
        of poset, 625–626, 634  
    of poset, 625–626, 634  
    upper, A-2  
Bounded lattices, 637  
Bound occurrence of variable, 44  
Bound variable, 44, 110  
Boxes, distributing objects into, 428–431  
    distinguishable, 428  
    indistinguishable, 428  
Breadth-first search, 789–791, 804  
Breaking codes, 296  
Bridge, in graphs, 683  
Bridge problem, Königsberg, 693–694, 696, 697  
Brute-force algorithm, 224  
Brute-force algorithm for closest pair of points, 225  
Brute-force paradigm, 232

Bubble sort, 196, 232  
    bidirectional, 233  
    worst-case complexity, 221  
Bug, computer, 872  
Building arguments using rules of inference, 73  
Buoyancy, principle of, A-4  
Busy beaver function, 896, 899  
Butane, 750  
Byte, 149  
  
Cabbage, 692  
Cactus, 806  
CAD programs, 834  
Caesar, Julius, 294  
Caesar cipher, 294  
    decryption, 295  
    encryption, 294  
    key, 295  
Cake, division of, 331  
Calculus  
    predicate, 40  
    propositional, 3  
Call graphs, 646  
    connected components of, 682  
Canterbury Puzzles, The (Dudeney), 504  
Cantor’s theorem, 177  
Cantor, Georg, 117, 118, 173, 176  
Cantor diagonalization argument, 173, 186  
Cantor digits, 438  
Cantor expansion, 256, 438  
Cardano, Girolamo, 445  
Card hands, 411, 429  
Cardinality, 121, 170–175, 185, 186  
    of a countable set ( $\aleph_0$ ), 171, 186  
    of union of sets, 128  
Cardinality of the set of real numbers, 186  
Cardinal number, 121  
Carmichael, Robert Daniel, 283  
Carmichael number, 283, 306  
Carroll, Lewis (Charles Dodgson), 50  
Carry, 250  
Cartesian product, 123  
Cartesian product of more than two sets, 123  
Cases, proof by, 92–110  
Cash box, 424–425  
Catalan, Eugène Charles, 507  
Catalan numbers, 507  
Caterpillar, 807  
Cathy, 305  
Cayley, Arthur, 745, 750  
Ceiling function, 149, 186  
    properties of, 150  
Celebrity problem, 332  
Cells, adjacent, 830  
Center, 757  
Ceres, 241  
Chain, 637  
Chain letter, 753  
Character cipher, 297, 306  
Characteristic equation, 515  
Characteristic roots, 515  
Chebyshev’s inequality, 491, 495  
Chebyshev, Pafnuty Lvovich, 490, 491  
Checkerboard  
    tiles, 103  
Check digit, 289–292  
    for airline ticket identification numbers, 293  
    ISBN, 291  
    ISBN-13, 308  
    ISSN, 293  
    RTN, 308  
    UPC, 290  
Checkerboard, 103

Checkerboard, tiling of, 326, 333  
Cheese, in Reve’s puzzle, 504  
Chen, J. R., 264  
Chess, game tree for, 769  
Chessboard  
    *n*-queens problem on, 792–793  
    knight’s tour on, 707  
    squares controlled by queen on, 740  
Chi (Greek letter), 728  
Chickens, 741  
Child of vertex, 747, 803  
Chinese meal, preparing, 635  
Chinese postman problem, 698, 744  
Chinese remainder theorem, 277, 306  
Chocolate bar, 342  
Chomp, 98, 342, 638  
    winning strategy for, 98  
Chomsky, Avram Noam, 847, 851, 853  
Chomsky classification of grammars, 851–852  
Chromatic number, 728, 737  
    *k*-critical, 734  
    edge, 734  
    of graph, 728  
Chung-Wu Ho, 340  
Church, Alonzo, 897  
Church–Turing thesis, 893  
Cipher  
    affine, 296, 306  
    autokey, 309  
    block, 306  
    Caesar, 294  
    character, 297, 306  
    monoalphabetic, 297  
    shift, 295, 306  
    transposition, 297  
    Vigenère, 304  
Cipher block, 297  
Circuits  
    combinational, 823  
    depth of, 828  
    examples of, 823–825  
    minimization of, 828–840  
digital, 21  
Euler, 693–698, 736  
Hamilton, 698–703, 736  
in directed graph, 599, 633  
in graph, 679  
logic, 20, 110  
multiple output, 826  
simple, 679  
Circular permutation, 415  
Circular reasoning, 90, 110  
Circular relation, 636  
Circular table, 394  
Citation graphs, 646  
Civil War, 38  
C language identifier, 857  
Class  
    congruence, 241  
    equivalence, 610–611, 633  
        and partitions, 612–614  
    definition of, 610  
    representative of, 610  
of nondeterministic polynomial-time problems, 900  
NP, 227, 896  
of NP-complete problems, 897, 900  
of polynomial-time problems, 227, 896, 900  
    Class P, 227, 896, 900  
Class A addresses, 392  
Class B addresses, 392  
Class C addresses, 392  
Class D addresses, 392  
Class E addresses, 392  
Clause, 74

- Climbing rock, 163  
Clique, 739  
Clock, 240  
Closed formula  
    for terms of a sequence, 159  
Closed interval, 117  
Closed walk, 679  
Closest-pair problem, 532–535  
Closure  
    for integers modulo  $m$ , 243  
    Kleene, 899  
closure  
    Kleene( $\cdot$ ), 866  
Closure, Kleene, 866  
Closure laws  
    for addition, A-1  
    for multiplication, A-1  
Closures of relations, 597–606, 633  
    reflexive, 598, 633  
    symmetric, 598, 634  
    transitive, 597, 600–603, 634  
    computing, 603–606  
Coast Survey, U. S., 38  
COBOL, 854, 872  
Cocks, Clifford, 299  
Code  
    breaking, 296  
Codes, Gray, 702–703  
Codes, prefix, 762–764, 804  
Codeword enumeration, 506  
Coding, Huffman, 763–764, 804  
Codomain  
    of a function, 139, 186  
    of partial function, 152  
Coefficient(s)  
    Bézout, 270, 306  
    binomial, 409, 415–421, 439  
    constant  
        linear homogenous recurrent relations with,  
            515–520, 565  
        linear nonhomogenous recurrent relations with,  
            520–524, 565  
    extended, 539  
    multinomial, 434  
Collaboration graphs, 645  
    paths in, 680  
Collatz problem, 107  
Collection of sets  
    intersection of, 133  
    union of, 133  
Collision  
    in hashing, 288  
    in hashing functions, probability of, 462–463  
Coloring  
    chromatic number in, 728  
    of bipartite graphs, 657  
    of graphs, 727–732, 736  
    of maps, 727  
Combinational circuits, 823  
    depth of, 828  
    examples of, 823–825  
    minimization of, 828–840  
Combinations, 409–413  
    generating, 437–438  
    of events, 449–450, 455–456  
    with repetition, 424–427  
Combinatorial identities, 417–421  
Combinatorial proof, 412, 439  
Combinatorics, 385, 404, 431, 439  
Comments in pseudocode, A-12  
Common difference, 157  
Common errors  
    with exhaustive proofs, 95  
    with proofs by cases, 95  
Common ratio, 157  
Commutative group, 244  
Commutative laws, 27  
    for addition, A-1  
    for Boolean algebra, 815, 818  
    for lattices, 637  
    for multiplication, A-1  
    for sets, 129  
Commutative ring, 244  
Commutativity  
    for integers modulo  $m$ , 243  
Comparable elements in poset, 619, 633  
Compatibility laws, A-2  
Compatible total ordering, 628, 634  
Compilers, 611, 872  
Complement, 811, 843  
    double, law of, in Boolean algebra, 815, 818, 819  
    of Boolean function, 811  
Complementary event, 449  
Complementary graph, 667  
Complementary relation, 582  
Complementation law, 129  
Complemented lattice, 637, 817  
Complement law, 129  
Complement of a fuzzy set, 138  
Complement of a set, 128, 129, 186  
Complete  $m$ -ary tree, 756  
Complete  $m$ -partite graph, 738  
Complete bipartite graph, 658, 736  
Complete graphs, 655, 736  
Complete induction, 334  
Complexity  
    computational, 219  
    constant, 225  
    exponential, 225  
    factorial, 225  
    linear, 225  
    linearithmic, 225  
    logarithmic, 225  
    of algorithm for Boolean product of zero–one  
        matrices, 223  
    of matrix multiplication, 223  
    polynomial, 225  
    space, 219, 232  
    time, 219, 232  
Complexity of algorithms, 218–229  
    average-case, 482–484  
    computational  
        of Dijkstra’s algorithm, 714  
    of breadth-first search algorithms, 791  
    of depth-first search algorithms, 789  
    of merge sort, 532  
Complexity of merge sort, 532  
Complex numbers  
    set of, 116  
Components of graphs, connected, 682–685  
    strongly, 686, 736  
Composite, 257  
Composite integer, 306  
Composite key, 585, 633  
Composite of relations, 580, 633  
Composition of functions, 146, 186  
Composition rule, 373  
Compound interest, 160  
Compound proposition, 25, 109  
    dual of, 35  
    satisfiable, 30, 110  
Compound propositions, 3  
    consistent, 110  
    equivalences of, in Boolean algebra, 812  
    equivalent, 8  
    logically equivalent, 25, 110  
    truth tables of, 10  
    well-formed formula for, 354  
Computable  
    function, 175  
Computable function, 177, 186, 896, 900  
Computable numbers, 886  
Computation, models of, 847–897  
Computational complexity, 219  
Computational complexity of algorithms  
    of Dijkstra’s algorithm, 714  
    Turing machine in making precise, 894  
Computational geometry, 338–340, 532–535  
Computer-aided design (CAD) programs, 834  
Computer arithmetic with large integers, 279  
Computer debugging, 872  
Computer file systems, 750  
Computer network, 641  
    interconnection networks, 661–663  
    local area networks, 661  
    multicasting over, 786  
    with diagnostic lines, 642  
    with multiple lines, 642  
    with multiple one-way lines, 642  
    with one-way lines, 643  
Computer programming, 854  
Computer representation of sets, 134  
Computer science, 854  
Computer time used by algorithms, 228  
Computer virus  
    invention of term, 300  
    transmission, 441  
Concatenation, 350, 866, 899  
Conclusion, 70, 110  
Conclusion of a condition statement, 6  
Concurrent processing, 647  
Condition  
    necessary, 6  
    sufficient, 6  
Conditional constructions, A-12–A-13  
Conditional probability, 453, 456–457, 494  
Conditional statement(s), 6–9  
    contrapositive, 110  
    contrapositive of, 8  
    converse, 110  
    converse of, 8  
    for program correctness, 373–375  
    inverse of, 8  
    truth table for, 6  
Conditions  
    don’t care, 836–837  
    initial, 158, 565  
Congruence, 240, 306  
    applications of, 287–292  
    linear, 275, 306  
Congruence class, 241  
Congruence modulo  $m$ , 609–610, 633  
Congruence quadratic, 285  
Congruent to, 240, 306  
Conjecture, 81, 110  
     $3x + 1$ , 107  
    Frame’s, 513  
    Goldbach’s, 264  
    twin prime, 264  
Conjectures about primes, 263  
Conjunction, 4, 110, 843  
    distributive law of disjunction over, 27  
    negating, 28  
    truth table for, 4  
Conjunction (rule of inference), 71  
Conjunctive normal form, 820  
Connected components of graphs, 682–685  
    strongly, 686, 736

I-6 Index

Connected graphs, 678–689

- directed, 685–687
- planar simple, 719–723
- strongly, 685
- undirected, 681–685
- weakly, 686

Connecting vertices, 651Connectives

- logical, 4

Connectivity

- edge, 684
- vertex, 684

Connectivity relation, 600, 633Consequence of a condition statement, 6Consistent compound propositions, 110Consistent system specifications, 18Constant coefficients

- linear homogenous recurrent relations with, 515–520, 565
- linear nonhomogenous recurrent relations with, 520–524, 565

Constant complexity, 225Constructing logical equivalences, 29Construction

- automaton that recognizes a regular set, 881

Construction of the real numbers, A-5Constructions

- conditional, A-12–A-13
- loop, A-14–A-15

Constructive existence proof, 96, 110Contains, 116Context-free grammar(s), 851, 886

- ambiguous, 901

Context-free language, 851Context-sensitive grammars, 851Context-sensitive languages, 886Contingency, 25, 110Continuum hypothesis, 175, 186Contraction, edge, 664Contradiction, 25, 110

- proof by, 110

Contradiction, proof by, 86Contraposition, 83

- proof by, 110

Contrapositive, 8, 110

- of a conditional statement, 110

Control unit

- Turing machine, 889

Converse, 8, 110

- of a conditional statement, 110
- of directed graph, 668

Conversion

- between bases, 247
- between binary and hexadecimal, 249
- between binary and octal, 249

Convex polygon, 338Cook, Stephen, 227Cook–Levin theorem, 227Cookie, 426Corollary, 110Correctness

- of an algorithm, 193
- of programs, 372–378
  - conditional statements for, 373–375
  - loop invariants for, 375–376
  - partial, 372
  - program verification for, 372–373
  - rules of inference for, 373
- of recursive algorithms, 364–365

Correspondence

- one-to-one, 144, 186

Countability of set of rational numbers, 172

Countable set, 171, 186

- cardinality of, 186

Counterexample(s), 88, 102, 110Counting, 385–444, 501–571

- basic principles of, 385–390
- bit strings, 388
  - without consecutive 0s, 505
- Boolean functions, 814
- by distributing objects into boxes, 428–431
- combinations, 409–413
- derangements, 562, 566
- functions, 387
- generating functions for, 541–546
- Internet addresses, 392
- one-to-one functions, 387
- onto functions, 560–562, 566
- passwords, 391
- paths between vertices, 688–689
- permutations, 407–409
- pigeonhole principle and, 399–405
- reflexive relations, 578
- relations, 578–579
- subsets of finite set, 388
- telephone numbers, 387
- tree diagrams for, 394–395
- variable names, 391
- with repetition, 423

Covariance, 494Covering relation, 623, 631Covers, 631CPM (Critical Path Method), 639C programming language, 398, 611Crawlers, 794Cricket, 97Criterion

- Euler’s, 286

Critical Path Method (CPM), 639Crossing number, 726Cryptanalysis, 296, 306

- for shift cipher, 296
- Vigenère cipher, 305

Cryptographic protocols, 302Cryptosystem, 297–306

- definition of, 297
- private key, 298, 306
- public key, 298
- RSA, 299, 306
- shift cipher, 298

Cunningham numbers, 262Cut

- edge, 683, 684
- set, 806
- vertex, 683, 684

Cycle

- in directed graph, 599, 633
- with  $n$  vertices, 655

Cylinder, 831Czekanowski, Jan, 800

Database

- composite key of, 585
- intension of, 585
- primary key of, 585
- records in, 584
- relational model of, 584–586, 633

Database query language, 588–589Data compression, 763Datagrams, 399Datalogy, 854Datatype, 117David Hilbert, 171de Bruijn sequences, 744Debugging, 872

Decidable problem, 895Decimal expansion of a real number, 174Decimal expansions, 246Decision problems, 894, 900Decision trees, 760–762, 804Deck, standard, 402Decreasing function, 143Decryption, 295, 306

- affine cipher, 296
- Caesar cipher, 295
- RSA, 300

Decryption key

- RSA system, 301

Dedekind, Richard, 175Deductive reasoning, 312Deep-Blue, 769Deferred acceptance algorithm, 204, 343Definiteness

- of an algorithm, 193

Definition

- recursive, 311, 344–357

Degree

- of  $n$ -ary relations, 584
- of linear homogenous recurrence relations, 514
- of region, 722
- of vertex in undirected graph, 652

Degree-constrained spanning tree, 806Degree of membership in a fuzzy set, 138de la Vallée-Poussin, Charles-Jean-Gustave-Nicholas, 262Delay machine, 861–862de Méré, Chevalier, 452De Morgan’s laws, 26, 27

- for Boolean algebra, 815, 819
- for propositions, 31, 28–31
- for quantifiers, 47
- for sets, 129
- proving by mathematical induction, 323–324

De Morgan, Augustus, 26, 29, 729Dense

- graph, 670
- poset, 632

Denying the hypothesis, fallacy of, 75Dependency notation, 846Depth-first search, 787–789, 804

- applications of, 794–795
- in directed graphs, 794–795

Depth of combinatorial circuit, 828Derangements, 562–565

- number of, 562, 566

Derivable, 899

- directly, 899

Derivable from, 849Derivation, 849Derivation tree, 899Derivation trees, 852–854Descartes René, 122Descendants of vertex, 747, 804Describing a set

- by listing its members, 116
- by the roster method, 116
- using set builder notation, 116

Designing finite-state automata, 869Detachment

- laws of, 71

Deterministic finite-state automata, 872, 899Deviation, standard, 487Devil’s pair, 678Diagnostic test results, 471–472Diagonalization argument, Cantor, 173, 186Diagonal of a polygon, 338Diagonal of a square matrix, 181Diagonal relation, 598

- Diagrams
  - Hasse, 622–626, 634
  - state, for finite-state machine, 860
  - tree, 394–395, 439
  - Venn, 118, 185
- Diameter of graph, 741
- Dice, 446
- Dictionary ordering, 435
- Die, 468, 488–489
  - dodecahedral, 496
  - octahedral, 496
- Difference, A-6
  - backward, 513
  - common, 157
  - forward, 568
- Difference equation, 513
- Difference of multisets, 138
- Difference of sets, 128, 186
- Diffie, Whitfield, 302
- Diffie–Helman key agreement protocol, 302
- Digit
  - binary, 11
- Digital circuit(s), 20–21
- Digital signatures, 303, 306
- Digital signatures in RSA system, 303
- Digits
  - Cantor, 438
- Digraphs, 633, 643, 735
  - circuit (cycle) in, 599, 633
  - connectedness in, 685–687
  - converse of, 668
  - depth-first search in, 794–795
  - edges of, 643, 653–654
  - Euler circuit of, 694
  - loops in, 594, 633
  - paths in, 599–600, 633, 736
  - representing relations using, 594–596
  - self-converse, 740
  - vertex of, 641, 654
- Dijkstra's algorithm, 709–714, 737
- Dijkstra, Edsger Wybe, 710
- Dimes, 199
- Diophantus, 106
- Dirac's theorem, 701
- Dirac, G. A., 701
- Directed edges, 644, 653–654, 735
- Directed graphs, 633, 643, 735
  - circuit (cycle) in, 599, 633
  - connectedness in, 685–687
  - converse of, 668
  - depth-first search in, 794–795
  - edges of, 643, 653–654
  - Euler circuit of, 694
  - loops in, 594, 633
  - paths in, 599–600, 633, 736
  - representing relations using, 594–596
  - self-converse, 740
  - vertex of, 641, 654
- Directed multigraph, 643, 735
  - paths in, 679
- Directly derivable, 849, 899
- Direct proof, 82, 110
- Dirichlet, G. Lejeune, 262, 400
- Dirichlet drawer principle, 400
- Discrete logarithm, 284, 306
- Discrete logarithm problem, 284
- Discrete mathematics
  - definition of, vii, viii, xviii
  - problems studied in, xviii
  - reasons to study, xviii
- Discrete probability, 445–500
  - assigning, 453–455
  - conditional, 453, 456–457, 494
  - finite, 445–448
  - Laplace's definition of, 445
  - of collision in hashing functions, 462–463
  - of combinations of events, 449–450, 455–456
- Disjoint sets, 128
- Disjunction(s), 4, 109, 843
  - associative law of, 27
  - distributive law of, over conjunction, 27
  - negating, 28
  - truth table for, 4
- Disjunctive normal form, 35
  - for Boolean variables, 820
- Disjunctive syllogism, 71
- Disquisitiones Arithmeticae* (Gauss), 241
- Distance
  - between distinct vertices, 741
  - between spanning trees, 797
- Distinguishable
  - boxes, 428
  - objects, 428
  - strings, 888
- Distributing objects into boxes, 428–431
- Distribution
  - binomial, 458–460
  - of random variable, 460, 494
  - geometric, 484–485, 494
  - probability, 453
  - uniform, 454, 494
- Distributive lattice, 637, 817
- Distributive laws, 27
  - for Boolean algebra, 815, 818
  - for propositions, 27
  - for sets, 129
- Distributivity
  - for integers modulo  $m$ , 243
- Divide-and-conquer
  - algorithms, 527, 565
  - recurrence relations, 527–535
- Dividend, 238, 239
- Divides, 238, 306
- Divine Benevolence (Bayes), 472
- Divisibility facts, proving, by mathematical induction, 321
- Divisibility relation, 619
- Division
  - of integers, 238–240
  - trial, 258
- Division algorithm, 239, 306
- Division of a cake, 331
- Division rule, 394
- Division rule for counting, 394
- Divisor, 238, 239
  - greatest common, 265–267, 306
- DNA (deoxyribonucleic acid), 388
- DNA sequencing, 698
- Dodecahedral die, 496
- Dodgson, Charles Lutwidge (Lewis Carroll), 50
- Domain
  - of  $n$ -ary relation, 584
  - of a function, 139, 186
  - of a quantifier, 40
  - of partial function, 152
  - of relation, 584
  - restricted
    - of quantifier, 44
- Domain of definition
  - of partial function, 152
- Domain of discourse, 40, 110
- Dominating set, 739
- Domination laws, 27
  - for Boolean algebra, 815
  - for sets, 129
- Domino(s), 103, 314
- Don't care conditions, 836–837
- Double complement, law of, in Boolean algebra, 815, 819
- Double counting proofs, 412
- Double hashing, 292
- Double negation law, 27
- Drug testing, 475
- Dual
  - of a compound proposition, 35
  - of Boolean expression, 816
  - of Boolean function, 816
  - of poset, 630
- Dual graph, 727
- Duality in lattice, 639
- Duality principle, for Boolean identities, 816
- Dudeney, Henry, 504
- Dynamic programming, 507
- Ear(s), 343
  - nonoverlapping, 343
- Earth, 476
- EBNF (extended Backus–Naur form), 858
- Eccentricity of vertex, 757
- Ecology, niche overlap graph in, 648
- Edge
  - adding from a graph, 664
  - removing a vertices from, 664
  - removing from a graph, 663
- Edge chromatic number, 734
- Edge coloring, 734
- Edge connectivity, 684
- Edge contraction, 664
- Edge(s)
  - cut, 683, 684
  - directed, 644, 654, 735
  - endpoints of, 651
  - incident, 651, 735
  - multiple, 642, 643, 735
  - of directed graph, 643, 653–654
  - of directed multigraph, 643
  - of multigraph, 642
  - of pseudograph, 643
  - of simple graph, 642, 667
  - of undirected graph, 644, 654
  - undirected, 644, 735
- Edge vertex, 594
- Effectiveness
  - of an algorithm, 193
- Egyptian (unit) fraction, 380
- Einstein, Albert, 24
- Electronic mail, 472
- Element
  - image of, 186
  - pre-image of, 186
- Elementary subdivision, 724, 736
- Element of a set, 116, 185
- Elements
  - comparable, in partially ordered set, 619, 633
  - equivalent, 608
  - fixed, 494
  - greatest, of partially ordered set, 625, 634
  - incomparable, in partially ordered set, 619, 633
  - least, of partially ordered set, 625, 634
  - maximal, of partially ordered set, 624, 634
  - minimal, of partially ordered set, 624, 625, 634
- Elements of Mathematical Logic (Łukasiewicz), 782
- Ellipses (...), 116
- Empty folder, 118
- Empty set, 118, 185
- Empty string(s), 157, 186, 849

I-8 Index

Encryption, 294, 306  
  affine transformation, 296  
  public key, 306  
  RSA, 299  
Encryption key, 306  
Encrytion  
  Caesar cipher, 294  
Endpoints of edge, 651  
Engine  
  Analytic, 31  
Entry of a matrix, 178  
Enumeration, 392, 439  
  codeword, 506  
Equal functions, 139  
Equality  
  of sets, 117, 185  
Equal matrices, 178  
Equation  
  characteristic, 515  
  difference, 513  
Equivalence  
  proof of, 87  
Equivalence(s)  
  logical, 27  
Equivalence classes, 610–611, 633  
  and partitions, 612–614  
  definition of, 610  
  representative of, 610  
Equivalence relations, 607–614, 633  
  definition of, 608  
Equivalent  
  compound propositions, 8  
  logically  
    compound propositions, 25  
Equivalent Boolean expressions, 813  
Equivalent elements, 608  
Equivalent finite-state automata, 868, 871–872  
Eratosthenes, 259, 560  
  sieve of, 259, 306, 565  
Erdős, Paul, 260, 263, 635, 636, 680  
Erdős number, 635, 680, 689  
Erdős number Project, 680  
Error  
  single, 291  
  transposition, 291  
Errors,  
  in exhaustive proofs, 95  
  in proofs by cases, 95  
  in proofs by mathematical induction 328–329  
Essential prime implicant, 832, 843  
Euclid, 267  
Euclidean algorithm, 267, 347  
Euler  $\phi$ -function, 272  
Euler's criterion, 286  
Euler's formula, 720–723, 737  
Euler's formula“Eureka,” A-4  
Euler, Leonhard, 693, 695  
Euler circuits, 693–698, 736  
Euler paths, 693–698, 736  
Evaluation functions, 769  
Even, 83  
Event(s), 446  
  combinations of, 449–450, 455–456  
  complementary, 449  
  independent, 452, 457–458, 494  
  mutually independent, 497  
Exams, scheduling, 731, 732  
Exchange  
  key, 302  
Exclusion rule, 349  
Exclusive or, 5, 6, 110  
  truth table for, 6

Exercises  
  difficult, xix  
  extremely challenging, xix  
  result used in book, xix  
  routine, xix  
Exhaustive proof, 93, 110  
  common errors with, 95  
Existence proof(s), 96  
  constructive, 96, 110  
  nonconstructive, 96, 110  
Existential generalization, 76  
Existential instantiation, 76  
Existential quantification, 42, 110  
Existential quantifier, 42  
Expansion(s)  
  balanced ternary, 256  
  base- $b$ , 246  
  binary, 246  
  binary coded decimal, 836  
  Cantor, 256  
  decimal, 246  
  hexadecimal, 246  
  octal, 246  
Expected values, 477–480, 494  
  in hatcheck problem, 481  
  linearity of, 477–484, 494  
  of inversions in permutation, 482–484  
Experiment, 446  
Exponential complexity, 225  
Exponential functions, A-7  
  big- $O$  estimates for, 212  
Exponential generating function, 551  
Exponentiation  
  modular, 253  
  recursive, 363  
Expression(s)  
  binomial, 415  
  Boolean, 812–814, 843  
  infix form of, 780  
  postfix form of, 781  
  prefix form of, 780  
  regular, 879, 899  
Expressions  
  logically equivalent, 110  
extended Backus–Naur form, 858  
Extended binary trees, 352  
Extended binomial coefficients, 539  
Extended binomial theorem, 540  
Extended Euclidean algorithm, 270, 273  
Extended transition function, 867  
Extension  
  of transition function, 867  
Exterior of simple polygon, 338

Facebook, 645  
Factor, 238  
Factorial complexity, 225  
Factorial function, 151  
Factorials, recursive procedure for, 361  
Factoring, 262  
Factorization  
  prime, 259  
Failure, 458  
Fairy, tooth, 112  
Fallacies, 69, 75, 110  
  of affirming the conclusion, 75  
  of denying the hypothesis, 75  
False  
  negative, 471, 472  
  positive, 471, 472  
Family trees, 745  
Farmer, 692

Fast multiplication  
  of integers, 528–529  
  of matrices, 529  
Female pessimal, 234  
Fermat's last theorem, 106, 349  
Fermat's little theorem, 281, 306  
  proof of, 285  
Fermat, Pierre de, 106, 281, 282  
Fibonacci, 348  
Fibonacci numbers, 347  
  and Huffman coding, 771  
  formula for, 517  
  iterative algorithm for, 366  
  rabbits and, 502–503  
  recursive algorithms for, 365  
Fibonacci sequence, 158  
Fibonacci trees, rooted, 757  
Field axioms, A-1  
Fields, 584  
Fields Medal, 263  
Filter, spam, 472–475  
Final assertion, 372, 378  
Final exams, scheduling, 731, 732  
Final state  
  finite-state automaton, 867  
  of a Turing machine, 891  
  Turing machine, 891  
Final value, A-14  
Finding maximum element in a sequence  
  algorithm for, 192  
Finite-state automata, 866–872  
  accepting state, 867  
  designing, 869  
  deterministic, 872, 899  
  equivalent, 868  
  final state, 867  
  initial state, 867  
  minimization, 872  
  nondeterministic, 873, 899  
  set not recognized by, 885  
Finite-state machine, 847, 858, 885, 899  
  for addition, 862  
  input string, 861  
  output string, 861  
  transition function extension, 867  
  transition function extension in, 867  
  with output, 859, 865  
  with outputs, 859, 863  
Finite-state transducer, 859  
Finite graph, 641  
Finiteness  
  of an algorithm, 193  
Finite probability, 445–448  
Finite set, 121, 185  
Finite sets, 553, 565  
  number of subsets, 323  
  subsets of  
    counting, 388  
    number of, 323  
  union of three, number of elements in, 554–556, 566  
  union of two, number of elements in, 553, 565  
First difference, 513  
First forward difference, 568  
Fixed elements, 494  
Fixture controlled by three switches, circuit for, 825  
Flavius Josephus, 512  
Fleury's algorithm, 697, 706  
Flip-flops, 846  
Floor function, 149, 186  
  properties of, 150  
Floyd's algorithm, 717

- Folder
  - empty, 118
- Forbidden pairs, 234
- Forests, 746
  - definition of, 803
  - minimum spanning, 802
  - spanning, 796
- Form
  - argument, 70
  - Backus–Naur, 854, 899
  - conjunctive normal, 820
  - disjunctive normal
    - for Boolean variables, 820
  - extended Backus–Naur form, 858
  - infix, 780
  - postfix, 781
  - prefix, 780
- Form, argument, 110
- Formal language, 848
- Formal power series, 538
- Formula(s)
  - Euler’s, 720–723, 737
  - for compound propositions, 354
  - for Fibonacci numbers, 517
  - of operators and operands, 351
  - Stirling’s, 151
  - summation, 315
  - well-formed, 350
- FORTRAN, 854
- Fortune cookie, 441
- Forward differences, 568
- Forward reasoning, 100
- Forward substitution
  - iteration using, 160
- Four color theorem, 728–731, 737
- Fraction, unit (Egyptian), 380
- Frame’s conjecture, 513
- Free variable, 44, 110
- Freud, Sophia, 29
- Frequency assignments, 732
- Friendship graph, 645
- Frisbee, rocket-powered, 812
- Full *m*-ary tree, 748, 752, 804
  - complete, 756
- Full adder, 826, 843
- Full binary trees, 352–353
  - height of, 355
  - number of vertices of, 355
- Full subtractor, 828
- Function(s), 139, 186
  - Addition of, 141
  - Ackermann’s, 359
  - asymptotic, 218
  - as relations, 574
  - big-*O* estimates of, 209
  - bijective, 144
  - Boolean, 811–819, 843
    - dual of, 816
    - functionally complete set of operators for, 821
    - implicant of, 832
    - minimization of, 828–840, 843
    - representing, 813–821
    - self-dual, 844
    - threshold, 845
  - busy beaver, 896,899
  - ceiling, 149, 186
  - codomain of, 139
  - codomain of *a*, 186
  - composition of, 146, 186
  - computable, 175, 177, 186, 896, 900
  - counting, 387
  - decreasing, 143
  - domain of, 186
  - equal, 139
  - Euler  $\phi$ , 272
  - evaluation, 769
  - exponential, A-7
  - factorial, 151
  - floor, 149, 186
  - generating, 537–548, 565
    - exponential, 551
    - for counting, 541–546
    - for proving identities, 548
    - for recurrence relations, 546–548
    - probability, 552
  - graph of, 148
  - greatest integer, 149
  - growth of, 209
  - growth of combinations of, 212–214
  - hashing, 287
    - collision in, probability of, 462–463
  - identity, 144
  - increasing, 143
  - injective, 141
    - counting, 387
  - integer-valued, 140
  - inverse, 145
  - inverse of, 186
  - invertible, 145
  - iterated, 360
  - iterated logarithm, 360
  - logarithmic, A-7–A-9
  - McCarthy, 380
  - multiplication of functions, 141
  - number-theoretic, 892
  - mod**, 239, 306
  - one-to-one, 141, 186
  - onto, 186
    - number of, 560–562, 566
  - partial, 152, 186, 889
  - probing, 288
  - propositional, 110
  - range of, 186
  - real-valued, 140
  - recursive, 345–349, 378
  - strictly decreasing, 143
  - strictly increasing, 143
  - surjective, 143
  - threshold, 845
  - total, 152
  - transition, 859
  - Turing machines computing, 892–893
  - uncomputable, 175, 186, 896, 900
- Functional completeness, 821
- Functional decomposition, 846
- Functionally complete logical operators, 35
- Functionally complete set of operators
  - for Boolean functions, 821, 843
- Fundamental theorem of algebra, 241
- Fundamental theorem of arithmetic, 258, 306
  - proof of, 271
- Fuzzy logic, 16
- Fuzzy set(s), 138
  - complement of, 138
  - degree of membership, 138
  - intersection of, 138
  - union of, 138
- Gödel, Escher, Bach (Hofstadter), 382
- Gale–Shapley algorithm, 204
- Gambling, 445
- Game
  - obligato, 112
- Game trees, 764–769, 804
- Gates, logic, 21, 110, 822–827
  - AND, 21, 823, 843
  - combination of, 823
  - NAND, 828
  - NOR, 828
  - OR, 21, 823, 843
  - threshold, 845
- Gating networks, 822–823
  - depth of, 828
  - examples of, 823–825
  - minimization of, 828–840
- Gauss, Karl Friedrich, 241
- Gecko, Gordon, 198
- Gene, 389
- Generality
  - of an algorithm, 193
- Generalization
  - existential, 76
  - universal, 76
- Generalized combinations, 423–427
- Generalized induction, 356–357
- Generalized permutations, 423
- Generalized pigeonhole principle, 401–403, 439
- Generating functions, 537–548, 565
  - exponential, 551
  - for counting, 541–546
  - for proving identities, 548
  - for recurrence relations, 546–548
  - probability, 552
- Generator, power, 292
- Gene sequencing, 389
- Genome, 389
- Geometric distribution, 484–485, 494
- Geometric mean, 100, 332
- Geometric progression, 157, 186
  - sum of terms of, 164
- Geometric progression(s)
  - sums of, 318–319
- Geometric series, 164
- Geometry, computational, 338–340, 532–535
- Giant strongly connected components (GSCC), 686
- GIMPS (Great Internet Mersenne Prime Search, 261
- Givens
  - in Sudoku, 32
- Goat, 692
- Goldbach’s conjecture, 264
- Goldbach, Christian, 264
- Golomb’s self-generating sequence, 382
- Golomb, Solomon, 105
- Google, 18, 794
- Gossip problem, by mathematical induction, 332
- Government Communications Headquarters
  - (GCHQ), U.K., 299
- Government Communications Headquarters
  - (GCHQ), U.K., 299
- Graceful trees, 807
- Graham, Ron, 636
- Grammar(s), 848
  - Backus–Naur form of, 854
  - context-free, 886
  - context-free (type 2), 851
  - context-sensitive, 851
  - language generated by, 850
  - language of, 850
  - monotonic, 852
  - noncontracting, 852
  - productions, 849
  - phrase-structure, 849–854, 899
  - regular, 884, 899
  - regular (type 3), 851
  - type 0, 851, 899
  - type 1, 851, 899
  - type 2, 851, 899
  - type 3, 851, 883, 899
- Grand Hotel, Hilbert’s, 171

- Graph(s), 641–744  
    *k*-connected, 684  
    *n*-regular, 667  
    academic collaboration, 645  
    acquaintanceship, 645  
    airline route, 647  
    bandwidth of, 741  
    biconnected, 684  
    bipartite, 656–658, 736  
    book number of, 744  
    call, 646  
        connected components of, 682  
    chromatically *k*-critical, 734  
    chromatic number of, 728  
    citation, 646  
    collaboration, 645  
    coloring, 727–732, 736  
    complementary, 667  
    complete, 655, 736  
    complete *m*-partite, 738  
    complete bipartite, 658, 736  
    connected components of, 682–685, 736  
    connectedness in, 678–689  
    cut set of, 806  
    definition of, 643  
    diameter of, 741  
    directed, 633, 643, 735  
        circuit (cycle) in, 599, 633  
        connectedness in, 685–687  
        converse of, 668  
        dense, 670  
        depth-first search in, 794–795  
        edges of, 643, 653–654  
        Euler circuit of, 694  
        loops in, 594, 633  
        paths in, 599–600, 633, 736  
        representing relations using, 594–596  
        self-converse, 740  
        simple, 643  
        vertex of, 641, 654  
    directed multigraph, 644, 735  
    dual, 727  
    finite, 641  
    friendship, 645  
    Hollywood, 645  
    homeomorphic, 724–725, 736  
    independence number of, 741  
    infinite, 641  
    influence, 645  
    in roadmap modeling, 647  
    intersection, 650  
    isomorphic, 668, 671–675, 736  
        paths and, 687–688  
    matching in, 659  
    mixed, 644  
    models, 644–649  
    module dependency, 647  
    monotone decreasing property of, 742  
    monotone increasing property of, 742  
    multigraphs, 642, 644, 735  
    niche overlap, 648  
    nonplanar, 724–725  
    nonseparable, 683  
    orientable, 740  
    paths in, 678–681  
    planar, 718–725, 736  
    precedence, 647  
    protein interaction, 648  
    pseudograph, 643, 644, 735  
    radius of, 741  
    regular, 667, 736  
    representing, 668–675  
    self-complementary, 677  
    simple, 642, 654–655, 735  
        coloring of, 727  
        connected planar, 719–723  
        crossing number of, 726  
        dense, 670  
        edges of, 642, 663  
        isomorphic, 671–675, 736  
        orientation of, 740  
        paths in, 785  
        random, 742  
        self-complementary, 677  
        sparse, 670  
        thickness of, 726  
        vertices of, 642, 663  
        with spanning trees, 785–787  
    simple directed, 643  
    sparse, 670, 802  
    strongly directed connected, 685  
    subgraph of, 663, 736  
    terminology of, 651–654  
    undirected, 644, 653, 736  
        connectedness in, 681–685  
        Euler circuit of, 694  
        Euler path of, 698  
        orientation of, 740  
        paths in, 679, 736  
        underlying, 654, 736  
    union of, 664, 736  
    very large scale integration, 744  
    Web, 646–647  
        strongly connected components of, 686  
    weighted, 736  
        shortest path between, 707–714  
        traveling salesman problem with, 714–716  
    wheel, 655, 736  
Graph of a function, 148  
Gray, Frank, 703  
Gray codes, 702–703  
“Greater than or equal” relation, 618–619  
Greatest common divisor, 265–267, 306  
    as linear combination, 269  
Greatest element of poset, 625, 634  
Greatest integer function, 149  
Greatest lower bound, 634  
    of poset, 625  
Great Internet Mersenne Prime Search (GIMPS), 261  
Greedy algorithm(s), 198, 232, 235, 325, 764, 798, 804  
    definition of, 198  
    for making change, 199  
    for minimizing maximum lateness of a job, 235  
    for scheduling talks, 200  
Green, Ben, 263  
Green–Tao theorem, 263  
Group commutative, 244  
Growth of functions, 209  
GSCC (giant strongly connected components), 686  
Guarding set, 735  
Guare, John, 680  
Guidelines for mathematical induction, 328  
Guthrie, Francis, 729  
  
Hadamard, Jacques, 262  
Haken, Wolfgang, 728  
Half adder, 826, 843  
Half subtractor, 828  
Hall’s marriage theorem, 659  
Hall, Philip, 659, 660  
Halting problem, 201, 895, 900  
Hamilton’s “Voyage Around the World” Puzzle, 700  
Hamilton, Sir William Rowan, 698, 700  
Hamilton, William Rowan, 729  
Hamilton circuits, 698–703, 736  
Hamilton paths, 698–703, 736  
Handle, 806  
Handshaking theorem, 653  
Hanoi, tower of, 503–504  
Hardware systems, 17  
Hardy, Godfrey Harold, 97  
Hardy, Godfrey Harold, 97  
Hardy–Weinberg law, 97  
Harmonic mean, 108  
Harmonic number(s)  
    inequality of, 320–321  
Harmonic series, 321  
Hashing  
    collision in, 288  
    double, 292  
    function, 287  
    key, 287  
Hashing functions  
    collision in, probability of, 462–463  
Hasse’s algorithm, 107  
Hasse, Helmut, 623  
Hasse diagrams, 622–626, 634  
Hatcheck problem, 481, 562  
Hazard-free switching circuits, 846  
Heaps, 809  
Heawood, Percy, 728  
Height, star, 901  
Height-balanced trees, 808  
Height of full binary tree, 355  
Height of rooted tree, 753, 804  
Hellman, Martin, 302  
Hexadecimal expansions, 246  
Hexadecimal representation, 306  
Hexagon identity, 421  
Hilbert’s 23 problems, 171, 895  
Hilbert’s Grand Hotel, 171  
Hilbert’s Tenth Problem, 895  
Hilbert, David, 171, 176, 895  
HIV, 476  
Ho, Chung-Wu, 340  
Hoare, C. Anthony R., 372, 374  
Hoare triple, 372  
Hofstadter, Douglas, 382  
Hollywood graph, 645  
    paths in, 680–681  
Homeomorphic graphs, 724–725, 736  
Hopper, Grace Brewster Murray, 872  
Hops, 662  
Horner’s method, 230  
Horse races, 31  
Host number (hostid), 392  
HTML, 858  
Huffman, David A., 763  
Huffman coding, 763–764, 804  
    variations of, 764  
Human genome, 389  
Husbands, jealous, 693  
Hybrid topology for local area network, 661  
Hydrocarbons, trees modeling, 750  
Hypercube, 662  
Hypothesis  
    continuum, 175, 186  
    inductive, 313  
Hypothesis of a conditional statement, 6  
Hypothetical syllogism, 71  
  
“Icosian Game,” 700  
Icosian Puzzle, 698  
Idempotent laws  
    for Boolean algebra, 815, 819  
    for lattices, 637  
    for propositions, 27  
    for sets, 129



- Identification number
  - single error in, 291
- Identification number(s)
  - for airline tickets, 293
- Identification numbers
  - for money orders, 293
- Identifier, 611
  - ALGOL, 855
  - C language, 857
- Identifying a sequence from its initial terms, 161
- Identities
  - Boolean algebra, 27
  - set, 129
  - set(, 129
  - set), 132
- Identities, combinatorial, 417–421
- Identities for Boolean algebra, 129
- Identity
  - Bézout's, 270
  - combinatorial, proof of, 412, 439
  - hexagon, 421
  - proving, generating functions for, 548
  - Vandermonde's, 420–421
- Identity element(s)
  - for integers modulo  $m$ , 243
- Identity elements axiom, A-1
- identity function, 144
- Identity laws, 27
  - additive, A-1
  - for Boolean algebra, 815, 816, 818
  - for sets, 129
  - multiplicative, A-1
- Identity matrix, 180, 186
- If-then construction, 8
- If then** statement, 6
- If and only if, 9
- Iff, 9
- Image of an element, 139, 186
- Image of a set, 141
- Implicant, 832
  - essential, 832
  - prime, 832
- Implication, 6, 110
- Implicit use of biconditionals, 10
- In-degree of vertex, 654, 736
- Incidence matrices, 671, 736
- Incident edge, 651
- Inclusion–exclusion principle, 128, 392–394, 553–557, 566
  - alternative form of, 558–559
  - applications with, 558–564
- Inclusion relation, 619
- Inclusive or, 5
- Incomparable elements in poset, 619, 633
- Incomplete induction, 334
- Incorrect proof by mathematical induction, 757
- Increasing function, 143
- Increment
  - for linear congruential method, 288
- Independence number, 741
- Independent events, 452, 453, 457–458, 494
- Independent random variables, 485–487, 494
- Independent set of vertices, 741
- Index of summation, 163
- Index registers, 732
- Indicator random variable, 492
- Indirect proofs, 83
- Indistinguishable
  - boxes, 428–431
  - objects, 428–431
  - objects, permutations with, 428
  - strings, 888
- Induction
  - complete, 334
  - generalized, 356–357
  - incomplete, 334
  - mathematical, 29, 311–329
  - principle of, 377
  - proofs by, 315–329
  - second principle of, 334
  - strong, 333–335, 378
  - structural, 353–356, 378
  - validity of, 326
  - well-ordered, 620, 634
- Inductive definitions, 345–357
  - of functions, 345–349, 378
  - of sets, 349–356, 378
  - of strings, 350
  - of structures, 349–356
- Inductive hypothesis, 313
- Inductive loading, 333, 343, 380
- Inductive reasoning, 312
- Inductive step, 313, 377, 752, 768
- Inequality
  - Bernoulli's, 330
  - Bonferroni's, 467
  - Boole's, 467
  - Chebyshev's, 491, 495
  - Markov's, 493
  - of harmonic numbers, 320–321
  - proving by mathematical induction, 319–320
  - triangle, 108
- Inference
  - for program correctness, 373
  - rule of, 110
  - rules of, 69–71
- Infinite graph, 641
- Infinite ladder, 311
  - by strong induction, 334
- Infinite series, 167
- Infinite set, 121
- Infinitude of primes, 260
- Infix form, 780
- Infix notation, 779–782, 804
- Influence graphs, 645
- Information flow, lattice model of, 627
- Initial assertion, 372, 378
- Initial conditions, 158, 565
- Initial position
  - of a Turing machine, 889
- Initial state, 859
  - finite-state automaton, 867
  - of a Turing machine, 889
- Initial terms
  - identifying a sequence using, 161
- Initial value, A-14
- Initial vertex, 594, 654
- Injection, 141, 186
- Injective (one-to-one) function
  - counting, 387
- Injective function, 141
- Inorder traversal, 773, 775, 778, 804
- Input
  - to an algorithm, 193
- Input alphabet, 859
- Input string
  - finite-state machine, 861
- Insertion sort, 196, 197, 232
  - average-case complexity of, 483–484
  - worst-case complexity, 222
- Instantiation
  - existential, 76
  - universal, 75
- Integer
  - composite, 257, 306
  - perfect, 272
  - prime, 257
  - signed, 855
- Integer(s)
  - linear combination of, 306
- Integer-valued function, 140
- Integers
  - axioms for, A-5
  - division of, 238–240
  - multiplication of
    - fast, 528–529
  - pairwise relatively prime, 306
  - partition of, 359
  - relatively prime, 306
  - set of, 116
  - squarefree, 564
- Integer sequences, 162
- Integers modulo  $m$ , 243
  - additive inverses, 243
  - associativity, 243
  - closure, 243
  - commutativity, 243
  - distributivity, 243
  - identity elements, 243
- Intension, of database, 585
- Interconnection networks for parallel computation, 661–663
- Interest, compound, 160
- Interior of simple polygon, 338
- Interior vertices, 603
- Internal vertices, 748, 804
- International Mathematical Olympiad (IMO), 263, 299
- International Standard Book Number (ISBN), 291
- International Standard Serial Number (ISSN), 293
- Internet, search engines on, 794
- Internet addresses, counting, 392
- Internet datagram, 399
- Internet Movie Database, 645
- Internet Protocol (IP) multicasting, 786
- Intersection
  - of fuzzy sets, 138
- Intersection graph, 650
- Intersection of a collection of sets, 133
- Intersection of multisets, 138
- Intersection of sets, 127, 185
- Interval(s), 117
  - closed, 117
  - open, 117, 332
- Intractable
  - problems, 226
- Intractable problem, 232, 897
- Invariant for graph isomorphism, 672, 736
- Invariants, loop, 375–376, 378
- Inverse, 8
  - modular, 275, 306
- Inverse, multiplicative, 60
- Inverse function, 145, 186
- Inverse law
  - for addition, A-2
  - for multiplication, A-2
- Inverse of a square matrix, 184
- Inverse relation, 582
- Inversions, in permutation, expected number of, 482–484
- Inverter, 21, 823, 843
- invertible function, 145
- Invertible matrix, 184
- IP multicasting, 786
- Irrationality of  $\sqrt{2}$ , 342, 381
- Irrational number(s), 85, 116
- Irreflexive relation, 581
- ISBN-10, 291
- ISBN-13, 291
  - check digit, 308

ISBN check digit, 291  
Isobutane, 750  
Isolated vertex, 652, 736  
Isomorphic graphs, 668, 671–675, 736  
  paths and, 687–688  
Iterated function, 360  
Iterated logarithm, 360  
Iteration, 160, 360  
  using to solve recurrence relations, 159  
Iteration using backward substitution, 160  
Iteration using forward substitution, 160  
Iterative algorithm, for Fibonacci numbers, 366  
Iterative procedure, for factorials, 366  
Iwaniec, Henryk, 264

Jacobian rebellion, 151  
Jacquard loom, 31  
Jarník, Vojtěch, 798  
Java, 855  
Jealous husband problem, 693  
Jersey crags, 163  
Jewish–Roman wars, 512  
Jigsaw puzzle, 342  
Job(s)  
  assignment of, 565, 658  
  lateness of, 235  
  slackness of, 235  
Join, in lattice, 637  
Join of  $n$ -ary relations, 588  
Join of zero–one matrices, 181  
Joint authorship, 645  
Jordan curve theorem, 338  
Josephus, Flavius, 512  
Josephus problem, 512  
Jug, 109, 693

$k$ -connected graph, 684  
 $k$ -tuple graph coloring, 734  
K-maps, 830–836, 843  
Königsberg, 171  
Königsberg bridge problem, 693–694, 696, 697  
Kakutani’s problem, 107  
Kaliningrad, Russia, 693  
Karnaugh, 830–836  
Karnaugh, Maurice, 830  
Karnaugh maps, 830–836, 843  
Kayal, Neeraj, 262  
Kempe, Alfred Bray, 728  
Key, 295  
  composite, 585  
  encryption, 306  
  for Caesar cipher, 295  
  hashing function, 287  
  primary, 585–586  
  public, 299  
Key exchange, 302  
Key exchange protocol, 305, 306  
Keystream  
  autokey cipher, 309  
King Hermeas, 2  
Kissing problem, 163  
Kleene’s theorem, 880, 900  
Kleene, Stephen Cole, 867, 878  
Kleene closure, 866, 899  
Knapsack problem, 235, 568  
Kneiphof Island, 693  
Knight’s tour, 707  
  reentrant, 707  
Knights, knaves, and normals puzzles, 112  
Knights, knaves, and spies puzzles, 112  
Knights and knaves puzzles, 19  
Knuth, Donald, 196, 206  
Knuth, Donald E., 208

Kruskal’s algorithm, 799–801, 804  
Kruskal, Joseph Bemard, 799, 800  
Kuratowski’s theorem, 724–725, 737  
Kuratowski, Kazimierz, 724

Löb’s paradox, 112  
Labeled tree, 756  
Ladder, infinite, 311–334  
Lady Byron, Annabella Millbanke, 31  
Lagarias, Jeffrey, 107  
Lamé’s theorem, 347  
Lamé, Gabriel, 349  
Landau, Edmund, 206, 207  
Landau symbol, 206  
Language, 847–899  
  context-free, 851  
  context-sensitive, 886  
  formal, 848  
  generated by grammar, 850  
  natural, 847–848  
  of a grammar, 850  
  recognized  
    by nondeterministic finite-state automaton, 873  
  recognized by an automaton, 899  
  recognized by finite-state automata, 868  
  regular, 851  
Language recognizer, 863  
Laplace’s definition of probability, 446  
Laplace, Pierre Simon, 445, 447, 472  
Large integers  
  computer arithmetic with, 279  
Large numbers, law of, 459  
Lateness of a job, 235  
Lattice model of information flow, 627  
Lattice point, 380  
Lattices, 626–627, 634  
  absorption laws for, 637  
  associative laws for, 637  
  bounded, 637  
  commutative laws for, 637  
  complemented, 637  
  distributive, 637  
  duality in, 639  
  idempotent laws for, 637  
  join in, 637  
  meet in, 637  
  modular, 639

Law  
  complement, 129  
  complementation, 129  
  Hardy–Weinberg, 97  
Law(s)  
  absorption  
    for Boolean algebra, 815, 816  
    for lattices, 637  
    for propositions, 27  
  associative  
    for addition, A-1  
    for Boolean algebra, 815, 818  
    for lattices, 637  
    for multiplication, A-1  
    for propositions, 27  
  closure  
    for addition, A-1  
    for multiplication, A-1  
  commutative  
    for addition, A-1  
    for Boolean algebra, 815, 818  
    for lattices, 637  
    for multiplication, A-1

  compatibility  
    additive, A-2  
    multiplicative, A-2  
  completeness, A-2  
  De Morgan’s  
    for Boolean algebra, 815, 819  
    for propositions, 28  
    proving by mathematical induction, 323–324  
  distributive, A-2  
    for Boolean algebra, 815, 818  
    for propositions, 27  
  domination  
    for Boolean algebra, 815  
  idempotent  
    for Boolean algebra, 815, 819  
    for lattices, 637  
    for propositions, 27  
  identity  
    additive, A-1  
    for Boolean algebra, 815, 816, 818  
    multiplicative, A-1  
  inverse  
    for addition, A-2  
    for multiplication, A-2  
  of detachment, 71  
  of double complement, in Boolean algebra, 815, 818  
  of large numbers, 459  
  of mathematical induction, A-5  
  transitivity, A-2  
  trichotomy, A-2  
  used to prove basic facts, A-3–A-5  
Law of total expectation, 492  
Laws  
  De Morgan’s, 26  
Laws of propositional logic, 27  
  absorption, 27  
  associative, 27  
  commutative, 27  
  De Morgan’s, 27  
  distributive, 27  
  domination, 27  
  double negation, 27  
  identity, 27  
Laws of Thought, The (Boole), 472, 811  
Leaf, 746, 804  
Least common multiple, 266, 306  
Least element of poset, 625, 634  
Least upper bound, 634, A-2  
  of poset, 625  
Left child of vertex, 749  
Left subtree, 749  
Lemma, 81, 110  
  pumping, 888  
Length of bit string, 505  
Length of path  
  in directed graph, 599  
  in weighted graph, 708  
Length of string  
  recursive definition of, 350  
“Less than or equals” relation, 619  
Letters of English  
  relative frequency, 296  
Level of vertex, 753, 804  
Level order of vertex, 806  
Levin, Leonid, 227  
Lewis Carroll (C. L. Dodgson), 50  
Lexicographic ordering, 356, 435, 620–622  
Liber Abaci (Fibonacci), 348  
Library sort, 196  
Light fixture controlled by three switches, circuit for, 825  
Limit, definition of, 61

- Linear array, 662
- Linear bounded automata, 886
- Linear combination of integers, 269, 306
- Linear complexity, 225
- Linear congruence, 275, 306
  - systems of, 277–279
- Linear congruence(s)
  - solving, 277
- Linear congruential method, 288
  - increment, 288
  - modulus, 288
  - multiplier, 288
  - seed, 288
- Linear homogenous recurrence relations, 514–520, 565
- Linearithmic complexity, 225
- Linearity of expectations, 477–484, 494
- Linearly ordered set, 619, 633
- Linear nonhomogenous recurrence relations, 520–524, 565
- Linear ordering, 619, 633
- Linear probing function, 288
- Linear search
  - average-case time complexity, 221
- Linear search algorithm, 194, 232
  - average-case complexity of, 482–484
  - recursive, 363
  - time complexity of, 220
- LISP, 855
- List of 23 problems
  - David Hilbert, 176
- Lists, merging two, 368
- Literal, 820, 843
- Little-*o* notation, 218
- Littlewood, John E., 97
- Load balancing problem, 235
- Loading, inductive, 333, 343, 380
- Load of a processor, 235
- Loan, 169
- Lobsters, 524
- Local area networks, 661
- Logarithm
  - discrete, 284
- Logarithm, iterated, 360
- Logarithm discrete, 306
- Logarithmic complexity, 225
- Logarithmic function, A-7–A-9
- logarithms
  - big-*O* estimates of, 212
- Logic, 1
  - fuzzy, 16
  - predicate, 37
  - propositional, 3
- Logical connectives, 4
- Logical equivalences, 27
  - constructing, 29
- Logical Expression(s)
  - translating English sentences into, 62–63
- Logical expressions
  - translating English sentences into, 16–17
  - translating mathematical statements into, 60, 61
- Logically equivalent compound propositions, 25, 110
- Logically equivalent expressions, 110
- Logically equivalent statements, 45
- Logical operators, 109
  - functionally complete, 35
  - precedence of, 11
- Logic circuit, 20, 110
- Logic gates, 21, 110, 822–827
  - AND, 21, 823, 843
  - combination of, 823
  - NAND, 828
  - NOR, 828
  - OR, 21, 823, 843
  - threshold, 845
- Logic programming, 51
- Logic puzzles, 19–20
- Long-distance telephone network, 646
- Longest common subsequence problem, 568
- Loom, Jacquard, 31
- Loop constructions, A-14–A-15
- Loop invariants, 375–376, 378
- Loops
  - in directed graphs, 594, 633
  - nested, 58
  - within loops, A-15
- Lord Byron, 31
- Lottery, 447
  - Mega Millions, 496
  - Powerball, 496
- Lovelace, Countess of (Augusta Ada), 29, 31
- Lower bound
  - of lattice, 637
  - of poset, 625, 634
- Lower limit of a summation, 163
- Lucas, Edouard, 503
- Lucas, François Édouard, 162
- Lucas numbers, 379, 525
- Lucas sequence, 162
- Lucky numbers, 570
- Łukasiewicz, Jan, 780, 782
- m*-ary tree, 748, 804
  - complete, 756
  - full, 748, 752
  - height of, 754–755
- m*-tuple, 586
- Ménages, probl’eme des, 571
- Machine
  - finite-state, 899
  - Mealy, 863, 899
  - Moore, 863, 865
  - Turing, 899
- machine
  - unit-delay, 861
- Machine(s)
  - delay, 861–862
  - finite-state, 847, 858–859
    - with no output, 865
    - with outputs, 859–863
  - Turing, 847, 886, 888, 889, 893
  - computing functions with, 892–893
  - definition of, 889
  - nondeterministic, 893
  - sets recognized by, 891–892
  - types of, 893
- Machine minimization, 872
  - vending, 858–859
- MAD Magazine*, 208
- Magic tricks, 20
- Majority voting, circuit for, 825
- Makespan, 235
- Making change
  - greedy algorithm, 199
- Male optimal, 234
- Mappings, 139
- Maps
  - coloring of, 727
- Markov’s inequality, 493
- markup languages, 858
- Massachusetts Institute of Technology (M.I.T.), 299
- Master theorem, 532
- Matching, 659
  - maximum, 659
  - stable, 204
  - string, 231
- Matchings with forbidden pairs, 234
- Mathematical induction, 29, 311–329
  - Axiom of, A-5
  - errors in, 328–329
  - generalized, 356–357
  - guidelines for, 328
  - incorrect proof by, 757
  - inductive loading with, 333
  - principle of, 377
  - proofs by, 315–329
    - errors in, 328–329
    - of divisibility facts, 321
    - of inequalities, 319–320
    - of results about algorithms, 324
    - of results about sets, 323–324
    - of summation formulae, 315
  - second principle of, 334
  - strong, 333–335, 378
  - structural, 353–356, 378
  - template for, 328
  - template for proofs, 329
  - validity of, 328
- Matrix (matrices)
  - addition, 178
  - adjacency, 669–671, 736
    - counting paths between vertices by, 688–689
  - entry of, 178
  - equal, 178
  - identity, 180, 186
  - incidence, 671, 736
  - invertible, multiplication
    - algorithm for, 222
    - complexity of, 223
    - noncommutativity of, 179
    - fast, 529
  - representing relations using, 591–594
  - row of a, 178
  - sparse, 670
  - square, 178
  - symmetric, 181, 186
  - transpose of, 181, 186
  - upper triangular, 231
  - zero–one, 181, 186
    - of transitive closure, 602–603
    - representing relations using, 591–594
    - Warshall’s algorithm and, 604–606
- Matrix-chain multiplication, 223
- Matrix-chain multiplication problem, 513
- Matrix product, 179
- Maurolico, Francesco, 313
- Maximal element of poset, 624, 634
- Maximum, of sequence, 528
- Maximum element
  - algorithm for finding, 193
  - in finite sequence, 192
- Maximum matching, 659
- Maximum satisfiability problems, 498
- Maximum spanning tree, 802
- Maxterm, 822
- McCarthy
  - function, 380
- McCarthy, John, 381
- McCluskey, Edward J., 837
- Mealy, G. H., 863
- Mealy machine, 863, 899
- Mean, 203
  - arithmetic, 100, 332
  - deviation from, 491
  - geometric, 100, 332
  - harmonic, 108
  - quadratic, 108
- Median, 203
- Meet, in lattice, 637
- Meet of zero–one matrices, 181

Mega Millions, Lottery, 496  
Meigu, Guan, 698  
Member of a set, 185  
Membership table, 186  
Members of a set, 116  
memoization, 510  
Merge sort, 196, 367–370, 378, 528  
    complexity of, 532  
    recursive, 368  
Merging two lists, 368  
Mersenne, Marin, 261  
Mersenne primes, 261, 306  
Mesh network, 662–663  
Mesh of trees, 809  
metacharacters, 858  
Metafont, 208  
Method  
    middle-square, 292  
    roster, 116  
Method(s)  
    Critical Path, 639  
    Horner's, 230  
    probabilistic, 465–466, 494  
    Quine–McCluskey, 830, 837–840  
Method(s) of proof, 82  
    by cases, 92, 95  
    by contradiction, 86  
    by contraposition, 83  
    by exhaustion, 93  
    direct, 82  
    exhaustive, 93  
    proofs of equivalence, 87  
    trivial, 84  
    vacuous, 84  
Method roster, 185  
Middle-square method, 292  
Millennium Prize problems, 227  
Miller's test, 286  
Miller's test for base  $b$ , 286  
Minimal element of poset, 624, 634  
Minimization  
    of Boolean functions, 828–840, 843  
    of combinational circuits, 828–840  
Minimization of a finite-state machine, 872  
Minimizing maximum lateness  
    greedy algorithm for, 235  
Minimum, of sequence, 528  
Minimum dominating set, 739  
Minimum spanning forest, 802  
Minimum spanning trees, 797–802, 804  
Minmax strategy, 767, 804  
Minterm, 820, 843  
Mistakes in proofs, 89–90  
Mixed graph, 644  
**mod** function, 239, 306  
Mode, 203  
Modeling  
    computation, 847–897  
    with graphs, 644–649  
    with recurrence relations, 502–507  
    with trees, 749–752  
Modular arithmetic, 240–306  
Modular exponentiation, 253  
    algorithm for, 253  
    recursive, 363  
Modular inverse, 275, 306  
Modular lattice, 639  
Modular properties, in Boolean algebra, 819  
Module dependency graphs, 647  
Modulus  
    for linear congruential method, 288  
Modus ponens, 71  
    universal, 77

Modus tollens, 71  
    universal, 77  
Mohammed's scimitars, 697  
Molecules, trees modeling, 750  
Money orders  
    identification numbers for, 293  
Monoalphabetic cipher, 297  
Monotone decreasing property of graph, 742  
Monotone increasing property of graph, 742  
Monotonic grammars, 852  
Monte Carlo algorithms, 463–465  
Montmort, Pierre Raymond de, 563, 571  
Monty Hall Three Door Puzzle, 450, 452, 476, 499  
Monty Python, 472  
Moore, E. F., 863  
Moore machine, 863, 865  
Moth, 872  
Motorized pogo stick, 812  
Mr. Fix-It, 263  
Muddy children puzzle, 19  
Multicasting, 786  
Multigraphs, 642, 644, 735  
    Euler circuit of, 697  
    Euler path of, 697  
    undirected, 644  
Multinomial coefficient, 434  
Multinomial theorem, 434  
Multiple, 238  
    least common, 266, 306  
Multiple edges, 642–644, 735  
Multiple output circuit, 826  
Multiplexer, 828  
Multiplication  
    of function, 141  
    matrix-chain, 223  
    of integers  
        fast, 528–529  
    of matrices  
        fast, 529  
Multiplication algorithm, 251  
Multiplicative Compatibility Law, A-2  
Multiplicative inverse, 60  
Multiplicities of elements in a multiset, 138  
Multiplier  
    for linear congruential method, 288  
Multiset, 138  
    multiplicities of elements, 138  
Multisets  
    difference of, 138  
    intersection of, 138  
Mutually independent events, 497  
Mutually independent trials, 458  
  
 $n$ -ary relations, 583–589, 633  
    domain of, 584  
    operations on, 586–588  
 $n$ -cubes, 655  
 $n$ -queens problem, 792–793  
 $n$ -regular graph, 667  
 $n$ -tuple  
    ordered, 122  
 $n$ -tuples, 584–585  
Naive set theory, 118  
Namagiri, 98  
NAND, 821, 843  
NAND gate, 828  
Natural language, 847–848  
Natural numbers  
    set of, 116  
Naur, Peter, 854

NAUTY, 674  
Naval Ordnance Laboratory, 872  
Navy WAVES, 872  
Necessary and sufficient conditions, 9  
Necessary condition, 6  
    expressing a conditional statement using, 6  
Necessary for, 6  
Negating conjunctions, 28  
Negating disjunctions, 28  
Negating Quantified Expressions, 46  
Negation, 109  
    of a proposition, 3  
    of nested quantifiers, 63–64  
    truth table for, 4  
Negation operator, 4  
Negative  
    false, 471  
    true, 471  
Neighbors in graphs, 651  
Neptune, 476  
Nested loops, 58  
Nested quantifiers, 57–64  
    negating, 63–64  
Network(s)  
    computer, 641  
        interconnection networks, 661–663  
        local area networks, 661  
        multicasting over, 786  
        with diagnostic lines, 642  
        with multiple lines, 642  
        with multiple one-way lines, 642  
        with one-way lines, 643  
    gating, 822–823  
        depth of, 828  
        examples of, 823–825  
        minimization of, 828–840  
    social, 644  
    tree-connected, 751–752  
Network number (netid), 392  
Newton–Pepys problem, 500  
Niche overlap graph, 648  
Nickels, 199  
Nim, 766, 768  
Nobel Prize, 119  
Nodes, 594, 641  
Noncommutativity of matrix multiplication, 179  
Nonconformists, 472  
Nonconstructive existence proof, 96, 110  
Noncontracting grammar, 851  
Nondeterministic finite-state automaton, 873, 899  
    equivalent finite-state automaton, 874  
    language recognized by, 873  
Nondeterministic polynomial-time problems, 227  
    class of, 900  
item Nondeterministic Turing machine, 893, 899  
Nonoverlapping ears, 343  
Nonplanar graphs, 724–725  
Nonregular set, 891  
    recognition by Turing machine, 891  
Nonresidue  
    quadratic, 286  
Nonseparable graph, 683  
Nonterminals, 849  
NOR, 821, 843  
NOR gate, 828  
Normal form  
    disjunction, 35  
    prenex, 68  
NOT, 18

- Notation
- big- $O$ , 205, 232
  - big-Omega ( $\Omega$ ), 214, 232
  - big-Theta, 215
  - big-Theta ( $\Theta$ ), 232
  - dependency, 846
  - for products
    - well-formed formula in, 784
  - infix, 779–782, 804
  - little- $o$ , 218
  - Polish, 780, 804
  - postfix, 779–782, 804, 858
  - prefix, 779–782, 804
  - product, 186
  - reverse Polish, 781, 804, 858
  - set builder, 116, 185
  - summation, 162, 186
- NOT gate, 21
- Noun, 848
- Noun phrase, 848
- Nova*, 107
- NP, class of nondeterministic polynomial-time problems, 900
- NP-complete problems, 227, 715, 830, 900
- Null quantification, 56
- Null set, 185
- Null string, 849
- Number(s)
- Bacon, 680
  - Bell, 618
  - cardinal, 121
  - Carmichael, 283, 306
  - Catalan, 507
  - chromatic, 728, 737
    - edge, 734
  - crossing, 726
  - computable, 886
  - Cunningham, 262
  - Erdős, 635, 680, 689
  - Fibonacci, 347, 365–367, 771
    - formula for, 517
    - iterative algorithm for, 366
    - rabbits and, 502–503
    - recursive algorithms for, 365
  - harmonic
    - inequality of, 320–321
  - independence, 741
  - irrational, 85, 116
  - large, law of, 459
  - Lucas, 379, 525
  - lucky, 570
  - natural, 116
  - pseudorandom, 288
  - Ramsey, 404
  - rational, 85, 116
  - real, A-1–A-5
  - Stirling, of the first kind, 431
    - signless, 443
  - Stirling, of the second kind, 430
  - Ten Most Wanted, 262
  - Ulam, 188
- Number-theoretic functions, 892
- Numbering plan, 387
- Number theory, 237
  - definition of, 237
- Object, 118
- Object(s)
- distinguishable, 428
    - and distinguishable boxes, 428–429
    - and indistinguishable boxes, 428–431
  - indistinguishable, 428
    - and indistinguishable boxes, 428–431
  - unlabeled, 428
- Obligato game, 112
- Octahedral die, 496
- Octal expansions, 246, 306
- Octal representation, 246, 306
- Odd, 83
- Odd pie fights, 325
- Odlyzko, Andrew, 163
- Odometer, 307
- One's complement representations, 256
- One-to-one (injective) function
  - counting, 387
- One-to-one correspondence, 144, 186
- One-to-one function, 141, 143, 186
- On-Line Encyclopedia of Integer Sequences (OEIS)*, 162
- Only if, expressing conditional statement using, 7
- Onto (surjective) function, 143, 186
  - number of, 560–562, 566
- Open interval, 117, 332
- Open problems, 106, 263–264
- Operands, well-formed formula of, 351
- Operation(s)
- bit, 11, 110
  - bitwise, 110
  - set, 127
- Operations
  - on  $n$ -ary relations, 586–588
- Operator(s)
- bitwise, 12
  - logical, 109
  - negation, 4
  - logical, 109
  - selection, 586
  - well-formed formula of, 351
- Opium, 475
- Optimal algorithm, 230
- Optimal for suitors, stable assignment, 343
- Optimal solution, 198
- Optimization problems, 198
- OR, 18
- Or
- exclusive, 5, 6
  - inclusive, 5
- Oracle of Bacon, 680
- Order, 207
  - of quantifiers, 58
- Ordered  $n$ -tuple, 122
- Ordered rooted tree, 749, 804, 806
- Ordering
- dictionary, 435
  - lexicographic, 356, 435, 620–622
  - linear, 619
  - partial, 618–629, 633
  - quasi-ordering, 637
  - total, 619, 633
- Ordered pair
  - defined using sets, 126
- Ordinary generating function, 537
- Ore's theorem, 701, 707
- Ore, O., 701
- Organizational tree, 750
- OR gate, 21, 823, 843
- Orientable graphs, 740
- Orientation of undirected graph, 740
- Out-degree of vertex, 654, 736
- Output
  - to an algorithm, 193
- Output alphabet, 859
- Outputs
  - finite-state machines with, 859–863
  - finite-state machines without, 865
- Output string
  - finite-state machine, 861
- $P(n, r)$ , 439
- P, class of polynomial-time problems, 900
- P=NP problem, 897
- Pair, devil's, 678
- Pairs, forbidden, 234
- Pairwise relatively prime integers, 306
- Palindrome(s), 202, 397, 857
  - set of, 888
- Paradigm
  - Algorithmic, 224, 232
- Paradox, 118, 185
  - barber, 16
  - Löb's, 112
  - Russell's, 126
  - St. Petersburg, 497
- Parallel algorithms, 661
- Parallel edges, 642
- Parallel processing, 229, 661
  - tree-connected, 751–752
- Parentheses, balanced strings of, 382
- Parent of vertex, 747, 803
- Parent relation, 580
- Parity
  - same, 83
- Parity check bit, 290
- Parse tree, 852–854, 899
- Parsing
  - bottom-up, 853
  - top-down, 853
- Partial correctness, 372
- Partial function, 152, 186, 889
  - codomain of, 152
  - domain of, 152
  - domain of definition, 152
  - undefined values, 152
- Partially ordered set, 618
  - antichain in, 637
  - chain in, 637
  - comparable elements in, 622, 633
  - dense, 632
  - dual of, 630
  - greatest element of, 625, 634
  - Hasse diagram of, 622–624, 634
  - incomparable elements in, 622, 633
  - least element of, 625, 634
  - lower bound of, 625, 634
  - maximal element of, 624, 634
  - minimal element of, 624, 625, 634
  - upper bound of, 625, 634
  - well-founded, 632
- Partial orderings, 618–629, 633
  - compatible total ordering from, 634
- Partition, 552
  - of positive integer, 359, 431
  - of set, 612–614, 633
  - refinement of, 617
- Partner
  - valid, 234
- Pascal's identity, 418–419, 439
- Pascal's triangle, 419, 439
- Pascal, Blaise, 282, 419, 445, 452
- Passwords, 66, 391

- Paths, 678–681
  - and graph isomorphism, 687–688
  - counting between vertices, 688–689
  - Euler, 693–698, 736
  - Hamilton, 698–703, 736
  - in acquaintanceship graphs, 680
  - in collaboration graphs, 680
  - in directed graphs, 599–600, 633, 736
  - in directed multigraphs, 679
  - in Hollywood graph, 680–681
  - in simple graphs, 679
  - in undirected graphs, 679
  - length of, in weighted graph, 708
  - of length  $n$ , 680
  - shortest, 707–716, 736
  - terminology of, 679
- Payoff, 765
- Pearl Harbor, 872
- Pecking order, 741
- Peirce, Charles Sanders, 38
- Peirce arrow, 36
- Pelc, A., 536
- Pendant vertex, 652, 736
- Pennies, 199
- Perfect integer, 272
- Perfect power, 93
- Perfect square, 83
- Peripatetics, 2
- Permutation, circular, 415
- Permutations, 407–409, 439
  - generating, 434–436
  - generating random, 499
  - inversions in, expected number of, 482–484
  - with indistinguishable objects, 427–428
  - with repetition, 423
- PERT (Program Evaluation and Review Technique), 639
- Petersen, Julius Peter Christian, 706
- Phrase-structure grammar, 849, 899
- Phrase-structure grammars, 849–854
- Pick’s theorem, 342
- Pie fights, odd, 325
- Pigeonhole principle, 86, 399–405, 439
  - applications with, 403–405
  - generalized, 401–403, 439
- Planar graphs, 718–725, 736
- Plato, 2
- Plato’s Academy, 2, 259
- PNF (prenex normal form, 68
- Pogo stick, motorized, 812
- Pointer, position of, digital representation of, 702–703
- Poisonous snakes, 763
- Poker hands, 411
- Polish notation, 780, 804
- Polygon, 338
  - convex, 338
  - diagonal of, 338
  - exterior of, 338
  - interior of, 338
  - nonconvex, 338
  - sides of, 338
  - simple, 338
  - vertices of, 338
  - with nonoverlapping ears, 343
- Polynomial-time algorithm for primality, 262
- Polynomial-time problems
  - class of, 900
- Polynomial complexity, 225
- Polynomials
  - big- $O$  estimates for, 212
  - big- $O$  estimates of, 209
  - big-Theta estimates for, 216
- Polynomials, rook, 571
- Polyominoes, 105, 326
- Ponens
  - modus, 71
- Population of the world, 168
- Poset, 618, 633
  - antichain in, 637
  - chain in, 637
  - comparable elements in, 619, 633
  - dense, 632
  - dual of, 630
  - greatest element of, 625, 634
  - Hasse diagram of, 622–624, 634
  - incomparable elements in, 619, 633
  - least element of, 625, 634
  - lower bound of, 625, 634
  - maximal element of, 624, 634
  - minimal element of, 624, 625, 634
  - upper bound of, 625, 634
  - well-founded, 632
- Positive
  - false, 471
  - true, 471
- Positive integers
  - axioms for, A-5
- Postcondition, 372
- Postconditions, 39
- Postfix form, 781
- Postfix notation, 779–782, 804, 858
- Postorder traversal, 773, 776–778, 804
- Postulates, 81
- Potrzenie System of Weights and Measures, 208
- Powerball, Lottery, 496
- Power generator, 292
- Powers
  - of relation, 580–581, 633
- Power series, 538–541
  - formal, 538
- Power set, 121, 185
- Pre-image of an element, 139, 186
- Precedence
  - of logical operators, 11
  - of quantifiers, 44
- Precedence graphs, 647
- Precondition(s), 39, 372
- Predicate, 110
  - truth set of, 125
- Predicate calculus, 40
- Predicate logic, 37
- Prefix codes, 762–764, 804
- Prefix form, 780
- Prefix notation, 779–782, 804
  - well-formed formula in, 784
- Premise of a condition statement, 6, 110
- Premises of an argument, 69, 70
- Prenex normal form (PNF), 68
- Preorder traversal, 773–775, 778, 804
- Prim’s algorithm, 798–799, 804
- Prim, Robert Clay, 798, 800
- Primality testing, 464–465
- Primary key, 585–586, 633
- Prime, 257, 306
  - Mersenne, 306
  - primitive root of a, 306
  - probability positive integer less than  $n$  is, 262
- Prime(s)
  - arithmetic progression of, 263
  - conjectures about, 263
  - distribution of, 261
  - in arithmetic progressions, 262
  - infinitude of, 260
  - Mersenne, 261, 306
  - of form  $n^2 + 1$ , 264
  - primitive root of a, 306
  - probability positive integer less than  $n$  is, 262
  - twin, 264
- Prime factorization, 259
- Prime implicant, 832, 843
  - essential, 832
- Prime number theorem, 262, 636
- Primitive root of a prime, 284, 306
- Prince of Mathematics, 241
- Princess of Parallelograms, 31
- Principia Mathematica (Whitehead and Russell), 34
- Principia Mathematica*, 119
- Principle(s)
  - duality, for Boolean identities, 816
  - of buoyancy, A-4
  - of counting, 385–390
  - of inclusion–exclusion, 392–394, 553–557, 566
    - alternative form of, 559
    - applications with, 558–564
  - of mathematical induction, 377
  - of well-founded induction, 635
  - of well-ordered induction, 620
- pigeonhole, 86, 399–405, 439
  - applications with, 403–405
  - generalized, 401–403, 439
- Principle of inclusion–exclusion, 128
- Private key
  - cryptosystem, 298, 306
  - RSA system, 301
- Prize, Nobel, 119
- Probabilistic algorithms, 445, 463–465, 494
- Probabilistic method, 465–466, 494
- Probabilistic primality testing, 464–465
- Probabilistic reasoning, 450
- Probability, discrete, 445–500
  - assigning, 453–455
  - conditional, 453, 456–457, 494
  - finite, 445–448
  - in medical test results, 471–472
  - Laplace’s definition of, 446
  - of collision in hashing functions, 462–463
  - of combinations of events, 449–450, 455–456
- Probability distribution, 453
- Probability generating function, 552
- Probability positive integer less than  $n$  is prime, 262
- Probability theory, 445, 452–466
- Probing function, 288
- Problem(s)
  - $n$ -queens, 792–793
  - art gallery, 735
  - birthday, 461–463
  - bridge, 693–694, 696, 697
  - celebrity, 332
  - Chinese postman, 698
  - class of NP-complete, 897
  - class P, 896
  - closest-pair, 532–535
  - Collatz, 107
  - decidable, 895
  - decision, 894, 900
  - discrete logarithm, 284
  - halting, 201, 895, 900
  - hatcheck, 481, 562
  - Hilbert’s 23, 895
  - Hilbert’s Tenth Problem, 895
  - intractable, 226, 232, 897
  - jealous husband, 693
  - Josephus, 512
  - Kakutani’s, 107
  - kissing, 163
  - knapsack, 235, 568
  - load balancing, 235
  - longest common subsequence, 568
  - matrix-chain multiplication, 513
  - maximum satisfiability, 498

- Millennium Prize, 227
- Newton–Pepys, 500
- NP, 227, 896
- NP-complete, 227, 715, 830, 900
- P, 227
- P=NP, 897
- P versus NP, 227
- open, 106, 263–264
- optimization, 198
- problem, two children, 498
- satisfiability, 34, 227
- Satisfiability
  - solving, 34
- scheduling greedy algorithm for
  - final exams, 731, 732
- searching, 194
- shortest-path, 707–716, 736
- solvable, 226, 232, 895, 900
- Syracuse, 107
- tiling, 895
- tractable, 226, 232, 897
- traveling salesman, 714–716, 736
- traveling salesperson, 702, 709
- two children, 498
- Ulam’s, 107
- undecidable, 895
- unsolvable, 226, 232, 895, 900
- utilities-and-houses, 718
- yes-or-no, 894
- Probl’eme de rencontres*, 563, 571
- Probl’eme des ménages*, 571
- Procedure statements, A-11
- Processing
  - concurrent, 647
  - parallel, 229, 661
  - tree-connected, 751–752
- Product
  - Boolean, 811–812, 821, 843
  - matrix, 179
- Product-of-sums expansion, 820
- Production, 899
- Productions, 849
  - of grammar, 849
- Product notation, 186
- Product rule, 386
- Program correctness, 372–378
  - conditional statements for, 373–375
  - loop invariants for, 375–376
  - partial, 372
  - program verification for, 372–373
  - rules of inference for, 373
- Program Evaluation and Review Technique (PERT), 639
- Programming
  - logic, 51
- Programming, dynamic, 507
- Programming languages, 398, 611
- Program verification, 372–373
- Progression
  - arithmetic, 186
  - geometric, 157, 186
  - sums of, 318–319
- Projection of  $n$ -ary relations, 586, 633
- Prolog, 51, 74
- Proof(s), 81, 110
  - adapting, 101
  - by cases, 92–110
    - common errors with, 95
  - by contradiction, 86, 110
  - by contraposition, 83, 110
  - by exhaustion, 93
  - by mathematical induction, 315–329
  - by structural induction, 353
  - combinatorial, 412, 439
  - constructive existence, 96
  - direct, 82, 1180
  - existence, 96
  - indirect, 83
  - mistakes in, 89
  - nonconstructive existence, 96
  - of equivalence, 87
  - of recursive algorithms, 364–367
  - trivial, 84, 110
  - uniqueness, 99, 110
  - vacuous, 84, 110
- Proof strategy, 85, 100–106
- Proper subset, 185
- Properties
  - of algorithms, 193
- Property
  - Archimedean, A-5
  - Completeness, A-2
  - Well-ordering, 340–341, 378, A-5
- Proposition(s), 2, 81, 109
  - compound, 3, 25, 27 109
  - negation of, 3, 109
- Propositional equivalences, 129
- Propositional calculus, 3
- Propositional function, 110
- Propositional logic, 3
  - applications of, 16
  - argument, 70
  - rules of inference for, 71
- Propositional variable(s), 2, 109
- Protein interaction graph, 648
- Protestant Nonconformists, 472
- Protocol(s)
  - cryptographic, 302
  - Diffie–Helman key agreement, 302
  - key exchange, 305, 306
- Pseudocode, 192, A-11–A-15
- Pseudograph, 643, 644, 735
- Pseudoprime, 282, 306
  - strong, 286
  - to the base  $b$ , 282
- Pseudorandom numbers, 288
  - generated by linear congruential method, 288
  - middle-square generator, 292
  - power generator for, 292
  - pure multiplicative generator of, 289
- Public key
  - cryptosystem, 298
  - encryption, 306
  - RSA system, 299
- Pumping lemma, 888
- Pure multiplicative generator, 289
- Pushdown automaton, 886
- Puzzle
  - “Voyage Around the World,” 700
  - Birthday Problem, 461–463
  - Icosian, 698
  - jigsaw, 342
  - knights, knaves, and normals, 112
  - knights, knaves, and spies, 112
  - knights and knaves, 19
  - the lady or the tiger, 24
  - logic(, 19
  - logic), 20
  - Monty Hall Three Door, 450, 452, 476, 499
  - muddy children, 19
  - Reve’s, 504
  - river crossing, 692
  - Sudoku, 32
  - Sun-Tsu’s, 277
  - Tower of Hanoi, 503–504
  - zebra, 24
- P versus NP problem, 227
- Pythagorean triples, 106
- Pāṇini, 854
- Quadratic congruence, 285
- Quadratic mean, 108
- Quadratic nonresidue, 286
- Quadratic residue, 286
- Quad trees, 809
- Quality control, 463
- Quantification, 40
  - as loops, 58
  - existential, 42, 110
  - null, 56
  - universal, 110
- Quantification, universal, 40
- Quantified Expressions
  - negating, 46
- Quantified statement(s)
  - restricted domain, 124
  - rules of inference for, 75
  - rules of inference for), 77
- Quantifier
  - existential, 42
  - scope of, 45, 110
  - uniqueness, 44
  - universal, 40
- Quantifiers
  - De Morgan’s law, 47
  - nested
    - negating, 63–64
  - nested(, 57
  - nested), 64
  - order of, 58
  - precedence of, 44
  - use in system specifications, 50
- Quarters, 199
- Quasi-ordering, 637
- Queen of mathematics, 241
- Queen of the sciences, 241
- Queens on chessboard, 740
- Question, begging the, 90, 110
- Quick sort, 196, 371
- Quine, Willard van Orman, 837, 839
- Quine–McCluskey method, 830, 837–840
- Quotient, 238, 239, A-6
- Quotient automaton, 878
- $r$ -combination, 410, 439
- $r$ -permutation, 407, 439
- Rabbits, 502–503
- Races, horse, 31
- Radius of graph, 741
- Rado, Tibor, 899
- Ramanujan, Srinivasa, 97, 98
- Ramaré, O., 264
- Ramsey, Frank Plumpton, 404
- Ramsey number, 404
- Ramsey theory, 404
- Random permutation, generating, 499
- Random simple graph, 742
- Random variables, 454, 460–461
  - covariance of, 494
  - definition of, 494
  - distribution of, 460, 494
  - geometric, 484–485
  - expected values of, 477–480, 491, 494
  - independent, 485–487, 494
  - indicator, 492
  - standard deviation of, 487
  - variance of, 477–480, 494
- Range of a function, 139, 186
- Ratio
  - common, 157

Rational number(s), 85, 116  
  countability of, 172  
Reachable, 807  
Reachable state, 901  
Real-valued function, 140  
Real number  
  decimal expansion of a, 174  
Real numbers  
  constructing, A-5  
  least upper bound, A-2  
  set of, 116  
  upper bound, A-2  
Reasoning  
  circular, 90, 110  
  deductive, 312  
  forward, 100  
  inductive, 312  
  probabilistic, 450  
Recognized language, 868  
Recognized strings, 868  
Recognizer  
  language, 863  
*Rencontres*, 563, 571  
Records, 584  
Recurrence relation(s), 158, 186, 501–510  
  associated homogenous, 520  
  definition of, 158, 565  
  divide-and-conquer, 527–535  
  initial condition for, 158  
  linear homogenous, 514–520, 565  
  linear nonhomogenous, 520–524, 565  
  modeling with, 502–507  
  simultaneous, 526  
  solution of, 158  
  solving, 514–524  
    generating functions for, 546–548  
  solving using iteration, 159  
Recursion, 344  
Recursive algorithms, 360–370, 378  
  correctness of, 364  
  for binary search, 363  
  for computing  $a^n$ , 361  
  for computing greatest common divisor, 362  
  for factorials, 361  
  for Fibonacci numbers, 365  
  for linear search, 363  
  for modular exponentiation, 363  
  proving correct, 364–367  
  trace of, 361, 362  
Recursive definitions, 311, 345–357  
  of extended binary trees, 352  
  of factorials, 361  
  of functions, 345–349, 378  
  of a sequence, 158  
  of sets, 349–356, 378  
  of strings, 349  
  of structures, 349–356  
Recursive merge sort, 368  
Recursive modular exponentiation, 363  
Recursive sequential search algorithm, 363  
Recursive step, 349  
Reentrant knight's tour, 707  
Refinement, of partition, 617  
Reflexive closure of relation, 598, 634  
Reflexive relation, 576, 633  
  representing  
    using digraphs, 594–596  
    using matrices, 591  
Regions of planar representation graphs, 719, 736  
Regular expression, 899  
Regular expressions, 879  
Regular grammar(s), 851, 884, 899, 900  
Regular graph, 667

Regular language, 851  
Regular set(s), 878–879, 884, 899, 900  
  constructing automaton to recognize, 881  
Relation, 124  
  recurrence, 158, 186  
Relation(s), 573–639  
   $n$ -ary, 583–589, 633  
  domain of, 584  
  operations on, 586–588  
  “greater than or equal,” 618–619  
  “less than or equals,” 619  
  antisymmetric, 577–578, 633  
  asymmetric, 582  
  binary, 573, 633  
  circular, 635  
  closures of, 597–606, 633  
    reflexive, 598, 633  
    symmetric, 598, 634  
    transitive, 597, 600–603, 634  
  combining, 579–580  
  complementary, 582  
  composite of, 580, 633  
  connectivity, 600, 633  
  counting, 578–579  
  covering, 623, 631  
  diagonal, 598  
  divide-and-conquer recurrence, 527  
  divisibility, 619  
  domains of, 584  
  equivalence, 607–614, 633  
  functions as, 574  
  inclusion, 619  
  inverse, 582, 633  
  irreflexive, 581  
  on set, 575–576  
  parent, 580  
  paths in, 599–600  
  powers of, 580–633  
  properties of, 576–579  
  reflexive, 576, 633  
  representing  
    using digraphs, 594–596  
    using matrices, 591–594  
  symmetric, 577–578, 634  
  transitive, 578–580, 633  
Relational database model, 584–586, 633  
Relation on a set, 124  
Relative frequency  
  letters of English, 296  
Relatively prime integers, 306  
Remainder, 239, 306  
Removing and edge from a graph, 663  
Removing an edge from a vertices, 664  
Repetition  
  combinations with, 424–427  
  permutations with, 423  
Replacement  
  sampling with, 448  
  sampling without, 448  
Representation  
  base  $b$ , 306  
  binary, 306  
  octal, 306  
  unary, 892  
Representation hexadecimal, 306  
Representations  
  one's complement, 256  
  two's complement, 256  
Representative, of equivalence class, 610  
Residue  
  quadratic, 286  
Resolution, 74  
Resolution (rule of inference), 71

Restricted domain  
  of quantified statement, 124  
  quantifier with, 44  
**return** statement, A-15  
Reve's puzzle, 504  
Reverse-delete algorithm, 803  
Reverse Polish notation, 781, 804  
reverse Polish notation, 858  
Right child of vertex, 749  
Right subtree, 749  
Right triominoes, 326, 333  
Ring commutative, 244  
Ring topology for local area network, 661  
River crossing puzzle, 692  
Rivest  
  Ronald, 300  
Rivest, Ronald, 299  
RNA (ribonucleic acid), 388  
RNA chain sequencing, 443  
Roadmaps, 647  
Rock climbing, 163  
Rocket-powered Frisbee, 812  
Rook polynomials, 571  
Root  
  primitive, 284  
Rooted Fibonacci trees, 757  
Rooted spanning tree, 797  
Rooted trees, 351, 747–749  
   $S_k$ -tree, 806  
  B-tree of degree  $k$ , 805  
  balanced, 753, 804  
  binomial, 805  
  decision trees, 760–762  
  definition of, 803  
  height of, 753, 804  
  level order of vertices of, 806  
  ordered, 749, 804, 806  
Roots, characteristic, 515  
Roster method, 116, 185  
Round-robin tournaments, 341, 649  
Routing transit number (RTN), 308  
  check digit, 308  
Row of a matrix, 178  
Roy, Bernard, 603  
Roy–Warshall algorithm, 603–606  
RSA system, 299  
  cryptosystem, 299, 301, 306  
  decryption, 300  
  decryption key, 301  
  digital signatures, 303  
  encryption 299  
  private key, 301  
  public key, 301  
Rule  
  division, 394  
  product, 386  
  subtraction, 393  
  sum, 386, 389, 439  
Rule(s) of inference, 69–71, 110  
  addition, 71  
  building arguments using, 73  
  conjunction, 71  
  disjunctive syllogism, 71  
  for program correctness, 373  
  for propositional logic, 71  
  for quantified statements, 75–77  
  hypothetical syllogism, 71  
  modus ponens, 71  
  modus tollens, 71  
  resolution, 71, 74  
  simplification, 71  
Run, 492  
Russell's paradox, 126  
Russell, Bertrand, 118, 119



- $S_k$ -tree, 806
- Same parity, 83
- Samos, Michael, 533
- Sample space, 446
- Sampling
  - without replacement, 448
  - with replacement, 448
- Sandwich, 858
- Sanskrit, 854
- Satisfiability, 30
- Satisfiability problem, 227
  - solving, 34
  - modeling Sudoku puzzle as, 32
- Satisfiability problem, maximum, 498
- Satisfiable compound proposition, 30, 110
- Saturated hydrocarbons, trees modeling, 750
- Saxena, Nitin, 262
- Scheduling problems
  - final exams, 731, 732
  - greedy algorithm for, 324–325
  - software projects, 633
  - talks, 200
  - tasks, 629
- Schröder, Ernst, 175
- Schröder–Bernstein theorem, 174
- Scimitars, Mohammed’s, 697
- Scope of a quantifier, 45, 110
- Screw, Archimedes, A-4
- Search
  - binary, 194
  - linear, 194
  - sequential, 194
- Search engines, 794
- Searches
  - Boolean, 18
- Searching algorithms, 194–196, 232
  - binary, 528
  - breadth-first, 789–791, 804
  - depth-first, 787–789, 804
    - applications with, 794–795
    - in directed graphs, 794–795
  - linear
    - average-case complexity of, 482–484
    - recursive, 363
    - recursive binary, 363
    - recursive linear, 363
    - recursive sequential, 363
- Searching problems, 194
- Search trees, binary, 757–759, 804
- Searcng
  - web pages, 18
- Second principle of mathematical induction, 334
- Secret key
  - exchange, 302
- Seed
  - for linear congruential method, 288
- Sees, 735
- Selection operator, 586, 633
- Selection sort, 196, 203
- Self-complementary graph, 677
- Self-converse directed graph, 740
- Self-dual, 844
- Self-generating sequences, 382
- Semantics, 847
- Sentence, 848, 849
- Separating set, 684
- Sequence(s), 156, 186
  - de Bruijn, 744
  - Fibonacci, 158
  - finding maximum and minimum of, 528
  - generating functions for, 537
  - integer, 162
  - Lucas, 162
  - recursive definition of, 158
  - self-generating, 382
  - strictly decreasing, 403
  - strictly increasing, 403
  - unimodal, 568
- Sequencing
  - RNA chains, 443
- Sequential search algorithm, 194
- Serial algorithms, 661
- Series
  - geometric, 164
  - harmonic, 321
  - infinite, 167
  - power, 538–541
  - formal, 538
- Set(s), 185
  - Cartesian product of, 123
  - complement of, 128, 129, 186
  - computer representation of, 134
  - countable, 171, 186
  - cut, 806
  - difference of, 128, 186
  - disjoint, 128
  - dominating, 739
  - element of, 185
  - elements of a, 116
  - empty, 118, 185
  - finite, 121, 185, 553, 565
    - combinations of, 437–438
    - counting of subsets, 388
    - number of subsets of, 323
    - union of three, number of elements in, 554–556, 566
    - union of two, number of elements in, 553, 565
  - fuzzy, 138
  - guarding, 735
  - image of, 141
  - infinite, 121
  - linearly ordered, 619, 633
  - member of, 185
  - members of a, 116
  - nonregular, 891
  - not recognized by finite-set automata, 885
  - null, 185
  - of complex numbers, 116
  - of irrational numbers, 116
  - of natural numbers, 116
  - of palindromes, 888
  - of rational numbers, 116
  - of real numbers, 116
  - partially ordered, 618, 633
    - antichain in, 637
    - chain in, 637
    - comparable elements in, 619, 633
    - dense, 632
    - dual of, 630
    - greatest element of, 625, 634
    - Hasse diagram of, 622–624, 634
    - incomparable elements in, 619, 622, 633
    - least element of, 625, 634
    - lower bound of, 625, 634
    - maximal element of, 624, 634
    - minimal element of, 624, 625, 634
    - upper bound of, 625, 634
    - well-founded, 632
  - partition of, 612–613, 633
  - power, 121, 185
  - proofs of facts about, by mathematical induction, 321
  - recognized by Turing machines, 891–892
  - recursively defined, 349–356, 378
  - regular, 878, 879, 884, 899
  - relation on, 575–576
  - relation on, 124
  - representing with a bit string, 134
  - separating, 684
  - singleton, 118
  - successor of, 137
  - symmetric difference of, 186
  - totally ordered, 619, 633
  - uncountable, 186
  - union of, 127, 185
  - universal, 118, 185
  - well-ordered, 381, 620, 633
- Set builder notation, 116, 185
- Set description
  - by listing its members, 116
  - by the roster method, 116
  - using set builder notation, 116
- Set equality, 117, 185
- Set identities, 129–132
  - absorption laws, 129
  - associative laws for, 129
  - Cartesian product of, 123
  - commutative laws for, 129
  - De Morgan’s laws for, 129
  - difference of, 128, 186
  - distributive laws for, 129
  - domination laws for, 129
  - idempotent laws for, 129
  - identity laws for, 129
  - intersection of, 127, 185
- Set of real numbers
  - cardinality of, 186
  - uncountability of, 173
- Set operations, 127
- Sex, 458
- Shamir, Adi, 299, 300
- Shannon, Claude, 20
- Shannon, Claude Elwood, 811, 812
- Sheffer, Henry Maurice, 34
- Sheffer stroke, 34, 36
- Shift cipher, 295, 306
  - cryptanalysis, 296
- Shift ciphers
  - cryptosystem, 298
- Shifting, 252
- Shifting index of summation, 164
- Shift register, 846
- Shortest-path algorithm, 709–714
- Shortest-path problems, 707–716, 736
- Showing two sets are equal, 121
- Sibling of vertex, 747, 803
- Sides of a polygon, 338
- Sieve of Eratosthenes, 259, 306, 560, 565
- Signature
  - digital, 306
- Signatures
  - digital, 303
- Signed integer, 855
- Simple circuit, 679
- Simple directed graph, 643
- Simple graphs, 642, 654–658, 735
  - coloring of, 727
  - connected planar, 719–723
  - crossing number of, 726
  - dense, 670
  - edges of, 642, 663
  - isomorphic, 671–675, 736
  - orientation of, 740
  - paths in, 679
  - random, 742
  - self-complementary, 677
  - sparse, 670
  - thickness of, 726
  - vertices of, 642, 663
  - with spanning trees, 785–787

Simple polygon, 338  
    triangulation of, 338  
Simplification (rule of inference), 71  
Single-elimination tournament, 649  
Single error in an identification number, 291  
Singleton set, 118  
Sink, 901  
*Six Degrees of Separation* (Guare), 680  
Slackness of a job, 235  
Sloane  
    Neil, 162  
Sloane, Neil, 163  
Smullyan, Raymond, 19, 20  
Snakes, poisonous, 763  
*Sneakers*, 300  
Soccer players, 475  
Social networks, 644  
Socks, 405  
Software  
    origin of term, 11  
Software systems, 17  
Sollin's algorithm, 803  
Solution  
    optimal, 198  
Solution of a recurrence relation, 158  
Solvable problem, 232, 895, 900  
Solvable problems, 226  
Solving linear congruences, 277  
Solving satisfiability problems, 34  
Solving Sudoku puzzles, 32  
Solving systems of linear congruences, 277–279  
    by back substitution, 279  
Solving using generating functions  
    counting problems, 541–546  
    recurrence relations, 546–548  
Sort  
    binary insertion, 203  
    binary insertion sort, 196  
    bubble, 196, 232  
        bidirectional, 233  
    insertion, 196, 197, 232  
        average-case complexity of, 483–484  
    library, 196  
    Merge, 196  
    merge, 367–370, 378, 528  
        complexity of, 532  
        recursive, 368  
    quick, 196, 371  
    selection, 196, 203  
    tournament, 196, 770  
Sorting, 196–198, 232  
Sorting algorithms, 196, 198  
    topological, 627–629, 634  
Space, sample, 446  
Space Complexity, 232  
Space complexity, 219  
Space probe, 476  
Spam, 472–475  
Spam filters, Bayesian, 472–475  
Spanning forest, 796  
    minimum, 802  
Spanning trees, 785–795, 804  
    building  
        by breadth-first search, 789–791  
        by depth-first search, 787–789  
    definition of, 785  
    degree-constrained, 806  
    distance between, 797  
    in IP multicasting, 786  
    maximum, 802  
    minimum, 797–802, 804  
    rooted, 797  
Sparse graphs, 670, 802

Sparse matrix, 670  
Specification  
    of a Turing machine, 889  
Specifications  
    system, 17  
Specifying  
    algorithms, 192  
Spiders, Web, 794  
Spies, 112  
SQL, 588–589, 855  
Square  
    perfect, 83  
Squarefree integer, 564  
Square Matrix  
    diagonal of, 181  
    inverse of, 184  
Square zero-one matrix  
    Boolean power of, 183  
St. Petersburg Paradox, 497  
Stable assignment, 343  
Stable matching, 204  
Stable matching problem  
    variations on, 234  
Standard deck, 402  
Standard deviation, 487  
Star Height, 901  
Star topology for local area network, 661  
Start symbol, 849  
State  
    accepting  
        finite-state automaton, 867  
    final  
        finite-state automaton, 867  
    initial, 859  
        finite-state automaton, 867  
    reachable, 901  
    transient, 901  
State diagram  
    for finite-state machine, 860  
Strategy  
    proof, 102  
Statement  
    conditional, XX  
    biconditional, 9  
Statement(s), A-11  
    **if then**, 6  
    **procedure**, A-11  
    assignment, A-11–A-12  
    blocks of, A-14–A-15  
    conditional, 6–9  
    for program correctness, 373–375  
Statement, **return**, A-15  
Statements  
    logically equivalent, 45  
Statement variables, 2  
States, 859  
State table  
    for finite-state machine, 860  
Stephen Cook, 227  
Steroids, 475  
Stirling's formula, 151  
Stirling, James, 151  
Stirling numbers of the first kind, 431  
    signless, 443  
Stirling numbers of the second kind, 430  
Strategies  
    minmax, 767, 804  
    proof(, 100, 106  
Strategy  
    proof, 85  
Strictly decreasing function, 143  
Strictly decreasing sequence, 403  
Strictly increasing function, 143

Strictly increasing sequence, 403  
String, 186  
    bit, 110  
    empty, 186, 849  
    null, 849  
    recognized  
        by Turing machine, 891  
String(s)  
    bit, 12  
String matching, 231  
Strings, 157  
    concatenation, 866  
    concatenation of, 350  
    counting, 388  
        without consecutive 0s, 505  
    decoding, 762–763  
    distinguishable, 888  
    generating next largest, 437  
    indistinguishable, 888  
    length of, 505  
        recursive definition of, 350  
    lexicographic ordering of, 620  
    of parentheses, balanced, 382  
    recognized (accepted), 868  
    recursively defined, 349  
    ternary, 511  
Stroke  
    Sheffer, 34  
Stroke, Sheffer, 36  
Strong induction, 333–335, 378  
Strongly connected components of graphs, 686, 736  
Strongly connected graphs, 685  
Strong pseudoprime, 286  
Structural induction, 353–356, 378  
    proof by, 353  
Structured query language, 588–589  
Structures, recursively defined, 349–356  
Stuarts, 151  
Subgraph, 663, 739  
Subsequence, 403  
Subset, 119, 185  
    proper, 185  
Subsets  
    of finite set counting, 388  
    number of, 323  
    sums of, 793  
Subtraction rule, 393  
Subtractors  
    full, 828  
    half, 828  
Subtree, 746, 748, 803  
Success, 458  
Successor  
    of integer, A-5  
Successor of a set, 137  
Sudoku  
    modeling as a satisfiability problem, 32  
Sudoku puzzle, 32  
Sufficient  
    necessary and, 9  
Sufficient condition, 6  
    expressing a conditional statement using, 6  
Sufficient for, 6  
Suitees, 204  
Suitors, 204, 343  
    optimal for, 343  
Sum(s)  
    Boolean, 811–812, 821, 843  
    of first *n* positive integers, 315  
    of first n positive integers, 317  
    of geometric progressions, 318–319  
    of subsets, 793  
Sum-of-products expansions, 820–821, 843  
    simplifying, 828–840

- Summation
  - index of, 163
  - lower limit, 163
  - notation, 162, 186
  - shifting index of, 164
  - upper limit, 163
- Summation formulae
  - proving by mathematical induction, 315–318
- Sum of multisets, 138
- Sum of terms of a geometric progression, 164
- Sum rule, 386, 389, 439
- Sun-Tsu, 277
- Superman, 80
- Surjection, 143, 186
- Surjective (onto) function
  - number of, 560–562, 566
- Surjective function, 143
- Switching circuits, hazard-free, 846
- Symbol(s), 849
  - start, 849
  - terminal, 849
- Symbol, Landau, 206
- Symbolic Logic* (Venn), 120
- Symmetric closure of relation, 598, 634
- Symmetric difference
  - of two sets, 186
- Symmetric matrix, 181, 186
- Symmetric relation, 577–578, 633
  - representing
    - using digraphs, 595
    - using matrices, 591–592
- Syntax, 847
- System
  - RSA, 299
- Systems
  - hardware, 17
  - software, 17
- Systems of linear congruence, 277–279
- System specifications, 17, 50
  - consistent, 18
- T-shirts, 395
- Table
  - truth, 4, 109
- Table(s)
  - state
    - for finite-state machine, 860
- Table, circular, 394
- Table membership, 186
- Tao, Terence, 263
- Tape
  - Turing machine, 889
- Tautology, 25, 110
- Tee-shirts, 395
- Telephone call graph, 682
- Telephone calls, 646
- Telephone lines
  - computer network with diagnostic, 642
  - computer network with multiple, 642
  - computer network with multiple one-way, 642
  - computer network with one-way, 643
- Telephone network, 646, 682
- Telephone number, 646
- Telephone numbering plan, 387
- Template for proofs by mathematical induction, 329
- “Ten Most Wanted” numbers, 262
- Terminals, 849
- Terminal vertex, 594, 654
- Terms of a sequence
  - closed formula for, 159
- Ternary search algorithm, 203
- Ternary string, 511
- Test
  - Miller’s, 286
  - primality, 464–465
  - probabilistic primality, 464–465
- Tetromino, 109
- TeX, 208
- The Art of Computer Programming* (Donald Knuth), 196
- THE BOOK, 260
- The Elements*, 260
- The Elements*(Euclid), 267
- The lady or the tiger puzzle, 24
- Theorem(s), 81, 110
  - alternate names for, 81
  - Archimedean property, A-5
  - art gallery, 735
  - Bayes’, 468–475
  - Bézout’s, 269, 306
  - binomial, 415–418, 439
  - Cantor’s, 177
  - Chinese remainder, 277, 306
  - Cook–Levin, 227
  - Dirac’s, 701
  - extended binomial, 540
  - Fermat’s last, 106
  - Fermat’s little, 281, 306
  - four color, 728–731, 737
  - fundamental, theorem of arithmetic, 258, 336–337
  - Green–Tao, 263
  - Hall’s marriage, 659
  - handshaking, 653
  - Jordan curve, 338
  - Kleene’s, 880, 900
  - Kuratowski’s, 724–725, 737
  - Lamé’s, 347
  - master, 532
  - methods of proof, 82
  - multinomial, 434
  - Ore’s, 701, 707
  - Pick’s, 342
  - prime number, 262
  - proving, automated, 114
  - Schröder–Bernstein, 174
  - Wilson’s, 285
- Theory, naive set, 118
- Theory, Ramsey, 404
- Thesis, Church–Turing, 893
- Thickness of a graph, 726
- Threshold function, 845
- Threshold gate, 845
- Threshold value, 845
- Thue, Axel, 849
- Tic-tac-toe, 766
- Tiger, 24
- Tiling(s), 103
- Tiling of checkerboard, 326
- Time complexity, 219, 232
  - average-case time, 232
  - average case, 220
  - of algorithm for finding maximum, 219
  - of linear search algorithm, 220
  - worst case, 220, 232
- Tooth fairy, 112
- Top-down parsing, 853
- Topological sorting, 627–629, 634
- Topology for local area network
  - hybrid, 661
  - ring, 661
  - star, 661
- Torus, 726
- Total expectation, law of, 492
- Total function, 152
- Totally ordered set, 619, 633
- Total ordering, 619, 633
  - compatible, 628, 634
- Tournament, 741
  - round-robin, 468, 649
  - single-elimination, 649
- Tournament sort, 196, 770
- Tower of Hanoi, 503–504
- Trace of recursive algorithm, 361, 362
- Tractable problem(s), 226, 232, 897
- Trail, 679
- Transducer(s)
  - finite-state, 859
- Transformation
  - affine, 296
- Transformations, 139
- Transient state, 901
- Transition function, 859
  - extended, 867
  - extending, 867
  - extension, 867
- Transition rule(s)
  - Turing machine, 889
- Transitive closure of relation, 597, 600–603, 634
  - computing, 603–606
- Transitive relation, 578–580, 633
  - representing, using digraphs, 596
- Transitivity law, A-2
- Translating
  - English sentences to logical expressions, 16–17, 62–63
  - mathematical statements to logical expressions, 60, 61
  - nested quantifiers into English, 61–62
  - logical statements into English, 61–62
- Transpose of a matrix, 181, 186
- Transposition cipher, 297
  - decryption, 297
  - encryption, 297
- Transposition error, 291
- “Traveler’s Dodecahedron,”, 698, 700
- Traveling salesperson problem, 702, 709, 714–716, 736
- Traversal of tree, 772–782, 804
  - inorder, 773, 775, 778, 804
  - level-order, 806
  - postorder, 773, 776–778, 804
  - preorder, 773–775, 778, 804
- Tree
  - derivation, 899
  - parse, 899
- Tree(s), 745–802
  - m*-ary, 748, 804
    - complete, 756
    - height of, 754–755
  - applications of, 757–769
  - as models, 749–752
  - AVL, 808
  - binary, 352–353, 748, 749
    - extended, 352
    - full, 352–353
  - binary search, 757–759, 804
  - binomial, 805
  - caterpillar, 807
  - decision, 760–762, 804
  - definition of, 746
  - derivation, 852–854
  - extended binary, 352
  - family, 745
  - full *m*-ary, 748, 752, 804
  - full binary, 352
  - game, 764–769
  - graceful, 807
  - height-balanced, 808
  - labeled, 756
  - mesh of, 809

- Tree(s)—*Cont.*  
parse, 852  
properties of, 752–755  
quad, 809  
rooted, 351, 747–749  
     $S_k$ -tree, 806  
    B-tree of degree  $k$ , 805  
    balanced, 753, 804  
    binomial, 805  
    decision trees, 760–762  
    definition of, 803  
    height of, 753, 804  
    level order of vertices of, 806  
    ordered, 749, 804, 806  
    rooted Fibonacci, 757  
    spanning, 785–795, 804  
        definition of, 785  
        degree-constrained, 806  
        distance between, 797  
        in IP multicasting, 786  
        maximum, 802  
        minimum, 797–802, 804  
        rooted, 797  
Tree-connected network, 751–752  
Tree-connected parallel processors, 751–752  
Tree diagrams, 394–395, 439  
Tree edges, 788  
Tree traversal, 772–782, 804  
    inorder, 773, 775, 778, 804  
    postorder, 773, 776–778, 804  
    preorder, 773–775, 778, 804  
Trial division, 258  
Triangle inequality, 108  
Triangle, Pascal’s, 419, 439  
Triangulation, 338  
Trichotomy Law, A-2  
Tricks, magic, 20  
Triomino(es), 105, 326, 333  
    Right, 105, 333  
    straight, 105  
Trivial proof, 84, 110  
True negative, 471  
True positive, 471  
Truth set  
    of a predicate, 125  
Truth table(s), 4, 109  
    for biconditional statements, 9  
    for conditional statement, 6  
    for conjunction, 4  
    for disjunction, 4  
    for exclusive or, 6  
    for logical equivalences, 27  
    for negation, 4  
    for XOR, 6  
    of compound propositions, 10  
Truth value, 3, 109  
    of implication, 6  
Tukey, John Wilder, 11  
    coining words, 11  
Turing, Alan Mathison, 226, 886  
Turing Award, 854  
Turing machine, 847, 886, 888, 889, 893, 899  
    computing functions with, 892–893  
    control unit, 889  
    definition of, 889  
    final state, 891  
    halts, 891  
    in computational complexity, 894  
    initial position, 889  
    initial state, 889  
    nondeterministic, 893, 899  
    recognition of nonregular set, 891  
    sets recognized by, 891, 892  
        specification, 889  
        string recognition by, 891  
        tape, 889  
        transition rules, 889  
        types of, 893  
Twin prime conjecture, 264  
Twin primes, 264  
Two’s complement representations, 256  
Two-dimensional array, 662–663  
Two children problem, 498  
Type, 117  
Type 0 grammar, 851, 899  
Type 1 grammar, 851, 899  
Type 2 grammar, 851, 899  
Type 3 grammar, 851, 883, 899  
  
U. S. Coast Survey, 38  
Ulam’s problem, 536  
Ulam, Stanislaw, 536  
Ulam numbers, 188  
Unary representations, 892  
Uncomputable function, 175, 186, 896, 900  
Uncountability  
    set of real numbers, 173  
Uncountable set, 186  
Undecidable problem, 895  
Undefined values  
    of partial function, 152  
Underlying undirected graph, 654, 736  
Undirected edges, 644, 735  
    of simple graph, 643  
Undirected graphs, 644, 653, 735  
    connectedness in, 681–685  
    Euler circuit of, 694  
    Euler path of, 698  
    orientation of, 740  
    paths in, 679, 736  
    underlying, 654, 736  
Unicasting, 786  
Unicorns, 112  
Unicycle, 812  
Uniform distribution, 454, 494  
Unimodal sequence, 568  
Union  
    of graphs, 664  
    of three finite sets, number of elements in,  
        554–556, 566  
    of two finite sets, number of elements in, 553, 565  
Union of  
    fuzzy sets, 138  
Union of a collection of sets, 133  
Union of multisets, 138  
Union of sets, 127, 185  
Uniqueness proof, 110  
Uniqueness quantifier, 44  
Uniqueness  
    proof, 99  
Unit (Egyptian) fraction, 380  
Unit-delay machine, 861–862  
unit-delay machine, 861  
United States Coast Survey, 38  
Unit property, in Boolean algebra, 815  
UNIVAC, 872  
Universal quantification, 110  
Universal address system, 772–773  
Universal generalization, 76  
Universal instantiation, 75  
Universal modus ponens, 77  
Universal modus tollens, 77  
Universal product code (UPC), 290  
Universal quantification, 40  
Universal quantifier, 40  
Universal set, 118, 185  
  
Universe of discourse, 40, 110  
Unlabeled  
    boxes, 428  
    objects, 428  
Unless, 6  
    expressing conditional statement using, 7  
Unsatisfiable compound proposition, 30  
Unsolvable problem, 232, 895, 900  
Unsolvable problems, 226  
UPC check digit, 290  
Upper bound, A-2  
    of lattice, 637  
    of poset, 625, 634  
Upper limit of a summation, 163  
Upper triangular matrix, 231  
Utilities-and-houses problem, 718  
Uzbekistan, 192  
  
Vacuous proof, 84, 110  
Valid argument, 69, 110  
Valid argument form, 70, 110  
Valid partner, 234  
Value  
    truth, 3, 109  
Value(s)  
    expected, 477–480, 491, 494  
        in hatcheck problem, 495  
        linearity of, 477–484, 494  
        of inversions in permutation, 482–484  
    final, A-14  
    initial, A-14  
    of tree, 767  
    of vertex in game tree, 767–769, 804  
    threshold, 845  
Vandermonde’s identity, 420–421  
Vandermonde, Alexandre-Théophile, 420  
Variable(s)  
    Boolean, 11, 110, 814, 820, 843  
    bound, 44, 110  
    free, 44, 110  
    propositional, 2, 109  
    random, 454, 460–461  
        covariance of, 494  
        definition of, 494  
        distribution of, 460, 494  
        expected values of geometric, 477–480  
        geometric, 484–485  
        geometric expected values of, 491, 494  
        independent, 485–487, 494  
        indicator, 492  
        standard deviation of, 487  
        variance of, 477–480, 494  
    statement, 2  
Variance, 477, 487–490, 494  
Veitch, E. W., 830  
Vending machine, 858–859  
Venn, John, 118, 120  
Venn diagrams, 118, 185  
Verb, 848  
Verb phrase, 848  
Vertex (vertices), 594  
    adjacent, 651, 654, 735  
    ancestor of, 747, 803  
    basis, 691  
    child of, 747, 749, 803  
    connecting, 651  
    connectivity, 684  
    counting paths between, 688–689  
    cut, 683, 684  
    degree of, 652  
    degree of, in undirected graph, 652  
    descendant of, 747, 804  
    distance between, 741  
    eccentricity of, 757  
    end, 654

- Vertex (vertices)—*Cont.*  
in-degree of, 654, 736  
independent set of, 741  
initial, 594, 654  
interior, 603  
intemal, 748, 804  
isolated, 652, 736  
level of, 753, 804  
level order of, 806  
number of, of full binary tree, 355  
of directed graph, 643, 654  
of directed multigraph, 644  
of multigraph, 642  
of polygon, 338  
of pseudograph, 643  
of simple graph, 642, 668  
of undirected graph, 644, 652, 654  
out-degree of, 654, 736  
parent of, 747, 803  
pendant, 652, 736  
sibling of, 747, 803  
terminal, 594, 654  
value of, in game tree, 767–769, 804
- Vertex set, 338  
bipartition of, 656
- Very large scale integration (VLSI) graphs, 744
- Vigenère cipher, 304  
cryptanalysis, 305
- Vocabulary, 849, 899
- “Voyage Around the World” Puzzle, 700
- Walk, 679  
closed, 679
- Wall Street*, 198
- Warshall’s algorithm, 603–606
- Warshall, Stephen, 603, 604
- WAVES, Navy, 872
- Weakly connected graphs, 686
- Web crawlers, 646
- Web graph, 646–647, 794  
strongly connected components of, 686
- Web page(s), 646, 686, 794  
searching, 18
- Web spiders, 794
- Weighted graphs, 736  
minimum spanning tree for, 798–802  
shortest path between, 707–714  
traveling salesperson problem with, 714–716
- Well-formed expressions, 354
- Well-formed formula, 350  
for compound propositions, 354  
in prefix notation, 784  
of operators and operands, 351  
structural induction and, 354
- Well-founded induction, principle of, 635
- Well-founded poset, 632
- Well-ordered induction, 634  
principle of, 620
- Well-ordered set, 381, 620, 633
- Well-ordering property, 340–341, 378, A-5
- WFF’N PROOF, The Game of Modern Logic* (Allen), 80, 114
- Wheels, 655, 736
- Wiles, Andrew, 107
- Williamson, Malcolm, 302
- Wilson’s theorem, 285
- Winning strategy  
for chomp, 98
- Without loss of Generality (WLOG), 95, 110
- Witness(es)  
to big-*O* relationship, 205, 232  
to an existence proof, 96
- Witnesses to a big-*O* relationship, 232
- WLOG (without loss of generality), 95
- Word, 849
- Word and Object* (Quine), 839
- World’s record, for twin primes, 264
- World Cup soccer tournament, 415
- World population, 168
- World Wide Web graph, 646–647
- Worst-case complexity  
insertion sort, 222  
of binary search, 220  
of bubble sort, 221
- Worst-case time complexity, 232
- Worst case  
time complexity, 220
- XML, 855, 858
- XOR, 110
- Yahoo, 794
- Yes-or-no problems, 894
- Zebra puzzle, 24
- Zermelo–Fraenel axioms, 176
- Zero–one matrices  
Boolean product of, 182  
join of, 181  
meet of, 181  
of transitive closure, 602–603  
representing relations using, 591–594
- Zero–one matrix, 181
- Zero–one matrix, 186
- Zero property, in Boolean algebra, 815
- Ziegler’s Giant Bar, 208
- Zodiac, signs of, 441