



A revised version of this material has been / will be published by Cambridge University Press as *Connecting Discrete Mathematics and Computer Science* by David Liben-Nowell, and an older edition of the material was published by John Wiley & Sons, Inc as *Discrete Mathematics for Computer Science*. This pre-publication version is free to view and download for personal use only. Not for re-distribution, re-sale, or use in derivative works. © David Liben-Nowell 2020–2021. This version was posted on April 5, 2021.

12

Index

- 2–3 and 2–3–4 trees, 545
- 9/11 Memorial, 1124
- 123456791, 752
- 987654263, 752

- \forall (universal quantifier), 333 ff.
- absolute value, 205, 427, 429
- abstract algebra, 736
- adjacency, *see* graphs
- Adleman, Leonard, 747
- affirming the consequent, *see* fallacy
- algorithms, 265 ff., *see also* randomized algorithms
 - asymptotic analysis, 617 ff.
 - brute force, 326, 515, 902, 959
 - divide and conquer, 647 ff., 655
 - dynamic programming, 515, 902, 959
 - greedy algorithms, 422, 918
 - recurrence relations, 633 ff.
 - time, space, and power, 626
- Alice and Bob, 745 ff.
- ambiguity
 - in natural language, 308, 309, 314
 - order of operations, 543, 805
 - order of quantification, 351 ff., 360
 - prefix-free/ Huffman codes, 918
- analysis (mathematics), 836
- antisymmetry, 820 ff.
- approximate equality, 205
- Ariane 5 rocket, 464
- arithmetic mean, 439, 456
- arithmetic series, 512
- Arrow’s Theorem, 823
- artificial intelligence
 - computer vision, 1132
 - game trees, 344, 941
- assertions, 360, 517
- associativity, 321, 545, 736
- assuming the antecedent, *see* proofs
- asymmetry, 820 ff.
- asymptotics
 - analysis of algorithms, 617 ff.
 - asymptotic analysis, 603 ff.
 - asymptotic relationships viewed as relations, 823 ff.
 - best- and average-case running time, 623 ff.
 - master method, 648 ff.
 - O (Big O), 604 ff.
 - o , Ω , ω , and Θ , 608 ff.
 - polynomials, logs, and exponentials, 606 ff.
 - recurrence relations, 633 ff.
 - worst-case analysis, 618 ff.
- automata, 846, 942
- automated theorem proving, 424
- average distance in a graph, 1145
- average-case analysis, *see* running time
- AVL trees, 643 ff.
- axiom of extensionality, 229

- Bacon, Kevin, 438, 1117
- balanced binary search trees, 643
- Bayes’ Rule, 1033 ff.
- begging the question, *see* fallacy
- Bernoulli distribution, 1013 ff., 1044, 1057
- betweenness, 812
- BFS, *see* breadth-first search
- biased coins, 1014 ff.

- big O , big Ω , and big Θ , 604 ff., 823 ff.
- bigrams, 1036
- bijections, 262, 928, 937
- binary numbers, *see* integers
- binary relation, *see* relations
- Binary Search, *see* searching
- binary search trees, *see* trees
- binary symmetric channel, 1033, 1034
- binary trees, *see* trees
- binomial coefficients, *see* combinations
- binomial distribution, 1014 ff., 1049
- Binomial Theorem, 954 ff.
- bipartite graphs, 1118 ff.
 - complete bipartite graphs, 1119
- birthday paradox, 526, 1052
- bitmaps, 243
- bits/ bitstrings, 203, 240
- Bletchley Park, 960
- Bloom filters, 1039
- Booleans, 203, 305, *see also* logic
- bound (vs. free) variables, 336
- breadth-first search, 1136 ff.
 - finding cycles, 1149
- brute force, *see* algorithms
- Bubble Sort, *see* sorting
- Buffon’s needle, 1062
- bugs, 217, 464, 517, 1129

- C (programming language), 327, 345, 534
- Caesar Cipher, *see* cryptography
- cardinality, 222–223, 903 ff.
 - infinite, 937
- Carmichael numbers, 741, 742, 744
- Cartesian product (\times), 237
- catchphrase, 1165

- Cauchy sequences, 836
- ceiling, 206
- cellular automata, 942
- Chain Rule (probability), 1031 ff.
- checkers, 344, 437, 925
- checksum, 403
- chess, 237, 344, 518–519, 913, 924, 1135
- Chinese Remainder Theorem, 725 ff.
- circle packing, 416
- circuits
 - printing and planar graphs, 1121
 - representing logical propositions, 322, 329
 - using nand gates, 445
- class-size paradox, 1045
- cliques, 1117 ff.
- closure, 736, 825 ff.
- clustering, 234
- coarsening equivalence relations, 836 ff.
- codomain (of a function), 255
- collaboration networks, 1117
- collaborative filtering, 236
- combinations, 945 ff.
 - k -combinations, 948 ff.
 - Binomial Theorem, 954 ff.
 - Pascal's identity, 953, 957
 - Pascal's Triangle, 957
- combinatorial proof, 951 ff.
- commutativity, 246, 321, 352, 545, 736
- comparability, *see* partial orders
- comparison-based sorting, *see* sorting
- compilers, 327, 543
- complement (of a set), 226
- complete graphs, 1117 ff.
- complexity, *see* computational complexity
- composite numbers, *see* prime numbers
- composition
 - of functions, 258, 811
 - of relations, 807, 823
- compression
 - entropy and compressibility, 1017
 - Huffman coding, 918
 - impossibility of lossless compression, 938
 - lossy vs. lossless, 938
 - quantization of images, 254, 268
 - URL shortening, 907
- computability, 449
- computational biology
 - genome rearrangements, 359, 942
 - motifs in gene networks, 1116
- computational complexity
 - and cryptography, 752
 - complexity classes, 628
 - graph isomorphism, 1115
 - input size, 706
 - P vs. NP, 326
 - regular languages, 830, 846
- computational geometry, 251
- computational linguistics, *see* natural language processing
- computer architecture, 322 ff., 445
 - and running times, 618
 - Moore's Law, 613
 - power consumption, 626
 - representation of numbers, 217
- computer graphics
 - hidden-surface removal, 847
 - morphing, 252
 - rotation matrices, 249
 - triangulation, 528
- computer security, 752, 753
- computer vision, 1132
- computing networking, 919
- conditional expectation, 1055 ff.
- conditional probability, 1027 ff.
 - Bayes' Rule, 1033
 - Chain Rule, 1031
 - Law of Total Probability, 1032
- Condorcet paradox, 823
- congruences (modular), 707 ff., 726 ff., 835
- conjunctive normal form, 323 ff., 441 ff., 540 ff.
- connectivity (in graphs), 1130 ff.
 - connected component, 1131 ff.
 - reachability, 1133 ff.
- constructive proofs, 432
- constructivism, 433
- context-free grammar, 543
- contradiction, 318
- contrapositive, 320, 428, *see also* proofs
- converse, 320
- Cook–Levin Theorem, 326
- correlation, 1021
 - correlation vs. causation, 463
 - positive and negative, 1024
- countable sets, 937
- counterexamples, 432 ff.
- counting
 - Binomial Theorem, 954 ff.
 - combinations, 945 ff.
 - combinatorial proofs, 951 ff.
 - combining products and sums, 915 ff.
 - Division Rule, 931 ff.
 - double counting, 909 ff.
 - Generalized Product Rule, 913 ff.
 - inclusion–exclusion, 909 ff.
 - for 3+ sets, 911
 - Mapping Rule, 927 ff.
 - order, 946 ff.
 - Pascal's Triangle, 957 ff.
 - permutations, 947 ff.
 - Pigeonhole Principle, 935 ff.
 - Product Rule (sequences), 906
 - repetition, 946 ff.
 - Sum Rule (unions), 903
- Counting Sort, *see* sorting
- coupon collector problem, 1064
- crossword puzzles, 358
- cryptography, 745 ff.
 - and pseudorandomness, 1013
 - Caesar Cipher, 746, 1038
 - Diffie–Hellman key exchange, 753
 - digital signatures, 748
 - Enigma Machine and WWII, 960
 - frequency analysis, 1025, 1038
 - key exchange, 753
 - man-in-the-middle attack, 753
 - one-time pads, 745
 - public-key cryptography, 746 ff.
 - RSA cryptosystem, 454, 747 ff.
 - secret sharing, 730
 - substitution cipher, 1024, 1031, 1038
- Currying, 357
- cycles, 840, 1147 ff.
 - acyclic graphs, 1149 ff.
 - cycle elimination algorithm, 1158
 - cycle rule for minimum spanning trees, 1170
 - kidney transplants, 1159
 - simple cycles, 1148
 - weighted cycle elimination algorithm, 1170
- DAG (directed acyclic graph), 1150
- data mining, *see* machine learning
- data visualization, 1110
- databases, 347, 815, 817

- De Morgan's Laws, 322
 decision problems, 448
 Deep Blue, 344
 degree (in a graph), 1107 ff., 1109
 degree distribution, 1123
 regular graphs, 1119
 degree (of a polynomial), 264
 density (of a graph), 615, 1127
 denying the hypothesis, *see* fallacy
 dependent events, 1021 ff.
 depth-first search, 1140 ff.
 Descartes, René, 239
 deterministic finite automata, 846
 DFS, *see* depth-first search
 diagonalization, 937
 diameter, 1144
 Diffie–Hellman key exchange, 753
 Dijkstra's algorithm, 1165 ff.
 directed graphs, 818
 disconnected, *see* connectivity in graphs
 disjoint sets, 230, 416
 disjunctive normal form, 323 ff., 441 ff., 540 ff.
 distance, *see also* metrics
 Euclidean, *see* Euclidean distance
 Hamming, *see* Hamming distance in a graph, 1135 ff.
 Manhattan, *see* Manhattan distance
 minimum distance of a code, 407 ff.
 divide and conquer, *see* algorithms
 divisibility, 210, 516, 841
 and modular arithmetic, 708 ff.
 common divisors, 709 ff.
 divisibility rules, 316, 425, 716
 Division Theorem, 703
 division, *see* mod
 in \mathbb{Z}_n , 735
 Division Rule, 931 ff.
 domain (of a function), 255
 dot product, 241 ff.
 Dunbar's number, 1125
 dynamic programming, *see* algorithms
 dynamic scope, 345

 \exists (existential quantifier), 333 ff.
 e (base of natural logarithm), 209
 edges, *see* graphs
 efficiency, *see* running time, *see also* computational complexity
 empty set, 226
 Enigma Machine, 960
 entropy, 1017
 equivalence relations, 833 ff.
 equivalence classes, 834
 refinements and coarsenings, 836
 Eratosthenes, 718, 732
 Erdős numbers, 438
 Erdős, Paul, 438, 1117
 error-correcting codes, 405 ff.
 Golay code, 422
 Hamming code, 412 ff., 926
 messages and codewords, 405 ff.
 minimum distance and rate, 407 ff.
 Reed–Solomon codes, 418, 731
 repetition code, 410 ff.
 upper bounds on rates, 415
 error-detecting codes, 405 ff.
 credit card numbers, 403, 419
 UPC, 940
 Euclid, 446, 447, 710
 Euclidean algorithm, 710, 722
 efficiency, 713, 716
 Extended Euclidean algorithm, 722
 Euclidean distance, 250, 456
 Euler's Theorem, 744
 Euler, Leonhard, 440, 744
 even numbers, 430
 evenly divides, *see* divisibility
 events (probability), 1007 ff.
 correlated, 1021
 independent events, 1021 ff.
 exclusive or (\oplus), 211, 308 ff.
 existential quantifier (\exists), 333 ff.
 expectation, 1044 ff.
 average-case analysis of algorithms, 624 ff.
 conditional expectation, 1055 ff.
 coupon collector problem, 1064
 deviation from expectation, 1056 ff.
 Markov's inequality, 1065
 Law of Total Expectation, 1056
 linearity of expectation, 1048 ff.
 exponentials, 206 ff., 545
 asymptotics, 606 ff.
 modular, 716
 EXPSPACE (complexity class), 628
 EXPTIME (complexity class), 628
 Extended Euclidean algorithm, 722

 Facebook, 1123

 factorial, 423–424, 515–516, 633, 636, 915, 921
 Stirling's approximation, 964
 factors, *see* divisibility, *see also* prime factorization
 fallacy, 458 ff.
 affirming the consequent, 460
 begging the question, 462
 denying the hypothesis, 461
 false dichotomy, 427, 461
 proving true, 460
 false dichotomy, *see* fallacy
 fencepost error, 1129
 Fermat pseudoprime, 741
 Fermat's Last Theorem, 739
 Fermat's Little Theorem, 739 ff.
 Fermat–Euler Theorem, 744
 Fibonacci numbers, 252, 530, 634, 640–642, 644, 963
 algorithms, 646
 and the Euclidean algorithm, 716
 filter, 233
 finite-state machines, 846
 float (floating point number), 217, 618
 floor, 206
 Division Theorem, 703
 forests, 1150
 spanning forests, 1157
 formal language theory, *see* computational complexity
 formal methods, 424, 825
 Four Color Theorem, 437, 1121
 fractals, 502, 508–510, 519–520, 532
 free (vs. bound) variables, 336
 frequency analysis, 1025
 functions, 253 ff.
 algorithms, 265 ff.
 characteristic function of a set, 806
 composition, 258
 domain/codomain, 255
 growth rates, 603 ff.
 inverses, 262
 one-to-one/onto functions, 259 ff.
 range/image, 256 ff.
 viewed as relations, 810 ff.
 visual representation, 258
 vs. macros, 345
 Fundamental Theorem of Arithmetic, 720

 Gödel's Incompleteness Theorem, 346

- Gödel, Kurt, 346
game trees, 344, 941
garbage collection, 627, 1143
Gates, Bill, 359, 438, 1006
GCD, *see* greatest common divisor
GCHQ, 747
Generalized Product Rule, 913 ff.
geometric distribution, 1015 ff., 1048
geometric mean, 439, 456
geometric series, 510 ff.
 infinite, 512
 master method, 648 ff.
giant component, 1142
Goldbach's conjecture, 303, 350, 360
golden ratio, 641
Google, 1174
grammars, 535, 543
graph drawing, 1121, 1124
graphs, 1103 ff.
 acyclic graphs, 1149 ff.
 adjacency lists, 1110 ff.
 adjacency matrices, 1111 ff.
 bipartite graphs, 1118 ff.
 breadth-first search, 1136 ff.
 complete graphs, 1117 ff.
 connected components, 1131 ff.
 connectivity, 1130 ff.
 cycles, 1147 ff.
 data structures, 1110 ff.
 degree, 1107, 1109 ff.
 Handshaking Lemma, 1108
 regular graphs, 1119
 density, 1127
 depth-first search, 1140 ff.
 forests, 1150
 isomorphism, 1114 ff.
 matchings, 934, 942, 960, 1120, 1159
 neighborhoods, 1106 ff., 1109 ff.
 paths, 1129 ff.
 shortest paths, 1135 ff.
 planar graphs, 1121 ff.
 shortest paths
 Dijkstra's algorithm, 1165 ff.
 simple graphs, 1104
 subgraphs, 1115 ff.
 trees, *see* trees
 undirected vs. directed, 1103 ff.
 weighted graphs, 1164 ff.
 Dijkstra's algorithm, 1165 ff.
greatest common divisor, 709 ff., *see also* Euclidean algorithm
 H_n , *see* harmonic number
Halting Problem, 346, 451 ff., 455
Hamiltonian path, 1145
Hamming code, 412 ff.
 number of valid codewords, 926
Hamming distance, 404
Hamming, Richard, 404, 412
Handshaking Lemma, 1108
harmonic number, 512–514
hashing, 267, 942, 1003–1004, 1050, 1064
 Bloom filters, 1039
 collisions, 1003 ff., 1010, 1020, 1039, 1051
 and pairwise independence, 1026
 chaining, 1003
 clustering, 1010, 1020
 double hashing, 1020
 linear probing, 1010, 1020
 quadratic probing, 1020
 simple uniform hashing, 1004
Hasse diagrams, 840
heaps, 269, 529, 544
heavy-tailed distribution, 1123
Heron's method, 218, 439
hidden-surface removal, 847
higher-order functions, 233, 357
Hopper, Grace, 464
Huffman coding, 918
hypercube, 1127
 I (identity matrix), 244
idempotence, 321
identity
 identity function, 263
 identity matrix, 244
 multiplicative identity, 735
 of a binary operator, 315, 545
if and only if (\Leftrightarrow), 308 ff.
image (of a function), 256
image processing
 blur filter, 218
 dithering, 330
 quantization, 254
 segmentation, 1132
imaginary numbers, 207
implication (\Rightarrow), 306 ff.
in-degree, *see* degree
in-neighbor, *see* neighbors (in graphs)
inclusion–exclusion, 909 ff.
incomparability, 610, 838
incompleteness (logic), 346
independent events, 1021 ff.
 pairwise independence, 1026
induction, *see* proofs
 checklist for inductive proofs, 507
 generating conjectures, 508
 proofs about algorithms, 514 ff.
 strengthening the inductive hypothesis, 540
infix notation, 805
information retrieval, 248
information theory, 1017, 1033
injective functions, *see* one-to-one functions
Insertion Sort, *see* sorting
integers, 203 ff.
 algorithms for arithmetic, 705, 715
 efficiency, 706
 division, *see* modular arithmetic
 primes and composites, *see* prime numbers
 recursive definition, 542
 representation
 binary numbers, 316, 506, 520, 530, 706, 714
 different bases, 530, 714
 ints, 217
 modular representation, 729
 unary, 706
 successor relation, 829
internet addresses, 919
intersection (of sets), 227
intervals, *see* real numbers
invalid inference, 458
inverse
 additive, 743
 multiplicative, 735 ff.
 of a function, 262
 of a matrix, 252
 of a relation, 806 ff., 821
 of an implication, 320
IP addresses, 919
irrationals, *see* rationals
 irrationality of $\sqrt{2}$, 431
irreflexivity, 819 ff.
isomorphism (of graphs), 1114 ff.
Jaccard coefficient, 236
Java (programming language), 256, 311, 327, 1143
Johnson's algorithm, 1066

- \mathcal{K}_n , *see* complete graphs
 $\mathcal{K}_{n,n}$, *see* bipartite graphs
 Kasparov, Garry, 344
 keyspace, *see* hashing
 kidney transplants, 1159
 Knuth, Donald, 710
 Kruskal's algorithm, 1171
 Kuratowski's Theorem, 1122
- L (complexity class), 628
 latchstring, 1165
 law of the excluded middle, 317
 Law of Total Expectation, 1056
 Law of Total Probability, 1032
 least common multiple, 709 ff.
 length (of a vector), 241
 lexical scope, 345
 lexicographic ordering, 349, 806
 Liar's Paradox, 225
 linearity of expectation, 1048
 linked lists, 544
 - adjacency lists for graphs, 1110 ff.
 - as graphs, 1125
 - recursive definition, 533
 list, *see* sequence
 little o and little ω , 608 ff., 823 ff.
 logarithms, 208–209
 - asymptotics, 606 ff.
 - discrete logarithm, 753
 - polylogarithmic functions, 615, 706
 logic
 - Boolean logic, 203, 736
 - consistency, 346
 - fuzzy logic, 314
 - incompleteness, 346
 - logical equivalence, 319, 338
 - logical fallacy, *see* fallacy
 - modal logic, 825
 - predicate logic, 331 ff.
 - games against the demon, 354
 - nested quantifiers, 349 ff.
 - order of quantification, 350 ff.
 - predicates, 331 ff.
 - quantifiers, 333 ff.
 - theorems in predicate logic, 337 ff.
 - propositional logic, 303 ff.
 - atomic vs. compound propositions, 304
 - logical connectives, 305 ff.
 - propositions, 303 ff.
- recursive definition of a well-formed formula, 535
 satisfiability, 318
 tautology, 317 ff.
 truth assignment, 311
 truth tables, 311 ff.
 truth values, 303, 535
 universal set of operators, 456
 temporal logic, 825
 longest common subsequence, 515, 964
 loop invariants, 517
- machine learning
 - classification problems, 927, 1037
 - clustering, 234
 - cross-validation, 963
 macros, 345
 Manhattan distance, 241, 250, 456
 map, 233
 Mapping Rule, 927 ff.
 MapReduce, 233
 maps, 437, 1121
 mark-and-sweep, 1143
 Markov's inequality, 1065
 master method, 648 ff.
 matchings, *see* graphs
 matrices, 243 ff.
 - adjacency matrices for graphs, 1111 ff.
 - identity matrix, 244
 - inverse of a matrix, 252
 - matrix multiplication, 245 ff.
 - Strassen's algorithm, 655
 - rotation matrices, 249
 - term–document matrix, 248
 maximal element, 841 ff.
 maximum element, 228, 266, 841 ff.
 mazes, 1140
 median (of an array), 1060 ff.
 memoization, 959
 memory management, 1143
 Merge Sort, *see* sorting
 metrics, 404, 419–420, 1145
 Milgram, Stanley, 438
 Miller–Rabin test, 454, 742
 minimal element, 841 ff.
 minimum element, 228, 841 ff.
 minimum spanning trees, 1170 ff.
 - cycle rule, 1170
 - Kruskal's algorithm, 1171
- weighted cycle elimination algorithm, 1170
 ML (programming language), 357, 539
 modal logic, 825
 modular arithmetic, 209–211, 703 ff.
 - Division Theorem, 703
 - mod-and-div** algorithm, 705 ff., 715
 - modular congruences, 707
 - modular exponentiation, 716
 - modular products, 707
 - modular sums, 707
 - multiplicative inverse, 735 ff.
 - primitive roots, 753
 modus ponens, 317
 modus tollens, 318
 Monte Carlo method, 1062
 Monty Hall Problem, 1012
 Moore's Law, 613
 multiples, *see* divisibility
 multiplicative identity, 735
 multiplicative inverse, 735 ff.
 multitasking, 627
- naïve Bayes classifier, 1037
 nand (not and), 445
 n -ary relations, 812 ff.
 - expressing n -ary relations as binary relations, 813
 natural language processing
 - ambiguity, 314
 - language model, 1036
 - speech processing, 234, 925
 - speech recognition, 1036
 - text classification, 1037
 - text-to-speech systems, 925
 natural logarithm, *see* logarithms
 neighbors (in graphs), 1106, 1109
 nested quantifiers, 349 ff.
 - games against the demon, 354
 - negations, 352
 - order of quantification, 350 ff.
 Newton's method, 218
 nodes, *see* graphs
 nonconstructive proofs, 432
 NP (complexity class), 326, 461, 628
 number theory, *see* modular arithmetic
 numerical methods, *see* scientific computing
- O (Big O), 604 ff., 823 ff.

- o (little o), 608, 823 ff.
- off-by-one error, 1129
- Omega (Ω) (asymptotics), 608, 823 ff.
- omega (ω) (asymptotics), 608, 823 ff.
- one-time pads, 745
- one-to-one functions, 260, 928
- onto functions, 259, 928
- operating systems, 358
 - multitasking, 627
 - virtual memory, 455
- optimizing compilers, 327
- orders, *see* partial orders
- out-degree, *see* degree
- out-neighbor, *see* neighbors (in graphs)
- outcome (probability), 1005
- overfitting, 1036
- overflow, 217, 464

- \mathcal{P} , *see* power set
- P (complexity class), 326, 461, 628
- PageRank, 1174
- Painter's Algorithm, 847
- pairwise independence, 1026
- palindromes, 545, 939
- paradoxes
 - birthday paradox, 1052
 - class-size paradox, 1045
 - Liar's paradox, 225
 - nontransitive dice, 1063
 - paradoxes of translation, 304
 - Russell's paradox, 225
 - Simpson's Paradox, 467
 - voting paradoxes, 823
- parallel edges, 1104
- parity, 211, 412 ff., 522–523, 530
- parsing, 543
- partial orders, 837 ff.
 - chains and antichains, 849
 - comparability, 838
 - extending to a total order, 843 ff.
 - Hasse diagrams, 840
 - immediate successors, 841
 - minimal/ maximal elements, 841
 - minimum/ maximum element, 841
 - strict partial order, 838
 - topological ordering, 843 ff.
 - total orders, 838
 - consistency with a partial order, 843 ff.
- partition (of a set), 231
- bipartite graphs, 1118
 - equivalence relations, 835
- Pascal's identity, 953, 957
- Pascal's Triangle, 957 ff.
- paths (in graphs), 1129 ff.
 - breadth-first search, 1136 ff.
 - connected graphs, 1130 ff.
 - depth-first search, 1140 ff.
 - Dijkstra's algorithm, 1165 ff.
 - internet routing, 919
 - shortest paths, 1135 ff.
 - simple paths, 1130
- Pentium chip, 464, 613
- perfect matchings, *see* graphs
- perfect square, 207
- Perl (programming language), 446
- permutations, 532, 914–915, 921
 - k -permutations, 947 ff.
- Petersen graph, 1115, 1122
- Pigeonhole Principle, 935 ff., 938
- planar graphs, 1121 ff.
 - Kuratowski's Theorem, 1122
- polylogarithmic, 615, 706
- polynomials, 263 ff., 418, *see also* P (complexity class)
 - asymptotics, 606 ff.
 - evaluating modulo a prime, 720, 730, 731
- postfix notation, 805
- Postscript (programming language), 805
- power set, 232
 - as a relation, 804
 - cardinality, 930
- power-law distribution, 1123
- powers, *see* exponentials
- precedence of operators, 227, 310, 336, 543
- predicate logic, *see* logic
- predicates, 331 ff., 806, *see also* logic
- prefix notation, 805
- prefix-free codes, 917
- preorder, 840
- prime numbers, 211, 449, 717 ff.
 - Carmichael numbers, 741, 744
 - distribution of the primes, 718
 - infinitude of primes, 447
 - primality testing, 447, 454, 617, 717
 - efficient algorithms, 742
 - prime factorization, 720, 752
 - cryptography, 454, 752
 - existence of, 523–524
 - Shor's algorithm, 1016
 - uniqueness of, 723–725
- Prime Number Theorem, 718
- Sieve of Eratosthenes, 718, 732
- priority queues, 529
- probability
 - Bayes' Rule, 1033 ff.
 - conditional expectation, 1055 ff.
 - conditional probability, 1027 ff.
 - coupon collector problem, 1064
 - events, 1007 ff.
 - expectation, 1044 ff.
 - infinitesimal probabilities, 1030
 - Law of Total Expectation, 1056
 - Law of Total Probability, 1032
 - linearity of expectation, 1048 ff.
 - Markov's inequality, 1065
 - Monty Hall Problem, 1012
 - outcomes, 1005 ff.
 - probability functions, 1005 ff.
 - random variables, 1041 ff.
 - random walks, 1174
 - standard deviation, 1056 ff.
 - tree diagrams, 1010 ff.
 - variance, 1056 ff.
- probability distributions
 - Bernoulli, 1013 ff.
 - binomial, 1014 ff.
 - entropy, 1017
 - geometric, 1015 ff.
 - posterior distribution, 1034
 - prior distribution, 1034
 - uniform, 1013 ff.
- product, 216 ff.
 - of a set, 228
- product of sums, *see* conjunctive normal form
- Product Rule, 906
 - cardinality of S^k , 908
- programming languages
 - compile-time optimization, 327
 - Currying, 357
 - garbage collection, 627, 1143
 - higher-order functions, 233, 357
 - parsing, 543
 - scoping/ functions/ macros, 345
 - short-circuit evaluation, 327
 - syntactic sugar, 322
- proofs, 423 ff.
 - by assuming the antecedent, 341,

- 426
 by cases, 415, 427 ff.
 by construction, 411, 432 ff.
 by contradiction, 416, 430 ff.
 by contrapositive, 428 ff.
 by induction, 503 ff.
 by mutual implication, 429
 by strong induction, 521 ff.
 by structural induction, 535 ff.
 combinatorial proofs, 951 ff.
 direct, 425 ff.
 nonconstructive, 432
 strategy for proofs, 433 ff.
 unprovable true statements, 346
 “without loss of generality”, 427
 writing proofs, 435 ff.
- proper subset and superset, 229
 propositional logic, *see* logic
 proving true, *see* fallacy
 pseudocode, 265
 pseudorandom generator, 1013
 PSPACE (complexity class), 628
 public-key cryptography, *see* cryptography
 Pythagorean Theorem, 435, 445–446, 456
 incorrect published proof, 468
 Python (programming language), 217, 233, 256, 315, 316, 345, 357, 449 ff., 937, 1143
- Q, *see* rationals
 quadrees, 645
 quantifiers, 333 ff.
 negating quantifiers, 340 ff.
 nested quantifiers, 349 ff.
 vacuous quantification, 342
 quantum computation, 1016
 Quick Sort, *see* sorting
- \mathbb{R} , *see* real numbers
 Radix Sort, *see* sorting
 raising to a power, *see* exponentials
 Random Surfer Model, 1174
 random variables, 1041 ff.
 expectation, 1044 ff.
 independent random variables, 1043
 indicator random variables, 1043
 random walks, 1174, 1176
 randomized algorithms, 626
 Buffon’s needle, 1062
 finding medians, 1060
 Johnson’s algorithm, 1066
 Monte Carlo method, 1062
 primality testing (Miller–Rabin), 742
 Quick Sort, 1018
 range (of a function), 256
 rate (of a code), 407 ff.
 rationals, 203 ff., 238, 426, 429, 710
 in lowest terms, 710, 835
 real numbers, 203 ff.
 absolute value/floor/ceiling, 205 ff.
 approximate equality (\approx), 205, 803
 defining via infinite sequences, 836
 exponentiation, 206 ff.
 floats (representation), 217
 intervals, 205
 logarithms, 208 ff.
 trichotomy, 611
 realization, *see* outcome (probability)
 recommender system, 236
 recurrence relations, 633 ff.
 iterating, 636
 master method, 648 ff.
 sloppiness, 640
 solving by induction, 635
 variable substitution, 637
 recursion tree, 631, 648 ff.
 recursively defined structures, 533 ff.
 Reed–Solomon codes, 418, 731
 reference counting, 1143
 refining equivalence relations, 836 ff.
 reflexivity, 405, 819 ff.
 reflexive closure, 826 ff.
 regular expressions, 830, 846
 regular graphs, 1119
 relational databases, *see* databases
 relations
 n -ary relations, 812 ff.
 binary relations, 804 ff.
 closures, 825 ff.
 composition, 807 ff.
 equivalence relations, 833 ff.
 functions as relations, 810 ff.
 inverses, 806 ff.
 partial orders, 837 ff.
 reflexivity, 819
 relational databases, 815
 symmetry, 820
 total orders, 838 ff.
 transitivity, 822 ff.
 visual representation, 805 ff., 818 ff.
 Hasse diagrams, 840 ff.
 vs. predicates, 806
 relative primality, 720 ff., 737 ff.
 Chinese Remainder Theorem, 725 ff.
 Extended Euclidean algorithm, 722
 remainder, *see* mod
 repeated squaring, 646, 716, 749
 repetition code, 410 ff.
 Rivest, Ron, 747
 roots (of a polynomial), 264, 418, 731
 RSA cryptosystem, 454, 747 ff.
 breaking the encryption, 752
 Rubik’s cube, 736, 922
 running time, 617 ff.
 average case, 624 ff., 1054
 best case, 623 ff.
 worst case, 618 ff.
 Russell’s paradox, 225
 Russell, Bertrand, 225
- sample space (probability), 1005
 sampling bias, 1045
 satisfiability, 318, 326, 450, 803, 1066
 scalars, 240
 SCC, *see* strongly connected components
 Scheme (programming language), 233, 238, 322, 357, 805
 scientific computing, 618
 Newton’s method, 218
 searching
 Binary Search, 517, 532, 622 ff., 634, 638–640, 647
 Linear Search, 621 ff.
 Ternary Search, 645
 secret sharing, 730, 962
 select, *see* median
 Selection Sort, *see* sorting
 self-loops, 1104
 self-reference, 225, 304, 346, 448, 1174, 1207
 sentinels, 945
 sequences, 237 ff.
 S^n (sequence of elements from the same set), 239
 cardinality, 906, 913
 sets, 222 ff.
 cardinality, 222 ff., 903 ff.
 characteristic function, 806

- complement, 226
- disjointness, *see* disjoint sets, *see also*
 - partitions
- empty set, 226
- intersection, 227
- set difference, 227
- singleton set, 226
- subsets/ supersets, 229 ff., *see also*
 - power set
- union, 227
 - inclusion–exclusion, 909 ff.
- Venn diagrams, 226
- well-ordered, 537
- Shamir, Adi, 730, 747, 962
- Shannon, Claude, 1017
- Sheffer stroke (\downarrow), 445
- Shor’s algorithm, 1016
- short-circuit evaluation, 327
- Sierpinski triangle/ carpet, 519 ff.
- Sieve of Eratosthenes, 718
- signed social networks, 1116
- Simpson’s Paradox, 467
- six degrees of separation, 438
- small-world phenomenon, 438, 1142
- social networks, 1116, 1123
 - Dunbar’s number, 1125
- sorting
 - Bubble Sort, 621, 626, 629
 - comparison-based, 629, 920
 - Counting Sort, 630, 921
 - Insertion Sort, 508, 620, 625, 629
 - average-case analysis, 1054, 1064
 - correctness using loop invariants, 517
 - lower bounds, 920–921
 - Merge Sort, 532, 631–632, 634, 636–638, 646, 647
 - Quick Sort, 630, 645
 - correctness (for any pivot rule), 526 ff.
 - randomized pivot selection, 1018
 - Radix Sort, 630
 - Selection Sort, 619, 626, 629, 920
- spam filter, 1037
- spanning trees, 1157 ff.
 - cycle elimination algorithm, 1158
 - minimum spanning trees, 1170 ff.
- speech processing, *see* natural language processing
- sphere packing, 416
- spreadsheets, 845, 849, 1135
- SQL (programming language), 815
- square roots, 218, *see* exponentials
 - Heron’s method, 439
- standard deviation, 1056 ff.
- Strassen’s algorithm, 655
- strings, 239
 - generating all strings of a given length, 714
 - regular expressions, 830
- strong induction, *see* proofs
- strongly connected components, 1133 ff.
- structural induction, *see* proofs
- subgraphs, *see* graphs
- subset, 229
- sum of products, *see* disjunctive normal form
- Sum Rule, 903
- summations, 212 ff.
 - arithmetic, 512
 - geometric, 510 ff., 648 ff.
 - infinite, 512
 - harmonic, 512 ff.
 - of a set, 228
 - reindexing summations, 213
 - reversing nested summations, 215, 1046
- superset, 230
- surjective functions, *see* onto functions
- symmetry, 405, 804, 820 ff.
 - symmetric closure, 826 ff.
- syntactic sugar, 322
- tautology, 317 ff.
- temporal logic, 825
- The Book, 438
- Therac-25, 464
- Theta (Θ) (asymptotics), 608, 823 ff.
- tic-tac-toe, 344, 941
- topological ordering, 843 ff.
- total orders, 838 ff., *see also* partial orders
- totient function, 744, 924
- Towers of Hanoi, 656
- transitivity, 822 ff.
 - nontransitive dice, 1063
 - nontransitivity in voting, 823
 - signed social networks, 1116
 - transitive closure, 826 ff.
- Traveling Salesman Problem, 959
- trees, 1147 ff.
 - 2–3 and 2–3–4 trees, 545
 - AVL trees, 643 ff.
 - binary search trees, 643, 1160
 - binary trees, 534, 643 ff., 1154 ff.
 - complete binary trees, 1162 ff.
 - heaps, 269, 529
 - decision trees, 921
 - forests, 1150
 - game trees, 344, 941
 - in counting problems, 918
 - parse trees, 543
 - quadrees, 645
 - recursion trees, 631 ff.
 - recursive definitions of trees, 534, 1154
 - rooted trees, 1151 ff.
 - spanning trees, 1157 ff.
 - minimum spanning trees, 1170 ff.
 - subtrees, 1153 ff.
 - tree traversal, 1154 ff.
 - van Emde Boas trees, 656
- triangle inequality, 405
- triangulation, 524–526, 528
- truth tables, 311 ff.
- truth values, 303 ff.
- tsktsks, 1165
- tuple, *see* sequence
- Turing Award, 224, 404, 604, 710, 747, 805, 1165
- Turing machines, 346, 449
- Turing, Alan, 448, 960
- unary numbers, *see* integers
- uncomputability, 346, 448–452, 455, 937
- undecidability, *see* uncomputability
- underflow, 217
- Unicode, 923
- uniform distribution, 1007, 1013 ff.
- unigrams, 1036
- union (of sets), 227
- Union Bound, 904
- unit vector, 241
- universal quantifier (\forall), 333 ff.
- URL squatting, 941
- vacuous quantification, 342
- valid inference, 458
- van Emde Boas trees, 656
- variance, 1056 ff.
- Vector Space Model, 248

- vectors, 239 ff.
 - dot product, 241 ff.
- Venn diagrams, 226
- virtual memory, 455
- Von Koch snowflake, 502, 509
- Voronoi diagram, 251
- voting systems, 823
- wall clocks, 627
- well-ordered set, 537
- “without loss of generality”, 427
- World War II, 960, 1116
- World-Wide Web, 1123, 1142
 - Google PageRank, 1174
- worst-case analysis, *see* running time
- xor, *see* exclusive or
- \mathbb{Z} , *see* integers
- \mathbb{Z}_n , 734 ff.
- zero (of a binary operator), 315, 545
- zyzzyvas, 806