

Index

- 2–3 and 2–3–4 trees, 5-59
- 9/11 Memorial, 11-28
- 123456791, 7-66
- 987654263, 7-66
- \forall (universal quantifier), 3-42 ff.
- absolute value, 2-7, 4-34, 4-36
- abstract algebra, 7-46
- abstraction, 4-2
- ACM Code of Ethics and Professional Conduct, 12-3
- ACM Conference on Fairness,
 - Accountability, and Transparency, 8-19
- adjacency, *see* graphs
- affirming the consequent, *see* fallacy
- algorithmic bias, 2-62, 4-86, 4-87, 8-19, 12-3
- algorithmic sentencing, 8-19
- algorithms, 2-83 ff., *see also* randomized algorithms
 - asymptotic analysis, 6-22 ff.
 - brute force, 3-32, 5-17, 9-2, 9-73
 - divide and conquer, 6-60 ff., 6-68
 - dynamic programming, 5-17, 9-2, 9-73
 - greedy algorithms, 4-28, 9-20
 - recurrence relations, 6-42 ff.
 - time, space, and power, 6-32
- Alice and Bob, 7-58 ff.
- ambiguity
 - in natural language, 3-10, 3-11, 3-17
 - order of operations, 5-56, 8-7
 - order of quantification, 3-65 ff., 3-78
 - prefix-free/Huffman codes, 9-20
- analysis (mathematics), 8-48
- ancestors (in a tree), 11-63
- and (\wedge), 3-7
- anonymization, 10-20
- antisymmetry, 8-26 ff.
- approximate equality, 2-6
- Ariane 5 rocket, 4-82
- arithmetic mean, 4-50, 4-72
- arithmetic series, 2-15, 5-14, 5-25
- Arrow's Theorem, 8-38
- artificial intelligence, 12-3
 - computer vision, 11-38
 - game trees, 3-54, 9-52
- assertions, 3-77, 5-20
- associativity, 3-27, 5-59, 7-46
- assuming the antecedent, *see* proofs
- asymmetry, 8-26 ff.
- asymptotics
 - analysis of algorithms, 6-22 ff.
 - asymptotic analysis, 6-4 ff.
 - asymptotic relationships viewed as relations, 8-31 ff.
 - best- and average-case running time, 6-29 ff.
 - divide and conquer, 6-61 ff.
 - O (Big O), 6-5 ff.
 - o , Ω , ω , and Θ , 6-10 ff.
 - polynomials, logs, and exponentials, 6-8 ff.
 - recurrence relations, 6-42 ff.
 - worst-case analysis, 6-23 ff.
- automata, 8-59, 9-54
- automated theorem proving, 4-31
- average distance in a graph, 11-54
- average-case analysis, *see* running time
- AVL trees, 6-53 ff.
- axiom of extensionality, 2-35
- Bacon, Kevin, 4-46, 11-20
- balanced binary search trees, 6-53
- Bayes' Rule, 10-44 ff.
- begging the question, *see* fallacy
- Bernoulli distribution, 10-16 ff., 10-60, 10-73
- Bernoulli's inequality, 5-26
- betweenness, 8-15
- BFS, *see* breadth-first search
- bias, *see* algorithmic bias
- biased coins, 10-17 ff.
- big O , big Ω , and big Θ , 6-5 ff., 8-31 ff.
- bigrams, 10-48
- bijections, 2-79, 9-35, 9-46
- binary numbers, *see* integers
- binary relation, *see* relations
- Binary Search, *see* searching
- binary search trees, *see* trees
- binary symmetric channel, 10-44, 10-45
- binary trees, *see* trees
- binomial coefficients, *see* combinations
- binomial distribution, 10-17 ff., 10-65
- Binomial Theorem, 9-67 ff.
- bipartite graphs, 11-21 ff.
 - complete bipartite graphs, 11-22
- birthday paradox, 5-34, 10-68
- Bitcoin, 12-2
- bitmaps, 2-56
- bits/bitstrings, 2-4, 2-51, 3-20, 4-5 ff., 7-58, 9-6, 9-37, 9-58 ff., 9-79
- Bletchley Park, 9-75
- blockchain, 12-2
- Bloom filters, 10-54
- Bob smells, 5-22
- Booleans, 2-4, 3-6, *see also* logic

12-6 Index

- bound (vs. free) variables, 3-46, 3-56
- breadth-first search, 11-42 ff.
finding cycles, 11-59
- brute force, *see* algorithms
- Bubble Sort, *see* sorting
- Buffon's needle, 10-76
- bugs, 2-20, 4-82, 5-20, 11-34
- butterfly ballots, 8-38
- C (programming language), 3-34, 3-56, 5-47
- Caesar Cipher, *see* cryptography
- cardinality, 2-28–2-29, 9-4 ff.
infinite, 9-46
- Carmichael numbers, 7-51, 7-53, 7-56
- Cartesian plane, 2-50
- Cartesian product (\times), 2-48
- catchphrase, 8-40, 11-81
- Cauchy sequences, 8-48
- ceiling, 2-7
- cellular automata, 9-54
- Chain Rule (probability), 10-43 ff.
change of index, 2-15
- checkers, 3-54, 4-48, 9-31
- checksum, 4-4, 4-15
- chess, 2-48, 3-54, 5-25, 9-15, 9-30, 11-40
- children (in a tree), 11-62
- Chinese Remainder Theorem, 7-30 ff.
- circle packing, 4-21
- circuits, 3-2, 3-20
printing and planar graphs, 11-24
representing logical propositions, 3-27, 3-37
using nand gates, 4-57
- class-size paradox, 10-61
- cliques, 11-19 ff.
- closure, 7-46, 8-33 ff.
- clustering, 2-42
- coarsening equivalence relations, 8-48 ff.
- codomain (of a function), 2-72
- collaboration networks, 11-20
- collaborative filtering, 2-45
- combinations, 9-57 ff.
 k -combinations, 9-60 ff.
- Binomial Theorem, 9-67 ff.
Pascal's identity, 9-66, 9-71
Pascal's triangle, 9-70
- combinatorial proof, 9-64 ff.
- commutativity, 2-58, 3-27, 3-66, 5-59, 7-46
- comparability, *see* partial orders
- comparison-based sorting, *see* sorting
- compilers, 2-71, 3-34, 5-56
- complement (of a set), 2-33
- complete graphs, 11-19 ff.
- complexity, *see* computational complexity
- composite numbers, 2-13, *see also* prime numbers
- composition
of functions, 2-76, 8-13
of relations, 8-9, 8-30
- compression
entropy and compressibility, 10-24
Huffman coding, 9-20, 9-48
impossibility of lossless compression, 9-48
lossy vs. lossless, 9-48
quantization of images, 2-71, 2-87
URL shortening, 9-9
- computability, 4-62
- computational biology
genome rearrangements, 3-76, 9-54
motifs in gene networks, 11-18
- computational complexity
and cryptography, 7-65
complexity classes, 6-35
graph isomorphism, 11-17
input size, 7-8
P vs. NP, 3-32
regular languages, 8-40, 8-59 ff.
- computational geometry, 2-66
- computational linguistics, *see* natural language processing
- computer architecture, 3-28 ff., 4-58
and running times, 6-23
Moore's Law, 6-16
power consumption, 6-32
representation of numbers, 2-20
- computer graphics
hidden-surface removal, 8-61
morphing, 2-68
rotation matrices, 2-63
triangulation, 5-36
- computer security, 7-65–7-67
- computer vision, 11-38
- computing networking, 9-22
- conditional expectation, 10-71 ff.
- conditional independence, 10-42
- conditional probability, 10-36 ff.
Bayes' Rule, 10-44
Chain Rule, 10-43
Law of Total Probability, 10-43
- Condorcet paradox, 8-38
- congruences (modular), 7-8 ff., 7-31 ff., 8-47
- conjunctive normal form, 3-29 ff., 4-53 ff., 5-52 ff.
- connectivity (in graphs), 11-36 ff.
connected component, 11-36 ff.
reachability, 11-38 ff.
- constructive proofs, 4-41
- constructivism, 4-42
- context-free grammar, 5-56
- contradiction, 3-23
- contrapositive, 3-25, 4-36, *see also* proofs
- converse, 3-25
- Cook–Levin Theorem, 3-32
- correlation, 10-30
correlation vs. causation, 4-81
positive and negative, 10-33
- countable sets, 9-46
- counterexamples, 4-40 ff.
- counting
Binomial Theorem, 9-67 ff.
combinations, 9-57 ff.
combinatorial proofs, 9-64 ff.
combining products and sums, 9-17 ff.
Division Rule, 9-38 ff.
double counting, 9-10 ff.
Generalized Product Rule, 9-14 ff.
inclusion–exclusion, 9-10 ff.
for 3+ sets, 9-13

- Mapping Rule, 9-34 ff.
 order, 9-58 ff.
 Pascal's triangle, 9-70 ff.
 permutations, 9-59 ff.
 Pigeonhole Principle, 9-43 ff.
 Product Rule (sequences), 9-8
 repetition, 9-58 ff.
 Sum Rule (unions), 9-5
- Counting Sort, *see* sorting
 coupon collector problem, 10-84
 crossword puzzles, 3-75
 cryptography, 5-22, 7-58 ff., 8-38, 12-2
 and pseudorandomness, 10-15
 Caesar Cipher, 7-59, 10-53
 Diffie–Hellman key exchange, 7-67
 digital signatures, 7-61
 Enigma Machine and WWII, 9-75
 frequency analysis, 10-34, 10-52
 key exchange, 7-67
 man-in-the-middle attack, 7-67
 one-time pads, 7-58
 public-key cryptography, 7-60 ff.
 RSA cryptosystem, 4-68, 7-60 ff.
 secret sharing, 7-36
 substitution cipher, 10-34, 10-40, 10-52
- Currying, 3-73
 cycles, 8-52, 11-57 ff.
 acyclic graphs, 11-59 ff.
 cycle elimination algorithm, 11-69
 cycle rule for minimum spanning trees, 11-86
 kidney transplants, 11-71
 simple cycles, 11-58
 weighted cycle elimination algorithm, 11-86
- DAG (directed acyclic graph), 11-60
 data mining, *see* machine learning
 data privacy, 10-20
 data visualization, 11-11, 11-28
 databases, 3-60, 8-17, 8-22
 De Morgan's Laws, 3-28
 decision problems, 4-62
 Deep Blue, 3-54
- degree (in a graph), 11-8 ff., 11-10
 degree distribution, 11-26
 regular graphs, 11-22
 degree (of a polynomial), 2-82
 density (of a graph), 6-20, 11-32
 denying the hypothesis, *see* fallacy
 dependent events, 10-30 ff.
 depth-first search, 11-46 ff.
 Descartes, René, 2-48
 descendants (in a tree), 11-63
 deterministic finite automata, 8-59
 DFS, *see* depth-first search
 diagonalization, 9-46
 diameter (of a graph), 11-53
 differential privacy, 10-20
 Diffie–Hellman key exchange, 7-67
 Dijkstra's algorithm, 11-80 ff.
 directed graphs, 8-24
 disconnected, *see* connectivity in graphs
 disjoint sets, 2-37, 4-20
 disjunctive normal form, 3-29 ff., 4-53 ff., 5-52 ff.
 distance, *see also* metrics
 Euclidean, *see* Euclidean distance
 Hamming, *see* Hamming distance
 in a graph, 11-41 ff.
 Manhattan, *see* Manhattan distance
 minimum distance of a code, 4-8 ff.
- divide and conquer, *see* algorithms
 divisibility, 2-12, 2-74, 5-18, 8-53
 and modular arithmetic, 7-9 ff.
 common divisors, 7-11 ff.
 divisibility rules, 3-20, 4-33, 4-50, 7-19
 Division Theorem, 7-4
 division, *see* mod
 in \mathbb{Z}_n , 7-44
 Division Rule, 9-38 ff.
 domain (of a function), 2-72
 dot product, 2-53 ff.
 Dunbar's number, 11-30
 dynamic programming, *see* algorithms
 dynamic scope, 3-56
- \exists (existential quantifier), 3-42 ff.
- e (base of natural logarithm), 2-11
 edges, *see* graphs
 efficiency, *see* running time, *see also*
 computational complexity
 ELIZA, 12-3
 Emacs, 9-29, 12-3
 empty set, 2-32
 Enigma Machine, 9-75
 entropy, 10-24
 equivalence relations, 8-45 ff.
 equivalence classes, 8-47
 refinements and coarsenings, 8-48
 Eratosthenes, 7-22, 7-40
 Erdős numbers, 4-46
 Erdős, Paul, 4-46, 11-20
 error-correcting codes, 4-6 ff.
 Golay code, 4-28
 Hamming code, 4-15 ff., 9-33
 messages and codewords, 4-6 ff.
 minimum distance and rate, 4-8 ff.
 Reed–Solomon codes, 4-23, 7-38
 repetition code, 4-13 ff.
 upper bounds on rates, 4-19
 error-detecting codes, 4-6 ff.
 credit card numbers, 4-4, 4-25
 UPC, 9-51
 ethics, 4-86, 5-22, 6-66, 8-19, 10-20, 12-2–12-4
 Euclid, 4-60, 7-12
 Euclidean algorithm, 7-12, 7-26
 efficiency, 7-15, 7-19
 Extended Euclidean algorithm, 7-27
 Euclidean distance, 2-66, 4-72
 Euler's Theorem, 7-56
 even numbers, 2-13, 4-38
 evenly divides, *see* divisibility
 events (probability), 10-8 ff.
 correlated, 10-30
 independent events, 10-30 ff.
 exclusive or (\oplus), 2-13, 3-10 ff., 4-15 ff.
 existential quantifier (\exists), 3-42 ff.
 expectation, 10-60 ff.
 average-case analysis of algorithms, 6-29 ff.

12-8 Index

- conditional expectation, 10-71 ff.
- coupon collector problem, 10-84
- deviation from expectation, 10-72 ff.
 - Markov's inequality, 10-84
- Law of Total Expectation, 10-72
- linearity of expectation, 10-64 ff.
- exponentials, 2-8 ff., 5-59
 - asymptotics, 6-9 ff.
 - modular, 7-19
- EXPSpace (complexity class), 6-35
- EXPTIME (complexity class), 6-35
- Extended Euclidean algorithm, 7-27

- facial recognition, 4-86, 4-87, 8-19, 12-3
- factorial, 4-30–4-31, 5-18, 6-43, 6-45, 9-16, 9-27
 - Stirling's approximation, 9-80
- factors, *see* divisibility, *see also* prime factorization
- fallacy, 4-75 ff.
 - affirming the consequent, 4-78
 - begging the question, 4-79
 - denying the hypothesis, 4-78
 - false dichotomy, 4-35, 4-79
 - proving true, 4-77
- false dichotomy, *see* fallacy
- Fast Fourier transform, 2-9
- fencepost error, 11-34
- Fermat pseudoprime, 7-51
- Fermat's Last Theorem, 7-48
- Fermat's Little Theorem, 7-48 ff.
- Fermat–Euler Theorem, 7-56
- Fibonacci numbers, 2-68, 5-41, 6-44, 6-49–6-52, 6-55, 9-80
 - algorithms, 6-58
 - and the Euclidean algorithm, 7-19
- filter, 2-40
- finite-state machines, 8-59
- float (floating point number), 2-20, 6-23
- floor, 2-7
 - Division Theorem, 7-4
- for loops
 - analogy for \prod , 2-19
 - analogy for \sum , 2-14, 2-16
- analogy for quantifiers, 3-45, 3-67, 3-78
- forests, 11-60
 - spanning forests, 11-68
- formal language theory, 8-40, *see* computational complexity
- formal methods, 4-31, 8-32
- Four Color Theorem, 4-48, 11-24
- fractals, 5-2, 5-10–5-11, 5-25–5-26, 5-42
- free (vs. bound) variables, 3-46, 3-56
- frequency analysis, 10-34
- functions, 2-70 ff.
 - algorithms, 2-83 ff.
 - characteristic function of a set, 8-7
 - composition, 2-76
 - domain/codomain, 2-72
 - growth rates, 6-4 ff.
 - inverses, 2-80
 - one-to-one/onto functions, 2-77 ff.
 - range/image, 2-73 ff.
 - viewed as relations, 8-12 ff.
 - visual representation, 2-75
 - vs. macros, 3-56
- Fundamental Theorem of Arithmetic, 7-24
- fuzzy logic, 3-18

- Game of Life, 9-54
- game trees, 3-54, 9-52
- garbage collection, 6-33, 11-51
- Gates, Bill, 3-76, 4-46
- GCD, *see* greatest common divisor
- GCHQ, 7-60
- Generalized Product Rule, 9-14 ff.
- geometric distribution, 10-18 ff., 10-64
- geometric mean, 4-50, 4-72
- geometric series, 2-15, 5-12 ff.
 - for recurrence relations, 6-61 ff.
 - infinite, 5-14
- giant component, 11-49
- Gödel's Incompleteness Theorem, 3-58
- Goldbach's conjecture, 3-4, 3-64, 3-78
- golden ratio, 6-51, 6-55
- grammars, 5-47, 5-56
- graph drawing, 11-23, 11-28
- graphs, 11-4 ff.
 - acyclic graphs, 11-59 ff.
 - adjacency lists, 11-12 ff.
 - adjacency matrices, 11-13 ff.
 - bipartite graphs, 11-21 ff.
 - breadth-first search, 11-42 ff.
 - complete graphs, 11-19 ff.
 - connected components, 11-36 ff.
 - connectivity, 11-36 ff.
 - cycles, 11-57 ff.
 - data structures, 11-11, 11-12 ff.
 - degree, 11-8, 11-10 ff.
 - Handshaking Lemma, 11-9
 - regular graphs, 11-22
 - density, 11-32
 - depth-first search, 11-46 ff.
 - forests, 11-60
 - isomorphism, 11-16 ff.
 - matchings, 9-42, 9-53, 9-75, 11-23, 11-71
 - neighborhoods, 11-7 ff., 11-10 ff.
 - paths, 11-34 ff.
 - shortest paths, 11-41 ff.
 - planar graphs, 11-23 ff.
 - shortest paths
 - Dijkstra's algorithm, 11-80 ff.
 - simple graphs, 11-6
 - subgraphs, 11-17 ff.
 - trees, *see* trees
 - undirected vs. directed, 11-4 ff.
 - weighted graphs, 11-79 ff.
 - Dijkstra's algorithm, 11-80 ff.
- grayscale, 2-2, 2-71, 3-38
- greatest common divisor, 7-11 ff., *see also* Euclidean algorithm
- H_n , *see* harmonic number
- Halting Problem, 3-58, 4-64 ff., 4-70
- Hamiltonian path, 11-54
- Hamming code, 2-69, 4-15 ff., 9-52
 - number of valid codewords, 9-33
- Hamming distance, 4-5
- Handshaking Lemma, 11-9
- harmonic number, 5-14–5-15, 5-26

- hashing, 2-85, 9-55, 10-3–10-5, 10-66, 10-84
 - Bloom filters, 10-54
 - chaining, 2-85
 - collisions, 2-85, 10-3 ff., 10-13, 10-28, 10-54, 10-67
 - and pairwise independence, 10-36
 - chaining, 10-3
 - clustering, 10-13, 10-28
 - double hashing, 10-29
 - linear probing, 10-13, 10-28
 - quadratic probing, 10-28
 - simple uniform hashing, 10-4
- Hasse diagrams, 8-52
- heaps, 2-88, 5-38, 5-59
- heavy-tailed distribution, 11-26
- height (of a tree), 11-63
- Heron's method, 2-22, 4-50
- hidden-surface removal, 8-61
- higher-order functions, 2-40, 3-73
- Hopper, Grace Murray, 2-71, 4-82
- Huffman coding, 9-20, 9-48
- hypercube, 11-32

- I (identity matrix), 2-56
- idempotence, 3-27
- identity
 - identity function, 2-80
 - identity matrix, 2-56
 - multiplicative identity, 7-44
 - of a binary operator, 3-19, 5-59
- if and only if (\Leftrightarrow), 3-10 ff.
- image (of a function), 2-73
- image processing
 - blur filter, 2-22
 - dithering, 3-38
 - grayscale conversion, 2-2
 - quantization, 2-71
 - seam carving, 9-73
 - segmentation, 11-38
- imaginary numbers, 2-9
- implication (\Rightarrow), 3-8 ff.
- in-degree, *see* degree
- in-neighbor, *see* neighbors (in graphs)
- inclusion–exclusion, 9-10 ff., 9-80
- inclusive naming, 6-66
- incomparability, 6-13, 8-50
- incompleteness (logic), 3-58
- inconsistency (logic), 3-58
- independent events, 10-30 ff.
 - pairwise independence, 10-36
- indicator random variables, 10-59
- induction, *see* proofs
 - checklist for inductive proofs, 5-6
 - generating conjectures, 5-10
 - proofs about algorithms, 5-16 ff., 6-46 ff.
 - strengthening the inductive hypothesis, 5-53
- infinite sequences, 2-15, 5-14
- infix notation, 8-6
- information retrieval, 2-61
- information theory, 10-24, 10-44
- injective functions, *see* one-to-one functions
- Insertion Sort, *see* sorting
- integers, 2-4 ff.
 - algorithms for arithmetic, 7-6, 7-18
 - efficiency, 7-8
 - division, *see* modular arithmetic
 - primes and composites, *see* prime numbers
 - recursive definition, 5-55
 - representation
 - binary numbers, 3-20, 5-7, 5-27, 5-40, 7-8, 7-16
 - different bases, 5-40, 7-16
 - ints, 2-20
 - modular representation, 7-35
 - unary, 7-8
 - successor relation, 8-36
- internet addresses, 9-22
- intersection (of sets), 2-33
- intervals, *see* real numbers
- invalid inference, 4-75
- inverse
 - additive, 7-55
 - multiplicative, 7-44 ff.
- of a function, 2-80
- of a matrix, 2-68
- of a relation, 8-8 ff., 8-29
- of an implication, 3-25
- IP addresses, 9-22
- irrationals, *see* rationals
 - irrationality of $\sqrt{2}$, 4-39
- irreflexivity, 8-25 ff.
- isomorphism (of graphs), 11-16 ff.

- Jaccard coefficient, 2-45
- Java (programming language), 2-73, 3-12, 3-34, 11-51
- Johnson's algorithm, 10-85
- join (database operation), 8-17

- \mathcal{K}_n , *see* complete graphs
- $\mathcal{K}_{n,n}$, *see* bipartite graphs
- Kasparov, Garry, 3-54
- Keller, Mary Kenneth, 4-75
- keyspace, *see* hashing
- kidney transplants, 11-71, 12-2
- Knuth, Donald, 7-12
- Kruskal's algorithm, 11-87
- Kuratowski's Theorem, 11-25

- L (complexity class), 6-35
- latchstring, 8-40, 11-81
- law of the excluded middle, 3-22
- Law of Total Expectation, 10-72
- Law of Total Probability, 10-43
- least common multiple, 7-11 ff.
- length (of a vector), 2-52
- lexical scope, 3-56
- lexicographic ordering, 3-63, 8-7
- Liar's Paradox, 2-31
- linearity of expectation, 10-64
- linked lists, 5-58
 - adjacency lists for graphs, 11-12 ff.
 - as graphs, 11-31
 - recursive definition, 5-45
- list, *see* sequence
- little o and little ω , 6-10 ff., 8-31 ff.
- logarithms, 2-10–2-11
 - asymptotics, 6-9 ff.

12-10 Index

- discrete logarithm, 7-67
- polylogarithmic functions, 6-19, 7-8
- logic
 - Boolean logic, 2-4, 7-46
 - consistency, 3-58
 - fuzzy logic, 3-17
 - incompleteness, 3-58
 - logical equivalence, 3-24, 3-47
 - logical fallacy, *see* fallacy
 - modal logic, 8-32
 - predicate logic, 3-40 ff.
 - games against the demon, 3-69
 - nested quantifiers, 3-63 ff.
 - order of quantification, 3-65 ff.
 - predicates, 3-40 ff.
 - quantifiers, 3-42 ff.
 - theorems in predicate logic, 3-47 ff.
 - propositional logic, 3-4 ff.
 - atomic vs. compound propositions, 3-6
 - logical connectives, 3-6 ff.
 - propositions, 3-4 ff.
 - recursive definition of a well-formed formula, 5-47
 - satisfiability, 3-23
 - tautology, 3-22 ff.
 - truth assignment, 3-13
 - truth tables, 3-13 ff.
 - truth values, 3-4, 5-48
 - universal set of operators, 4-72
 - temporal logic, 8-32
- longest common subsequence, 5-17, 9-80
- loop invariants, 5-20
- Lovelace, Ada, 2-22, 2-48
- machine learning
 - bias, 2-62
 - classification problems, 9-35, 10-50
 - clustering, 2-42
 - cross-validation, 9-79
- macros, 3-56
- Manhattan distance, 2-52, 2-66, 4-72
- map, 2-40
- Mapping Rule, 9-34 ff.
- MapReduce, 2-40
- maps, 4-48, 11-24
- mark-and-sweep, 11-51
- Markov's inequality, 10-84
- matchings, *see* graphs
- matrices, 2-55 ff.
 - adjacency matrices for graphs, 11-13 ff.
 - identity matrix, 2-56
 - inverse of a matrix, 2-68
 - matrix multiplication, 2-57 ff.
 - Strassen's algorithm, 6-68
 - rotation matrices, 2-63, 4-73
 - term-document matrix, 2-61
- maximal element, 8-54 ff.
- maximum element, 2-35, 2-84, 8-54 ff.
- mazes, 11-46
- median (of an array), 2-89, 10-78 ff.
- memoization, 9-73
- memory management, 11-51
- Merge Sort, *see* sorting
- metrics, 4-5, 4-25-4-26, 11-54
- Milgram, Stanley, 4-46
- Miller-Rabin test, 4-68, 7-53
- minimal element, 8-54 ff.
- minimum element, 2-35, 8-54 ff.
- minimum spanning trees, 11-85 ff.
 - cycle rule, 11-86
 - Kruskal's algorithm, 11-87
 - weighted cycle elimination algorithm, 11-86
- ML (programming language), 3-73, 5-52
- modal logic, 8-32
- modular arithmetic, 2-11-2-13, 7-4 ff.
 - Division Theorem, 7-4
 - mod-and-div** algorithm, 7-6 ff., 7-18
- modular congruences, 7-8
- modular exponentiation, 7-19
- modular products, 7-9
- modular sums, 7-9
- multiplicative inverse, 7-44 ff.
 - primitive roots, 7-67
- Modus Ponens, 3-23
- Modus Tollens, 3-23
- Monte Carlo method, 10-76
- Monty Hall Problem, 10-14
- Moore's Law, 6-16
- multiples, *see* divisibility
- multiplicative identity, 7-44
- multiplicative inverse, 7-44 ff.
- multitasking, 6-33
- naïve Bayes classifier, 10-50
- nand (not and), 4-57, 5-60
- n -ary relations, 8-14 ff.
 - expressing n -ary relations as binary relations, 8-15
- natural language processing, 12-3
 - ambiguity, 3-17
 - language model, 10-48
 - speech processing, 2-42, 9-32
 - speech recognition, 10-48
 - text classification, 10-50
 - text-to-speech systems, 9-32
- natural logarithm, *see* logarithms
- neighbors (in graphs), 11-7, 11-10
- nested quantifiers, 3-63 ff.
 - games against the demon, 3-69
 - negations, 3-67
 - order of quantification, 3-65 ff.
- nested sums, 2-16, 10-63
- Newton's method, 2-22
- nodes, *see* graphs
- nonconstructive proofs, 4-41
- nor (not or), 4-58, 5-60
- not (\neg), 2-70, 3-7
- NP (complexity class), 3-32, 4-79, 6-35
- number line, 2-6
- number theory, *see* modular arithmetic
- numerical methods, *see* scientific computing
- O (Big O), 6-5 ff., 8-31 ff.
- o (little o), 6-10, 8-31 ff.
- odd numbers, 2-13
- off-by-one error, 11-34
- Omega (Ω) (asymptotics), 6-10, 8-31 ff.
- omega (ω) (asymptotics), 6-10, 8-31 ff.
- one-time pads, 7-58

- one-to-one functions, 2-78, 8-14, 9-35
- onion routing, 5-22
- onto functions, 2-77, 3-63, 8-14, 9-35
- operating systems, 3-75
 - multitasking, 6-33
 - virtual memory, 4-70
- optimizing compilers, 3-34, 3-37
- or (\vee), 3-7
- order of operations, *see* precedence of operators
- orders, *see* partial orders
- organ donation, 11-71
- out-degree, *see* degree
- out-neighbor, *see* neighbors (in graphs)
- outcome (probability), 10-6
- overfitting, 10-48
- overflow, 2-20, 4-82
- \mathcal{P} , *see* power set
- P (complexity class), 3-32, 4-79, 6-35
- PageRank, 11-90
- Painter's Algorithm, 8-61
- pairwise independence, 10-36
- palindromes, 5-60, 9-50
- paradoxes
 - birthday paradox, 10-68
 - class-size paradox, 10-61
 - Liar's paradox, 2-31
 - nontransitive dice, 10-82
 - paradoxes of translation, 3-5
 - Russell's paradox, 2-31
 - Simpson's Paradox, 4-87
 - voting paradoxes, 8-38
- parallel edges, 11-5
- parent (in a tree), 11-62
- parity, 2-13, 4-15 ff., 5-29–5-30, 5-40
- parsing, 5-56
- partial orders, 8-50 ff.
 - chains and antichains, 8-65
 - comparability, 8-50
 - extending to a total order, 8-56 ff.
 - Hasse diagrams, 8-52
 - immediate successors, 8-53
 - minimal/maximal elements, 8-54
 - minimum/maximum element, 8-54
 - strict partial order, 8-50
 - topological ordering, 8-56 ff.
 - total orders, 8-50
 - consistency with a partial order, 8-56 ff.
- partition (of a set), 2-38
 - bipartite graphs, 11-21
 - equivalence relations, 8-47
- Pascal's identity, 9-66, 9-71
- Pascal's triangle, 9-70 ff.
- paths (in graphs), 11-34 ff.
 - breadth-first search, 11-42 ff.
 - connected graphs, 11-36 ff.
 - depth-first search, 11-46 ff.
 - Dijkstra's algorithm, 11-80 ff.
 - internet routing, 9-22
 - shortest paths, 11-41 ff.
 - simple paths, 11-35
- Peirce's arrow (\downarrow), 4-58, 5-60
- Pentium chip, 4-82, 6-16
- perfect matchings, *see* graphs
- perfect numbers, 2-26
- perfect square, 2-9
- Perl (programming language), 4-60
- permutations, 5-42, 9-16–9-17, 9-27
 - k -permutations, 9-59 ff.
- Petersen graph, 11-17, 11-25
- Pigeonhole Principle, 9-43 ff., 9-48
- planar graphs, 4-48, 11-23 ff.
 - Kuratowski's Theorem, 11-25
- polygons, 2-63, 5-27, 5-32, 5-36, 5-42, 10-76
- polylogarithmic, 6-19, 7-8
- polynomials, 2-81 ff., 4-23, *see also* P (complexity class)
 - asymptotics, 6-8 ff.
 - evaluating modulo a prime, 7-25, 7-36, 7-38
- postfix notation, 8-6
- Postscript (programming language), 8-6
- power set, 2-39
 - as a relation, 8-6
 - cardinality, 9-37
- power-law distribution, 11-26
- powers, *see* exponentials
- precedence of operators, 2-34, 3-12, 3-45, 5-56
- predicate logic, *see* logic
- predicates, 3-40 ff., 8-7, *see also* logic
- prefix notation, 8-6
- prefix-free codes, 9-19
- preorder, 8-52
- prime numbers, 2-13, 4-63, 7-21 ff.
 - Carmichael numbers, 7-51, 7-56
 - distribution of the primes, 7-22
 - infinitude of primes, 4-60
 - primality testing, 4-60, 4-68, 6-22, 7-21
 - efficient algorithms, 7-53
 - prime factorization, 7-24, 7-66
 - cryptography, 4-68, 7-65
 - existence of, 5-30–5-32
 - Shor's algorithm, 10-22
 - uniqueness of, 7-28–7-30
 - Prime Number Theorem, 7-22
 - Sieve of Eratosthenes, 7-22, 7-40
- priority queues, 5-38
- privacy, 5-22, 10-20, 12-2
- probability
 - Bayes' Rule, 10-44 ff.
 - conditional expectation, 10-71 ff.
 - conditional probability, 10-36 ff.
 - coupon collector problem, 10-84
 - events, 10-8 ff.
 - expectation, 10-60 ff.
 - infinitesimal probabilities, 10-40
 - Law of Total Expectation, 10-72
 - Law of Total Probability, 10-43
 - linearity of expectation, 10-64 ff.
 - Markov's inequality, 10-84
 - Monty Hall Problem, 10-14
 - outcomes, 10-6 ff.
 - probability functions, 10-6 ff.
 - random variables, 10-57 ff.
 - random walks, 11-90
 - standard deviation, 10-72 ff.
 - tree diagrams, 10-12 ff.
 - variance, 10-72 ff.

12-12 Index

- probability distributions
- Bernoulli, 10-16 ff.
 - binomial, 10-17 ff.
 - entropy, 10-24
 - geometric, 10-18 ff.
 - posterior distribution, 10-46
 - prior distribution, 10-46
 - uniform, 10-16 ff.
- product, 2-18 ff.
- of a set, 2-35
- product of sums, *see* conjunctive normal form
- Product Rule, 9-8
- cardinality of S^k , 9-9
- programming languages
- compile-time optimization, 3-34
 - Currying, 3-73
 - garbage collection, 6-33, 11-51
 - higher-order functions, 2-40, 3-73
 - parsing, 5-56
 - scoping/functions/macros, 3-56
 - short-circuit evaluation, 3-34
 - syntactic sugar, 3-28
- project (database operation), 8-17
- proofs, 4-30 ff.
- by assuming the antecedent, 3-51, 4-33
 - by cases, 4-18, 4-34 ff.
 - by construction, 4-14, 4-41 ff.
 - by contradiction, 4-21, 4-38 ff.
 - by contrapositive, 4-36 ff.
 - by induction, 2-83, 5-4 ff.
 - by mutual implication, 4-37
 - by strong induction, 5-28 ff.
 - by structural induction, 5-48 ff.
 - combinatorial proofs, 9-64 ff.
 - direct, 4-32 ff.
 - nonconstructive, 4-41
 - strategy for proofs, 4-42 ff.
 - unprovable true statements, 3-58
 - “without loss of generality”, 4-35
 - writing proofs, 4-44 ff.
- proper subset and superset, 2-36
- propositional logic, *see* logic
- proving true, *see* fallacy
- pseudocode, 2-84
- pseudorandom generator, 10-15
- PSPACE (complexity class), 6-35
- public-key cryptography, *see* cryptography
- Pythagorean Theorem, 4-44, 4-58–4-60, 4-72
- incorrect published proof, 4-87
- Python (programming language), 2-20, 2-40, 2-73, 3-20, 3-56, 3-73, 4-62 ff., 9-46, 11-51
- \mathbb{Q} , *see* rationals
- QR codes, 4-4, 4-23
- quadtrees, 6-57
- quantifiers, 3-42 ff.
- negating quantifiers, 3-49 ff.
 - nested quantifiers, 3-63 ff.
 - vacuous quantification, 3-52
- quantum computation, 10-22
- Quick Sort, *see* sorting
- \mathbb{R} , *see* real numbers
- Radix Sort, *see* sorting
- raising to a power, *see* exponentials
- Random Surfer Model, 11-90
- random variables, 10-57 ff.
- expectation, 10-60 ff.
 - independent random variables, 10-59
 - indicator random variables, 10-59
- random walks, 11-90, 11-93
- randomized algorithms, 6-32
- Buffon’s needle, 10-76
 - finding medians, 10-78
 - Johnson’s algorithm, 10-85
 - Monte Carlo method, 10-76
 - primality testing (Miller–Rabin), 7-53
 - Quick Sort, 10-27
- range (of a function), 2-73
- rate (of a code), 4-8 ff.
- rational numbers, 2-4 ff., 2-50, 4-33, 4-37, 7-11
- in lowest terms, 7-11, 8-47
- real numbers, 2-4 ff.
- absolute value/floor/ceiling, 2-7 ff.
 - approximate equality (\approx), 2-6, 8-4
 - defining via infinite sequences, 8-48
 - exponentiation, 2-8 ff.
 - floats (representation), 2-20
 - intervals, 2-6
 - logarithms, 2-10 ff.
 - trichotomy, 6-14
- realization, *see* outcome (probability)
- recommender system, 2-45
- recurrence relations, 6-42 ff.
- divide and conquer, 6-61 ff.
 - iterating, 6-45
 - sloppiness, 6-49
 - solving by induction, 6-44
 - variable substitution, 6-47
- recursion tree, 6-40, 6-61 ff.
- recursively defined structures, 5-45 ff.
- Reed–Solomon codes, 4-23, 7-38
- reference counting, 11-51
- refining equivalence relations, 8-48 ff.
- reflexivity, 4-6, 8-25 ff.
- reflexive closure, 8-33 ff.
- regular expressions, 8-40, 8-59
- regular graphs, 11-22
- reindexing, 2-15
- relational databases, *see* databases
- relations
- n -ary relations, 8-14 ff.
 - binary relations, 8-5 ff.
 - closures, 8-33 ff.
 - composition, 8-9 ff.
 - equivalence relations, 8-45 ff.
 - functions as relations, 8-12 ff.
 - inverses, 8-8 ff.
 - partial orders, 8-50 ff.
 - reflexivity, 8-25
 - relational databases, 8-17
 - symmetry, 8-26
 - total orders, 8-50 ff.
 - transitivity, 8-29 ff.
 - visual representation, 8-7 ff., 8-24 ff.
 - Hasse diagrams, 8-52 ff.
 - vs. predicates, 8-7
- relative primality, 7-24 ff., 7-46 ff.

- Chinese Remainder Theorem, 7-30 ff.
- Extended Euclidean algorithm, 7-27
- remainder, *see* mod
- repeated squaring, 6-58, 7-19, 7-63
- repetition code, 4-13 ff.
- roots (of a polynomial), 2-82, 4-23, 7-38
- rotation matrices, *see* matrices
- roulette, 10-11, 10-73
- RSA cryptosystem, 4-68, 5-22, 7-60 ff.
 - breaking the encryption, 7-65
- Rubik's cube, 7-46, 9-28
- running time, 6-22 ff.
 - average case, 6-29 ff., 10-70
 - best case, 6-29 ff.
 - worst case, 6-23 ff.
- Russell's paradox, 2-31
- sample space (probability), 10-6
- sampling bias, 10-61
- satisfiability, 3-23, 3-32, 4-63, 8-4, 10-85
- scalars, 2-51
- SCC, *see* strongly connected components
- Scheme (programming language), 2-40, 2-50, 3-28, 3-73, 8-6
- scientific computing, 6-23
 - Newton's method, 2-22
- seam carving, 9-73
- searching
 - Binary Search, 5-20, 5-42, 6-28 ff., 6-44, 6-48–6-49, 6-60, 7-18
 - Linear Search, 6-27 ff.
 - Ternary Search, 6-57
- secret sharing, 7-36, 9-79
- select, *see* median
- select (database operation), 8-17
- Selection Sort, *see* sorting
- self-loops, 11-5
- self-reference, 2-31, 3-5, 3-58, 4-61, 11-90, 12-13
- sentinels, 9-57
- sequences, 2-48 ff.
 - S^n (sequence of elements from the same set), 2-50
 - cardinality, 9-8, 9-14
- sets, 2-28 ff.
 - cardinality, 2-28 ff., 9-4 ff.
 - characteristic function, 8-7
 - complement, 2-33
 - disjointness, *see* disjoint sets, *see also* partitions
 - empty set, 2-32
 - intersection, 2-33
 - set difference, 2-34
 - singleton set, 2-32
 - subsets/supersets, 2-35 ff., *see also* power set
 - union, 2-33
 - inclusion–exclusion, 9-10 ff.
 - Venn diagrams, 2-32
 - well-ordered, 5-49
- Sheffer stroke (\uparrow), 4-57, 5-60
- Shor's algorithm, 10-22
- short-circuit evaluation, 3-34
- Sierpiński triangle/carpet, 5-25 ff.
- Sieve of Eratosthenes, 7-22, 7-40
- signed social networks, 11-18
- Simpson's Paradox, 4-87
- six degrees of separation, 4-46
- skite, 11-56
- small-world phenomenon, 4-46, 11-49
- social networks, 4-46, 11-2, 11-18, 11-26
 - Dunbar's number, 11-30
- sorting
 - Bubble Sort, 6-26, 6-32, 6-37
 - comparison-based, 6-37, 9-24
 - Counting Sort, 6-38, 9-27
 - Insertion Sort, 5-10, 6-25, 6-30, 6-37
 - average-case analysis, 10-70, 10-83
 - correctness using loop invariants, 5-20
 - lower bounds, 9-24–9-27
 - Merge Sort, 5-42, 6-40–6-43, 6-46–6-47, 6-58, 6-60
 - Quick Sort, 6-38, 6-58
 - correctness (for any pivot rule), 5-33 ff.
 - randomized pivot selection, 10-27
 - Radix Sort, 6-38
- Selection Sort, 6-24, 6-31, 6-37, 9-24
- spam filter, 10-50
- spanning trees, 11-68 ff.
 - cycle elimination algorithm, 11-69
 - minimum spanning trees, 11-85 ff.
- speech processing, *see* natural language processing
- sphere packing, 4-21
- spreadsheets, 8-58, 8-65, 11-40
- SQL (programming language), 8-17
- square roots, 2-9, 2-22, *see* exponentials
 - Heron's method, 2-22, 4-50
- standard deviation, 10-72 ff.
- steganography, 5-22
- Strassen's algorithm, 6-68
- strings, 2-50, 2-65
 - generating all strings of a given length, 7-16
 - regular expressions, 8-40
- strong induction, *see* proofs
- strongly connected components, 11-38 ff.
- structural induction, *see* proofs
- subgraphs, *see* graphs
- subsequences, 5-17, 8-21, 9-51, 9-64, 9-78, 9-80
- subset, 2-36
- Sudoku, 3-32
- sum of products, *see* disjunctive normal form
- Sum Rule, 9-5
- summations, 2-14 ff.
 - arithmetic, 2-15, 5-14, 5-25
 - geometric, 2-15, 5-12 ff., 6-61 ff.
 - infinite, 5-14
 - harmonic, 5-14 ff.
 - of a set, 2-35
 - reindexing summations, 2-15
 - reversing nested summations, 2-17, 10-62
- superset, 2-36
- surjective functions, *see* onto functions
- symmetry, 4-6, 8-5, 8-26 ff.
 - symmetric closure, 8-33 ff.
- syntactic sugar, 3-28

12-14 Index

- syzygy, 11-25, 11-81
 $T(n) = aT(n/b) + n^k$, 6-61 ff.
 tautology, 3-22 ff.
 temporal logic, 8-32
 term frequency–inverse document
 frequency (TFIDF), 2-61
 The Book (of proofs), 4-46
 Therac-25, 4-82, 12-2
 Theta (Θ) (asymptotics), 6-10, 8-31 ff.
 tic-tac-toe, 3-54, 9-52
 topological ordering, 8-56 ff.
 Tor, 5-22, 12-2
 total orders, 8-50 ff., *see also* partial
 orders
 totient function, 7-56, 9-30
 Towers of Hanoi, 6-70
 transitivity, 8-29 ff.
 nontransitive dice, 10-82
 nontransitivity in voting, 8-38
 signed social networks, 11-18
 transitive closure, 8-33 ff.
 Traveling Salesperson Problem, 9-73
 trees, 11-57 ff.
 2–3 and 2–3–4 trees, 5-59
 AVL trees, 6-53 ff.
 binary search trees, 5-58, 6-53, 11-73
 binary trees, 5-46, 6-53 ff., 11-65 ff.
 complete binary trees, 11-77 ff.
 heaps, 2-88, 5-38
 decision trees, 9-26
 forests, 11-60
 game trees, 3-54, 9-52
 in counting problems, 9-20
 parse trees, 5-56
 quadrees, 6-57
 recursion trees, 6-40 ff.
 recursive definitions of trees, 5-46,
 11-65
 rooted trees, 11-62 ff.
 spanning trees, 11-68 ff.
 minimum spanning trees, 11-85 ff.
 subtrees, 11-63 ff.
 tree traversal, 11-65 ff.
 van Emde Boas trees, 6-71
 triangle inequality, 4-6, 4-35
 triangulation, 5-32–5-33, 5-36
 truth tables, 3-13 ff.
 truth values, 3-4 ff.
 tsksks, 8-40, 11-81
 tuple, *see* sequence
 Turing Award, 2-30, 3-26, 4-5, 6-5, 7-12,
 7-60, 7-67, 8-6, 8-17, 11-80
 Turing machines, 3-58, 4-62, 6-23
 Turing, Alan, 2-30, 4-61, 6-23, 9-75
 unary numbers, *see* integers
 uncomputability, 3-58, 4-61–4-66, 4-70,
 9-46
 undecidability, *see* uncomputability
 underflow, 2-20
 Unicode, 9-30
 uniform distribution, 10-8, 10-16 ff.
 unigrams, 10-48
 union (of sets), 2-33
 Union Bound, 9-6
 unit vector, 2-53
 universal quantifier (\forall), 3-42 ff.
 unsatisfiability, 3-23
 URL squatting, 9-52
 vacuous quantification, 3-52
 valid inference, 4-75
 van Emde Boas trees, 6-71
 variance, 10-72 ff.
 Vector Space Model, 2-61
 vectors, 2-51 ff.
 dot product, 2-53 ff.
 Venn diagrams, 2-32
 virtual memory, 4-70
 Von Koch snowflake, 5-2, 5-10, 5-25 ff.
 Voronoi diagram, 2-66
 voting systems, 8-38
 wall clocks, 6-33
 Weizenbaum, Joseph, 12-3
 well-ordered set, 5-49
 What Three Words, 9-2
 “without loss of generality”, 4-35
 word2vec, 2-62
 World War II, 9-75, 11-18
 World-Wide Web, 11-26, 11-49
 PageRank, 11-90
 worst-case analysis, *see* running time
 xor, *see* exclusive or
 \mathbb{Z} , *see* integers
 \mathbb{Z}_n , 7-43 ff.
 zero (of a binary operator), 3-19, 5-59
 zzyzvas, 8-7

References

- [1] Harold Abelson and Gerald Jay Sussman with Julie Sussman. *Structure and Interpretation of Computer Programs*. MIT Press/McGraw-Hill, 2nd edition, 1996.
- [2] David Abraham, Avrim Blum, and Tuomas Sandholm. Clearing algorithms for barter exchange markets: Enabling nationwide kidney exchanges. In *Proceedings of the 8th ACM Conference on Electronic Commerce*, pages 295–304, 2007.
- [3] A. Adelson-Velskii and E. M. Landis. An algorithm for the organization of information. *Proceedings of the USSR Academy of Sciences*, 146:263–266, 1962.
- [4] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in P. *Annals of Mathematics*, 160:781–793, 2004.
- [5] Alfred V. Aho, Monica S. Lam, Ravi Sethi, and Jeffrey D. Ullman. *Compilers: Principles, Techniques, and Tools*. Prentice Hall, 2nd edition, 2006.
- [6] Martin Aigner and Günter Ziegler. *Proofs from The Book*. Springer, 4th edition, 2009.
- [7] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner. Machine bias. *ProPublica*, 23 May 2016.
- [8] Kenneth Appel and Wolfgang Haken. Solution of the four color map problem. *Scientific American*, 237(4):108–121, October 1977.
- [9] David Appell. The sun will eventually engulf Earth—maybe. *Scientific American*, September 2008.
- [10] Kenneth Arrow. *Social Choice and Individual Values*. Wiley, 1951.
- [11] Frank Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.
- [12] Shai Avidan and Ariel Shamir. Seam carving for content-aware image resizing. In *ACM SIGGRAPH*, 2007.
- [13] Jon Louis Bentley, Dorothea Haken, and James B. Saxe. A general method for solving divide-and-conquer recurrences. *ACM SIGACT News*, 12(3):36–44, 1980.
- [14] Ambrose Bierce. *The Devil’s Dictionary*. Neale, New York, 1911.
- [15] Burton Bloom. Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426, July 1970.
- [16] Paul Boersma and David Weenink. Praat: doing phonetics by computer. <http://www.praat.org>, 2012. Version 5.3.22.
- [17] Tolga Bolukbasi, Kai-Wei Chang, James Zou, Venkatesh Saligrama, and Adam Kalai. Man is to computer programmer as woman is to homemaker? Debiasing word embeddings. In *Proceedings of the 29th International Conference on Neural Information Processing Systems*, volume 29, pages 4349–4357, 2016.
- [18] Katy Börner. *Atlas of Science: Visualizing What We Know*. MIT Press, 2010.

12-16 References

- [19] Otakar Borůvka. O jistém problému minimálním. *Práce Moravské Přírodovědecké Společnosti*, 3(3):37–58, 1926.
- [20] Prosenjit Bose, Hua Guo, Evangelos Kranakis, Anil Maheshwari, Pat Morin, Jason Morrison, Michiel Smid, and Yihui Tang. On the false-positive rate of Bloom filters. *Information Processing Letters*, 108(4):210–213, 2008.
- [21] Sergei Brin and Larry Page. The anatomy of a large-scale hypertextual web search engine. In *7th International World-Wide Web Conference*, pages 107–117, 1998.
- [22] Andrei Broder, Ravi Kumar, Farzin Maghoul, Prabhakar Raghavan, Sridhar Rajagopalan, Raymie Stata, Andrew Tomkins, and Janet Wiener. Graph structure in the web. *Computer Networks*, 33(1–6):309–320, 2000.
- [23] Stephen Boudiansky. *Journey to the Edge of Reason: The Life of Kurt Gödel*. Oxford University Press, 2021.
- [24] Joy Buolamwini and Timnit Gebru. Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on Fairness, Accountability and Transparency*, pages 77–91, 2018.
- [25] Aylin Caliskan, Joanna J. Bryson, and Arvind Narayanan. Semantics derived automatically from language corpora contain human-like biases. *Science*, 356(6334):183–186, 2017.
- [26] Murray Campbell, A. Joseph Hoane Jr., and Feng-hsiung Hsu. Deep Blue. *Artificial Intelligence*, 134:57–83, 2002.
- [27] Dorwin Cartwright and Frank Harary. Structural balance: a generalization of Heider’s theory. *Psychological Review*, 63(5):277–293, 1956.
- [28] Alhaji Cherif, Nadja Grobe, Xiaoling Wang, and Peter Kotanko. Simulation of pool testing to identify patients with coronavirus disease 2019 under conditions of limited test availability. *JAMA Network Open*, 3(6):e2013075–e2013075, June 2020.
- [29] Ken Christensen, Allen Roginsky, and Miguel Jimeno. A new analysis of the false positive rate of a Bloom filter. *Information Processing Letters*, 110:944–949, 2010.
- [30] Edgar F. Codd. A relational model of data for large shared data banks. *Communications of the ACM*, 13(6):377–387, 1970.
- [31] Stephen Cook. The complexity of theorem proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, pages 151–158, 1971.
- [32] James W. Cooley and John W. Tukey. An algorithm for the machine calculation of complex Fourier series. *Mathematics of Computation*, 19(90):297–301, 1965.
- [33] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms*. MIT Press, 3rd edition, 2009.
- [34] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, 1991.
- [35] Jeffrey Dastin. Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*, 10 October 2018.
- [36] Mark de Berg, Marc van Kreveld, Mark Overmars, and Otfried Schwarzkopf. *Computational Geometry*. Springer-Verlag, 2nd edition, 2000.
- [37] Jeffrey Dean and Sanjay Ghemawat. MapReduce: simplified data processing on large clusters. *Communications of the ACM*, 51(1):107–113, 2008.
- [38] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, pages 644–654, November 1976.
- [39] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion

References 12-17

- router. Technical report, Naval Research Lab Washington DC, 2004.
- [40] Robin Dunbar. *How Many Friends Does One Person Need?: Dunbar's Number and Other Evolutionary Quirks*. Harvard University Press, 2010.
- [41] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference*, pages 265–284, 2006.
- [42] Cynthia Dwork and Aaron Roth. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3–4):211–407, 2014.
- [43] David A. Easley and Jon M. Kleinberg. *Networks, Crowds, and Markets: Reasoning About a Highly Connected World*. Cambridge University Press, 2010.
- [44] Michael Eisen. Amazon's \$23,698,655.93 book about flies. it is NOT junk blog, April 2011. <https://www.michael Eisen.org/blog/?p=358>, retrieved 16 August 2021.
- [45] Jacob Eisenstein. *Introduction to Natural Language Processing*. MIT press, 2019.
- [46] Scott L. Feld. Why your friends have more friends than you do. *American Journal of Sociology*, 96(6):1464–1477, May 1991.
- [47] Judith Flanders. *A Place for Everything: The Curious History of Alphabetical Order*. Basic Books, 2020.
- [48] Robert W. Floyd. Assigning meanings to programs. In *Proceedings of Symposia in Applied Mathematics XIX*, American Mathematical Society, pages 19–32, 1967.
- [49] Simpson Garfinkel. History's worst software bugs. *Wired Magazine*, 2005.
- [50] W. H. Gates and C. H. Papadimitriou. Bounds for sorting by prefix reversals. *Discrete Mathematics*, 27:47–57, 1979.
- [51] Alexander George. Letter to the editor. *The New Yorker*, page 12, 24 December 2007.
- [52] Oded Goldreich. *Foundations of Cryptography*. Cambridge University Press, 2006.
- [53] R. W. Hamming. Error detecting and error correcting codes. *The Bell System Technical Journal*, XXIX(2):147–160, April 1950.
- [54] Kashmir Hill. Wrongfully accused by an algorithm. *The New York Times*, 24 June 2020.
- [55] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–585, October 1969.
- [56] Douglas Hofstadter. *Gödel, Escher, Bach: An Eternal Golden Braid*. Vintage, 1980.
- [57] Douglas Hofstadter. *Le Ton Beau de Marot: In Praise of the Music of Language*. Basic Books, 1998.
- [58] Michael Huber and V. Frederick Rickey. What is 0^0 ? *Convergence*, July 2012. <https://www.maa.org/press/periodicals/convergence/what-is-00>.
- [59] David A. Huffman. A method for the construction of minimum-redundancy codes. *Proceedings of the IRE*, 40(9):1098–1101, 1952.
- [60] G. E. Hughes and M. J. Cresswell. *A New Introduction to Modal Logic*. Routledge, 1996.
- [61] John F. Hughes, Andries van Dam, Morgan McGuire, David F. Sklar, James D. Foley, Steven K. Feiner, and Kurt Akeley. *Computer Graphics: Principles and Practice*. Addison-Wesley, 3rd edition, 2013.
- [62] Tobias Isenberg, Knut Hartmann, and Henry König. Interest value driven adaptive subdivision. In *Simulation and Visualisation (SimVis)*, pages 139–149. SCS European Publishing House, 2003.

12-18 References

- [63] P. Jaccard. Distribution de la flore alpine dans le bassin des dranses et dans quelques régions voisines. *Bulletin de la Société Vaudoise des Sciences Naturelles*, 37:241–272, 1901.
- [64] Karen Spärck Jones. A statistical interpretation of term specificity and its application in retrieval. *Journal of Documentation*, 28:11–21, 1972.
- [65] Richard Jones. *Garbage Collection: Algorithms for Automatic Dynamic Memory Management*. Wiley, 1996.
- [66] Daniel Jurafsky and James H. Martin. *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition*. Pearson Prentice Hall, 2nd edition, 2008.
- [67] Frank Kafka. “Fürsprecher” [“Advocates”], c. 1922. Translation by Tania and James Stern. Available in *Franz Kafka: The Complete Stories*. Edited by Nahum Glatzer. New York: Schocken, 1971, pp. 449–451.
- [68] Richard M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85–103. Springer, 1972.
- [69] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC Press, 2007.
- [70] Stefanos Kaxiras and Margaret Martonosi. *Computer Architecture Techniques for Power-Efficiency*. Morgan Claypool, 2008.
- [71] Alfred B. Kempe. On the geographical problem of the four colours. *American Journal of Mathematics*, 2(3):193–200, 1879.
- [72] Donald E. Knuth. *The Art of Computer Programming: Seminumerical Algorithms (Volume 2)*. Addison-Wesley Longman, 3rd edition, 1997.
- [73] Dexter Kozen. *Automata and Computability*. Springer, 1997.
- [74] Joseph Kruskal. On the shortest spanning subtree of a graph and the traveling salesman problem. *Proceedings of the American Mathematical Society*, 7:48–50, 1956.
- [75] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach*. Addison-Wesley, 6th edition, 2013.
- [76] Jure Leskovec, Anand Rajaraman, and Jeff Ullman. *Mining of Massive Datasets*. Cambridge University Press, 2nd edition, 2014.
- [77] Nancy Leveson. *Safeware*. Pearson, 1995.
- [78] Nancy Leveson. *Engineering a Safer World*. MIT Press, 2016.
- [79] Leonid Levin. Universal search problems. *Problems of Information Transmission*, 9(3):265–266, 1973.
- [80] J. L. Lions. Ariane 5 flight 501 failure report: Report by the enquiry board, 1996.
- [81] Elisha Scott Loomis. *The Pythagorean Proposition*. National Council of Teachers of Mathematics, June 1968.
- [82] Joel Lovell. Left-hand-turn elimination. *The New York Times*, 9 December 2007.
- [83] David J. C. MacKay. *Information Theory, Inference and Learning Algorithms*. Cambridge University Press, 2003.
- [84] Christopher D. Manning, Prabhakar Raghavan, and Hinrich Schütze. *Introduction to Information Retrieval*. Cambridge University Press, 2008.
- [85] Steve Martin. *Born Standing Up: A Comic’s Life*. Simon & Schuster, 2008.
- [86] N. David Mermin. *Quantum Computer Science: An Introduction*. Cambridge University Press, 2007.
- [87] Tomas Mikolov, Ilya Sutskever, Kai Chen, Greg Corrado, and Jeffrey Dean. Distributed representations of words and phrases and their compositionality. In *Proceedings of the 26th International Conference on Neural*

References 12-19

- Information Processing Systems*, pages 3111–3119, 2013.
- [88] Stanley Milgram. The small world problem. *Psychology Today*, 1:61–67, May 1967.
- [89] Gary L. Miller. Riemann’s hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13(3):300–317, 1976.
- [90] Michael Mitzenmacher and Eli Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005.
- [91] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8):114–117, April 1965.
- [92] Gordon E. Moore. No exponential is forever: but “forever” can be delayed! In *International Solid-State Circuits Conference*, pages 20–23, 2003.
- [93] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, 1995.
- [94] National Academies of Sciences, Engineering, and Medicine. *Securing the Vote: Protecting American Democracy*. National Academies Press, 2018.
- [95] Sydney Padua. *The Thrilling Adventures of Lovelace and Babbage: The (Mostly) True Story of the First Computer*. Pantheon Books, 2015.
- [96] Christos H. Papadimitriou. *Computational Complexity*. Addison Wesley, 1994.
- [97] David A. Patterson and John L. Hennessy. *Computer Organization and Design: the Hardware/Software Interface*. Morgan Kaufmann, 4th edition, 2008.
- [98] Nick Paumgard. The names. *The New Yorker*, 16 May 2011.
- [99] Caroline Criado Perez. *Invisible Women: Exposing Data Bias in a World Designed for Men*. Random House, 2019.
- [100] Ivars Peterson. MathTrek: Pentium bug revisited. *MAA Online*, May 1997.
- [101] Madsen Pirie. *How to Win Every Argument: The Use and Abuse of Logic*. Continuum, 2007.
- [102] George Pólya. *How to Solve It*. Doubleday, 1957.
- [103] William Press, Saul Teukolsky, William Vetterling, and Brian Flannery. *Numerical Recipes*. Cambridge University Press, 3rd edition, 2007.
- [104] Richard Preston. The Ebola wars. *The New Yorker*, 27 October 2014.
- [105] Michael O. Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12(1):128–138, 1980.
- [106] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, February 1978.
- [107] Tomas Rokicki, Herbert Kociemba, Morley Davidson, and John Dethridge. The diameter of the Rubik’s cube group is twenty. *SIAM Review*, 56(4):645–670, 2014.
- [108] Mike Rosulek. *The Joy of Cryptography*. Oregon State, 2020.
- [109] Walter Rudin. *Principles of Mathematical Analysis*. McGraw–Hill, 3rd edition, 1976.
- [110] Stuart Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Prentice Hall, 3rd edition, 2009.
- [111] R. M. Sainsbury. *Paradoxes*. Cambridge University Press, 3rd edition, 2009.
- [112] Jonathan Schaeffer, Neil Burch, Yngvi Bjornsson, Akihiro Kishimoto, Martin Muller, Rob Lake, Paul Lu, and Steve Sutphen. Checkers is solved. *Science*, 317(5844):1518–1522, 14 September 2007.
- [113] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

12-20 References

- [114] Claude E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.
- [115] Margot Lee Shetterly. *Hidden Figures: The American Dream and the Untold Story of the Black Women Who Helped Win the Space Race*. William Morrow and Company, 2016.
- [116] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999.
- [117] Avi Silberschatz, Henry F. Korth, and S. Sudarshan. *Database System Concepts*. McGraw-Hill, 6th edition, 2010.
- [118] Simon Singh. *The Code Book: The Secret History of Codes and Code-breaking*. Fourth Estate Ltd., 1999.
- [119] Simon Singh. *Fermat’s Last Theorem: The Story of a Riddle That Confounded the World’s Greatest Minds for 358 Years*. Fourth Estate Ltd., 2002.
- [120] Michael Sipser. *Introduction to the Theory of Computation*. Course Technology, 3rd edition, 2012.
- [121] Laura Stark. *Behind Closed Doors: IRBs and the Making of Ethical Research*. University of Chicago, 2011.
- [122] Tom Stoppard. *Rosencrantz and Guildenstern are Dead*. Grove/Atlantic, Inc., 1967.
- [123] Latanya Sweeney. Simple demographics often identify people uniquely. Data Privacy Working Paper, Carnegie Mellon University, 2000.
- [124] T. Taylor, G. VanDyk, L. Funk, R. Hutcheon, and S. Schriber. Therac 25: A new medical accelerator concept. *IEEE Transactions on Nuclear Science*, 30(2):1768–1771, 1983.
- [125] Amanda L. Traud, Peter J. Mucha, and Mason A. Porter. Social structure of Facebook networks. *CoRR*, abs/1102.2166, 2011.
- [126] A. M. Turing. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1):230–265, 1937.
- [127] Marilyn vos Savant. Ask Marilyn. *Parade Magazine*, 9 September 1990.
- [128] Marilyn vos Savant. Ask Marilyn. *Parade Magazine*, 2 December 1990.
- [129] Joseph Weizenbaum. ELIZA: a computer program for the study of natural language communication between man and machine. *Communications of the ACM*, 9(1):36–45, January 1966.
- [130] Joseph Weizenbaum. *Computer Power and Human Reason: From Judgment to Calculation*. W. H. Freeman & Co, 1976.
- [131] Virginia Vassilevska Williams. An overview of the recent progress on matrix multiplication. *ACM SIGACT News*, 43(4), December 2012.
- [132] Wayne Zachary. An information flow model for conflict and fission in small groups. *Journal of Anthropological Research*, 33(4):452–473, 1977.
- [133] Jieyu Zhao, Tianlu Wang, Mark Yatskar, Vicente Ordonez, and Kai-Wei Chang. Men also like shopping: Reducing gender bias amplification using corpus-level constraints. In *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*, pages 2979–2989, 2017.
- [134] Jacob Ziv and Abraham Lempel. A universal algorithm for sequential data compression. *IEEE Transactions on Information Theory*, 23(3):337–343, 1977.

