Index

2–3 and 2–3–4 trees, 261
9/11 Memorial, 600
123456791, 378
987654263, 378

∀ (universal quantifier), 111 ff.
absolute value, 9, 170, 172
abstract algebra, 362
abstraction, 144
ACM Code of Ethics and Professional Conduct, 659
ACM Conference on Fairness, Accountability, and Transparency, 399
adjacency, *see* graphs
affirming the consequent, *see* fallacy
algorithmic bias, 53, 210, 399, 658
algorithmic sentencing, 399
algorithms, 70 ff., *see also* randomized algorithms
  asymptotic analysis, 283 ff.
  brute force, 104, 229, 440, 496
  divide and conquer, 314 ff., 321
  dynamic programming, 229, 440, 496
  greedy algorithms, 165, 455
  recurrence relations, 300 ff.
  time, space, and power, 292
Alice and Bob, 371 ff.
ambiguity
  in natural language, 86, 87, 92
  order of operations, 259, 389
  order of quantification, 129 ff., 139
  prefix-free/Huffman codes, 455
analysis (mathematics), 421
ancestors (in a tree), 628
and (∧), 83
anonymization, 521
antisymmetry, 404 ff.
approximate equality, 9
Ariane 5 rocket, 207
arithmetic mean, 182, 199
arithmetic series, 17, 226, 233
Arrow's Theorem, 414
artificial intelligence, 659
  computer vision, 608
  game trees, 121, 478
assertions, 137, 231
associativity, 99, 261, 362
assuming the antecedent, *see* proofs
asymmetry, 404 ff.
asymptotics
  analysis of algorithms, 283 ff.
  asymptotic analysis, 269 ff.
  asymptotic relationships viewed as relations, 408 ff.
  best- and average-case running time, 289 ff.
  divide and conquer, 314 ff.
  O (Big O), 269 ff.
  o, Ω, ω, and Θ, 274 ff.
  polynomials, logs, and exponentials, 273 ff.
  recurrence relations, 300 ff.
  worst-case analysis, 284 ff.
automata, 430, 479
automated theorem proving, 167
average distance in a graph, 621
average-case analysis, *see* running time
AVL trees, 309 ff.
axiom of extensionality, 32

Bacon, Kevin, 180, 593
balanced binary search trees, 309
Bayes' Rule, 540 ff.
begging the question, *see* fallacy
Bernoulli distribution, 518 ff., 552, 563
Bernoulli's inequality, 235
betweenness, 396
BFS, *see* breadth-first search
bias, *see* algorithmic bias
biased coins, 518 ff.
big O, big Ω, and big Θ, 269 ff., 408 ff.
bigrams, 543
bijections, 67, 465, 474
binary numbers, *see* integers
binary relation, *see* relations
Binary Search, *see* searching
binary search trees, *see* trees
binary symmetric channel, 539, 540
binary trees, *see* trees
binomial coefficients, *see* combinations
binomial distribution, 519 ff., 556
Binomial Theorem, 490 ff.
bipartite graphs, 594 ff.
  complete bipartite graphs, 595
birthday paradox, 242, 559
Bitcoin, 658
bitmaps, 49
bits/bitstrings, 7, 45, 94, 146 ff., 371, 442, 466, 482 ff., 500
Bletchley Park, 497
blockchain, 658
Bloom filters, 547
Bob smells, 232
Booleans, 7, 83, *see also* logic
bound (vs. free) variables, 114, 122
breadth-first search, 612 ff.
  finding cycles, 625
brute force, *see* algorithms
Bubble Sort, *see* sorting
Buffon's needle, 566
bugs, 21, 207, 231, 605
butterfly ballots, 414

C (programming language), 105, 122, 251
Caesar cipher, *see* cryptography
cardinality, 26–27, 441 ff.
  infinite, 474
Carmichael numbers, 367, 368, 370
Cartesian plane, 44
Cartesian product (×), 42
catchphrase, 415, 642
Cauchy sequences, 421
ceiling, 9
cellular automata, 479
Chain Rule (probability), 538 ff.
change of index, 17
checkers, 121, 181, 462
checksum, 145, 154
chess, 42, 121, 234, 451, 460, 611
children (in a tree), 628
Chinese Remainder Theorem, 351 ff.
circle packing, 159
circuits, 80, 94
  printing and planar graphs, 597
  representing logical propositions, 100, 107
  using nand gates, 188
class-size paradox, 552

cliques, 593 ff.
closure, 362, 409 ff.
clustering, 38
coarsening equivalence relations, 421 ff.
codomain (of a function), 61
collaboration networks, 593
collaborative filtering, 40
combinations, 482 ff.
  k-combinations, 485 ff.
  Binomial Theorem, 490 ff.
  Pascal's identity, 489, 493
  Pascal's triangle, 493
combinatorial proof, 488 ff.
commutativity, 51, 99, 130, 261, 362
comparability, *see* partial orders
comparison-based sorting, *see* sorting
compilers, 60, 105, 259
complement (of a set), 30
complete graphs, 593 ff.
complexity, *see* computational complexity
composite numbers, 15, *see also* prime numbers
composition
  of functions, 64, 395
  of relations, 391, 407
compression
  entropy and compressibility, 523
  Huffman coding, 455, 475
  impossibility of lossless compression, 475
  lossy vs. lossless, 475
  quantization of images, 60, 73
  URL shortening, 445
computability, 192
computational biology
  genome rearrangements, 137, 479
  motifs in gene networks, 592
computational complexity
  and cryptography, 378
  complexity classes, 294
  graph isomorphism, 591
  input size, 332
  P vs. NP, 104
  regular languages, 415, 430
computational geometry, 56
computational linguistics, *see* natural language processing
computer architecture, 101 ff., 188
  and running times, 284
  Moore's Law, 279
  power consumption, 292
  representation of numbers, 21
computer graphics
  hidden-surface removal, 431
  morphing, 57
  rotation matrices, 54
  triangulation, 244
computer security, 378, 379
computer vision, 608
computing networking, 456
conditional expectation, 561 ff.
conditional independence, 537
conditional probability, 532 ff.
  Bayes' Rule, 540
  Chain Rule, 538
  Law of Total Probability, 539
Condorcet paradox, 414
congruences (modular), 332 ff., 352 ff., 420
conjunctive normal form, 101 ff., 184 ff., 256 ff.
connectivity (in graphs), 606 ff.
  connected component, 607 ff.
  reachability, 609 ff.
constructive proofs, 175
constructivism, 176
context-free grammar, 259
contradiction, 96
contrapositive, 98, 171, *see also* proofs
converse, 98
Cook–Levin Theorem, 104
correlation, 527
  correlation vs. causation, 206
  positive and negative, 530
countable sets, 474
counterexamples, 175 ff.
counting
  Binomial Theorem, 490 ff.
  combinations, 482 ff.
  combinatorial proofs, 488 ff.
  combining products and sums, 453 ff.
  Division Rule, 467 ff.
  double counting, 446 ff.
  Generalized Product Rule, 450 ff.
  Inclusion–Exclusion, 446 ff.
    for 3+ sets, 449
  Mapping Rule, 463 ff.
  order, 483 ff.
  Pascal's triangle, 493 ff.
  permutations, 484 ff.
  Pigeonhole Principle, 471 ff.
  Product Rule (sequences), 444
  repetition, 483 ff.
  Sum Rule (unions), 441
Counting Sort, *see* sorting
coupon collector problem, 570
crossword puzzles, 136
cryptography, 232, 371 ff., 414, 658
  and pseudorandomness, 517
  Caesar cipher, 372, 545
  Diffie–Hellman key exchange, 379
  digital signatures, 374
  Enigma machine and WWII, 497
  frequency analysis, 531, 545
  key exchange, 379
  man-in-the-middle attack, 379
  one-time pads, 371
  public-key cryptography, 373 ff.
  RSA cryptosystem, 197, 373 ff.
  secret sharing, 356
  substitution cipher, 530, 536, 545
Currying, 135
cycles, 424, 623 ff.
  acyclic graphs, 625 ff.
  Cycle Elimination algorithm, 634
  cycle rule for minimum spanning trees, 647
  kidney transplants, 636
  simple cycles, 624
  Weighted Cycle Elimination algorithm, 647

DAG (directed acyclic graph), 626
data mining, *see* machine learning
data privacy, 521
data visualization, 586, 600
databases, 124, 398, 401
De Morgan's Laws, 100
decision problems, 191
Deep Blue, 121
degree (in a graph), 583 ff., 585
  degree distribution, 599
  regular graphs, 596
degree (of a polynomial), 69
density (of a graph), 281, 602
denying the hypothesis, *see* fallacy
dependent events, 527 ff.
depth-first search, 615 ff.
Descartes, René, 42
descendants (in a tree), 628
deterministic finite automata, 430
DFS, *see* depth-first search
diagonalization, 474
diameter (of a graph), 620
differential privacy, 521
Diffie–Hellman key exchange, 379
Dijkstra's algorithm, 642 ff.
directed graphs, 402
disconnected, *see* connectivity in graphs
disjoint sets, 34, 159
disjunctive normal form, 101 ff., 184 ff., 256 ff.
distance, *see also* metrics
  Euclidean, *see* Euclidean distance
  Hamming, *see* Hamming distance

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-15049-1 — Connecting Discrete Mathematics and Computer Science
David Liben-Nowell
Index
More Information

in a graph, 611 ff.
Manhattan, *see* Manhattan distance
minimum distance of a code, 149 ff.
divide and conquer, *see* algorithms
divisibility, 14, 62, 230, 426
and modular arithmetic, 333 ff.
common divisors, 334 ff.
divisibility rules, 94, 168, 182, 342
Division Theorem, 329
division, *see* mod
in $\mathbb{Z}_n$, 361
Division Rule, 467 ff.
domain (of a function), 61
dot product, 47 ff.
Dunbar's number, 601
dynamic programming, *see* algorithms
dynamic scope, 122

∃ (existential quantifier), 111 ff.
e (base of natural logarithm), 13
edges, *see* graphs
efficiency, *see* running time, *see also* computational complexity
ELIZA, 659
Emacs, 460, 659
empty set, 30
Enigma machine, 497
entropy, 523
equivalence relations, 418 ff.
equivalence classes, 419
refinements and coarsenings, 421
Eratosthenes, 344, 358
Erdős numbers, 180
Erdős, Paul, 180, 593
error-correcting codes, 146 ff.
Golay code, 165
Hamming code, 154 ff., 463
messages and codewords, 146 ff.
minimum distance and rate, 149 ff.
Reed–Solomon codes, 161, 357
repetition code, 153 ff.
upper bounds on rates, 158
error-detecting codes, 146 ff.
credit-card numbers, 145, 162
UPC, 477
ethics, 210, 232, 319, 399, 521, 658–660
Euclid, 190, 335
Euclidean algorithm, 335, 348
efficiency, 338, 342
extended Euclidean algorithm, 348
Euclidean distance, 55, 199
Euler's Theorem, 370
even numbers, 15, 173
evenly divides, *see* divisibility
events (probability), 511 ff.
correlated, 527
independent events, 527 ff.
exclusive or (⊕), 15, 86 ff., 154 ff.
existential quantifier (∃), 111 ff.
expectation, 551 ff.
average-case analysis of algorithms, 289 ff.
conditional expectation, 561 ff.
coupon collector problem, 570
deviation from expectation, 562 ff.
Markov's inequality, 571
Law of Total Expectation, 562
linearity of expectation, 554 ff.
exponentials, 10 ff., 261
asymptotics, 273 ff.
modular, 342
EXPSPACE (complexity class), 294
EXPTIME (complexity class), 294
extended Euclidean algorithm, 348

facial recognition, 210, 399, 658
factorial, 166–167, 229, 300, 302, 452, 458
Stirling's approximation, 501
factors, *see* divisibility, *see also* prime factorization
fallacy, 201 ff.
affirming the consequent, 203
begging the question, 205
denying the hypothesis, 204
false dichotomy, 170, 204
proving true, 203
false dichotomy, *see* fallacy
Fast Fourier transform, 11
fencepost error, 605
Fermat pseudoprime, 367
Fermat's Last Theorem, 365
Fermat's Little Theorem, 365 ff.
Fermat–Euler Theorem, 370
Fibonacci numbers, 58, 247, 301, 306–308, 310, 500
algorithms, 312
and the Euclidean algorithm, 342
`filter`, 37
finite-state machines, 430
float (floating-point number), 21, 284
floor, 9
Division Theorem, 329
for loops
analogy for $\prod$, 20
analogy for $\sum$, 16, 18
analogy for quantifiers, 113, 130, 139
forests, 626
spanning forests, 634
formal language theory, 415, *see* computational complexity
formal methods, 167, 409
Four-Color Theorem, 181, 597
fractals, 216, 222–224, 234, 248
free (vs. bound) variables, 114, 122
frequency analysis, 531
functions, 59 ff.
algorithms, 70 ff.
characteristic function of a set, 389
composition, 63
domain/codomain, 61
growth rates, 269 ff.
inverses, 67
one-to-one/onto functions, 65 ff.
range/image, 62 ff.
viewed as relations, 394 ff.
visual representation, 63
vs. macros, 122
Fundamental Theorem of Arithmetic, 346
fuzzy logic, 92

Game of Life, 479
game trees, 121, 478
garbage collection, 293, 619
Gates, Bill, 137, 180
GCD, *see* greatest common divisor
GCHQ, 373
Generalized Product Rule, 450 ff.
geometric distribution, 520 ff., 554
geometric mean, 182, 199
geometric series, 17, 224 ff.
for recurrence relations, 314 ff.
infinite, 225
giant component, 618
Gödel's Incompleteness Theorem, 123
Goldbach's conjecture, 81, 128, 138
golden ratio, 307, 310
grammars, 252, 259
graph drawing, 596, 600
graphs, 579 ff.
acyclic graphs, 625 ff.
adjacency lists, 586 ff.
adjacency matrices, 587 ff.
bipartite graphs, 594 ff.
breadth-first search, 612 ff.
complete graphs, 593 ff.
connected components, 607 ff.
connectivity, 606 ff.
cycles, 623 ff.
data structures, 586 ff.
degree, 583, 585 ff.
handshaking lemma, 584
regular graphs, 596
density, 602

© in this web service Cambridge University Press & Assessment www.cambridge.org

  depth-first search, 615 ff.
  forests, 626
  isomorphism, 590 ff.
  matchings, 470, 478, 497, 596, 636
  neighborhoods, 581 ff., 585 ff.
  paths, 605 ff.
    shortest paths, 611 ff.
  planar graphs, 596 ff.
  shortest paths
    Dijkstra's algorithm, 642 ff.
  simple graphs, 580
  subgraphs, 591 ff.
  trees, *see* trees
  undirected vs. directed, 579 ff.
  weighted graphs, 641 ff.
    Dijkstra's algorithm, 642 ff.
grayscale, 6, 60, 107
greatest common divisor, 334 ff., *see also* Euclidean algorithm

H_n, *see* harmonic number
halting problem, 123, 194 ff., 198
Hamiltonian path, 620
Hamming code, 58, 154 ff., 477
  number of valid codewords, 463
Hamming distance, 146
handshaking lemma, 584
harmonic number, 226–227, 234
hashing, 72, 480, 507–508, 557, 570
  Bloom filters, 547
  chaining, 72
  collisions, 72, 507 ff., 515, 525, 546, 558
    and pairwise independence, 532
    chaining, 507
    clustering, 515, 525
    double hashing, 526
    linear probing, 515, 525
    quadratic probing, 526
  simple uniform hashing, 508
Hasse diagrams, 425
heaps, 74, 245, 261
heavy-tailed distribution, 599
height (of a tree), 630
Heron's method, 22, 182
hidden-surface removal, 431
higher-order functions, 37, 135
Hopper, Grace Murray, 60, 207
Huffman coding, 455, 475
hypercube, 603

I (identity matrix), 49
idempotence, 99
identity
  identity function, 68
  identity matrix, 49
  multiplicative identity, 361
  of a binary operator, 93, 261
if and only if ($\Leftrightarrow$), 87 ff.
image (of a function), 62
image processing
  blur filter, 22
  dithering, 107
  grayscale conversion, 6
  quantization, 60
  seam carving, 496
  segmentation, 608
imaginary numbers, 11
implication ($\Rightarrow$), 84 ff.
in-degree, *see* degree
in-neighbor, *see* neighbors (in graphs)
Inclusion–Exclusion, 446 ff., 501
inclusive naming, 319
incomparability, 277, 423
incompleteness (logic), 123
inconsistency (logic), 123
independent events, 527 ff.
  pairwise independence, 532
indicator random variables, 550
induction, *see* proofs
  checklist for inductive proofs, 219
  generating conjectures, 222
  proofs about algorithms, 228 ff., 303 ff.
  strengthening the inductive hypothesis, 256
infinite sequences, 17, 225
infix notation, 389
information retrieval, 53
information theory, 523, 539
injective functions, *see* one-to-one functions
Insertion Sort, *see* sorting
integers, 7 ff.
  algorithms for arithmetic, 331, 341
    efficiency, 332
  division, *see* modular arithmetic
  primes and composites, *see* prime numbers
  recursive definition, 258
  representation
    binary numbers, 94, 220, 236, 246, 332, 340
    different bases, 246, 340
    `ints`, 21
    modular representation, 355
    unary, 332
  successor relation, 413
internet addresses, 456
intersection (of sets), 31
intervals, *see* real numbers
invalid inference, 201
inverse
  additive, 369
  multiplicative, 361 ff.
  of a function, 67
  of a matrix, 58
  of a relation, 390 ff., 406
  of an implication, 98
IP addresses, 456
irrationals, *see* rationals
  irrationality of $\sqrt{2}$, 174
irreflexivity, 403 ff.
isomorphism (of graphs), 590 ff.

Jaccard coefficient, 40
Java (programming language), 61, 88, 105, 619
Johnson's algorithm, 572
join (database operation), 398

$\mathcal{K}_n$, *see* complete graphs
$\mathcal{K}_{n,n}$, *see* bipartite graphs
Kasparov, Garry, 121
Keller, Mary Kenneth, 201
keyspace, *see* hashing
kidney transplants, 636, 658
Knuth, Donald, 336
Kruskal's algorithm, 648
Kuratowski's Theorem, 598

L (complexity class), 294
latchstring, 415, 642
Law of the Excluded Middle, 95
Law of Total Expectation, 562
Law of Total Probability, 539
least common multiple, 334 ff.
length (of a vector), 46
lexical scope, 122
lexicographic ordering, 127, 389
Liar's paradox, 29, 195
linearity of expectation, 554
linked lists, 260
  adjacency lists for graphs, 586 ff.
  as graphs, 602
  recursive definition, 250
list, *see* sequence
little o and little ω, 274 ff., 408 ff.
logarithms, 12–13
  asymptotics, 273 ff.
  discrete logarithm, 379
  polylogarithmic functions, 281, 332
logic
  Boolean logic, 7, 362
  consistency, 123
  fuzzy logic, 92

incompleteness, 123
logical equivalence, 97, 115
logical fallacy, *see* fallacy
modal logic, 409
predicate logic, 109 ff.
games against the demon, 132
nested quantifiers, 127 ff.
order of quantification, 128 ff.
predicates, 109 ff.
quantifiers, 111 ff.
theorems in predicate logic, 115 ff.
propositional logic, 81 ff.
atomic vs. compound propositions, 82
logical connectives, 83 ff.
propositions, 81 ff.
recursive definition of a well-formed formula, 252
satisfiability, 96
tautology, 95 ff.
truth assignment, 89
truth tables, 89 ff.
truth values, 81, 252
universal set of operators, 199
temporal logic, 409
longest common subsequence, 229, 501
loop invariants, 231
Lovelace, Ada, 22, 42

machine learning
bias, 53
classification problems, 464, 544
clustering, 38
cross-validation, 500
macros, 122
Manhattan distance, 46, 55, 199
`map`, 37
Mapping Rule, 463 ff.
MapReduce, 37
maps, 181, 597
mark-and-sweep, 619
Markov's inequality, 571
matchings, *see* graphs
matrices, 48 ff.
adjacency matrices for graphs, 587 ff.
identity matrix, 49
inverse of a matrix, 58
matrix multiplication, 50 ff.
Strassen's algorithm, 321
rotation matrices, 54, 200
term–document matrix, 53
maximal element, 425 ff.
maximum element, 32, 71, 425 ff.
mazes, 616
median (of an array), 74, 567 ff.
memoization, 496
memory management, 619
Merge Sort, *see* sorting
metrics, 146, 162–163, 621
Milgram, Stanley, 180
Miller–Rabin test, 197, 368
minimal element, 425 ff.
minimum element, 32, 425 ff.
minimum spanning trees, 646 ff.
cycle rule, 647
Kruskal's algorithm, 648
Weighted Cycle Elimination algorithm, 647
ML (programming language), 135, 256
modal logic, 409
modular arithmetic, 13–14, 329 ff.
Division Theorem, 329
mod-and-div algorithm, 331 ff., 341
modular congruences, 332
modular exponentiation, 342
modular products, 333
modular sums, 333
multiplicative inverse, 361 ff.
primitive roots, 379
Modus Ponens, 96
Modus Tollens, 96
Monte Carlo method, 566
Monty Hall Problem, 516
Moore's Law, 279
multiples, *see* divisibility
multiplicative identity, 361
multiplicative inverse, 361 ff.
multitasking, 293

naïve Bayes classifier, 544
nand (not and), 188, 261
n-ary relations, 395 ff.
expressing n-ary relations as binary relations, 397
natural language processing, 659
ambiguity, 92
language model, 543
speech processing, 38, 462
speech recognition, 543
text classification, 544
text-to-speech systems, 462
natural logarithm, *see* logarithms
neighbors (in graphs), 581, 585
nested quantifiers, 127 ff.
games against the demon, 132
negations, 130
order of quantification, 128 ff.
nested sums, 18, 555
Newton's method, 22
nodes, *see* graphs
nonconstructive proofs, 175
nor (not or), 188, 261
not (¬), 59, 83
NP (complexity class), 104, 204, 294
number line, 9
number theory, *see* modular arithmetic
numerical methods, *see* scientific computing

O (Big O), 269 ff., 408 ff.
o (little o), 274, 408 ff.
odd numbers, 15
off-by-one error, 605
Omega (Ω) (asymptotics), 274, 408 ff.
omega (ω) (asymptotics), 274, 408 ff.
one-time pads, 371
one-to-one functions, 66, 395, 465
onion routing, 232
onto functions, 65, 127, 395, 465
operating systems, 136
multitasking, 293
virtual memory, 198
optimizing compilers, 105, 107
or (∨), 83
order of operations, *see* precedence of operators
orders, *see* partial orders
organ donation, 636
out-degree, *see* degree
out-neighbor, *see* neighbors (in graphs)
outcome (probability), 509
overfitting, 543
overflow, 21, 207

$\mathscr{P}$, *see* power set
P (complexity class), 104, 204, 294
PageRank, 650
painter's algorithm, 431
pairwise independence, 532
palindromes, 262, 476
paradoxes
birthday paradox, 559
class-size paradox, 552
Liar's paradox, 29, 195
nontransitive dice, 569
paradoxes of translation, 82
Russell's paradox, 29
Simpson's paradox, 210
voting paradoxes, 414
parallel edges, 580
parent (in a tree), 628
parity, 15, 154 ff., 238–239, 246
parsing, 259
partial orders, 422 ff.
chains and antichains, 434

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-15049-1 — Connecting Discrete Mathematics and Computer Science
David Liben-Nowell
Index
More Information

- comparability, 423
- extending to a total order, 427 ff.
- Hasse diagrams, 425
- immediate successors, 425
- minimal/maximal elements, 425
- minimum/maximum element, 425
- strict partial order, 422
- topological ordering, 427 ff.
- total orders, 423
  - consistency with a partial order, 427 ff.

partition (of a set), 35
- bipartite graphs, 594
- equivalence relations, 420

Pascal's identity, 489, 493
Pascal's triangle, 493 ff.
paths (in graphs), 605 ff.
- breadth-first search, 612 ff.
- connected graphs, 606 ff.
- depth-first search, 615 ff.
- Dijkstra's algorithm, 642 ff.
- internet routing, 456
- shortest paths, 611 ff.
- simple paths, 606

Peirce's arrow (↓), 188, 261
Pentium chip, 207, 279
perfect matchings, *see* graphs
perfect numbers, 24
perfect square, 11
Perl (programming language), 190
permutations, 249, 452, 458
- k-permutations, 484 ff.

Petersen graph, 590, 598
Pigeonhole Principle, 471 ff., 475
planar graphs, 181, 596 ff.
- Kuratowski's Theorem, 598

polygons, 54, 236, 240, 244, 248, 566
polylogarithmic, 281, 332
polynomials, 68 ff., 161, *see also* P (complexity class)
- asymptotics, 273 ff.
- evaluating modulo a prime, 346, 356, 357

postfix notation, 389
Postscript (programming language), 389
power set, 36
- as a relation, 388
- cardinality, 466

power-law distribution, 599
powers, *see* exponentials
precedence of operators, 31, 88, 113, 259
predicate logic, *see* logic
predicates, 109 ff., 389, *see also* logic
prefix notation, 389
prefix-free codes, 454
preorder, 424
prime numbers, 15, 192, 343 ff.
- Carmichael numbers, 367, 370
- distribution of the primes, 344
- infinitude of primes, 190
- primality testing, 190, 197, 283, 343
  - efficient algorithms, 368
- prime factorization, 346, 378
  - cryptography, 197, 378
  - existence of, 239–240
  - Shor's algorithm, 522
  - uniqueness of, 349–351
- Prime Number Theorem, 344
- Sieve of Eratosthenes, 344, 358

priority queues, 245
privacy, 232, 521, 658
probability
- Bayes' Rule, 540 ff.
- conditional expectation, 561 ff.
- conditional probability, 532 ff.
- coupon collector problem, 570
- events, 511 ff.
- expectation, 551 ff.
- infinitesimal probabilities, 535
- Law of Total Expectation, 562
- Law of Total Probability, 539
- linearity of expectation, 554 ff.
- Markov's inequality, 571
- Monty Hall Problem, 516
- outcomes, 509 ff.
- probability functions, 509 ff.
- random variables, 549 ff.
- random walks, 650
- standard deviation, 562 ff.
- tree diagrams, 514 ff.
- variance, 562 ff.

probability distributions
- Bernoulli, 518 ff.
- binomial, 519 ff.
- entropy, 523
- geometric, 520 ff.
- posterior distribution, 541
- prior distribution, 541
- uniform, 517 ff.

product, 20 ff.
- of a set, 32

product of sums, *see* conjunctive normal form
Product Rule, 444
- cardinality of S^k, 445

programming languages
- compile-time optimization, 105
- Currying, 135
- garbage collection, 293, 619
- higher-order functions, 37, 135
- parsing, 259
- scoping/functions/macros, 122
- short-circuit evaluation, 105
- syntactic sugar, 100

project (database operation), 398
proofs, 166 ff.
- by assuming the antecedent, 118, 169
- by cases, 157, 169 ff.
- by construction, 154, 175 ff.
- by contradiction, 159, 173 ff.
- by contrapositive, 171 ff.
- by induction, 70, 217 ff.
- by mutual implication, 172
- by strong induction, 237 ff.
- by structural induction, 252 ff.
- combinatorial proofs, 488 ff.
- direct, 168 ff.
- nonconstructive, 175
- strategy for proofs, 176 ff.
- unprovable true statements, 123
- without loss of generality, 170
- writing proofs, 178 ff.

proper subset and superset, 33
propositional logic, *see* logic
proving true, *see* fallacy
pseudocode, 71
pseudorandom generator, 517
PSPACE (complexity class), 294
public-key cryptography, *see* cryptography
Pythagorean Theorem, 178, 188–190, 199
- incorrect published proof, 211

Python (programming language), 21, 37, 61, 93, 94, 122, 135, 192 ff., 474, 619

$\mathbb{Q}$, *see* rationals
QR codes, 145, 161
quadtrees, 311
quantifiers, 111 ff.
- negating quantifiers, 116 ff.
- nested quantifiers, 127 ff.
- vacuous quantification, 119

quantum computation, 522
Quick Sort, *see* sorting

$\mathbb{R}$, *see* real numbers
Radix Sort, *see* sorting
raising to a power, *see* exponentials
Random Surfer Model, 650
random variables, 549 ff.
- expectation, 551 ff.
- independent random variables, 551
- indicator random variables, 550

random walks, 650, 652
randomized algorithms, 292

© in this web service Cambridge University Press & Assessment www.cambridge.org

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-15049-1 — Connecting Discrete Mathematics and Computer Science
David Liben-Nowell
Index
More Information

  - Buffon’s needle, 566
  - finding medians, 567
  - Johnson’s algorithm, 572
  - Monte Carlo method, 566
  - primality testing (Miller–Rabin), 368
  - Quick Sort, 524
- range (of a function), 62
- rate (of a code), 149 ff.
- rationals, 7 ff., 44, 169, 172, 335
  - in lowest terms, 335, 420
- real numbers, 7 ff.
  - absolute value/floor/ceiling, 9 ff.
  - approximate equality (≈), 9, 387
  - defining via infinite sequences, 421
  - exponentiation, 10 ff.
  - `floats` (representation), 21
  - intervals, 9
  - logarithms, 12 ff.
  - trichotomy, 277
- realization, *see* outcome (probability)
- recommender system, 40
- recurrence relations, 300 ff.
  - divide and conquer, 314 ff.
  - iterating, 302
  - sloppiness, 306
  - solving by induction, 302
  - variable substitution, 304
- recursion tree, 298, 314 ff.
- recursively defined structures, 250 ff.
- Reed–Solomon codes, 161, 357
- reference counting, 619
- refining equivalence relations, 421 ff.
- reflexivity, 146, 403 ff.
  - reflexive closure, 409 ff.
- regular expressions, 415, 430
- regular graphs, 596
- reindexing, 17
- relational databases, *see* databases
- relations
  - *n*-ary relations, 395 ff.
  - binary relations, 388 ff.
  - closures, 409 ff.
  - composition, 391 ff.
  - equivalence relations, 418 ff.
  - functions as relations, 394 ff.
  - inverses, 390 ff.
  - partial orders, 422 ff.
  - reflexivity, 403
  - relational databases, 398
  - symmetry, 404
  - total orders, 423 ff.
  - transitivity, 406 ff.
  - visual representation, 389 ff., 402 ff.
    - Hasse diagrams, 425 ff.
  - vs. predicates, 389
- relative primality, 346 ff., 363 ff.
  - Chinese Remainder Theorem, 351 ff.
  - extended Euclidean algorithm, 348
- remainder, *see* mod
- repeated squaring, 312, 342, 375
- repetition code, 153 ff.
- roots (of a polynomial), 69, 161, 357
- rotation matrices, *see* matrices
- roulette, 513, 563
- RSA cryptosystem, 197, 232, 373 ff.
  - breaking the encryption, 378
- Rubik’s cube, 362, 459
- running time, 283 ff.
  - average case, 289 ff., 560
  - best case, 289 ff.
  - worst case, 284 ff.
- Russell’s paradox, 29

- sample space (probability), 509
- sampling bias, 552
- satisfiability, 96, 104, 193, 387, 572
- scalars, 45
- SCC, *see* strongly connected components
- Scheme (programming language), 37, 43, 100, 135, 389
- scientific computing, 284
  - Newton’s method, 22
- seam carving, 496
- searching
  - Binary Search, 231, 248, 288 ff., 301, 304–306, 314, 341
  - Linear Search, 288 ff.
  - Ternary Search, 311
- secret sharing, 356, 500
- select, *see* median
- select (database operation), 398
- Selection Sort, *see* sorting
- self-loops, 580
- self-reference, 29, 82, 123, 191, 650, 673
- sentinels, 482
- sequences, 42 ff.
  - S^n (sequence of elements from the same set), 44
  - cardinality, 444, 450
- sets, 26 ff.
  - cardinality, 26 ff., 441 ff.
  - characteristic function, 389
  - complement, 30
  - disjointness, *see* disjoint sets, *see also* partitions
  - empty set, 30
  - intersection, 31
  - set difference, 31
  - singleton set, 30
  - subsets/supersets, 32 ff., *see also* power set
  - union, 31
    - Inclusion–Exclusion, 446 ff.
  - Venn diagrams, 30
  - well-ordered, 254
- Sheffer stroke (|), 188, 261
- Shor’s algorithm, 522
- short-circuit evaluation, 105
- Sierpiński triangle/carpet, 234 ff.
- Sieve of Eratosthenes, 344, 358
- signed social networks, 592
- Simpson’s paradox, 210
- six degrees of separation, 180
- skite, 622
- small-world phenomenon, 180, 618
- social networks, 180, 578, 592, 599
  - Dunbar’s number, 601
- sorting
  - Bubble Sort, 287, 291, 295
  - comparison-based, 295, 457
  - Counting Sort, 296, 458
  - Insertion Sort, 222, 286, 290, 295
    - average-case analysis, 560, 570
    - correctness using loop invariants, 231
  - lower bounds, 457–458
  - Merge Sort, 248, 298–301, 303–304, 312, 314
  - Quick Sort, 296, 311
    - correctness (for any pivot rule), 241 ff.
    - randomized pivot selection, 524
  - Radix Sort, 296
  - Selection Sort, 284, 291, 295, 457
- spam filter, 544
- spanning trees, 633 ff.
  - Cycle Elimination algorithm, 634
  - minimum spanning trees, 646 ff.
- speech processing, *see* natural language processing
- sphere packing, 159
- spreadsheets, 429, 434, 611
- SQL (programming language), 398
- square roots, 11, 22, *see* exponentials
  - Heron’s method, 22, 182
- standard deviation, 562 ff.
- steganography, 232
- Strassen’s algorithm, 321
- strings, 44, 55
  - generating all strings of a given length, 340
  - regular expressions, 415
- strong induction, *see* proofs
- strongly connected components, 609 ff.
- structural induction, *see* proofs

© in this web service Cambridge University Press & Assessment www.cambridge.org

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-15049-1 — Connecting Discrete Mathematics and Computer Science
David Liben-Nowell
Index
More Information

subgraphs, *see* graphs
subsequences, 229, 400, 477, 488, 499, 501
subset, 33
Sudoku, 104
sum of products, *see* disjunctive normal form
Sum Rule, 441
summations, 15 ff.
  arithmetic, 17, 226, 233
  geometric, 17, 224 ff., 314 ff.
    infinite, 225
  harmonic, 226 ff.
  of a set, 32
  reindexing summations, 17
  reversing nested summations, 18, 553
superset, 33
surjective functions, *see* onto functions
symmetry, 146, 387, 404 ff.
  symmetric closure, 409 ff.
syntactic sugar, 100
syzygy, 598, 642

$T(n) = aT(n/b) + n^k$, 314 ff.
tautology, 95 ff.
temporal logic, 409
term frequency–inverse document frequency (TFIDF), 53
The Book (of proofs), 180
Therac-25, 207, 658
Theta (Θ) (asymptotics), 274, 408 ff.
tic-tac-toe, 121, 478
topological ordering, 427 ff.
Tor, 232, 658
total orders, 423 ff., *see also* partial orders
totient function, 370, 461
Towers of Hanoi, 322
transitivity, 406 ff.
  nontransitive dice, 569
  nontransitivity in voting, 414
  signed social networks, 592
  transitive closure, 409 ff.
Traveling Salesperson Problem, 496
trees, 623 ff.
  2–3 and 2–3–4 trees, 261
  AVL trees, 309 ff.
  binary search trees, 260, 309, 637
  binary trees, 251, 309 ff., 630 ff.
    complete binary trees, 640 ff.
    heaps, 74, 245
  decision trees, 458
  forests, 626
  game trees, 121, 478
  in counting problems, 455
  parse trees, 259
  quadtrees, 311
  recursion trees, 298 ff.
  recursive definitions of trees, 251, 630
  rooted trees, 628 ff.
  spanning trees, 633 ff.
    minimum spanning trees, 646 ff.
  subtrees, 628 ff.
  tree traversal, 631 ff.
  van Emde Boas trees, 322
triangle inequality, 146, 170
triangulation, 240–241, 244
truth tables, 89 ff.
truth values, 81 ff.
tsktsks, 415, 642
tuple, *see* sequence
Turing Award, 28, 98, 146, 270, 336, 373, 379, 388, 398, 642
Turing machines, 123, 192, 284
Turing, Alan, 28, 191, 284, 497

unary numbers, *see* integers
uncomputability, 123, 191–195, 198, 474
undecidability, *see* uncomputability
underflow, 21
Unicode, 460
uniform distribution, 510, 517 ff.
unigrams, 543
union (of sets), 31
Union Bound, 442
unit vector, 46
universal quantifier ($\forall$), 111 ff.
unsatisfiability, 96
URL squatting, 477

vacuous quantification, 119
valid inference, 201
van Emde Boas trees, 322
variance, 562 ff.
Vector Space Model, 53
vectors, 44 ff.
  dot product, 47 ff.
Venn diagrams, 30
virtual memory, 198
Von Koch snowflake, 216, 223, 234 ff.
Voronoi diagram, 56
voting systems, 414

wall clocks, 293
Weizenbaum, Joseph, 659
well-ordered set, 254
What Three Words, 440
without loss of generality, 170
word2vec, 53
World War II, 497, 592
World Wide Web, 599, 618
  PageRank, 650
worst-case analysis, *see* running time

xor, *see* exclusive or

$\mathbb{Z}$, *see* integers
$\mathbb{Z}_n$, 360 ff.
zero (of a binary operator), 93, 261
zyzzyvas, 389

© in this web service Cambridge University Press & Assessment www.cambridge.org