

Contents

I	Low level algorithms	1
1	Bit wizardry	2
1.1	Trivia	2
1.2	Operations on individual bits	7
1.3	Operations on low bits or blocks of a word	8
1.4	Extraction of ones, zeros, or blocks near transitions	11
1.5	Computing the index of a single set bit	13
1.6	Operations on high bits or blocks of a word	14
1.7	Functions related to the base-2 logarithm	17
1.8	Counting the bits and blocks of a word	18
1.9	Words as bitsets	23
1.10	Index of the i -th set bit	25
1.11	Avoiding branches	25
1.12	Bit-wise rotation of a word	27
1.13	Binary necklaces ‡	29
1.14	Reversing the bits of a word	33
1.15	Bit-wise zip	38
1.16	Gray code and parity	41
1.17	Bit sequency ‡	46
1.18	Powers of the Gray code ‡	48
1.19	Invertible transforms on words ‡	49
1.20	Scanning for zero bytes	55
1.21	Inverse and square root modulo 2^n	56
1.22	Radix -2 (minus two) representation	58
1.23	A sparse signed binary representation	61
1.24	Generating bit combinations	62
1.25	Generating bit subsets of a given word	68
1.26	Binary words in lexicographic order for subsets	70
1.27	Fibonacci words ‡	74
1.28	Binary words and parentheses strings ‡	78
1.29	Permutations via primitives ‡	80
1.30	CPU instructions often missed	82
1.31	Some space filling curves ‡	83
2	Permutations and their operations	102
2.1	Basic definitions and operations	102
2.2	Representation as disjoint cycles	104
2.3	Compositions of permutations	105

2.4	In-place methods to apply permutations to data	109
2.5	Random permutations	111
2.6	The revbin permutation	118
2.7	The radix permutation	121
2.8	In-place matrix transposition	122
2.9	Rotation by triple reversal	123
2.10	The zip permutation	125
2.11	The XOR permutation	127
2.12	The Gray permutation	128
2.13	The reversed Gray permutation	131
3	Sorting and searching	134
3.1	Sorting algorithms	134
3.2	Binary search	141
3.3	Variants of sorting methods	142
3.4	Searching in unsorted arrays	147
3.5	Determination of equivalence classes	148
4	Data structures	153
4.1	Stack (LIFO)	153
4.2	Ring buffer	155
4.3	Queue (FIFO)	156
4.4	Deque (double-ended queue)	158
4.5	Heap and priority queue	160
4.6	Bit-array	164
4.7	Left-right array	166
II	Combinatorial generation	171
5	Conventions and considerations	172
5.1	Representations and orders	172
5.2	Ranking, unranking, and counting	172
5.3	Characteristics of the algorithms	173
5.4	Optimization techniques	174
5.5	Implementations, demo-programs, and timings	174
6	Combinations	176
6.1	Binomial coefficients	176
6.2	Lexicographic and co-lexicographic order	177
6.3	Order by prefix shifts (cool-lex)	180
6.4	Minimal-change order	182
6.5	The Eades-McKay strong minimal-change order	183
6.6	Two-close orderings via endo/enup moves	186
6.7	Recursive generation of certain orderings	191
7	Compositions	194
7.1	Co-lexicographic order	194
7.2	Co-lexicographic order for compositions into exactly k parts	196
7.3	Compositions and combinations	198
7.4	Minimal-change orders	199
8	Subsets	202
8.1	Lexicographic order	202
8.2	Minimal-change order	204

8.3	Ordering with De Bruijn sequences	208
8.4	Shifts-order for subsets	208
8.5	k -subsets where k lies in a given range	210
9	Mixed radix numbers	217
9.1	Counting (lexicographic) order	217
9.2	Minimal-change (Gray code) order	220
9.3	gslex order	224
9.4	endo order	226
9.5	Gray code for endo order	228
9.6	Fixed sum of digits	229
10	Permutations	232
10.1	Factorial representations of permutations	232
10.2	Lexicographic order	242
10.3	Co-lexicographic order	243
10.4	An order from reversing prefixes	245
10.5	Minimal-change order (Heap's algorithm)	248
10.6	Lipski's Minimal-change orders	250
10.7	Strong minimal-change order (Trotter's algorithm)	254
10.8	Star-transposition order	257
10.9	Minimal-change orders from factorial numbers	258
10.10	Derangement order	264
10.11	Orders where the smallest element always moves right	267
10.12	Single track orders	271
11	Permutations with special properties	277
11.1	The number of certain permutations	277
11.2	Permutations with distance restrictions	282
11.3	Self-inverse permutations (involutions)	284
11.4	Cyclic permutations	285
12	k-permutations	291
12.1	Lexicographic order	292
12.2	Minimal-change order	293
13	Multisets	295
13.1	Subsets of a multiset	295
13.2	Permutations of a multiset	296
14	Gray codes for strings with restrictions	304
14.1	List recursions	304
14.2	Fibonacci words	305
14.3	Generalized Fibonacci words	307
14.4	Run-length limited (RLL) words	310
14.5	Digit x followed by at least x zeros	311
14.6	Generalized Pell words	313
14.7	Sparse signed binary words	315
14.8	Strings with no two consecutive nonzero digits	317
14.9	Strings with no two consecutive zeros	318
14.10	Binary strings without substrings $1x1$ or $1x11$ ‡	320
15	Parentheses strings	323
15.1	Co-lexicographic order	323
15.2	Gray code via restricted growth strings	325

15.3	Order by prefix shifts (cool-lex)	330
15.4	Catalan numbers	331
15.5	Increment- i RGS, k -ary Dyck words, and k -ary trees	333
16	Integer partitions	339
16.1	Solution of a generalized problem	339
16.2	Iterative algorithm	341
16.3	Partitions into m parts	342
16.4	The number of integer partitions	344
17	Set partitions	354
17.1	Recursive generation	354
17.2	The number of set partitions: Stirling set numbers and Bell numbers	358
17.3	Restricted growth strings	360
18	Necklaces and Lyndon words	370
18.1	Generating all necklaces	371
18.2	Lex-min De Bruijn sequence from necklaces	377
18.3	The number of binary necklaces	379
18.4	Sums of roots of unity that are zero ‡	383
19	Hadamard and conference matrices	384
19.1	Hadamard matrices via LFSR	384
19.2	Hadamard matrices via conference matrices	386
19.3	Conference matrices via finite fields	388
20	Searching paths in directed graphs ‡	391
20.1	Representation of digraphs	392
20.2	Searching full paths	393
20.3	Conditional search	398
20.4	Edge sorting and lucky paths	402
20.5	Gray codes for Lyndon words	403
III	Fast transforms	409
21	The Fourier transform	410
21.1	The discrete Fourier transform	410
21.2	Radix-2 FFT algorithms	411
21.3	Saving trigonometric computations	416
21.4	Higher radix FFT algorithms	418
21.5	Split-radix algorithm	425
21.6	Symmetries of the Fourier transform	428
21.7	Inverse FFT for free	430
21.8	Real-valued Fourier transforms	431
21.9	Multi-dimensional Fourier transforms	437
21.10	The matrix Fourier algorithm (MFA)	438
22	Convolution, correlation, and more FFT algorithms	440
22.1	Convolution	440
22.2	Correlation	444
22.3	Correlation, convolution, and circulant matrices ‡	447
22.4	Weighted Fourier transforms and convolutions	448
22.5	Convolution using the MFA	451
22.6	The z -transform (ZT)	454

22.7	Prime length FFTs	457
23	The Walsh transform and its relatives	459
23.1	Transform with Walsh-Kronecker basis	459
23.2	Eigenvectors of the Walsh transform $\ddagger$	461
23.3	The Kronecker product	462
23.4	Higher radix Walsh transforms	465
23.5	Localized Walsh transforms	468
23.6	Transform with Walsh-Paley basis	473
23.7	Sequency-ordered Walsh transforms	474
23.8	XOR (dyadic) convolution	481
23.9	Slant transform	482
23.10	Arithmetic transform	483
23.11	Reed-Muller transform	486
23.12	The OR-convolution and the AND-convolution	489
23.13	The MAX-convolution $\ddagger$	491
23.14	Weighted arithmetic transform and subset convolution	492
24	The Haar transform	497
24.1	The ‘standard’ Haar transform	497
24.2	In-place Haar transform	499
24.3	Non-normalized Haar transforms	501
24.4	Transposed Haar transforms $\ddagger$	503
24.5	The reversed Haar transform $\ddagger$	505
24.6	Relations between Walsh and Haar transforms	507
24.7	Prefix transform and prefix convolution	510
24.8	Nonstandard splitting schemes $\ddagger$	512
25	The Hartley transform	515
25.1	Definition and symmetries	515
25.2	Radix-2 FHT algorithms	515
25.3	Complex FFT by FHT	521
25.4	Complex FFT by complex FHT and vice versa	522
25.5	Real FFT by FHT and vice versa	523
25.6	Higher radix FHT algorithms	524
25.7	Convolution via FHT	525
25.8	Localized FHT algorithms	529
25.9	2-dimensional FHTs	530
25.10	Automatic generation of transform code	531
25.11	Eigenvectors of the Fourier and Hartley transform $\ddagger$	533
26	Number theoretic transforms (NTTs)	535
26.1	Prime moduli for NTTs	535
26.2	Implementation of NTTs	537
26.3	Convolution with NTTs	542
27	Fast wavelet transforms	543
27.1	Wavelet filters	543
27.2	Implementation	544
27.3	Moment conditions	546
IV	Fast arithmetic	549
28	Fast multiplication and exponentiation	550

28.1	Splitting schemes for multiplication	550
28.2	Fast multiplication via FFT	558
28.3	Radix/precision considerations with FFT multiplication	560
28.4	The sum-of-digits test	562
28.5	Binary exponentiation	563
29	Root extraction	567
29.1	Division, square root and cube root	567
29.2	Root extraction for rationals	570
29.3	Divisionless iterations for the inverse a -th root	572
29.4	Initial approximations for iterations	575
29.5	Some applications of the matrix square root	576
29.6	Goldschmidt's algorithm	581
29.7	Products for the a -th root $\ddagger$	583
29.8	Divisionless iterations for polynomial roots	586
30	Iterations for the inversion of a function	587
30.1	Iterations and their rate of convergence	587
30.2	Schröder's formula	588
30.3	Householder's formula	592
30.4	Dealing with multiple roots	593
30.5	More iterations	594
30.6	Convergence improvement by the delta squared process	598
31	The AGM, elliptic integrals, and algorithms for computing π	599
31.1	The arithmetic-geometric mean (AGM)	599
31.2	The elliptic integrals K and E	600
31.3	Theta functions, eta functions, and singular values	604
31.4	AGM-type algorithms for hypergeometric functions	611
31.5	Computation of π	615
32	Logarithm and exponential function	622
32.1	Logarithm	622
32.2	Exponential function	627
32.3	Logarithm and exponential function of power series	630
32.4	Simultaneous computation of logarithms of small primes	632
32.5	Arctangent relations for π $\ddagger$	633
33	Computing the elementary functions with limited resources	641
33.1	Shift-and-add algorithms for $\log_b(x)$ and b^x	641
33.2	CORDIC algorithms	646
34	Numerical evaluation of power series	651
34.1	The binary splitting algorithm for rational series	651
34.2	Rectangular schemes for evaluation of power series	658
34.3	The magic sumalt algorithm for alternating series	662
35	Recurrences and Chebyshev polynomials	666
35.1	Recurrences	666
35.2	Chebyshev polynomials	676
36	Hypergeometric series	685
36.1	Definition and basic operations	685
36.2	Transformations of hypergeometric series	688
36.3	Examples: elementary functions	694

36.4	Transformations for elliptic integrals ‡	700
36.5	The function x^x ‡	702
37	Cyclotomic polynomials, product forms, and continued fractions	704
37.1	Cyclotomic polynomials, Möbius inversion, Lambert series	704
37.2	Conversion of power series to infinite products	709
37.3	Continued fractions	716
38	Synthetic Iterations ‡	726
38.1	A variation of the iteration for the inverse	726
38.2	An iteration related to the Thue constant	730
38.3	An iteration related to the Golay-Rudin-Shapiro sequence	731
38.4	Iteration related to the ruler function	733
38.5	An iteration related to the period-doubling sequence	734
38.6	An iteration from substitution rules with sign	738
38.7	Iterations related to the sum of digits	739
38.8	Iterations related to the binary Gray code	741
38.9	A function encoding the Hilbert curve	747
38.10	Sparse power series	750
38.11	An iteration related to the Fibonacci numbers	753
38.12	Iterations related to the Pell numbers	757
V	Algorithms for finite fields	763
39	Modular arithmetic and some number theory	764
39.1	Implementation of the arithmetic operations	764
39.2	Modular reduction with structured primes	768
39.3	The sieve of Eratosthenes	770
39.4	The Chinese Remainder Theorem (CRT)	772
39.5	The order of an element	774
39.6	Prime modulus: the field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p = \text{GF}(p)$	776
39.7	Composite modulus: the ring $\mathbb{Z}/m\mathbb{Z}$	776
39.8	Quadratic residues	781
39.9	Computation of a square root modulo m	784
39.10	The Rabin-Miller test for compositeness	786
39.11	Proving primality	792
39.12	Complex modulus: the field $\text{GF}(p^2)$	801
39.13	Solving the Pell equation	812
39.14	Multiplication of hypercomplex numbers ‡	815
40	Binary polynomials	822
40.1	The basic arithmetical operations	822
40.2	Multiplying binary polynomials of high degree	827
40.3	Modular arithmetic with binary polynomials	832
40.4	Irreducible polynomials	837
40.5	Primitive polynomials	841
40.6	The number of irreducible and primitive polynomials	843
40.7	Transformations that preserve irreducibility	845
40.8	Self-reciprocal polynomials	846
40.9	Irreducible and primitive polynomials of special forms ‡	848
40.10	Generating irreducible polynomials from Lyndon words	856
40.11	Irreducible and cyclotomic polynomials ‡	857
40.12	Factorization of binary polynomials	858

41 Shift registers	864
41.1 Linear feedback shift registers (LFSR)	864
41.2 Galois and Fibonacci setup	867
41.3 Error detection by hashing: the CRC	868
41.4 Generating all revbin pairs	873
41.5 The number of m-sequences and De Bruijn sequences	873
41.6 Auto-correlation of m-sequences	875
41.7 Feedback carry shift registers (FCSR)	876
41.8 Linear hybrid cellular automata (LHCA)	878
41.9 Additive linear hybrid cellular automata	882
42 Binary finite fields: $\text{GF}(2^n)$	886
42.1 Arithmetic and basic properties	886
42.2 Minimal polynomials	892
42.3 Fast computation of the trace vector	895
42.4 Solving quadratic equations	896
42.5 Representation by matrices $\ddagger$	899
42.6 Representation by normal bases	900
42.7 Conversion between normal and polynomial representation	910
42.8 Optimal normal bases (ONB)	912
42.9 Gaussian normal bases	914
A The electronic version of the book	921
B Machine used for benchmarking	922
C The GP language	923
Bibliography	931
Index	951