
Index

- \square **23**
 $[\cdot]$ **11, 65**
 $\lceil \cdot \rceil$ **11, 66**
 $|\cdot|$ **16**
 $\|\cdot\|$ **16**
 $*$ **17**
 $+$ **17**
 $-$ **17**
 \cup **17**
 \cap **17**
 \top **18**
 \top^* **18**
 \neg **29, 30**
 \vee **29, 30**
 \wedge **29, 30**
 \implies **29, 30**
 \iff **29, 30**
 \oplus **147, 258**
 \triangle **239**
 \bigvee *see* \exists
 \bigwedge *see* \forall
 \exists **32**
 \exists^p **190, 191, 196, 198**
 \exists^+ **278, 279–295, 301**
 \forall **32**
 \forall^p **190, 191, 196, 198**
 \vee **174, 241**
 \wedge **174, 241**
 Δ **256**
 \boxtimes **189, 243**
 \equiv **31, 36, 50**
 \cong **43**
 \cong_p **117**
 \circ **37, 59, 271**
 \leq **38**
 $\leq_{ae}, <_{ae}, \geq_{ae}, >_{ae}$ **59**
 $\leq_{io}, <_{io}, \geq_{io}, >_{io}$ **59**
 $\preceq, \prec, \succeq, \succ$ **60**
 $\preceq_{io}, \prec_{io}, \succeq_{io}, \succ_{io}$ **60**
 \leq_m^{\log} **79, 81, 82, 84, 86, 87, 121, 122, 193, 231, 232, 244**
 \leq_m^{\log} -completeness **79, 82, 84, 121, 122, 231, 232**
 \leq_m^{\log} -hardness **79**
 \leq_m^p **77, 78, 116, 185, 193, 194, 236–239, 244, 246, 255, 272, 276, 292, 295, 301, 307, 308**
 \leq_m^p -completeness **77, 109, 110, 112, 213, 236–239, 246, 255, 272, 276, 292, 295**

- $\bigwedge_{\text{BE}}^{\text{P}}$ -hardness **77**
- $\bigwedge_{\text{HP}}^{\text{NP}}$ **193**, 244, 252
- $\bigwedge_{\text{HP}}^{\text{NP}}$ -hardness 218
- $\bigwedge_{\text{HP}}^{\text{NP}}$ **233**, 236, 245, 246, 257
- $\bigwedge_{\text{HP}}^{\text{NP}}$ -completeness **233**
- $\bigwedge_{\text{HT}}^{\text{NP}}$ -hardness **233**
- $\bigwedge_{\text{pos-T}}^{\text{P}}$ 194, **244**, 252
- $\bigwedge_{\text{T}}^{\text{P}}$ 125, **193**, 194, 238, 244, 246, 252, 254, 291, 306
- $\bigwedge_{\text{T}}^{\text{P}}$ -completeness **193**, 233, 255
- $\bigwedge_{\text{T}}^{\text{P}}$ -hardness 125, **193**, 244, 254
- $\bigwedge_{\text{ff}}^{\text{P}}$ **202**, 203, 252, 255
- $\bigwedge_{\text{ff}}^{\text{P}}$ -completeness **202**
- $\bigwedge_{\text{ff}}^{\text{P}}$ -hardness **202**
- $\binom{m}{r}$ **40**
- $\#P$ 124, 260, 288, **289**, 301–303, 306
 - closure properties of, *see* function class, closure of a
- $\#P$ -completeness **124**
- $\#P_1$ **124**, 125
- $\#P_1$ -completeness 124
- $\#RA$ 356
- $\oplus P$ 125, 289, **290**, 291, 292, 296, 300, 301, 304, 306–308
- $\oplus P$ -low 291, 306
- $\oplus P^{\text{SPP}}$ 291
- 2-Colorability **95**, 116
- 2^{Lin} **59**
- $2^{\text{Lin}(\cdot)}$ **59**
- 2^{Pol} **59**
- $2^{\text{Pol}(\cdot)}$ **59**
- 2-SAT 55, **83**, 84, 87, 121
- 3-Colorability 5, 55, **95**, 116, 172, 185, 250
- 3-DM **99**, 100, 117, 190
- 3-SAT 55, **83**, 92, 185, 120, 250, 260–263, 304
- 4-SAT 261, 304
- 5-SAT 261, 304
- 6-SAT 261, 304
- A**
- $\alpha(\cdot)$ **202**
- absorption **31**
- accepting computation
 - see* Turing machine, computation of a, accepting
 - number of —s *see* acc_M
- acc_M **268**
- adjoint matrix **138**
- Adleman, L. 257, 309, 310, 355, 356, 406
- Advanced Encryption Standard, *see also* AES 170
- AES 170
- affine cipher *see* cipher, affine
- affine linear cipher *see* cipher, affine linear
- AGAP **232**
- Agrawal, M. 106, 118, 252, 309, 333, 342, 355
- Ajtai, M. 407, 408
- Alberti, B. 168
- AL **231**
- algebra **37–41**, 51
- al Choresmi, M. 9
- algorithm, *see also* Turing machine 9
 - baby-step giant-step *see* SHANKS
 - *see* BACKTRACKING-SAT
 - *see* EUCLID
 - execution time of an 61
 - *see* EXTENDED-EUCLID
 - *see* FERMAT
 - Monte Carlo 6, 259, 266, **269**, 321
 - no-biased, *see also* RP **269**, 271, 319, 321, 327, 331, 356
 - yes-biased, *see also* coRP **269**, 271, 319
 - Las Vegas, *see also* ZPP 6, 259, 266, **271**, 355, 378–380
 - *see* LERC
 - *see* LLL
 - *see* MILLER-RABIN
 - *see* POLLARD
 - randomized 6, 7, 46, 110, 241, **259–308**, 378, 379
 - *see* RANDOM-FACTOR

- *see* RANDOM-SAT
- random walk 264
- *see* SHANKS
- *see* SOLOVAY-STRASSEN
- *see* SQUARE-AND-MULTIPLY
- *see* TRIAL-DIVISION
- algorithmic device 54
- algorithmics **9–16**, 51
- Alice 1
- Al-Khowarizmi, A. *see* al Choesmi, M.
- Allen, W. 142, 163
- Allender, E. 119, 123, 258
- ALOGTIME **224**
- alphabet **16**
 - set of strings over an, *see also* Σ^* **16**
- alternating logarithmic space, *see also* AL 6, **231**
- alternating logarithmic time, *see also* ALOGTIME 53, **224**
- alternating polynomial time, *see also* AP 6, **228**
- alternating sums hierarchy 250
 - *see also* boolean hierarchy, normal form
- alternating Turing machine *see* ATM; *see also* Turing machine, alternating
- alternation 221–232
- alternative *see* candidate
- AM **284**, 285, 286, 288, 290, 294, 301, 308
 - *see also* Arthur-Merlin games
- $AM^{AM \cap coAM}$ 288
- AMA **284**, 285, 286, 301
 - *see also* Arthur-Merlin games
- AMH **284**, 285, 386
 - *see also* Arthur-Merlin games
- Ambos-Spies, K. VI, 8
- Anton, H. 51
- AP **228**
- approximability 8, 121, 251, 254
- arithmetics modulo an integer
 - see* \mathbb{Z}_n , arithmetics in
- Arora, S. 251
- Arrow, K. 206
- Arthur *see* Arthur-Merlin games
- Arthur’s labyrinth 383
- Arthur-Merlin games 7, 251, 259, 260, **277–288**, 294, 301, 305, 308, 357, **382–389**, 405
- Arthur-Merlin hierarchy *see* AMH; *see also* Arthur-Merlin games
- artificial intelligence 251, 254
- Arvind, V. 122, 255, 297, 307
- ASPACE(\cdot) **223**, 228–231, 245
- Assing, S. VI
- associativity **31, 37, 394**
 - weak **394**, 407
- asymmetric cryptography
 - see* cryptography, asymmetric;
 - see* cryptography, public-key
- asymmetric cryptosystem
 - see* cryptosystem, asymmetric;
 - see* cryptosystem, public-key
- ATIME(\cdot) **223**, 225–228, 245
- ATM 53, 54, 58, 171, **221**, 222, 223
- attack, *see also* cryptanalytic attack
 - active 129, 361
 - chosen-ciphertext **128**, 314, 351, 356, 381, 400
 - chosen-message
 - see* attack, chosen-plaintext
 - chosen-plaintext **128**, 142, 314, 350, 351, 373, 381
 - ciphertext-only **128**, 132, 133, 155, 167
 - impersonation 129
 - key-only **128**, 373
 - known-message
 - see* attack, known-plaintext
 - known-plaintext **128**, 142, 144, 155, 162, 165, 373
 - man-in-the-middle 129, 361, 382
 - passive 129
 - substitution 129
- Aurich, V. VI
- Ausiello, G. 8, 251
- Aut(\cdot) **43**

authentication 2, 7, 129, 357, 361,
 382–389, 406
 authentication code 129
 authentication problem 129
 – *see* message authentication
 – *see* message integrity
 – *see* user authentication
 authentication protocol 382–389
 – *see* challenge-and-response
 protocol
 – *see* zero-knowledge protocol
 auto 297, 299, 303
 automorphism of a graph, *see also*
 $\text{Aut}(\cdot)$ 43
 axe *see* tools, axe

B
 Babai, L. 7, 305, 405
 Babbage, C. 140, 151, 168
 baby cloning 4, 100
 baby-step giant-step algorithm
 see SHANKS
 BACKTRACKING-SAT 262, 263, 300
 Baker, T. 258
 balanced immunity 258
 Balcázar, J. 8, 118, 121, 257, 305,
 306, 405
 Bartholdi III, J. 253
 Bauer, F. 2, 168, 169
 Bayes, T. 46
 Bayes's Theorem
 see Theorem, Bayes's
 $\text{BC}(\mathcal{C})$ 174, 175, 242
 $\text{BC}(\text{NP})$ 174, 176, 216, 241
 Beatles 162
 Beaufort, F. 164
 Beaufort cipher
 see cipher, Beaufort
 Beaufort square 164
 Beckwith, J. V
 Beigel, R. 218, 250, 254, 256, 305,
 306
 Berman, L. 6, 108–110, 122, 123,
 125, 255, 408

Berman–Hartmanis conjecture
 see isomorphism conjecture
 Bernstein, D. 355, 356
 Bernstein, F. 108
 Bertoni, A. 250
 Beutelspacher, A. 168, 305, 405
 Beygelzimer, A. V, 168, 407
 $\text{BH}(\mathcal{C})$ 175, 242
 $\text{BH}_k(\mathcal{C})$ 175, 242, 256
 $\text{BH}(\text{NP})$ 174, 176, 177, 216, 242,
 254
 $\text{BH}_2(\text{NP})$ 173, 174, 176, 177, 180,
 184, 188, 243, 247, 248
 $\text{BH}_k(\text{NP})$ 174, 176, 177, 179, 180,
 188, 213, 217, 242, 245, 250,
 256
 $\text{BH}_k(\text{NP})$ -complete 179, 180, 188,
 213, 242, 245
 $\text{BH}_k(\text{NP})$ -hard 179, 250
 BHT 217
 bi-immunity 258
 $\text{bin}(\cdot)$ 17
 $\text{Bin}(\cdot)$ 71
 binary search 191, 201, 215
 Blass, A. 249
 Bletchley Park 2, 169
 block cipher *see* cipher, block
 Bleichenbacher, D. 356
 Blömer, J. 356
 Blum, M. 57, 114, 119, 378
 Blum complexity measure 57, 114,
 119
 Blum number *see* number, Blum
 Blum's axioms 57
 Bob 1
 Boneh, D. 356
 Book, R. 66, 70, 119, 124, 217, 257
 boolean algebra 175
 boolean closure, *see also* set class,
 closure of a, boolean
 – of \mathcal{C} , *see also* $\text{BC}(\mathcal{C})$ 174,
 175, 242
 – of NP, *see also* $\text{BC}(\text{NP})$ 174,
 176, 216, 241
 boolean constant 30

- boolean expression
 - see* boolean formula
 - boolean formula 29, **30**, 34, 83
 - conjunctive normal form of a, *see also* CNF **30**
 - disjunctive normal form of a, *see also* DNF **48**
 - in predicate logic **34**
see also structure
see also term
 - in propositional logic **29**
 - isomorphic —s **252**
 - satisfiable **31**
 - truth assignment of a **31**
 - quantified
 - see* quantified boolean formula
 - semantically equivalent —s, *see also* \equiv **31, 36**
 - boolean hierarchy
 - extended 250
 - normal form
 - alternating sums
see alternating sums hierarchy
 - Hausdorff
see Hausdorff hierarchy
 - nested difference
see nested difference hierarchy
 - symmetric difference *see* symmetric difference hierarchy
 - union-of-differences
see Hausdorff hierarchy
 - over \mathcal{C} , *see also* $\text{BH}(\mathcal{C})$ **175**, 242
 k th level of the *see* $\text{BH}_k(\mathcal{C})$
 - over NP, *see also* $\text{BH}(\text{NP})$ 6, 171, **174**, 176, 177, 216, 217, 242, 249, 250, 254, 256
collapse of the 177, 217, 249
 k th level of the *see* $\text{BH}_k(\text{NP})$
second level of the
see $\text{BH}_2(\text{NP})$; *see also* DP
 - over RP 250
 - over UP 250
 - Boolean Hierarchy Tower, *see also* BHT 177, 217
 - boolean operation
 - *see* conjunction, *see also* \wedge
 - *see* disjunction, *see also* \vee
 - *see* equivalence, *see also* \iff
 - *see* exclusive-or, *see also* \oplus
 - *see* implication, *see also* \implies
 - *see* negation, *see also* \neg
 - boolean variable **30**
 - bound **32**
 - free **32**
 - quantified *see* boolean variable, bound
 - Boppana, R. 305, 405
 - Borchert, B. V, 252
 - Borges, J. 4
 - Borodin, A. 123
 - Borodin–Demers Theorem
see Theorem, Borodin–Demers
 - Bovet, D. 8, 118, 405
 - BPP 6, 125, 259, 273, **274**, 275–279, 281, 283–286, 288, 301, 303–306, 308
 - BPP^{BPP} 286
 - BPP_{path} 301, **303**, 304, 305
 - Brandstädt, A. 51, 118, 120
 - Brassard, G. 406, 408
 - Brauer, W. VI
 - break-elgamal **369**, 370
 - break-rabin **379**, 380, 381
 - Brent, R. 342
 - Brickell, E. 406, 407
 - Brillhart, J. 342
 - Bruschi, D. 306
 - Bshouty, N. 252
 - \mathfrak{B} -smooth **339**, 340, 341
 - Buchmann, J. 4, 168, 305, 355, 356, 365, 404, 405
 - Buhrman, H. 119, 121, 252, 256
 - Bush, G. W. 206
 - Buss, S. 216, 254
- C**
- Caesar cipher *see* cipher, Caesar
 - Caesar, J. 2, 132, 168
 - Cai, J. 122, 124, 168, 248, 249, 254–257, 407

- candidate 207
 Canetti, R. 255
 Cantor, G. 108
 Cantor–Bernstein Theorem
 see Theorem, Cantor–Bernstein
 Carmichael number *see* number, Carmichael
 Carroll, L. *see* Dodgson, C.
 Carter, J. 293, 307
 Castro, J. 254
 CBC **146, 147**, 148–150, 165
 census_L **109**, 110
 certificate *see* witness
 CF **19**, 20, 50
 CFB **148, 149**, 165
 chain-saw *see* tools, chain-saw
 challenge-and-response protocol 384,
 386
 Chandra, A. 257
 Chang, R. 218, 249, 250, 256
 Chakaravarthy, V. 255
 characteristic function *see* function,
 characteristic
 Chen, Z. 252
 Chinese Remainder Theorem *see* The-
 orem, Chinese Remainder
 choice set **207**
 Chomsky hierarchy **19**
 Chomsky, N. 19
 Chor, B. 406
 Chor–Rivest cryptosystem 406
 chosen-ciphertext attack *see* attack,
 chosen-ciphertext
 chosen-plaintext attack *see* attack,
 chosen-plaintext
 Cicero, Q. 168
 cipher, *see also* cryptosystem;
 see also cryptanalytic attack
 – affine **6, 132**
 – affine linear block **6, 135, 137,**
 138, 139, 142, 165
 – Beaufort **164**
 – block **6, 130**, 135–149
 – Caesar **132**
 – Hill **6, 139**, 144, 150, 162, 163,
 165
 – linear block **138**
 – permutation **6, 130, 131**, 139,
 146, 148, 161, 165, 168
 – shift **131**, 132, 133, 135, 162,
 166
 – stream **6, 145, 150**, 165, 166,
 168, 169
 – substitution **6, 130**
 – transposition
 see cipher, permutation
 – Vigenère **6, 136**, 137, 139–141,
 143, 145, 150, 151, 162, 163,
 165, 168, 169
 cipherblock chaining mode *see* CBC
 cipher feedback mode *see* CFB
 ciphertext **127**
 ciphertext-only attack
 see attack, ciphertext-only
 ciphertext space **127**
 circuit complexity 118,
 – *see also* polynomial-size circuit
 Clique **93**, 116
 Clique-Facet **249**, 243
 clique polytope,
 see also Polytope(·) 249
 clique problem **93**, 116, 190, 248
 see also Clique
 CNF, *see also* *k*-CNF **30**
 coAM 287, 288, 290, 294, 308, 384
 coBPP 275
 Cobham, A. 120
 co \mathcal{C} *see* set class, co operator, ap-
 plied to a
 Cocks, C. 355
 co $\mathbb{C}\mathbb{P}$ 290, 308
 codebreakers 2
 coDP **174**, 176, 177, 249
 co-graph **93**
 Cohen, S. V
 colorability problem 55, **95**
 see 2-Colorability;
 see 3-Colorability;
 see *k*-Colorability

- exact, *see also*
Exact- i -Colorability **184**,
188, 251
- generalized exact, *see also*
Exact- M_k -Colorability **184**,
184, 188
- coMA 286, 301, 308
- coMAM 287
- communication network
see network, communication
- commutativity **31, 395**
- completeness
see \leq_m^{\log} -completeness;
see \leq_m^p -completeness;
see \leq_T^p -completeness;
see \leq_{tt}^p -completeness;
see #P-completeness;
see #P₁-completeness;
see BH_k(NP)-complete;
see coNP-complete;
see Δ_2^p -complete;
see DP-complete;
see NL-complete;
see NP-complete;
see Π_2^p -complete;
see Π_i^p -complete;
see P-complete;
see PP-complete;
see PSPACE-complete;
see Σ_2^p -complete;
see Σ_i^p -complete;
see Θ_2^p -complete
- complete right transversal **42, 299**
- complete search reducing to partial
search 122
- complex intersection *see* set class,
complex intersection of —es
- complexity class 5
 - alternating time and space **223**
 - average-case 5
 - \leq_m^{\log} -closure of a **79**, 81, 116
 - \leq_m^p -closure of a **78**, 116, 194,
258, 301
 - \leq_T^{NP} -closure of a, *see also* NP^c
193
- \leq_T^p -closure of a, *see also* P^c
193, 194, 244, 291
- \leq_{tt}^p -closure of a, *see also* P_{tt}^c
203
- deterministic time and space **57**
- name of a *see* complexity
class, resource function of a
- nondeterministic time and space
58
- probabilistic 6, 257
- resource function of a 57, 59
- worst-case 5, **56–62**
- complexity measure 5, 54
 - alternating time and space **222**
 - average-case 5
 - deterministic time and space **56**
 - nondeterministic time and space
58
 - worst-case 5, **56–62**
- complexity theory
see theory, complexity
- complex symmetric difference *see*
set class, complex symmetric dif-
ference of —es
- complex union *see* set class, com-
plex union of —es
- computability **25**
- computability theory
see theory, recursive function
- computable function
see function, partial recursive;
see function, total recursive
- computation *see* Turing machine,
computation of a
 - efficient 5, **61**, 120
 - feasible
see computation, efficient
 - inefficient 5, **61**
 - intractable
see computation, inefficient
 - parallel 223, 228
 - threshold **268**, 305
- computational model
see algorithmic device;
see Turing machine

- computational paradigm *see* Turing machine, acceptance mode of a
- computational politics 206, 254
- computer network
 - see* network, computer
- Condorcet, the Marquis de,
 - M. de Caritat 207
- Condorcet Paradox **207**
- Condorcet Principle **207**, 253, 254
- Condorcet SCF **207**
- Condorcet winner **207**, 253
- congruence modulo an integer, *see also* \equiv **50**
- conjunction, *see also* \wedge **29**, 30
- coNL **77**, 121
- coNLINSPACE **77**
- coNP **110**, 118, 123, 173, **174**, 176, 177, 195, 196, 218, 233, 241–243, 245, 249, 251, 252, 254–256, 278, 290, 278, 290, 301, 304, 306, 308
- coNP-complete 117, 218, 242, 245, 251, 252, 255
- coNP-hard 122, 184, 218, 243, 245, 249, 251
- coNP^{NP}, *see also* Π_2^P 195, 196
- Conrad, S. VI
- coNSPACE(\cdot) **77**
- constructible in time **67**
- continued fraction expansion **347**
 - convergent of a **347**
- conveyor flow shop problem 250
- Cook, S. 6, 55, 88, 112, 113, 120, 120, 116, 252
- Cook–Levin Theorem
 - see* Theorem, Cook’s
- Cook’s criterion 6 228
- Cook reduction *see* Theorem, Cook’s
- Cook’s Theorem *see* Theorem, Cook’s
- co operator *see* set class, co operator, applied to a
- Coppersmith, D. 356, 406
- Cormen, T. 51
- coRP 269, 271, 308, 321, 324, 352
- coRP_q 352
- counting classes 288–292
- counting hierarchy 306
- coUP 113, 117, 123, 303, 308, 334, 356, 395, 408
- $\mathbb{C}P$ 125, 289, **290**, 291, 292, 296, 300, 301, 304, 306–308
- $\mathbb{C}P$ -low 291, 308
- $\mathbb{C}P^{SPP}$ 291
- Crepeau, C. 406
- Crescenzi, P. 8, 118, 251, 405
- Critical-Clique **248**, 249
- critical problem 6, 171, 248
 - *see* Critical-Clique
 - *see* Minimal-3-Uncolorability
 - *see* Minimal-3-UNSAT
 - *see* MDNHC
 - *see* MNHC
- cryptanalysis 2, 6, 7, 127–170, 343–351, 357–408
- cryptanalytic attack
 - see also* cryptanalysis
 - on affine ciphers 6, **133**, **134**, 162
 - on affine linear block ciphers **142–145**, 162–164
 - on Diffie–Hellman 357, **361–365**
 - by frequency counts **134**, 162
 - on ElGamal **369–376**, 399, 400
see also break-elgamal
 - on the Hill cipher 6, **144**, 162, 163
 - on Merkle–Hellman **402**, 406
 - on permutation ciphers 6, 161
 - on Rabin **379–381**, 400
see also break-rabin
 - on RSA 7, 333–335, 342, **343–351**, 354–356
see low-exponent attack
see RSA superencryption
see small-message attack
see Wiener’s attack
 - on the shift cipher 162
 - on stream ciphers 165, 166
 - on substitution ciphers 6, 133, 134, 162

- on triple encryption 161
- on the Vigenère cipher 6, **140–143**, 162, 163
- cryptography 1–8, 127–170, 310–314, 357–408
 - asymmetric
 - see* cryptosystem, public-key
 - lattice-based 350, 406, 408
 - private-key
 - see* cryptosystem, private-key
 - public-key
 - see* cryptosystem, public-key
 - symmetric
 - see* cryptosystem, private-key
 - worst-case 5, 361, 392, 407, 408
- cryptology 1–8
- cryptosystem
 - asymmetric
 - see* cryptosystem, public-key
 - Chor–Rivest
 - see* Chor–Rivest cryptosystem
 - ElGamal
 - see* ElGamal cryptosystem
 - entropy of a 157
 - monoalphabetic
 - see* monoalphabetic cryptosystem
 - NTRU *see* NTRU cryptosystem
 - polyalphabetic
 - see* polyalphabetic cryptosystem
 - private-key 6, **128**
 - public-key 5, 7, **128**
 - Rabin *see* Rabin cryptosystem
 - Merkle–Hellman *see* Merkle–Hellman cryptosystem
 - RSA *see* RSA cryptosystem
 - security of a 2
 - symmetric,
 - see* cryptosystem, private-key
- CS **19**, 20, 77
- cs($\cdot|\cdot$) **118**
- D**
- $\delta(\cdot)$ **97**, 172
- Δ_2^p , *see also* P^{NP} **194**, 195, 196, 252, 254, 306, 308
- Δ_2^p -complete 252
- Δ_2^p -hard 252
- Δ_3^p , *see also* $P^{NP^{NP}}$ **194**, 195, 196, 256
- Δ_i^p **194**, 194–196, 198, 244, 257
- $D_{(\cdot)}$ **28**, 57
- DAAD VI
- Dantsin, E. 261, 263, 304
- Daemen, J. 170
- Data Encryption Standard, *see also* DES 169
- decidability **25**
- deck *see* graph, deck of a
 - legitimate **307**
 - preimage of a **307**
- Deck-Checking **307**
- Demers, A. 123
- deMorgan, A. 31
- deMorgan’s rule **31**
- DES 169
- det 124, **138**, 167
- determinant of a matrix
 - see* matrix, determinant of a
- deterministic polynomial time *see* P
- Deutsche Wehrmacht 2, 166
- DFA **21**, 22, 48
- DFG VI
- Díaz, J. 8, 118, 305, 405
- Dietzfelbinger, M. 333, 352, 355, 356
- diffie-hellman **362**, 369, 398
- Diffie–Hellman 362, 398
- Diffie–Hellman protocol 7, 310, 355, 357, **358–365**, 366, 367, 369, 370, 382, 392, 398, 404, 408
 - security of the *see* cryptanalytic attack, on Diffie–Hellman
- Diffie–Hellman problem **362**, 369, 398, 408
 - as a decision problem
 - see* Diffie–Hellman
 - as a functional problem
 - see* diffie-hellman

- Diffie, W. 7, 355, 358, 404
 digital signature 7, **129**
 – forgery of a *see* forgery
 – *see* protocol, digital signature
 digital signature scheme
 see protocol, digital signature
 digital signature standard *see* United States Digital Signature Standard
 discrete logarithm **39**, 359
 – bit security of the 370, 402
 – *see* function, logarithm, discrete
 — with module p and base r
 discrete logarithm bit problem, *see* also *dlogbit* **370**, 371, 372
 discrete logarithm problem 7, 357–359, 361, **362**, 363, 365, 367, 369, 373, 389, 398, 404, 405, 408
 – as a decision problem
 see DLog
 – as a functional problem
 see *dlog*
 disjunction, *see* also \vee **29**, 30
 distance map **248**
 distributivity **31**
 divide-and-conquer **11**, 263
 Dixon, J. 356
dlog **362**, 398
 DLog **398**
dlogbit **370**, 371, 372
 DNA tests 4, 100, 101
 DNF **48**
 DNF-SAT **48**
 DNP **97**, 172
 Dodgson, C. 253
 Dodgson election system 253
 – homogeneous variant of the 253
 – ranking problem for the 253
 – winner problem for the 253
 Dodgson score **253**
 Dodgson voting scheme
 see Dodgson election system
 Dodgson winner **253**
 dogma 4, **61**, 62
 domatic number problem, *see* also DNP **96**, 97, 120, 172
 – approximation of the 121
 – exact, *see* also *Exact- i -DNP* **172**, 180, 184, 241, 242
 – generalized exact, *see* also *Exact- M_k -DNP* **173**, 180
 DOTM **28**
 double negation **31**
 downward collapse
 see upward separation
 downward separation
 see upward collapse
 DP **173**, 174, 176, 177, 180, 184, 188, 241, 243, 247–249, 251, 252
 DP-complete 173, 180, 188, 241, 243, 247–249, 251, 252
 DPOTM **28**, 193
 dragon 4, 383
 DSPACE(\cdot) **57**, 60, 67, 69, 74, 114, 115, 225–228, 245
 DTM 56, **24**
 DTIME(\cdot) **57**, 60, 63, 64, 70, 74, 114, 228–231, 245
 Du, D. 8, 118, 123, 405
 Durfee, G. 356
 Dwork, C. 254, 407, 408

E
 ε **16**
 e 271, 300
 E **61**, 70, 71, 116, 124
 E(\cdot) **47**
 E(\cdot) **81**
 EASY \forall **123**
 easy-hard technique 218, **219**
 eavesdropper *see* Erich
 ECB **145**, **146**, 147, 165
 edge *see* graph, edge set of a
 Edmonds, J. 120
 Eiter, T. 251, 254
 election system 206, **207**, 253
 – homogeneity of an **253**
 – manipulation of an 254

- monotonicity of an 206
- properties of an 253
- see* Condorcet Principle;
- see* election system, homogeneity of an;
- see* independence of irrelevant alternatives;
- see* election system, monotonicity of an;
- see* nondictatorship;
- see* Pareto Principle;
- *see also* Dodgson election system
- *see also* Kemeny election system
- *see also* majority rule
- *see also* Young election system
- electronic codebook mode *see* ECB
- ElGamal, T. 7, 357, 365, 367, 369
- ElGamal digital signature 7, **367–369**, 399, 404
 - security of the *see* cryptanalytic attack, on ElGamal
- ElGamal cryptosystem 357, **365–367**, 379, 389, 399, 404
 - security of the *see* cryptanalytic attack, on ElGamal
- Ella *see* Rothe, E.
- Ellis, J. 355
- ELow₂ **258**
- ELow_k **258**
- Enigma 2, 166
- entropy 6, 151, 155, **156**, 157, 167, 169, 266
 - conditional **159**, 160, 166
 - grouping property of **158**
 - properties of **158**, 160, 166
 - subadditivity of **158**
- equivalence, *see also* \iff **29**, 30
- equivalence relation **117**
- Eratosthenes 316
 - sieve of
 - see* sieve of Eratosthenes
- Erdélyi, G. VI
- Erich 1
- Erlkönig 171
- Espelage, W. 250
- Euclid 10
 - algorithm of *see* EUCLID
 - extended algorithm of *see* EXTENDED-EUCLID
- EUCLID **10**, 15, 16, 347, 348
- Euclidean Algorithm *see* EUCLID
- Euler function, *see also* $\varphi(\cdot)$ **38**, 39, 49, 133, 310, 344
- Euler, L. 38–41, 49, 133, 271, 300, 310, 327, 328, 342, 344, 371, 372, 378
- Euler’s constant, *see also* e 271, 300
- Euler’s criterion **40**, 41, 327, 328, 371, 372, 378
- Euler’s Theorem
 - see* Theorem, Euler’s
- eval(\cdot) **221**
- Even, S. 307, 407
- event **46**
- exact conveyor flow shop problem 250
- exact cover by 3-sets problem 98, **103**
 - *see also* X-3-Cover
- exact domatic number problem *see* domatic number problem, exact
 - generalized *see* domatic number problem, generalized exact
- Exact- i -Clique 243
- Exact- M_k -Clique 243
- Exact-3-Colorability 184, 251
- Exact-4-Colorability 188, 251
- Exact-7-Colorability 242
- Exact- i -Colorability **184**
- Exact- M_k -Colorability **184**, 188, 242
- Exact-2-DNP 184, 242
- Exact-3-DNP 184
- Exact-4-DNP 184
- Exact-5-DNP 180
- Exact- i -DNP **172**
- Exact- M_k -DNP **173**, 180
- Exact- i -Favorite 243
- Exact- M_k -Favorite 243
- Exact- i -IS 243
- Exact- M_k -IS 243

exclusive-or, *see also* \oplus **147**

existential forgery

see forgery, existential

existential quantifier *see* quantifier, existential

– polynomially length-bounded

see \exists^p

EXP **61**, 70

expectation value, *see also* $E(\cdot)$ **47**

exponential space

– deterministic *see* EXPSPACE

– nondeterministic *see* NEXPSPACE

exponential time **61**

– deterministic *see* E; *see* EXP

– nondeterministic

see NE; *see* NEXP

$\exp_{r,p}(\cdot)$ **39**, 359

EXPSPACE **61**, 69, 115

EXTENDED-EUCLID **11**, **12**

extended lowness

– *see* $ELow_2$

– *see* $ELow_k$

– *see* low hierarchy, extended

F

$\varphi(\cdot)$ **38**

F_m **342**, 354

f_n **12**

facet *see* clique polytope

facet problem **6**, **248**

– *see* Clique-Facet

– *see* TSP-Facet

factor base 339

factoring **334**, 353

Factoring **353**, 356

factoring algorithm **7**, 309, **333–343**

344, 354, 356

– elliptic curve 341, 342, 344, 356

– general-purpose **344**

– number field sieve 341, 342, 344, 356

– Pollard's $p-1$ *see* Pollard's $p-1$ factoring algorithm

– quadratic sieve **7**, **336–341**, 344, 354, 356

– special-purpose **344**

– trial division **335**, 254

see also TRIAL-DIVISION

factoring attack 343

– brute force **343**

– elliptic curve 344

– general-purpose **344**

– special-purpose **344**

factoring method

see factoring algorithm

factoring problem **5**, **7**, 106, 333, **334**, 343, 355

– as a decision problem

see Factoring

– as a functional problem

see factoring

Favorite 206, 243

Favorite-Equ 206

Favorite-Geq 206

Favorite-Odd 206

Feige, U. 121, 406

Feigenbaum, J. 168, 405

Feller, W. 51

Fellows, M. 334, 356

Fenner, S. 123, 306, 408

Fermat, P. de 39, 342

FERMAT **318**

Fermat liar **317**, 319

Fermat number *see* number, Fermat

Fermat's Little Theorem

see Theorem, Fermat's Little

Fermat test

see primality test, Fermat

Fermat witness **317**, 319

FewE 119

FewP 119, **123**, 124, 255, 257, 269

FI **252**

Fiat, A. 388, 389, 406

Fiat-Shamir identification scheme

388, 400, 406

see also zero-knowledge

Fibonacci number

see number, Fibonacci

- field **38**
- finite automaton
 - deterministic, *see also* DFA **20**,
21, 22, 48, 53
 - extended transition function of a
20, 21
 - final state of a **20, 21**
 - Gödelization of 48
 - initial state of a **20, 21**
 - language accepted by a **20, 21**
 - nondeterministic, *see also* NFA
21, 22, 48, 52, 53
 - state of a **20, 21**
 - stochastic **263**, 264
 - absorbing state of a **263**
 - transition graph of a
see Markov chain
 - transition function of a **20, 21**
- Fishburn, P. 207, 253
- FL **79**
- F-Liars_n **320**, 321, 325, 331
- forgery
 - existential **372**
 - selective **372**
 - *see also* total break
- formula isomorphism problem,
see also FI **252**
- Forstinger, C. VI
- Fortnow, L. 123, 124, 256, 258, 304–
306, 408
- Fortune, S. 109, 408
- FP **77**, 124
- FP^{NP} 192, 252
- FP-invertibility **110**
- frequency counts method *see* cryptana-
lytic attack, by frequency counts
- Friedberg, R. 121
- Friedberg–Muehnik Theorem
see Theorem, Friedberg–Muehnik
- function
 - associative **394**
 - census, *see also* census_L **109**,
124, 125
 - characteristic, *see also* χ_B **202**
 - commutative **395**
 - composition of —s, *see also* \circ
59
 - computable
see function, partial recursive
 - domain of a, *see also* $D_{(\cdot)}$ **28**,
57
 - Euler *see* Euler function
 - exponential
 - modular — with module p and
base r , *see also* $\exp_{r,p}$ **39**,
359
 - with linear exponent,
see also 2^{Lin} 59
 - with polynomial exponent,
see also 2^{Pol} 59
 - FP-invertible *see* FP-invertibility
 - growth rate of a **59**, 61, 62
 - honest **110**, 393, 401
 - linear, *see also* Lin 59
 - logarithm, *see also* \log 16
 - discrete — with module p and base r ,
see also $\log_r \alpha \bmod p$ **39**, 359
 - log-space computable,
see also FL **79**
 - one-way *see* one-way function
 - partial recursive, *see also* IP
25
 - Gödelization of —s 57
 - effective enumeration of —s
see function, partial recursive,
Gödelization of —s
 - polynomial, *see also* Pol 59
 - polynomial-time computable,
see also FP **77**
 - productive **110**
 - range of a, *see also* $R_{(\cdot)}$ **28**
 - s-honest **393**, 401
 - social choice *see* social choice
function; *see* SCF
 - space, *see also* $\text{Space}_M(\cdot)$ **56**
 - space-constructible **67**, 115
 - time, *see also* $\text{Time}_M(\cdot)$ **56**
 - time-constructible **67**, 115
 - total 25

– total recursive, *see also* \mathbb{R} **25**,
57

function class, *see also* complexity
class

- closure of a
 - under addition **289, 301**
 - under binomial coefficients **289**,
301, 302
 - under exponentiation **289, 301**,
302
 - under limited composition **289**,
301, 302
 - under multiplication **289, 301**
 - under subtraction **289, 301**

function symbol **34**

Furst, M. 306

G

γ -reducibility 257

GA **43**

Gabarró, J. 8, 118, 305, 405

Gács, P. 305

Gál, A. 122, 247

Gandalf 383, 384

Ganesan, K. 123

GAP 55, **82**, 121

$\text{GAP}_{\text{acyclic}}$ **86**, 87, 116

gap_M **289**

GapP 260, 288, **289**, 291, 292, 301,
302, 304, 306

- closure properties of,
see function class, closure of a

GapP-low 290, 291

Garey, M. 8, 62, 88, 99, 118, 120,
250

Gasarch, W. 106

Gauß, C. 124

Gaussian elimination 124

$\text{gcd}(\cdot, \cdot)$ **10**

GCHQ *see* Government Communi-
cations Head Quarters

GI **43**

Gibb's Lemma, *see also* entropy,
properties of **158**

Gill, J. 258, 305

GNI **294**

Gödel, K. 27, 120

Gödelization

- *see* finite automata, Gödelization
of
- *see* function, partial recursive,
Gödelization of —s
- *see* Turing machine, Gödelization
of —s

Gödel number *see* number, Gödel

Goethe, J. W. von 171

golden cut 14, **47**

Goldreich–Micali–Wigderson protocol
384–388, 400, 406

Goldreich, O. 8, 168, 251, 305, 307,
355, 384, 387, 388, 404–406

Goldschlager, L. 306

Goldsmith, J. V, 122–124

Goldwasser, S. 8, 168, 305, 307,
350, 405, 407

Golumbic, M. 51, 118, 120

Gottlob, G. 251, 254

Government Communications Head
Quarters 355

grammar **17**

- context-free **19**
- context-sensitive **19**
- derivation relation with respect to
a, *see also* \vdash **18**
- reflexive, transitive closure of \vdash ,
see also \vdash^* **18**
- language of a **17**
- productions of a
see grammar, rules of a
- rules of a **17**
- start symbol of a **17**
- terminals of a **17**
- nonterminals of a **17**
- regular **19**
- type 0 **19**
- type of a **19**
- variables of a
see grammar, nonterminals of a
- words of a **18**

graph **43**, 81

- alternating **231**
 reachability in an **231**
- bipartite **98, 121**
- critical **248**
- deck of a **307**
- directed **81**
 acyclic **86**
 cycle in a **86**
 hamiltonian circuit in a **246**
 path in a **82**
- edge set of a, *see also* $E(\cdot)$ **81**
- isomorphic —s, *see also* \cong **43**
- join of —s, *see also* \bowtie **189, 243**
- minimum degree of a, *see also* $\text{min-deg}(\cdot)$ **97, 181**
- network **172**
- planar **248**
- simple **43**
- undirected **93**
 automorphism of an
 see automorphism of a graph
- chromatic number of an
 see number, chromatic
- clique of an **93**
- coloring of an **95**
- domatic number of an
 see number, domatic
- dominating set of an **96, 172**
- hamiltonian circuit in an **246**
- independence number of an
 see number, independence
- independent set of an **93**
- isomorphism between —s
 see isomorphism between graphs
- k -colorable **95**
- vertex cover of an **93**
- vertex set of a, *see also* $V(\cdot)$ **81**
- graph accessibility problem, *see also* GAP **55, 82, 82, 121**
- alternating, *see also* AGAP **231**
- restricted to acyclic graphs,
 see also GAP_{acyclic} **86, 86, 87, 116**
- graph automorphism problem,
 see also GA **43, 307**
- graph isomorphism problem,
 see also GI **5, 7, 55, 43, 106, 107, 117, 121, 122, 171, 241, 252, 257, 292–300, 303, 306–308, 334, 384–388, 400, 406**
- smallest solution of the **192**
- graph nonisomorphism problem,
 see also GNI **294**
- Graph Reconstruction Conjecture **307, 308**
- graph three-colorability problem
 see 3-Colorability
- greatest common divisor, *see also* $\text{gcd}(\cdot, \cdot)$ **10**
- Green, F. **306**
- Greibach, S. **66**
- Grollmann, J. **123, 407, 408**
- Große, A. **V, VI, 122, 247, 252**
- group **37**
 - abelian **38**
 - commutative **38**
 - closure property of a **37**
 - inverse element in a **37**
 - neutral element of a **37**
 - order of a finite — **38**
 - order of a — element **37**
 - operation, *see also* \circ **37**
 - permutation
 see permutation group
 - subgroup of a, *see also* \leq **38**
- group axioms **37**
- Gundermann, T. **249, 250**
- Gupta, S. **306**
- Gurevich, Y. **249**
- Guruswami, V. **185, 188, 250**
- Guruswami–Khanna reduction
 185, 189, 250

HHalevi, S. **122, 247**

- Halldórsson, M. 8, 121, 251
 halting problem 235
 Han, Y. 305
 hamiltonian circuit problem **246**
 – for directed graphs **246**
 – for undirected graphs **246**
 Harary, J. 51
 hardness *see* \leq_m^{\log} -hardness;
see \leq_m^P -hardness;
see \leq_T^P -hardness;
see \leq_{tt}^P -hardness;
see $BH_k(NP)$ -hard;
see Δ_2^P -hard;
see coNP-hard;
see NP-hard;
see Θ_2^P -hard
 Hardy, G. 51
 Hartmanis, J. 6, 108–111, 119, 122,
 123, 125, 255
 hashing
 – universal **293**, 307
 hashing function **293**
 – family of —s **293**
 collision-free **293**
 Hassan, N. V
 Håstad, J. 305, 350, 356, 405
 Hausdorff, F. 175, 249
 Hausdorff hierarchy **175**, 250
 – *see also* boolean hierarchy, normal form
 Hay, L. 216, 254
 Heggernes, P. 250
 Heller, H. 281, 305, 405
 Hellman, M. 7, 355, 357, 358, 389,
 404, 406, 407
 Hemachandra, L.
see Hemaspaandra, L.
 Hemaspaandra, E. V, 119, 121, 218,
 251–254, 256, 257, 308
 Hemaspaandra, L. V, 8, 62, 111,
 118, 119, 122–125, 175, 216,
 218, 249, 250, 252–258, 302,
 305–308, 401, 402, 407, 408
 Hempel, H. VI, 218, 256, 257
 Hennie, F. 70, 119
 HH **232**, 234, 235, 239, 240, 246
 hierarchy
 – alternating sums
see alternating sums hierarchy
 – Arthur-Merlin
see Arthur-Merlin games
 – boolean *see* boolean hierarchy
 normal form *see* boolean hierarchy normal form
 – Chomsky
see Chomsky hierarchy
 – counting
see counting hierarchy
 – Hausdorff
see Hausdorff hierarchy
 – high *see* high hierarchy
 – low *see* low hierarchy
 – nested difference
see nested difference hierarchy
 – parallel query *see* query hierarchy over NP, parallel
 – polynomial
see polynomial hierarchy
 – query *see* query hierarchy over NP
 – space *see* space hierarchy
 – symmetric difference *see* symmetric difference hierarchy
 – time *see* time hierarchy
 – truth-table query *see* query hierarchy over NP, parallel
 – union-of-differences
see Hausdorff hierarchy
 High₀ 233, 292
 High₁ 233
 High₂ 292
 high hierarchy, *see also* HH 6,
232, 234, 235, 239, 240, 246,
 257
 – first level of the *see* High₁
 – *k*th level of the *see* High_{*k*}
 – second level of the *see* High₂
 – zeroth level of the *see* High₀
 High_{*k*} **232**, 234, 235, 238, 240, 246
 highness 232, 238, 257
see also high hierarchy

- Hill cipher *see* cipher, Hill
 Hinrichs, M. VI
 Hoffman, C. 307
 Hoffstein, J. 406
 Hofmann, A. VI
 Holy Grail 4, 383
 Homan, C. V, 407, 408
 Homer, S. 8, 118, 51, 123, 123, 255
 honesty *see* function, honest
 Hopcroft, J. 51, 99, 408
 Hörner, H. 406
 Huang, M. 356
- I**
 IBM 169
 id 41
 id 41
 idempotence 31
 Immerman, N. 77, 119, 121
 immunity 258
 Impagliazzo, R. 407
 impersonation attack *see* attack, im-
 personation
 implication, *see also* \implies 29, 30
 impossibility theorem 206
 independence number problems 202
 – IN-Equ 202, 204, 245
 – IN-Geq 202, 204, 245, 253
 – IN-0dd 202, 204, 245, 253
 independence of irrelevant alternatives
 206
 independent set problem, *see also*
 IS 93, 94, 116
 – approximation heuristics for the
 254
 information and coding theory *see*
 theory, information and coding
 integer linear programming
see linear programming
 problem, integer
 integer *see* number, integer
 interactive proof system
see proof system, interactive
 intruder-in-the-middle attack
see attack, man-in-the-middle
- IP 244, 305, 306
 – *see also* proof system, interactive
 IS 93, 94, 116
 ISO(\cdot, \cdot) 43
 isomorphism
 – between boolean formulas 252
 – between graphs,
see also ISO(\cdot, \cdot) 43
 – between sets 108
 isomorphism conjecture 6, 108, 109,
 110, 122, 125, 255, 408
 Ito, T. 405
 Iwama, K. 261, 304
- J**
 Jacobi symbol, *see also* $\left(\frac{m}{n}\right)$ 40
 Jacobson, N. 51
 Jensen’s inequality 157, 158
 Jerschow, Y. 4
 Jha, S. 119
 Jiang, Z. V, 258
 Johnson, D. 8, 62, 88, 99, 118, 120,
 250
 Jones, N. 121
 Joseph, D. 110, 111, 122, 123
 jump operator 235
- K**
 $\kappa(\cdot)$ 103, 208
 K 235, 236, 246
 $K(\cdot)$ 236, 238, 246
 K^n 236, 237, 238, 246
 $K^n(\cdot)$ 236, 237, 238, 246
 K-operator *see* $K(\cdot)$; *see* K
 – iterated *see* $K^n(\cdot)$; *see* K^n
 Kadin, J. 217, 218, 249, 254–256
 Kahn, D. 168
 Kann, V. 8, 251
 Kaplan, H. 120
 Karp, R. 99, 120, 254
 Karp–Lipton Theorem
see Theorem, Karp–Lipton
 Karpinski, M. 8, 251
 Kaliski, B. 169, 356

Kasiski, F. 140, 141, 143, 145, 151, 163, 168
 Kasiski's method **140**, 141, 143, 145, 163
 see also cryptanalytic attack, on the Vigenère cipher
 Kayal, N. 106, 118, 309, 333, 342, 355, 356
k-CNF **31**
k-Colorability **95**
 Kellerer, H. 406
 Kelly, P. 307
 Kemenization
 – local 254
 Kemeny election system 253, 254
 Kerckhoffs von Nieuwenhof, J. 129
 Kerckhoffs's Principle **129**
 key **127**
 – spurious **167**
 key equivocation 151, 155, **159**, 160
 key-only attack *see* attack, key-only
 key space **127**
 key stream *see* cipher, stream
 Khanna, S. 185, 188, 250, 251
 Khuller, S. 252
 Kiometzis, C. VI
 Kleene, S. 17, 51, 394
 knapsack problem 5, 98, **104**
 – high-density 406
 – low-density 406
 known-plaintext attack *see* attack, known-plaintext
 Ko, K. 8, 118, 123, 257, 306, 405, 408
 Köbler, J. 121, 216, 250, 254, 255, 257, 258, 303, 305–308, 405
 Koblitz, N. 334, 355, 356
 Königstein, G. VI
 Kortsarz, G. 121
 Kozen, D. 257
 Kratsch, D. VI, 307
 Krentel, M. 252, 254
k-SAT **83**, 304
 Kumar, R. 168, 254, 407
 Kuroda, S. 77

Kurosawa, K. 405
 Kurtz, S. 111, 122, 123, 306
 Kurur, P. 297, 307

L

L **61**, 69, 72, 81, 122, 193, 116, 244
 $L(\cdot)$ 56, **25**
 \mathcal{L}_0 **19**, 20, 28
 \mathcal{L}_1 *see* CS
 \mathcal{L}_2 *see* CF
 \mathcal{L}_3 *see* REG
 Laaser, W. 121
 Ladner, R. 106, 106, 121, 121, 241, 252
 Lagarias, J. 406, 407
 Lagrange, J. 39
 Lagrange's Theorem
 see Theorem, Lagrange's
 LaMacchia, B. 404
 Landers-Appell, C. V
 Landers-Appell, K. V
 Landry, F. 342
 Lange, K. 257
 language **16**
 – cardinality of a **16**
 – complement of a, *see also* $\bar{}$ **17**
 – concatenation of —es **17**
 – context-free, *see also* CF; \mathcal{L}_2 **19**, 20, 50
 – context-sensitive, *see also* CS; \mathcal{L}_1 **19**, 20, 77
 – ε -free iteration, *see also* $^+$ **17**
 – formal **16**
 – intersection of —es, *see also* \cap **17**
 – iteration of a, *see also* * **17**
 – Kleene closure of a
 see language, iteration of a
 – nontrivial **78**
 – operation on —es **17**
 – recursively enumerable, *see also* RE **27**, 28
 – reduction to a 254, 255
 – redundancy of a 167, 169

- regular, *see also* REG; \mathcal{L}_3 **19**, 20, 50
- sparse 109, 110, 119, 122, 123, 125, **218**, 254, 257
- tally **71**, 124, 125
 - binary representation of a, *see also* Bin(\cdot) **71**
 - tally encoding of a, *see also* Tally(\cdot) **71**
 - type 0, *see also* \mathcal{L}_0 **19**, 20, 28
 - type of a **19**
 - union of —es, *see also* \cup **17**
- Las Vegas algorithm *see* algorithm, Las Vegas
- lattice problem 350, 406, 408
 - average-case hardness of —s 408
 - worst-case hardness of —s 408
- lattice reduction 350, 406, 408
- lattice-based cryptography
 - see* cryptography, lattice-based
- Lautemann, C. 305
- Legendre symbol, *see also* $\left(\frac{m}{n}\right)$ **40**
- legitimate deck *see* deck, legitimate
- Legitimate-Deck **307**, 308
- Leibert, M. V
- Leiserson, C. 51
- Le Lasseur, H. 342
- Lenstra, A. 342, 356, 406
- Lenstra Jr., H. 104, 342, 344, 356, 402, 406
- LERC **296**, 297–299
- Levin, L. 88, 120
- Lewis, P. 119
- LH **232**, 234, 235, 239, 240, 246
- Lien, Y. 121
- Lin **59**
- Lin(\cdot) **59**
- Lindner, C. 4
- linear bounded automaton **26**
- linear feedback shift register **151**
- linear programming problem **104**, 249, 253, 253
 - integer 104, 253
- linear space
 - deterministic *see* LINSPACE
 - nondeterministic *see* NLINSPACE
- linear speed-up theorem
 - see* theorem, linear speed-up
- linear tape-compression theorem
 - see* theorem, linear tape-compression
- linear time *see* LINTIME
- Linial, N. 251
- LINSPACE **61**, 69, 115
- LINTIME **61**, 66
- Lipton, R. 122, 247, 254
- Lischke, G. VI, 258
- Liśkiewicz, M. 124
- LLL algorithm 406
- log 16
- logarithm function
 - see* function, logarithm
- logarithmic space
 - alternating *see* AL
 - deterministic *see* L
 - nondeterministic *see* NL
- logic 4, **29–37**, 51
 - modal 254
 - nonmonotonic 252
 - predicate **34–37**
 - first-order 37
 - second-order 37
 - propositional **29–33**
- $\log_r \alpha \bmod p$ **39**
- Long, T. 123, 255, 257, 258
- Longpré, L. 119, 255
- Lovász, L. 249, 406
- Low₀ 233
- Low₁ 233
- Low₂ 288, 290, 292, 294, 295
- low-exponent attack **349**, 356
- low hierarchy, *see also* LH 6, 7, 171, **232**, 234, 235, 239, 240, 246, 257, 258
 - extended, *see also* ELow_k **258**,
 - first level of the *see* Low₁
 - k th level of the *see* Low_k
 - second level of the *see* Low₂;
see also Σ_2^p -low
 - zeroth level of the *see* Low₀

- Low_k **232**, 234, 235, 238, 240, 246, 290
 lowness 232, 238, 257, 260, 288, **290**, 292–300, 304, 305, 307
see also low hierarchy;
see also self-lowness
 Luby, M. 8, 168
 Lund, C. 251
 Lutz, D. V
 Lynch, N. 121, 252
- M**
 MA **284**, 285–288, 290, 301, 304, 305, 308
 – *see also* Arthur-Merlin games
 Mahaney, S. 109, 111, 122, 123, 255
 majority quantifier
 – *see* quantifier, polynomially length-bounded, majority
 – *see* \exists^+
 majority rule **207**
 – defeat according to the **207**
 – win according to the **207**
 – winner according to the
see Condorcet winner
 Majority-SAT **272**
 MAM **284**, 285, 286, 301
 – *see also* Arthur-Merlin games
 Manasse, M. 342
 Manders, K. 257
 man-in-the-middle attack
see attack, man-in-the-middle
 many-one reducibility
see reducibility, many-one;
see \leq_m^{\log} ;
see \leq_m^p
- Markov chain **263**, 264
 marriage problem *see* matching problem, bipartite
 matching
 – bipartite 98
 – tripartite 99, 117
 matching problem **98**
 – bipartite 98
 – three-dimensional
see 3-DM
 – tripartite *see* matching problem, three-dimensional
 – two-dimensional
see matching problem, bipartite
- matrix
 – adjoint *see* adjoint matrix
 – determinant of a, *see also* det 124, **138**, 167
 – inverse of a **138**
 – permanent of a,
see also $perm(\cdot)$ **124**
 Maurer, U. 408
 Mauve, M. VI
 maximal non-hamiltonian circuit problem **246**, 249
 – for directed graphs,
see also MNHC **246**, 249
 – for undirected graphs,
see also MDNHC **246**
 Max-SetPacking-Geq **208**, 245
 May, A. 356
 Mayer, I. VI
 MEE-DNF 245, **251**
 Merkle–Hellman cryptosystem 357, **389–392**, 401, 402, 406, 407
 – iterated 406
 – security of the *see* cryptanalytic attack, on Merkle–Hellman
 Merkle, R. 357, 389, 406, 407
 Merlin, *see also*
 Arthur-Merlin games 4
 Merz, J. VI
 message *see* plaintext
 message authentication **130**
 message integrity **130**
 message space *see* plaintext space
 Meyer, A. 107, 121, 251, 254
 Meyer, G. 248
 Micali, S. 305, 307, 384, 387, 388, 405, 406
 Micciancio, D. 8, 168
 Miller, G. 7, 309, 321–327, 333, 352, 354–356

MILLER-RABIN **322**
 Miller–Rabin liar *see* MR-liar
 Miller–Rabin test *see* primality test,
 Miller–Rabin
 Miller–Rabin witness
 see MR-witness
 mind-change technique **214**
min-deg(\cdot) **97**, 181
 Minimal-3-Uncolorability **248**,
 – restricted to planar graphs 248
 Minimal-3-UNSAT **248**, 247
 minimum equivalent expression prob-
 lem, *see also* MEE-DNF 171,
 245, **251**
 MDNHC **246**
 MNHC **246**, 249
 mod *see* congruence modulo an
 integer
 modular *see also* function, logarithm,
 discrete — with module p and
 base r
 Monien, B. 261, 263
 monoalphabetic cryptosystem 131,
 132, **134**, 135, 140, 142, 167–
 169
 monoid **37**
 – abelian **38**
 – commutative **38**
 Monte Carlo algorithm
 see algorithm, Monte Carlo
 Moore, J. 356
 Moran, S. 7, 305, 405
 Morgenstern, C. 161
 Morrison, M. 342
 Mothers of Invention 163
 Muchnik, A. 121
 Motwani, R. 51, 251
 MR-liar **323**
 MR-Liars $_n$ **325**, 353
 MR-LIARS $_n$ **325**, 326
 MR-witness **323**
 Müller, H. VI, 258
 multiset **207**

N

\mathbb{N} **10**
 Nader, R. 206
 Naik, A. 121, 123, 408
 nail file *see* tools, nail file
 Naor, M. 254, 407
 Nasser, N. 250
 natural *see* number, natural
 Navajo code 169
 NE **61**, 71, 116, 124
 negation, *see also* \neg **29**, 30
 nested difference hierarchy 175, **176**,
 250, 250
 – *see also* boolean hierarchy, nor-
 mal form
 network
 – communication **172**
 – computer 172, **172**
 NEXP **61**
 NEXPSPACE **61**
 NFA **21**, 22, 48
 Nguyen, P. 168, 407
 Niedermeier, R. 257
 NIST 170, 404
 NL 5, **61**, 72, 76, 77, 81, 82, 84, 86,
 116, 121, 122
 NL-complete 82, 84, 86, 116, 121,
 122
 see also \leq_m^{\log} -completeness
 NLINSPACE **61**, 77, 115
 Nöckel, B. VI
 nonapproximability 8, 121, 251, 254
 nondeterministic polynomial time
 see NP
 nondictatorship 206
 nonresidue
 – quadratic, *see also* QNR **40**
 Norris, M. 345, 356
 NOTM **28**
 NP 5, **61**, 71, 72, 78, 106–110, 116,
 118, 120, 122, 123, 125, 174,
 176, 177, 179, 184, 191, 193–
 196, 218, 232–236, 238, 241,
 248, 253–256, 241, 243, 244,
 246, 247, 269, 276–278, 290,

- 292, 285, 288, 308, 353, 384, 395, 398, 406–408
 - certificate of an problem
see witness
 - P versus NP question 5, **106–108**, 120
 - solution of an problem
see witness
 - $\leq_{\text{tt}}^{\text{p}}$ -closure of,
see also $\text{P}_{\text{tt}}^{\text{NP}}$ **213**, 254
 - NP^{c} **193**, 244
 - NP-complete 5, 6, 7, 88, 92, 93, 95, 97, 100, 103, 105, 106, 108, 109, 116, 120, 121, 236, 241, 243, 246–248, 253, 255, 333, 334, 356, 357
see also $\leq_{\text{m}}^{\text{log}}$ -completeness;
see also $\leq_{\text{m}}^{\text{p}}$ -completeness
 - exact variant of — problems 6, 171, 173, 248
 - *see also* theory of NP-completeness
 - NP-hard 172, 185, 241, 249, 251–253
 - NP^{NP} , *see also* Σ_2^{p} 194, 195, 196, 245
 - NPOTM **28**, 193
 - NP^{P} 193, 244
 - $\text{NP}^{\text{PSPACE}}$ 193, 244
 - NPSpace **61**, 76
 - NSF VI
 - $\text{NSpace}_M(\cdot)$ **58**
 - $\text{NSpace}(\cdot)$ **59**, 66, 74, 77, 114, 228, 231
 - NTM **23**, 56
 - $\text{NTime}_M(\cdot)$ **58**
 - $\text{NTime}(\cdot)$ **59**, 66, 74, 114, 225, 228
 - NTRU cryptosystem 406
 - Nugent, R. VI
 - number
 - Blum **378**
 - Carmichael **319**, 320, 321, 323, 325, 326, 352, 353
 - chromatic, *see also* $\chi(\cdot)$ **95**
 - domatic, *see also* $\delta(\cdot)$ **97**, 121, 172
 - Fermat, *see also* F_m **342**, 354
 - Fibonacci, *see also* f_n **12**
 - Gödel **27**
 - independence, *see also* $\alpha(\cdot)$ **202**
 - integer, *see also* \mathbb{Z} 10
 - natural, *see also* \mathbb{N} **10**
 - binary representation of a,
see also $\text{bin}(\cdot)$ 17
 - prime 38, **315**
 - primitive element of a **7**, 358
 - rational, *see also* \mathbb{Q} 49
 - real, *see also* \mathbb{R} 49
 - RSA- d 342, 343
 - number theory *see* theory, number
- O**
- $o(\cdot)$ **60**
 - $\mathcal{O}(\cdot)$ 16, 34, **59**
 - $\tilde{\mathcal{O}}(\cdot)$ **260**
 - Odd- k -SAT **213**
 - Odd-Max-SAT **252**
 - Odd-SAT **245**
 - Odifreddi, P. 51
 - Odlyzko, A. 404, 406, 407
 - OFB **149**, 165
 - Ogihara, M. V, 8, 62, 109, 118, 121, 122, 124, 218, 250, 255, 256, 302, 305, 306
 - Ogiwara, M. *see* Ogihara, M.
 - one-time pad
see Vernam’s one-time pad
 - one-way conjecture **111**
 - one-way function 2, 5, 8, 108, **110**, 111, 123, 123,
 - associative **394**
 - commutative **395**
 - polynomial-to-one 123
 - one-to-one 123
 - onto 113, 117
 - strong **393**, **394**, 395, 401
 - trapdoor 8, **389**, 390
 - worst-case 357, 361, 392, 407, 408

one-way/isomorphism conjecture **111**
 one-way permutation **124**
 Orponen, P. 257
 Ottmann, T. 51
 output feedback mode *see* OFB

P

Π_2^p , *see also* coNP^{NP} **194**, 195,
 196, 251, 252, 256, 281, 283,
 286–288, 308
 $\Pi_2^{\text{p,AM} \cap \text{coAM}}$ 287
 Π_2^p -complete 251, 252
 Π_3^p 278
 Π_i^p **194**, 195, 196, 198, 200, 256
 Π_i^p -complete 200, 217, 218
 $\Pi_i\text{SAT}$ **200**, 244
 $\Pi_i\text{SAT}$ formula **200**
 P 5, 6, **61**, 70–72, 78, 106, 108,
 109, 111–113, 116, 120–122, 174,
 176, 177, 191, 193–196, 198,
 231–233, 241, 244, 260, 269,
 279, 290, 308, 333, 355, 356,
 407, 408
 – P versus NP question 5, **106–**
108, 120

P 25

$\mathfrak{P}(\cdot)$ **103**
 P^C **193**, 244
 P^{NP} , *see also* Δ_2^p 194–196
 $\text{P}^A[k]$ **213**
 $\text{P}^C[k]$ **213**
 $\text{P}^{\text{NP}[k]}$ **212**, 213
 $\text{P}^{\text{NP}[\mathcal{O}(1)]}$ **212**, 216
 $\text{P}^{\text{NP}[\mathcal{O}(\log)]}$, *see also* Θ_2^p **202**, **212**,
 216, 254, 255
 $\text{P}^{\Sigma_{i-1}^p[\mathcal{O}(\log)]}$ **202**
 $\text{P}_{k\text{-tt}}^A$ **213**
 $\text{P}_{k\text{-tt}}^C$ **213**
 $\text{P}_{k\text{-tt}}^{\text{NP}}$ 253
 $\text{P}_{k\text{-tt}}^{\text{bfNP}}$ **213**, 216, 254
 $\text{P}_{k\text{-tt}}^{\text{bitNP}}$ **213**
 $\text{P}_{k\text{-tt}}^{\Sigma_i^p}$ 256
 $\text{P}_{k\text{-tt}}^{\Sigma_i^p}$ 256
 P_{tt}^C **203**
 $\text{P}_{\text{tt}}^{\text{NP}}$ **213**, 216, 253, 254

$\text{P}^{\text{NP}^{\text{NP}}}$, *see also* Δ_3^p 195, 256
 P^P 193, 244
 P^{PP} 306, 308
 $\text{P}^{\text{PP}^{\text{PH}}}$ 306
 P^{PSPACE} 193, 244
 P^{SPP} 291
 Papadimitriou, C. 8, 51, 118, 173,
 202, 248, 249, 252, 305, 306,
 405
 parallel access to NP, *see also* Θ_2^p ;
 $\text{P}^{\text{NP}[\mathcal{O}(\log)]}$; $\text{P}_{\text{tt}}^{\text{NP}}$ 201, **203**, 206,
 208, 254
 parallel oracle access 203
 parallel time 228
 Parberry, I. 306
 Pareto Principle 206
 partial order
 – polynomially length-related **107**
 – polynomially well-founded **107**
 partial recursive function
see function, partial recursive
 Pasanen, K. V, 401, 407
 Paterson, M. 107, 121
 Paturi, R. 261, 304
 Paula *see* Rothe, P.
 Pavan, A. 124
 P-complete 121, 122, 231, 232, 238,
 239
 PCP **251**
 PCP theorem *see* theorem, PCP
 perfect secrecy 6, **151–155**, 166
 $\text{perm}(\cdot)$ **124**
 permanent of a matrix
see matrix, permanent of a
 permutation, *see also* \mathfrak{S}_n **41**
 – composition of —s, **41**
 permutation group **41**
 – complete right transversal in a
42
 – generator of a **42**
 – identity of a, *see also* id **41**
 – (pointwise) stabilizer in a **42**
 – right co-set of a **42**
 – strong generator of a **42**
 – tower of stabilizers in a **42**

- Petrack, E. 122, 247
 Pferschy, U. 406
 PH 125, 171, **194**, 195, 196, 198, 200, 217, 218, 234, 244, 249, 252, 254–256, 308
 PHT **217**
 Pipher, J. 406
 Pisinger, D. 406
 p -isomorphism, *see also* \cong_p **108**, 117
 plaintext **127**
 plaintext space **127**
 Poe, Edgar A. 127, 167
 Pollard, J. 335, 336, 341, 342, 344, 353, 356
 POLLARD **335**
 Pollard's $p - 1$ factoring algorithm, *see also* POLLARD **335**, 336, 341, 342, 344, 353, 356
 IPol **59**
 IPol(\cdot) **59**
 polyalphabetic cryptosystem **135**, 136, 140, 163
 polygamy 4, 99
 POLYLOGSPACE **69**, 115
 polymer chemistry 124
 polynomial hierarchy, *see also* PH 6, 125, 171, **194**, 195, 196, 198, 200, 217, 218, 232, 234, 235, 240, 251, 252, 254, 257, 259, 275, 279, 284, 286, 292, 295, 305–307
 – collapse of the 198, 217, 218, 234, 235, 240, 249, 252, 255–257, 295
 – downward collapse within the 256
 – i th level of the, *see also* Σ_i^p ; Π_i^p ; Δ_i^p ; Θ_i^p **194**, 195, 196, 198, 200, 201, 217, 218, 232, 234, 237, 238, 240, 246, 256, 257
 – second level of the, *see also* Σ_2^p ; NP^{NP} ; Π_2^p ; coNP^{NP} ; Δ_2^p ; P^{NP} ; Θ_2^p ; $\text{P}^{\text{NP}[O(\log)]}$ **194**, 195, 196, 212, 245, 251, 252, 256, 257
 Polynomial Hierarchy Tower, *see also* PHT 217
 polynomial-size 254, 257
 polynomial space
 – deterministic *see* PSPACE
 – nondeterministic *see* NPSPACE
 polynomial time **61**
 – alternating *see* AP
 – deterministic *see* P
 – nondeterministic *see* NP
 – probabilistic *see* PP
 bounded-error — *see* BPP
 one-sided error — *see* RP; *see also* coRP
 stoic — *see* SPP
 zero-error — *see* ZPP
 – random *see* RP
 – unambiguous *see* UP
 Polytope(\cdot) 249
 Pomerance, C. 356
 Porta, G. 168
 Post, E. 121
 Post's problem 121
 Potthoff, M. VI
 PP 6, 7, 124, 257, 259, **268**, 269, 272, 275, 288–292, 296, 300, 301, 303–306, 308
 PP-complete 7, 272
 PP-low 291, 306, 308
 PP_{path} 301, **303**, 304
 P-printability **123**, 125
 PP^{SPP} 291
 Pr(\cdot) **46**
 Pr($\cdot | \cdot$) **46**
 Pratt, V. 118
 predicate symbol **34**
 preference order **207**
 preference profile **207**
 prefix search 191, 220
 primality problem, *see also* Primes 7, 62, 106, 118, 309, **315**, 316–319, 322, 324, 328, 331, 333, 334, 352, 355, 356

- primality test 7, **315–333**
 - Fermat, *see also* FERMAT 7, **317–321**, 324, 351
 - Miller–Rabin, *see also* MILLER-RABIN 7, 309, **321–327**, 352, 354, 356
 - Solovay–Strassen, *see also* SOLOVAY-STRASSEN 7, 309, **327–333**, 356
- prime number *see* number, prime
- prime number theorem *see* theorem, prime number
- Primes 315
- primitive element *see* number, primitive element of a
- private-key cryptography *see* cryptography, private-key
- private-key cryptosystem *see* cryptosystem, private-key
- probabilistically checkable proof system *see* proof system, probabilistically checkable
- probabilistic polynomial time *see* PP
 - bounded-error *see* BPP
 - one-sided error *see* RP; *see also* coRP
 - stoic *see* SPP
 - zero-error *see* ZPP
- probability, *see also* $\Pr(\cdot)$ **46**
 - conditional, *see also* $\Pr(\cdot | \cdot)$ **46**
- probability amplification 7, 270, 274
- probability distribution **46**
 - uniform **46**
- probability space **46**
- probability theory *see* theory, probability
- problem of breaking ElGamal *see* break-elgama1
- problem of breaking Rabin *see* break-rabin
- projection theorem *see* theorem, projection
- promise class 55, **269**, 271, 274, 290, 301, 306
- promise problem 306, 307, 407
- proof system
 - interactive 2, 7, 251, 252, 256 *see also* Arthur-Merlin games
 - probabilistically checkable, *see also* PCP 251
- prover 305
 - *see also* proof system, interactive
 - *see also* zero-knowledge protocol
- proof verification 251 *see also* PCP
- protocol
 - authentication *see* authentication protocol
 - challenge-and-response *see* challenge-and-response protocol
 - digital signature
 - ElGamal *see* ElGamal digital signature
 - Rabi–Sherman *see* Rabi-Sherman digital signature
 - RSA *see* RSA digital signature
 - ElGamal *see* ElGamal cryptosystem
 - Merkle–Hellman *see* Merkle–Hellman cryptosystem
 - Rabin *see* Rabin cryptosystem
 - RSA *see* RSA cryptosystem
 - secret-key agreement
 - Diffie–Hellman *see* Diffie–Hellman protocol
 - Rivest–Sherman *see* Rivest–Sherman protocol
 - Shamir’s no-key *see* Shamir’s no-key protocol
 - zero-knowledge *see* zero-knowledge protocol
- p-selectivity *see* set, p-selective
- PSPACE 6, **61**, 69, 72, 76, 78, 115, 193, 194, 200, 201, 228, 241, 244, 269, 306, 308
- PSPACE-complete 200, 228, 244
- public-key cryptography *see* cryptography, public-key
- public-key cryptosystem *see* cryptosystem, public-key
- Pumping Lemma

- for context-free languages **50**
 - for regular languages **50**
- Q**
- Q** **49**
- QBF** **32**
- QBF** **199**, 200, 201, 228, 244
- QBF_{simple}** **244**
- $(\Omega_1 \mid \Omega_2)$ **278**
- quadratic nonresidue
see nonresidue, quadratic
- quadratic residue
see residue, quadratic
- quadratic sieve *see* factoring
 algorithm, quadratic sieve
- QNR** **40**
- QR** **40**, 371
- QR_p** **371**
- quantified boolean formula,
see also **QBF** **32**
- closed **32**
 - open **32**
 - in prenex form **33**
 - satisfiable **36**
 - simple, *see also* **QBF_{simple}** **244**
 - valid **36**
- quantified boolean formula problem
199
- with a bounded number of alter-
 nations, *see also* Σ_i SAT;
 Π_i SAT **6**, **200**, 244
 - with an unbounded number of al-
 ternations, *see also* **QBF** **6**,
199, 200, 201
- quantifier
- existential, *see also* \exists ; \bigvee **32**
 - polynomially length-bounded
 existential, *see also* \exists^p **190**,
191, 196, 198
 - majority, *see also* \exists^+ **278**,
 279–295, 301
 - universal, *see also* \forall^p **190**,
191, 196, 198
 - universal, *see also* \forall ; \bigwedge **32**
- quantifier string **278**
- sensible pair of —s **278**
 - complexity class defined by —s,
see also $(\Omega_1 \mid \Omega_2)$ **278**
- query hierarchy over NP, *see also*
 $P^{NP[\mathcal{O}(1)]}$; $P^{NP[\mathcal{O}(\log)]}$ **6**, **212**,
 254
- k th level of the, *see also* $P^{NP[k]}$
212, 213
 - parallel, *see also* P_{btt}^{NP} ; P_{tt}^{NP} **212**,
213, 254, 256
 - k th level of the,
see also $P_{k\text{-tt}}^{NP}$ **213**
 - truth-table *see* query hierarchy
 over NP, parallel
- query order **257**
- R**
- R** **25**, 57
- \mathbb{R} **49**
- $R_{(\cdot)}$ **28**
- Rabin, M. **357**, 392, 401, 402, 407
- Rabin cryptosystem **357**, **376–381**,
 400, 405
- Rabin, M. **7**, 22, 52, 63, 309, 321–
 327, 333, 352, 354–357, 376–
 381, 400, 405
- Rabin’s Theorem
see Theorem, Rabin’s
- Rabi–Sherman digital signature **401**
- security of the **407**, 408
- Rackoff, C. **123**, 305, 405
- Radziszowski, S. **308**
- Rajasethupathy, K. **254**
- RANDOM-FACTOR **380**, 381
- randomized algorithm
see algorithm, randomized
- random polynomial time *see* RP
- RANDOM-SAT **260**, **264**, 265, 266,
 300, 304
- random walk algorithm
see algorithm, random walk
- random variable **47**
- Ranjan, D. **252**
- Rao, R. **V**, 119

- rate of growth
see function, growth rate of a
- rationals *see* number, rational
- Razborov, A. 306
- RE 27, 28, 121, 191, 235
- real *see* number, real
- real-time, *see also* REALTIME 53, 66, 117
- REALTIME 61, 66
- recursive enumerability *see* language, recursively enumerable;
see also RE
- recursive function theory
see theory, recursive function
- recursively presentable 239, 240, 246
- reducibility 5
- many-one
 - log-space *see also* \leq_m^{\log} 55, 79, 81, 82, 84, 86, 87, 121, 122, 193, 231, 232, 244, 252
 - polynomial-time, *see also* \leq_m^P 55, 77, 78, 116, 120, 185, 193, 194, 236, 238, 239, 244, 246, 252, 255, 272, 276, 292, 295, 301, 307
 - polynomial-time randomized 249, 254
 - polynomial-time truth-table, *see also* \leq_{tt}^P 202, 203, 252, 255
 - disjunctive 255
 - polynomial-time Turing deterministic, *see also* \leq_T^P 125, 193, 194, 238, 244, 246, 252, 254, 255, 306, 362, 370
 - nondeterministic, *see also* \leq_T^{NP} 193, 193, 252, 244
 - positive, *see also* \leq_{pos-T}^P 194, 252, 244
 - randomized 353, 356, 379
 - strong nondeterministic, *see also* \leq_{sT}^{NP} 233, 236, 245, 246, 257
 - *see also* γ -reducibility
 - *see also* self-reducibility
- reflexivity 50, 117
- REG 19, 20, 50
- Reingold, N. 304, 305
- Reischuk, R. 8, 118
- Reith, S. 256
- rejecting computation
see Turing machine, computation of a, rejecting
- number of —s *see* rej_M
- rej_M 289
- relativization 258
- relativized world
 – *see* relativization
- *see* set, oracle
- remainder class 50
- residue
 – quadratic, *see also* QR 40
- class of —s *see* remainder class
- resource *see* complexity measure
- resource function *see* complexity class, resource function of a
- Riege, T. V, VI, 4, 250
- right co-set *see* permutation group, right co-set of a
 – *see also* LERC 42
- Rijmen, V. 170
- ring 38
- commutative 38
 - invertibility in a 38
 - one element of a 38
 - zero element of a 38
- ring automorphism 356
- counting problem for —s, *see also* #RA 356
- ring with one 38
- Rivest, R. 51, 169, 309, 310, 355, 357, 392–395, 398, 401, 402, 406–408
- Rivest–Sherman protocol 357, 392–398
- security of the 407, 408
- Robshaw, M. 356
- Rogers, J. 111, 123, 408
- Rogers Jr., H. 51, 108, 235, 257
- Rohatgi, P. 249, 254
- Rosen, A. 51

- Rosenberg, A. 66
 Rossmanith, P. 257
 Rothe, E. VI, 70, 137, 165, 217, 403, 404
 Rothe, I. VI
 Rothe, J. 119, 122–124, 168, 175, 206, 247, 250–254, 257, 258, 306, 356, 401, 402, 407, 408
 Rothe, P. VI, 70, 142, 165, 217, 403, 404
 Royer, J. 111, 122, 123
 Rozenberg, G. VI
 RP 6, 250, 255, 259, 266, **268**, 269–271, 275, 276, 288, 300, 301, 303, 305, 308, 321
 RP_{path} 269, 301, **303**, 304
 RP_q **270**, 352
 RSA cryptosystem 5, 7, 106, 309, **310–314**, 318, 333–335, 342, 355, 357, 379, 389
 – security of the *see* cryptanalytic attack, on RSA
 RSA digital signature 7, **314**, 351, 372
 – forging —s **341**
 – security of —s *see* cryptanalytic attack, on RSA
 RSA-*d* number *see* number, RSA-*d*
 RSA superencryption **345**, 354, 356
 Rubinstein, R. 123
 Rueppel, R. 168
 Ruling Ring 4, 383
 Russel, A. 255
 Russo, D. 257, 306
- S**
 Σ^* **16**
 Σ_2^p , *see also* NP^{NP} **194**, 195, 196, 245, 251, 252, 256, 257, 281, 283, 286, 287, 292, 295, 304, 307, 308
 $\Sigma_2^{p, \text{AM} \cap \text{coAM}}$ 287, 290
 Σ_2^p -complete 200, 245, 251, 252
 Σ_2^p -low, *see also* Low₂ 287, 290
 Σ_3^p 278
- Σ_i^p **194**, 195, 196, 198, 200, 201, 217, 218, 232, 234, 237, 238, 240, 246, 256, 257
 Σ_i^p -complete 200, 237, 238, 246
 Σ_i SAT **200**, 244
 Σ_i SAT formula **200**
 \mathfrak{S}_n **41**
 $S^{\leq n}$ 109, **218**
 S_2^p **256**
 Saari, D. 206
 Safra, S. 251
 Salomaa, A. VI, 8, 51, 134, 168, 305, 355, 404, 407
 Saruman 383–388, 400
 SAT 55, **83**, 88, 107, 111–113, 218, 249, 259–266, 276
 satisfiability problem 5, 55, **83**, 88, 101, 109, 190, 199, 228, 236, 259–266, 276
 – *see* 2-SAT
 – *see* 3-SAT
 – *see* 4-SAT
 – *see* 5-SAT
 – *see* 6-SAT
 – *see* DNF-SAT
 – *see* *k*-SAT
 – *see* Majority-SAT
 – *see* Minimal-3-UNSAT
 – *see* Odd-*k*-SAT
 – *see* Odd-Max-SAT
 – *see* Odd-SAT
 – *see* SAT
 – *see* SAT-UNSAT
 – *see* Threshold-SAT
 – *see* Unique-SAT
 SAT-UNSAT **218**, 241, 241
 Savitch, W. 74, 120, 121, 200, 227, 244
 Savitch's Theorem
see Theorem, Savitch's
 Saxe, J. 306
 Saxena, A. V
 Saxena, N. 106, 118, 309, 333, 342, 355, 356
 SCF **207**

- Schaefer, M. 252
 Schlüter, T. 4
 Schneider, D. 4
 Schneier, B. 8, 168
 Schnorr, C. 121, 252, 367, 404–406
 Schöning, U. VI, 8, 51, 106, 121, 216, 232, 235, 236, 238, 240, 250, 254, 257, 261, 263, 287, 288, 295, 303–306, 405
 Scott, D. 22, 52
 Seara, C. 254
 search engine 254
 search reducing to decision 122
 secret-key agreement 7, 8, 310, 355, 357, **358** *see also* protocol, secret-key agreement
 secret-key agreement problem 310, **358**
 selective forgery
 see forgery, selective
 self-avoiding walk problem **124**
 self-lowness **290**, 291, 292, 303, 304, 306
 self-reducibility **107**, 109, 114, 121, 252
 – disjunctive **108**
 self-reducibility tree **107**
 Selman, A. 8, 51, 118, 168, 121, 123, 124, 233, 252, 257, 258, 307, 407, 408
 separation 258
 – by immune sets *see* separation, strong
 – strong 258
 – downward *see* upward collapse
 – upward *see* upward separation
 sequential space 228
 set, *see also* language
 – balanced-immune *see* balanced immunity
 – bi-immune *see* bi-immunity
 – choice *see* choice set
 – cofinite 240
 – creative **110**
 – decidable **25**, 191
 – finite 108, 240
 – immune *see* immunity
 – isomorphic —s **108**
 – join of —s, *see also* \oplus **258**
 – k -creative **110**
 – non-p-isomorphic —s **111**
 – non-sparse **109**
 – oracle **28**, 190, 191
 generic 258
 random 258
 – of strings up to length n , *see also* $S^{\leq n}$ **109**, **218**
 – p-isomorphic —s
 see p-isomorphism
 – P-printable *see* P-printability
 – p-selective 252, 257, 258
 – power set of a , *see also* $\mathfrak{P}(\cdot)$ **103**
 – recursively enumerable **27**, 28, 191, 235, 239
 – self-reducible *see* self-reducibility
 – sparse *see* language, sparse
 – symmetric difference of —s, *see also* Δ **239**
 set class, *see also* complexity class
 – closure of a
 boolean **174**, 258
 under complement **174**
 under finite variations **239**, 240, 246
 under intersection **174**, 241, 258
 under union **174**, 241, 258
 – complex intersection of —es, *see also* \wedge **174**, 241
 – complex symmetric difference of —es, *see also* Δ **256**
 – complex union of —es, *see also* \vee **174**, 241
 – co operator, applied to a , *see also* $\text{co}C$ **77**, **174**
 SetCovering **103**
 set covering problem 98, **103**
 Sethupathy, P. 254
 SetPacking **103**, 117
 set packing problem 98, **103**

- set ring **175**, 241
 Sewelson, V. 119
 Shamir, A. 244, 306, 309, 310, 355, 356, 388, 389, 402, 404–407
 Shamir, R. 120
 Shamir’s no-key protocol **403**, 404
 SHANKS **363**, 364, 371, 399
 Shanks, D. 363, 364, 371, 399, 404
 Shannon, C. 6, 151, 153–155, 169
 Shannon’s Theorem
 see Theorem, Shannon’s
 Sherman, A. 169, 357, 392, 394, 395, 401, 402, 407, 408,
 Sheu, M. 258
 shift cipher *see* cipher, shift
 s-honesty *see* function, s-honest
 shortest lattice vector problem 408
 Shoenfield, J. 51
 sieve of Eratosthenes **316**, 334, 335
 Silverman, J. 406
 Simmons, G. 345, 356
 Simon, J. 305, 306
 simulated annealing 254
 Singh, S. 2, 168, 169, 356
 Sipser, M. 67, 120, 254, 305–307
 Sipser’s Coding Lemma 307
 Sivakumar, D. 168, 122, 124, 254, 407
 small-message attack **346**
 Smolensky, R. 306
 Soare, R. 257
 social choice function, *see also* SCF **207**
 – Condorcet *see* Condorcet SCF
 social choice theory *see* theory, social choice
 Solovay, R. 258, 309, 327–333, 356
 SOLOVAY-STRASSEN **328**, 330
 Solovay–Strassen liar *see* SS-liar
 Solovay–Strassen test *see* primality test, Solovay–Strassen
 Solovay–Strassen witness
 see SS-witness
 SOS **104**, 105, 117, 390, 391, 395, 401
 – sizes of an — instance **104**
 – target sum of an — instance **104**
 – *see also* superincreasing sequence
 Spaan, E. *see* Hemaspaandra, E.
 Spielman, D. 305
 space-constructible *see* function, space-constructible
 space function *see* function, space
 space_M(·) **56**, 114
 Space_M(·) **56**
 space hierarchy 5, **67**, 119
 space hierarchy theorem
 see theorem, space hierarchy
 Spakowski, H. V, VI, 206, 251, 253, 254
 spamming 254
 sparse set *see* language, sparse
 Speckenmeyer, E. 261, 263
 SPP 125, 289, **290**, 291, 292, 296, 300, 301, 304, 306–308
 SPP 307
 SPP^{SPP} 291
 SQUARE-AND-MULTIPLY **312**
 Srinivasan, A. 121
 SS-liar **331**
 SS-Liars_n **331**, 332
 SS-witness **331**
 statistical physics 124
 Stearns, R. 70, 119
 Steiglitz, K. 118
 Stein, C. 51
 Stelzer, A. VI, 4
 Stephan, F. 252
 Stern, J. 168, 407
 Stinson, D. 8, 168, 169, 305, 341, 354–356, 365, 402, 404, 405
 stochastic automaton
 see finite automaton, stochastic
 Stöcker, P. 4
 Stockmeyer, L. 120, 250, 251, 257
 Stoyan, D. VI
 Strassen, V. 309, 327–333, 356
 strategic voting *see* election system, manipulation of an
 stream cipher *see* cipher, stream

- string **16**
 - easy **219**
 - empty, *see also* ε **16**
 - hard **219**
 - length of a, *see also* $|\cdot|$ **16**
 - operation on —s **17**
 - concatenation of —s **17**
 - Stromnes, M. **V**
 - strong exponential-time hierarchy
 - collapse of the **125**
 - strong noninvertibility *see* one-way function, strong
 - structure **35**
 - subset-of-sums problem, *see also* SOS **104**, 105, 117, 390, 391, 395, 401
 - substitution attack
 - see* attack, substitution
 - Sudan, M. **251**
 - Sundaram, R. **255**
 - superincreasing sequence **390**, 391, 401
 - symmetric alternation, *see also* S_2^p **256**
 - symmetric cryptography
 - *see* cryptography, private-key
 - *see* cryptography, symmetric
 - symmetric cryptosystem
 - *see* cryptosystem, private-key
 - *see* cryptosystem, symmetric
 - symmetric difference hierarchy **250**
 - *see also* boolean hierarchy, normal form
 - symmetry **50**, 117
 - Szegedy, M. **251**
 - Szelepcsényi, R. **77**, 121
- T**
- Θ_2^p , *see also* $\text{P}^{\text{NP}^{[\mathcal{O}(\log)]}}$ **202**, 204, 208, 211, 212, 216, 245, 251, 253–255, 306, 308
 - Θ_2^p -complete **204**, 208, 211, 245, 253, 254
 - Θ_2^p -hard **204**, 208, 245, 251
 - Θ_i^p , *see also* $\text{P}^{\Sigma_{i-1}^{\text{P}}^{[\mathcal{O}(\log)]}}$ **202**
 - Takeuchi, M. **405**
 - Tally(\cdot) **71**, 116
 - TALLY **71**
 - tally set *see* language, tally
 - Tamaki, S. **261**, 304
 - Tarjan, R. **120**
 - Tarui, J. **306**
 - tautology **30**, **31**, 49
 - tautology problem **245**
 - tautology rule **31**
 - Tchernin, A. **4**
 - technique
 - easy-hard
 - see* easy-hard technique
 - mind-change
 - see* mind-change technique
 - Wagner *see* Wagner technique
 - Telle, J. **250**
 - Tenenbaum, P. **4**
 - term **35**
 - Thakur, M. **408**
 - theorem
 - impossibility **206**
 - linear speed-up **5**, 54, 59, 63, **64**, 119
 - for nondeterministic classes **66**
 - linear tape-compression **5**, 54, **63**, 119
 - for nondeterministic classes **66**
 - PCP **251**
 - prime number **313**, **315**, 341
 - projection **191**
 - space hierarchy **5**, **67**, 119
 - time hierarchy **5**, **70**, 119
 - uniform diagonalization **240**
 - Theorem
 - Bayes’s **46**
 - Borodin–Demers **123**
 - Cantor–Bernstein **108**
 - Chinese Remainder **41**
 - Cook–Levin *see* Theorem, Cook’s
 - Cook’s **55**, **88**, 112, 113, 116, 120
 - Euler’s **39**

- Fermat’s Little **39**, 40, 312, 317, 318, 323, 324, 335, 368
- Friedberg–Muchnik 121
- Karp–Lipton 254, 255
- Lagrange’s 39
- Rabin’s **63**
- Savitch’s **74**, 200, 227, 244
- Shannon’s **153**, 154
- Vieta’s 344
- theory
 - complexity 1–8, 53–125, 171–258, 259–308, 315–343, 382–398
 - computability
 - see* theory, recursive function
 - graph 4, 9, **37–41**, 51
 - information and coding 6, 155
 - learning 252
 - number 4, 9, **37–41**, 51
 - probability 5, 9, **46–47**, 51
 - recursive function 2, 4, 9, **16–28**, 51, 108, 110, 191, 235, 252, 257, 258
 - social choice 206, 253, 254
 - of data compression 155
 - of formal languages 9, **16–28**, 51
 - of NP-completeness **88–106**, 120, 99, 116
- thermodynamics 155
 - second principle of 155
- Thierauf, T. 252, 305
- Threshold-SAT **272**
- time-constructible *see* function, time-constructible
- time function *see* function, time
- $\text{time}_M(\cdot)$ **56**, 63, 114
- $\text{Time}_M(\cdot)$ **56**
- time hierarchy 5, **70**, 119
- time hierarchy theorem
 - see* theorem, time hierarchy
- Toda, S. 124, 252, 257, 306
- Tomaschewski, J. VI
- tools
 - axe 54
 - chain-saw 4, 54
 - nail file 54
 - *see* Turing machine
- Torán, J. 121, 255, 257, 303, 305–308, 405
- Torenvliet, T. 121, 252, 253
- total break **372**
- total function *see* function, total
- total recursive function
 - see* function, total recursive
- Tovey, C. 253
- transducer **239**
- transitivity **50**, 117
- transmitting group **172**
- trapdoor information **389**, 390, 391
- trapdoor one-way function
 - see* one-way function, trapdoor
- traveling salesperson problem, *see also* TSP **248**
- traveling salesperson tour **248**
 - unique optimal 252
- TRIAL-DIVISION **316**, 317
- Trick, M. 253
- tripartite matching problem *see* matching problem, three-dimensional
- Tripathi, R. 308
- Triple-DES 170
- triple encryption **145**
- Trithemius, J. 168
- truth-table reducibility
 - *see* reducibility, polynomial-time truth-table
 - *see* $\leq_{\text{tt}}^{\text{p}}$
- truth-table closure of NP *see* NP, $\leq_{\text{tt}}^{\text{p}}$ -closure of; *see* $\text{P}_{\text{tt}}^{\text{NP}}$
- TSP **248**
- TSP-Facet 247, 249
- Turing, A. 2, 9, 22, 51
- Turing Award 52, 119, 120
- Turing closure
 - *see* complexity class, $\leq_{\text{T}}^{\text{p}}$ -closure of a
 - *see* P^{c}
- Turing degree 121

- Turing machine 2, 9, 22, **23**, **24**,
26–28, 48, 51, 53
- acceptance mode of a 54, 224
 - alphabet of a
input **23**
working **23**
 - alternating, *see also* ATM 6,
53, 54, 58, 106, 171, **221**, 222,
223, 228, 257
 - accepting alternating subtree of an
221, **222**
 - address register of an *see* Tur-
ing machine, alternating, index
tape of an
 - evaluation function of an, *see*
also $\text{eval}(\cdot)$ **221**
 - index tape of an **224**
 - language of an **222**
 - semantics of an **221**
 - syntax of an **221**
 - blank symbol of a,
see also \square **23**
 - categorical *see* Turing machine,
unambiguous
 - composition of —s, *see also* \circ
271
 - computation of a 56
accepting **25**
rejecting **25**
 - configuration of a **24**, 56
accepting **221**, 260
existential **221**
final **24**, 56
halting *see* Turing machine,
configuration of a, final
initial **24**, 56
rejecting **221**, 260
universal **221**
 - crossing sequence of a, *see also*
 $\text{cs}(\cdot|\cdot)$ **118**
 - deterministic, *see also* DTM
24, 54, 56
computation of a 56
 - effective enumeration of —s *see*
Turing machine, Gödelization of
—s
 - Gödelization of —s **27**, 63, 68,
70, 239
 - language of a, *see also* $L(\cdot)$
25, 56
 - multitape 54
 - nondeterministic, *see also* NTM
23, 54, 56
computation of a 56
 - normalized **268**, 303
 - one-way 53
 - oracle **28**, 190, 191
see also DOTM; NOTM
deterministic polynomial-time,
see also DPOTM **193**
nondeterministic polynomial-time,
see also NPOTM **193**
positive **244**
 - probabilistic 54, **267**, 305
 - randomized 384
see also Turing machine, prob-
abilistic
 - semantics of a **24**
 - state of a **23**
accepting **25**, 221
existential 221
final **23**
halting *see* Turing machine,
state of a, final
initial **23**
rejecting **25**, 221
universal 221
 - syntax of a **23**
 - threshold **268**, 305
 - transition function of a **23**
 - two-way 54
 - unambiguous 54, **111**
- Turing reducibility
– *see* reducibility, Turing
– *see* \leq_T^p

U

Ulam, S. 307

- Ullman, J. 51
 Umans, C. 251, 252
 Umanski, O. 4
 unambiguous polynomial time *see* UP
 uniqueness distance 167, 169
 uniform diagonalization theorem *see*
 theorem, uniform diagonalization
 unique solution problem 248, 249
 Unique-SAT 243, **249**
 United States Digital Signature Stan-
 dard 7, 367, 404
 universal quantifier *see* quantifier,
 universal
 – polynomially length-bounded
see \forall^p
 unsatisfiability rule **31**
 UP 5, **111**, 112, 113, 117, 119, 123,
 124, 175, 242, 250, 269, 290,
 292, 303, 306, 308, 334, 356,
 395, 407, 408
 upward collapse **177**, 198
 upward separation **70**, 71, 119, 124
 – limitations of 119
 U.S. Congress 254
 user authentication **130**
 U.S. Presidential Election 206
 U.S. Secretary of Defense 382
- V**
 $V(\cdot)$ **47**
 $V(\cdot)$ **81**
 Valiant, L. 111, 123, 124, 249, 306
 van Helden, P. 121
 variance, *see also* $V(\cdot)$ **47**
 Vaudenay, S. 406
 Vazirani, V. 8, 248, 249, 251, 252,
 306
 VC **93**, 116
 Vereshchagin, N. 305
 verifier 305, 405
 – dishonest 405
 – honest 405
 – *see also* proof system, interactive
 – *see also* zero-knowledge protocol
 Vernam, G. 151, 154
 Vernam’s one-time pad 151, **154**,
 155
 vertex *see* graph, vertex set of a
 – degree of a **181**
 vertex cover problem, *see also* VC
93, 116
 – approximation heuristics for the
 254
 Vieta, F. 344
 Vieta’s Theorem
see Theorem, Vieta’s
 Vigenère, B. de 135
 Vigenère cipher
see cipher, Vigenère
 Vigenère square **136**, 163
 Vogel, J. V, VI, 206, 251, 253
 Voigt, L. VI
 Vollmer, H. 8, 79, 118
 von Haeseler, A. VI
 von Neumann, J. 120
 voter 207
 voting scheme *see* election system
 voting system *see* election system
 Vyskoč, J. 257
- W**
 Wagner, K. VI, 8, 76, 118, 179,
 180, 204, 216, 218, 249, 250,
 253, 254, 256, 306
 Wagner technique **179**, 184, 188,
 189, **203**, 206, 251
 Wang, J. 5
 Wanke, E. VI, 250
 Watanabe, O. V, 109, 119, 122, 123,
 255, 257, 258
 weakly associative
see associativity, weak
 website ranking 254
 – manipulation of a 254
 Wechsung, G. V, VI, 8, 76, 118,
 119, 122–124, 171, 247, 249–
 254, 256, 305, 306, 405, 408
 Wegener, I. 8, 118
 Wegman, M. 293, 307
 Welsh, D. 8, 124, 168

Widmayer, P. 51
 Wigderson, M. 307, 384, 387, 388, 406
 Wiener, M. 346, 348, 354, 356
 Wiener's attack 346, **348**, 354, 356
 Williams, H. 405
 Williamson, M. 355
 witness **190**, 214
 – number of —es *see* accepting computation, number of —s;
see acc_M ;
see also $\#P$
 – set of —es *see* witness set
 $Wit_M(\cdot)$ **191**
 witness set, *see also* $Wit_M(\cdot)$ **191**
 Woeginger, G. 8, 251
 Wolf, S. 408
 Wolfe, D. 248, 249
 Wollermann, O. 4
 Wolters, I. 4
 World War II 2, 166, 169
 worst-case cryptography
see cryptography, worst-case
 Wrathall, C. 251
 Wright, E. 51

X

$\chi(\cdot)$ 95
 χ_B **202**
 X-3-Cover **103**
 – *see also* exact cover by 3-sets problem
 XP 306

Y

Yacobi, Y. 307, 407
 Yamakami, T. 258
 Yannakakis, M. 173, 248, 249
 Yap, C. 218, 254
 Young election system 206, 207, **208**, 253
 – homogeneous variant of the 253
 – ranking problem for the, *see also* YoungRanking **208**, 245

– winner problem for the, *see also* YoungWinner 206, **208**, 211, 245

Young, H. 206–208, 253
 Young, P. 110, 111, 122, 123
 YoungRanking **208**, 245
 Young score, *see also* YScore(\cdot, \cdot, \cdot) **208**
 Young voting scheme
see Young election system
 Young winner **208**
 YoungWinner 206, **208**, 211, 245
 YScore(\cdot, \cdot, \cdot) **208**

Z

\mathbb{Z} **10**
 \mathbb{Z}^+ **248**
 \mathbb{Z}_n **38**
 – arithmetics in **50**
 \mathbb{Z}_n^* **38**
 Zachos, S. 281, 305, 306, 405
 Zappa, F. 163
 zero-knowledge **382–389**, 405
 – almost-perfect 405
 – computational 405
 – honest-verifier 386, 405
 – perfect 386, 405
 – statistical 405
 zero-knowledge property 384, **386**, 400
 zero-knowledge protocol 2, 7, 41, 260, 357, **382–389**, 405
 – *see* Goldreich–Micali–Wigderson protocol
 – *see* Fiat–Shamir identification scheme
 Zimand, M. 251, 254, 258
 Zippel, R. 402, 406
 ZPP 6, 255, 259, 266, **271**, 272, 288, 301, 305, 308
 $ZPP^{AM \cap coAM}$ 356
 ZPP^{NP} 255, 256, 307
 ZUP 306