

Index zu den KT-Folien WS '07/08

- abgeschlossen unter Reduktionen, 180
- Abzählargument, 740
- ACC^k , **803**
- AC^k , **786**
- Algorithmus
 - Black-Box-, *siehe* Black-Box-Algorithmus
 - evolutionärer, 124
 - hybrider, 130
 - Metropolis-, 124
- Alice, 571
- alternierender Schaltkreis, **786**
- $AM(k)$, **292**
- Approximationsalgorithmus, **61**
 - echt polynomielles Approximationsschema, **67**
 - für MAX-3-SAT, 71–75
 - für MAX-Clique, 63
 - für MIN-BP, 76–77
 - für Vertex-Cover, 69–70
 - polynomielles Approximationsschema, **66**
 - Selbstverbesserung, 436
- Approximationsgüte, *siehe* Güte
- Approximationsproblem, **61**
- APX, 112
 - als Teilmenge von NPO, 113
 - APX-vollständig, **114**
- Arithmetisierung von 3-SAT-Formel, 385–388
- Artus-Merlin-Protokoll, 290
- asymptotische Approximationsgüte, *siehe* Güte
- asymptotisches FPTAS, **93**
- Austauschlemma, **796**
- Auswertungsvariante, **39**
- Auszahlung, 140
- Automorphismengruppe, 304
- Automorphismus, 304

- Bandkompression, 476
- Bausteineliminierung, 745
- Beweisverifizierer für wohlgeformte Beweise, **393**
- BFD (Best-Fit-Decreasing), 77
- BFL-Code, **989**
- Bitfestlegungsverfahren, **353**

- Black-Box
 - Algorithmus, **129**
 - Komplexität, **135**, 147–173
 - Optimierung, 123–142
 - Problem, 122–173
- Bob, 269, 571
- Boosting-Technik, 94
- Borodin-Cook-Methode, 866–887
- BP (Bin-Packing), 33, 97, 441
 - Approximationsalgorithmus, 76–77
 - MIN-BP nicht in PTAS, 93
 - MIN-BP nicht in FPTAS, 90–91
- BP-Quantor, 288
- BPL, **501**
- BPP, 218–246
- Branchingprogramm, **562**
 - BP-Größe vs. Speicherplatz, 565–568
 - Länge vs. Rechenzeit, 839
 - OBDD und k OBDD, **843**
 - stereotypes, **838**, 850–865, 893

- Carrybit, 624, 807
- Chernoff-Schranken, **681**
- Chomsky-Hierarchie, 478
- Circuit-Acceptance-Probability-Estimation, 945–947
- Clique, *siehe* MAX-Clique
- Code, **984**
 - BFL-, **989**
 - lokal decodierbarer, **985**
- Codierungstheorie, 983
- CVP (Circuit-Value-Problem), 831
- CZK (Computational Zero-Knowledge), **349**

- De-Morgan-Regeln, 200, 209, 765, 785, 802
- Δ_k , **192**
- Derandomisierung, 514
 - BPP hat poly. Schaltkreise, 937
 - von Approximationsalgorithmus, 74–75
 - von Komplexitätsklassen, 903–1009
- Direkte-Summen-Probleme, 1006

Disjointness, **604**
 rand. Kommunikationskomplexität, 712–722
 Diskrepanzmethode, 694–702
 Disperser, 917
 Chor-Goldreich-, 921–926
 Konstruktion aus Expander, 930–931
 Majoritäts-, 927
 DSTCON, **519**
 dynamische Programmierung, 43

 echt polynomielles Approximationsschema, **67**
 Eigenwertlücke, **532**
 Einwegfunktion, **351**, 911, 941
 Entropie
 Min-, **914**
 Shannon-, **912**
 Entscheidungsproblem, **9**
 Entscheidungsvariante, 30, **39**, 62, 92
 Equality, **590**
 Erfüllbarkeitsproblem k -ter Stufe, **213**, 488
 erwartete Auszahlung, 140
 evolutionärer Algorithmus, 124
 EXP, **483**, 941
 Expander, 528, 529, 928
 für Konstruktion von Disperser, 930–931
 Gabber-Galil-, 929
 Expandergraph, *siehe* Expander
 Expansionsfaktor, 529
 Extra-Eingabeband, 249

 Faktorisierung, 352
 Fehlermatrix, 678, 939
 FF (First-Fit), 76
 Fingerprinting, 666
 Fooling-Set, *siehe* Unterscheidungsmenge
 Formelgröße, 752
 FPTAS, **67**, 83
 als Teilmenge von NPO, 113
 asymptotisches, **93**

 GC (Graph-Coloring), 97, 440
 asymptotische Approximationsgüte, 94
 nicht in PTAS, 93
 gemischte Strategie, 689
 GI (Graph-Isomorphism), *siehe* Graph-Isomorphie

 Glättung des Lösungsraums, 82
 Glättung des Suchraums, 83
 Graph-Isomorphie, 177, 276–285, 303–322, 338–
 346, 348
 AM-Protokoll für $\overline{\text{GI}}$, 303–322
 IP(2)-Protokoll für $\overline{\text{GI}}$, 278–285
 Grapherreichbarkeit, **519**
 Graphprodukte, 534–538
 Greater-Than, **590**
 Reduktion auf Multiplikation, 624
 Güte, **55**
 asymptotische Approximationsgüte, **60**
 bei Lückenproblem, 86
 triviale Approximationsalgorithmen für MAX-
 Clique, 63
 von Approximationsalgorithmus für KP, 84
 von Approximationsalgorithmus für MAX-3-
 SAT, 75
 von BFD, 77
 von FF, 76
 von Greedy-Matching, 70
 von Least-Loaded, 82
 Gütetransformation, 100, 120

 Hadamardmatrix, 614
 Halten
 fast sicheres vs. absolutes, 500
 Hardness-Randomness-Tradeoff, 911, 942–943
 Hashfunktion, 253, 667
 Hashklasse
 k -fach unabhängige, 258
 Matrixklasse, 259–263
 universelle, 256, 307
 HC (Hamiltonian-Circuit)
 Reduktion auf TSP, 88
 Zero-Knowledge-Protokoll, 357
 Hierarchiesätze, 248–252, 486
 Hilfsinformationsband, 557

 interaktives Beweissystem, **269**
 Definition für Beweis des PCP-Theorems, **372**
 IP (inneres Produkt), 604, 818
 IP (interactive proof system), **271**
 IP(k), **273**

Karchmer-Wigderson-Methode, 762–783
*k*OBDD, *siehe* OBDD
 Kommunikationskomplexität, **573**
 Kommunikationsmatrix, **590**
 Kommunikationsprotokoll, **572**
 für Median, 581–586
 fehlerfreies nichtdeterministisches, 652–659
 nichtdeterministisches, **632**
 randomisiertes, 630–631, 661–722
 Komplexitätslandschaft, 252, 486
 AM- und IP-Klassen, 324
 für rand. Log-Platz-Klassen, 515
 für tiefenbeschränkte Schaltkreise, 832
 innerhalb von $NP \cup co-NP$, 181
 innerhalb von PH, 195
 Komplexitätstheorie
 relativierte, 247
 konjunktive Form, 788
 Konsistenztest, **397**, **413**
 Korruptionsmethode, 703–722
 KP (Knapsack), 35, **43**, 97
 Approximationsalgorithmus, 83–84
 nicht stark NP-vollständig, 46
 kryptographische Standardannahme, 352

 L, *siehe* LOGSPACE
 Lava-Lamp-Generator, 905
 LBA-Problem, 497
 Lemma
 sehr wichtiges, *siehe* sehr wichtiges Lemma
 Linearitätstest, **395**, **402**
 LL (Least-Loaded), 80
 logarithmisch platzreduzierbar, **517**
 LOGSPACE, 251, **475**
 lokal decodierbarer Code, **985**
 lokale Ersetzung, 34
 LP (Lineare Programmierung), 177
 Lückenproblem, 86, 423
 Lückentechnik, 85–97, 367, 423
 Anwendung auf TSP, 89

 magische Tür, 334–337
 Majoritäts-Dispenser, 927
 Majority, 801, 805, 896

 Makespan-Scheduling
 Approximationsalgorithmus, 79–82
 nicht in FPTAS, 92
 Markoff-Ungleichung, **320**
 Markoffkette, 503
 Maskentechnik, 619
 Matrix-Vektor-Multiplikation, 874
 Matrixklasse, 259–263, 922
 mit Toeplitzmatrizen, 926
 MAX-3-SAT
 Approximationsalgorithmus, 71–75
 APX-vollständig, 114
 Nichtapproximierbarkeit via PCP-Theorem, 423–430
 PTAS-Reduktion auf MAX-Clique, 104, 436
 MAX-4-SAT, 108
 MAX-Clique, 441
 als Funktionenklasse, 127
 nicht in APX, 432
 PTAS-Reduktion von MAX-3-SAT, 104, 436
 triviale Approximationsalgorithmen, 63
 MAX-IS
 PTAS-Äquivalenz zu MAX-Clique, 104
 MAX-SAT, 87, 440
 Äquivalenz von Problemvarianten, 40
 Approximationsalgorithmus für MAX-3-SAT, 71–75
 nicht in FPTAS, 90–91
 MAX-W-SAT, **115**
 Maximierungsproblem, 52
 Mersenne Twister, 909
 Metropolis-Algorithmus, 124
 Minimax-Prinzip, 143–146
 für Kommunikationsprotokolle, 685–692
 Minimax-Theorem, 692
 Minimierungsproblem, 52
 Minimum-Equivalent-Circuit (MEC), 189
 monoton
 Funktion bzw. Schaltkreis, 750
 multilineares Polynom, **986**
 Multiplikation
 Kommunikationskomplexität, 621
 Reduktion von Majority, 896

NC^k , **822**
 Nechiporuk
 -Methode für Branchingprogramme, 833–837
 -Methode für Formeln, 754–761
 New York Times, 421
 nichtuniforme Turingmaschine, 557
 Nick's Class, **822**
 Nisan-Wigderson-Generator, 972
 NL, **475**
 ZPL = RL = NL, 510
 NOTM, **183**
 NP
 als Teilklasse von IP, 275
 NP-schwer, -einfach, -äquivalent, **38**
 NP-vollständig, 29–36, 175
 stark NP-vollständig, **44**, 44–49
 NPC (NP-complete problems), **175**
 NPI (NP-incomplete problems), **176**
 NPO, **111**, 455, 463
 NPO-vollständig, **114**
 Nullsummenspiel, 138, 689

 OBDD, **843**, 893
 untere Schranken, 844–849
 Optimierungsproblem, 51
 asymptotische Approximationsgüte, **60**
 Güte, **55**
 technische Annahmen, 53, 111
 Optimierungsvariante, **39**
 OR-Nichtdeterminismus, 633
 Orakelklasse, 182–190
 Orakelturingmaschine, **183**, 182–190
 OTM, *siehe* Orakelturingmaschine

 Parity nicht in AC^0 , 792
 Partition, 33
 nicht stark NP-vollständig, 46
 PCP($r(n)$, $q(n)$), **374**
 PCP-Theorem, 87, **379**, 367–470
 Anwendung für Nichtapproximierbarkeit, 432–435
 APX-Vollständigkeit von MAX-3-SAT, 442–470
 perfekt bindend (Bitfestlegung), **356**

 PH (polynomielle Hierarchie), **192**, 191–217
 Teilklasse von PSPACE, 216
 Zusammenbruch, 210
 Π_k
 Definition für Turingmaschinen, **192**
 Π_k -Schaltkreis, **787**
 platzkonstruierbar, 249
 Polynom
 für 3-SAT-Formel (Arithmetisierung), 385–388
 multilineares, **986**
 polynomielle Hierarchie, *siehe* PH
 polynomielles Approximationsschema, **66**
 PRAM, **820**, 819–832
 Primzahltest, 177
 Private vs. Public Coins
 für interaktive Beweissysteme, 291
 für Kommunikationsprotokolle, 672–683
 PRNG (pseudorandom number generator), *siehe*
 Pseudozufallsgenerator
 probabilistische Methode, 679, 795
 Probability-Amplification, **21**
 für Kommunikationsprotokolle, 661
 für platzbeschränkte Algorithmen, 500
 für Zero-Knowledge-Protokolle, 346
 mit wenig Zufallsbits, 915–931
 Problem
 algorithmisches, 9
 Black-Box-, 122–173
 Direkte-Summen-, 1006
 Maximierungs- bzw. Minimierungs-, 52
 mit kleinen Lösungswerten, **90**
 mit Versprechen, 945
 Optimierungs-, *siehe* Optimierungsproblem
 stark NP-schwer, **92**
 Zahl-, 45
 Projektion, **889**
 Promise-Problem, *siehe* Problem mit Versprechen
 Protokollbaum, 573
 pseudoboolesches Polynom, 136
 pseudopolynomiell
 Algorithmus bzw. Rechenzeit, **43**
 Pseudozufallsgenerator, **907**, **948**
 Nisan-Wigderson-, 972
 praktische Anwendung, 909

PSPACE, 214, **475**
 PSPACE-vollständig, 487
 PSPACE-vollständige Probleme, 494
 PTAS, **66**
 als Teilmenge von NPO, 113
 PTAS-vollständig, **114**
 PTAS-Reduktion, **100**, 98–109
 für Anwendung der Lückentechnik, 368
 für MAX-W-SAT-Vollständigkeit in NPO, 116
 NPO-Vollständigkeit, 114
 von MAX-3-SAT auf MAX-Clique, 436
 PZK (perfect zero-knowledge), **331**

 QBF, 488
 Quantenrechner, 22, 277
 Quantorenklassen, 286–289

 Random Walk, 525
 randomisierte lokale Suche, 124
 randomisierter Zähler, 507, 512
 randomisiertes Zählen, 307
 Rangmethode, 609–615
 und EXOR-Nichtdeterminismus, 644
 Rechenwegtester, 221
 Rechenzeit für Turingmaschinen, **12**
 Rechteckmaßmethode, 595–608
 für nichtdeterministische Protokolle, 643
 Rechteckreduktion, **616**
 Reduktion
 logarithmische, **517**
 nichtuniforme Konzepte, 888–902
 PTAS-, *siehe* PTAS-Reduktion
 Turing-, **37**
 regulär, 531
 reine Strategie, 140, 689
 relativierte Komplexitätstheorie, 247
 Restriktion
 Reduktion durch, 33
 RL, **501**
 ZPL = RL = NL, 510
 robuster Funktionsauswerter, **396**, **411**
 ROTM, **183**, 231
 Rucksackproblem, *siehe* KP
 Rundenanzahl, 574

 SAT, 236
 als Orakel, 186
 Erfüllbarkeitsproblem k -ter Stufe, 488
 Satz
 von Cook, 87, 118
 von Immerman und Szelepcsényi, **498**, 510
 von Ladner, **176**
 von Savitch, **495**
 von Sipser, Gács, Lautemann, **219**, 302
 von Wrathall, **198**, 287
 Schaltkreis
 alternierender, **786**
 boolescher, **547**
 Schaltkreisgröße, **548**, 744–751
 Schaltkreistiefe, **548**, 752–783
 Schichttiefe, **852**
 sehr wichtiges Lemma, **261**, 388, 410, 418, 607, 673
 Selbstreduzierbarkeit, 239
 Selbstverbesserung, 436
 Shannon, 740
 Σ_k , 198, 210, 216
 Definition für Turingmaschinen, **192**
 Σ_k -Schaltkreis, **787**
 Σ_k -vollständig, 213
 Simulated Annealing, 124
 Simulationsparadigma, 329
 Speicherplatz
 für nichtuniforme TM, **558**
 für Turingmaschinen, **12**
 SSS (Subset-Sum), **35**
 nicht stark NP-vollständig, 46
 stark NP-schweres Problem, **92**
 stark NP-vollständig, **44**, 44–49
 TSP, 47
 stationäre Verteilung, 503
 stereotype Turingmaschine, 554
 stereotypes Branchingprogramm, *siehe* Branchingprogramm
 stochastische Matrix, 503
 Strategie
 gemischte, 689
 reine, 140, 689
 Suchproblem, **9**

Suchraum, 83, 129, 145
 Switching Lemma, **796**
 SZK (Statistical Zero-Knowledge), **349**

Tensorprodukt, 413
 Teufel, 144
 Thresholdschaltkreis, 807–818
 Toeplitzmatrix, 883, 926
 Tschebyscheff-Ungleichung, **319**
 TSP, 97, 441

- als Funktionenklasse, 127
- Approximierbarkeit von Varianten, 78
- nicht in APX, 89

Turingmaschine

- nichtuniforme, 557
- stereotype, 554
- untere Schranke mit Kommunikationskomplexität, 731

Turingreduktion, **37**
 turingreduzierbar, **37**

Übergangswahrscheinlichkeiten, 503
 Ungleichung

- Markoff-, **320**
- Tschebyscheff-, **319**

universelle Relation, 726
 universelles Hashing, 253–263, 307
 Unterscheidungsmenge, 601
 Unterscheidungsmengenmethode, 602, 643
 USTCON, 523

- in L, 527–545

VC (Vertex-Cover), 440

- Approximationsalgorithmus, 69–70
- MIN-VC nicht in FPTAS, 90–91

verbundene Komponenten, 35
 Verifizierer

- ressourcenbeschränkter, **372**

versteckend (Bitfestlegung), **356**
 Vertauschungslemma, **240**, 322
 Verwirrmenge, *siehe* Unterscheidungsmenge
 Victoria, 269
 VLSI-Schaltkreis, 728

wohlgeformter Beweis, **384**

Yaos Minimax-Prinzip, *siehe* Minimax-Prinzip
 Yaos XOR-Lemma, 1004

Zeit-Platz-Tradeoff, 863, 865–887
 zeitkonstruierbar, 249
 Zero-Knowledge-Protokoll, **331**, 349

- Probability-Amplification, 347

ZPL, **501**

- ZPL = RL = NL, 510

zufallserhaltende Funktion, **871**
 Zwei-Personen-Nullsummenspiel, 138, 689