

Contents

1. Introduction	1
1.1 Issues in Computational Complexity	1
1.1.1 The Power of Randomness	1
1.1.2 The Power of Guessing	5
1.1.3 The Power of Memory	6
1.2 Contributions in This Dissertation	8
1.2.1 Simulations	8
1.2.2 Separations	9
2. Preliminaries	13
2.1 Computational Problems	13
2.2 Models of Computation, Resource Bounds, and Complexity Classes	18
2.2.1 Turing Machines	19
2.2.2 Uniform Families of Boolean Circuits	21
2.2.3 Nondeterministic Turing Machines	24
2.2.4 Alternating Turing Machines	27
2.3 Randomness	31
2.3.1 Randomized Computations	32
2.3.2 Randomized Proof Checking	35
2.3.3 Pseudo-Random Generators	37
2.4 Reductions and Completeness	42
2.4.1 Relativization	42
2.4.2 Reductions	44
2.4.3 Complete Problems	46
2.5 Resource-Bounded Measure	47
2.5.1 Motivation	47
2.5.2 Martingales	48
2.5.3 Properties	50
3. Derandomizing Arthur-Merlin Games	53
3.1 Introduction	53
3.2 Notation	56

3.3	Derandomizing Arthur-Merlin Games	57
3.3.1	Proof of Lemma 3.3.1	60
3.3.2	Proof of Theorem 3.3.1	61
3.3.3	Proof of Theorem 3.3.2	63
3.4	A General Framework for Derandomization	64
3.5	More Applications	66
3.5.1	Valiant-Vazirani	66
3.5.2	Learning Circuits	69
3.5.3	Rigid Matrices	70
3.5.4	Universal Traversal Sequences	72
3.6	Conclusion and Open Questions	76
4.	Sparseness of Complete Languages	77
4.1	Introduction	77
4.1.1	The Sparse Hard Language Problem for NP	77
4.1.2	The Sparse Hard Language Problem for P	78
4.1.3	Overview of this Chapter	79
4.2	Deterministic Reductions	81
4.2.1	Previous Work	81
4.2.2	Main Result	85
4.2.3	Generic Theorem for P	92
4.2.4	Extension to Classes Other Than P	95
4.3	Randomized Reductions	98
4.3.1	Previous Work	98
4.3.2	Main Result	99
4.3.3	Randomized Generic Theorem for P	106
4.3.4	Extension to Classes Other Than P	109
4.4	Conclusion and Open Questions	112
5.	Autoreducibility of Complete Languages	113
5.1	Introduction	113
5.2	Definitions	115
5.3	Nonautoreducibility Results	115
5.3.1	Adaptive Autoreductions	116
5.3.2	Nonadaptive Autoreductions	121
5.4	Autoreducibility Results	122
5.4.1	Adaptive Autoreductions	123
5.4.2	Nonadaptive Autoreductions	130
5.4.3	Randomized and Nonuniform Autoreductions	134
5.5	Separation Results	137
5.6	Conclusion and Open Questions	139

6. The Size of Randomized Polynomial Time	141
6.1 Introduction	141
6.2 The Zero-One Law for BPP	142
6.3 Generalization	143
6.4 Conclusion and Open Questions	144
7. The Frequency of Complete Languages	145
7.1 Introduction	145
7.2 Complete Languages under Nonadaptive Reductions with n^α Queries and a Small Span Theorem	146
7.3 Complete Languages for EXP under Adaptive Reductions with n^c Queries	152
7.4 Complete Languages for EXP under Nonadaptive Reductions .	154
7.5 Conclusion and Open Questions	159
8. The Frequency of Autoreducible Languages	161
8.1 Introduction	161
8.2 Betting Games	163
8.3 From Betting Games to Martingales	165
8.4 Sampling Results	168
8.5 Autoreducible Languages	172
8.5.1 Adaptively Autoreducible Languages	172
8.5.2 Nonadaptively Autoreducible Languages	174
8.5.3 Covering Autoreducible Languages by Martingales	175
8.6 Conclusion and Open Questions	181
References	183
Notation Index	191
Subject Index	195