

Contents

Preface	ix
1 Introduction	1
1.1 The Third Theory of Randomness	2
1.2 Organization of the Primer	4
1.3 Standard Conventions	5
1.4 The General Paradigm	6
1.4.1 Three fundamental aspects	6
1.4.2 Notational conventions	7
1.4.3 Some instantiations of the general paradigm	8
Notes	8
Exercises	9
2 General-Purpose Pseudorandom Generators	11
2.1 The Basic Definition	11
2.2 The Archetypical Application	12
2.3 Computational Indistinguishability	15
2.3.1 The general formulation	15
2.3.2 Relation to statistical closeness	16
2.3.3 Indistinguishability by multiple samples	16
2.4 Amplifying the Stretch Function	19
2.5 Constructions	21
2.5.1 Background: one-way functions	21
2.5.2 A simple construction	23
2.5.3 An alternative presentation	23
2.5.4 A necessary and sufficient condition	24
2.6 Non-uniformly Strong Pseudorandom Generators	25
2.7 Stronger (Uniform-Complexity) Notions	27
2.7.1 Fooling stronger distinguishers	27
2.7.2 Pseudorandom functions	27
2.8 Conceptual Reflections	29
Notes	30
Exercises	31

3	Derandomization of Time-Complexity Classes	35
3.1	Defining Canonical Derandomizers	35
3.2	Constructing Canonical Derandomizers	37
3.2.1	The construction and its consequences	38
3.2.2	Analyzing the construction	40
3.2.3	Construction 3.4 as a general framework	41
3.3	Reflections Regarding Derandomization	43
	Notes	43
	Exercises	44
4	Space-Bounded Distinguishers	47
4.1	Definitional Issues	47
4.2	Two Constructions	50
4.2.1	Sketches of the proofs of Theorems 4.2 and 4.3	51
4.2.2	Derandomization of space-complexity classes	54
	Notes	56
	Exercises	56
5	Special Purpose Generators	59
5.1	Pairwise Independence Generators	60
5.1.1	Constructions	60
5.1.2	A taste of the applications	62
5.2	Small-Bias Generators	63
5.2.1	Constructions	64
5.2.2	A taste of the applications	65
5.2.3	Generalization	66
5.3	Random Walks on Expanders	66
5.3.1	Background: expanders and random walks on them	67
5.3.2	The generator	68
	Notes	69
	Exercises	69
	Concluding Remarks	77
	Appendices	79
A	Hashing Functions	79
A.1	Definitions	79
A.2	Constructions	80
A.3	The Leftover Hash Lemma	81
B	On Randomness Extractors	83
B.1	Definitions	84
B.2	Constructions	85

<i>CONTENTS</i>	vii
C A Generic Hard-Core Predicate	89
D Using Randomness in Computation	93
D.1 A Simple Probabilistic Polynomial-Time Primality Test	93
D.2 Testing Polynomial Identity	95
D.3 The Accidental Tourist Sees It All	96
E Cryptographic Applications of Pseudorandom Functions	99
E.1 Secret Communication	99
E.2 Authenticated Communication	101
F Some Basic Complexity Classes	103
Bibliography	107
Index	113