

Pseudorandomness

By Salil P. Vadhan

Contents

1 Introduction	2
1.1 Overview of this Survey	2
1.2 Background Required and Teaching Tips	7
1.3 Notational Conventions	8
1.4 Chapter Notes and References	8
2 The Power of Randomness	10
2.1 Polynomial Identity Testing	10
2.2 The Computational Model and Complexity Classes	17
2.3 Sampling and Approximation Problems	23
2.4 Random Walks and S-T Connectivity	32
2.5 Exercises	40
2.6 Chapter Notes and References	46
3 Basic Derandomization Techniques	50
3.1 Enumeration	51
3.2 Nonconstructive/Nonuniform Derandomization	52
3.3 Nondeterminism	56
3.4 The Method of Conditional Expectations	58
3.5 Pairwise Independence	62
3.6 Exercises	73
3.7 Chapter Notes and References	77

4 Expander Graphs	80
4.1 Measures of Expansion	80
4.2 Random Walks on Expanders	92
4.3 Explicit Constructions	102
4.4 Undirected S-T Connectivity in Deterministic Logspace	116
4.5 Exercises	121
4.6 Chapter Notes and References	127
5 List-Decodable Codes	131
5.1 Definitions and Existence	131
5.2 List-Decoding Algorithms	141
5.3 List-decoding Views of Samplers and Expanders	151
5.4 Expanders from Parvaresh–Vardy Codes	155
5.5 Exercises	159
5.6 Chapter Notes and References	163
6 Randomness Extractors	166
6.1 Motivation and Definition	167
6.2 Connections to Other Pseudorandom Objects	178
6.3 Constructing Extractors	188
6.4 Exercises	202
6.5 Chapter Notes and References	209
7 Pseudorandom Generators	212
7.1 Motivation and Definition	212
7.2 Cryptographic PRGs	219
7.3 Hybrid Arguments	224
7.4 Pseudorandom Generators from Average-Case Hardness	230
7.5 Worst-Case/Average-Case Reductions and Locally Decodable Codes	239
7.6 Local List Decoding and PRGs from Worst-Case Hardness	252
7.7 Connections to Other Pseudorandom Objects	261

7.8 Exercises	270
7.9 Chapter Notes and References	278
8 Conclusions	284
8.1 A Unified Theory of Pseudorandomness	284
8.2 Other Topics in Pseudorandomness	290
Acknowledgments	309
References	311

Pseudorandomness

Salil P. Vadhan

School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, 02138, USA, salil@seas.harvard.edu

Abstract

This is a survey of *pseudorandomness*, the theory of efficiently generating objects that “look random” despite being constructed using little or no randomness. This theory has significance for a number of areas in computer science and mathematics, including computational complexity, algorithms, cryptography, combinatorics, communications, and additive number theory. Our treatment places particular emphasis on the intimate connections that have been discovered between a variety of fundamental “pseudorandom objects” that at first seem very different in nature: expander graphs, randomness extractors, list-decodable error-correcting codes, samplers, and pseudorandom generators. The structure of the presentation is meant to be suitable for teaching in a graduate-level course, with exercises accompanying each section.