

Contents

1	Introduction	1
1.1	Organization of This Book	1
1.2	The Classical Story	1
1.2.1	Seeded Extractors	3
1.2.2	Deterministic Extraction for Restricted Classes	3
1.3	Other Motivations	3
1.4	Techniques — the Recycling Paradigm	5
1.4.1	A Simple Example	5
1.4.2	The General Principle and the Application for Affine Sources	6
1.4.3	The Recycling Paradigm in Bit-Fixing Sources	8
1.4.4	The Recycling Paradigm for Zero-Error Dispersers	9
1.4.5	What Else Is There in This Book?	10
2	Deterministic Extractors for Bit-Fixing Sources by Obtaining an Independent Seed	11
2.1	Introduction	12
2.1.1	Bit-Fixing Sources	12
2.1.2	Our Results	13
2.1.3	Overview of Techniques	13
2.1.4	Outline	18
2.2	Preliminaries	18
2.2.1	Averaging Samplers	18
2.2.2	Probability Distributions	19
2.3	Obtaining an Independent Seed	21
2.3.1	Seed Obtainers and Their Application	21
2.3.2	Constructing Seed Obtainers	22
2.4	Extracting a Few Bits for Any k	25
2.5	Sampling and Partitioning with a Short Seed	25
2.6	A Seeded Bit-Fixing Source Extractor with a Short Seed	27

2.7	Deterministic Extractors for Bit-Fixing Sources	28
2.7.1	An Extractor for Large k (Proof of Theorem 2.1) . . .	28
2.7.2	An Extractor for Small k (Proof of Theorem 2.2) . . .	30
2.8	Discussion and Open Problems	31
3	Deterministic Extractors for Affine Sources over Large Fields	33
3.1	Introduction	33
3.1.1	Affine Source Extractors	34
3.1.2	Our Results	34
3.1.3	Previous Work	35
3.2	Overview of Techniques	35
3.2.1	Extracting Many Bits from Lines	36
3.2.2	Linear Seeded Affine Source Extractors	37
3.2.3	Using the Correlated Randomness as a Seed	38
3.3	Preliminaries	39
3.3.1	Probability Distributions	39
3.3.2	Characters of Finite Fields	41
3.4	Extracting One Bit from Lines	44
3.5	Extracting Many Bits from Lines	45
3.6	A Linear Seeded Extractor for Affine Sources	49
3.7	Composing Extractors	51
3.8	Putting It All Together	53
4	Extractors and Rank Extractors for Polynomial Sources	55
4.1	Introduction	56
4.1.1	Rank Extractors	57
4.1.2	Extractors and Condensers for Polynomial Sources . .	58
4.1.3	Rank Versus Entropy — Weak Polynomial Sources . .	61
4.1.4	Organization	62
4.2	General Preliminaries	62
4.2.1	Probability Distributions	62
4.2.2	Polynomials over Finite Fields	63
4.2.3	The Number of Solutions to a System of Polynomial Equations	65
4.3	Algebraic Independence and Rank	66
4.4	An Explicit Rank Extractor	68
4.4.1	Preliminaries for the Proof of Theorem 4.4	69
4.4.2	Proof of Theorem 4.4	70
4.5	Extractors for Polynomial Sources	73
4.5.1	Preliminaries for the Proof of Theorem 4.5	74
4.5.2	Proof of Theorem 4.5	77
4.6	Improving the Output Length	80
4.7	Extractors for Weak Polynomial Sources	82
4.7.1	Proof of Theorem 4.9	83
4.7.2	The Entropy of a Polynomial Mapping	86

4.8	Rank Extractors over the Complex Numbers	87
4.9	Discussion and Open Problems	88
5	Increasing the Output Length of Zero-Error Dispersers	91
5.1	Introduction	92
5.1.1	Randomness Extractors and Dispersers	92
5.1.2	Zero-Error Dispersers	93
5.1.3	Increasing the Output Length of Zero-Error Dispersers	94
5.1.4	Applications	96
5.1.5	Outline	102
5.2	Preliminaries	102
5.3	A Composition Theorem	105
5.3.1	Zero-Error Dispersers	105
5.3.2	Strongly Hitting Dispersers	106
5.4	Zero-Error Dispersers for Multiple Independent Sources . . .	108
5.4.1	Formal Definition of Multiple Independent Sources . .	108
5.4.2	A Subsource Hitter for 2-Sources	108
5.4.3	Zero-Error Dispersers for 2-Sources	111
5.4.4	Zero-Error Dispersers for $O(1)$ -Sources	113
5.4.5	Rainbows and Implicit $O(1)$ Probe Search	114
5.5	Zero-Error Dispersers for Bit-Fixing Sources	116
5.6	Zero-Error Dispersers for Affine Sources	119
5.7	Open Problems	121
A	Sampling and Partitioning	123
A.1	Sampling Using ℓ -wise Independence	123
A.2	Sampling and Partitioning Using Fewer Bits	125
B	Basic Notions from Algebraic Geometry	129
B.1	Affine and Projective Varieties	129
B.2	Varieties and Ideals	131
B.3	The Dimension and Degree of a Variety	132
B.4	The Projective Closure of an Affine Variety	135
B.5	The Dimension of Intersections of Hypersurfaces	136
B.6	The Degree of Intersections of Hypersurfaces	138
B.7	Bombieri's Theorem	140
	Bibliography	143

Deterministic Extraction from Weak Random Sources

Gabizon, A.

2011, XII, 148 p., Hardcover

ISBN: 978-3-642-14902-3