

Lenore Blum
Felipe Cucker
Michael Shub
Steve Smale

Complexity and Real Computation

Foreword by Richard M. Karp

With 47 Illustrations and 3 Color Plates



Springer

Contents

Foreword	v
Preface	ix
I Basic Development	
1 Introduction	3
1.1 Aim	3
1.2 Seven Examples	4
1.2.1 Is the Mandelbrot Set Decidable?	4
1.2.2 Example of the Julia Set of $T(z) = z^2 + 4$	8
1.2.3 Newton's Method	10
1.2.4 The Knapsack Problem	12
1.2.5 The Hilbert Nullstellensatz as a Decision Problem	15
1.2.6 Feasibility of Real Polynomials	17
1.2.7 Linear Programming and Integer Programming	18
1.3 The Classical Theory of Computation	20
1.4 Toward a Mathematical Foundation of Numerical Analysis	22
1.5 Classical Complexity Theory and Its Extension	24
1.6 Complexity Theory in Numerical Analysis	28
1.7 Summary	30
1.8 Brief History and Comparison with Other Models of Computation	31

2	Definitions and First Properties of Computation	37
2.1	The Model of Computation: The Finite-Dimensional Case	38
2.2	The Input–Output Map, Halting Set, and the Computing Endomorphism	44
2.3	Halting Sets and Computable Maps	48
2.4	The Mandelbrot Set Is Undecidable	55
2.5	The Canonical Path Construction	56
2.6	The Register Equations and Succinct Descriptions	58
2.7	More Succinct Descriptions	63
2.8	Additional Comments and Bibliographical Remarks	67
3	Computation over a Ring	69
3.1	R^∞ and R_∞	70
3.2	Machines over R	71
3.3	Path Decomposition and Reduction to the Finite-Dimensional Case	74
3.4	The Register Equations	77
3.5	Product Spaces, Codes and Universal Machines	79
3.6	Additional Comments and Bibliographical Remarks	81
4	Decision Problems and Complexity over a Ring	83
4.1	Decision Problems	83
4.2	Complexity and the Class P	86
4.3	Polynomial Time Reductions	90
4.4	Management, Machines and Algorithms	93
4.5	Additional Comments and Bibliographical Remarks	96
5	The Class NP and NP-Complete Problems	99
5.1	The Class NP	100
5.2	Important NP Problems	103
5.3	NP-Completeness	104
5.4	NP-Complete Problems over \mathbb{C} , \mathbb{R} , and \mathbb{Z}	104
5.5	NP-Complete Problems over \mathbb{Z}_2	107
5.6	Additional Comments and Bibliographical Remarks	110
6	Integer Machines	113
6.1	Polynomial Equivalence of Machines over \mathbb{Z} and \mathbb{Z}_2	113
6.2	Some Results on Linear Inequalities	116
6.3	The Complexity of Integer Programming	121
6.4	Additional Comments and Bibliographical Remarks	124
7	Algebraic Settings for the Problem “P \neq NP?”	125
7.1	Statement of Main Theorems	125
7.2	Eliminating Constants: Easy Cases	127
7.3	Witness Theorem	129

Appendix to Section 7.3	135
7.4 Elimination of Constants: General Case	136
7.5 Twenty Questions	137
7.6 Proof of Theorems 2 and 3	140
7.7 Main Theorem, an Algebraic Proof of the Converse	141
7.8 Main Theorem, a Model-Theoretic Proof of the Converse	143
7.9 Additional Comments and Bibliographical Remarks	145
Appendix A	
A.1 Basic Notions of Algebraic Geometry	147
A.2 Additional Comments and Bibliographical Remarks	149
II Some Geometry of Numerical Algorithms	
8 Newton's Method	153
8.1 Approximate Zeros	154
8.2 Point Estimates for Approximate Zeros	159
8.3 Additional Comments and Bibliographical Remarks	168
9 Fundamental Theorem of Algebra: Complexity Aspects	169
9.1 The Fundamental Theorem of Algebra	169
9.2 A Homotopy Method	172
9.3 Where to Begin the Homotopy	178
9.4 The Algorithm and Its Complexity	184
9.5 Additional Comments and Bibliographical Remarks	185
10 Bézout's Theorem	187
10.1 The Fundamental Theorem of Algebra Revisited	187
10.2 Projective Space	190
10.3 The Varieties V , Σ' , and Σ	193
10.4 The Discriminant Variety in One Variable	194
10.5 Bézout's Theorem	198
10.6 Additional Comments and Bibliographical Remarks	199
11 Condition Numbers and the Loss of Precision of Linear Equations	201
11.1 The Eckart–Young Theorem	202
11.2 Probabilities and Integrals	204
11.3 Some Integration Formulas	205
11.4 A Linear Algebra Estimate	209
11.5 The Main Theorems for the Reals	210
11.6 The Main Theorems for the Complex Numbers	213
11.7 Additional Comments and Bibliographical Remarks	214
12 The Condition Number for Nonlinear Problems	217
12.1 Unitary Invariance	217

12.2	Hermitian Structures and Distances in Projective Space	222
12.3	The Condition Number (Nonlinear)	227
12.4	The Condition Number Theorem	232
12.5	Additional Comments and Bibliographical Remarks	236
13	The Condition Number in $\mathbb{P}(\mathcal{H}_{(d)})$	237
13.1	Integration on Manifolds	237
13.2	A General Integral Formula	240
13.3	Integration in V and the Average Number of Real Roots	244
13.4	The Condition Number in $\mathcal{M}_{(n,n+1)}^{\mathbb{C}}$	248
13.5	A Linear Algebra Estimate and the Distribution of the Condition Number	250
13.6	The Distribution of the Normalized Condition Number for $\mathbb{P}(\mathcal{H}_{(d)})$	255
13.7	Additional Comments and Bibliographical Remarks	258
14	Complexity and the Condition Number	261
14.1	Newton's Method in Projective Space	261
14.2	The Higher Derivative Estimate	267
14.3	Complexity of Homotopy Methods	271
14.4	Additional Comments and Bibliographical Remarks	273
15	Linear Programming	275
15.1	Machines over \mathbb{Q}	275
15.2	The Barrier Method in Linear Programming	277
15.3	Linear Programming over \mathbb{Q}	286
15.4	Polynomial Cost	289
15.5	On the Cost of Inverting a Matrix	292
15.6	Additional Comments and Bibliographical Remarks	296
Appendix B		
B.1	The Main Theorem of Elimination Theory	297
B.2	Additional Comments and Bibliographical Remarks	299
 III Complexity Classes over the Reals		
16	Deterministic Lower Bounds	303
16.1	A Geometric Upper Bound	303
16.2	A Complexity Lower Bound	309
16.3	On the Number of Connected Components of Semi-Algebraic Sets	312
16.4	Additional Comments and Bibliographical Remarks	315
17	Probabilistic Machines	317
17.1	Machines That Flip Coins	318

17.2	Simulating Probabilistic Trees	320
17.3	Two Bounds for the Tail of the Binomial distribution	323
17.4	Approximating the Volume of Bounded Semi-Algebraic Sets	326
17.5	Machines That Pick Real Numbers in $[0, 1]$	330
17.6	Simulating Probabilistic Machines	332
17.7	Additional Comments and Bibliographical Remarks	333
18	Parallel Computations	335
18.1	Some Old Problems Revisited	335
18.2	A Parallel Model of Computation	342
18.3	Deterministic Upper Bounds for $\text{NP}_{\mathbb{R}}$	348
18.4	Algebraic Circuits	349
18.5	The Class $\text{NC}_{\mathbb{R}}$	352
18.6	Additional Comments and Bibliographical Remarks	356
19	Some Separations of Complexity Classes	359
19.1	A Separation Result	359
19.2	Lower Bounds for Parallel Time	365
19.3	Completeness in $\text{P}_{\mathbb{R}}$	366
19.4	Digital Nondeterminism	370
19.5	The Complexity of the Knapsack Problem	371
19.6	Additional Comments and Bibliographical Remarks	374
20	Weak Machines	377
20.1	A Restriction on the Number of Multiplications	377
20.2	A Characterization of Digital Nondeterminism	381
20.3	Linear Programming and Digital Nondeterminism	383
20.4	Additional Comments and Bibliographical Remarks	384
21	Additive Machines	385
21.1	Additive Machines and Complexity Classes	385
21.2	The Polynomial Hierarchy	389
21.3	On the Definition of the Polynomial Hierarchy	393
21.4	The Polynomial Hierarchy for Unrestricted Machines	398
21.5	Additional Comments and Bibliographical Remarks	399
22	Nonuniform Complexity Classes	401
22.1	Complexity Classes Defined by Advice Functions	401
22.2	Boolean Parts	404
22.3	Additional Comments and Bibliographical Remarks	408
23	Descriptive Complexity	411
23.1	Vocabularies, Structures, and First-Order Logic	412
23.2	Logics on \mathbb{R} -Structures	415
23.3	Capturing $\text{P}_{\mathbb{R}}$ with Fixed Point First-Order Logic	420
23.4	Capturing $\text{NP}_{\mathbb{R}}$ with Existential Second-Order Logic	426

23.5 Additional Comments and Bibliographical Remarks	429
References	431
Index	447