Contents

UNCORRECTED PROOF

Part I The Basics

1 Our Adversary: The Circuit 3

1.1 Boolean Functions 3

1.2 Circuits 12

1.3 Branching Programs 17

1.4 Almost All Functions are Complex 21

1.4.1 Circuits 22

1.4.2 Approximation Complexity 26

1.4.3 The Circuit Hierarchy Theorem 29

1.4.4 Switching Networks and Formulas 30

1.4.5 Invariant Classes 33

1.5 So Where are the Complex Functions? 36

1.5.1 On Explicitness 36

1.5.2 Explicit Lower Bounds 37

1.6 A $3n$ Lower Bound for Circuits 38

1.7 Graph Complexity 40

1.7.1 Clique Complexity of Graphs 41

1.7.2 Star Complexity of Graphs 42

1.8 A Constant Factor Away From $P \neq NP$? 45

Exercises 48

2 Analysis of Boolean Functions 55

2.1 Boolean Functions as Polynomials 55

2.2 Real Degree of Boolean Functions 56

2.3 The Fourier Transform 59

2.4 Boolean 0/1 Versus Fourier ±1 Representation 62

2.5 Approximating the Values 0 and 1 63

2.6 Approximation by Low-Degree Polynomials 64

2.7 Sign-Approximation 67

2.8 Sensitivity and Influences 68

Exercises 76

Part II Communication Complexity

3 Games on Relations 81
3.1 Communication Protocols and Rectangles 81
3.2 Protocols and Tiling 84
3.3 Games and Circuit Depth 88
3.3.1 Monotone Depth 90
Exercises 91

4 Games on 0-1 Matrices 93
4.1 Deterministic Communication 93
4.2 Nondeterministic Communication 96
4.2.1 Greedy Bounds 98
4.2.2 Fooling-Set Bounds 99
4.3 $\mathrm{P} = \mathrm{NP} \cap \text{co-NP}$ for Fixed-Partition Games 101
4.4 Clique vs. Independent Set Game 104
4.5 Communication and Rank 106
4.6 The Log-Rank Conjecture 107
4.6.1 Known Gaps 108
4.6.2 Small Rank Implies Large Discrepancy 110
4.6.3 Rank and Chromatic Number 112
4.7 Communication with Restricted Advice 114
4.8 $\mathrm{P} \neq \mathrm{NP} \cap \text{co-NP}$ for Best-Partition Games 116
4.9 Randomized Communication 119
4.9.1 Distributional Complexity 119
4.10 Lower Bound for the Disjointness Function 121
4.11 Unbounded Error Communication and Sign-Rank 124
4.12 Private vs. Public Randomness 128
Exercises 130

5 Multi-Party Games 135
5.1 The “Number-in-Hand” Model 136
5.2 The Approximate Set Packing Problem 137
5.3 Application: Streaming Algorithms 139
5.4 The “Number-on-Forehead” Model 140
5.5 The Discrepancy Bound 143
5.6 Generalized Inner Product 146
5.7 Matrix Multiplication 148
5.8 Best-Partition k-Party Communication 150
Exercises 153

Part III Circuit Complexity

6 Formulas 159
6.1 Size Versus Depth 159
6.2 A Quadratic Lower Bound for Universal Functions 164

UNCORRECTED PROOF

6.3 The Effect of Random Restrictions 167
6.4 A Cubic Lower Bound 170
6.5 Nechiporuk's Theorem 172
6.6 Lower Bounds for Symmetric Functions 174
6.7 Formulas and Rectangles 176
6.8 Khrapchenko's Theorem 179
6.9 Complexity is not Convex 182
6.10 Complexity is not Submodular 187
6.11 The Drag-Along Principle 189
6.12 Bounds Based on Graph Measures 190
6.13 Lower Bounds via Graph Entropy 193
6.14 Formula Size, Rank and Affine Dimension 196
6.14.1 Affine Dimension and Formulas 197
6.14.2 Projective Dimension and Branching Programs 199
Exercises 200

7 Monotone Formulas 205
7.1 The Rank Argument 205
7.2 Lower Bounds for Quadratic Functions 206
7.3 A Super-Polynomial Size Lower Bound 209
7.3.1 Rank of Disjointness Matrices 210
7.3.2 A Lower Bound for Paley Functions 211
7.4 A $\log^2 n$ Depth Lower Bound for Connectivity 213
7.4.1 Reduction to the Fork Game 214
7.4.2 Lower Bound for the Fork Game 216
7.5 An $n^{1/6}$ Depth Lower Bound for Clique Function 219
7.6 An $n^{1/2}$ Depth Lower Bound for Matching 224
Exercises 227

8 Span Programs 229
8.1 The Model 229
8.2 The Power of Span Programs 231
8.3 Power of Monotone Span Programs 232
8.4 Threshold Functions 233
8.5 The Weakness of Monotone Span Programs 235
8.6 Self-Avoiding Families 236
8.7 Characterization of Span Program Size 238
8.8 Monotone Span Programs and Secret Sharing 240
Exercises 241

9 Monotone Circuits 245
9.1 Large Cliques are Hard to Detect 245
9.1.1 Construction of the Approximated Circuit 247
9.1.2 Bounding Errors of Approximation 248
9.2 Very Large Cliques are Easy to Detect 251
9.2.1 Properties of τ-Critical Graphs 252
9.2.2 Proof of Theorem 9.7 254

UNCORRECTED PROOF

9.3 The Monotone Switching Lemma 257
9.4 The Lower-Bounds Criterion 259
9.5 Explicit Lower Bounds 261
9.5.1 Detecting Triangles 261
9.5.2 Graphs of Polynomials 262
9.6 Circuits with Real-Valued Gates 263
9.7 Criterion for Graph Properties 267
9.8 Clique-Like Problems 269
9.9 What About Circuits with NOT Gates? 273
9.10 Razborov's Method of Approximations 274
9.10.1 Construction of Legitimate Lattices 275
9.11 A Lower Bound for Perfect Matching 276
9.11.1 Error-Probability on Accepted Inputs 278
9.11.2 Error-Probability on Rejected Inputs 279
Exercises 282

10 The Mystery of Negations 285
10.1 When are NOT Gates Useless? 285
10.1.1 Slice Functions 286
10.1.2 Negated Inputs as New Variables 288
10.2 Markov's Theorem 289
10.3 Formulas Require Exponentially More NOT Gates 293
10.4 Fischer's Theorem 295
10.5 How Many Negations are Enough to Prove P $\neq$ NP? 297
Exercises 299

Part IV Bounded Depth Circuits

11 Depth-3 Circuits 303
11.1 Why is Depth 3 Interesting? 303
11.2 An Easy Lower Bound for Parity 306
11.3 The Method of Finite Limits 306
11.4 A Lower Bound for Majority 309
11.5 NP $\neq$ co-NP for Depth-3 Circuits 310
11.6 Graph Theoretic Lower Bounds 313
11.7 Depth-2 Circuits and Ramsey Graphs 315
11.8 Depth-3 Circuits and Signum Rank 317
11.9 Depth-3 Circuits with Parity Gates 321
11.10 Threshold Circuits 326
11.10.1 General Threshold Circuits 327
11.10.2 Threshold Circuits of Depth Two 329
11.10.3 Threshold Circuits of Depth Three 333
Exercises 336

12 Large-Depth Circuits 339
12.1 Håstad's Switching Lemma 339
12.2 Razborov's Proof of the Switching Lemma 341

UNCORRECTED PROOF

12.3 Parity and Majority Are Not in AC^0 343
12.3.1 Majority of AC^0 Circuits 348
12.3.2 Parity is Even Hard to Approximate 349
12.4 Constant-Depth Circuits and Average Sensitivity 350
12.5 Circuits with Parity Gates 354
12.6 Circuits with Modular Gates 357
12.6.1 ACC^0 and Symmetric Depth-2 Circuits 360
12.6.2 ACC^0 and Low-Degree Polynomials 360
12.6.3 ACC^0 and Graph Complexity 361
12.6.4 ACC^0 and Communication Complexity 362
12.7 Circuits with Symmetric Gates 363
12.8 Rigid Matrices Require Large Circuits 365
Exercises 369

13 Circuits with Arbitrary Gates 371
13.1 Entropy and the Number of Wires 372
13.2 Entropy and Depth-Two Circuits 374
13.3 Matrix Product Is Hard in Depth Two 376
13.3.1 Restricted Matrix Product Is Easy in Depth Three 377
13.4 Larger-Depth Circuits 378
13.5 Linear Circuits for Linear Operators 382
13.6 Circuits with OR Gates: Rectifier Networks 386
13.6.1 Circuits with OR and AND Gates 388
13.6.2 Asymptotic Bounds 390
13.7 Non-linear Circuits for Linear Operators 391
13.8 Relation to Circuits of Logarithmic Depth 394
Exercises 399

Part V Branching Programs

14 Decision Trees 405
14.1 Adversary Arguments 405
14.2 P = NP ∩ co-NP for Decision Tree Depth 407
14.3 Certificates, Sensitivity and Block Sensitivity 409
14.3.1 Block Sensitivity Versus Certificate Complexity 412
14.3.2 Block Sensitivity Versus Depth 412
14.3.3 Sensitivity and Degree of Polynomials 414
14.4 Sensitivity and Subgraphs of the n-Cube 416
14.5 Evasive Boolean Functions 418
14.6 Decision Trees for Search Problems 421
14.7 Linear Decision Trees 424
14.8 Element Distinctness and Turán's Theorem 425
14.9 P ≠ NP ∩ co-NP for Decision Tree Size 427
14.9.1 Spectral Lower Bound 430
14.9.2 Explicit Lower Bounds 432
Exercises 435

UNCORRECTED PROOF

15 General Branching Programs 439
15.1 Nechiporuk's Lower Bounds 439
15.1.1 Lower Bounds for Symmetric Functions 441
15.2 Branching Programs Over Large Domains 442
15.3 Counting Versus Nondeterminism 445
15.4 A Surprise: Barrington's Theorem 447
15.5 Oblivious Branching Programs 451
Exercises 454

16 Bounded Replication 457
16.1 Read-Once Programs: No Replications 458
16.2 P $\neq$ NP $\cap$ co-NP for Read-Once Programs 460
16.3 Branching Programs Without Null-Paths 461
16.4 Parity Branching Programs 465
16.5 Linear Codes Require Large Replication 467
16.6 Expanders Require Almost Maximal Replication 470
16.6.1 Quadratic Functions of Expanders are Hard 474
Exercises 477

17 Bounded Time 479
17.1 The Rectangle Lemma 480
17.2 A Lower Bound for Code Functions 481
17.3 Proof of the Rectangle Lemma 483
Exercises 489

Part VI Fragments of Proof Complexity

18 Resolution 493
18.1 Resolution Refutation Proofs 494
18.2 Resolution and Branching Programs 495
18.3 Lower Bounds for Tree-Like Resolution 498
18.4 Tree-Like Versus Regular Resolution 503
18.5 Lower Bounds for General Resolution 505
18.6 Size Versus Width 508
18.7 Tseitin Formulas 511
18.8 Expanders Force Large Width 514
18.9 Matching Principles for Graphs 516
Exercises 517

19 Cutting Plane Proofs 521
19.1 Cutting Planes as Proofs 521
19.2 Cutting Planes and Resolution 523
19.3 Lower Bounds for Tree-Like CP Proofs 526
19.3.1 Lower Bound for the Matching CNF 528
19.4 Lower Bounds for General CP Proofs 530
19.4.1 The Clique-Coloring Polytope 533

UNCORRECTED PROOF

19.5 Chvátal Rank ... 536
19.6 Rank Versus Depth of CP Proofs ... 539
19.7 Lower Bounds on Chvátal Rank ... 540
19.7.1 The Maximum Independent Set Problem ... 541
19.7.2 The Set-Covering Problem ... 545
19.7.3 The Knapsack Problem ... 547
19.7.4 An Upper Bounds on the Proof Size ... 548
19.8 General CP Proofs Cannot be Balanced ... 549
19.8.1 Size Versus Depth of CP Proofs ... 550
19.9 Integrality Gaps ... 551
Exercises ... 553

20 Epilogue ... 557
20.1 Pseudo-Random Generators ... 557
20.2 Natural Proofs ... 561
20.3 The Fusion Method ... 564
20.4 Indirect Proofs ... 568
20.4.1 Williams' Lower Bound ... 569
20.4.2 Kannan's Lower Bound ... 569

A Mathematical Background ... 575
A.1 Basics and Notation ... 575
A.2 Graphs ... 575
A.3 Linear Algebra ... 577
A.4 Probability Theory ... 585

References ... 591

Index ... 611

UNCORRECTED PROOF