

# Contents

<b>1. Boolean Functions and Circuits</b> .....	1
1.1 Introduction .....	1
1.2 Boolean Functions and Formulas .....	2
1.3 Circuit Model .....	7
1.4 Basic Functions and Reductions .....	8
1.5 Nomenclature .....	11
1.6 Parsing Regular and Context-Free Languages .....	12
1.7 Circuits for Integer Arithmetic .....	17
1.7.1 Circuits for Addition and Multiplication .....	17
1.7.2 Division Using Newton Iteration .....	21
1.7.3 Division Using Iterated Product .....	24
1.8 Synthesis of Circuits .....	30
1.8.1 Elementary Methods .....	30
1.8.2 Shannon's Method .....	31
1.8.3 Lupanov's Method .....	32
1.8.4 Symmetric Functions .....	34
1.9 Reducing the Fan-out .....	35
1.10 Relating Formula Size and Depth .....	39
1.11 Other Models .....	45
1.11.1 Switching Networks .....	45
1.11.2 VLSI Circuits .....	45
1.11.3 Energy Consumption .....	45
1.11.4 Boolean Cellular Automata .....	46
1.11.5 Branching Programs .....	48
1.11.6 Hopfield Nets .....	53
1.11.7 Communication Complexity .....	54
1.11.8 Anonymous Networks .....	54
1.12 Historical and Bibliographical Remarks .....	55
1.13 Exercises .....	56
<b>2. Circuit Lower Bounds</b> .....	61
2.1 Introduction .....	61
2.2 Shannon's Lower Bound .....	63
2.3 Nechiporuk's Bound .....	65

2.4	Monotonic Real Circuits	68
2.4.1	Broken Mosquito Screen	68
2.4.2	Monotonic Real Circuits Are Powerful	77
2.4.3	$st$ -Connectivity	78
2.5	Parity and the Random Restriction Method	90
2.6	Probabilistic Methods	95
2.6.1	Håstad's Lower Bound for Parity	96
2.6.2	Depth- $k$ Versus Depth- $(k-1)$	99
2.6.3	Razborov's Simplification and Decision Trees	102
2.6.4	A Hybrid Switching Lemma and $st$ -Connectivity	107
2.6.5	Hybrid Switching with the Uniform Distribution	110
2.7	Algebraic Methods	124
2.7.1	Razborov's Lower Bound for Majority over Boolean Circuits with Parity	124
2.7.2	Smolensky's Lower Bound for $\text{MOD}_p$ Versus $\text{MOD}_q$	129
2.8	Polynomial Method	132
2.8.1	On the Strength of $\text{MOD}_m$ Gates	132
2.8.2	The $\text{MOD}_m$ -Degree of Threshold Functions	135
2.9	Method of Filters	137
2.10	Eliminating Majority Gates	140
2.11	Circuits for Symmetric Functions	141
2.11.1	Negative Results	143
2.11.2	Positive Results	145
2.12	Probabilistic Circuits	146
2.13	Historical and Bibliographical Remarks	148
2.14	Exercises	150
<b>3.</b>	<b>Circuit Upper Bounds</b>	155
3.1	Introduction	155
3.2	Definitions and Elementary Properties	156
3.3	Pólya's Enumeration Theory	162
3.4	Representability of Permutation Groups	164
3.5	Algorithm for Representing Cyclic Groups	168
3.6	Asymptotics for Invariance Groups	172
3.7	Almost Symmetric Languages	174
3.8	Symmetry and Complexity	178
3.9	Applications to Anonymous Networks	184
3.9.1	Rings	185
3.9.2	Hypercubes	185
3.10	Historical and Bibliographical Remarks	194
3.11	Exercises	194
<b>4.</b>	<b>Randomness and Satisfiability</b>	207
4.1	Introduction	207
4.2	Threshold for 2-SAT	209

4.3	Unsatisfiability Threshold for 3-SAT . . . . .	212
4.3.1	A General Method and Local Maxima . . . . .	213
4.3.2	Method of Single Flips . . . . .	214
4.3.3	Approximating the Threshold . . . . .	217
4.3.4	Method of Double Flips . . . . .	217
4.3.5	Probability Calculations . . . . .	218
4.4	Satisfiability Threshold for 3-SAT . . . . .	224
4.4.1	Satisfiability Heuristics . . . . .	224
4.4.2	Threshold . . . . .	226
4.5	$(2 + p)$ -SAT . . . . .	229
4.5.1	Unsatisfiability Threshold . . . . .	230
4.5.2	Transition from 2-SAT to 3-SAT . . . . .	232
4.6	Constraint Programming . . . . .	235
4.6.1	Models of CSP . . . . .	236
4.6.2	A New Model for Random CSP . . . . .	238
4.6.3	The Method of Local Maxima . . . . .	239
4.6.4	Threshold for Model E . . . . .	241
4.7	Historical and Bibliographical Remarks . . . . .	242
4.8	Exercises . . . . .	243
<b>5.</b>	<b>Propositional Proof Systems . . . . .</b>	<b>247</b>
5.1	Introduction . . . . .	247
5.2	Complexity of Proofs . . . . .	249
5.3	Gentzen Sequent Calculus LK . . . . .	255
5.3.1	Completeness . . . . .	257
5.3.2	Lower Bound for Cut-Free Gentzen . . . . .	259
5.3.3	Monotonic Sequent Calculus . . . . .	267
5.4	Resolution . . . . .	268
5.4.1	Resolution and the PHP . . . . .	271
5.4.2	Resolution and Odd-Charged Graphs . . . . .	279
5.4.3	Schöning's Expander Graphs and Resolution . . . . .	285
5.4.4	Width-Bounded Resolution Proofs . . . . .	291
5.4.5	Interpolation and <i>st</i> -Connectivity . . . . .	296
5.4.6	Phase Transition and Length of Resolution Proofs . . . . .	300
5.5	Algebraic Refutation Systems . . . . .	306
5.5.1	Nullstellensatz . . . . .	308
5.5.2	Polynomial Calculus . . . . .	316
5.5.3	Gaussian Calculus . . . . .	324
5.5.4	Binomial Calculus . . . . .	326
5.5.5	Lower Bounds for the Polynomial Calculus . . . . .	332
5.5.6	Random CNF Formulas and the Polynomial Calculus . . . . .	337
5.6	Cutting Planes CP . . . . .	343
5.6.1	Completeness of CP . . . . .	345
5.6.2	Cutting Planes and the PHP . . . . .	348
5.6.3	Polynomial Equivalence of $CP_2$ and CP . . . . .	353

5.6.4	Normal Form for CP Proofs	355
5.6.5	Lower Bounds for CP	359
5.6.6	Threshold Logic PTK	366
5.7	Frege Systems	370
5.7.1	Bounded Depth Frege Systems	372
5.7.2	Extended Frege Systems	393
5.7.3	Frege Systems and the PHP	398
5.8	Open Problems	403
5.9	Historical and Bibliographical Remarks	405
5.10	Exercises	406
<b>6.</b>	<b>Machine Models and Function Algebras</b>	<b>413</b>
6.1	Introduction	413
6.2	Machine Models	415
6.2.1	Turing Machines	415
6.2.2	Parallel Machine Model	424
6.2.3	Example Parallel Algorithms	427
6.2.4	<i>LogP</i> Model	433
6.2.5	Circuit Families	434
6.3	Some Recursion Schemes	437
6.3.1	An Algebra for the Logtime Hierarchy LH	438
6.3.2	Bounded Recursion on Notation	450
6.3.3	Bounded Recursion	458
6.3.4	Bounded Minimization	465
6.3.5	Miscellaneous	470
6.3.6	Safe Recursion	478
6.4	A Glimpse of Other Work	487
6.5	Historical and Bibliographical Remarks	488
6.6	Exercises	489
<b>7.</b>	<b>Higher Types</b>	<b>497</b>
7.1	Introduction	497
7.2	Type 2 Functionals	497
7.3	Some Closure Properties of $\mathcal{A}_0$	502
7.4	Square-Root and Multiple Recursion	511
7.5	Parallel Machine Model	527
7.6	$\lambda$ -Calculi for Parallel Computable Higher Type Functionals	554
7.6.1	Introduction to Higher Types	555
7.6.2	$p$ -Types	556
7.6.3	Finite Typed Lambda Calculus	558
7.7	Historical and Bibliographical Remarks	564
7.8	Exercises	565
	<b>References</b>	<b>569</b>
	<b>Index</b>	<b>591</b>

Boolean Functions and Computation Models

Clote, P.; Kranakis, E.

2002, XIV, 602 p., Hardcover

ISBN: 978-3-540-59436-9