

CONTENTS

| | |
|---|------|
| PREFACE | xiii |
| CHAPTER I. INTRODUCTION | 1 |
| CHAPTER II. THE PREDICATE CALCULUS AND THE SYSTEM LK | 9 |
| II.1. Propositional Calculus | 9 |
| II.1.1. Gentzen's Propositional Proof System PK | 10 |
| II.1.2. Soundness and Completeness of PK | 12 |
| II.1.3. PK Proofs from Assumptions | 13 |
| II.1.4. Propositional Compactness | 16 |
| II.2. Predicate Calculus | 17 |
| II.2.1. Syntax of the Predicate Calculus | 17 |
| II.2.2. Semantics of Predicate Calculus | 19 |
| II.2.3. The First-Order Proof System LK | 21 |
| II.2.4. Free Variable Normal Form | 23 |
| II.2.5. Completeness of LK without Equality | 24 |
| II.3. Equality Axioms | 31 |
| II.3.1. Equality Axioms for LK | 32 |
| II.3.2. Revised Soundness and Completeness of LK | 33 |
| II.4. Major Corollaries of Completeness | 34 |
| II.5. The Herbrand Theorem | 35 |
| II.6. Notes | 38 |
| CHAPTER III. PEANO ARITHMETIC AND ITS SUBSYSTEMS | 39 |
| III.1. Peano Arithmetic | 39 |
| III.1.1. Minimization | 44 |
| III.1.2. Bounded Induction Scheme | 44 |
| III.1.3. Strong Induction Scheme | 44 |
| III.2. Parikh's Theorem | 44 |
| III.3. Conservative Extensions of $\mathbf{I}\Delta_0$ | 49 |
| III.3.1. Introducing New Function and Predicate Symbols | 50 |
| III.3.2. $\overline{\mathbf{I}\Delta_0}$: A Universal Conservative Extension of $\mathbf{I}\Delta_0$ | 54 |
| III.3.3. Defining $y = 2^x$ and $\mathbf{BIT}(i, x)$ in $\mathbf{I}\Delta_0$ | 59 |
| III.4. $\mathbf{I}\Delta_0$ and the Linear Time Hierarchy | 65 |

| | | |
|-------------|---|-----|
| viii | CONTENTS | |
| III.4.1. | The Polynomial and Linear Time Hierarchies | 65 |
| III.4.2. | Representability of <i>LTH</i> Relations | 66 |
| III.4.3. | Characterizing the <i>LTH</i> by IA_0 | 69 |
| III.5. | Buss's S_2^i Hierarchy: The Road Not Taken | 70 |
| III.6. | Notes | 71 |
| CHAPTER IV. | TWO-SORTED LOGIC AND COMPLEXITY CLASSES | 73 |
| IV.1. | Basic Descriptive Complexity Theory | 74 |
| IV.2. | Two-Sorted First-Order Logic | 76 |
| IV.2.1. | Syntax | 76 |
| IV.2.2. | Semantics | 78 |
| IV.3. | Two-Sorted Complexity Classes | 80 |
| IV.3.1. | Notation for Numbers and Finite Sets | 80 |
| IV.3.2. | Representation Theorems | 81 |
| IV.3.3. | The <i>LTH</i> Revisited | 86 |
| IV.4. | The Proof System LK^2 | 87 |
| IV.4.1. | Two-Sorted Free Variable Normal Form | 90 |
| IV.5. | Single-Sorted Logic Interpretation | 91 |
| IV.6. | Notes | 93 |
| CHAPTER V. | THE THEORY V^0 AND AC^0 | 95 |
| V.1. | Definition and Basic Properties of V^i | 95 |
| V.2. | Two-Sorted Functions | 101 |
| V.3. | Parikh's Theorem for Two-Sorted Logic | 104 |
| V.4. | Definability in V^0 | 106 |
| V.4.1. | Δ_1^1 -Definable Predicates | 115 |
| V.5. | The Witnessing Theorem for V^0 | 117 |
| V.5.1. | Independence Follows from the Witnessing Theorem for V^0 | 118 |
| V.5.2. | Proof of the Witnessing Theorem for V^0 | 119 |
| V.6. | \overline{V}^0 : Universal Conservative Extension of V^0 | 124 |
| V.6.1. | Alternative Proof of the Witnessing Theorem for V^0 | 127 |
| V.7. | Finite Axiomatizability | 129 |
| V.8. | Notes | 130 |
| CHAPTER VI. | THE THEORY V^1 AND POLYNOMIAL TIME | 133 |
| VI.1. | Induction Schemes in V^i | 133 |
| VI.2. | Characterizing P by V^1 | 135 |
| VI.2.1. | The "If" Direction of Theorem VI.2.2 | 137 |
| VI.2.2. | Application of Cobham's Theorem | 140 |
| VI.3. | The Replacement Axiom Scheme | 142 |
| VI.3.1. | Extending V^1 by Polytime Functions | 145 |
| VI.4. | The Witnessing Theorem for V^1 | 147 |
| VI.4.1. | The Sequent System $LK^2\text{-}\tilde{V}^1$ | 150 |

CONTENTS

ix

| | | |
|---|--|-----|
| VI.4.2. | Proof of the Witnessing Theorem for V^1 | 154 |
| VI.5. | Notes | 156 |
| CHAPTER VII. PROPOSITIONAL TRANSLATIONS | | 159 |
| VII.1. | Propositional Proof Systems | 160 |
| VII.1.1. | Treelike vs Daglike Proof Systems | 162 |
| VII.1.2. | The Pigeonhole Principle and Bounded Depth PK | 163 |
| VII.2. | Translating V^0 to bPK | 165 |
| VII.2.1. | Translating Σ_0^B Formulas | 166 |
| VII.2.2. | \tilde{V}^0 and $LK^2\text{-}\tilde{V}^0$ | 169 |
| VII.2.3. | Proof of the Translation Theorem for V^0 | 170 |
| VII.3. | Quantified Propositional Calculus | 173 |
| VII.3.1. | QPC Proof Systems | 175 |
| VII.3.2. | The System G | 175 |
| VII.4. | The Systems G_i and G_i^* | 179 |
| VII.4.1. | Extended Frege Systems and Witnessing in G_1^* | 186 |
| VII.5. | Propositional Translations for V^i | 191 |
| VII.5.1. | Translating V^0 to Bounded Depth G_0^* | 195 |
| VII.6. | Notes | 198 |
| CHAPTER VIII. THEORIES FOR POLYNOMIAL TIME AND BEYOND | | 201 |
| VIII.1. | The Theory VP and Aggregate Functions | 201 |
| VIII.1.1. | The Theory \widehat{VP} | 207 |
| VIII.2. | The Theory VPV | 210 |
| VIII.2.1. | Comparing VPV and V^1 | 213 |
| VIII.2.2. | VPV Is Conservative over VP | 214 |
| VIII.3. | TV^0 and the TV^i Hierarchy | 217 |
| VIII.3.1. | $TV^0 \subseteq VPV$ | 220 |
| VIII.3.2. | Bit Recursion | 222 |
| VIII.4. | The Theory $V^1\text{-HORN}$ | 223 |
| VIII.5. | TV^1 and Polynomial Local Search | 228 |
| VIII.6. | KPT Witnessing and Replacement | 237 |
| VIII.6.1. | Applying KPT Witnessing | 239 |
| VIII.7. | More on V^i and TV^i | 243 |
| VIII.7.1. | Finite Axiomatizability | 243 |
| VIII.7.2. | Definability in the V^∞ Hierarchy | 245 |
| VIII.7.3. | Collapse of V^∞ vs Collapse of PH | 253 |
| VIII.8. | RSUV Isomorphism | 256 |
| VIII.8.1. | The Theories S_2^i and T_2^i | 256 |
| VIII.8.2. | RSUV Isomorphism | 258 |
| VIII.8.3. | The $\#$ Translation | 260 |
| VIII.8.4. | The b Translation | 262 |
| VIII.8.5. | The RSUV Isomorphism between S_2^i and V^i | 263 |
| VIII.9. | Notes | 266 |

| | |
|--|-----|
| CHAPTER IX. THEORIES FOR SMALL CLASSES | 267 |
| IX.1. AC^0 Reductions | 269 |
| IX.2. Theories for Subclasses of P | 272 |
| IX.2.1. The Theories VC | 273 |
| IX.2.2. The Theory \widehat{VC} | 274 |
| IX.2.3. The Theory \overline{VC} | 278 |
| IX.2.4. Obtaining Theories for the Classes of Interest | 280 |
| IX.3. Theories for TC^0 | 281 |
| IX.3.1. The Class TC^0 | 282 |
| IX.3.2. The Theories VTC^0 , $\widehat{VTC^0}$, and $\overline{VTC^0}$ | 283 |
| IX.3.3. Number Recursion and Number Summation | 287 |
| IX.3.4. The Theory VTC^0V | 289 |
| IX.3.5. Proving the Pigeonhole Principle in VTC^0 | 291 |
| IX.3.6. Defining String Multiplication in VTC^0 | 293 |
| IX.3.7. Proving Finite Szpilrajn's Theorem in VTC^0 | 298 |
| IX.3.8. Proving Bondy's Theorem | 299 |
| IX.4. Theories for $AC^0(m)$ and ACC | 303 |
| IX.4.1. The Classes $AC^0(m)$ and ACC | 303 |
| IX.4.2. The Theories $V^0(2)$, $\widehat{V^0(2)}$, and $\overline{V^0(2)}$ | 304 |
| IX.4.3. The "onto" PHP and Parity Principle | 306 |
| IX.4.4. The Theory $VAC^0(2)V$ | 308 |
| IX.4.5. The Jordan Curve Theorem and Related Principles | 309 |
| IX.4.6. The Theories for $AC^0(m)$ and ACC | 313 |
| IX.4.7. The Modulo m Counting Principles | 316 |
| IX.4.8. The Theory $VAC^0(6)V$ | 318 |
| IX.5. Theories for NC^1 and the NC Hierarchy | 319 |
| IX.5.1. Definitions of the Classes | 320 |
| IX.5.2. BSV P and NC^1 | 321 |
| IX.5.3. The Theories VNC^1 , $\widehat{VNC^1}$, and $\overline{VNC^1}$ | 323 |
| IX.5.4. $VTC^0 \subseteq VNC^1$ | 326 |
| IX.5.5. The Theory VNC^1V | 333 |
| IX.5.6. Theories for the NC Hierarchy | 335 |
| IX.6. Theories for NL and L | 339 |
| IX.6.1. The Theories VNL , \widehat{VNL} , and \overline{VNL} | 339 |
| IX.6.2. The Theory $V^1\text{-}KROM$ | 343 |
| IX.6.3. The Theories VL , \widehat{VL} , and \overline{VL} | 351 |
| IX.6.4. The Theory VLV | 356 |
| IX.7. Open Problems | 358 |
| IX.7.1. Proving Cayley–Hamilton in VNC^2 | 358 |
| IX.7.2. VSL and $VSL \stackrel{?}{=} VL$ | 358 |
| IX.7.3. Defining $\lfloor X/Y \rfloor$ in VTC^0 | 360 |
| IX.7.4. Proving PHP and $Count_{m'}$ in $V^0(m)$ | 360 |
| IX.8. Notes | 360 |

CONTENTS

xi

| | |
|---|-----|
| CHAPTER X. PROOF SYSTEMS AND THE REFLECTION PRINCIPLE | 363 |
| X.1. Formalizing Propositional Translations | 364 |
| X.1.1. Verifying Proofs in TC^0 | 364 |
| X.1.2. Computing Propositional Translations in TC^0 | 373 |
| X.1.3. The Propositional Translation Theorem for TV^i | 377 |
| X.2. The Reflection Principle | 382 |
| X.2.1. Truth Definitions | 383 |
| X.2.2. Truth Definitions vs Propositional Translations | 387 |
| X.2.3. RFN and Consistency for Subsystems of G | 396 |
| X.2.4. Axiomatizations Using RFN | 403 |
| X.2.5. Proving p -Simulations Using RFN | 407 |
| X.2.6. The Witnessing Problems for G | 408 |
| X.3. VNC^1 and G_0^* | 410 |
| X.3.1. Propositional Translation for VNC^1 | 410 |
| X.3.2. The Boolean Sentence Value Problem | 414 |
| X.3.3. Reflection Principle for PK | 421 |
| X.4. VTC^0 and Threshold Logic | 428 |
| X.4.1. The Sequent Calculus PTK | 428 |
| X.4.2. Reflection Principles for Bounded Depth PTK | 433 |
| X.4.3. Propositional Translation for VTC^0 | 434 |
| X.4.4. Bounded Depth GTC_0 | 441 |
| X.5. Notes | 442 |
| APPENDIX A. COMPUTATION MODELS | 445 |
| A.1. Deterministic Turing Machines | 445 |
| A.1.1. L , P , $PSPACE$, and EXP | 447 |
| A.2. Nondeterministic Turing Machines | 449 |
| A.3. Oracle Turing Machines | 451 |
| A.4. Alternating Turing Machines | 452 |
| A.5. Uniform Circuit Families | 453 |
| BIBLIOGRAPHY | 457 |
| INDEX | 465 |