

# Logic in Computer Science: Modelling and Reasoning about Systems

MICHAEL HUTH  
Department of Computing and Information Sciences  
Kansas State University, USA.

MARK RYAN  
School of Computer Science  
University of Birmingham, UK.



# Contents

<i>Preface</i>	<b>1</b>
<i>Acknowledgments</i>	<b>8</b>
<b>1 Propositional Logic</b>	<b>9</b>
1.1 Declarative sentences . . . . .	10
1.2 Natural deduction . . . . .	14
1.2.1 Rules for natural deduction . . . . .	15
1.2.2 Derived rules . . . . .	36
1.2.3 Natural deduction in summary . . . . .	38
1.2.4 Provable equivalence . . . . .	41
1.2.5 An aside: proof by contradiction . . . . .	42
1.3 Propositional logic as a formal language . . . . .	46
1.4 Semantics of propositional logic . . . . .	55
1.4.1 The meaning of logical connectives . . . . .	55
1.4.2 Mathematical induction . . . . .	60
1.4.3 Soundness of propositional logic . . . . .	65
1.4.4 Completeness of propositional logic . . . . .	70
1.5 Normal forms . . . . .	78
1.5.1 Semantic equivalence, satisfiability, and validity . . . . .	78
1.5.2 Conjunctive normal forms and validity . . . . .	85
1.5.3 Horn clauses and satisfiability . . . . .	94
1.6 Bibliographic notes . . . . .	98
<b>2 Predicate Logic</b>	<b>100</b>
2.1 The need for a richer language . . . . .	100
2.2 Predicate logic as a formal language . . . . .	106

2.2.1	Terms . . . . .	106
2.2.2	Formulas . . . . .	108
2.2.3	Free and bound variables . . . . .	113
2.2.4	Substitution . . . . .	115
2.3	Proof theory of predicate logic . . . . .	119
2.3.1	Natural deduction rules . . . . .	119
2.3.2	Quantifier equivalences . . . . .	131
2.4	Semantics of predicate logic . . . . .	139
2.4.1	Models . . . . .	140
2.4.2	Semantic entailment . . . . .	147
2.4.3	The semantics of equality . . . . .	149
2.5	Undecidability of predicate logic . . . . .	152
2.6	Bibliographic notes . . . . .	158
<b>3</b>	<b>Verification by Model Checking</b>	<b>160</b>
3.1	Motivation for verification . . . . .	160
3.2	Syntax of computation tree logic . . . . .	164
3.3	Semantics of computation tree logic . . . . .	168
3.3.1	Practical patterns of specifications . . . . .	177
3.3.2	Important equivalences between CTL formulas . . . . .	178
3.4	Example: mutual exclusion . . . . .	181
3.4.1	First modelling attempt . . . . .	182
3.4.2	Second modelling attempt . . . . .	183
3.5	A model checking algorithm . . . . .	184
3.5.1	The labelling algorithm . . . . .	185
3.5.2	Pseudo-code of the model checking algorithm . . . . .	189
3.5.3	The ‘state explosion’ problem . . . . .	190
3.6	The SMV system . . . . .	193
3.6.1	Modules in SMV . . . . .	195
3.6.2	Synchronous and asynchronous composition . . . . .	196
3.6.3	Mutual exclusion revisited . . . . .	197
3.6.4	The Alternating Bit protocol . . . . .	201
3.7	Model checking with fairness . . . . .	205
3.8	Alternatives and extensions of CTL . . . . .	207
3.8.1	Linear-time temporal logic . . . . .	207
3.8.2	CTL* . . . . .	210
3.8.3	The expressive power of CTL . . . . .	213
3.9	The fixed-point characterization of CTL . . . . .	215
3.9.1	Monotone functions . . . . .	218
3.9.2	The correctness of SAT <sub>EG</sub> . . . . .	220

3.9.3	The correctness of SAT <sub>EU</sub>	222
3.10	Bibliographic notes	226
<b>4</b>	<b><i>Program Verification</i></b>	<b>228</b>
4.1	Why should we specify and verify code?	229
4.2	A framework for software verification	230
4.2.1	A core programming language	232
4.2.2	Hoare triples	235
4.2.3	Partial and total correctness	238
4.2.4	Program variables and logical variables	241
4.3	Proof calculus for partial correctness	242
4.3.1	Proof rules	242
4.3.2	Proof tableaux	246
4.3.3	A case study: minimal-sum section	264
4.4	Proof calculus for total correctness	270
4.5	Bibliographic notes	273
<b>5</b>	<b><i>Modal Logics and Agents</i></b>	<b>274</b>
5.1	Modes of truth	274
5.2	Basic modal logic	275
5.2.1	Syntax	275
5.2.2	Semantics	276
5.3	Logic engineering	286
5.3.1	The stock of valid formulas	287
5.3.2	Important properties of the accessibility relation	291
5.3.3	Correspondence theory	293
5.3.4	Some modal logics	297
5.3.5	Semantic entailment	301
5.4	Natural deduction	302
5.5	Reasoning about knowledge in a multi-agent system	306
5.5.1	Some examples	306
5.5.2	The modal logic KT45 <sup>n</sup>	309
5.5.3	Natural deduction for KT45 <sup>n</sup>	315
5.5.4	Formalising the examples	317
5.6	Bibliographic notes	328
<b>6</b>	<b><i>Binary Decision Diagrams</i></b>	<b>330</b>
6.1	Representing boolean functions	330
6.1.1	Propositional formulas and truth tables	331
6.1.2	Binary decision diagrams	333

6.1.3	Ordered BDDs . . . . .	340
6.2	Algorithms for reduced OBDDs . . . . .	348
6.2.1	The algorithm <code>reduce</code> . . . . .	348
6.2.2	The algorithm <code>apply</code> . . . . .	350
6.2.3	The algorithm <code>restrict</code> . . . . .	357
6.2.4	The algorithm <code>exists</code> . . . . .	359
6.2.5	Assessment of OBDDs . . . . .	361
6.3	Symbolic model checking . . . . .	365
6.3.1	Representing subsets of the set of states . . . . .	365
6.3.2	Representing the transition relation . . . . .	369
6.3.3	Implementing the functions $\text{pre}_\exists$ and $\text{pre}_\forall$ . . . . .	370
6.3.4	Synthesising OBDDs . . . . .	372
6.4	The relational $\mu$ -calculus . . . . .	375
6.4.1	Syntax and semantics . . . . .	376
6.4.2	Coding CTL models and specifications . . . . .	380
6.5	Bibliographic notes . . . . .	388
<i>Index</i>		<b>389</b>
<i>Bibliography</i>		<b>399</b>

# Preface

## *Our motivation for writing this book*

Recent years have brought about the development of powerful tools for verifying specifications of hardware and software systems. By now, the IT industry has realized the impact and importance of such tools in their own design and implementation processes. Major companies, such as Intel, Siemens, BT, AT&T, and IBM, are now actively investigating this technology and its incorporation into their planning and production departments. This necessitates the availability of a basic formal training which allows *undergraduate* students as well as working programmers and beginning graduate students to gain sufficient proficiency in using and reasoning with such frameworks.

The recent shift of information technologies toward internet-based data access and processing means that there is also an increased demand in qualified individuals who can reason about sophisticated autonomous agent-based software which is able to interact with other agents and gather desired information on large networks.

This book addresses these needs by providing a sound basis in logic, followed by an introduction to the logical frameworks which are used in modelling and reasoning about computer systems. It provides simple and clear presentation of material. A carefully chosen core of essential terminology is introduced; further technicalities are introduced only where they are required by the applications.

We believe that our proposed course material makes a vital contribution to preparing undergraduate students for today's fast paced and changeable professional environments. This confidence stems not only from the topicality of our proposed applications, but also from the conviction that a solid background in logical structures and formalisms can very well serve as a buoy in the rough waters of future software and hardware developments.

There is an abundance of books on mathematical logic or logic in computer science on the market. However, we are not aware of any book that suits the contemporary and applications-driven courses that we teach and are beginning to be taught in most computer science curricula. Existing books tend to be written for logicians rather than computer science students and are thus too “heavy”, and overloaded with technical terminology. The ties to computer science are merely of a foundational nature, such as the Curry-Howard isomorphism, or cut-elimination in sequent calculi. There is an evident need for a book which introduces the contemporary applications of logic which are beginning to be taken up by industry; the book should be accessible to students who do not want to learn logic for its own sake.

It is important to say what the book does not provide: we completely omitted applications like the design and use of theorem-provers, and the exposure to constructive type theories (such as the Calculus of Constructions and the Logical Framework) as a mathematical foundation for program synthesis; and the design, analysis and implementation of programming languages. This decision is by no means meant to represent a judgment of such topics. Indeed, we hope and anticipate that others will address these important issues in a text that is suitable for undergraduates.

### ***Reasons for adopting this book***

Our book zooms in on concepts at the heart of logic and presents them in a contemporary fashion. In that way, and by discussing the implementation of such principles, our material creates stimulating overlaps with other standard courses such as *Formal Language Theory* or an *Introduction to Data Types and Programming*.

It differs from existing books on that subject in the following ways:

- New technical concepts are introduced as they are needed, and never for their own sake. The emphasis is always on applications rather than on mathematical technicalities. Yet, technicalities are always treated with the necessary rigour.
- We introduce, at an accessible level, a framework for program verification (symbolic model checking) which is currently available only in research papers. This is at present a hot topic in industry, and graduates fluent in this material are highly sought.
- Our text is supplemented by a worldwide web site<sup>1</sup> which offers additional

<sup>1</sup> [www.cs.bham.ac.uk/research/lics/](http://www.cs.bham.ac.uk/research/lics/)

material useful for classroom presentations; such as postscript files of figures for online, or overhead projector, presentations; and html files of all the SMV code featured in the book.

- All sections of the book have several exercises marked with an \* as in

EXERCISES 0.1

- \* 1. ...
  - 2. ...
  - \* 3. ...
  - 4. ...
- 

for which we have provided sample solutions in L<sup>A</sup>T<sub>E</sub>X. Bona fide teachers and instructors may obtain the postscript files directly from Cambridge University Press. Exercises end with a short bar, as shown, in order that the reader know where to pick up the text.

*Outline of the book*

One of the leitmotifs of our book is the observation that most logics used in the design, specification, and verification of computer systems fundamentally deal with a *satisfaction relation*

$$\mathcal{M} \models \phi$$

where  $\mathcal{M}$  is some sort of *situation* or *model*, like the snapshot of a system, and  $\phi$  is a specification, a formula of that logic, expressing what should be true in situation  $\mathcal{M}$ . For example,  $\mathcal{M}$  could model a communications protocol and  $\phi$  the property that the protocol be fair. At the heart of this setup is that  $\models$  is actually computable in a compositional way. Fixing the situation  $\mathcal{M}$ , we determine whether  $\mathcal{M} \models \phi$  holds by recursively determining this for all subformulas of  $\phi$ . We expand this view for a particular logic (CTL), where this computation and the modelling of a situation may be done purely symbolically using boolean formulas. Tools which support this reasoning make the approach applicable to quite a few realistic systems and designs.

Here is a brief synopsis of what the book covers:

**Chapter 1**, on propositional logic, should be the common starting point and backbone for any course based on this book; it might also be used as a reference text for courses that presuppose a knowledge of propositional logic. Its sections provide

- a complete presentation of a natural deduction style proof system for propositional logic with a discussion of the intuitionistic fragment;
- a section on propositional logic as a formal language;
- the semantics of propositional logic, where:
  - we constructively prove soundness *and* completeness of the proof system with respect to the usual truth table semantics;
  - we discuss the notions of equivalence, satisfiability, and validity;
  - we cover the principle of mathematical induction, which is needed for soundness, often employed in our book, and is one of the central reasoning tools in computer science; and
  - we feature a section on disjunctive normal forms and Horn formulas; our presentation highlights the development of algorithms computing such normal forms as well as discussing their correctness.

**Chapter 2** addresses predicate logic. In this chapter we

- first motivate the need for richer logics via symbolic representations of natural language sentences;
- define and study predicate logic as a formal language with the standard notions of static scoping (free and bound variables) and substitution;
- familiarize students with its semantics,
- introduce a natural deduction style proof system for predicate logic by “enriching” the proof system of Chapter 1 with the introduction and elimination rules for quantifiers; we use this system to prove the standard quantifier equivalences; and
- present Church’s proof of the undecidability of satisfaction in predicate logic (via reduction to the Post correspondence problem).

**Chapter 3** introduces students to *model checking*, a state-of-the-art technique in verifying concurrent systems. We

- focus on the syntax and semantics of CTL (Computation Tree Logic), and derive the standard algorithm for model checking CTL formulas;
- let students practice the synthesis and interpretation of practically relevant, and frequently occurring, specifications in CTL;
- present two case studies in great detail: a mutual exclusion protocol and an alternating bit protocol; both protocols are developed as labelled transition systems;

- introduce the symbolic model verifier SMV, and provide SMV code for our case studies and discuss the relevant CTL specifications;
- explain how CTL and SMV manage to incorporate fairness constraints;
- discuss the logics LTL and CTL\* and compare their expressive power to that of CTL;
- give a fixed-point characterization of those CTL operators which express invariant behaviour; and
- conclude by pointing out that practical specifications often obey common patterns and offer pointers to web-sites, where such patterns are developed, surveyed, and documented.

**Chapter 4** covers program verification by discussing deductive reasoning about imperative programs; it presents a Floyd-Hoare style program logic for a sequential imperative core programming language, reminiscent to a fragment of the C programming language. The emphasis will be on correctness proofs (partial and total correctness) for fairly simple programs. The main objective is to challenge students to systematically develop small programs meeting required input/output behaviour. In particular, they need to develop the ability to come up with characterizing invariants of while-loops.

**Chapter 5** discusses modal logics and agents. Modal logics are motivated through a desire to have possible world semantics.

- We discuss general syntax, semantics, and an extension of the propositional logic deduction calculus for basic modal logic. The theme of the first part of this chapter is that of “logic engineering”: e.g. if  $\Box\phi$  means that an agent *knows*  $\phi$ , then what axioms and inference rules for  $\Box$  should we engineer? We carry out such a task for various meanings of  $\Box$ .
- The second part of this chapter is devoted to the study of a modal logic modelling general reasoning about knowledge in a Multi-Agent System ( $KT45^n$ ). It carefully explains how some epistemological puzzles can be solved using this modal logic.

**Chapter 6** introduces binary decision diagrams, which are a data structure for boolean functions.

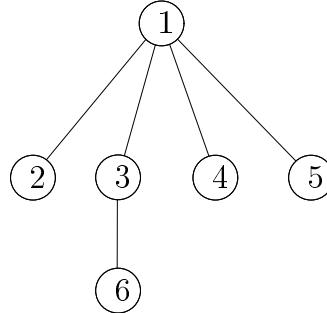
- We describe ordered binary decision diagrams (OBDDs) and their accompanying algorithms;
- We discuss extensions and variations of OBDDs as well as their limitations;
- We explain how CTL models can be coded as boolean formulas;

- We present the syntax and semantics of the relational mu-calculus within which we code CTL models and their specification in the presence of simple fairness constraints.

That chapter should create stimulating links to courses on algorithms and data structures, courses on circuit design, and can also be used as a foundation for implementation projects which develop tools supporting reasoning with the concepts developed in other chapters.

At the end of each chapter, we provide pointers to the literature and to sites where free software may be downloaded, if applicable. A detailed index should allow for the quick discovery of cross-connections between most of these chapters.

**Dependency of chapters and prerequisites.** The book requires that students know the basics of elementary arithmetic and naive set theoretic concepts and notation. The core material of Chapter 1 (everything except Sections 1.4.3 to 1.5.3) is essential for all of the chapters that follow. Other than that, only Chapter 6 depends on Chapter 3, and a basic understanding of the static scoping rules covered in Chapter 2 — although one may easily cover Sections 6.1 and 6.2 without having done Chapter 3 at all. The dependency graph of chapters can be seen below:



### *Suggested course outlines*

We suggest at least three different ways of teaching with this text (based on a 12-15 week course).

- A course based on Chapters 1, 2, and 5 would be suitable for students specialising in database and information systems or artificial intelligence; this choice of material should prepare them for more advanced topics in database programming and automated deduction.

- A course based on Chapters 1, 3, and 6 would focus on the complete development of a verification framework for concurrent systems down to the implementation level.
- A course based on Chapters 1, 3, and 4 would provide a broader presentation of the logical foundations of programming.

**Suitable courses based on the book.** This book can be used as the main text book in a course on the introduction to logic in computer science, and the specification and verification of computer systems and programs. It may be quite useful as an additional text in courses on algorithms and data structures, the introduction to logic in artificial intelligence, sequential circuit and chip design and validation, discrete mathematics for computer scientists, formal language theory, as well as courses in networks and operating systems.

#### *WWW page*

This book is supported by a WWW page, which contains a list of errata, the SMV source code for examples in Chapter 3, some further exercises, and details of how to obtain the solutions to exercises in this book which are marked with a \*. There are also links to other relevant pages. The URL for the book's page is

[www.cs.bham.ac.uk/research/lics/](http://www.cs.bham.ac.uk/research/lics/)

## Acknowledgments

Many people have, directly or indirectly, assisted us in writing this book. David Schmidt kindly provided several exercises for Chapter 4. Krysia Broda has pointed out some typographical errors, and she and the other authors of [BEKV94] have allowed us to use some exercises from that book (notably Exercises 1.6(1(b)), 2.2(5), 2.5(4, 9, 10)). We also borrowed exercises or examples from [Hod77] and [FHMV95]. Zena Matilde Ariola, Josh Hodas, Jan Komorowski, Sergey Kotov, Scott A. Smolka and Steve Vickers have corresponded with us about this text; their comments are appreciated. Matt Dwyer and John Hatcliff made useful comments on drafts of Chapter 3. A number of people read and provided useful comments on several chapters, including: Graham Clark, Christian Haack, Anthony Hook, Achim Jung, Kevin Lucas, Roberto Segala, Alan Sexton, and Allen Stoughton. Numerous students at Kansas State University and the University of Birmingham have given us feedback of various kinds, which have influenced our choice and presentation of the topics. We acknowledge Paul Taylor’s L<sup>A</sup>T<sub>E</sub>X package for proof boxes. About half a dozen anonymous referees made critical, but constructive comments which helped to improve this text in various ways. In spite of these contributions, there may still be errors in the book, and we alone must take responsibility for those.

# Index

- ABP, 201
  - acknowledgment channel, 201
  - alternating the control bit, 201
  - fairness, 201
  - main SMV program, 204
- absorption laws, 84
- abstract data type
  - sets, 190
- abstraction, 163, 192, 205
  - and non-determinism, 194
- accessibility relation, 277, 291, 311
- adequate set of connectives
  - for CTL, 179, 180, 185, 207, 210, 385
  - for propositional logic, 80, 99
- agent, 275, 289, 298
- algebraic specification, 158
- algorithm
  - deterministic, 85
  - algorithm **apply**, 350
    - complexity, 361
    - control structure, 351
    - recursive descent, 352
  - algorithm CNF, 85
  - algorithm **reduce**, 348
    - complexity, 361
  - algorithm **restrict**, 357
    - complexity, 361
  - algorithm **reduce**
    - example execution, 350
  - alternating bit protocol, 201
  - always in the future, 289
  - and-elimination, 15, 316
  - and-introduction, 15, 316
  - application domain, 161, 228
  - approach
    - model-based, 161
    - proof-based, 161
  - approximants
    - $\mu_m Z.f$ , 378
    - $\nu_m Z.f$ , 378
  - arity, 106, 107
  - array, 235
  - bounds, 264
  - field, 264
    - of integers, 264
    - section, 264
  - artificial intelligence, 274
  - artificial language, 100
  - assignment, 193
    - initial, 268
    - non-deterministic, 202, 206
    - program notation, 233
    - statement, 163, 233
  - associativity laws, 81, 84
  - assumption
    - discharging, 40, 302
    - stack of assumptions, 67
    - temporary, 21, 136
  - asynchronous
    - circuit, 330
    - interleaving, 182
  - atom
    - marking, 95
  - atomic formula, 309
    - of modal logic, 275
    - of predicate logic
    - meaning, 141
  - axiom
    - 5**, 304, 305
    - T**, 318
    - 4, 299, 304, 315
    - 5**, 304, 315
    - T**, 299, 304, 315, 320
    - for assignment, 243
    - for equality, 120
    - for modal logic, 297
    - instance, 244
    - schemes, 301
  - Backus Naur form (BNF), 48
  - backwards breadth-first search, 188, 207
  - base case, 60, 61, 65
  - basic modal logic, 275
  - BDD, 338
    - hi( $n$ ), 349
    - lo( $n$ ), 349

- as boolean function, 338
- complement, 340
- consistent path, 339
- edge, 333
- examples, 338
- has an ordering, 341
- layer of variables, 333
- line
  - dashed, 334, 338
  - solid, 334, 338
- ordered, 341
- read-1, 357
- reduced, 338
- removal of duplicate non-terminals, 337
- removal of duplicate terminals, 337
- removal of redundant tests, 337
- satisfiable, 339
- subBDD, 336
- which is not a read-1-BDD, 358
- which is not an OBDD, 342
- with duplicated subBDDs, 336
- belief, 289
- binary decision diagram, 338
- binary decision tree, 333
- redundancies in, 335
- binding priorities, 165
  - for basic modal logic, 275
  - for integer expressions, 232
  - for  $KT45^n$ , 310
  - for predicate logic, 109
  - for propositional logic, 13
  - for relational mu-calculus, 376
- bit, 154
  - control, 201
  - least significant, 363
  - most significant, 363
  - one-bit channel, 202
  - two-bit channel, 202
- blocks of code, 233
- Boole, G., 98, 351
- boolean algebra, 29
- boolean connective, 166, 278
- boolean existential quantification, 359
- boolean expression, 233, 245
- boolean forall quantification, 361
- boolean formula
  - independent of a variable, 352
  - semantically equivalent, 351
  - truth table, 331
- boolean function
  - 'don't care' conditions, 355
  - as a binary decision tree, 333
  - symbolic representation, 330
- boolean guard, 258
- boolean variable, 330
- bottom, 32
- bottom-elimination, 33
- bottom-introduction (see "not-elimination"), 33
- box-elimination, 303
- box-introduction, 303
- branching-time logic, 162
- case
  - overlap, 88
- case analysis, 87, 89, 126
- case-statement, 28, 194
- characteristic function, 366
- Church, A., 153
- circuit
  - 2-bit comparator, 374
  - asynchronous, 197, 373
  - sequential, 331
  - synchronous, 197, 330, 373, 385
- circular definition, 180
- Clarke, E., 163, 227
- classical logic, 42, 300
- client, 231
- clock tick, 184
- closure under propositional logic, 297
- CNF, 81
- code
  - specification, 229
  - verification, 229
- coding
  - AF, 382
  - EF, 381
  - EG, 382
  - EU, 382
  - EX, 381
  - examples of symbolic evaluation, 382
  - fair EG, 386
  - fair EU, 386
  - fair EX, 386
  - set of fair states, 385
- command, 233
  - atomic, 233
  - compound, 233
- common knowledge, 306, 310
  - as invariant, 375
- communicating processes, 228
- communication protocol, 197
- completeness
  - of natural deduction for predicate logic, 103
  - of natural deduction for propositional logic, 78
- complexity
  - exponential, 190
  - of apply, 356
  - of brute force minimal-sum section algorithm, 265
  - of fairness, 386
  - of labelling algorithm, 187, 188
  - of labelling  $EG_C$ , 207
- composition
  - sequential, 252
  - synchronous, 196
- compositional semantics, 57
- compositionality
  - in model checking, 193
- computability, 152
- computation

- intractable, 70
- computation path, 171
  - fair, 207
- computation trace, 260
- computation tree logic, 163, 274, 289
- computational behaviour, 274
- computer program, 114
- concatenation, 142, 153
- conclusion, 12, 246, 257
- concurrency, 229
- conjunct, 82
- conjunction, 12, 267
  - infinite, 310
- connective
  - adequate set, 190
  - unary, 165
- consistency, 151, 276, 287
- constant symbol, 111
- contradiction, 31, 132, 289, 296
- control structure, 233, 234
- controlling value, 356
- copy rule, 30, 303
- core programming language, 232, 264
- correspondence theory, 297
- counter example, 140, 149, 287, 305
- counter trace, 162
- critical section, 181
- CTL, 163, 227, 274, 289
  - as a subset of CTL\*, 211
  - expressive power, 213
  - modalities, 274
  - model checker, 193
  - with boolean combinations of path formulas, 213, 214
- CTL connectives
  - fair, 385
- CTL formula
  - square brackets, 166
- CTL\*, 210, 227
- dag, 338
- dashed box
  - flavour, 315
- data structure, 141
- de Morgan laws, 83, 179, 215
  - for modalities, 282
- deadlock, 168, 177, 212
- debugging systems, 185, 229
- decision problem, 152
  - of validity in predicate logic, 153
- decision procedure, 79
- declarative explanation, 38
- declarative sentence, 10, 100
  - truth value, 55
- default case, 194
- definition
  - inductive, 48
- description
  - informal, 230, 236, 265
  - language, 160, 162
- Dijkstra, E., 259
- directed graph, 168, 337
  - acyclic, 338
  - cycle, 337
- disjunction, 12
  - of literals, 81, 83
- distributivity laws
  - of box modality, 282
  - of F connective, 209
  - of propositional logic, 29, 84, 87
- dividend, 263
- don't care links, 369
- double negation-elimination, 301
- double negation-introduction, 301
- elimination rule, 15, 120
- Emerson, E. A., 163, 227
- encoding, 146
- entailment
  - in program logics, 251
- environment
  - and non-determinism, 194
  - for concurrent programs, 161
  - for predicate logic formulas, 144
- equality, 235
  - intentional, 120
  - program notation, 233
  - symbol, 119
- equivalence relation, 292, 298, 314
- equivalent formulas
  - of basic modal logic, 283
  - of CTL, 178–180
  - of KT4, 299
  - of KT45, 298
  - of LTL, 209
  - of predicate logic, 132
  - of propositional logic, 26, 179
  - of relational mu-calculus, 380
- exclusive-or, 333, 364
- existential quantifier, 179
- exists-elimination, 126
- exists-introduction, 126
- factorial
  - of a natural number, 234
  - program, 234, 260
- fairness
  - nested fixed points, 386
  - symbolic model checking, 385
- fairness constraint, 184, 197
  - simple, 205, 206
- FAIRNESS running, 202
- Fibonacci numbers, 76
- field index, 264
- finite automata, 358
- finite data structure, 185
- first order logic, 100
- fixed point, 218
  - greatest, 218, 219
  - least, 218, 219
  - semantics for CTL, 180, 215
- flow of control, 234

- Floyd, R., 242
- for-loop, 235
- forall-elimination, 122
- forall-introduction, 123
- formal
  - path, 211
- formula
  - height, 63, 77
  - Horn, 94
  - immediate subformula, 186
  - of basic modal logic, 282
  - of CTL, 164
    - atomic, 164
    - ill-formed, 165
    - well-formed, 165
  - of LTL
    - valid, 215
  - of predicate logic, 109, 250
  - of propositional logic, 48, 71, 178
    - well-formed, 47, 48, 63
  - of relational mu-calculus, 376
  - positive, 300, 319, 325
  - scheme, 179, 280, 288
    - K**, 283
    - in propositional logic, 280
    - instance, 280
  - subformula, 50
- frame, 293
- free for  $x$  in  $\phi$ , 117, 122
- Frege, G., 158
- function
  - in predicate logic, 142
  - monotone, 218
    - a non-example, 218
  - recursive, 181
  - SAT, 189, 191
    - termination, 226
  - SATaf, 192, 216
  - SATag, 226
  - SATeg, 193
  - SATEu, 192
  - SATEx, 191
  - symbol, 104, 105, 111
    - binary, 106
  - translate, 181
- function  $\text{pre}_\exists(X)$ , 368
- function  $\text{pre}_\forall(X)$ , 368
- function SAT
  - correctness, 218
- future
  - excludes the present, 176, 301
  - includes the present, 174, 176, 301
  - whether it includes the present, 289
- world, 162
- G-reachable, 312
  - in  $k$  steps, 312
- Gödel, K., 103
- Gentzen, G., 98
- grammar, 48
- clause, 242
- Halpern, J., 227
- Hoare triple, 236
- Hoare, C.A.R., 236, 242
- Hodges, W., 158
- Horn clause, 94
- hybrid rule, 320
- if-statement, 255
- implication, 12
  - logical, 251
- implies-elimination, 18
- implies-introduction, 21
- in-order representation, 51
- inconsistency, 231
- index, 153
- induction
  - course-of-values, 63
  - hypothesis, 60, 61
  - in model checking, 192
  - mathematical, 60
- inductive step, 60
- infix notation, 142, 166
- information
  - negative, 320
- information content, 32
- input parameter, 87
- integer
  - expression, 232
- integer label, 348
- integer multiplication, 363
- interface between logics, 250
- interleaving
  - formulas with code, 248
  - transitions, 182, 197
- introduction rules, 15, 120
- introspection
  - negative, 290, 298
  - positive, 290, 298
- intuitionistic logic, 42, 134, 299
- invariants, 246
  - discovering, 258
- iterative squaring, 388
- Jape, 158
- justification, 249, 250, 303
- Knaster-Tarski Theorem, 219
- knowledge
  - common, 307
  - distributed, 310
  - false, 292
  - formula
    - positive, 320
  - idealised, 290, 298
  - in a multi-agent system, 275
  - modality, 309
    - of agent, 275, 290
- Kozen, D., 388
- Kripke model, 277
  - as a counter example, 305
  - for  $\text{KT}45^n$ , 311

- Kripke, S., 277, 283
- label  
adding, 186  
deleting, 187
- labelling  
AF, 186  
EG, 187  
 $EG_C$ , 207  
EU, 186  
EX, 186
- labelling algorithm, 185
- labelling function  
coding subsets, 366  
for CTL model, 168  
for Kripke model, 277  
frame does not have one, 294
- language construct, 235
- law of excluded middle, 38
- laws of arithmetic, 250
- LEM  
instance, 300
- linear-time logic, 162
- linear-time temporal logic, 208
- literal, 81, 89
- liveness, 183, 197  
property, 181, 183, 204, 206
- logic engineering, 275, 286
- logic programming, 70, 158
- logical level, 251
- look-up table, 144  
up-dated, 144
- LTL, 208, 227
- machine state, 235
- Manna, Z., 227
- McMillan, K., 227
- memoisation  
of computed OBDDs, 352
- midcondition, 249
- minimal-sum section, 264
- minimal-sum section problem, 273
- modal connective  
 $C_G$ , 310  
 $K_t$ , 309
- modal logic, 274  
K, 298  
KT4, 299  
KT45, 298  
normal, 297  
S4, 299  
S5, 298
- modality, 162, 276  
diamond, 276  
path, 213
- model  
of KT45 $n$ , 311  
of basic modal logic, 277, 296  
of CTL, 168, 278  
pictorial representation, 168, 176, 177  
of intuitionistic propositional logic, 300
- of KT45, 311  
of KT45 $n$ , 312  
of predicate logic, 103, 142  
of propositional logic, 57
- model checker, 162
- model checking, 161, 163, 228  
algorithm, 180, 189, 206, 289  
debugging, 381  
example, 175  
with fairness constraints, 206
- model of CTL, 168
- model-based verification, 160, 162
- module, 237
- modulo 8 counter, 375
- modus ponens, 18
- modus tollens, 19, 300
- muddy children puzzle, 317, 320
- Mutex model  
pictorial representation, 182
- mutual exclusion, 181
- natural deduction  
extension to predicate logic, 103  
for modal logic, 306  
for temporal logic, 162  
inventor, 98
- natural deduction rules  
for basic modal logic, 303  
for KT45 $n$ , 316, 327  
for predicate logic, 120  
for propositional logic, 39
- necessity  
logical, 162, 276, 288  
physical, 288
- negation, 12
- negation-elimination (see  
“bottom-elimination”), 33
- negation-introduction, 33
- nested boolean quantification, 381
- network  
architecture, 163  
synchronous, 162
- no strict sequencing, 182, 183
- node  
initial, 338  
leaf, 114  
non-terminal, 333  
terminal, 334, 338
- non-blocking protocol, 181, 183
- non-determinism, 162, 183
- non-termination, 234
- normal form, 78, 80  
conjunctive, 81, 332  
disjunctive, 332  
negation, 86  
CTL\*, 211  
LTL, 210  
product-of-sums, 363  
sum-of-products, 356
- not-elimination, 33
- not-introduction, 33

- OBDD, 341
  - absence of redundant variables, 346
  - canonical form, 343
  - complementation, 368
  - definition, 341
  - extensions, 364
  - for  $\text{pre}_{\exists}(X)$ , 370
  - for  $\text{pre}_{\forall}(X)$ , 370
  - integer multiplication, 363
  - intersection, 368
  - limitations, 363
  - memoisation, 352
  - nested boolean quantification, 362
  - of an even parity function, 344
  - of the odd parity function, 344
  - of transition relation, 369
  - optimal ordering, 364
  - reduced, 342
    - unique representation, 342
    - reduced one for logical “iff”, 344
  - representing subsets, 365
  - running-time of algorithms
    - upper bounds, 362
  - sensitivity of size, 346
  - synthesis of boolean formula, 362
  - test
    - for implication, 347
    - for satisfiability, 347
    - for semantic equivalence, 346
    - for validity, 347
  - union, 368
  - variations, 364
- odd parity function, 344
- omniscience
  - logical, 289, 290
- or-elimination, 27
- or-introduction, 27
- overloading, 148
  - of proof rules, 120
- parity function
  - even, 343
    - as OBDD, 344
- parity OBDD, 364
- parse tree
  - for a predicate logic formula, 114
  - of a term, 108
  - of a basic modal logic formula, 275
  - of a CTL formula, 166
  - of propositional logic formula, 49
  - root, 50
  - subtree, 50
    - underspecified, 280
- partial correctness, 238
- partial order reduction, 192
- pattern
  - $\text{checkEU}(f, g)$ , 386
  - $\text{checkEX}(f)$ , 386
- pattern matching, 15, 125, 253
- place holder, 101
- Pnueli, A., 227
- possibility, 286
  - logical, 162, 276
- possible world
  - semantics, 283
- Post correspondence problem, 153
- postcondition
  - in program logic, 236
- Prawitz, D., 98
- precondition
  - in program logic, 236
  - weakest, 249
  - of algorithm, 90
- predicate, 100
  - binary, 102
  - number of arguments, 102
  - symbols, 108
  - unary, 102
- predicate logic, 100
  - extension, 250
- prefix, 142
  - notation, 166
  - ordering, 142
- premise, 12, 243
- preprocessing, 190
- Prior, A., 227
- problem
  - instance, 153
  - reduction, 152
- procedural interpretation, 40
- process
  - concurrent, 181
  - instantiation, 204
- processor, 229
- program
  - behaviour, 237
  - bug, 229
  - code, 249
  - construct, 233
  - correctness, 90, 96, 189
  - derived, 235
  - diverging, 238
  - documentation, 229
  - environment, 230
  - finite-state, 330
  - fragment, 235
  - logic, 248
  - methodology, 231
  - procedures, 235
  - sequential, 228
  - termination, 96, 97, 219, 238
  - variable, 190, 241
  - verification, 243
    - formal, 232
- program execution, 286, 290
- programming language
  - imperative, 232
- proof
  - box
    - for  $\rightarrow i$ , 21
    - for forall-introduction, 123
    - for modal logic, 302

- opening, 40
  - side by side, 33
- by contradiction, 37
- calculus, 228, 232
- construction, 242
- constructive, 134
- dashed box, 303, 317
- fragment, 252
- indirect, 42
- of correctness, 216
- of termination, 238
- partial, 255
- partial correctness, 242, 254
- search, 70
- solid box, 303
- strategy, 129, 237
- subproof, 245
- tableaux, 242
- theory, 100, 139, 162
  - total correctness, 270
- proof rules, 14
  - for implication, 246
  - for assignment, 242
  - for conjunction, 15
  - for disjunction, 26
  - for double negation, 17
  - for equality, 120
  - for existential quantification, 126
  - for if-statements, 245, 255
    - modified, 256
  - for implication, 21, 250
  - for KT45<sup>n</sup>, 316
  - for negation, 31
  - for quantifiers, 125
  - for sequential composition, 242, 248
  - for universal quantification, 122
  - for while-statements, 246, 258, 264
  - schema, 125
  - subformula property, 127
- proof tableaux
  - complete, 268
- proof-based verification, 160, 228
- proposition, 10
- propositional logic, 100
- protocol, 181, 182
- provability
  - undecidability of predicate logic, 157
- quantifier, 279, 282
  - equivalences, 209
  - in predicate logic, 102
    - binding priorities, 109
    - equivalences, 148
    - meaning, 141
- Quielle, J., 227
- reasoning
  - about knowledge, 298, 306
  - constructive, 42
  - in an arbitrary related world, 303
  - informal, 319
- quantitative, 231
- unsound, 254
- record
  - field, 196
- recursion
  - mutual, 211
- recursive call, 255
- reductio ad absurdum, 37, 133, 152
- reduction to absurdity, 37
- regular language, 358
- relation
  - binary, 163, 168
  - Euclidean, 292, 298
  - functional, 292
  - linear, 292
  - reflexive, 292
    - as formula, 121
  - serial, 292, 302
  - symmetric, 292, 301
    - as formula, 121
  - total, 292, 301
  - transition, 168
  - transitive, 292, 295
    - as formula, 121
- relational mu-calculus
  - explicit substitution, 376
  - fixed-point operators, 378
- restriction, 351
- root of a parse tree, 155
- rule
  - derived, 36
  - hybrid, 19
- safety property, 181, 183, 204
- satisfaction
  - in a frame, 294
  - in a frame for KT45<sup>n</sup>, 312
- satisfaction relation
  - for relational mu-calculus, 376
  - for basic modal logic, 278
  - for CTL, 169
  - for KT45, 311
  - for LTL, 209
  - for partial correctness, 238
  - for predicate logic, 145
  - for relational mu-calculus, 377
  - for total correctness, 238
- satisfiability, 332
  - 3SAT, 363
  - deciding, 94
    - of a predicate logic formula, 148
    - of a propositional logic formula, 59
    - undecidability of predicate logic, 156
- SCC
  - fair, 207
- scheduler
  - fair, 199
- scope
  - of a dummy variable, 131
  - of a variable, 114, 115, 127
  - of an assumption, 40, 127, 302

- search space, 127, 153
- semantic entailment
  - for basic modal logic, 281
  - for KT45, 300
  - for normal modal logics, 301
  - for predicate logic, 103
  - for propositional logic, 66
  - for relational mu-calculus, 380
- semantic equivalence, 56
- semantics
  - of  $\mu Z.f$ , 378
  - of  $\nu Z.f$ , 378
  - of basic modal logic, 278
  - of boolean quantification, 377
  - of CTL, 168
  - of EG, 217
  - of equality, 150
  - of predicate logic, 139
  - of propositional logic, 57
  - of relational mu-calculus, 377
  - of Until, 174
- sentence
  - atomic, 12
  - components, 100
  - declarative, 100
  - in predicate logic, 145
- sequent, 14
  - invalid, 76
  - unsound, 130
- Shannon expansion, 351
- side condition, 120, 123
- Sifakis, J., 227
- SMV, 166, 227
  - main program for ABP, 204
  - module, 195
    - receiver**, 203
    - sender**, 202
    - for channel, 203
    - instantiation, 195
  - process, 373
- program
  - example, 194
  - for Mutex, 197
- specification, 194
- soundness
  - of forall-elimination, 122
  - of natural deduction
    - basic modal logic, 306
    - predicate logic, 103, 139
    - propositional logic, 65
  - of program logics, 240
  - of proof rule for while-statements, 258
  - of the substitution principle, 121
- SPEC, 194, 202
- specification
  - as CTL formula, 193
  - for ABP, 204
  - formal, 231
  - informal, 231
  - language, 160
  - of a predicate, 111
- patterns, 227
- practical pattern, 177
- symmetric, 183
- truth table, 83
- Spin, 227
- state
  - critical, 182
  - explosion, 190, 191
  - explosion problem, 227
  - fair, 386
  - formula, 211
  - global, 182
  - graph, 171
  - initial, 183, 184, 193, 205, 236
  - non-critical, 182
  - of a system, 242
  - reachable, 205
  - resulting, 235, 236
  - space, 191
  - splitting states, 183
  - transition, 163
  - trying, 182
- storage
  - location, 265
  - state, 233
- string, 167, 275
  - binary, 142, 153
  - empty, 142
- strongly connected component, 188
- structural induction, 63, 72
- substitution
  - in predicate logic, 116
  - instance, 294
  - instance of tautology, 283
  - principle, 120
- symbolic model checking, 365
- symbolic model verifier, 193
- syntactic
  - category, 85, 98
  - domain, 232, 233
- syntax
  - of basic modal logic, 275
  - of boolean expressions, 233
  - of boolean formulas, 333
  - of CTI, 164
  - of CTL\*, 211
  - of Horn formulas, 98
  - of KT45<sup>n</sup>, 310
  - of literals, 85
  - of LTL, 208
  - of predicate logic, 109
  - of propositional logic, 48
  - of relational mu-calculus, 376
  - of terms, 107
- system
  - asynchronous, 227
  - interleaving model, 374
  - simultaneous model, 374
- axiomatic, 99
- commercial-critical, 160, 229
- component, 204

- concurrent, 161
- debugging, 162
- description, 195
- design, 162
- development, 161
- elevator, 177, 214
- finite-state, 228
- hybrid, 250
- infinite-state, 228
- mission-critical, 160
- multi-agent, 306
- physical, 163
- reactive, 161, 229, 330
- safety-critical, 160, 229
- transition, 162
- verification, 228
  
- tautology, 71
- temporal connective
  - AF, 170
  - AG, 170
  - AU, 170
  - AX, 169
  - EF, 170
  - EG, 170
  - EU, 170
  - EX, 170
- temporal connectives, 164
- temporal logic, 162, 274
- term, 106
  - interpretation, 145
- term-rewriting system, 158
- termination
  - proof, 238
- tertium non datur, 37
- theorem, 23
  - prover, 118, 157
  - proving, 158
- time
  - continuous, 162
  - discrete, 162
- top, 32
- total correctness, 238
- transition relation, 168
  - for SMV programs, 372
- transition system, 162
  - of ABP program, 205
  - of Mutex code, 200
  - of SMV program, 194
  - unwinding, 171, 185
- translation
  - English into predicate logic, 102, 109
- tree, 242
  - infinite, 171
- truth
  - dynamic, 162
  - mode, 274, 276
  - of knowledge, 298
  - static, 162
  - value
    - for predicate logic, 144
- for propositional logic, 11
- truth table
  - for conjunction, 55
- truth tables, 57
- type, 21, 299
  - checking, 22
  - theory, 158
  
- unary connective, 275
- undecidability
  - of provability, 157
  - of satisfiability, 156
  - of validity in predicate logic, 153
- universal quantification, 241
- universal quantifier, 179
- universe of concrete values, 142
- unsound sequent, 158
- Until, 174
  - in natural language, 174
  - negating, 209
  - weak, 213
- updated valuation, 377
  
- validity
  - in basic modal logic, 282
  - in  $KT45^n$ , 313
  - in propositional logic, 59
  - undecidability in predicate logic, 153
- valuation
  - in predicate logic, 140
  - in propositional logic, 57
  - in relational mu-calculus, 376
- value
  - initial, 204, 241, 242
- variable, 101, 163, 232
  - boolean, 190, 205, 330
  - bound, 114
  - capture, 117
  - dummy, 123
  - free, 114
  - local, 235
  - logical, 241, 267
- variable ordering
  - compatible, 342
  - list, 341
- variant, 270
- verification
  - full, 161
  - method, 160
  - of communication protocols, 163
  - of hardware, 163
  - of software, 163
  - of systems, 228
  - post-development, 161, 229
  - pre-development, 161, 229
  - process, 244
  - program, 243
  - property, 161
  - property-oriented, 228
  - semi-automatic, 228
  - techniques, 160

- weak Until, 213
  - in CTL, 214
  - in CTL\*, 214
  - in LTL, 214
- weakest precondition, 249
- while-statement, 233, 234
  - body, 246, 258, 261
  - non-termination, 270
- wise men puzzle, 317
- word
  - empty, 142
- world
  - possible, 277, 311
  - related, 277
- year 2000 problem, 230

## Bibliography

- [Ake78] S. B. Akers. Binary decision diagrams. *IEEE Transactions on Computers*, C-27(6):509–516, 1978.
- [AO91] K. R. Apt and E.-R. Olderog. *Verification of Sequential and Concurrent Programs*. Springer-Verlag, 1991.
- [Bac86] R. C. Backhouse. *Program Construction and Verification*. Prentice Hall, 1986.
- [BCM<sup>+</sup>90] J. R. Burch, J. M. Clarke, K. L. McMillan, D. L. Dill, and J. Hwang. Symbolic model checking:  $10^{20}$  states and beyond. In *IEEE Symposium on Logic in Computer Science*. IEEE Computer Society Press, 1990.
- [BEKV94] K. Broda, S. Eisenbach, H. Khoshnevisan, and S. Vickers. *Reasoned Programming*. Prentice Hall, 1994.
- [BJ80] G. Boolos and R. Jeffrey. *Computability and Logic*. Cambridge University Press, 2nd edition, 1980.
- [Boo54] George Boole. *An Investigation of the Laws of Thought*. Dover, New York, NY, USA, 1854.
- [Bra91] J. C. Bradfield. *Verifying Temporal Properties of Systems*. Birkhaeuser, Boston, Mass., 1991.
- [Bry86] R. E. Bryant. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Compilers*, C-35(8), 1986.
- [Bry91] R. E. Bryant. On the Complexity of VLSI Implementations and Graph Representations of Boolean Functions with Applications to Integer Multiplication. *IEEE Transactions on Computers*, 40(2):205–213, February 1991.
- [Bry92] R. E. Bryant. Symbolic Boolean Manipulation with Ordered Binary-decision Diagrams. *ACM Computing Surveys*, 24(3):293–318, September 1992.
- [CE81] E. M. Clarke and E. A. Emerson. Synthesis of synchronization skeletons for branching time temporal logic. In D. Kozen, editor, *Logic of Programs Workshop*, number 131 in LNCS. Springer Verlag, 1981.
- [CGL93] E. Clarke, O. Grumberg, and D. Long. Verification tools for finite-state concurrent systems. In *A Decade of Concurrency*, number 803 in Lecture Notes in Computer Science, pages 124–175. Springer Verlag, 1993.
- [CGL94] E. M. Clarke, O. Grumberg, and D. E. Long. Model checking and Abstraction. *ACM Transactions on Programming Languages and Systems*, 16(5):1512–1542, September 1994.

- [Che80] B. F. Chellas. *Modal Logic – an Introduction*. Cambridge University Press, 1980.
- [Dam96] D. R. Dams. *Abstract Interpretation and Partition Refinement for Model Checking*. PhD thesis, Institute for Programming research and Algorithmics. Eindhoven University of Technology, July 1996.
- [Dij76] E. W. Dijkstra. *A Discipline of Programming*. Prentice Hall, 1976.
- [DP96] R. Davies and F. Pfenning. A Modal Analysis of Staged Computation. In *23rd Annual ACM Symposium on Principles of Programming Languages*. ACM Press, January 1996.
- [EN94] R. Elmasri and S. B. Navathe. *Fundamentals of Database Systems*. Benjamin/Cummings, 1994.
- [FHMV95] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about Knowledge*. MIT Press, Cambridge, 1995.
- [Fit93] M. Fitting. Basic modal logic. In D. Gabbay, C. Hogger, and J. Robinson, editors, *Handbook of Logic in Artificial Intelligence and Logic Programming*, volume 1. Oxford University Press, 1993.
- [Fit96] M. Fitting. *First-Order Logic and Automated Theorem Proving*. Springer, 2nd edition, 1996.
- [Fra92] N. Francez. *Program Verification*. Addison-Wesley, 1992.
- [Fre03] G. Frege. *Grundgesetze der Arithmetik, begriffsschriftlich abgeleitet*. 1903. Vol. I and II (Jena).
- [Gal87] J. H. Gallier. *Logic for Computer Science*. John Wiley, 1987.
- [Gen69] G. Gentzen. Investigations into logical deduction. In M. E. Szabo, editor, *The Collected Papers of Gerhard Gentzen*, chapter 3, pages 68–129. North-Holland Publishing Company, 1969.
- [Gol87] R. Goldblatt. *Logics of Time and Computation*. CSLI Lecture Notes, 1987.
- [Gri82] D. Gries. A note on a standard strategy for developing loop invariants and loops. *Science of Computer Programming*, 2:207–214, 1982.
- [Ham78] A. G. Hamilton. *Logic for Mathematicians*. Cambridge University Press, 1978.
- [Hoa69] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12:576–580, 1969.
- [Hod77] W. Hodges. *Logic*. Penguin Books, 1977.
- [Hod83] W. Hodges. Elementary predicate logic. In D. Gabbay and F. Guenther, editors, *Handbook of Philosophical Logic*, volume 1. Dordrecht: D. Reidel, 1983.
- [Hol90] G. Holzmann. *Design and Validation of Computer Protocols*. Prentice Hall, 1990.
- [Koz83] D. Kozen. Results on the propositional mu-calculus. *Theoretical Computer Science*, 27:333–354, 1983.
- [Lee59] C. Y. Lee. Representation of switching circuits by binary-decision programs. *Bell System Technical Journal*, 38:985–999, 1959.
- [Lon83] D. E. Long. *Model Checking, Abstraction, and Compositional Verification*. PhD thesis, School of Computer Science, Carnegie Mellon University, July 1983.
- [McM93] K. L. McMillan. *Symbolic Model Checking*. Kluwer Academic Publishers, 1993.
- [MP91] Z. Manna and A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems: Specification*. Springer-Verlag, 1991.

- [MP95] Z. Manna and A. Pnueli. *Temporal Verification of Reactive Systems: Safety*. Springer-Verlag, 1995.
- [MvdH95] J.-J. Ch. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science*, volume 41 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1995.
- [Pap94] C. H. Papadimitriou. *Computational Complexity*. Addison Wesley, 1994.
- [Pau91] L.C. Paulson. *ML for the Working Programmer*. Cambridge University Press, 1991.
- [Pnu81] A. Pnueli. A temporal logic of programs. *Theoretical Computer Science*, 13:45–60, 1981.
- [Pop94] S. Popkorn. *First Steps in Modal Logic*. Cambridge University Press, 1994.
- [Pra65] D. Prawitz. *Natural Deduction: A Proof-Theoretical Study*. Almqvist & Wiksell, 1965.
- [QS81] J. P. Quielle and J. Sifakis. Specification and verification of concurrent systems in cesar. In *Proceedings of the fifth International Symposium on Programming*, 1981.
- [Ros97] A. W. Roscoe. *The Theory and Practice of Concurrency*. Prentice Hall, 1997.
- [SA91] V. Sperschneider and G. Antoniou. *Logic, A Foundation for Computer Science*. Addison Wesley, 1991.
- [Sch92] U. Schoening. *Logik Für Informatiker*. B.I. Wissenschaftsverlag, 1992.
- [Sch94] D. A. Schmidt. *The Structure of Typed Programming Languages*. Foundations of Computing. The MIT Press, 1994.
- [Sim94] A. K. Simpson. *The Proof Theory and Semantics of Intuitionistic Modal Logic*. PhD thesis, The University of Edinburgh, Department of Computer Science, 1994.
- [Tay98] R. G. Taylor. *Models Of Computation and Formal Languages*. Oxford University Press, 1998.
- [Ten91] R. D. Tennent. *Semantics of Programming Languages*. Prentice Hall, 1991.
- [Tur91] R. Turner. *Constructive Foundations for Functional Languages*. McGraw Hill, 1991.
- [vD89] D. van Dalen. *Logic and Structure*. Universitext. Springer-Verlag, 3rd edition, 1989.
- [Wei98] M. A. Weiss. *Data Structures and Problem Solving Using Java*. Addison-Wesley, 1998.