J Logic Lang Inf
DOI 10.1007/s10849-006-9017-y

BOOK REVIEW

Book review

Valentin Goranko

Logic in Computer Science: Modelling and Reasoning About Systems (2nd edition), Michael Huth and Mark Ryan (eds.), Cambridge: Cambridge University Press, 2004. Price: £30.00 (US$55.00), xiv + 427 pages, Paperback, ISBN: 0-521-54310-X.

The book consists of 6 chapters, a short bibliography (about 3 pages) and a subject index. Each chapter ends with many exercises and brief bibliographic notes.

Chapter 1 is an introduction to *propositional logic*. It first presents in detail a system of natural deduction, and only then it introduces the formal syntax and semantics of propositional logic. This peculiarity of the order of exposition, partly repeated in Chapter 2, is in my view the most controversial feature of the book, as it can create in the reader with little or no prior experience in logic (to whom the book is clearly addressed) the wrong impression that logical semantics is mainly used to give meaning to deductive systems, rather than that deductive systems are designed in order to capture logical validity and consequence.

On a minor note, I find the terminology 'well-founded formulas', adopted in the book, somewhat obsolete (though still in use) and certainly redundant, since no other kinds of 'formulae' are ever introduced. Another minor remark refers to the section on induction (1.4.2, p. 40 and further): I wonder why the authors do not introduce structural induction on formulae, derivations etc., but rather reduce all these to induction on natural numbers. While mathematically correct, this approach somehow obscures the concepts of definitions and proofs by structural induction, so deeply permeating logic and computer science.

Further in Chapter 1 the authors explain and prove the soundness and completeness of the earlier introduced system of natural deduction (*not* of the propositional logic itself, as the subsection titles suggest). The proof of completeness is not based on the best-known standard method of maximal theories, but essentially on provable reduction of a formula to a normal form determined by its truth-table. This proof is interesting, but somewhat long and very specific to classical propositional logic. Given that the emphasis of the book is on

V. Goranko
School of Mathematics, University of the Witwatersrand, Johannesburg, South Africa
e-mail: goranko@maths.wits.ac.za

applications of logic, rather than on theory, I am not convinced that including this (or, any other) completeness proof is really useful for the intended reader.

The chapter then discusses transformation of formulae to conjunctive normal forms and Horn clauses, and ends with an exposition of two satisfiability (SAT) solvers working on DAG representation of formulae, one running in linear-time but succeeding only on a fragment of the language, and another running in cubic time and covering a larger fragment.

Chapter 2 is an introduction to *first-order ('predicate') logic*. It begins with a discussion on first-order languages, introduces their formal syntax and the associated with it basic concepts of quantifier scope, free and bound variables, and substitutions. The authors then extend the system of propositional natural deduction with rules for the quantifiers, give several examples of derivations, and in particular, derive some important quantifier equivalences. As in the chapter on propositional logic, only then the formal semantics of predicate logic is introduced. Again, I see neither scientific, nor methodological merits in such order of the exposition, while the danger of confusion of the unexperienced reader is clear.

Section 2.5 proves the undecidability of the validity in first-order logic by reduction to the Post correspondence problem. The proof is elegant and instructive. Section 2.6 discusses some basic model-theoretic results characterizing the expressiveness of predicate logic, such as compactness. The section ends with a brief discussion of the existential and universal fragments of second-order logic. The last Section 2.7 in the chapter, entitled 'Micromodels of software', presents an application of predicate logic to modelling and verifying properties of software, by means of state transition systems called 'state machines', using the tool Alloy.

For some corrections and specific remarks on this chapter I refer the reader to the book's errata web page http://www.cs.bham.ac.uk/research/lics/.

Chapter 3 is devoted to *verification by model checking*. After a brief general discussion of the problem of verification of state transition systems, in Section 3.2 the authors present the linear time temporal logic LTL, as the most widely studied and used formalism for specification and verification of safety, liveness, and fairness properties of infinite computations in concurrent or reactive systems. After the formal presentation and theoretical discussion of LTL, in Section 3.3 the authors demonstrate its use for specification and verification of some important problems in the theory of concurrent and communicating processes, viz. the 'mutual exclusion' and the 'alternating bit' protocols, as well as the 'ferryman's problem' (aka the popular 'cabbage, goat, and wolf' puzzle), the practical verification of which they illustrate with the Open Source model checking tool NuSMV ('New Symbolic Model Verifier').

The chapter then continues with an exposition of the syntax and semantics of the branching time temporal logic CTL in Section 3.4. Both LTL and CTL are fragments of the very expressive but computationally expensive full branching time logic CTL*. While LTL is suited (and very expressive) for reasoning about a single computation, its rival CTL allows for quantification over all computations emerging from the current state, and is thus more adequate for global reasoning about the transition system, but with a syntactically restricted expressiveness resulting in better computational complexity than the full CTL*. Section 3.6 presents in detail a model-checking algorithm for CTL based on state-labelling and discusses the 'state explosion problem'. Then it outlines an automata-based model-checking algorithm for LTL and its implementation in NuSMV, tacitly assuming that the reader has the necessary background in automata theory. The chapter's utility would have gained if it had included a brief exposition of that background, as it clearly targets a more general and theoretically unexperienced audience.

Section 3.7 goes back to the formal semantics of CTL, discussing the fixed-point characterization of the temporal operators of CTL and the correctness of the respective model-checking clauses. In my view, this material should have appeared before, not after, the section on model checking CTL, as it bears the theoretical background for proper understanding of its semantics.

Chapter 4 is a good and clear classical exposition of the classical topic of *program verification*. It discusses partial and total correctness of programs, loop invariants, etc. and presents and illustrates the use of Hoare's calculus of preconditions and postconditions with some case studies.

Chapter 5, on *modal logics and agents* somehow steps aside of the main story developed in the book so far, viz. program verification. The bulk of this chapter is a standard background material on basic modal logic: syntax, Kripke semantics, validities and semantic equivalences in Section 5.2; a discussion of various interpretations of the modal operators (physical or logical necessity, temporality, obligation, belief, knowledge, program execution, etc.) and of some important formulae formalizing features of these, along with the associated properties of the accessibility relation, leading eventually to basic facts from correspondence theory in Section 5.3. Section 5.4 introduces a system of natural deduction for modal logic, extending the one for propositional logic with a new kind of boxes representing reasoning in any possible world accessible from the current one. Specific additional rules are given for the modal logic KT45, known as the basic modal logic for reasoning about an agent's knowledge. Accordingly, the many-dimensional extension KT45^n of this logic is discussed in Section 5.5 as the basic logic of knowledge of multi-agent systems, further extended with operators for common and distributed knowledge and used to formalize the 'three wise men' and 'the muddy children' puzzles.

Some of the terminology and definitions in this chapter are potentially confusing, and corrections have been made on the book's errata web page (see errata associated with pages 321–353).

Again, I find the order of exposition and arrangement of some topics somewhat puzzling: the authors introduce basics of modal logic two chapters after studying in detail LTL and CTL, which are two of its rather advanced species. On a more minor scale: the notion of 'Kripke model' is introduced on p. 309, while its component notion of 'frame' and validity in a frame are only introduced on p. 322.

Chapter 6 is devoted to *binary decision diagrams* (BDDs) – a very useful formalism for succinct representation and manipulation of Boolean functions, used in symbolic model checking. The chapter introduces BDDs and ordered BDDs (OBDDs), and methods for their optimization and reduction. In Section 6.2. the authors present algorithms for manipulation of Boolean functions represented by reduced OBDDs, and discusses their time complexity. Section 6.3 outlines the main ideas of symbolic model checking in state transition systems and briefly deals with synthesizing OBDDs and modelling sequential circuits with OBDDs. The chapter ends with a concise introduction to a 'relational mu-calculus', a fixpoint extension of the calculus of boolean functions with quantification over Boolean variables. The authors show how CTL can be encoded into that relational mu-calculus, and discuss symbolic model checking in it.

In summary, despite some shortcomings mentioned above, this is a nice and useful book, offering a good selection of topics on logic in computer science, without attempting comprehensive coverage of that field. Inevitably, many important relevant topics are not treated at all, e.g. relational databases, constraint satisfaction, descriptive complexity, etc. Of those which are covered, I find the more applied topics generally better presented than the theoretical ones. The detailed exposition, often on a beginner's level, and the numerous examples and

exercises at the end of each chapter make it a suitable textbook for a higher undergraduate or lower graduate course on logic in computer science, but I would advise the instructor to consider re-arrangement of the presentation of some of the content, in line with my remarks above. The book can also be successfully used by researchers and computer system developers who wish to enter the field.