

Preface

Motivation and Objectives

In control theory, complex models of physical processes, such as systems of differential or difference equations, are usually checked against simple specifications, such as stability and set invariance. In formal methods, rich specifications, such as languages and formulas of temporal logics, are checked against simple models of software programs and digital circuits, such as finite transition systems. With the development and integration of cyber-physical and safety-critical systems, there is an increasing need for computational tools for verification and control of complex systems from rich, temporal logic specifications. For example, in a persistent surveillance application, an unmanned aerial vehicle might be required to “take photos of areas A and B infinitely often while always avoiding unsafe areas C and D .” In the emergent area of synthetic biology, the goal is to design small gene networks from specifications that are naturally given as temporal logic statements about the concentrations of species of interest, e.g., “if inducer u_1 is low and inducer u_2 is high, then protein y should eventually be expressed and remain in this state for all future times.”

Central to the existing approaches for formal verification and control of infinite-state systems is the notion of abstraction. Roughly, an abstract model can be seen as a finite transition graph, whose states label equivalent sets of states of the original system, and whose transitions match the trajectories of the original system among the equivalence classes. Once constructed, such an abstraction can be used for verification (using off-the-shelf model checking tools) or control (using automata game techniques) in lieu of the original system.

The main objective of this book is to present formal verification and control algorithms for a class of discrete-time systems generically referred to as *linear*. Most of the results are formulated for piecewise linear (or affine) systems, which are described by a collection of linear (affine) dynamics associated to the regions of a polytopic partition of the state space. Such systems are quite general, as they have been shown to approximate nonlinear system with arbitrary accuracy. There also

exist computational tools for identifying such systems (both the polytopes and the corresponding dynamics) from experimental data.

This book is based on the work of the authors, and is, as a result, biased and non-comprehensive. The specifications are restricted to formulas of Linear Temporal Logic (LTL) and fragments of LTL, even though other temporal logics have been used by other authors. While some of the results can be extended to continuous-time systems, the focus is on discrete-time systems only. We only cover deterministic and purely non-deterministic systems, even though existing results, including ours, show that extensions to stochastic systems and probabilistic temporal logics are possible. The equivalence notion that we use is classical bisimulation—extensions to approximate bisimulations and probabilistic bisimulations have been developed recently.

Intended Audience

This book is intended to a broad audience of scientists and engineers with interest in formal methods and controls. In particular, it is our hope that this book will help bridge the gap between the computer science and control theory communities. Computer scientists are shown that simulations and bisimulations, normally used to reduce the size of finite models of computer programs, can be used to abstract infinite-state systems. The book also provides a self-contained exposition of temporal logic control for finite non-deterministic systems, which is useful even for seasoned formal methods researchers. Control theorists are introduced to notions such as abstractions, temporal logics, formal verification, and formal synthesis, and are shown that such techniques can be used for classical systems such as discrete-time linear systems.

Book Outline and Usage

This book is self-contained. While some level of mathematical maturity is expected, no mathematical background in control or automata theory is necessary. Most of the formal definitions and algorithms are explained in plain language and illustrated with several examples. Most examples include explanatory illustrations.

The book is organized in three parts. Part I covers the types of systems and specifications used throughout the rest of the book. Specifically, it introduces (non-deterministic) transition systems, a formalism that can be used to model a large spectrum of dynamical systems. Simulation and bisimulations relations and corresponding abstractions for transitions systems are defined. The syntax and semantics of Linear Temporal Logic (LTL) and one of its fragments, called syntactically co-safe LTL (scLTL), are introduced and illustrated with several

examples. Finite state automata, Büchi automata, and Rabin automata accepting languages satisfying LTL formulas are also defined.

Part II focuses on finite systems, i.e., transition systems with finitely many states, inputs, and observations. After reviewing the classical LTL model checking problem, we solve the problem of finding the largest set of states from which all trajectories of a system satisfy an LTL formula. We show that the control version of this problem can be mapped to a Büchi game, a Rabin game, or a graph reachability problem depending on the structure of the specification formula. We present ready to implement solutions to all these problems and include illustrative examples.

In Part III, which is the most involved part of the book, we bring together the concepts and techniques introduced in Parts I and II and present computational frameworks for verification and control of (infinite) discrete-time linear and piecewise affine systems from LTL specifications. We cover LTL verification problems for systems with fixed and uncertain parameters, parameter synthesis problems, and control synthesis problems. We also provide algorithms for the construction of finite bisimulations for some classes of discrete-time linear systems. Finally, we establish a connection between optimality and correctness by requiring a linear system to satisfy a temporal logic correctness requirement while optimizing a cost function.

This book can be read and used in two ways. First, by covering Parts I and II (excluding Sect. 1.2 from Chap. 1 in Part I), it can be used as a stand-alone introduction to verification and control for finite non-deterministic transition systems from LTL formulas. This can be used as a first mini-course on formal methods for engineers and computer scientists. It can also be useful for formal methods researchers who have expertise in verification only. Second, the whole book can be used as a graduate level course on formal methods for dynamical systems, with particular focus on discrete-time linear and piecewise affine systems. Most of the algorithms presented in this book were implemented as user-friendly software packages that can be downloaded from the first author's webpage or can be provided on request.

Related Books

The related books on formal methods for dynamical systems are [123, 5, 162, 144]: [123, 5] are comprehensive expositions of theory and practice of embedded and cyber-physical systems, together with corresponding verification and synthesis techniques; [162, 144] are research monographs on formal methods for hybrid systems, which combine continuous and discrete dynamics. The focus in [144] is on theorem proving. The closest related to this book is [162].

There are three main features that set this book apart from [123, 5, 162, 144]. First, we provide a complete and self-contained treatment of the formal synthesis problem from specifications given as LTL formulas. This can be, for example, combined with the partition-based abstraction method from [162] to implement a

computational tool for LTL synthesis for a quite large class of dynamical systems. Second, we focus on particular types of dynamical systems (i.e., discrete-time piecewise affine systems) and exploit their geometry to efficiently construct abstractions. Third, we explore the connection between optimality and correctness in control.

Acknowledgements

It is a great pleasure to acknowledge George J. Pappas, Rajeev Alur, and Vijay Kumar (all from the University of Pennsylvania), who fostered the interest of the first author in this topic early in his career. Jana Tumova, Ivana Cerna, and Jiri Barnat from Masaryk University contributed to the results presented in Chap. 9. Mircea Lazar from the Technical University of Eindhoven was a collaborator for the work described in Chaps. 10–12. The authors are grateful to support from the National Science Foundation (NSF), the Air Force Office of Scientific Research (AFOSR), the Office of Naval Research (ONR), and the Army Research Office (ARO). The first author would particularly like to thank Helen Gill, Fariba Fahroo, and Marc Steinberg for their enthusiastic support over the past several years.

Finally, we would like to thank our numerous colleagues and friends who provided comments and suggestions on earlier versions of the manuscript. In particular, we would like to thank Ezio Bartocci, Sam Coogan, Mircea Lazar, Rupak Majumdar, Necmiye Ozay, Giordano Pola, Vasumathi Raman, Paulo Tabuada, and Jana Tumova.

Boston, MA, USA
Cambridge, UK
Ankara, Turkey

Calin Belta
Boyan Yordanov
Ebru Aydin Gol

Formal Methods for Discrete-Time Dynamical Systems

Belta, C.; Yordanov, B.; GÖL, E.

2017, XVIII, 284 p. 93 illus., 39 illus. in color., Hardcover

ISBN: 978-3-319-50762-0