Automated Formal Synthesis of Digital Controllers for State-Space Physical Plants*

Alessandro Abate[1], Iury Bessa[2], Dario Cattaruzza[1], Lucas Cordeiro[1,2], Cristina David[1], Pascal Kesseli[1], Daniel Kroening[1], and Elizabeth Polgreen[1]

[1] University of Oxford, UK
[2] Federal University of Amazonas, Manaus, Brazil

Abstract. We present a sound and automated approach to synthesize safe digital feedback controllers for physical plants represented as linear, time-invariant models. Models are given as dynamical equations with inputs, evolving over a continuous state space and accounting for errors due to the digitization of signals by the controller. Our counterexample guided inductive synthesis (CEGIS) approach has two phases: We synthesize a static feedback controller that stabilizes the system but that may not be safe for all initial conditions. Safety is then verified either via BMC or abstract acceleration; if the verification step fails, a counterexample is provided to the synthesis engine and the process iterates until a safe controller is obtained. We demonstrate the practical value of this approach by automatically synthesizing safe controllers for intricate physical plant models from the digital control literature.

1 Introduction

Linear Time Invariant (LTI) models represent a broad class of dynamical systems with significant impact in numerous application areas such as life sciences, robotics, and engineering [2, 11]. The synthesis of controllers for LTI models is well understood, however the use of digital control architectures adds new challenges due to the effects of finite-precision arithmetic, time discretization, and quantization noise, which is typically introduced by Analogue-to-Digital (ADC) and Digital-to-Analogue (DAC) conversion. While research on digital control is well developed [2], automated and sound control synthesis is challenging, particularly when the synthesis objective goes beyond classical stability. There are recent methods for verifying reachability properties of a given controller [13]. However, these methods have not been generalized to control synthesis. Note that a synthesis algorithm that guarantees stability does not ensure safety: the system might transitively visit an unsafe state resulting in unrecoverable failure.

We propose a novel algorithm for the synthesis of control algorithms for LTI models that are guaranteed to be safe, considering both the continuous dynamics of the plant and the finite-precision discrete dynamics of the controller,

* Supported by EPSRC grant EP/J012564/1, ERC project 280053 (CPROVER) and the H2020 FET OPEN 712689 SC^2.