Reachability in Cyber-Physical Systems

Maria Prandini

Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milan, Italy
maria.prandini@polimi.it

Reachability analysis consists in determining the region of the state space that a given dynamical system will visit starting from some set of initial states, subject to a disturbance input modeling uncertainty in the system dynamics and/or the fact that the system is operating in an uncertain environment that can affect its evolution.

A main application of reachability analysis – that makes it relevant to various application domains – is the automatic verification of the correct behavior of a system, which is typically coded by requiring that all its trajectories remain within some desired range of operation and do not enter any forbidden region of the state space. If the outcome of the verification is negative, then, the system has to be redesigned. The availability of some counter-example showing a violation of the correct behavior can be useful to this purpose.

In reachability analysis, the region of the state space that is visited by the system during its evolution is determined by propagating the set of initial states through the uncertain system dynamics, thus computing the so-call reach sets.

The main issue in reachability analysis is indeed the ability to compute with sets. In systems with a finite state space, sets can be represented by enumeration and reach sets can be computed starting from the given initial set and progressively adding one-step successors. If we consider systems involving a continuous state space, then, representation and propagation of reach sets generally become a challenge. One should in fact choose a class of sets that can be efficiently represented and such that, when one applies to these sets the operations involved in their propagation through the system dynamics, then, sets in the same class are obtained. If this is not possible, some outer-approximation of the obtained sets should be adopted to bring their description back to the same class.

Scalability of reach set computations arises as an issue, and calls for abstraction of models through simulation or approximate simulation relations. In the case of a simulation relation, the abstracted model can be used for verifying the correct behavior of the original system since all trajectories of the original system can be generated by simulating the abstracted model (but not vice-versa). For instance, a nonlinear continuous system with smooth dynamics can be reduced to a piecewise affine system that satisfies a simulation relation if the abstraction procedure appropriately accounts for the modeling error through a (fictitious) disturbance input.

We shall consider reachability analysis for cyber-physical systems that represent engineering systems where communication, computation, and control (the cyber part)

Supported by the European Commission under the project UnCoVerCPS with grant number 643921.

are integrated within natural and/or human-made systems (the physical part) governed by the laws of physics. Hybrid models are used to describe this class of systems, since the interleaved discrete and continuous state components of a hybrid model can represent the cyber and physical parts integrated in a cyber-physical system.

Reachability analysis of hybrid systems is challenging since their hybrid state has a continuous component and the propagation of the reach sets in the continuous state space depends on the value taken by the hybrid state. Typically, a reach set in the continuous state space can split in subsets that propagate according to different continuous dynamics, thus growing the effort in reach set computations.

In this invited talk, we shall focus on discrete time piecewise affine systems, which often arise as a model for cyber-physical systems and have also some potential as a unifying modeling framework for automatic verification of nonlinear continuous systems. More specifically, we address verification of discrete time piecewise affine systems based on reach set computations, including the generation of counter-examples, and the use of abstraction and invariant sets to improve scalability. We also address the case when a control input is available to impose the correct system behavior via disturbance compensation, and describe a set-based approach to feedback control design integrating reach set computations.