

Games for Formal Design and Analysis of Reactive Systems

Rajeev Alur

University of Pennsylvania

<http://www.cis.upenn.edu/~alur/>

With recent advances in algorithms for state-space traversal and in techniques for automatic abstraction of source code, model checking has emerged as a key tool for analyzing and debugging software systems. This talk discusses the role of games in modeling and analysis of software systems.

Games are useful in modeling open systems where the distinction among the choices controlled by different components is made explicit. We first describe the model checker Mocha that supports a game-based temporal logic for writing requirements, and its applications to analysis of multi-party security protocols. Then, we describe how to automatically extract dynamic interfaces for Java classes using predicate abstraction for extracting a boolean model from a class file, and learning algorithms for constructing the most general strategy for invoking the methods of the model. We discuss an implementation in the tool JIST---Java Interface Synthesis Tool, and demonstrate that the tool can construct interfaces, accurately and efficiently, for sample Java2SDK library classes.

We will conclude with a discussion of how game-based analysis can be used to synthesize systems from their specifications.