Symbolic timing analysis for the verification of asynchronous circuits

Robert Clarisó  Jordi Cortadella
Universitat Politècnica de Catalunya, Barcelona, Spain

Timing analysis can be used to detect hazards in an asynchronous circuit for a given set of delays of gates and environment events. However, this analysis provides little or no information about the existence of hazards for other delay values. The goal of the work to be presented is to perform symbolic timing analysis of asynchronous circuits, i.e. some or all the delays of the gates and environment events are symbols. With this analysis, a restriction on the symbolic delays that is sufficient to ensure the absence of hazards can be discovered automatically.

There has been other work on symbolic timing analysis, such as the work of Amon and Hulgaard on time separation of events. The proposed approach is used for a different problem, the verification of hazards, and uses complete different techniques from the domain of abstract interpretation.

The overall flow of the algorithm can be divided in the following step:

1. **Construction of a timed transition system**: The implementation and specification of the asynchronous circuit are modeled as a timed transition system, where some lower and upper bound delays for events are symbols instead of constants.

2. **Detection of hazards**: In this formalism, a hazard can be modeled as a transition that disables another transition which was previously enabled. Each transition corresponds to the firing of an event.

3. **Timing analysis**: The timing analysis algorithm of the timed transition system relies on abstract interpretation analysis, a family of static analysis techniques which relies on expressing the state of a system as a system of equations that are solved approximately with fixed point techniques. In our problem, this approximate analysis computes a conservative upper approximation of the set of valid assignments to clock values and symbolic delays in each state of the timed transition system. This “set of valid assignments” can be approximated as “the assignments that satisfy a system of linear inequalities on the values of clocks and symbolic delays” with a convex polyhedron.

4. **Building the property that ensures the absence of hazards**: The result of the timing analysis can be seen as the system of inequalities satisfied in each state and transition of the timed transition system, and specifically, in all hazard transitions. By combining the inequalities that are satisfied in the hazard transitions, we can discover linear restrictions on the values of symbolic delays that are sufficient to make all hazards transitions unreachable.

Experimental results show that small circuits can be analyzed with this algorithm within reasonable CPU time and memory limits. The examples that have been tested contain more than 10 symbolic delays.