Abstract: We present our work on developing efficient algorithms related to the formal analysis of infinite state reactive systems. Our research focus is the discovery and implementation of decision procedures that can provide a formal proof regarding the realizability of the given specification, as well as the extension of these procedures to enable synthesis of correct-by-construction witnesses. Contrary to the traditional view of a witness as a solution with deterministic behavior, we strive for synthesis algorithms that allow more general solutions through nondeterministic designs.

Reactive System: Maintains an ongoing interaction with environment
- Systems are defined in terms of inputs i and states s.
- A symbolic transition system is defined as: (I, T)
  - Initial states allowed by I
  - Transitions allowed by T
- A contract is a pair (A, G) with
  - Assumptions: A: (state x input) → bool
  - Guarantees: G_I: state → bool, G_T: (state x input x state) → bool

Synthesis of Infinite State Reactive Systems

Validity-Guided Reactive Synthesis

Validity-Guided Reactive Synthesis

Achieving Synthesis of Nondeterministic Designs

Applications of Nondeterministic Reactive Systems