Summary of Changes to mr

Srinivas Nedunuri

August 28, 2025

The current mr V2 code (which was an extension of mr V1 to handle multi-node models) has been modified in a number of ways so as to accommodate the constraints of some newer examples.

Previous (V1) Formulation

Define a formula, the *weakest controllable predecessor* (*wcp*) as a predicate transformer:

$$wcp \equiv \forall e \cdot E(s,e,u) \rightarrow L(f_a(s,e,u)) \tag{1}$$

That is, *wcp* is the weakest formula characterizing those states s and control values u such that for any adversary input e conforming to some condition E, the transition a is assured to reach a state as defined by plant dynamics f_a satisfying the state invariant L. The formula characterizes those system states from which the system transitions to a legal state regardless of the adversary input. Then, the control predicate $U(s,u)$ on any given arc in state s must ensure the wcp:

$$U_a(s,u) \rightarrow wcp \tag{2}$$

Finally, to close the loop, the invariant L characterizes those states from which for some arc a there is a control value that satisfies the control predicate on the arc. Define

$$someGuard \equiv \bigvee \exists u \cdot U_a(s,u) \tag{3}$$

Then it is required that:

$$L(s) \rightarrow someGuard$$

Current (V2) Formulation

The guard is not explicitly computed. Instead *wcp* is computed as

$$\exists u \cdot U_a(s,u) \wedge \forall e \cdot E(s,e,u) \rightarrow L(f_a(s,e,u))$$

and

$$L(s) \rightarrow wcp$$

In place of a guard, when the model refinement has terminated, a deterministic control function that selects a control value is synthesized ("*generateControlStrategyByCases*"). Note also that there is no disjunction of all the arc conditions out of a node. Rather the invariant is strengthened for each arc in turn, implying a conjunction of all the arc conditions. This seems overly strong.

Changes (V3)

1. The first change is that the explicit computation of the guard and the guard disjunction has been reinstated. This is because there are problems for which a guard and not a control function is specifically required. An example is shield synthesis for reinforcement learning agents, in which an agent proposes an action (control value) and the shield checks it by evaluating the guard.

2. The second change is to handle situations in which the system is allowed to react to the choices of the environment. In the current formulation given above, the choice of control value has to work for all choices of the environment that satisfy the env predicate E. The revised formulation is as follows: The guard U_a of an arc a must ensure that for a given starting state and environment input, the state at the target satisfies the node invariant L:

$$U_a(s, e, u) \rightarrow L(f_a(s, e, u))$$

Then regardless of environment input e (subject again to the environmental constraint E) at least one of the guards must hold i.e. some arc out of the node is enabled. That is,

$$\forall e \cdot E(s, e) \rightarrow \bigvee_a \exists u \cdot U_a(s, e, u)$$

or, equivalently,

$$\bigvee_a (\forall e \cdot E(s, e) \rightarrow \exists u \cdot U_a(s, e, u))$$

which is referred to as *someGuard.* Compare this with (3). Then, as before, the following must hold:

$$L(s) \rightarrow someGuard$$

The synthesis algorithm is told which situation holds by a boolean flag on the model called "DOING_FORALL_EXISTS"