

Tamarin prover basics: Dependency Graphs



Green rectangular boxes represent rule instances. For a rule LHS \rightarrow ACT \rightarrow RHS, the top line represents the LHS, the middle line the ACT, and the bottom line the RHS.

Red arrows show the adversary learning a term from the network (through an Out fact)

The actions line also shows the concrete timepoint variable (here $\#vr.2$) of this rule instance and the rule name ($A1$) with the set of actions (if any).

Ellipses represent adversary actions (knowledge derivation, sending, etc.)

(Technical internals:
 isend : adversary sending message to 'In' fact.
 !KU : terms used during construction path
 coerce : start of construction path (after possible deconstruction path))

Black arrows denote where a produced fact is consumed by another rule.

Grey arrows show where a persistent fact/adversary knowledge is used by another rule.

Dotted arrows indicate temporal ordering, i.e., precedence.

Slightly different shades of green are used to distinguish between instances of different rules. Users can also choose to specify the color for each rule if they want to.

Grey ellipses indicate where the adversary chooses a term (here $t1$); !KU is a specific case of K , i.e., learning a term.

time

