The complexity of automated addition of fault-tolerance without explicit legitimate states.


Summary: Existing algorithms for automated model repair for adding fault-tolerance to fault-intolerant models incur an impediment that designers have to identify the set of legitimate states of the original model. This set determines states from where the original model meets its specification in the absence of faults. Experience suggests that of the inputs required for model repair, identifying such legitimate states is the most difficult. In this paper, we consider the problem of automated model repair for adding fault-tolerance where legitimate states are not explicitly given as input. We show that without this input, in some instances, the complexity of model repair increases substantially (from polynomial-time to NP-complete). In spite of this increase, we find that this formulation is relatively complete; i.e., if it was possible to perform model repair with explicit legitimate states, then it is also possible to do so without the explicit identification of the legitimate states. Finally, we show that if the problem of model repair can be solved with explicit legitimate states, then the increased cost of solving it without explicit legitimate states is very small. In summary, the results in this paper identify instances of automated addition of fault-tolerance, where the explicit knowledge of legitimate state is beneficial and where it is not very crucial.

Keywords: model repair; program synthesis; fault-tolerance; automated formal methods
doi:10.1007/s00446-014-0227-2