Model checking of component connectors

Izadi, M.

9 Conclusions and Future Work

In this chapter, we conclude the presentation of our work in this thesis, summarize its results, and list topics for our future work.

9.1 Results and Conclusions

In this thesis, we presented a framework for automata theoretic model checking of coordination systems specified in Reo. As an operational modeling formalism that covers several intended behaviors of Reo connectors, such as fairness, I/O synchronization, and context dependency, we introduced Büchi automata of records (BAR) and their augmented version (ABAR). We showed that every constraint automaton (the first introduced operational semantics for Reo) can be translated into an essentially equivalent BAR. However, there are some Reo connectors whose behavior can be expressed in BAR or ABAR, but not in constraint automata.

To specify the properties to be verified, we introduced an action based linear temporal logic called ρ-LTL, interpreted over the executions of augmented Büchi automata of records. We showed how ρ-LTL formulas can be translated into their equivalent ABARs. The translation can be done inductively or using an on-the-fly method.

To deal with large state spaces, we showed that ABARs can be implemented using ordered binary decision diagrams (OBDD) as dense data structures. We described the implementation and case studies to show the applicability of our method to large state spaces.

We also showed that the state explosion problem can be tackled by a form of compositional minimization using some suitable equivalence relations. To this end, we proved that two failure based equivalence relations, called CFFD and NDFD, are congruence relations with respect to the join and hiding operators of constraint automata. These congruency results, together with the fact that CFFD and NDFD equivalences are minimal and preserve linear time temporal logic properties can be used for compositional minimization of constraint automata models in model checking. We showed the application of this method to some practical case studies.

9.2 Future Work

To continue the research presented in this thesis, in this section we list a number of topics that can be considered as future work. On the theoretical side, the following problems can be considered:

- Introducing *timed* versions of BARs and ABARs to be able to model real-time constraints with Reo connectors.

- Based on the above suggestion, introducing a timed version of the temporal logic ρLTL and its model checking, both globally and on-the-fly.

- Introducing *probabilistic* versions of BARs and ABARs to be able to model connectors with inherently probabilistic behaviors.
- Based on the above suggestion, introducing a probabilistic version of the temporal logic ρLTL and its model checking, both globally and on-the-fly.
- Introducing action based *branching time* temporal logics for BAR and ABAR models.
- Based on the above suggestion, investigating the model checking of branching time properties of connectors modeled by BAR and ABAR.
- The branching time case can also be considered for timed BAR and ABAR and their model checking.
- The branching time case can also be considered for probabilistic BAR and ABAR and their model checking.
- The results of this thesis can be focused in particular for some more practical fields of software engineering such as *software quality measurement*, *service-oriented models* of software, and several other *non-functional* properties.
- Some other methods to deal with the state explosion problem seem to be very suitable for the case of Reo nets modeled by BAR and ABAR or by constraint automata. We suggest considering the methods of *abstraction*, *symmetry*, and *assume-guarantee based compositional reasoning*.
- The method of compositional minimization introduced in thesis was based on constraint automata. Using this method for BAR and ABAR models seems to be more realistic and achievable. This can be investigated in the future. To this end we need the following theoretical results:
  - Proving that the failure based equivalences CFFD and NDFD are congruences with respect to all composition operators of BARs and ABARs.
  - Proving that CFFD and NDFD preserve sets of linear temporal properties interpreted over BAR and ABAR models, and that they are the weakest congruences that satisfy the preservation of these properties.
  - Introducing minimization algorithms for BAR and ABAR models using CFFD and NDFD equivalences.

We intend to enhance our tool, especially by incorporating the global and on-the-fly translations of ρLTL formulas into augmented Büchi automata of records that we introduced in this thesis. Moreover, we plan to integrate our BDD-based model checker and our tool for compositional minimization of constraint automata in our tool set. Finally, we will integrate our tool set within the Extensible Coordination Tools [2] programming environment for Reo.