Atlanstic 2·0·2·0
Recherche, Formation & Innovation en PAYS de la LOIRE

Constraints in Parametric Sytems (CoPaS)

Nowadays, automata-based modeling and verification methods are mainly used in two different ways :

- **Designing Systems.** In order to design digital systems, formal models are built based on (mostly informal) specifications expressed by the end-user of these systems or obtained from the knowledge designers have of their environment. These abstract models are then incrementally refined until a sufficiently detailed model is produced, which can then be implemented. In this setting, formal verification is performed at several stages of development in order to guarantee that the intermediate models and the implemented product conform to the properties expressed in the specifications.

- **Understanding Systems.** Automata-based modeling and verification methods are also used in order to abstract existing (not necessarily software) systems that are too complex to be apprehended in their entirety. In this setting, researchers or engineers build models from observations of the existing system and perform verification in order to either show that the abstract model conforms to the system under study or to gain new information that allows to refine it until it does. Once an accurate model is obtained, verification is performed in order to study whether the system satisfies given properties.

One common trait that drives these two ways of using automata-based models is the need for abstraction : as more and more realistic aspects of the systems under study are taken into account in their models, the size of these models grows exponentially, which often renders their verification untractable.

Abstraction, which allows to reduce the size of the models, is thus a key point in broadening the applicability of such modelling and verification methods. Among the numerous ways of abstracting models, one can find the theory of parametric models, where certain aspects of interest of the systems are replaced with parameters, allowing the use of formal methods for e.g. synthesising the best value of these parameters with respect to some properties of interest. This area of research is still in its infancy and several research projects have been dedicated to developing new ways of integrating such parameters in existing abstract models and adapting existing formal verification techniques to this new setting.

The results of these projects seem promising and several new parametric models have been developed along with adapted verification techniques. Most of the time, using existing verification techniques for these new models allows to derive constraints over the parameter space which are then resolved by using “of the shelf”constraint solvers. Unfortunately, most “of the shelf” constraint solvers are very general and not necessarily adapted or optimized to this particular setting. As a consequence, existing formal methods and tools can only be applied to models of a reasonable size (a few thousand states) exhibiting very few parameters (2 to 3 parameters at most if using PROPHESY [1] - the state of the art parametric model checker for parametric probabilistic systems).

A concrete example from epidemiologics is the control of bovine tuberculosis spread [2]. In order to study this problem, researchers model bovine herds using probabilistic systems and use parameters in order to encode transmission rates within and between herds, as well as several aspects of control strategies. As far as we know, formal verification techniques have thus far been unable to handle this problem because of the size of the resulting models and the number of parameters involved. We therefore conjecture that developing, in close collaboration with the constraint community, new dedicated methods for parameter synthesis in the context of complex parametric systems would have a great impact on the applicability of formal methods in practice.

The aim of CoPaS is therefore to explore this new field of verification. We plan on building on our experience and the new modeling formalisms developed in the ongoing ANR PACS project to address this new problem in collaboration with researchers from the constraints community.

There is a long history of collaboration between the constraints and verification communities. Most of the time, constraint programming, SAT and SMT solvers are used on symbolic abstract models in order to enhance the performance of model checkers [3]. However, to the best of our knowledge, dedicated methods for deriving, manipulating and solving constraints over parameter values in parametric models have never been considered.

In particular, when considering “simple” parametric models where parameters only range over a single aspect of the system (such as probabilities, time or costs), the constraints that can typically be derived from the parameter synthesis problem are quite simple. Most of the time, linear “local” constraints over the parameter values are derived from the model structure and then combined together in order to produce linear, polynomial or rational “global” constraints, depending on the type of property we are interested in. While these resulting constraints can be solved in a brutal way by using existing constraint solvers, the practical applicability of this technique is quite limited (as explained above, the state-of-the art parametric model checker PROPHESY [1] is limited to models with a few thousand states and up to 3 parameters). Nevertheless, we conjecture that a clever, dynamic, manipulation of the local constraints during the verification process could greatly enhance the performance of parametric model-checkers. Combining such resolution techniques with new abstraction techniques for parametric models could then potentially enhance the applicability of such methods by an order of magnitude.

In the long term (beyond the one-year duration of CoPaS), our ambition will be to make these techniques applicable in practice. We will therefore devote a lot of efforts to implementing our techniques, demonstrating the efficiency of the developed tools on real-life case studies and communicating our results not only to the computer-science community but also to all scientific domains that already make use of modeling and verification techniques (biology, chemistry, electronics, automation...).

[1] Dehnert, C., Junges, S., Jansen, N., Corzilius, F., Volk, M., Bruintjes, H., Katoen, J.P., Abraham, E. : *Prophesy : A probabilistic parameter synthesis tool*. In : CAV. LNCS, Springer (2015).

[2] Brooks-Pollock, E., Roberts, G.O., Keeling, M.J. : *A dynamic model of bovine tuberculosis spread and control in great britain*. Nature 511, 228–231 (2014).

[3] Abdulla, P.A., Bjesse, P., Eén, N. : *Symbolic reachability analysis based on sat-solvers*. In : TACAS. LNCS, vol. 1785, pp. 411–425. Springer (2000).