Report on the PhD dissertation of Michał KNAPIK
"Parametric Model Checking"

Laure Petrucci
November 30, 2015

1 Subject and research area of the dissertation

Verification and validation of computer systems has become a critical subject over the years. Many modelling languages such as automata and Petri nets offer a convenient and easy to use formalism, providing a graphical view of the system considered as well as powerful formal analysis tools. The limitation of classical model-checking techniques is that most base on static systems, completely defined a priori. But in practice some details are unknown, maybe over-specified or on the contrary some values are enforced, giving less latitude to the actual implementation.

To overcome such restriction and enhance the system design process, some parametric approaches have recently been proposed. From a global point of view, they aim at providing answers for tuning the design of systems so that desired properties are satisfied. The thesis presented by Michał KNAPIK provides significant contributions in this area. More specifically, it addresses two parameter synthesis problems: action synthesis for discrete time models; time synthesis for real-time models. The work of Michał KNAPIK not only presents the theory, but also provides software tools implementing it.

The work presented in this dissertation has been published in very good quality conferences (5, including a best paper award at AAMAS 2012) and journals (2).

2 Dissertation contents and results

The dissertation is written in English and is divided into 4 chapters. Actually, two of them (introduction and conclusion) are short as could be expected, and the other two contain the contributions of Michał KNAPIK to his research area. These could be seen as parts rather than chapters.
I did appreciate the presentation which provides, for each problem tackled, a clear positioning of the existing works this research bases on, the construction of the theoretical aspects of the proposal, examples illustrating each step, leading to the design of an algorithm which is implemented and experimented on case studies. An access to these software tools has been made available to the reviewer. Although the theoretical complexity might be high, elaborate encodings, such as the use of BDDs, make these algorithms amenable in practice. The experimental results are good and prove the interest of such approaches. I would however have expected a more in-depth analysis of these experiments, pointing out all possible conclusions.

The first chapter (Introduction) first show the relevance of parameter synthesis as compared to traditional model-checking approaches. Noting that in practice all values manipulated in the system are not known a priori in the early stages of the design, finding acceptable values for free variables is a worthy challenge.

It also introduces the lines of research followed in the next chapters. First, parameter synthesis in the context of discrete time models for 3 different logics. The approach presented by Michal Knapik is exhaustive, as it provides all parameter valuations for which a property holds. Second, time synthesis for real-time models is tackled. As it is known that the existence of a parameter valuation is undecidable, Michal Knapik proposes under-approximations using a parametric region graph.

This introduction also comprises an extensive description of related works, which is very adequate. The problem at hand is a difficult one, and very few works addressed it, starting with the seminal paper of Alur et al. in 2001.

The second chapter (Symbolic parameter synthesis for discrete time systems) addresses action synthesis in the context of CTL-like logics. It considers 3 different logics. The first one applies to Mixed Transition Systems while the other two are used to analyse Multi-Agents Systems.

1. pmARCTL (parametric Action Restricted CTL) considers formulae in which path quantifiers are subscripted with the sets of actions used in the considered paths. In the parametric case, these actions can either be explicitly stated or free variables. The synthesis provides all sets of actions that can be considered in paths, and thus those that should be avoided for the property to hold. In practice this means that some actions should not be taken.

2. CTLPK (CTL with Parametric Knowledge) expresses epistemic formulae which can include information about the knowledge of a group of agents. It can be local knowledge (an individual agent knows that \( \phi \) holds), its extension to a group of agent (everyone in the group knows \( \phi \)), distributed knowledge (\( \phi \) holds in all undistinguishable states) or common knowledge (everyone in the group knows \( \phi \) and knows that everyone knows, etc.).
Such groups of agents can either be fixed or be a parameter, in which case
the synthesis algorithm provides the groups composition.

3. PATL (Parametric Alternating Time Temporal Logic) expresses strategic
capabilities of groups of agents. Thus, agents can behave so as to enforce a
property. The synthesis provides the adequate group of agents, according
to strategies based on perfect information. In this ATL semantics, local
actions depend on global state. They can be also with perfect recall, i.e.
depending on visited states, or without.

The chapter concludes with possible avenues opened for research: approximating
the full set of solutions, handling non fixed pint properties and more extended
applications.

The third chapter (Parameter synthesis for real-time systems) deals with
time parameters synthesis for real time systems. In this chapter, models con-
considered are PTA(Parametric Timed Automata) in which clocks are compared
to other clocks and time values or parameters. Although undecidable in the
general case, this problem is for L/U automata, where clocks have lower and
upper bounds. Michal KnapiK proposes first to extend the region graph used
in Timed Automata analysis to the parametric case with Parametric Region
Graphs. This is done in a very natural way. The synthesis can then be pos-
sible by examining runs in that graph. They are considered up to a certain
length, following a bounded model checking paradigm. The algorithm provided
by Michal KnapiK leads to an under approximation of the set of solutions, with
linear expressions that the parameters should satisfy for the property of interest
to be valid. He also explains in detail how to encode the PTA so as to use a
SMT solver for dealing with the constraints.

The possible developments of then presented: investigate the conditions for
boundedness of clocks in PTA — and eventually go further than L/U automata;
provide a better loop detection process, e.g. by abstracting time for loops
detection; address other properties than reachability using a bounded model
checking inspired framework for LTL or TCTL; discretise the parametric region
states.

Finally, chapter 4 (Conclusion) summarises the contributions of the thesis.

3 Conclusions

The dissertation presented by Michal KnapiK constitutes a significant con-
tribution to the research domain of model checking, and more precisely to pa-
rameter synthesis. It addresses on the one hand action synthesis and on the
other time synthesis. Although some theoretical parts are rather technical, the
structure of the presentation, the illustration with examples, make things clear
and easy to read.
Therefore, the dissertation of Michal Knapik fully meets the requirements of the Act on Scientific Degrees and Scientific Title, and can be admitted to public defence.

Laure Petrucci
Full Professor,
LIPN, CNRS UMR 7030
Université Paris 13