Parametric model checking (abstract)

Michał Knapik

With the proliferation of computers in most of the areas of human activity we become more and more dependent on their correct functioning. Formal methods put forward various techniques for ensuring that the behaviour of the analysed systems is consistent with their specification. Model checking is one of such techniques. In this approach the system in question is represented as a mathematical model and its specification is expressed using a formal language – usually a formula of temporal logic. A tool for model checking supplied with this input is then expected to provide a binary output: *the model is/is not compliant with the specification.* One of the limitations of this approach is that it is most suitable for verifying fully specified systems. This is often not possible, especially at the initial stages of design. Moreover, if a bug is found, then a model checking tool is only able to provide a trace leading to an erroneous behaviour.

The focus of this dissertation is in parametric model checking, also known as parameter synthesis. In this approach the model of a system or the properties to be verified are only partially specified, with the unknown elements replaced by free variables called parameters. A parametric model checking tool is expected to provide at least a partial characterisation of the set of parameter valuations under which the model is compliant with its specification.

The goal of the work presented here is to develop and analyse selected techniques of parametric model checking. We raise two, largely independent, subjects.

Firstly, we deal with discrete-time models. In this setting, we extend the classical methods for the verification of logics that have a fixed-point characterisation to the case of parameter synthesis. As we show, the fixed-point dependencies in the ground logics are inherited by their parametric extensions, leading to natural and rather simple algorithms. We devise a theory of parameter synthesis for three logics: Parametric Action-Restricted Computation Tree Logic (pmARCTL), Parametric Computation Tree Logic with Knowledge (CTLPK), and Parametric Alternating-time Temporal Logic (PATL). The presented approach is exhaustive, i.e., we obtain the characterisation of the set of all the parameter valuations under which a given property holds. We implement the theory in a stand-alone program called SPATULA (for pmARCTL) and in an extension of the established tool for verifying multi-agent systems called MCMAS (for CTLPK and PATL). We provide an extensive evaluation of our approach, showing that it can be up to four orders of magnitude faster than the brute-force one.

Secondly, we deal with real-time models, namely parametric timed automata (PTA). It is known that the emptiness for the parametric reachability, i.e., the existence of a parameter valuation under which a given state is reachable, is not decidable for PTA. We therefore focus on approximative techniques for parameter synthesis. To this end we introduce the notion of the parametric region graph, inspired by the classical concept of the region graph for timed automata. We show that the parametric region graph can be used to simulate all the finite behaviours of a parametric timed automaton, hence its unfolding up to a finite depth enables approximative parameter synthesis, similar in spirit to bounded model checking. However, as we show, the techniques of loop detection that allow to identify infinite paths in the finite unrollings of region graphs are here only of limited use. Additionally, we provide a simple translation from the problem of parametric reachability for Lower/Upper Bound PTA to the problem of model synthesis for formulae of Quantifier-Free Linear Arithmetics, implemented in a SMT-based stand-alone tool PTA2SMT.

***Keywords*:** formal methods, parameter synthesis, parametric model checking
***ACM Classification*:** D.2.4, F.4.1, I.2.11

Parametryczna Weryfikacja Modelowa (streszczenie)

Michał Knapik

Wraz z rozpowszechnianiem się systemów komputerowych stajemy się coraz bardziej zależni od ich poprawnego funkcjonowania. Weryfikacja modelowa jest jedną z metod formalnych, mających zapewnić zgodność systemu ze specyfikacją. Podejście to opiera się na budowie matematycznego modelu systemu i opisie jego pożądanych własności przy pomocy precyzyjnego języka logiki. Wynikiem działania narzędzia przeznaczonego do automatycznej weryfikacji modelowej jest zero-jedynkowa odpowiedź: *model jest/nie jest zgodny z podaną specyfikacją*. Jednym z ograniczeń weryfikacji modelowej jest to, iż do stworzenia dokładnego modelu konieczna jest dobra znajomość istniejącego systemu. W wielu przypadkach, a w szczególności w początkowych fazach projektowania, nie jest to możliwe.

W niniejszej dysertacji zajęto się parametryczną weryfikacją modelową, zwaną również syntezą parametrów. W podejściu tym umożliwia się obecność w modelu lub w badanej własności wolnych zmiennych zwanych parametrami. Wynikiem działania narzędzia przeznaczonego do parametrycznej weryfikacji modelowej jest całkowita lub częściowa charakteryzacja wartościowań parametrów przy których model jest zgodny ze specyfikacją. Celem rozprawy jest budowa teorii syntezy parametrów dla wybranych metod specyfikacji oraz zbadanie jej praktycznej stosowalności. Skupiono się na dwóch głównych zagadnieniach.

Pierwszym z nich jest synteza parametrów dla modeli z czasem dyskretnym. Zaproponowano w tym celu parametryczne wersje trzech wybranych logik posiadających charakteryzację stałopunktową. Pierwszą z nich jest Parametryczna Logika Czasu Rozgałęzionego z Akcjami (skr. pmARCTL), pozostałe dwie to Parametryczna Logika Czasu Rozgałęzionego z Wiedzą (CTLPK) oraz Parametryczna Logika Czasu Alternującego (PATL). Jak wykazano, stałopunktowe zależności obecne w nieparametrycznych logikach są w tych przypadkach dziedziczone przez ich parametryczne rozszerzenia. Prowadzi to do naturalnych algorytmów syntezy parametrów, które zaimplementowano w dwóch narzędziach. Pierwsze z nich, SPATULA, służy do parametrycznej weryfikacji pmARCTL. Drugie, będące rozszerzeniem weryfikatora dla systemów wieloagentowych MCMAS, akceptuje formuły CTLPK i PATL. Przedstawiona analiza eksperymentalna pokazuje, iż zaproponowane rozwiązania potrafią być do czterech rzędów wielkości szybsze od podejścia siłowego. W omawianym przypadku dokonuje się syntezy pełnego rozwiązania, tj. zbioru wszystkich wartościowań parametrów przy których dana formuła jest spełniona w modelu.

Drugim z zagadnień jest synteza parametrów dla modeli z czasem ciągłym: parametrycznych automatów czasowych (PTA). Jak wiadomo, problem istnienia wartościowania parametrów, przy którym dany stan automatu jest osiągalny, jest nierozstrzygalny w klasie PTA. W drugiej części rozprawy skupiono się zatem na technikach aproksymacyjnej syntezy parametrów. Wprowadzono w tym celu nowe pojęcie parametrycznego grafu regionów, będącego odpowiednikiem grafu regionów dla automatów czasowych. Jak pokazano, struktury te pozwalają na wierną symulację skończonych ścieżek PTA, stąd też ich ograniczone rozwinięcia umożliwiają dolną aproksymację szukanego zbioru wartościowań parametrów. Podejście to zbliżone jest koncepcyjnie do ograniczonej weryfikacji modelowej (BMC). Jak jednak zilustrowano, typowe dla BMC techniki wykrywania pętli mają tu ograniczone zastosowanie. Dodatkowo, przedstawiono prostą translację z problemu parametrycznej osiągalności do problemu syntezy modelu dla logiki QF_LRA, zaimplementowaną w autorskim narzędziu PTA2SMT, wykorzystującym techniki SMT.

***Słowa kluczowe*:** metody formalne, synteza parametrów, parametryczna weryfikacja modelowa
***Klasyfikacja tematyczna ACM*:** D.2.4, F.4.1, I.2.11