



Technische Universität Dresden, 01062 Dresden

Prof. Dr. rer. nat.
Christel Baier

Sekretariat: Karina Wauer
Telefon: 0351 463-38549
Telefax: 0351 463-38348
E-Mail: christel.baier@tu-dresden.de

Dresden, 13th June 2018

Review for the PhD Thesis

Automata for Formal Methods: Little Steps Towards Perfection
submitted by František Blahoudek

The translation of LTL (linear temporal logic) formulas into NBA (nondeterministic Büchi automata) is one of the core elements of verifying systems against linear-time specifications. Since the seminal work by Vardi and Wolper in the mid 80th's, a variety of LTL-2-NBA algorithms have been proposed, refined by heuristics and implemented in tools. The translation of LTL formulas into NBA or other types of automata over infinite words is still a very active research field. While NBA are sufficient for verifying systems represented by ordinary transition systems, they are not when the system exhibits probabilistic behaviors and the task is to show that a given formula φ holds almost surely or to compute the probability of the paths satisfying the formula. The conceptually simplest approach for the latter task is to generate a deterministic automaton D for φ and then to analyze the product of D with the probabilistic system model M . This approach has the disadvantage that in the worst-case a double-exponential blow-up for the translation of LTL formulas into deterministic automata can be unavoidable. This motivated research on weaker forms of deterministic automata that are sufficient for certain verification purposes. One such class are automata that are deterministic-in-the-limit (called semi-deterministic in the thesis).

The thesis makes contributions in this field in three directions: by introducing techniques that incorporate information about the system to be verified in the LTL-2-NBA translation, by presenting a new algorithm for the translation of LTL formulas into deterministic automata and by introducing a refinement of a known algorithm to generate semi-deterministic automata from LTL formulas and as well as a new algorithm for the complementation of semi-deterministic automata.


Postadresse (Briefe)
TU Dresden,
01062 Dresden

Besucheradresse
Nöthnitzer Straße 46
Zimmer 3004/3005
01187 Dresden

Steuernummer
(Inland)
203/149/02549

Bankverbindung
Commerzbank AG,
Filiale Dresden

Postadresse (Pakete u.ä.)
TU Dresden,
Helmholtzstraße 10,
01069 Dresden

 Zufahrt für
Rollstuhlfahrer
Rampe Seiteneingang,
gekennzeichnete Parkflächen

Umsatzsteuer-Id-Nr.
(Ausland)
DE 188 369 991

IBAN
DE52 8504 0000 0800 4004 00
BIC COBADEFF850

Internet <https://tu-dresden.de>

Kein Zugang für elektronisch signierte sowie verschlüsselte elektronische Dokumente.



**DRESDEN
concept**
Exzellenz durch
Wissenschaft
und Kultur

The thesis starts with a well written introduction that motivates the considered research questions and briefly summarizes the main results. The second chapter briefly explains the notations used in the thesis. The main contribution is in Chapters 3-8. The material of each of these six chapters is a revised version of a conference paper.

Chapters 3 and 4, based on material published at SPIN'14 and SPIN'15, carefully analyze the demands of LTL-2-NBA translators for verification purposes with the prominent model checker SPIN. It relies on an explicit representation of the state space and uses the nested depth-first search for an on-the-fly approach to search for ultimately periodic paths in the product of the system and the automaton for the negated formula satisfying the acceptance condition of the automaton and therefore violating the original formula. The thesis reports on exhaustive experiments providing evidence that the NBA-sizes have crucial impact on the run time, but are not the only criterion that matters. Instead the thesis shows that more subtle optimization criteria that attempt to minimize the number of reachable states in the product and support the nested depth-first search to find accepting cycles (emptiness check) can have significant impact as well. These observations motivated the development of techniques to manipulate a given LTL or automata specification, which have been evaluated on the basis of more than 3 000 verification tasks. Although there is no deep technical contribution in Chapters 3 and 4, the experimental studies provide interesting insights and evidence for the general usefulness of refinement strategies. As stated at the end of chapter 4, the comparative studies also revealed a bug in SPIN.

Chapter 5 presents a new algorithm for the generation of deterministic automata from formulas of certain LTL fragments. It borrows ideas from Gastin and Oddoux and proceeds in two steps. The first step generates a very weak alternating automaton. The second step then transforms the obtained very weak alternating automaton into an equivalent deterministic automaton with generalized Rabin acceptance condition. The considered LTL fragments are the fragment built by propositional logic in positive normal form and the eventually and always modalities (denoted $LTL(F_s, G_s)$) and the fragment where no until or next step modality appears in the scope of an always modality (denoted $LTL_{\forall}(U, X)$). The presented approach for constructing very weak automata from $LTL(F_s, G_s)$ formulas departs from the classical algorithm (for full LTL) proposed by Gastin and Oddoux and yields an automaton where the states can be classified into may states, must states or loopless states. Such automata are called MMAA and are shown to have the exact power of $LTL(F_s, G_s)$. The determinization of MMAA relies on a double powerset set construction (i.e., states in the deterministic automaton are subsets of the powerset of the state space of the given MMAA). The same ideas are applicable for the larger fragment $LTL_{\forall}(U, X)$, the essential difference being that the first step yields very weak alternating automata that satisfy the may-must property "in the limit" rather than globally. This approach has been implemented in the tool LTL3DRA. The thesis nicely describes the details of the algorithm and provides soundness proofs for the main part (the MMAA-2-DA translation). The treatment of the $LTL_{\forall}(U, X)$ formulas is a bit short. Implementation details have been explained at the end of Chapter 5. (At the first reading, I was wondering why nothing is said about experiments. But then I saw that these are included in Chapter 6. This, however, is just a very minor comment on the presentation.)

Chapter 6 reports on comparative experimental studies with different implementations (algorithms and tools) for the translation of LTL formulas into deterministic automata. The thesis reports on a huge number of experiments that vary in the type of considered LTL formulas and the criteria to compare implementations (e.g., number of states, size of the acceptance condition, time requirements). Although there is no clear winner, the experiments indicate a clear superiority of the tools Spot and Rabinizer.

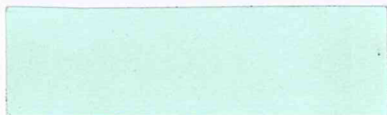
Chapter 7 revisits the Courcoubetis and Yannakakis approach to generate semi-deterministic Büchi automata from NBA using a variant of the classical powerset construction where states in the semi-deterministic automaton are pairs of sets of states in the original NBA. It presents a simplification ("SCC-aware optimization"), explains how to modify the approach for generating cut-deterministic automata (which is a strong form of semi-determinism) and discusses the semi- or

cut-determinization for generalized Büchi automata. Comparative studies have been carried out with two other recent implementations for the construction of semi-deterministic automata from LTL by Sickert et al and by Kini and Viswanathan.

A complementation operator for semi-deterministic automata has been presented in Chapter 6. This work was motivated by the demand of a learning approach for the termination analysis. The algorithm generates an unambiguous Büchi automaton and relies on a powerset construction with quadruples of sets of states. Soundness is shown using the concept of run graphs and ranks. Experiments indicate the superiority of this approach compared to other approaches.

The presentation is very good. At all relevant places, the theoretical background has been worked out in detail. New concepts are explained with care and nicely illustrated by well chosen examples and pictures. All new algorithms have been implemented and carefully evaluated in comparative studies. In all cases, the experiments are impressive and illumine many interesting aspects. Only in Chapter 6, I was wondering why the algorithms for semi-deterministic automata have not been evaluated in the verification context. Another minor issue is that I miss some conclusions.

In conclusion, the thesis presents a number of original and significant contributions to the research field and clearly fulfills the requirements for a PhD degree in Computer Science and Engineering, under the usual international standards. Without hesitation, I strongly recommend the submitted thesis for the award of the PhD degree in Computer Science. To my opinion, the thesis deserves the highest grade A.



Prof. Dr. rer. nat. Christel Baier

Technische Universität Dresden
Fakultät Informatik
Institut Theoretische Informatik
01062 DRESDEN