האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM

Prof. Orna Kupferman
The Selim and Rachel Benin
School of Engineering and Computer Science
Edmond J. Safra Campus
Givat Ram
Jerusalem 91904 Israel

פרופ. אורנה קופרמן
בית הספר להנדסה ולמדעי המחשב
ע"ש רחל וסלים בנין
קרית אדמונד י' ספרא
גבעת רם, ירושלים 91904

May 16, 2018

A report on the Ph.D. thesis of Trantisek Blahoudek

Automata on infinite words play a very important role in reasoning about reactive systems. They are extensively used in verification and synthesis algorithms. The challenge of translating specifications in linear temporal logic (LTL) to automata goes back to the 80s. The importance of the translation in practice has led to extensive research and to a development of several tools that translate LTL formulas to nondeterministic Büchi automata (NBAs) and to deterministic Büchi automata (DBAs). Automata on infinite words form a very rich and interesting mathematical model. Their analysis involves complicated combinatorial considerations, and ideas from graph theory and logic theory. Their applications involve rich and interesting implementation issues, like optimizations that are geared toward specific algorithms, symbolic implementations, and combinations with existing tools and algorithms. The thesis includes very nice and interesting contributions in all the above fronts.

Contributions In the context of NBAs, the thesis examines the relative advantages of the different translations for LTL to NBAs in practice, focusing on their performance in the explicit model checker SPIN. Technically, this corresponds to an examination of which translation is best for applications that involves reasoning on the state space on the depth-first search manner.

More in the context of NBAs, the thesis introduces an original method for optimizing the automata by simplifying the labels on the edges. In conventional translations, the labels are truth assignments to the atomic propositions in the formula. Sets of assignments are represented by propositional formulas. The suggested method use information about the system to be verified in order to simplify these formulas.

In the context of DBAs, the thesis introduces a new class of automata, termed may/must alternating automata (MMAA). In these automata, each state can be of one of three classes, where each class restricts the type of transitions from states in it. The thesis proves that MMAAs recognize exactly languages definable by the (F_s, G_s) fragment of LTL, which includes only strict invariants and eventualities, and describes a determinization construction for them (in fact, for a wider class, which corresponds to a larger fragment of LTL). The thesis also analyzes and compares the performance of different translations of LTL into DBAs. The analysis is very comprehensive and is of great both theoretical and practical interest.

Sometimes, algorithms can use automata that are not fully deterministic, but have some

Telephone: +972-2-5494558 Fax: +972-2-5494558 E-mail: orna@cs.huji.ac.il

elements of determinization. The thesis studies two such classes, namely semi-deterministic and cut-deterministic automata, and describes algorithms for semi- and cut- determinization of Büchi and generalized Büchi automata, and analyzes the performance of the constructions as well as their applications in complementation constructions.

Evaluation As explained above, the topic of automata on infinite words is very challenging from a technical point of view and has been extensively studied. Entering it requires a wide background, and making new contributions requires coming up with original and clever ideas. The thesis covers many aspects of the LTL to NBW/DBW translation – both theoretical and practical, and includes some very nice and interesting ideas, observations, and techniques. The thesis also includes comprehensive experimental components. I thus find the thesis to be of a very high quality.

The thesis is very well written. It includes an excellent introduction to the research topic, with a very good coverage of earlier work. The thesis is very esthetic and easy to follow, and the author makes an effort to explain the intuition and to give examples of the used notations and concepts. Sometimes, however, a repetition of formal definitions could be helpful and save the reader a search for earlier definitions. For example, in the introduction of MMAA (page 65), the definition of the three classes of states is colorful and accompanied by helpful examples, yet the reader would benefit from a formal exposition, namely something like "s is a may state if for every letter $a \in \Sigma$, we have that..." It is true that the definitions of looping transitions and self loops are one page earlier, so everything is well defined, but it's good to see the combination of the notations with the specific definition. Another point for this example: may/must is not the best name, as "may" and "must" are traditionally used in the formal-verification community for transitions in over- and under- approximation abstractions.

The author has demonstrated the ability to work independently and creatively in the specific field. The thesis meets the standard requirements imposed on a dissertation thesis in the specific field. I reccommend its acceptance, and I give it grade B with respect to "European standard". The reason I do not give grade A is that while the theis includes clever and original ideas, it forms a collection of (again, excellent) contributions in a known challenge, and is thus incremental in its nature. I give an A only to a thesis that opens a new line of research or settles a long-standing open problem.

Sincerely,

Orna Kupferman