UNIVERSITÉ SORBONNE PARIS NORD

cnrs

LIPN

In Villetaneuse, November 17, 2023

Report on the PhD thesis of Nicolas Amat

"A PolyHedral Framework for Reachability Problems in Petri Nets"

Verification and validation of computer systems has become a critical subject over the years. Modelling languages and model checking techniques allow for assessing the correct behaviour of systems. Among the main properties of interest are reachability and concurrency, which are studied in this thesis with a novel prism to enhance performance. Although reachability in Petri nets has been known as decidable for decades, its high complexity leads to use symbolic techniques or different kinds of reductions in practice.

Therefore, the thesis presented by Nicolas Amat aims at proposing novel approaches to accelerate the verification of reachability problems in Petri nets, based on structural reductions. It provides the theoretical foundations as well as proven algorithms, their implementation and extensive experiments on a recognized benchmark.

The thesis document submitted comprises eight chapters (of approximately 25 pages each), preceded by a general introduction, and finally a conclusion with perspectives.

The manuscript is well structured, with a similar outline for each chapter: an introduction with context, challenges, proposal, and outline of the chapter ; the theoretical contributions and their proofs ; the algorithms to put these contributions into practice, as well as their proof ; experimental results with comparison to the best existing tools for the problems addressed ; a summary with some perspectives ; and finally the associated publications and the access to the tools developed.

To start with, the introduction clearly states the context of this thesis and the relevance of the topics addressed. The goal is to accelerate the verification of reachability problems in Petri nets, using a novel structural reduction approach, called *polyhedral reduction*. This leads to verification using a *property directed verification* method. The introduction ends with an outline of the manuscript and a roadmap as a dependency graph between chapters.

Chapter 1 recalls the basic concepts used in this thesis: Petri nets, their behaviour, reachability and boundedness properties, observable sequences. It sets also the context for expressing reachable markings and invariants as linear arithmetic constraints. Encoding Petri nets semantics with Presburger arithmetic then allows for using the full power of mature SMT solvers. Non-reachability can be guaranteed by a certificate of invariance. A review of reachability related problems sets the properties of interest in this thesis: reachability of markings that satisfy a combination of linear constraints, where a witness for existential quantifiers, or a counterexample in the case of universal quantifiers ; invariants ; coverability properties ; concurrent places.

Nicolas Amat also reviews the decidability and complexity results for these, stressing that even though some problems have long be known as decidable, recent results on complexity show the difficulty of designing efficient algorithms, thus confirming that the best results are obtained via a portfolio of approaches.

Model Checking methods are thus various and use diverse optimisations such as symbolic encoding, random walk, bounded model checking, induction, etc., each with some drawbacks. The thesis contributions are compared with this context.

The first contributions are presented in Chapter 2, where a semi-decision procedure for reachability in Petri nets is designed with a double objective of expressiveness and performance. Considering scenarios composed of a marking m, a sequence ρ and a formula F satisfied by the target state of the sequence, Nicolas Amat defines three generalisations. They are predicates G satisfied by m such that all other markings satisfying G are also part of a scenario with F. This introduces three characteristics that are used in different parts of the thesis as well: monotonicity, hurdles and acceleration. It is noteworthy that notions like the hurdle are rather old but were little used, showing the extent of the literature review Nicolas Amat performed and his accurate choice of notions to exploit in his work.

The thesis includes generalisations algorithms within property directed reachability (PDR). It consists in computing an over approximated sequence of linear predicates on the net places. This incremental procedure is repeated until a counterexample is found or a predicate is inductive. When a witness is found, generalisations abstract it into a predicate that abstract similar (dangerous) states, and the predicate is added to the clauses considered. Without saturation, PDR is not complete, but saturation is not sufficient for completeness.

The algorithm is implemented in the tool SMPT. The evaluation of expressiveness is performed on 5 examples proposed in the thesis that exhibit different characteristics. SMPT can handle all of them within a timeout of 1 hour where other well-known and recent tools (`ITS-Tools`, `LoLA`, TAPAAL, Kreach, FastForward) fail on at least one example (and some one all). The evaluation of performance uses a larger benchmark of 30 models from the literature. They show good results, similar to those of TAPAAL. Beyond this nice evaluation, an originality of SMPT is to output certificate of invariance.

The next Chapter 3 defines polyhedral reduction equivalences and provides an immediate use of these. The idea is to track the relations between markings of places of an original net and of its reduced net. The proposal is to express them as a Presburger formula, so that it is possible to rebuild the reachable markings of a net from those of the reduced net plus the formula. This is formalised by a notion of equivalence between markings up to the formula constraints. The reduction rules considered come from the literature, and the construction of the formula definitely constitutes an advance in net reductions usage. The chaining of different reductions allows for a compositional approach that is proven sound. Moreover polyhedral reduction can be combined with other reachability checking approaches. All this is implemented within SMPT, performing reductions with the tool Reduce of the tina toolbox and was experimented successfully at the 2023 edition of the MCC over almost 10 000 test cases of net and formula. The analysis of the results highlights the relevance of such an approach, according to the reduction ratio. They are particularly impressive when the ratio is high.

Chapter 4 goes one step further by capturing the structure of the constraints stemming from polyhedral reductions within a graph structure called the *Token Flow Graph* (TFG). This is particularly smart as sequences of reductions could be seen as graph transformations on a simple structure. Vertices represent places or constants, and are connected by two types of arcs depending on whether they are redundant or agglomerated places. When such a TFG exists, its well-formed version, holding natural characteristics, is unique. Markings can be projected on such a graph for testing their reachability at low cost. The corresponding algorithm is implemented in the tool Kong, using Reduce for nets reductions and Sift for state space exploration. It is evaluated for more than 1 000 net instances and 4 reachability queries each.

In Chapter 5, Nicolas Amat uses projections also on formulas to decrease the size of the formula to check. Two examples of formulas are given for a net, its reduced version and the corresponding well-formed TFG. The computations on these examples are not that obvious, and additional details would have helped the reader. Three reductions on formulas are formally defined, based on the Token Flow Graph, two of them preserving the formula semantics while the last one might lose some markings, thus leading to an under-approximation, as shown in the soundness and completeness theorems. Nevertheless, the under-approximation can help finding witnesses of the existence of reachable markings. The experimental results with the tool Octant show improvements when model checking using random walk, and better ones with k-induction. The most interesting results are the ability of using this as a front-end to other tools (`ITS-Tools`, `LoLA`, tapaal) which enables them to solve challenging queries they failed to handle otherwise. Moreover, for quantifier elimination, Octant solves 60% more queries than `isl` and 3 times mores than `Redlog`.

Chapter 6 focuses on computing the concurrency relation, i.e. all pairs of places that can be marked simultaneously. The concurrency relation on 1-safe nets is used for decomposing the net into Nest Unit Petri Nets. The contributions of the previous chapters preserve safeness. Thus it was natural to derive both concurrency and non-concurrency of places in a net from those in the reduced net, even though it may output a partial result. The proposed algorithm is more technical and its correctness proof quite involved, but presented step by step through several lemmas. It is part of the Kong tool that can be used as a front-end to `Caesar.BDD`, demonstrating once more the efficiency of the approach.

Polyhedral equivalences are at the core of this thesis, well defined and extensively used. Proving automatically such an equivalence is addressed by Chapter 7. To achieve that, instead of considering nets with a single initial marking, Nicolas Amat extends them to parametric nets in the sense that there is a set of initial markings. Coherency constraints are defined, considering firing sequences that end with an action transition. Parametric reduction rules and equivalences follow. This leads to an automated proof procedure using a Presburger encoding of parametric Petri nets semantics as well as core requirements. It states whether an input candidate reduction rule is sound or not. Accelerating silent transition sequences extends the algorithm.

The experimental evaluation of this algorithm implemented in Reductron within a toolchain with `fast` for Presburger formula, and `z3` as SMT solver exhibits both sound and unsound equivalence rules. The experiments are less detailed than those in the other chapters.

Finally, Chapter 8 summarises the experimental parts. The benchmarks from the MCC comprise both models and formulas. Each of the tools developed by Nicolas Amat (smpt, Kong, Octant, Reductron) is detailed with the capabilities it provides and a short usage manual. This chapter shows that a software design effort, driven by three years of participation in the Model Checking Contest, led to already mature tools and not only prototypes. The availability of benchmarks and artifacts supports reproducible science.

The manuscript ends with a short conclusion chapter that provides a nice general summary and draws some perspectives. They concern not only relevant extensions of the proposed approaches, but also the selection and tuning of portfolios, thus providing a wide palette of optimised tools to attack the reachability problems from different angles.

To conclude, the thesis submitted by Nicolas Amat is a very valuable contribution to reachability analysis in Petri Nets. It contains an extensive amount of results ranging from theory to experiments and compares to the best state-of-the-art software tools, resulting in a 3rd rank in the last two editions of the international *Model Checking Contest*, for the reachability competition.

The manuscript is well written, all lemmas and theorems are thoroughly proven, and there are a few small examples. The thesis work led to the publication of 3 papers in journals (ToPNoC, FI, STTT), and 6 at top-level conferences (FM, 3 PetriNets, SPIN, TACAS). The experiments are supported by 4 open-source software tools, embedded in a package accompanying the thesis.

The work presented by Nicolas Amat is clearly of very high quality. Thus, I strongly support it for a PhD in computer science.

Laure Petrucci

Full professor