LABORATOIRE
BORDELAIS
DE RECHERCHE
EN INFORMATIQUE
LaBRI

15 November, 2023

Report on the PhD Thesis of Nicolas Amat Entitled: A Polyhedral Framework for Reachability Problems in Petri Nets

The thesis contributes notable advancements in the automated analysis of Petri nets, which are classical models of concurrent systems. Automated analysis of Petri nets constitutes a well-established branch of Computer-Aided Verification. Within this domain, one of the central problems is the reachability problem, which involves determining whether a specific marking or a set of markings can be reached from the initial marking of a Petri net. In addition to addressing the reachability problem, the thesis also explores the computation of invariants and the computation of the concurrency relation. The primary novel concept introduced in the thesis is the notion of "reduction," which is thoroughly studied and refined in various ways. To substantiate theoretical developments, the thesis provides extensive experimental evidence demonstrating their advantages across a comprehensive test dataset.

Chapter 3 introduces the notion of a reduction between two Petri nets. A reduction is defined by the nets themselves and a reduction predicate denoted as $E(x, y)$, which relates markings of these nets. The predicate must relate the initial markings of the two nets. Additionally, for every reachable marking m of net N, all markings related to m must also be reachable in m', and there must be at least one such reachable marking. In essence, a reduction predicate E shares some similarities with an invariant in a Petri Net, but with a key distinction: an invariant refers to places within a single net, whereas a reduction involves a relationship between markings of two distinct nets.

The thesis shows that this type of reduction can be effectively employed for tasks such as checking reachability and invariance. Instead of examining a potentially larger net N, one can work with a smaller net N' and derive the answer using the reduction predicate E. For instance, to verify the reachability of a predicate $F(x)$ in net N, it suffices to check if $F'(y) \equiv \exists x.E(x, y) \wedge F(y)$ is reachable in the reduced net N'.

These reductions can be applied as rewriting rules in a graph rewriting style, where a reduction modifies a portion of the net and imposes a reduction predicate as a constraint. The thesis shows that rules can be composed, thus giving a framework for simplifying Petri nets. A significant challenge, which is addressed later in the thesis, involves identifying and verifying the correctness of these reduction rules.

The approach of reducing nets with rules has been implemented in a tool called SMPT and evaluated using formulas from the 2023 edition of the Model Checking Contest. The experimental results indicate that approximately half of the nets in the test set are reduced by about 30%. This is significant because the complexity of the reachability problem grows exponentially with the size of the net.

Chapter 4 goes deeper into the structure of reduction predicates $E(x, y)$ and introduces the concept of Token Flow Graphs (TFG), which is the second major innovation of this thesis.

In the approach discussed in the previous chapter, the reduced reachability formula, $F'(y) \equiv \exists x.E(x, y) \wedge F(y)$, could become quite complex. However, when $E(x, y)$ can be represented as a TFG, there is a one-to-one correspondence between markings of the original net N and the reduced net N'. Consequently, to determine if a marking m is reachable in N, it becomes sufficient to check if a corresponding marking m' is reachable in N', for the unique m' such that $E(m, m')$ holds. Thus, when given m, it is enough to find m' and assess its reachability in N'.

The central contribution of this chapter lies in defining TFG in a manner that is both comprehensive, encompassing many of the rules discussed in the previous section, and straightforward, enabling the efficient computation of m' for a given m in polynomial time. This approach has been implemented, and experimental results demonstrate that a significant portion of the reductions presented in Chapter 3 can be achieved using rules based on TFG. This is particularly useful for checking reachability of a particular marking as it entirely eliminates the need to employ an SMT solver over Presburger formulas, which was a primary source of additional complexity in the previous approach.

Chapter 5 highlights another significant advantage of the Token Flow Graph (TFG) representation. While the previous chapter demonstrated how TFGs can simplify the reachability of a single marking, this chapter explores their utility in streamlining the reachability of a more complex formula.

As a quick recap, the reduction method proposed in this thesis transforms the problem of verifying the reachability of a formula $F(x)$ into assessing the reachability of $F'(y) \equiv \exists x.E(x, y) \wedge F(y)$. The latter expression represents a quantified Presburger formula, which necessitates the elimination of quantifiers to make use of standard tools. Traditional quantifier elimination methods have exponential complexity in the worst case.

The primary achievement of this chapter lies in the development of a linear-time quantifier elimination procedure tailored for formulas $F(x)$ of a specific structure and for $E(x, y)$ defined by a TFG. This procedure has been implemented and rigorously tested. Experimental results reveal that the considered class of formulas is non-trivial, applies to relevant examples, and is not covered by existing quantifier elimination implementations. These results are not only promising but also indicate that this reduction method complements other optimizations in existing tools. Consequently, the results of this chapter show that this reduction approach could serve as a beneficial preprocessing step for all tools for reachability checking.

Chapter 6 addresses the challenge of calculating the concurrency relation of a Petri net. The goal is to determine all pairs of places that can be marked simultaneously in some reachable state. The primary result presented in this chapter is that when provided with a reduction (N, E, N') and information regarding the concurrency of N', it is possible to compute the concurrency information for N under the condition that E is presented as a Token Flow Graph (TFG). This is achieved through an elegant definition of the concurrency relation for E and an examination of its properties. Once again, this method has been put into practice and rigorously tested. The experimental results reaffirm the effectiveness and relevance of this approach.

Up to **Chapter 7**, the thesis primarily focuses on demonstrating the effectiveness of the proposed reduction method. It illustrates significant advantages in both reachability testing and the computation of concurrency relations. Yet, the strength of this method relies on the specific reduction rules it employs.

It's worth noting that verifying the correctness of reduction rules is undecidable, indeed the marking equivalence problem is essentially a special case of the rule correctness problem. However, it is crucial to ensure the correctness of the reduction rules used in algorithms, especially considering that the implemented algorithms make use of a substantial number of rules, each of which requires manual verification.

The introduction of an automated proof method not only enhances confidence in the correctness of proofs but also streamlines the process of adding new reduction rules. The idea is to use coherence constraints that are a form of invariants for the two nets, enabling the restriction of verification to single-letter sequences, thereby making equivalence a decidable property. Therefore, to establish the soundness of a reduction rule, it suffices to devise appropriate invariants and apply the automated procedure proposed in the thesis.

As with all other results, this theoretical framework has been implemented and rigorously tested. Once again, the results of the experiments have yielded highly positive outcomes.

Chapter 8 gives an overview of the experimental tools. The foundation upon which all the results presented in the thesis are built is the development of a tool called SMTP, designed for reachability checking. On top of it tools have been developed for the purposes of quantifier elimination and computation of concurrency relations. Finally, there is a tool dedicated to the automated verification of the correctness of reductions. In this concluding chapter of the thesis, the author provides a more detailed description of these tools, with special emphasis placed on ensuring the reproducibility of the results.

The general structure of the thesis is clear. Each chapter starts with an informative introduction and ends with an experiments section. Mathematical writing is good, notations are well-chosen. There is a number of interesting open problems mentioned in passing in the thesis, and some perspectives in the conclusions.

In summary, this thesis contributes important insights to the classical field of algorithmic analysis of Petri nets. Each chapter introduces a novel advancement, and the practicality of each improvement is thoroughly substantiated through an extensive array of experiments. The thesis makes a strong case for the adoption of the innovative concept of reduction between Petri nets. Reductions may become an integral component of the standard toolkit for reachability checking and other analysis problems. Reductions are particularly compelling because they can be seamlessly integrated with other analysis methods and do not require the assumption that the nets are bounded. The thesis represents a substantial body of work, marking a significant step forward in the development of algorithmic analysis techniques for Petri nets.

In my opinion the thesis satisfies all the requirements, and I declare that it merits to be accepted.

I. Walukiewicz

Igor Walukiewicz
Directeur de recherche CNRS