EXCURSION E1: INVARIANTS AND REACHABILITY IN PETRI NETS

GEORG ZETZSCHE

Over the course of section 2, we have seen a number of methods for proving that from a marking $M_1 \in \mathbb{N}^S$, one cannot reach a marking $M_2 \in \mathbb{N}^S$. While these methods are sufficient for many use cases, they share one crucial shortcoming: They are not *complete*. This means, they do not guarantee that if M_2 is unreachable from M_1, we are able to prove this using one of those methods.

The property of completeness is extraordinarily useful because, as we will see, it permits the construction of algorithms for the reachability problem. In this excursion, we get to know a particular method for proving unreachability that exhibits completeness. This method is again based on an *invariant*—a property of markings that is preserved by firing transitions. Surprisingly, this type of invariant is just a very slight extension of the linear algebraic invariants discussed so far.

Forward inductive invariants. The type of invariants that provide the aforementioned completeness are the "forward inductive invariants". They can be represented as semilinear sets.

Definition E1.1 (Semilinear set)**.** *Let $k \in \mathbb{N}$. A* linear set *is a subset of $\mathbb{N}^k$ that has the form*

$$\{x_0 + a_1 \cdot x_1 + \cdots + a_n \cdot x_n \mid a_1, \ldots, a_n \in \mathbb{N}\},$$

for some fixed $x_0, \ldots, x_n \in \mathbb{N}^k$. A subset of $\mathbb{N}^k$ is called semilinear *if it is a finite union of linear sets.*

A convenient way to work with semilinear sets is to represent them by first-order formulae over the structure $(\mathbb{N}, +)$. We recall the following definition from the lecture on Logics (or Automata Theory).

Definition E1.2. *The first-order theory over the structure $(\mathbb{N}, +)$, where $+$ denotes the usual binary addition, is called* Presburger arithmetic*. Formulae over the corresponding signature are called* Presburger formulae*. A Presburger formula φ with free variables $\mathsf{x}_1, \ldots, \mathsf{x}_k$* defines *the set*

$$\{(x_1, \ldots, x_k) \in \mathbb{N}^k \mid (x_1, \ldots, x_k) \models \varphi\},$$

where $(x_1, \ldots, x_k) \models \varphi$ denotes the fact that φ is satisfied if the variables $\mathsf{x}_1, \ldots, \mathsf{x}_k$ are assigned the values $x_1, \ldots, x_k$.

Presburger arithmetic derives its name from Mojźesz Presburger, who was the first to prove its decidability (as opposed to the first-order theory of arithmetic with multiplication, which is undecidable). Today, we have a much deeper understanding, of its expressiveness: The equivalence between semilinear sets and Presburger formulae has been discovered by Ginsburg and Spanier [1]. For a proof, please consult the lecture on Automata Theory.

Theorem E1.3 (Ginsburg and Spanier [1])**.** *A subset of $\mathbb{N}^k$ is definable by some Presburger formula if and only if it is semilinear.*

Now, forward inductive invariants are those semilinear sets with the property that membership is preserved by firing transitions. More precisely:

Definition E1.4. *Let $N = (S, T, W)$ be a Petri net. A semilinear set $A \subseteq \mathbb{N}^{|S|}$ is called an* forward inductive invariant *if for each $M \in A$ and $t \in T$, we have: If $M[t\rangle M'$, then $M' \in A$.*

We have already seen an example of a forward inductive invariant in the last lecture, namely those determined by structural invariants: If $I \in \mathbb{Z}^{|S|}$ is a structural invariant and $P \in \mathbb{Z}^{|S|}$ is any vector, we define

$$A_{I,P} = \{M \in \mathbb{N}^{|S|} \mid I^T \cdot M = P\}.$$

Then, Theorem 2.1 in section 2.2 tells us that if $M \in A_{I,P}$ and $M[t\rangle M'$, then $M' \in A_{I,P}$. Furthermore, it is easy to see that $A_{I,P}$ is Presburger definable and hence semilinear. Thus, $A_{I,P}$ is a forward inductive invariant.

What makes forward inductive invariants important is their completeness: As shown by Leroux [4], whenever a marking M_2 is unreachable from a marking M_1, there is a forward inductive invariant containing M_1, but not M_2.

Theorem E1.5 (Leroux [4])**.** *Let $N = (S, T, W)$ be a Petri net and $M_1, M_2 \in \mathbb{N}^{|S|}$ such that $M_2 \notin R(M_1)$. Then, there is a forward inductive invariant A such that $M_1 \in A$ and $M_2 \notin A$.*

Note that the converse of this theorem is immediate from the definition: If there is a forward inductive invariant A such that $M_1 \in A$ and $M_2 \notin A$, then M_2 is certainly unreachable from M_1.

Reachability in Petri nets. We will now see how to devise a very simple algorithm for the Petri net reachability problem using Theorem E1.5. Whether this problem is decidable at all had been a long-standing open problem in Theoretical Computer Science until the first solutions were proposed by Mayr [5] and Kosaraju [2]. A simplified proof has been presented by Lambert [3]. However, arguably the simplest algorithm known to date is the following by Leroux [4].

The only missing ingredient in the algorithm is a procedure to decide whether a given Presburger formula φ with $|S|$ free variables defines a forward inductive invariant. To this end, we use the fact that satisfaction of Presburger formulae is deciable. Given φ, we construct the new formula ψ with

$$\psi \equiv \forall M \in \mathbb{N}^{|S|} \forall M' \in \mathbb{N}^{|S|} \colon \left(\left(\varphi(M) \wedge \bigvee_{t \in T} M[t\rangle M' \right) \to \varphi(M') \right).$$

Here, of course, quantification over elements of $\mathbb{N}^{|S|}$ is actually one over $|S|$ variables. Moreover, by $\varphi(M)$, we denote the formula obtained by replacing the free variables of φ with the variables represented by M. By definition of forward inductive invariants, ψ is satisfied if and only if φ defines a forward inductive invariant. Hence, it is decidable whether a given Presburger formula defines a forward inductive invariant.

This allows us to formulate Algorithm E1.1. Note that its correctness (meaning: whenever it answers "reachable" or "unreachable", this answer is correct) is immediate from the definitions. Its completeness (meaning: it gives an answer for every input), on the other hand, follows from Theorem E1.5.

Algorithm E1.1 Petri net reachability using forward inductive invariants

```
input: Petri net $N = (S, T, W)$ and two markings $M_1, M_2 \in \mathbb{N}^{|S|}$
  $n \leftarrow 0$
  loop
    for each transition sequence $\sigma \in T^*$, $|\sigma| = n$:
      if $M_1[\sigma\rangle M_2$ then
        output "reachable"
        exit
      end if
    end
    for each Presburger formula $\varphi$ with $|S|$ free variables, $|\varphi| = n$:
      if $\varphi$ defines a forward inductive invariant and $M_1 \models \varphi$ and $M_2 \not\models \varphi$ then
        output "unreachable"
        exit
      end if
    end
    $n \leftarrow n + 1$
  end loop
```

References

[1] S. Ginsburg and E. H. Spanier. "Semigroups, Presburger Formulas, and Languages". In: *Pacific Journal of Mathematics* 16.2 (1966), pp. 285–296.

[2] S. R. Kosaraju. "Decidability of reachability in vector addition systems (preliminary version)". In: *Proceedings of the fourteenth annual ACM symposium on Theory of computing.* ACM. 1982, pp. 267–281.

[3] J.-L. Lambert. "A structure to decide reachability in Petri nets". In: *Theoretical Computer Science* 99.1 (1992), pp. 79–104.

[4] J. Leroux. "The General Vector Addition System Reachability Problem by Presburger Inductive Invariants". In: *Proceedings of the 24th Annual IEEE Symposium on Logic in Computer Science (LICS 2009).* 2009, pp. 4–13.

[5] E. W. Mayr. "An algorithm for the general Petri net reachability problem". In: *SIAM Journal on computing* 13.3 (1984), pp. 441–460.