

## Skeleton Abstraction for Universal Temporal Properties

Sophie Wallner\*, Karsten Wolf

University of Rostock, Germany

sophie.wallner@uni-rostock.de

---

**Abstract.** Uniform coloured Petri nets can be abstracted to their *skeleton*, the place/transition net that simply turns the coloured tokens into black tokens. A coloured net and its skeleton are related by a *net morphism* [1, 2]. For the application of the skeleton as an abstraction method in the model checking process, we need to establish a *simulation relation* [3] between the state spaces of the two nets. Then, universal temporal properties (properties of the *ACTL\** logic) are preserved. The abstraction relation induced by a net morphism is not necessarily a simulation relation, due to a subtle issue related to deadlocks [4]. We discuss several situations where the abstraction relation induced by a net morphism is as well a simulation relation, thus preserving *ACTL\** properties. We further propose a partition refinement algorithm for folding a place/transition net into a coloured net. This way, skeleton abstraction becomes available for models given as place/transition nets. Experiments demonstrate the capabilities of the proposed technology. Using skeleton abstraction, we are capable of solving problems that have not been solved before in the Model Checking Contest [5].

### 1. Introduction

In the model checking process for coloured Petri nets, one of the biggest issues is the state explosion problem, which makes the verification of a property impossible, as the state space is getting too big to handle. A way to deal with these big systems, is the well known technique of abstraction. Given a coloured Petri net  $C$ , we can form its *skeleton*  $S$ , which has the structure of  $C$  and simply decolours its components and tokens. This skeleton is an abstraction of the coloured net. To use this abstraction technique in the model checking process, we need to guarantee, that properties are preserved through this abstraction, i.e. that the validity of a property in  $S$  indicates the validity of the property in  $C$ .

---

\*Address for correspondence: University of Rostock, 18051 Rostock, Germany

Unfortunately, this is not the case for every coloured net. The issue is that some deadlocks of  $C$  are not preserved in  $S$ , as the additional behaviour of  $S$  changes the validity of the property. Deadlocks in a coloured net can have two different causes. First, they can be caused by an insufficient number of tokens in the preset of a transition. These deadlocks are preserved in the skeleton, as the number of tokens will neither be sufficient in the skeleton. Second, they can be caused by a wrong colour set of tokens, as the number of tokens in the preset of a transition is sufficient, but the colour distribution of the tokens violates the guard of the transition. This type of deadlocks is usually not preserved in the skeleton, as the skeleton does not distinguish colors at all. Consider the following example:

**Example 1.1.** Let  $C$  be a coloured Petri net, for which we build its skeleton  $S$  by removing the colour sets of the places, the guard of the transition and making the tokens all indistinguishable. The two nets are pictured in Figure 1. We consider the  $ACTL^*$  formula  $\varphi : \mathbf{AF} p \leq 1$ . The guard of the only transition  $t$  expresses that  $t$  requires three tokens of the same colour to be activated and then produces one token of this colour. In the given marking of  $C$ ,  $t$  is not enabled, so this marking is a deadlock. The corresponding marking of  $S$  is not a deadlock, as the number of tokens is sufficient and  $t$  is activated. Firing  $t$  in  $S$  leads to a marking, where all tokens are removed from  $p$ , so  $\varphi$  is true for  $S$ . However,  $\varphi$  is not true for  $C$ . Transferring the validity of  $\varphi$  from  $S$  to  $C$  will draw a wrong conclusion.

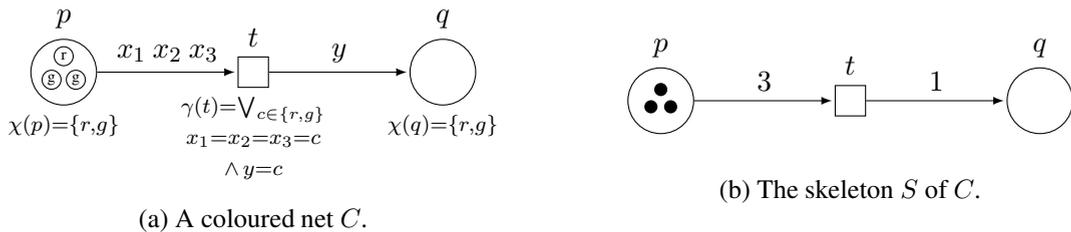


Figure 1: A coloured net  $C$  with a deadlock not preserved in its skeleton  $S$ .

This paper is an improved version of the conference paper [6] and gives a detailed analysis of situations, where the skeleton as an abstraction technique is soundly applicable in the model checking process for coloured Petri nets. With respect to [6], we improved the folding algorithm in Section 7.1 in a way, that it is now more liberal, i.e. the resulting coloured nets are smaller. The efficiency of this new folding algorithm is examined through new experiments. Overall, the more liberal folding algorithm helps to generate more results. We as well formalized the folding algorithm in Section 7.1 and added some explanation for this algorithm to make the construction more understandable. Furthermore, we extended the description of the automaton approach to check whether a transition class is full or not. We therefore introduced more formal definitions of the arc inscriptions and guards. This topic is now covered in an extra section (Section 6) in which we describe how to generate an automaton for terms resp. guard expressions and finally a transition class. This will make the process of checking fullness more understandable. Based on our new folding algorithm, Section 8 describes updated experimental results. The paper is structured as follows: The next Section 2 will give an overview of the application of skeleton nets in other contexts, Section 3 provides necessary basic definitions. After that, Section 4 will introduce the different concepts of relations, which can hold between reachability graphs of Petri

nets. Section 5 will set the focus on the simulation relation between reachability graphs as the core concept for keeping validity through abstraction. We present a survey, in which cases the skeleton is a valid abstraction method for a coloured Petri net, distinguishing different classes of nets and types of formulas. Section 6 provides an approach to check whether a coloured net has a deadlock-preserving skeleton; a property a net might fulfill to make the skeleton abstraction a valid verification extension. With the folding algorithm in Section 7, we extend the scope of application of the skeleton abstraction to place/transition nets. The experimental results in Section 8 underline the powerfullness of this abstraction method.

## 2. Related work

The idea of a skeleton-based analysis of a Petri net is subject of [7]. Based on this, [4] examines the role of deadlocks within this topic more precisely. The results are also applied in other contexts. In [8] extended Pr/T-Nets are used as a modeling formalism for embedded real-time systems due to the multitude of analysis methods for Petri nets. With the skeleton of a Pr/T-Net, properties like reachability of states or deadlock freeness can be examined. [9] transfers Findlow's results [4] to algebraic nets. They are used as an application for a folding construction, which is described there. Findlow's observations on deadlock-preserving skeletons are further used in [10] for a skeleton-based analysis of G-Nets, an object-based Petri net formalism. The preservation of predicates in temporal logic under morphisms has also already been discussed. [2] describes a rule-based modification of algebraic high-level nets extended with morphisms such that safety properties described in temporal logic are preserved. This provides a technique which allows to transfer safety properties between the source and the target net.

## 3. Basic definitions

First, we present definitions for place/transition nets.

### Definition 3.1. (Place/Transition Net)

A *place/transition net* (P/T net) is a tuple  $N = [P, T, F, W, m_0]$ , where  $P$  is a finite set of *places* and  $T$  is a finite set of *transitions* with  $P \cap T = \emptyset$ . The *arcs*  $F \subseteq (P \times T) \cup (T \times P)$  of the net are labeled by a *weight function*  $W : F \rightarrow \mathbb{N}$ , with  $W(x, y) = 0$  iff  $(x, y) \notin F$ . A marking is a mapping  $m : P \rightarrow \mathbb{N}$  and  $m_0$  is the *initial marking*.

The behavior of a P/T net is defined by the transition rule.

### Definition 3.2. (Transition rule of a P/T net)

Let  $N = [P, T, F, W, m_0]$  be a P/T net. Transition  $t \in T$  is enabled in marking  $m$  if  $\forall p \in P : W(p, t) \leq m(p)$ . Firing Transition  $t$  leads from marking  $m$  to marking  $m'$  (denoted as  $m \xrightarrow{t} m'$ ) in  $N$ , if  $t$  is enabled in  $m$  and  $\forall p : m'(p) = m(p) - W(p, t) + W(t, p)$ .

A marking  $m'$  is *reachable* from a marking  $m$  (denoted as  $m \xrightarrow{*} m'$ ), if there is a firing sequence  $t_1 t_2 \dots t_n \in T^*$ , such that  $m \xrightarrow{t_1} m_1 \xrightarrow{t_2} \dots \xrightarrow{t_n} m'$ . We extend the notation of reachability to

firing sequences  $\omega \in T^*$  and we call  $RS(N) = \{m \mid \exists \omega \in T^* : m_0 \xrightarrow{\omega} m\}$  the *reachability set*, which contains all of  $N$ 's reachable markings. Using the transition rule, a Petri net induces a labeled transition system, called the *reachability graph*.

**Definition 3.3. (Labeled Transition System, Reachability Graph)**

A *transition system*  $TS = [Q, q_0, R, A]$  is a labeled, directed graph, where  $Q$  is the set of *states*,  $q_0 \in Q$  is the initial state and a transition relation  $R \subseteq Q \times A \times Q$  with some set of actions  $A$ . The *reachability graph*  $R_N(m_0)$  of a Petri net  $N$  is a transition system, where the set of states is  $RS(N)$ ,  $m_0$  serves as the initial state and  $(m, t, m') \in R$  iff  $m \xrightarrow{t} m'$ .

Furthermore, we introduce a simple notion for coloured Petri nets with finite colour domains.

**Definition 3.4. (Coloured Petri net)**

A *coloured Petri net*  $C = [P_c, T_c, F_c, W_c, \chi, \gamma, m_{0c}]$  consists of a finite set  $P_c$  of *places*, a finite set  $T_c$  of *transitions* where  $P_c \cap T_c = \emptyset$  and a set of *arcs*  $F_c \subseteq (P_c \times T_c) \cup (T_c \times P_c)$ . The *weight function*  $W_c$  assigns a finite set of variables to each element of  $F_c$ . If  $(x, y) \notin F_c$ , we assume  $W_c(x, y) = \emptyset$ . The *colouring function*  $\chi$  assigns a finite set  $\chi(p)$  of colours to each place  $p \in P_c$ , called colour domain of  $p$ . The *guard function*  $\gamma$  assigns a boolean predicate  $\gamma(t)$  to each transition  $t \in T_c$ , which ranges over the variables of  $W_c(p, t) \cup W_c(t, p)$  for all  $p \in P_c$ . The initial marking  $m_0$  is a multiset over  $\chi(p)$  for every  $p \in P_c$ . The number of tokens of colour  $c$  on place  $p$  in marking  $m$  is described as  $m(p)(c)$ .

For a transition  $t \in T_c$ , we define a *firing mode* of  $t$  as a mapping  $g : \bigcup_{p \in P_c} (W_c(p, t) \cup W_c(t, p)) \rightarrow \bigcup_{p \in P_c} \chi(p)$ , which assigns a colour from  $\chi(p)$  for every place  $p \in P_c$  and for each variable  $x \in W_c(p, t) \cup W_c(t, p)$ . A firing mode  $g$  of a transition  $t$  satisfies the guard  $\gamma(t)$ , denoted as  $g \models \gamma(t)$ , if the assignment of colours to variables is a model of the guard.

Usually, definitions of coloured nets permit a richer syntax for arc weights and provide a more detailed description of the guard. In Chapter 6 we give more specific definitions for arc weights and guards; furthermore we present a solution how to simplify arc weights to variables without undermining expressivity. Until then, consider arc weights and guards as defined in the definition above.

For a coloured net, we define its unfolding.

**Definition 3.5. (Unfolding)**

Let  $C = [P_c, T_c, F_c, W_c, \chi, \gamma, m_{0c}]$  be a coloured Petri net. A P/T net  $U = [P_u, T_u, F_u, W_u, m_{0u}]$  is the *unfolding* of  $C$  if

- $P_u = \{[p, c] \mid p \in P_c, c \in \chi(p)\}$
- $T_u = \{[t, g] \mid t \in T_c, g \models \gamma(t)\}$
- $([p, c], [t, g]) \in F_u$ , iff  $(p, t) \in F_c$  and  $c \in g(W_c(p, t))$
- $([t, g], [p, c]) \in F_u$ , iff  $(t, p) \in F_c$  and  $c \in g(W_c(t, p))$
- $W_u([p, c], [t, g]) = \text{card}(\{x \mid x \in W_c(p, t), g(x) = c\})$
- $W_u([t, g], [p, c]) = \text{card}(\{x \mid x \in W_c(t, p), g(x) = c\})$
- $m_{0u}([p, c]) = m_{0c}(p)(c)$ .

In the sequel, refer to the transition system defined by a coloured net  $C$  as the transition system of its unfolding  $U$ , as they are isomorphic [11]. Coloured nets as defined above are *uniform*. This means that the number of tokens consumed or produced by a transition is independent of the particular firing mode, i.e. always  $\text{card}(W(x, y))$  tokens. There exist non-uniform variants of coloured nets. They use variables that take multisets over  $\chi(p)$  as values. They are, however, out of the scope of this article since the core artifact studied in this paper, the skeleton, is not applicable to non-uniform nets. For a uniform net, we can assign a second P/T net, its skeleton.

**Definition 3.6. (Skeleton)**

Let  $C = [P_c, T_c, F_c, W_c, \chi, \gamma, m_{0c}]$  be a coloured net. Its *skeleton*  $S = [P_s, T_s, F_s, W_s, m_{0s}]$  is a P/T net where

- $P_s = P_c, T_s = T_c, F_s = F_c$
- for all  $x, y \in P \cup T : W_s(x, y) = \text{card}(W_c(x, y))$
- for all  $p \in P : m_{0s}(p) = \sum_{c \in \chi(p)} m_{0c}(p)(c)$ .

The following example will help to understand the concepts of the unfolding and the skeleton of a coloured net.

**Example 3.7.** Let  $C$  be the given coloured Petri net, as depicted in Figure 2. Place  $p$  and  $q$  have the colour domain  $\chi(p) = \chi(q) = \{r, g, b\}$ . Unfolding  $C$  leads to the corresponding places  $[p, g], [p, r], [p, b]$  resp.  $[q, g], [q, r], [q, b]$ . For every firing mode, which satisfies the guard of transition  $t$ , we introduce one transition in the unfolding, so the unfolding has three transitions  $t_g, t_r, t_b$ . Building the skeleton makes all tokens on  $p$  indistinguishable and removes the colour sets of  $p$  and  $q$ . The transition  $t$  in the skeleton has no guard and is simply activated, if there is a sufficient number of tokens on  $p$ .

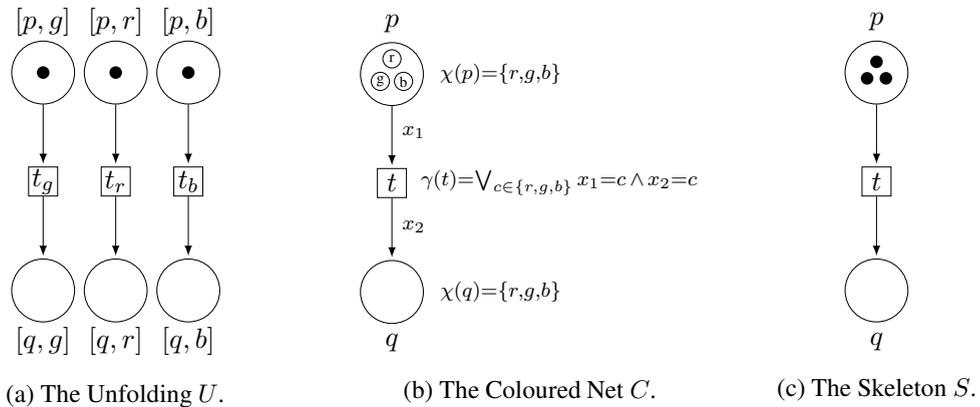


Figure 2: A coloured Petri net  $C$ , its unfolding  $U$  and its skeleton net  $S$ .

In the sequel, unless stated otherwise, let  $C$  be an arbitrary but fixed coloured net,  $U$  its unfolding, and  $S$  its skeleton.  $U$  and  $S$  are related by a net morphism.

**Definition 3.8. (Net Morphism [1])**

Let  $N_1 = [P_1, T_1, F_1, W_1, m_{01}]$  and  $N_2 = [P_2, T_2, F_2, W_2, m_{02}]$  be arbitrary P/T nets. A *net morphism* from  $N_1$  to  $N_2$  is a mapping  $\mu : (P_1 \cup T_1) \rightarrow (P_2 \cup T_2)$  such that  $\mu(P_1) \subseteq P_2$ ,  $\mu(T_1) \subseteq T_2$  and  $\forall x, y \in P_1 \cup T_1 : W(\mu(x), \mu(y)) = W(x, y)$ . For the initial markings, it holds that  $\forall p_2 \in P_2 : m_{02}(p_2) = \sum_{p_1 \in P_1 : (p_1, p_2) \in \mu} m_{01}(p_1)$ .

A net morphism can be extended to a mapping from markings of  $N_1$  to markings of  $N_2$  by setting  $m_2(p_2) = \sum_{p_1 \in P_1 : (p_1, p_2) \in \mu} m_1(p_1)$  for all  $p_2 \in P_2$ , where  $m_1 \in RS(N_1)$  and  $m_2 \in RS(N_2)$ . A net morphism preserves the reachability between the related nets.

**Lemma 3.9. (Net Morphism preserves reachability [12])**

Let  $N_1, N_2$  be two P/T nets, related by a net morphism  $\mu$ . The transition  $m \xrightarrow{t} m'$  in  $N_1$  implies the transition  $\mu(m) \xrightarrow{\mu(t)} \mu(m')$  in  $N_2$ .

It is easy to see that  $U$  and  $S$  are related by a net morphism.

**Lemma 3.10. (Net morphism from unfolding to skeleton [1, 2])**

Let  $C$  be a coloured Petri net,  $U$  its unfolding and  $S$  its skeleton. The mapping  $\mu : (P_U \cup T_U) \rightarrow (P_S \cup T_S)$  is a net morphism from  $U$  to  $S$ , where

- $\forall [p, c] \in P_U : \mu([p, c]) = p \in P_S$
- $\forall [t, g] \in T_U : \mu([t, g]) = t \in T_S$

The net morphism  $\mu$  between  $U$  and  $S$  can as well be extended to the markings of  $U$  and  $S$ , such as  $m_s(p) = \sum_{[p, c] \in P_U : ([p, c], p) \in \mu} m_u([p, c])$  for all  $p \in P_S$ , where  $m_u \in RS(U)$  and  $m_s \in RS(S)$ .

We continue with the introduction of the syntax and semantics of the temporal logic  $CTL^*$  [13]. The foundation for this logic are atomic propositions, properties which are either true or false in a given state.  $CTL^*$  distinguishes state formulas and path formulas.

**Definition 3.11. (Syntax of  $CTL^*$ )**

The temporal logic  $CTL^*$  is inductively defined as follows:

- every atomic proposition is a state formula
- if  $\varphi$  and  $\psi$  are state formulas, so are  $(\varphi \wedge \psi)$ ,  $(\varphi \vee \psi)$ , and  $\neg\varphi$
- every state formula is a path formula
- if  $\varphi$  and  $\psi$  are path formulas, so are  $(\varphi \wedge \psi)$ ,  $(\varphi \vee \psi)$ ,  $\neg\varphi$ ,  $\mathbf{X}\varphi$ ,  $\mathbf{F}\varphi$ ,  $\mathbf{G}\varphi$ ,  $(\varphi \mathbf{U}\psi)$ ,  $(\varphi \mathbf{W}\psi)$ , and  $(\varphi \mathbf{R}\psi)$
- if  $\varphi$  is a path formula then  $\mathbf{E}\varphi$  and  $\mathbf{A}\varphi$  are state formulas.

The semantics of  $CTL^*$  relies on the concept of paths in the considered system, given as a transition system.

**Definition 3.12. (Path,Suffix)**

Let  $TS = [Q, q_0, R, A]$  be a transition system. A *finite path* starting in state  $q_0$  is a sequence  $\pi = q_0 \dots q_n$  of states where  $\forall i \in \{0, \dots, n-1\} : (q_i, a, q_{i+1}) \in R$ . An *infinite path* starting in  $q_0$  is an infinite sequence  $\pi = q_0 q_1 \dots$  where  $\forall i \in \mathbb{N} : (q_i, a, q_{i+1}) \in R$ . A path is a finite or infinite path. A path is *maximal*, if it is infinite, or is a finite path  $q_1 \dots q_n$  where  $q_n$  is a *deadlock*, i.e. a state where, for all  $q \in Q$ ,  $(q_n, a, q) \notin R$ . As a *Suffix* of a path  $\pi$  we define  $\pi_i$  as the part of  $\pi$ , starting in  $q_i$ .

The semantics of  $CTL^*$  is defined on infinite paths, as we find them in *Kripke structures*. A Kripke structure is a transition system  $K = [Q, q_0, R, A, L]$  where  $R$  is total, i.e. every state has at least one successor state. Thus the maximal paths are always infinite here. Additionally, Kripke structures have a labelling function  $L : Q \rightarrow 2^{AP}$ , which assigns the set of atomic propositions to every state, which are true in this state. Every transition system can canonically be transformed into a Kripke structure by adding a *silent transition action*  $(q_d, \tau, q_d)$  to  $R$  for each deadlock state  $q_d$  of the system, which does not have a successor state. The semantics of  $CTL^*$  is defined by two satisfaction relations, both denoted with  $\models$ , that relate markings and state formulas resp. infinite paths and path formulas according to the following rules.

**Definition 3.13. (Semantics of  $CTL^*$ )**

Let  $K = [Q, q_0, R, A, L]$  be a Kripke structure. Let  $q \in Q$  be a state and  $\pi = q_0 q_1 \dots$  an infinite path of the system. Let further be  $\Pi(q)$  the set of paths starting from  $q$ . The satisfaction of a  $CTL^*$  formula is defined:

- For an atomic proposition  $\varphi$ : let  $q \models \varphi$  if  $\varphi \in L(q)$ .
- For a state formula  $\varphi$ :  $\pi \models \varphi$ , if  $q_0 \models \varphi$ .
- Boolean connectors:
  - $q \models \neg\varphi$ , if  $q \not\models \varphi$ ;  $\pi \models \neg\varphi$  if  $q_0 \not\models \varphi$
  - $q \models (\varphi \wedge \psi)$ , if  $q \models \varphi$  and  $q \models \psi$ ;  $\pi \models (\varphi \vee \psi)$  if  $\pi \models \varphi$  or  $\pi \models \psi$ .
- Temporal operators:
  - $\pi \models \mathbf{X} \varphi$ , if  $\pi_1 \models \varphi$
  - $\pi \models (\varphi \mathbf{U} \psi)$ , if  $\exists i \geq 0 : \pi_i \models \psi$  and  $\forall 0 \leq j < i : \pi_j \models \varphi$ .
- Path quantifier:  $q_0 \models \mathbf{E} \varphi$ , if  $\exists \pi \in \Pi(q_0) : \pi \models \varphi$ .

Let further  $\varphi \vee \psi$  be equivalent to  $\neg(\neg\varphi \wedge \neg\psi)$ ,  $\mathbf{F} \varphi$  to true  $\mathbf{U} \varphi$ ,  $\mathbf{G} \varphi$  to  $\neg \mathbf{F} \neg\varphi$ ,  $\varphi \mathbf{R} \psi$  to  $\neg(\neg\varphi \mathbf{U} \neg\psi)$ ,  $\varphi \mathbf{W} \psi$  to  $\mathbf{G} \varphi \vee (\varphi \mathbf{U} \psi)$  and  $\mathbf{A} \varphi$  to  $\neg \mathbf{E} \neg\varphi$ .

A Kripke structure satisfies a state formula if its initial states does. It satisfies a path formula if all paths starting in the initial state do. For  $CTL^*$ , several fragments are frequently studied.

**Definition 3.14. (Fragments of  $CTL^*$ )**

$CTL^*$  formula  $\varphi$  is in

- *LTL* if  $\varphi$  does neither contain  $\mathbf{E}$  nor  $\mathbf{A}$

- $ACTL^*$  if  $\varphi$  does neither contain  $\mathbf{E}$  nor  $\neg$
- $CTL$  if every occurrence of  $\mathbf{X}, \mathbf{U}, \mathbf{F}, \mathbf{G}, \mathbf{R}$  is immediately preceded by an occurrence of  $\mathbf{A}$  or  $\mathbf{E}$
- $ACTL$  if  $\varphi$  is in  $ACTL^*$  and  $CTL$
- for any fragment  $F$ ,  $\varphi$  is in the fragment  $F_X$  if  $\varphi$  is in  $F$  and does not contain  $\mathbf{X}$ .

Since  $CTL$  and  $LTL$  contain, for all their operators, the dual operator w.r.t negation, we can push negations to the bottom of formulas. Consequently,  $LTL$  is indeed a subset of  $ACTL^*$ .

## 4. Relations between reachability graphs

For describing relations between reachability graphs, we use the concepts of abstraction relation and simulation relation, defined for Kripke structures.

### Definition 4.1. (Abstraction Relation [3])

Let  $K = [Q, q_0, R, A, L]$  and  $\hat{K} = [\hat{Q}, \hat{q}_0, \hat{R}, \hat{A}, \hat{L}]$  be Kripke structures. An *abstraction relation* exists between  $K$  and  $\hat{K}$ , if there is a surjective abstraction function  $\sigma : Q \rightarrow \hat{Q}$ , for which it holds that for every  $\hat{q} \in \hat{Q}$  and  $\forall a \in AP : \hat{q} \models a \Leftrightarrow \forall q \in Q$  with  $(q, \hat{q}) \in \sigma : q \models a$ .

If such an abstraction relation exists between  $K$  and  $\hat{K}$ , we say that  $\hat{K}$  (abstract system) abstracts  $K$  (concrete system). A particular type of abstraction relation is the simulation relation.

### Definition 4.2. (Simulation Relation [14])

An abstraction relation between  $K = [Q, q_0, R, A, L]$  and  $\hat{K} = [\hat{Q}, \hat{q}_0, \hat{R}, \hat{A}, \hat{L}]$  with the abstraction function  $\sigma : Q \rightarrow \hat{Q}$  is a *simulation relation*, if  $\forall q, q_1 \in Q : q \xrightarrow{*} q_1$  and  $(q, \hat{q}) \in \sigma \rightarrow \exists \hat{q}_1 \in \hat{Q} : \hat{q} \xrightarrow{*} \hat{q}_1$  for  $\hat{q} \in \hat{Q}$  and  $(q_1, \hat{q}_1) \in \sigma$ .

If a simulation relation exists between  $K$  and  $\hat{K}$ , we say that  $\hat{K}$  simulates  $K$ .  $ACTL^*$  properties are preserved through a simulation relation.

### Lemma 4.3. (Simulation Relation preserves $ACTL^*$ [13])

Let  $K = [Q, q_0, R, A, L]$  and  $\hat{K} = [\hat{Q}, \hat{q}_0, \hat{R}, \hat{A}, \hat{L}]$  be Kripke structures. If there is a simulation relation between  $K$  and  $\hat{K}$ , for every  $ACTL^*$  formula  $\varphi$ , it holds that  $\hat{K} \models \varphi \Rightarrow K \models \varphi$ .

As deadlocks may occur in Petri nets, a reachability graph is not necessarily a Kripke structure. To make the concepts of abstraction and simulation formally applicable to Petri nets, we need to transform the reachability graphs into Kripke structures, as described above. Thus, for every deadlock marking  $m_d$  in a reachability graph, we add a self-loop  $(m_d, \tau, m_d)$  with a silent transition  $\tau$  to  $R$ . From now on, consider the reachability graphs of Petri nets as Kripke structures, arose out of this transformation. For an abstraction relation, atomic propositions are essential, so we first specify atomic propositions in the context of Petri nets.

**Definition 4.4. (Atomic proposition)**

Let  $N$  be a Petri net. An *atomic proposition* is an expression  $k_1 p_1 + \dots + k_n p_n \leq k$ , for some  $n \in \mathbb{N}$  with  $k_1, \dots, k_n, k \in \mathbb{Z}$ , and  $p_1, \dots, p_n \in P$ , where  $P$  is the set of places of  $N$ . A marking  $m$  of a P/T net *satisfies* the proposition  $k_1 p_1 + \dots + k_n p_n \leq k$ , iff the term  $\sum_{i=1}^n k_i \cdot m(p_i)$  evaluates to a number less than or equal to  $k$ . A marking  $m$  of coloured net *satisfies* proposition  $k_1 p_1 + \dots + k_n p_n \leq k$ , iff the term  $\sum_{i=1}^n k_i \cdot \sum_{c \in \chi(p_i)} m(p_i)(c)$  evaluates to a number less than or equal to  $k$ . For both,  $m \models a$  denotes the fact that  $m$  satisfies atomic proposition  $a$ .

The net morphism  $\mu : (P_U \cup T_U) \rightarrow (P_S \cup T_S)$  between the unfolding  $U$  of a coloured net  $C$  and its skeleton  $S$  induces an abstraction relation between their reachability graphs. To show this, we need to specify the unfolding of atomic propositions of coloured nets. As  $S$  resp.  $C$  normally have another set of places as  $U$ , the equisatisfiability between the concrete and the abstract states, required in Definition 4.1, is not trivial.

**Definition 4.5. (Unfolding of Atomic Propositions)**

Let  $\mu : (P_U \cup T_U) \rightarrow (P_S \cup T_S)$  be the net morphism between  $U$  and  $S$ . Let  $a_C \in AP_C$  an atomic proposition of a coloured net  $C$ . Proposition  $a_C$  can be unfolded to an atomic proposition  $a_U \in AP_U$  by substituting every occurrence of any place  $p \in P_C$  by  $\sum_{[p,c] \in P_U: \mu([p,c])=p} [p, c]$ .

An atomic proposition  $a_C$  and its unfolding  $a_U$  are equisatisfiable. To make the unfolding of atomic propositions more clear, consider example 1.1 and the atomic proposition  $p \leq 3$ . As the colour domain of  $p$  is  $\chi(p) = \{g, r, b\}$  and  $p$  would be unfolded to the places  $[p, g]$ ,  $[p, r]$ , and  $[p, b]$ , we unfold the atomic proposition to  $[p, g] + [p, r] + [p, b] \leq 3$ .

With the definition of atomic propositions and their unfolding we can build an abstraction relation between the unfolding of a coloured net and its skeleton.

**Theorem 4.6. (Abstraction Relation between  $U$  and  $S$ )**

Let  $U$  and  $S$  be related by the net morphism  $\mu : (P_U \cup T_U) \rightarrow (P_S \cup T_S)$  from proposition 3.10. The extension of  $\mu$  on the markings of  $U$  and  $S$  yields to a surjective abstraction function  $\sigma$  with  $(m_U, m_S) \in \sigma$  for  $(m_U, m_S) \in \mu$ . Therefore, an abstraction relation between the markings of  $U$  and  $S$  exists.

It is worth mentioning that markings here include reachable and non-reachable markings.

**Proof:**

Let  $a_U \in AP_U$ ,  $a_C \in AP_C$  and  $a_S \in AP_S$  be atomic propositions. The relation  $\sigma$  is an abstraction relation indeed, if for a marking  $m_S$  of  $S$ ,  $m_S \models a_S \Leftrightarrow \forall m_U \models a_U$  with  $(m_U, m_S) \in \sigma$ . If  $m_S \models a_S$ , then  $\sum_{i=1}^n k_i \cdot m_S(p_i) \leq k$ . For every corresponding marking  $m_C$  of  $C$ , it holds that  $m_C \models a_C$ , as  $m_S(p_i) = \sum_{c \in \chi(p_i)} m_C(p_i)(c)$  for every  $i \in \{1, \dots, n\}$  and so,  $\sum_{i=1}^n k_i \cdot \sum_{c \in \chi(p_i)} m_C(p_i)(c) \leq k$ . Notice that  $m_C$  may be unreachable. As the corresponding markings of the unfoldings are equisatisfiable, for every  $m_U$  of  $U$ , it holds that  $m_U \models a_U$ . Reversed, it must hold that if for a marking  $m_S$  with  $m_S \not\models a_S$ , there is a marking  $m_U$  with  $(m_U, m_S) \in \sigma$ , for which it holds that  $m_U \not\models a_U$ . Let  $\sum_{i=1}^n k_i \cdot m_S(p_i) > k$ . For the marking  $m_C$  also holds that  $m_C \not\models a_C$ . This  $m_C$  might be unreachable again. We can see, that for  $m_U, m_U \not\models a_U$  as well.  $\square$

The existence of an abstraction relation is not sufficient for transferring the validity results on the markings of  $S$  to  $U$ . We need in fact a simulation relation. A simulation  $\sigma$  requires the preservation of the transitions between the simulating systems, so it should hold that  $\forall m_U, m_{U1} \in RS(U) : m_U \xrightarrow{*} m_{U1}$  and  $(m_U, m_S) \in \sigma \Rightarrow \exists m_{S1} \in RS(S) : m_S \xrightarrow{*} m_{S1}$  and  $(m_{U1}, m_{S1}) \in \sigma$  for  $m_S \in RS(S)$ . As the coloured net may have deadlocks, which are not preserved in the skeleton as shown in the opening example, there may be silent transitions at the deadlock states of  $U$ , which are not preserved in the skeleton  $S$ . Let  $m_U \in RS(U)$  be a deadlock of  $U$  not preserved in  $S$ , so  $m_U \xrightarrow{\tau} m_U$ . Let  $m_S \in RS(S)$  be the corresponding marking of  $S$  with  $(m_U, m_S) \in \sigma$ . Since  $m_S$  is not a deadlock, there is no silent transition added for  $m_S$  and consequentially, there is no marking  $m_{S1} \in RS(S)$  with  $m_S \xrightarrow{*} m_{S1}$  and  $(m_U, m_{S1}) \in \sigma$ , as  $m_U, m_{S1}$  do not fulfill atomic propositions equally.

## 5. Simulation relation between reachability graphs

In this section, we discuss the existence of a simulation relation between the unfolding and the skeleton under various conditions. As mentioned above, deadlocks that are not preserved in the skeleton, may cause problems. We therefore distinguish coloured nets, where

- a) no deadlocks occur at all (Section 5.1),
- b) all deadlocks are preserved in the skeleton (Section 5.2),
- c) deadlocks are not always preserved. (Section 5.3)

The kind of the  $ACTL^*$  formula is significant as well.  $ACTL^*$  safety properties permit the use of the skeleton approach even if deadlocks are not preserved, as shown in Section 5.4.

### 5.1. Deadlock-free nets

When the net  $C$  resp.  $U$  has no deadlocks, the net morphism directly leads to a simulation relation between the markings of  $U$  and  $S$ . There is no need to add silent transitions in  $U$  that are not preserved in  $S$ .

**Theorem 5.1.** Let  $C$  be a coloured net without deadlocks,  $U$  its unfolding and  $S$  its skeleton. The net morphism  $\mu : (P_U \cup T_U) \rightarrow (P_S \cup T_S)$  from Lemma 3.10 induces a simulation relation between the markings of  $U$  and  $S$ .

#### Proof:

The reachability graph  $R_U(m_0)$  is a Kripke structure, without adding silent transitions. Let  $m_U, m_{U1} \in RS(U)$  and  $m_S \in RS(S)$  be the corresponding marking of  $m_U$  with  $(m_U, m_S) \in \mu$ . The markings  $m_U$  and  $m_S$  are then related by the abstraction relation  $\sigma$  from Theorem 4.6:  $(m_U, m_S) \in \sigma$ . Because net morphisms preserve reachability, for  $t_U \in T_U$ , if it holds that if  $m_U \xrightarrow{t_U} m_{U1}$  in  $R_U(m_0)$ , then there is a marking  $m_{S1} \in RS(S)$  with  $m_S \xrightarrow{\mu(t_U)} m_{S1}$  in  $R_S(m_0)$ , for which  $(m_{U1}, m_{S1}) \in \mu$ . Consequently, for all markings  $m_U, m_{U1} \in RS(U)$  with  $m_U \xrightarrow{*} m_{U1}$  and  $(m_U, m_S) \in \sigma$ , there is a marking  $m_{S1} \in RS(S)$  with  $m_S \xrightarrow{*} m_{S1}$  in  $R_S(m_0)$  and  $(m_{U1}, m_{S1}) \in \sigma$ .  $\square$

Thus, according to proposition 4.3,  $ACTL^*$  properties are preserved. If we can guarantee, that the considered net is deadlock-free, the skeleton abstraction can be used for transferring positive results of an  $ACTL^*$  verification in  $S$  to  $U$ .

## 5.2. Deadlock preservation

We now consider the case where a Petri net has deadlocks. The reachability graph of this net is not readily a Kripke structure, hence all deadlock states were extended with a self loop with a silent action. In [4], two necessary and sufficient criteria are formulated, defining a class of coloured Petri nets which have a *deadlock-preserving skeleton*.

This means that every dead marking of the coloured net has a dead skeletal image, thus no deadlock of the coloured net is invisible in the skeleton. By that it is possible to detect all deadlocks just by the skeletal analysis. The two criteria have both characteristic advantages for our skeleton-based analysis and verification. The first criterion relates to an equivalence relation of the transitions of the coloured net. The second one concerns the liveness of markings. To determine, whether a given coloured Petri net has a deadlock-preserving skeleton, it is appropriate to use the first criterion, as it refers exclusively to the net structure and does not consider the behaviour of the net.

As we assume that the coloured net  $C = [P_c, T_c, F_c, W_c, \chi, \gamma, m_{0c}]$  is uniform, the number of input tokens a transition  $t \in T_c$  requires from each place  $p_i$  for  $i \in \{1, \dots, n\}$  with  $n = |P_c|$  is unambiguous. From now on, this number of input tokens for a transition  $t$  is denoted as  $f_i(t)$ , where  $f_i(t) = |W_c(p_i, t)|$  for  $i \in \{1, \dots, n\}$ . These numbers form an input vector  $f : T \rightarrow \mathbb{N}^n$  for every transition  $t \in T_c : f(t) = (f_1(t), f_2(t), \dots, f_n(t))$ . Building on that, we can determine a preorder  $(T_c, \lesssim)$  of the transitions of  $C$ , such that  $\forall t, t' \in T_c : t \lesssim t'$ , iff  $f(t) \leq f(t')$ . This leads to an equivalence relation  $\sim$  on  $T_c$ , such that  $\forall t, t' \in T_c : t \sim t'$ , iff  $f(t) = f(t')$ . Transitions with an identical input are aggregated in one equivalence class of this equivalence relation. Let  $T_c/\sim$  be the set of equivalence classes of  $T_c$ . The preorder  $(T_c, \lesssim)$  induces a partial order  $(T_c/\sim, \leq)$  on the equivalence classes, such that  $\forall [t], [t'] \in T_c/\sim : [t] \leq [t']$ , iff  $t \lesssim t'$ .

### Definition 5.2. (Full Transition Class)

An equivalence class  $[t] \in T_c/\sim$  is *full*, if for every marking  $m_c$  of  $C$  with  $|m_c(p_i)| = f_i(t)$  for all  $i \in \{1, \dots, n\}$ , there is a transition  $t \in [t]$  that is enabled in  $m_c$ .

In other words,  $[t]$  is full, if any collection of bags matching the input size requirements of  $[t]$  also matches the input colour distribution requirements of one transition  $t \in [t]$  of this equivalence class. This leads to the following lemma:

### Lemma 5.3. (Deadlock-Preserving Skeleton [4])

Let  $C$  be a uniform, coloured Petri net.  $C$  has a deadlock-preserving skeleton, iff every minimal transition class of  $C$  regarding  $(T_c/\sim, \leq)$  is full.

This is a necessary and sufficient condition. With this criterion, we can show that the simulation relation between a coloured net and its skeleton is preserved for a subclass of coloured nets, which have a deadlock-preserving skeleton. If the criterion holds, the net morphism  $\mu : (P_v \cup T_v) \rightarrow (P_s \cup T_s)$  induces a simulation relation. If a coloured net has a deadlock-preserving skeleton, for every added

silent transition for a dead marking  $m_v \in RS(U)$  of  $U$ , there is an added silent transition for the dead skeletal image  $m_s \in RS(S)$  with  $(m_v, m_s) \in \mu$  as well. With regard to Lemma 4.3, we can verify the  $ACTL^*$  properties only in  $S$  without risking wrong conclusions about the behavior of  $C$ .

### 5.3. Inject deadlocks to skeleton

The main focus of this section are nets with deadlocks, but without deadlock-preserving skeleton. Here, the net morphism does not induce a simulation relation, so the  $ACTL^*$  results cannot be transferred directly from the skeleton to the coloured net. We present an approach to modify the skeleton net such that every deadlock of the unfolding occurs in the new skeleton, but potentially with some delay. In this case we cannot guarantee that every dead marking has a dead skeletal image, but we can at least guarantee that for a dead marking, the corresponding skeletal deadlock occurs after a finite number of actions.

#### Definition 5.4. (Modified Skeleton Net)

Let  $C = [P_c, T_c, F_c, W_c, \chi, \gamma, m_{0c}]$  be a uniform coloured net. The *modified skeleton*  $S'$  can be constructed from the skeleton  $S$  as, for every preset place  $p \in P_c$  of a non-full minimal transition class  $[t]$ , a complement place  $\bar{p}$  and a recipient transition  $t_r$  with  $\bullet t_r = \{p\}$  and  $t_r \bullet = \{\bar{p}\}$  are introduced with  $W(p, t_r) = W(t_r, \bar{p}) = 1$ . Apart from that,  $S'$  and  $S$  are identical.

The modified skeleton has another behaviour than the original skeleton. Every recipient transition  $t_r$  can successively empty its preset place  $p$  and stores the tokens on the complement place  $\bar{p}$ . These actions can be considered as silent actions of  $S'$ . Once a token is stored on  $\bar{p}$ , it cannot leave this place anymore. So, after a finite number of actions of the recipient transitions, the preset of  $[t]$  is empty and the transitions in  $[t]$  cannot fire anymore. The deadlock of  $U$  occurs in  $S'$  after a finite number of silent actions of the recipient transitions. Between  $U$  and  $S'$  a stuttering simulation holds, which is a weakened version of a simulation relation. The next definition talks about partitions of infinite paths. A partition of a path  $\pi$  consists of finite or infinite subpaths  $B_i$ , such that their concatenation yields the whole  $\pi$ .

#### Definition 5.5. (Stuttering Simulation [15])

Let  $K = [Q, q_0, R, A, L]$  and  $\hat{K} = [\hat{Q}, \hat{q}_0, \hat{R}, \hat{A}, \hat{L}]$  be Kripke structures and  $a$  be an atomic proposition. A mapping  $\sigma_s : Q \rightarrow \hat{Q}$  is a *stuttering simulation relation* if the following conditions hold:

- $(q_0, \hat{q}_0) \in \sigma_s$
- $(q, \hat{q}) \in \sigma_s \Rightarrow q \models a \Leftrightarrow \hat{q} \models a$  and for every path  $\pi = q_0 q_1 q_2 \dots$  of  $K$ , there is a path  $\hat{\pi} = \hat{q}_0 \hat{q}_1 \hat{q}_2 \dots$  of  $\hat{K}$ , such that we can find partitions  $B_0, B_1, B_2, \dots$  for  $\pi$  resp.  $\hat{B}_0, \hat{B}_1, \hat{B}_2, \dots$  for  $\hat{\pi}$  for which holds that:
  - $\forall i \geq 0 : B_i, \hat{B}_i$  are not empty and finite
  - every state of  $\hat{B}_i$  is related with every state of  $B_i$  by  $\sigma_s$ .

If two systems are related by a stuttering simulation, the behaviour of the concrete system  $K$  is simulated by the abstract system  $\hat{K}$ , but  $\hat{K}$  can run internal silent actions while simulating. Between

the unfolding and the modified skeleton, we can observe this stuttering simulation. To prove this, we first need to establish a relation between the markings of  $U$  and  $S'$ . Therefore, we create a relation between the markings of  $S$  and the markings of  $S'$ . A Marking  $m_s$  of  $S$  and a marking  $m_{s'}$  of  $S'$  are related, if

- $m_s(p) = m_{s'}(p) + m_{s'}(\bar{p})$  for  $p \in \bullet[t]$ , where  $[t]$  is a non-full minimal transition class
- $m_s(p) = m_{s'}(p)$  otherwise.

The relation between a marking  $m_u$  and a marking  $m_{s'}$  can then be established by composing the abstraction relation from  $m_u$  to  $m_s$  and with the one just defined. Thus, the relation between the markings of  $U$  and  $S'$  is an abstraction relation. The silent actions of the recipient transitions move the tokens of the preset places to their complementary places. No matter if they have moved one or all tokens, the sum over the places  $p$  and  $\bar{p}$  is always invariant.

**Theorem 5.6. (Stuttering Simulation between  $U$  and  $S'$ )**

Let  $C$  be a uniform coloured net,  $U$  its unfolding and  $S'$  its modified skeleton. Between the markings of  $U$  and  $S'$ , a stuttering simulation  $\sigma_s$  holds.

**Proof:**

The definition of the marking guarantees, that an abstraction relation exists between the markings of  $U$  and  $S'$ . States, which are related by the  $\sigma_s$ , fulfill atomic propositions equally. Between the initial markings  $m_{0U}$  and  $m_{0S'}$  the stuttering simulation holds. Now consider the path  $\pi_U = m_{1U}m_{2U} \dots$  of  $U$  and the corresponding path  $\pi_{S'} = m_{1S'}m_{2S'} \dots$  of  $S'$ , where  $(m_{iU}, m_{iS'}) \in \mu$  for all  $i$ . The partitioning of  $\pi_U$  and the corresponding path  $\pi_{S'}$  in  $S'$  is obtained as follows: For a marking  $m_{iU}$  of path  $\pi_U$ , which is not a deadlock, the corresponding part of  $\pi_{S'}$  is simply  $m_{iS'}$  with  $(m_{iU}, m_{iS'}) \in \sigma_s$ . The partitioning of the paths for this parts is trivial:  $B_{iU} = \{m_{iU}\}$  resp.  $B_{iS'} = \{m_{iS'}\}$ . Let now be  $m_{iU}$  a deadlock, which is only followed by the self-loop- $\tau$ -actions. The corresponding marking  $m_{iS'}$  is not necessarily a deadlock. Firing the recipient transitions in  $m_{iS'}$  yields to a sequence  $\tau^*$  which ends in a deadlock marking  $m_{dS'}$ , where only the self-loop- $\tau$ -action is possible as well. For partitioning,  $B_{iU}$  contains only the deadlock state  $m_{iU}$  of  $U$ .  $B_{iS'}$  contains the states  $m_{iS'}, m_{i+1S'}, m_{i+2S'}, \dots, m_{dS'}$ , where  $m_{i+1S'}, m_{i+2S'}, \dots$  are the markings, reached by actions of the recipient transitions and  $m_{dS'}$  is the delayed deadlock marking. All states in  $B_{iS'}$  have the same validity of atomic propositions and so they can be related with  $m_{iU}$  by  $\sigma_s$ . So, between  $U$  and  $S'$  a stuttering simulation holds.  $\square$

A stuttering simulation preserves  $ACTL_X^*$  properties.

**Lemma 5.7. (Stuttering simulation preserves  $ACTL_X^*$  [15])**

Let  $K = [Q, q_0, R, A, L]$  and  $\hat{K} = [\hat{Q}, \hat{q}_0, \hat{R}, \hat{A}, \hat{L}]$  be Kripke structures, which are related by a stuttering simulation. Then  $\hat{K} \models \varphi \Rightarrow K \models \varphi$  for any  $ACTL_X^*$  formula  $\varphi$ .

$ACTL_X^*$  formulas permit claims about the overall behaviour of the system, except for referring to next states. The silent actions in the abstract system can generate new next states, which replace the actual simulating next state. Because of this, assumptions on next states can be falsified, which explains the restriction to  $ACTL_X^*$ . Nevertheless, the validity of at least a subset of  $ACTL^*$  formulas can be transferred from the modified skeleton to the unfolding.

## 5.4. Safety properties

In the context of net morphisms, safety properties make an exception with regard of their validation.

### Definition 5.8. (Safety Property [16])

An  $ACTL^*$  property is a *safety property*, if only the temporal operators **W**, **X** and the path quantifier **A** occur.

We claim that a safety property  $\varphi$  is preserved by a net morphism even if that morphism does not induce a simulation relation. In the context of the skeleton abstraction, the abstraction relation between the markings of  $U$  and  $S$  is sufficient for the preservation of  $ACTL^*$  safety formulas. This fact was already informally mentioned in [2]. However, that paper did not precisely define the class of properties and did not prove the claim.

### Theorem 5.9. (Net Morphisms preserve $ACTL^*$ Safety Properties)

Let  $C$  be a coloured net,  $U$  its unfolding and  $S$  its skeleton. Let  $\mu : (P_U \cup T_U) \rightarrow (P_S \cup T_S)$  a net morphism,  $\varphi_s$  an  $ACTL^*$  safety property and  $\varphi_U$  its unfolding after Definition 4.5. Let  $m$  be a marking of  $U$ . Then it holds that:  $\mu(m) \models \varphi_s \Rightarrow m \models \varphi_U$ .

#### Proof:

We prove the contraposition  $m \not\models \varphi_U \Rightarrow \mu(m) \not\models \varphi_s$  by induction on the structure of  $\varphi_U$ .

*Base:* If  $m \not\models \varphi_U$ , then  $\mu(m) \not\models \varphi_s$ , corresponding to Definition 4.1.

*Step:* We therefore distinguish between the possible structures of  $\varphi_U$  and  $\varphi_s$ :

1.  $\varphi_U = \psi_U \wedge \xi_U$  resp.  $\varphi_U = \psi_U \vee \xi_U$ : the induction hypothesis can directly be applied to  $\psi_U$  and  $\xi_U$ .
2.  $\varphi_U = \mathbf{A}\psi_U$ : If  $m \not\models \varphi_U$ , there is a path  $\pi = m m_1 m_2 \dots$  with  $\pi \not\models \psi_U$ . Because reachability is preserved, there is a path  $\mu(\pi) = \mu(m)\mu(m_1)\mu(m_2)\dots$  with  $\mu(\pi) \not\models \psi_s$ . So,  $\mu(m) \not\models \mathbf{A}\psi_s$  resp.  $\mu(m) \not\models \varphi_s$ .
3.  $\varphi_U = \mathbf{A}\mathbf{X}\psi_U$ : If  $m \not\models \varphi_U$ , there is a path  $\pi = m m_1 m_2 \dots$  where  $m_1 \not\models \psi_U$ . For the skeleton, there is a path  $\mu(\pi) = \mu(m)\mu(m_1)\mu(m_2)\dots$  where  $\mu(m_1) \not\models \psi_s$ . So,  $\mu(m) \not\models \mathbf{A}\mathbf{X}\psi_s$  resp.  $\mu(m) \not\models \varphi_s$ .
4.  $\varphi_U = \mathbf{A}\psi_U \mathbf{W}\xi_U$ , which is the disjunction between
  - a)  $\varphi_U = \mathbf{A}\mathbf{G}\psi_U$ : If  $m \not\models \mathbf{A}\mathbf{G}\psi_U$ , there is a path  $\pi = m m_1 m_2 \dots$  with a marking  $m_i \not\models \psi_U$ . Hence,  $\pi \not\models \mathbf{G}\psi_U$ . Again, the preservation of reachability leads to a path  $\mu(\pi) = \mu(m)\mu(m_1)\mu(m_2)\dots$  with a marking  $\mu(m_i) \not\models \psi_s$ . So,  $\mu(\pi) \not\models \mathbf{G}\psi_s$  and thus  $\mu(m) \not\models \mathbf{A}\mathbf{G}\psi_s$ ;
  - b)  $\varphi_U = \mathbf{A}\psi_U \mathbf{U}\xi_U$ : If  $m \not\models \mathbf{A}\psi_U \mathbf{U}\xi_U$  there is a path  $\pi = m m_1 m_2 \dots$  with  $\pi \not\models (\psi_U \mathbf{U}\xi_U)$ . This is possible in two different ways: On the one hand, for all  $i \geq 0 : m_i \not\models \xi_U$  can hold, hence  $\pi \not\models \mathbf{G}\xi_U$ . This can be treated analogously to case 4.a). On the other hand, there might be a  $m_i \models \xi_U$ , but there is also a  $m_j$  with  $j < i$  and  $m_j \not\models \psi_U$ . Then, there is a path  $\mu(\pi) = \mu(m)\mu(m_1)\mu(m_2)\dots$  with  $\mu(m_i) \models \xi_s$  and  $\mu(m_j) \not\models \psi_s$  as well. Hence, it holds  $\mu(m) \not\models \mathbf{A}\psi_s \mathbf{U}\xi_s$ .

In both cases,  $\mu(m) \not\models \varphi_s$ .

The invalidity of  $\varphi_v$  can always be proven with a finite counterexample path. Deadlocks may just occur in the last marking of this path. Let  $m_i$ , the last marking of the counterexample were we can see the invalidity of  $\varphi_v$ , be a deadlock. Because we consider Kripke structures, every path of the system is infinite. The counterexample path  $\pi$  is therefore continued to an infinite path  $\pi = m m_1 m_2 \dots m_i m_i m_i \dots$  by repeating the deadlock state  $m_i$ . This repetition does not change the finiteness of the counterexample. If the deadlock  $m_i$  is preserved in the skeleton, this leads to an corresponding path  $\mu(\pi)$  with repetitions as well:  $\mu(\pi) = \mu(m)\mu(m_1)\mu(m_2) \dots \mu(m_i)\mu(m_i)\mu(m_i) \dots$ . The invalidity of  $\varphi_s$  remains unchanged. If the deadlock is not preserved, the path  $\mu(\pi)$  has another sequel:  $\mu(\pi) = \mu(m)\mu(m_1)\mu(m_2) \dots \mu(m_i)\mu(m_{i+1})\mu(m_{i+2}) \dots$  with  $\mu(m_{i+1}) \neq \mu(m_i)$ . The counterexample is transferred exactly up to and including  $m_i$ , the markings  $\mu(m_{i+1})\mu(m_{i+2}) \dots$  do not change the invalidity of  $\varphi_s$ .  $\square$

## 6. Checking full transition classes in symmetric nets

We proceed with an algorithmic approach to check whether a transition class is full. A brute-force solution would be to enumerate all firing modes of the transitions in the class and to check whether these firing modes cover all distributions of colors on their pre-places as stated in Definition 5.2. This approach may be very inefficient, as already observed in [17]. It would in particular prevent the application of the skeleton approach to colored nets that have an unfolding too large to be constructed. Following the approach of [17], we rather create an automaton that accepts precisely those assignments to the variables on the arcs to resp. from transition  $t$ , which are firing modes of  $t$ , i.e. that satisfy the guard  $\gamma(t)$ . We therefore assume the set of all variables to be ordered. Then an assignment to the variables  $x_{i_1}, \dots, x_{i_n}$  with  $x_{i_j} < x_{i_k}$ , for  $j < k$ , is a sequence of length  $n$  and the  $j$ -th element of the sequence is in the domain of variable  $x_{i_j}$ . A set of assignments to some set of variables is a set of sequences, all having same length. The domains of the variables serve as alphabet for these sequences. We adapt the concept of classical finite automata to this setting.

### Definition 6.1. (Automaton)

Given a coloured net  $C$ , a finite automaton  $[X, Q, q_0, \delta, F]$  consists of a set  $X$  of all variables occurring in  $C$ , a finite set  $Q$  of states, an initial state  $q_0 \in Q$ , a set  $F$  of final states ( $F \subseteq Q$ ), and a deterministic transition function  $\delta : Q \times D \rightarrow Q$ , where  $D$  is the union of all domains for the variables in  $X$ .

With this definition, we permit an assignment of the variables of  $X$  with elements from the domain  $D$  as an input for our automaton. The domain for a variable  $x$  on arc  $F_c(p, t)$  resp.  $F_c(t, p)$  is the colour domain  $\chi(p)$  of place  $p$ . As usual, a sequence is accepted if a run starting in  $q_0$  with this sequence ends in a final state.

In the sequel, we show how to construct an automaton that accepts the enabled firing modes of a transition. The resulting automaton can then be used to represent all distributions of tokens that can be consumed by this transition. This information can finally be combined for all transitions of a transition class for checking whether it is full. For constructing the automaton, we first need to consider the arc inscriptions and the guards more precisely. We therefore choose the syntax of *symmetric high level nets*, also known as stochastic well formed nets [18] although our approach may be easily adapted to other dialects of high-level nets. The syntax of symmetric nets is simple and reasonably formalized in

the PNML standard [19]. All high-level nets in the yearly model checking contests [20] are modeled as symmetric nets. Until now, we only suppose the arc inscriptions as a finite set of variables and the guard as a boolean predicate, which can be evaluated to true or false.

In detail, for symmetric nets, arc inscriptions are formal sums of terms or tuples of terms. They have a rather restricted syntax for terms.

**Definition 6.2. (Term)**

Let  $X$  be a set of variables and  $\mathbb{Z}$  the set of integers. A *term* can be

- a variable  $x \in X$ ,
- a constant  $k \in \mathbb{Z}$ , or
- an increment term  $\mathcal{T}++$  or decrement term  $\mathcal{T}--$ , for a term  $\mathcal{T}$ .

Given an assignment  $\alpha$  to the variables in  $X$ , the semantics  $\text{val}$  of a term is defined by the conditions  $\text{val}(x, \alpha) = \alpha(x)$ ,  $\text{val}(k, \alpha) = k$ ,  $\text{val}(\mathcal{T}++, \alpha) = \text{val}(\mathcal{T}, \alpha) + 1$ , and  $\text{val}(\mathcal{T}--, \alpha) = \text{val}(\mathcal{T}, \alpha) - 1$ . Addition and subtraction is supposed to be modulo the boundaries of the domain. Terms may occur positive or negative in the formal sum of an arc inscription.

In symmetric nets, a guard consists of expressions, which are basically a comparison of terms of their boolean connections.

**Definition 6.3. (Expression)**

An *expression* can be a comparison  $\mathcal{T}_1 \oplus \mathcal{T}_2$  ( $\oplus \in \{<, >, \leq, \geq, =, \neq\}$ ) between two terms  $\mathcal{T}_1$  and  $\mathcal{T}_2$ , or a Boolean combination of expressions. We use the standard semantics for all operators.

We only consider conjunction and disjunction as Boolean operators since negation can be removed using de Morgan's rules and the set of comparisons is closed under negation.

## 6.1. Simplification of arc inscriptions

Before constructing the automata, we present a simplification for the arc inscriptions, that turns the formal sum of terms resp. tuples of terms into a formal sum of simple variables resp. tuples of simple variables such that every variable occurs only once in any arc connected to a transition.

In general, assume an arc inscription  $\mathcal{T}_1 + \dots + \mathcal{T}_p - \mathcal{T}'_1 - \dots - \mathcal{T}'_n$  with  $p$  positive and  $n$  negative terms. This formal sum has size  $m = p - n$  with  $m > 0$  (otherwise, the arc inscription does not make sense). We introduce  $m$  variables  $x_1, \dots, x_m$ . The number of variables is the same as the number of token which pass this arc.

The arc inscription is replaced with the (positive) formal sum  $x_1 + \dots + x_m$  of the fresh variables and the guard  $\gamma(t)$  of the transition  $t$  is extended to

$$\gamma(t) \wedge \bigvee_{\pi \in \text{permutations}(p)} \left( \bigwedge_{i=1}^m x_i = \mathcal{T}_{\pi(i)} \wedge \bigwedge_{j=1}^n \mathcal{T}'_j = \mathcal{T}_{\pi(m+j)} \right).$$

Each permutation  $\pi \in \text{permutations}(p)$  is a bijection mapping variables and negative terms to occurring the positive terms here.

The combinatorics in this construction reflects the fact that tokens on places are not ordered. This fact can be ignored in subsequent constructions. The combinatorics furthermore reflects the fact that negative terms in a formal sum must match some positive term since the resulting multiset cannot contain negative multiplicities. It is obvious that the modification does not change the semantics of the net.

**Example 6.4.** If an arc inscription has the shape  $\mathcal{T}_1 + \mathcal{T}_2 + \mathcal{T}_3 - \mathcal{T}_4$ , we introduce two fresh variables  $x_1$  and  $x_2$  (as the size of the formal sum is 2). We then replace the arc inscription with  $x_1 + x_2$  and extend the guard  $\gamma(t)$  of transition  $t$  to

$$\gamma(t) \wedge ((x_1 = \mathcal{T}_1 \wedge x_2 = \mathcal{T}_2 \wedge \mathcal{T}_4 = \mathcal{T}_3) \vee (x_1 = \mathcal{T}_2 \wedge x_2 = \mathcal{T}_1 \wedge \mathcal{T}_4 = \mathcal{T}_3) \vee (x_1 = \mathcal{T}_1 \wedge x_2 = \mathcal{T}_3 \wedge \mathcal{T}_4 = \mathcal{T}_2) \vee (x_1 = \mathcal{T}_3 \wedge x_2 = \mathcal{T}_1 \wedge \mathcal{T}_4 = \mathcal{T}_2) \vee (x_1 = \mathcal{T}_2 \wedge x_2 = \mathcal{T}_3 \wedge \mathcal{T}_4 = \mathcal{T}_1) \vee (x_1 = \mathcal{T}_3 \wedge x_2 = \mathcal{T}_1 \wedge \mathcal{T}_4 = \mathcal{T}_1)).$$

If tuples appear in arc inscriptions, we replace them by a tuple of variables instead of a single variable. For instance, arc inscription  $\langle \mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \rangle$  is replaced with  $\langle x_1, x_2, x_3 \rangle$  and the guard  $\gamma(t)$  is extended to  $\gamma(t) \wedge x_1 = \mathcal{T}_1 \wedge x_2 = \mathcal{T}_2 \wedge x_3 = \mathcal{T}_3$ . This way, we may reduce all future considerations to variables that represent basic domains (color sets that are not cross products of other color sets). Tuple variables in the guard itself are replaced accordingly. Again, the semantics of the net is preserved by the modification. From now on, consider the arc inscriptions as simplified.

In a typical symmetric net, formal sums are small, so the introduced combinatorics is moderate. There is one exception, though. Beyond the formal sums considered so far, symmetric nets permit some  $all(\chi(p))$  construct that represents the formal sum of all elements of color domain  $\chi(p)$  of a place  $p \in P_c$ . Since the combinatorics introduced by that construct is intractable, we disregard it. In our implementation, all transition classes where an  $all$  construct is used in an arc inscription, are treated as if they were not full. This way, correctness of our approach is not at stake.

The following subsections show how to represent terms and expressions as automata. This way, we obtain an automaton that accepts all firing modes of a transition. We map that automaton to token distributions on the pre-places and finally aggregate the resulting automata for checking whether a transition class is full.

## 6.2. Term and expression automata

A term basically represents a value that may depend on an assignment to its occurring variables. In the field of symmetric coloured level nets this value is an element of the color domain of the connected place. Color domains in symmetric nets are enumerations or intervals of integer numbers. Since enumerations can be coded as integers, we shall treat all domains as integer intervals. Thanks to the simplifications in the previous section, we may disregard cross-product domains.

We represent a term  $\mathcal{T}$  as a term automaton  $A_{\mathcal{T}}$ . A term automaton extends automata as in Definition 6.1 with a mapping  $V : F \rightarrow D$  which maps an element from the domains to every final state. The idea is that, for a sequence representing assignment  $\alpha$ , the reached final state  $q_f$  satisfies  $V(q_f) = \text{val}(\mathcal{T}, \alpha)$ . The construction itself is rather obvious, so we reduce our presentation to a few examples, shown in Figure 3. Regarding Figure 3c, remind that incrementation is interpreted modulo the domain size, so the bottom right state is indeed  $q_{c_1}$ .

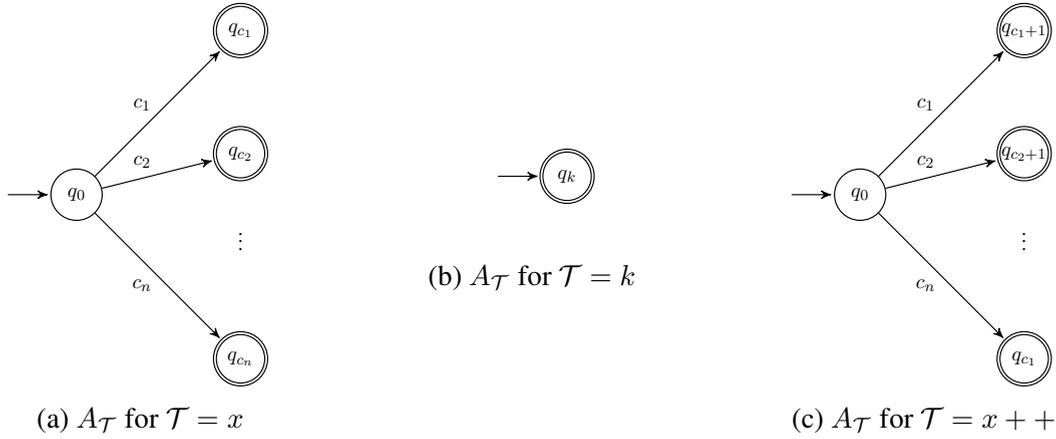


Figure 3: Examples of term automata. The domain for variable  $x$  is  $\{c_1, \dots, c_n\}$  and  $k$  is a constant.

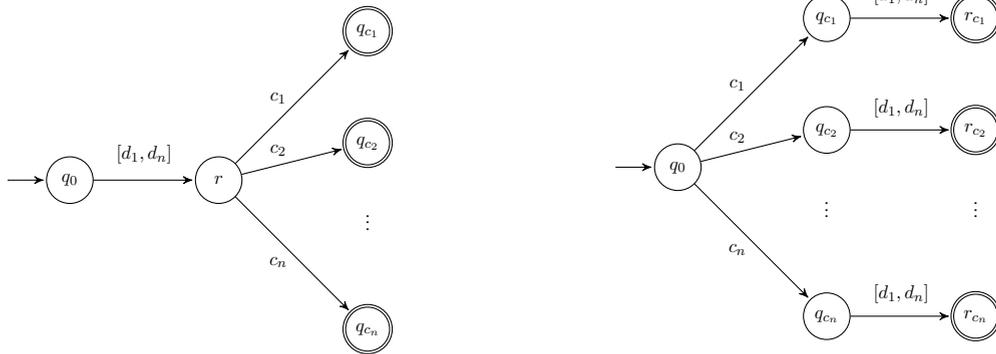


Figure 4: Insertion of an unused variable with domain  $\{d_1, \dots, d_n\}$  into a term automaton

An automaton for an expression is generated using the well-known product automaton construction. However, before applying the product construction, we need to harmonize the operand automata. Harmonizing means that we need to make sure that they talk about the same set of variables. An unused variable is inserted into a term automaton or an automaton as shown in Figure 4.

Once two automata represent assignments to the same set of variables, we can use the well-known product construction for combining them. The different operations basically concern the set of final states, so we leave that open for a moment.

**Definition 6.5. (Product automaton)**

Let  $A_1 = [X, Q_1, q_{01}, \delta_1, F_1]$  and  $A_2 = [X, Q_2, q_{02}, \delta_2, F_2]$  be automata. Automaton  $A = [X, Q, q_0, \delta, F]$  is a product of  $A_1$  and  $A_2$  if  $Q = Q_1 \times Q_2$ ,  $q_0 = [q_{01}, q_{02}]$ , and, for all  $q_1 \in Q_1$  and  $q_2 \in Q_2$  and values  $a$ ,  $\delta([q_1, q_2], a) = [\delta_1(q_1, a), \delta_2(q_2, a)]$ .

For a comparison  $\oplus \in \{=, \leq, \geq\}$ , we build the product of two term automata. The set of final states of the resulting automaton is defined based on the mappings  $V_1$  and  $V_2$  introduced for term automata:  $[q_1, q_2] \in F$  if and only if  $q_1 \in F_1$  and  $q_2 \in F_2$  and  $V(q_1) \oplus V(q_2)$ . For conjunction (resp. disjunction), the set of final states is defined as follows:  $[q_1, q_2] \in F$  if and only if  $q_1 \in F_1$  and (resp. or)  $q_2 \in F_2$ . State explosion in the constructions can be alleviated by automata minimization.

**Example 6.6.** As an example, consider the expression  $x ++ = 2$  and assume that the domain of  $x$  is  $\{1, 2, 3\}$ . The term automata for  $x ++$  and  $2$  are depicted in Figure 3, where the automaton for  $2$  needs to be extended to the unused variable  $x$ . The result is shown in Figure 5a. Figure 5b shows the product automaton. Finally, minimization will merge states  $[q_1, r_2]$  and  $[q_3, r_2]$ . From [17], we borrow the idea of merging edges with consecutive annotations into one edge that is annotated with an interval. The final result is shown in Figure 5c.

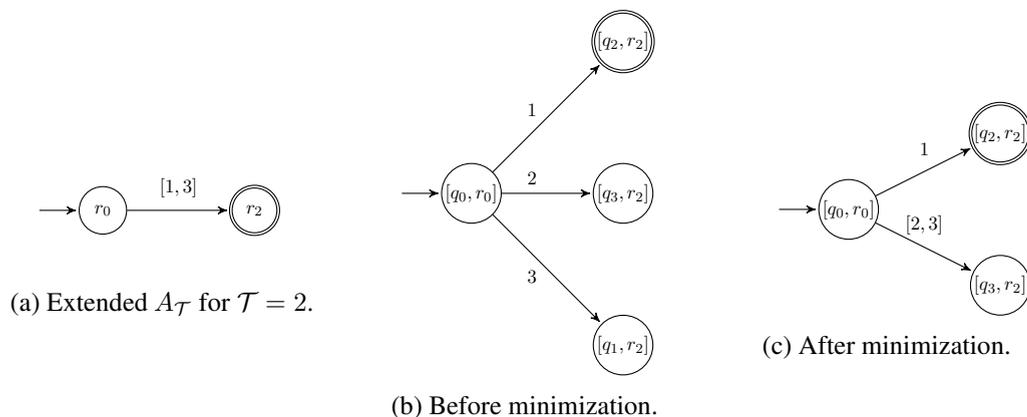


Figure 5: Product automaton for expression  $x ++ = 2$

### 6.3. Checking full transition classes

For checking whether a transition class is full, we need to transform assignments that satisfy the guard into token distributions that are consumed from pre-places. Thanks to our initial simplifications, all we need to do is to project the assignments to the variables that occur on incoming arcs. This can be easily done with the following considerations.

First, we make sure that the variables at incoming arcs occur first in the order of variables. Second, we make sure that variables of different transitions but concerning the same place occur in the same position in the respective order.

Next, assume that there are  $n$  variables at incoming arcs to a transition and make sure that there is no state in the corresponding automaton that is reached by a sequence of length  $n$  and another sequence of different length. If such state exists it can be split into two equivalent states to satisfy the condition. Then, every state  $q$  reached by a sequence of length  $n$  is made final if a final state is reachable from  $q$ . This way, all other variables are existentially quantified. The result is the set of all tokens distributions on pre-places that can be consumed by any enabled firing mode of a transition.

Finally, the resulting automata are combined using the or-product construction. This way, we obtain an automaton that represents all tokens distributions that can be consumed by any transition in the class. The full transition class criterion is satisfied if and only if the resulting automaton accepts every sequence of length  $n$ . This can be easily seen in the structure of the automaton if the resulting automaton has been minimized.

**Example 6.7.** As an example, consider the transition class  $[t]$  shown in Figure 6a. Assume that the domain of  $x$  is  $\{1, 2, 3, 4\}$  while the domain of  $y$  is  $\{1, 2, 3\}$ . Let  $x < y$ . Figures 6b and 6c show the automata representing the token distributions for  $t_1$  and  $t_2$ , respectively. The or-product of these automata is shown in Figure 7a. Minimization leads to the automaton in Figure 7b from which it is easy to see that the transition class is full.

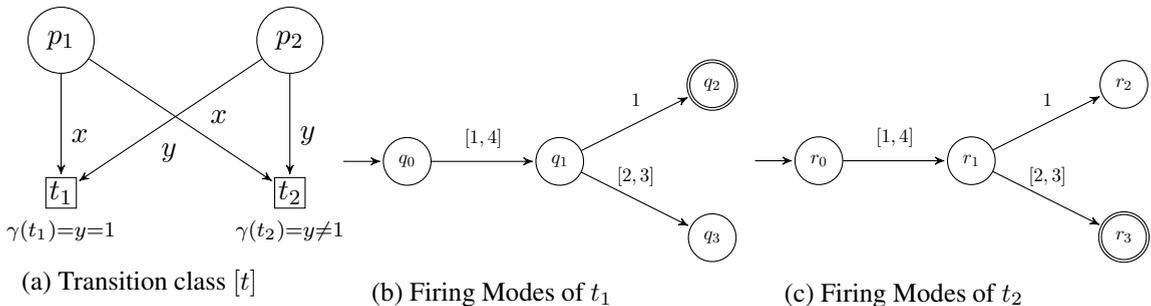


Figure 6: A Transition class and the automata representing its firing modes

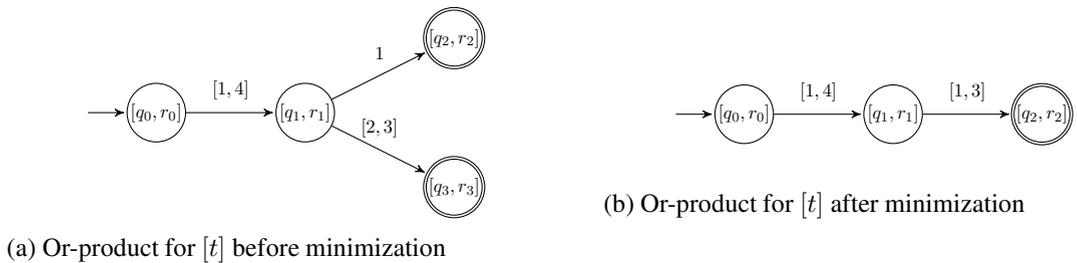


Figure 7: Checking for full transition class

Our experiments revealed that we are able to decide the full transition class criterion for coloured nets where, so far, no participant in the model checking contest could create its unfolding. We managed to get some verification results for those nets using the skeleton approach.

## 7. Extension to place/transition nets

With the results presented so far, the skeleton abstraction is only available for systems modeled as coloured Petri nets. In this section, we extend the applicability to nets that are originally modeled as

P/T nets. There exist translations from various high level system descriptions directly into P/T nets that could as well have been translated into coloured nets. We propose an efficient procedure to fold a P/T net  $N$  into a coloured net  $C_N$ , for which we then can build the skeleton  $S_N$ .

## 7.1. Folding P/T nets

The idea of folding a P/T net into a coloured net is as old as coloured nets as such. To our best knowledge, however, the efficiency of an actual implementation has not been observed so far. Our approach is based on partition refinement. The goal here is to partition a set  $\mathcal{M}$  into a partition  $M$  of disjoint subsets  $M_1, \dots, M_n$ . First,  $M$  contains only one subset, which is  $\mathcal{M}$ . The partition is then refined by the application of a split function.

**Definition 7.1.** Let  $M = \{M_1, \dots, M_n\}$  be a partition of the set  $\mathcal{M}$  and  $f : \mathcal{M} \rightarrow \mathbb{Z}$  be a split function. The application of  $f$  on the partition  $M$  is defined as:  $\text{split}(M, f) = \{\{x \mid x \in M_i, f(x) = j\}\}$  for  $1 \leq i \leq n, j \in \mathbb{Z}$ .

Informally, we separate elements, where  $f$  yields different values. This leads to a new partition of  $\mathcal{M}$ . For two subsets  $M_i, M_j$ , it should hold that  $M_i \neq \emptyset$ ,  $M_i \cap M_j = \emptyset$  and also  $M_1 \cup \dots \cup M_n = \mathcal{M}$ . For implementing a split operation, we assume an array where every element of  $\mathcal{M}$  appears exactly once. For every class in the partition, there is a pair of indices  $i$  and  $j$  such that the elements of the class are the array entries between  $i$  and  $j$ . For a split operation, we separately sort the elements of each class and then introduce new classes where adjacent elements have different  $f$ -values. Given a P/T net  $N = [P, T, F, W, m_0]$ , the initial set, which should be partitioned is  $\mathcal{M} = P \cup T$ . The coarsest partition fitting all requirements is  $M = \{P, T\}$ . We refine this partition such that, ultimately, every class of places of the given net serves as a place of the resulting coloured net  $C_N$  while every class of transitions of the given net serves as a transition.

While folding, We need to conform the restrictions of uniformity, that building a skeleton is possible. The uniformity criterion used here is more liberal than the one in [6]. There, we required that, for every two low level transitions  $t_1$  and  $t_2$  in some transition class, every place class  $M$  and every weight  $k$ ,  $t_1$  and  $t_2$  have the same number of pre-places (resp. post-places) with weight  $k$  in  $M$ . Here, we only require that the sum of all weights between  $t_1$  and places in  $M$  is the same as for  $M_2$ .

This modification yields coarser classes (thus smaller skeletons) and the algorithms run faster. This way, in an otherwise equivalent experimental setting, the number of cases where the skeleton approach responded as the fastest member of our portfolio rose from 3168 to 3702. The number of queries we could answer but no participant of the model checking contest could answer in 2019 climbed from 226 to 248.

The folding happens with regard to an  $ACTL^*$  formula  $\varphi$ . Let  $AP_\varphi$  denote the set of atomic propositions occurring in  $\varphi$ . The procedure for folding a P/T net into a coloured net is described in Figure 8.

In this procedure, the guard expressions  $\gamma$  deserve additional explanation. If  $M^*$  is a transition in the folded net, its elements  $\{t_1, \dots, t_m\}$  serve as firing modes of transition  $M^*$ . For each of these firing modes, we need to specify the effect on the pre-places and post-places. That is why the general structure of the guard starts with  $\bigvee_{t_i \in M^*} \dots$ . Since every pre- and every post-place needs to be

**Input:** Petri net  $N = [P, T, F, W, m_0]$   
**Output:** Partition  $M$  of  $P \cup T$  resp.  $C_N = [P_{CN}, T_{CN}, F_{CN}, W_{CN}, \chi, \gamma, m_{0CN}]$   
Let  $M = \{P, T\}$ ;  
 $M = \text{split}(M, f)$  where  $f(x) = \text{card}(\bullet x)$ ;  
 $M = \text{split}(M, f)$  where  $f(x) = \text{card}(x \bullet)$ ;  
**for all** atomic propositions  $p \in AP_\varphi$  with the form  $k_1 p_1 + \dots + k_n p_n \leq k$  **do**  
     $M = \text{split}(M, f)$  where for all occurring places  $p_i \in p : f(p_i) = k_i$  for  $i \in \{1, \dots, n\}$ , else  
     $f(x) = 0$ ;  
**end for**  
**for all** place classes  $M^* \in M$  **do**  
     $M = \text{split}(M, f)$  where  $f(x) = \sum_{p \in M^*} W(p, x)$ ;  
     $M = \text{split}(M, f)$  where  $f(x) = \sum_{p \in M^*} W(x, p)$ ;  
**end for**  
 $P_{CN} =$  place classes of  $M$ ,  $T_{CN} =$  transition classes of  $M$ ;  
 $(M^*, M^{*'}) \in F_{CN}$ ,  $W_{CN}(M^*, M^{*'}) = \{x_1, \dots, x_k\}$ , iff  $\exists x \in M^*, \exists y \in M^{*'} :$   
 $(x, y) \in F$ ,  $W(x, y) = k$  for  $k \in \mathbb{N}$  and  $M^*, M^{*'} \in M$ ;  
 $m_{0CN}(M^*) = \sum_{p \in M^*} m_0(p)$ ,  $\chi(M^*) = \{p \mid p \in M^*\}$  for every place class  $M^* \in M$ ;  
 $\gamma(M^*) = \bigvee_{t_i \in M^*} \left( \left( \bigwedge_{M^{*'} = \{p_1, \dots, p_n\} \in \bullet M^*} \bigwedge_{j=1}^n \bigwedge_{k=1}^n x_{p_{\sum_{\ell=1}^{j-1} W(p_\ell, t_i) + k}} = p_j \right) \wedge \right.$   
 $\left. \left( \bigwedge_{M^{*'} = \{p_1, \dots, p_n\} \in M^* \bullet} \bigwedge_{j=1}^n \bigwedge_{k=1}^n x_{p_{\sum_{\ell=1}^{j-1} W(p_\ell, t_i) + k}} = p_j \right) \right)$  for every transition class  
 $M^* \in M$ ;

Figure 8: Algorithm for folding a P/T net into a coloured net.

considered, we have the conjunctions  $\bigwedge_{M^{*'} = \{p_1, \dots, p_n\} \in \bullet M^*} \dots$  and  $\bigwedge_{M^{*'} = \{p_1, \dots, p_n\} \in M^* \bullet} \dots$ . The remaining content of the guard expressions is the same for pre- and post-places. It specifies for a given firing mode (i.e. low level transition  $t_i$ ) how many tokens of some colour (i.e. low level place  $p_j \in M^{*'}$ ) need to be consumed or produced. This number is  $W(p_j, t_i)$  (or  $W(t_i, p_j)$ , respectively). For consuming  $k$  tokens of some colour  $p_j$  (leading to conjunction  $\bigwedge_{j=1}^n \dots$ ), we need to bind  $k$  of the arc variables to colour  $p_j$  (leading to conjunction  $(\bigwedge_{k=1}^n \dots)$ ). If these bindings are done in consecutive order of the low level places  $p_1, \dots, p_n$ , the  $k$  variables bound to  $p_j$  are those that start with index  $\sum_{\ell=1}^{j-1} W(p_\ell, t_i)$  (or  $\sum_{\ell=1}^{j-1} W(t_i, p_\ell)$ ).

To make this algorithm more understandable, we demonstrate it with an example.

**Example 7.2.** We consider a P/T net  $N$ , which shows the dilemma of five dining philosophers. The P/T net is structured as follows: For every  $i \in \{0, \dots, 4\}$  there is a place  $th_i$  (philosopher  $i$  is thinking), a place  $hl_i$  (has left fork),  $hr_i$  (has right fork),  $ea_i$  (philosopher  $i$  is eating) and  $fo_i$  (fork  $i$  is on the table). There are the transitions  $tl_i$  (take left fork) that consume tokens from  $th_i$  and  $fo_i$ , and produce on  $hl_i$ , transitions  $tr_i$  (take right fork) that consume from  $hl_i$  and  $fo_{i+1 \bmod 5}$  and produce on  $ea_i$ , transitions  $rl_i$  (release left fork) that consume from  $ea_i$  and produce on  $hr_i$  and  $fo_i$ , and, finally, transitions  $rr_i$  (release right fork) that consume from  $hr_i$  and produce on  $fo_{i+1 \bmod 5}$  and  $th_i$ . Places  $th_i$  and  $fo_i$  are initially marked, and all arc weights are 1. For better readability,  $x_i$  describes the

set  $x_0, \dots, x_4$  for every node  $x \in P \cup T$  of the net. The folding is regarding the  $ACTL^*$  formula  $\varphi : \mathbf{AG} \neg(\sum_i hr_i = 4) \wedge (\sum_i hl_i = 1)$  for  $i \in \{0, \dots, 4\}$ . Initially the coarsest partition distinguishes between places and transitions:  $M = \{\{th_i, ea_i, fo_i, hl_i, hr_i\}, \{tr_i, tl_i, rl_i, rr_i\}\}$ . Then, the sets are split according to the *number of incoming and outgoing arcs*. All places  $fo_i$  have two incoming and two outgoing transitions, all remaining places only have one incoming and one outgoing transition. The  $tr_i$  and  $tl_i$  transitions have two incoming places and one outgoing place,  $rl_i$  and  $rr_i$  the other way round. This leads to partition  $M = \{\{th_i, ea_i, hl_i, hr_i\}, \{fo_i\}, \{tr_i, tl_i\}, \{rl_i, rr_i\}\}$ . The *atomic propositions* of  $\varphi$  give additional restrictions, as the elements of the subsets finally should satisfy those propositions equally. So, for the atomic propositions  $\sum_{i=0}^4 hr_i = 4$  and  $\sum_{i=0}^4 hl_i = 1$ , every place is mapped to its coefficient in the corresponding proposition. Transitions are not affected here, so  $M = \{\{th_i, ea_i\}, \{hl_i\}, \{hr_i\}, \{fo_i\}, \{tr_i, tl_i\}, \{rl_i, rr_i\}\}$ . For obtaining *uniformity*, we split  $\{tr_i, tl_i\}$  into  $\{tr_i\}$  and  $\{tl_i\}$  since every transition  $tl_i$  has a pre-places in  $\{th_i, ea_i\}$  while no transition  $tr_i$  has, and we split  $\{rl_i, rr_i\}$  into  $\{rl_i\}$  and  $\{rr_i\}$  since every transition  $rl_i$  has a pre-place in  $\{th_i, ea_i\}$  while no transition  $rr_i$  has. The resulting partition is  $M = \{\{th_i, ea_i\}, \{hl_i\}, \{hr_i\}, \{fo_i\}, \{tr_i\}, \{tl_i\}, \{rl_i\}, \{rr_i\}\}$  and is uniform.

Finally, every place class  $M_i$  is turned into a place  $p_{M_i}$  with  $\sum_{p \in M_i} m(p)$  tokens and the colour domain  $\chi(p_{M_i}) = M_i$ , and every transition class  $M_j$  into a transition  $t_{M_j}$ . We obtain the places  $thea, fo, hl, hr$  and the transitions  $tr, tl, rl, rr$ . Let there be an arc from  $p_{M_i}$  to  $t_{M_j}$ , if there exists some  $p \in M_i$  and  $t \in M_j$  with  $(p, t) \in F$ . Arcs from transitions to places are formed analogously. An Arc  $(p_{M_i}, t_{M_j})$  is assigned with the variables  $x_1, \dots, x_w$  where  $w = W(p, t)$  for  $p \in M_i$  and  $t \in M_j$ . In the end, we need to formulate the guard of the transitions, which needs to ensure, that the coloured transition only fires if the right coloured tokens lay on the pre-places. We therefore build the disjunction of the input requirements of the transitions according the arcs and weights of  $N$ . As an example, the guard of transition  $tl$  is

$$\begin{aligned} \gamma(tl) &= x_{11} = th_0 \wedge x_{12} = fo_0 \wedge x_1 = hl_0 && \text{(firing mode } tl_0) \\ &\vee x_{11} = th_1 \wedge x_{12} = fo_1 \wedge x_1 = hl_1 && \text{(firing mode } tl_1) \\ &\vee x_{11} = th_2 \wedge x_{12} = fo_2 \wedge x_1 = hl_2 && \text{(firing mode } tl_2) \\ &\vee x_{11} = th_3 \wedge x_{12} = fo_3 \wedge x_1 = hl_3 && \text{(firing mode } tl_3) \\ &\vee x_{11} = th_4 \wedge x_{12} = fo_4 \wedge x_1 = hl_4 && \text{(firing mode } tl_4) \end{aligned}$$

Figure 9 presents the coloured net, which results from the described folding. The coloured net can subsequently be decoloured to a skeleton.

## 7.2. Checking fullness for a P/T net

The resulting coloured net does not necessarily have full minimal transition classes (cf. Sec. 5.2), thus it does not have a deadlock-preserving skeleton. Due to the process for deriving the folded coloured net, the guards do not permit the approach outlined there for checking whether or not a transition class is full. We may, however, approach that criterion differently. The idea is to check the criterion right after the folding procedure, just as we have the final partitioning of the P/T nodes. If we cannot prove the deadlock preservation at this point, we can abort the skeletal analysis of this net, as we don't expect useful results.

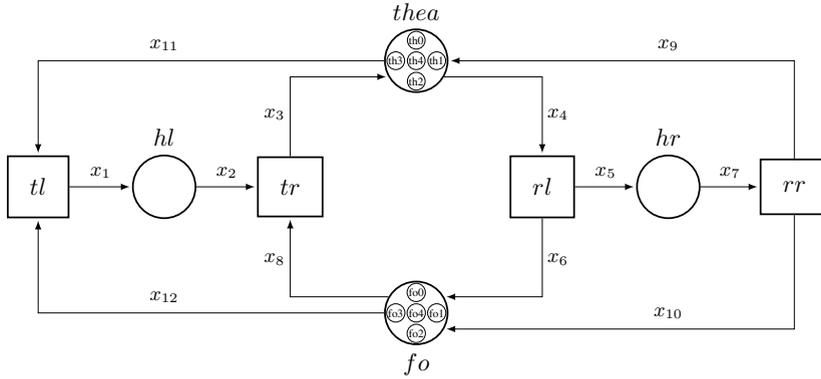


Figure 9: A coloured net version of the five dining philosophers.

**Theorem 7.3.** (Deadlock Preservation for P/T Nets) Let  $N$  be a P/T net and  $C_N$  its folding. Let  $[t] = \{t_1, t_2, \dots, t_k\}$  be a minimal transition class of  $C_N$ , where each transition  $t_j$  has  $s_j$  firing modes for  $j \in \{1, \dots, k\}$ . Let  $p_1, p_2, \dots, p_\ell$  be the pre-places of  $[t]$ , with the colour domains  $\chi(p_i)$  for  $i \in \{1, \dots, \ell\}$ . Every pre-place  $p_i$  is connected to every transition  $t_j$  of  $[t]$  by an arc with the weight  $w_{ij}$ . The folding  $C_N$  resp. the underlying P/T net  $N$  has a deadlock-preserving skeleton, if  $\prod_{i=1}^{\ell} \binom{|\chi(p_i)|}{w_{ij}} = \sum_{j=1}^k s_j$  for every minimal transition class of  $C_N$ .

**Proof:**

The folding  $C_N$  has a deadlock-preserving skeleton, if all of its minimal transition classes are full. A minimal transition class  $[t] = \{t_1, t_2, \dots, t_k\}$  is full, if for every marking  $m_{C_N}$  with  $|m_{C_N}(p_i)| = f_i(t)$  for  $i \in \{1, \dots, \ell\}$ , there is one transition in  $[t]$ , for which the marking is a firing mode. This is expressed by the equation  $\prod_{i=1}^{\ell} \binom{|\chi(p_i)|}{w_{ij}} = \sum_{j=1}^k s_j$ . The binomial coefficient  $\binom{|\chi(p_i)|}{w_{ij}}$  gives the number of sufficient tokensubsets of  $\chi(p_i)$  for one pre-place  $p_i$  of  $[t]$ , where  $i \in \{1, \dots, \ell\}$  and  $j \in \{1, \dots, k\}$ . Multiplying these numbers for every pre-place  $p_i$  for  $i \in \{1, \dots, \ell\}$ , leads to the total number of sufficient combinations of tokens, i.e the number of possible markings  $m_{C_N}$  with sufficient input requirements  $|m(p_i)| = f_i(t)$  with  $i \in \{1, \dots, \ell\}$  for  $[t]$ . Each of the transitions  $t_j$  in  $[t]$  for  $j \in \{1, \dots, k\}$  has  $s_j$  firing modes, thus in  $[t]$ , we have  $\sum_{j=1}^k s_j$  firing modes overall. If  $\prod_{i=1}^{\ell} \binom{|\chi(p_i)|}{w_{ij}} = \sum_{j=1}^k s_j$ , for every sufficient combination of the coloured tokens, there is a firing mode of one transition in  $[t]$ . If  $\prod_{i=1}^{\ell} \binom{|\chi(p_i)|}{w_{ij}} = \sum_{j=1}^k s_j$ , the minimal transition class  $[t]$  is full, thus if the equation holds for every minimal transition class,  $C_N$  has a deadlock-preserving skeleton. Transferring this to  $N$ , for every combination of tokens of the P/T pre-places (represented by  $\chi(p_i)$ ), there is one P/T transition related to  $[t]$  enabled (represented by  $s_j$ ). So, if a marking of  $N$  fits with regard to the cardinality, there must be one activated P/T transition if the equation holds. Then,  $N$  has a deadlock-preserving skeleton. It is important to mention, that the firing modes  $s_j$  need to be all different from each other, resp. all of the P/T transitions need to have different presets. Otherwise the equality of combinations and firing modes will not hold, although every combination activates a transition.  $\square$

This equation is sufficient for the fullness of  $[t]$ , but it is not necessary.

If  $\prod_{i=1}^l \binom{|x(p_i)|}{w_{ij}} > \sum_{j=1}^k s_j$ , which means there is a combination of tokens which does not activate a transition, these too many combinations might be unreachable, thus are not in need of an activated transition. If the equation holds for every minimal transition class we know that  $C_N$  will have a deadlock-preserving skeleton and the method of skeletal abstraction can be applied to  $N$  and all its  $ACTL^*$  formulas.

## 8. Experimental results

We conducted our experiments on the benchmark provided by the Model Checking Contest (MCC) 2019 [5]. On that page, the reader may find a detailed specification of the machine “tajo” that was used to execute the experiments. The benchmark comprises 1018 nets (193 coloured nets and 825 P/T nets). For the majority of colored nets, their unfolding is among the P/T nets of the benchmark, too. We covered the three categories Reachability, CTL, and LTL where the skeleton approach makes sense. For every net and category, there are 16 formulas with place-based atomic propositions and 16 formulas with transition-based propositions. That makes a total of 97,728 formulas. If a P/T net is the unfolding of a coloured net, some but not all formulas of the P/T net accord with formulas used for the coloured net.

In every single run, we allowed 4 cores, 30 minutes, and 16 MB of RAM for the verification of a group of 16 formulas. The runs used the full portfolio [21] of verification methods available in our tool LoLA [22], now including the skeleton approach. For the skeleton, we applied the same search based model checking routines as for the unfolded net, and the state equation approach [23]. In our approach, the skeleton is directly derived from the PNML description of a coloured net, so the skeleton related verification tasks start before the unfolding of the net is generated in parallel (and only then the remaining verification routines are launched). If the input is a P/T net, we first launch the verification tasks for the given net, before trying to fold the net (in parallel to the already running routines). We launch skeleton related tasks only if the size of the skeleton is less than one third of the size of the given P/T net. This way, we avoid situations where the skeleton is too close to the given net. Since folding depends on the formula, we have to execute up to 16 individual folding procedures per run. We do not fold a net if the formula is trivial (i.e. does not contain temporal operators). Trivial formulas are mostly the result of sophisticated application of logical tautologies and preprocessing based on linear programming [24]. We also stop the folding procedure as soon as some other portfolio member has determined the value of the formula.

For the 79,200 formulas for P/T nets, 66,546 skeletons were created. Of the remaining 12,654 formulas, 11,086 contain no temporal operators, so no folding was launched. For the remaining 1,568 formulas, some other portfolio member may have delivered a result before folding completed. Folding took at most 287 seconds, with an average of half a second. Generation of the skeleton for a coloured net takes no time at all as it appears as an intermediate step of the unfolding process. Generating the skeleton naturally succeeded for all coloured nets. It also succeeded whenever both net and formula were derived from a coloured net. There are a few other cases where the skeleton could be generated. Although more nets have a regular, foldable structure, formulas, if not derived from coloured nets, are generated randomly, so they tend to break symmetry more frequently than in practical situations.

On the other hand, the formula syntax for coloured nets in the MCC does not permit references to individual colours or firing modes, so the skeleton approach is applicable more frequently than in practice. Since there are more P/T nets than coloured nets in the contest, results obtained for the MCC benchmark should be a lower bound for the performance to be observed in practice.

The 66,546 skeletons include those that are considered to be too large to make a difference compared to the given net. After ruling them out, 34,906 formulas have useful skeletons, including coloured and P/T nets. In 15,315 cases, we launched the skeleton related tasks. In the remaining 19,591 cases, the formula (nor its negation) are not in  $ACTL^*$ , or none of the criteria discussed in the paper would certify preservation of the formula. We need to mention here that deadlock injection has not been implemented so far.

Of the 15,315 formulas where we launched the skeleton related tasks, they were the first (among the whole portfolio) to deliver results in 3702 cases. The remaining 12,147 formulas include those where some other portfolio member responded earlier, or where the skeleton approach evaluated its  $ACTL^*$  query to false (so the value is not inherited by the unfolded net).

Among the 97,728 formulas considered, there have been 7,768 formulas none of the participants in the MCC 2019 could solve. With the skeleton approach, we have now been able to solve 248 of these particularly involved problems. These include but are not restricted to nets that have a prohibitively large unfolding.

Given that we run the skeleton approach as part of a powerful portfolio, with LoLA being a competitive participant in the MCC, we may conclude that the skeleton approach nicely complements the existing portfolio.

## 9. Conclusion

With our contribution, we turned the skeleton approach into an executable and useful member of a verification portfolio. We investigated the gap between the concepts of net morphisms and simulation relations and proposed algorithms for checking the required criteria. Through folding, we extended the approach to P/T nets. Experiments underpin the usefulness of the approach.

Future work may include the implementation of deadlock injection. Furthermore, we may enhance the approach to the full transition classes. First, we may try to use place invariants to rule out certain token distributions in the pre-set of transition classes thus being able to certify more transition classes as full. Second, we may try to split places and transitions in the skeleton turning non-full transition classes into full ones. Furthermore, we may determine a larger number of  $LTL$  safety properties by the analysis of the respective Büchi automaton. So far, we assume all  $LTL$  properties which do not use  $X$ ,  $F$  and  $U$  as safety properties. Libraries like [25] are able to identify more  $LTL$  properties as safety properties. This might extend the use of the skeleton approach.

## References

- [1] Desel J. On abstractions of nets. In: Advances in Petri Nets 1991. Springer-Verlag, Berlin/ Heidelberg, 1991 pp. 78–92. doi:10.1007/BFb0019970.

- [2] Padbergx J, Gajewsky M, Ermel C. Rule-based refinement of high-level nets preserving safety properties. In: Proc. FASE, volume 1382, Springer, Berlin, Heidelberg, 1998 pp. 221–238. doi:10.1007/BFb0053593.
- [3] Milner R. Communication and Concurrency. Prentice Hall international series in computer science. Prentice Hall, New York, 1989. ISBN:978-0-13-114984-7.
- [4] Findlow G. Obtaining deadlock-preserving skeletons for coloured nets. In: Application and Theory of Petri Nets. Springer, Berlin, Heidelberg, 1992 pp. 173–192. doi:10.1007/3-540-55676-1\_10.  
Download citation.
- [5] Kordon F, Garavel H, Hillah LM, Hulin-Hubard F, Amparore E, Beccuti M, Berthomieu B, Ciardo G, Dal Zilio S, Liebke T, Li S, Meijer J, Miner A, Srba J, Thierry-Mieg Y, van de Pol J, van Dirk T, Wolf K. Complete Results for the 2019 Edition of the Model Checking Contest. <http://mcc.lip6.fr/2019/results.php>, 2019.
- [6] Wallner S, Wolf K. Skeleton Abstraction for Universal Temporal Properties. In: Buchs D, Carmona J (eds.), Application and Theory of Petri Nets and Concurrency - 42nd International Conference, PETRI NETS 2021, Virtual Event, June 23-25, 2021, Proceedings, volume 12734 of *Lecture Notes in Computer Science*. Springer, 2021 pp. 186–207. doi:10.48550/arXiv.2112.08884.
- [7] Vautherin J. Parallel systems specifications with coloured Petri nets and algebraic specifications. In: Advances in Petri Nets. Springer, Berlin, Heidelberg, 1987 pp. 293–308. doi:10.1007/3-540-18086-9\_31.
- [8] Rust C, Böke JTC. Pr/T-Net Based Seamless Design of Embedded Real-Time Systems. In: Applications and Theory of Petri Nets, Springer Berlin Heidelberg, Berlin, Heidelberg, 2001 pp. 343–362. doi:10.1007/3-540-45740-2\_20.
- [9] Lilius J. On the folding of algebraic nets. Helsinki University of Technology, 1995.
- [10] Sliva V, Muratax T, Shatz S. Protocol Specification Design Using an Object-Based Petri Net Formalism. *Int. Journal of Software Engineering and Knowledge Engineering*, 1999. **09**(01):97–125. doi:10.1142/S0218194099000073.
- [11] Jensen K, Kristensen L. Coloured Petri Nets. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
- [12] Pinna G. How Much Is Worth to Remember? A Taxonomy Based on Petri Nets Unfoldings. In: Applications and Theory of Petri Nets, volume 6709, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011 pp. 109–128. doi:10.1007/978-3-642-21834-7\_7.
- [13] Clarke E, Emerson E, Sistla A. Automatic verification of finite-state concurrent systems using temporal logic specifications. *ACM Transactions on Programming Languages and Systems*, 1986. **8**(2):244–263.
- [14] Grumberg O, Long D. Model checking and modular verification. *ACM Transactions on Programming Languages and Systems*, 1994. **16**(3):843–871. doi:10.1145/177492.177725.
- [15] Penczek W, Szreter M, Gerth R, Kuiper R. Improving Partial Order Reductions for Universal Branching Time Properties. *Fund. Inf.*, 2000. **43**(1-4):245–267. doi:10.3233/FI-2000-43123413.
- [16] Katz S, Grumberg O, Geist D. "Have I written enough Properties?" - A Method of Comparison between Specification and Implementation. In: Proc. CHARME. 1999 pp. 280–297. doi:10.1007/3-540-48153-2\_21.
- [17] Schwarick M, Rohr C, Liu F, Assaf G, xChodak J, Heiner M. Efficient Unfolding of Coloured Petri Nets Using Interval Decision Diagrams. In: Proc. PETRI NETS, volume 12152 of *LNCS*. 2020 pp. 324–344. doi:10.1007/978-3-030-51831-8\_16.

- [18] Chiola G, Dutheillet C, Franceschinis G, Haddad S. Stochastic well-formed colored nets and symmetric modeling applications. *IEEE Transactions on Computers*, 1993. **42**(11):1343–1360. doi:10.1109/12.247838.
- [19] PNML Standard. <https://www.pnml.org/index.php>. Accessed: 2021-12-15.
- [20] Kordon F, Bouvier P, Garavel H, Hillah LM, Hulin-Hubard F, Amat N, Amparore E, Berthomieu B, Biswal S, Donatelli D, Galla F, , Dal Zilio S, Jensen P, He C, Le Botlan D, Li S, , Srba J, Thierry-Mieg, Walner A, Wolf K. Complete Results for the 2020 Edition of the Model Checking Contest. <http://mcc.lip6.fr/2021/results.php>, 2021.
- [21] Wolf K. Portfolio Management in Explicit Model Checking. In: Proc. PNSE, volume 2651 of *CEUR Workshop Proceedings*. 2020 pp. 10–28. URL <http://ceur-ws.org/Vol-2651/paper2.pdf>.
- [22] Wolf K. Petri Net Model Checking with LoLA 2. In: Proc. PETRI NETS. 2018 pp. 351–362. doi:10.1007/978-3-319-91268-4\_18.
- [23] Wimmel H, Wolf K. Applying CEGAR to the Petri Net State Equation. *Log. Methods Comput. Sci.*, 2012. **8**(3). doi:10.2168/LMCS-8(3:27)2012.
- [24] Bønneland F, Dyhr J, Jensen PG, Johannsen M, Srba J. Simplification of CTL Formulae for Efficient Model Checking of Petri Nets. In: Proc. PETRI NETS, volume 10877 of *LNCS*. 2018 pp. 143–163. doi:10.1007/978-3-319-91268-4\_8.
- [25] Duret-Lutz A. LTL Translation Improvements in Spot 1.0. *International Journal on Critical Computer-Based Systems*, 2014. **5**(1-2):31–54. doi:10.1504/IJCCBS.2014.059594.