Towards Efficient Verification of Elementary Object Systems

Ismaila Jihad Abdullahi, and Berndt Müller
University of South Wales
(Ismaila.abdullahi, bertie.muller)@southwales.ac.uk

Abstract. Elementary Object Systems (EOS) is a class of Object Petri Nets that follows the "*nets-within-nets*" paradigm. It combines several practical as well as theoretical properties for the needs of multi-agent-systems. However, it comes with some constraints that limit their expressiveness for automatic verification purposes due to the highly expressive nature of the underlying class of Petri nets. In this paper, we proposed a set of transformation rules from EOS to basic Petri nets nets and show isomorphism of the state spaces in order to make verification feasible.

Keywords: Elementary Reference-net System, nets-within-nets, Petri nets, isomorphic property, computational complexity

1 Introduction

Elementary Object Systems (EOS for short) are based on the *nets-within-nets* paradigm of (Valk, 1991,2003) in which the nesting of nets involved in the model is restricted to two levels and are generalised in (Köhler and Heitmann, 2009) for arbitrary nesting structure. This formalism provides a modelling technique that allows tokens of Petri nets to be Petri nets themselves, called *object nets*. Object nets are tokens with internal structure and inner activity and have been applied in a variety of scenarios, e.g., multi-agent systems.

We aim to provide a path to verification of properties of a slightly modified version of EOS, called *elementary reference-net systems (ERS)*, with reference semantics that is practically relevant and overcomes fundamental decidability issues with other formalists as shown in (Köhler and Rölke, 2004) and (Lomazova, and Schnoebelen, 1999). As in similar formalists, we have to distinguish autonomous and synchronous transitions. The need for application of a *partial order (unfolding)* approach for dynamic analysis of EOS have encouraged and driven the development of this new formalism. We refer the reader to (Valk, 1991) for an introduction to the nets-within-nets.

Compared to EOS, two main additions are introduced for ERS: Firstly, we provide each marked object net located in places of the system net with a *unique name* so that object nets with the same marking can be distinguished. Secondly, we use variables to label arcs of the system net. So that when firing transitions, variables are bound to

object nets names instead of statically *typing* system net places allowing dynamic use of net-tokens without fixing *types* for places of the system net.

We extend the notion of 1-safe P/T nets to ERS to guarantee that the state space is finite and markings are bounded. Further to the definition of ERS, we propose a set of transformation rules from 1-safe ERS into P/T nets and show isomorphism of the state spaces of ERS with its generated P/T net.

In Section 2 we review some preliminaries from Petri net theory. Section 3 gives an introduction to ERS. Section 4 presents the set of transformation rules from 1-safe ERS to 1-safe P/T nets. Section 5 proves the isomorphism of the state spaces of 1-safe ERS and of the transformed 1-safe P/T net.

2 Fundamentals of Petri nets

Here we give some definitions from theory of P/T-net, Relevant for our study.

Definition 2.1(P/T net) *A place/transition is a tuple* $N = (P, T, F, W)$*where* P is a finite set of places, T is a finite set of transitions, disjoint from P, $F \subseteq (P \times T) \cup (T \times P)$ is the flow relation, and $W: F \longrightarrow \mathbb{N}\backslash\{0\}$ is the arc weight function. *The pre-set of a node* $x \in P \cup T$*, denoted* $\bullet x$*, is the set containing the elements that immediately precede* x *in the net i.e.:* $\bullet x = \{y \in P \cup T | (y, x) \in F\}$*. Analogously, the postset of a node is denoted* $x\bullet$.

Definition 2.2 (Marking and Enabled transition). A marking of a P/T-net $N = (P, T, F, W)$ is a function $m: P \longrightarrow \mathbb{N}$. *A P/T net system* $\Sigma = (N, m_0)$ *is a net* $N = (P, T, F)$ *together with an initial marking* m_0*. Let* $\Sigma = (N, m_0)$ *be a net system. A transition* $t \in T$ *is enabled in a marking* m *iff* $m(p) \geq W(p, t)$*for all* $p \in \bullet t$*. An enabled transition* t *in marking* m *is denoted by* $m[t >$*. A transition that is enabled in a marking may or may not fire.* Firing of transition removes tokens from input places of t and puts new tokens onto output places of t. *The successor marking* m' *is defined as* $m'(p) = m(p) - W(p, t) + W(t, p)$*. We denote this by* $m[t > m'$*. For a finite sequence of transition* $\sigma = t_1, \ldots t_k$*, we write* $m[\sigma > m'$ *if there are markings* $m_1, \ldots m_{k+1}$ *such that* $m_1 = m, m_{k+1} = m'$ *and* $m_i[t_i > m_{i+1}$*, for all* $i = 1, \ldots, k$. The set of reachable markings of Σ is the set of all markings reachable from the initial marking. Σ is k-bounded if, for every reachable marking m and every place p ∈ P, m(p) ≤ k, and Σ is safe if it is 1-bounded. Moreover, Σ is bounded if it is k-bounded, for some k ∈ N. One can show that the set RM(Σ) is finite if Σ is bounded i.e. if $|\mathrm{RM}(\Sigma)| < \infty$.

3 Elementary Reference-net System (ERS)

By convention, the components of the system net will carry a hat: $\hat{P}, \hat{T}, \hat{p}, \hat{t}$, ... etc.

Definition 3.1 *Let the triple* $\eta_i = (i, N_i, m_i)$ *be a named marked object net, where* i*, is a unique name of an object net;* N_i *is a structure of the object net, and* m_i *is a marking in* N_i*. (Let* $\Sigma = \{(i_1, N_1, m_1), \ldots, (i_k, N_k, m_k)\}$ *be a finite set of unique*

marked named object nets). The structure of an object net with a unique name $i \in \Sigma$ is a P/T- net $N_i = (P_i, T_i, F_i)$, where P_i, is the set of places of the object net, T_i is the set of its transitions and $F_i \subseteq (P_i \times T_i) \cup (T_i \times P_i)$ is the flow relation. We assumed that all sets of nodes are pairwise disjoint and set $P_\Sigma \coloneqq \bigcup_{\eta_i \in \Sigma} P_{\eta_i}$ and $T_\Sigma \coloneqq \bigcup_{\eta_i \in \Sigma} T_{\eta_i}$. By $N_\bullet$ we denote the name of ordinary black tokens.

Definition 3.2 (ERS) *Let Var be a finite set of named variables. An elementary reference-net system is a tuple $RS = (\widehat{N}, \Sigma_{m^0}, \ell, w, \boldsymbol{R^0})$ where*

- $\widehat{N} = (\hat{P}, \hat{T}, \hat{F})$ is a p/t net called a system net, where $\hat{P}$ is its set of places, $\hat{T}$is its set of transitions and $\hat{F} \subseteq (\hat{P} \times \hat{T}) \cup (\hat{T} \times \hat{P})$ is the flow relation.
- $\Sigma_{m^0} \coloneqq \{(i_1, N_1, m_1^0), \dots, (i_k, N_k, m_k^0)\}$, is a finite set of marked named object nets.
- $\ell \subseteq (\hat{T} \cup \{\hat{\tau}\}) \times (T_{1\mathrm{i}} \cup \{\tau\}) \times, \dots, (T_k \cup \{\tau\}) \backslash \{\hat{\tau}, \tau, \dots, \tau)\}$, is the synchronisation relation, where $\hat{\tau}$ and τ are special symbols intended to denote inactions at the system and the object net levels respectively. If $\boldsymbol{t} = (\hat{t}, t_1, \dots, t_k)$ and $\hat{t}, \neq \tau$ and $\exists i \in \{1, \dots, k\}$ such that $t_i \neq \tau$, then we say that $\widehat{N} and\ N_i \in \Sigma$ for every $i \in \{1, \dots, k\}$ with $k = |\Sigma|$, participate in $\boldsymbol{t}$. This is the reason why $(\hat{t}, \tau, \dots, \tau)$ is excluded from the set of synchronisation relation: at least one object net must participate in every synchronisation action with the system net.
- $w: \hat{F} \longrightarrow Var \cup \{N_\bullet\}$ is an arc labelling function such that for an arc $\hat{a} \in (\hat{F})$ adjacent to a place $\hat{p}$ the inscription of $w(\hat{a})$ matches the name of object net in $\hat{p}$
- $\boldsymbol{R^0}$ specifies the initial making, where $\boldsymbol{R^0}: \hat{P} \to \mathbb{N} \cup MS(\Sigma)\ with\ \Sigma = \{(i_1, N_1, m_1), \dots, (i_k, N_k, m_k\}$. It has to satisfy the condition $\boldsymbol{R^0}(\hat{p}) \in \mathbb{N} \Leftrightarrow \boldsymbol{R^0}(\hat{p}) \in \{N_\bullet\}$.

In the example of Fig. 1 an $RS = (\widehat{N}, \Sigma, \ell, w, \boldsymbol{M^0})$ is shown, where $\Sigma = \{N_1, N_2\}$. Arcs of $\widehat{N}$ can be identified by their labelling from $w(\hat{t})$. Hence {x, y,} can be bound to marked named object nets in places $\hat{p}_1\ and\ \hat{p}_2$ adjacent to transition $\hat{t}'$ to enable it. In the initial marking, places $\hat{p}_1\ and\ \hat{p}_2$ contain references to the marked named object nets $N_1 and\ N_2$ respectively.

We denote by $\mathcal{N} = \{i | (i, N_{i,}, m_i) \in \Sigma\}$, a finite set of object nets names.

Moreover, variables appearing on arcs adjacent to a transition $\hat{t}$ of the system net must satisfy the following four conditions:

$$\forall \hat{t} \in \hat{T}\ and\ \forall \hat{p} \in {}^\bullet\hat{t}, \exists \hat{p}' \in \hat{t}^\bullet, such\ that\ w(\hat{p}, \hat{t}) = w(\hat{t}, \hat{p}')\ or\ w(\hat{p}, \hat{t}) = N_\bullet \quad (1)$$

$$\forall \hat{t} \in \hat{T}\ and\ \forall \hat{p} \in {}^\bullet\hat{t}, \exists \hat{p}' \in \hat{t}^\bullet, such\ that\ w(\hat{p}', \hat{t}) = w(\hat{t}, \hat{p})\ or\ w(\hat{p}, \hat{t}) = N_\bullet \quad (2)$$

$$\forall \hat{t} \in \hat{T} \text{ and for any two places } \hat{p}_1, \hat{p}_2, \in {}^\bullet\hat{t}, if\ \hat{p}_1 \neq \hat{p}_2\ then\ w(\hat{p}_1, \hat{t}) \neq w(\hat{p}_2, \hat{t}). \quad (3)$$

$$\forall \hat{t} \in \hat{T} \text{ and } \hat{p}'_1, \hat{p}'_2, \in \hat{t}^\bullet, if\ \hat{p}_1 \neq \hat{p}_2\ then\ w(\hat{t}, \hat{p}'_1) \neq w(\hat{t}, \hat{p}'_2). \quad (4)$$

Condition (1) says that each variable appearing in the incoming arc of a system net transition $\hat{t}$ also has to appear in the outgoing arc of $\hat{t}$ or no such variable exist. Condition (2) says that each variable appearing in the outgoing arc of a system net transition $\hat{t}$ also has to appear in the incoming arc of $\hat{t}$ or no such variable exist. These two

conditions means that no new object net is created and no destroyed after a transition firing in the system net. Condition (3) prevents the ability to join two object nets, and (4) prevents the splitting of an object net. This is because in reality, complex physical entities cannot be cloned at run time. With these restrictions, ERS still retain the ability to describe nesting of object nets, synchronisation, and mobility, but does not allow splitting of the inner marking of an object net or joining the inner marking of several object nets. Assuming these inner markings as modelling the inner state of an agent, this is a reasonable restriction and ERSs are then well suitable to model physical entities

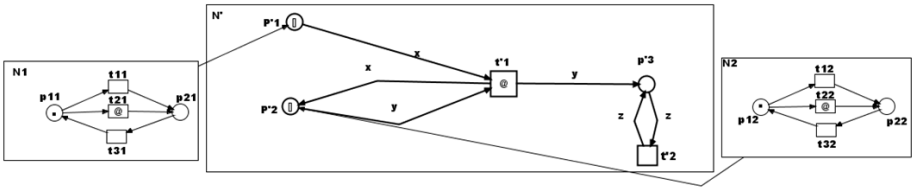


Fig. 1. An example of an ERS

For its behaviour, we introduce the notion of marking for elementary reference-net system ERS under *reference semantics.* Hence in general a marking is given by

1. a distribution of object nets or black tokens $\boldsymbol{R}: \hat{P} \to \mathbb{N} \cup MS(\Sigma)$ and
2. The vector $\boldsymbol{M} = (m_1, \dots, m_k)$ with the current marking of each N_i $(1 \leq i \leq k)$.

$\boldsymbol{R}$ specifies for each system net place $\hat{p}$ a number of black tokens or a multiset of marked named object nets (if $\hat{p}$ contain reference(s) to marked named object nets). If we abbreviate $(m_1, \dots, m_k)$ by $\boldsymbol{M}$ and the set of all such vectors by $\mathcal{M}$, we obtain the following Definition 3.3. By $\Pi_i(\boldsymbol{M})$ we denote the $i-th$ component m_i of $\boldsymbol{M}$ and by $\boldsymbol{M}_{\boldsymbol{i \to m_i}}$ the tuple, where the $i-th$ component is substituted by m_i, $M \in \mathbb{N}^k$.

In what follows a marked named object net is referred to as *net-token.* For a given ERS, by $\sum_{nt} = \Sigma \cup \{N_\bullet\}$ we denote the set of all marked named net-tokens. Only when not introduced in the marking! Sometimes by abuse of notation, for a named object net (i, N_i, m_i) in a place $\hat{p}$ of a marking $\boldsymbol{R}$ of the system net we write $\boldsymbol{R}(\hat{p}) = i$

Definition 3.3 Given *an elementary reference-net system* $RS = \left(\hat{N}, \Sigma_{nt}, \ell, \omega, \boldsymbol{R^0}\right)$ *we define* $\mathcal{M} \coloneqq \{M | M = (m_1, \dots, m_k) \wedge m_i \in MS(P_i)\}$. *Then a marking of an elementary reference-net system is a pair* (R, M) *where* $M \in \mathcal{M}$ *and* $\boldsymbol{R}: \hat{P} \to MS(\Sigma_{nt})$. *Specifying* M^0 *by the initial markings of the marked named object nets* $M^0 = (m_1^0, \dots, m_k^0)$ *we obtain the initial marking* $(\boldsymbol{R^0}, \boldsymbol{M^0})$ *of RS. The set of all markings of RS is denoted by* $\mathcal{M}_\mathrm{r}$.

Let $\hat{t} \in \hat{T}$ be a transition in the system net $\hat{N}$, then $\bullet\hat{t} = \left\{\hat{p} | (\hat{p}, \hat{t}) \in \hat{F}\right\}$, and $\hat{t}\bullet = \{\hat{p} | (\hat{t}, \hat{p}) \in \hat{F}\}$ are sets of its pre- and post-conditions. We denote by $\omega(\hat{t}) \coloneqq \left\{\omega(\hat{p}, \hat{t}) \middle| (\hat{p}, \hat{t}) \in \hat{F}\right\} \cup \left\{\omega(\hat{t}, \hat{p}) \middle| (\hat{t}, \hat{p}) \in \hat{F}\right\} = \bullet\hat{t} \times \{\hat{t}\} \cup \{t\} \times \hat{t}\bullet$ the set of all variables on arcs adjacent to $\hat{t}$. A binding β *specifie*s which variables are bound to names, *where* $\beta: \omega(\hat{t}) \cup \{\bullet\} \longrightarrow \mathcal{N} \cup \{N_\bullet\}$*with* $\mathcal{N} = \left\{i \middle| \left(i, N_{i,}, m_i\right) \in \Sigma\right\}$ *satisfying the condi-*

tions: for each $x \in \mathcal{w}(\hat{t}) \cup \{\bullet\}$, there exist $i \in \mathcal{N}$ *such that* $\beta(x) = i$ *and if* $x = \bullet$ *then* $\beta(x) = N_{\bullet}$.

The *firing rule* will be introduced in three modes.

Definition 3.4 (synchronisation firing mode) *Let* $(\boldsymbol{R}, \boldsymbol{M})$*be a marking of an elementary reference-net system,* $\hat{t} \in \hat{T}$ *a transition of* $\hat{N}$*, and let* β *be a variable binding defined for all* $x \in \mathcal{w}(\hat{t}) \cup \{\bullet\}$*. Let* $\alpha_1, \ldots, \alpha_k \in \Sigma_{nt}$ *be object nets involved in the firing of* $\hat{t}$*. Then* $\hat{t}$ *can fire provided that in each* $\alpha_i \in \Sigma_{nt}$ *for every* $i \in \{1, \ldots, k\}$ *a transition* $t_i \in T_\Sigma$ *such that*$(\hat{t}, t_1, \ldots, t_k) \in \ell$*. Then* $(\hat{t}, t_1, \ldots, t_k)$ *is enabled in* $(\boldsymbol{R}, \boldsymbol{M})$ *if:* $\forall \hat{p} \in \hat{P}$: $(\beta(\mathcal{w}(\hat{p}, \hat{t})), N_{\beta(\mathcal{w}(\hat{p},\hat{t}))}, m_{\beta(\mathcal{w}(\hat{p},\hat{t}))}) \in \boldsymbol{R}(\hat{p})$ and

$$\forall p \in P_i : \Pi_i(\boldsymbol{M}) \geq F_i(p, t_i), \tag{5}$$

This is denoted by $(\boldsymbol{R}, \boldsymbol{M})[\hat{t}, t_i >$ *Let be* $m_i[t_i > m'_i$ *(w.r.t* N_i*). The successor marking* $(\boldsymbol{R}', \boldsymbol{M}')$ *is defined by*

$$\boldsymbol{R}'^{(\hat{p})} = \boldsymbol{R}(\hat{p}) \setminus \left(\beta\left(\mathcal{w}(\hat{p}, \hat{t})\right), N_{\beta(\mathcal{w}(\hat{p},\hat{t}))}, m_{\beta(\mathcal{w}(\hat{p},\hat{t}))}\right) \cup$$
$$\left(\beta\left(\mathcal{w}(\hat{t}, \hat{p})\right), N_{\beta(\mathcal{w}(\hat{t},\hat{p}))}, m_{\beta(\mathcal{w}(\hat{t},\hat{p}))}\right) : \forall \hat{p} \in \hat{P} \text{ and}$$

$$\boldsymbol{M}' = \boldsymbol{M}_{\boldsymbol{i} \to \boldsymbol{m_i}}. \tag{6}$$

This is denoted by $(R, M)[\hat{\boldsymbol{t}}, \boldsymbol{t_i} > (\boldsymbol{R}', \boldsymbol{M}')$.

Definition 3.*5(system-autonomous firing mode)* *Let* $(\boldsymbol{R}, \boldsymbol{M})$ *be a marking of an elementary reference-net system RS* $= \left(\hat{N}, \Sigma_{nt}, \ell, \mathcal{w}, \boldsymbol{R^0}\right)$*and* $\hat{t} \in \hat{T}$ *a transition of* $\hat{N}$ *with a binding* β *such that* $\nexists(\hat{t}, x_i, \ldots, x_k) \in \ell : \exists\, i \in \{1, \ldots, k\} : x_i \neq \tau$**.** *Then* $\hat{t}$ *is activated in* $(\boldsymbol{R}, \boldsymbol{M})$ *if there is a net token such that:*

$$(\beta(\mathcal{w}(\hat{p}, \hat{t})), N_{\beta(\mathcal{w}(\hat{p},\hat{t}))}, m_{\beta(\mathcal{w}(\hat{p},\hat{t}))}) \in \boldsymbol{R}(\hat{p}) \forall \hat{p} \in \hat{P}. \tag{7}$$

Since we use τ*, for in action, this is denoted by* $(\boldsymbol{R}, \boldsymbol{M})[(\hat{t}, \tau) >$*. The successor marking* $(\boldsymbol{R}', \boldsymbol{M}')$*is defined by*

$$\forall \hat{p} \in \hat{P} : \boldsymbol{R}'(\hat{p}) = \boldsymbol{R}(\hat{p}) \setminus \left(\beta\left(\mathcal{w}(\hat{p}, \hat{t})\right), N_{\beta(\mathcal{w}(\hat{p},\hat{t}))}, m_{\beta(\mathcal{w}(\hat{p},\hat{t}))}\right) \cup \left(\beta\left(\mathcal{w}(\hat{t}, \hat{p})\right), N_{\beta(\mathcal{w}(\hat{t},\hat{p}))}, m_{\beta(\mathcal{w}(\hat{t},\hat{p}))}\right)$$

$$\boldsymbol{M}' = \boldsymbol{M}. \tag{8}$$

This is denoted by $(\boldsymbol{R}.\boldsymbol{M})[(\hat{t}_1, \tau) > (\boldsymbol{R}', \boldsymbol{M}')$.

***Definition 3.6*(object –autonomous firing mode)** *Let* $(\boldsymbol{R}, \boldsymbol{M})$ *be a marking of an elementary reference-net system RS* $= \left(\hat{N}, \Sigma_{nt}, \ell, \mathcal{w}, \boldsymbol{R^0}\right)$*and* $t_i \in T_i$ *a transition of a net-token* $i = (i, N_i, m_i) \in \boldsymbol{R}(\hat{p})$ *for some* $\hat{p} \in \hat{P}$*, such that* $\nexists(\hat{t}, x_i, \ldots, t_i, \ldots, x_k) \in \ell$*, and* t_i *is activated in* N_i*. Then we say that* $(\hat{\tau}, t_i)$ *is activated in* $(\boldsymbol{R}, \boldsymbol{M})$ *(denoted*$(\boldsymbol{R}, \boldsymbol{M})[(\hat{\tau}, t_i) >]$*. The successor marking* $(\boldsymbol{R}', \boldsymbol{M}')$ *of RS is defined by*

$\boldsymbol{R}' = \boldsymbol{R}$ and

$$\boldsymbol{M}' = \boldsymbol{M}_{1 \to \mathrm{m_i}} \text{if } m_i[\, t_i > m'_i \text{ for } \Pi_i(\boldsymbol{M}) = m_{\boldsymbol{i}}. \tag{9}$$

We denote this by $(\boldsymbol{R},\boldsymbol{M})[(\hat{\tau},\ t_i) > (\boldsymbol{R'},\boldsymbol{M'})$.

To introduce the occurrence sequences for ERS we assume an ERS as defined in Definition 3.2. Let RS be an ERS and $(\boldsymbol{R},\boldsymbol{M}),(\boldsymbol{R'},\boldsymbol{M'}) \in \mathcal{M}_r$.

Definition 3.7 *For a new alphabet* $\Gamma \coloneqq (\hat{T} \cup \{\hat{\tau}\}) \times (T_1 \cup \{\tau\}) \times, \dots, (T_k \cup \{\tau\}) \backslash (\hat{\tau},\tau,\dots,\tau)$ *where* $(\hat{\tau},\tau,\dots,\tau)$ *denotes the neutral element of* Γ^**, we define:*

$$(\boldsymbol{R},\boldsymbol{M})[(\hat{\tau},\tau,\dots,\tau) > (\boldsymbol{R'},\boldsymbol{M'}) \text{ if } (\boldsymbol{R},\boldsymbol{M}) = (\boldsymbol{R'},\boldsymbol{M'}) \text{ and}$$

$$(\boldsymbol{R},\boldsymbol{M})[\breve{w}(\hat{t},\alpha) > (\boldsymbol{R'},\boldsymbol{M'}) \text{ if } \exists(\boldsymbol{R''},\boldsymbol{M''}) : (\boldsymbol{R},\boldsymbol{M})[\breve{w} > (\boldsymbol{R''},\boldsymbol{M''}) \text{ and}$$

$$(\boldsymbol{R''},\boldsymbol{M''})[(\hat{t},\alpha) > (R',M') \text{ for some } \breve{w} \in \Gamma^*, \hat{t}, \in \hat{T} \cup \{\hat{\tau}\} \text{ and } \alpha \in ((T_1 \cup \{\tau\}) \times, \dots, (T_k \cup \{\tau\}). \quad (10)$$

To denote that $(\boldsymbol{R'},\boldsymbol{M'})$ *is reachable from* $(\boldsymbol{R},\boldsymbol{M})$ *by some occurrence sequence of actions we write* $(\boldsymbol{R},\boldsymbol{M}) \xrightarrow{*} (\boldsymbol{R'},\boldsymbol{M'})$.

The set of reachable markings of a reference system RS from a marking $(\boldsymbol{R},\boldsymbol{M})$ *is denoted by* $R(RS,(\boldsymbol{R},\boldsymbol{M}))$. $R(RS)$, *is the set of markings reachable from the initial marking* $(\boldsymbol{R^0},\boldsymbol{M^0})$. *The reachability graph* $(RG(RS)$ *is obtain as for P/T-net systems, which is a digraph whose nodes is the set of reachable markings and edges are the tuples* $((\boldsymbol{R},\boldsymbol{M}),(\hat{t},\alpha),(\boldsymbol{R'},\boldsymbol{M'})) \in \mathcal{M}_r \times (\hat{t},\alpha) \times \mathcal{M}_r$ *where* $(\boldsymbol{R},\boldsymbol{M}) \xrightarrow{(\hat{t},\alpha)} (\boldsymbol{R'},\boldsymbol{M'})$.

We now extend the definition of 1-safe P/T-net to ERS. We introduce two conditions for safeness of ERS as a generalisation of the safeness notion for P/T-nets.

Definition 3.8 (1-safe ERS) *Let* $RS = (\hat{N},\Sigma,\ell,\omega,\ \boldsymbol{R^0})$*be an ERS. RS is 1-safe if and only if all reachable markings are 1-safe and if and only if in all reachable markings there is at most one net-token on each system net place and each net-token is 1-safe i.e.,:*

- $\forall(\boldsymbol{R},\boldsymbol{M}) \in R(RS), \forall\hat{p} \in \hat{P}$: $(R(\hat{p}),) \leq 1$ and
- $\forall(i,N_i,m_i) \in \boldsymbol{R}(\hat{p})$:$\forall p_i \in P_i : \forall\hat{p} \in \hat{P}\ (\boldsymbol{R}(\hat{p}),\Pi_i(\boldsymbol{M}(p_i)) > 0 \Longrightarrow \Pi_i(\boldsymbol{M}(p_i)) \leq 1.$

Observation 3.9: *Given an ERS if for all reachable markings there is at most one token on each system net place and each net-token is 1-safe, then all reachable markings are 1-safe.*

Theorem 3.10 *If an ERS is safe, then its set of reachable markings is finite. The proof to this theorem is presented in appendix A.*

4 Transformation of ERS into P/T- nets

We construct a behaviorally equivalent finite P/T-net model for the entire ERS model and show this by strong bisimulation equivalence between states of the two models. By doing so, we develop a set of transformation rules that provide the same behavioral properties as the original one for formal verification and analysis.

Related work can be found in (Miyamoto & Horiguchi, 2013; Lomazova & Ermakova, 2016). We highlight the similarities and differences between the proposed ap-

proach and these related studies. Miyamoto and Horiguchi present a translation technique for transforming classical Multi-Agent nets (MANs) into Modular Nets (MNs) and show isomorphism of state spaces of both nets including the computational complexity for transforming MAN into MNs. The major similarities between our work and that of (Lomazova&Ermakova, 2016) is that they developed a set of rules for translating a safe conservative nested Petri net (NP-net) into an equivalent P/T net. The main differences are that we established clearly an important relation between the isomorphic properties of state space of safe-ERS and a 1-safe P/T net. Among such results are the establish Lemmas, and proof of a theorem for the isomorphism. Moreover, we adopt a different way of introducing the procedure for transforming nets-within-nets into 1-safe P/T net, which consequently give a neater and easier-to-understand presentation.

4.1 Transformation Rules

This subsection gives a set of transformation rules for transforming Elementary Reference-net system (Section 3) into P/T-net. There exist five rules and they must be applied in sequence from Rule 1 to Rule 5. With these rules ERS can be translated into a P/T net system N^*.

Let $RS = (\widehat{N}, \Sigma, \ell, \omega, \boldsymbol{R^0})$*be an ERS with a set* Σ_{nt} *of all marked named net tokens in the initial marking. By* $\mathbb{R}$ *we denote the set of all names used in* Σ_{nt}*. The net will be translated into a P/T-net system* $N^* = (P^*_{N^*}, T^*_{N^*}, F^*_{N^*}, M^*_0)$

Rule 1: *Generate the set* $P^*_{N^*}$ *of places of a P/T-net* N^**. The first, is the set* P'_{N^*} *of places from the system net* $\widehat{N}$*, and the second the set* P_{N^*} *of all places of each net-token in the initial marking of the system net. Finally, we take the union of these set as the set* $P^*_{N^*}$ *of a target P/T-net* N^**, with the assumption that* $P'_{N^*} \cap P^*_{N^*} = \emptyset$*.*

P'_{N^*} *is generated by duplicating all places of the system net for each net-token name* i *used in the initial marking of the system net and labelled it with a pair* (p', i) *where* p'*is a place in* $\hat{P}$*. Thus the set is defined as follows:*

$$P'_{N^*} := \bigcup_{p' \in \hat{P}} \{(p', i) | i \in \mathbb{R}, i \geq 1\}. \quad (11)$$

P_{N^*} *is generated by taking a copy of each place in the set* P_i *for each net-token and labelled it with a pair* (p_i, i) *where* p_i *is a place in* P_i*. It is defined as follows:*

$$P_{N^*} := \bigcup_{i \in \Sigma_{nt}} \{(p_i, i) | p_i \in P_i, i \in \mathbb{R}, i \geq 1\}. \quad (12)$$

Therefore the set $P^*_{N^*}$ *of a target P/T-net* N^* *as shown in Fig.2 is the union of these set, namely*

$$P^*_{N^*} := P'_{N^*} \cup P_{N^*}. \quad (13)$$

Rule 2: *Define the initial marking for* N^**. For a P/T-net* N^* *we define an encoding of markings on places from the set of places* $\hat{P}$ *in an ERS by markings on the generated places from* $P^*_{N^*}$*. If a net-token with name* $i \in \mathbb{R}_i$ *resides in a place* $\hat{p}$ *in an initial*

marking $R^0(\hat{p})$ *of the system net, then a black token in placed on* $(\hat{p}, i) \in P^*_{N^*}$ *as the initial marking* M^*_0 *of the constructed, namely*

$$M^*_0(\hat{p}, i) = R^0(\hat{p}). \tag{14}$$

Also, we define an encoding of markings on places from the set of places P_i *on the generated places from* $P^*_{N^*}$. *If all places* (p, i) *for all* p *such that* $(p, i) \in P^*_{N^*}$ *is marked in the initial marking* M^0 *of the net-token* $i \in \mathbb{R}_i$, *then of black token is placed on* $(\hat{p}, i) \in P^*_{N^*}$ *in* M^*_0 ,*namely*

$$(p, i) = M^0(p). \tag{15}$$

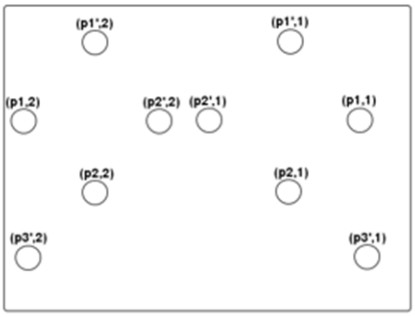


Fig. 2. Set of places of P/T net

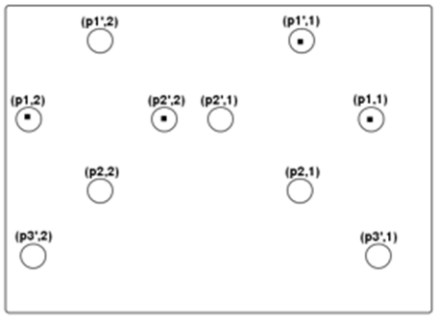


Fig 3: initial marking

If *a place in the system net is a place that contains a black token, then the unique copy corresponding to the place in* N^* *is also marked with a black token. In the given ERS, reference to the net-token* N_1 *resides in* $\hat{p}_1$, *and reference to the net-token resides in* $\hat{p}_2$. *Hence, we have tokens in* $(p'_1, 1)$ *and*$(p'_2, 2)$ *for* N^*. *Likewise, we define the markings for places* $(p_1, 1)$ *and* $(p_1, 2)$. *This is illustrated in Fig.3 above.*

Rule 3: *Generate a family of P/T-net transitions from a system net. We define a set* T^*_{sat} *of transitions of* N^* *obtained from each autonomous transition of the system net* $\widehat{N}$ *by duplicating each autonomous transition for each input arc variable of* $\hat{t}$ *that may be bound to any of the named net-token name in each place adjacent to* $\hat{t}$ *with appropriate input and output arcs, in* N^*.

$$T^*_{sat} \coloneqq \cup_{\hat{t} \in \hat{T}} \{ t'_{\beta_i(x)} | x \in w(\hat{t}) : \hat{t} \text{ is a system autonomous transition} \}. \tag{16}$$

In the example ERS, the set $w(\hat{t})$ *of input arc variables that can be bound to a named net-token for* t'_2 *is as follows:*

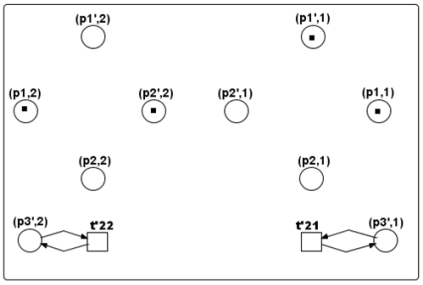
$$\beta(w(t'_2)) = \{\beta_1 = (z = 1) \quad \beta_2 = (z = 2)\}. \tag{17}$$

Where β_1 *and* β_2 *are bound to the input arc variable* z, *respectively. Therefore, two transitions* t'_{21} *and* t'_{22} *are generated for transition* t'_2 *from Rule 3.*

We define a set F^*_{sat} *of arcs for system autonomous transitions in* N^**as follows:*

$$F^*_{sat} = \bigcup_{\hat{a}\in\hat{F}}\{(x', y'|(x, y) = w(\hat{a}), x' \in P'_{N^*}(x) \cup T^*_{sat}(x), y' \in P'_{N^*}(y) \cup T^*_{sat}(y)\}. \quad (18)$$

Rule 4: *Generate a family of transitions representing autonomous transitions in each net-token. For a set T^*_{nat} of transitions of N^* we define a set of similar autonomous transitions as follows.*



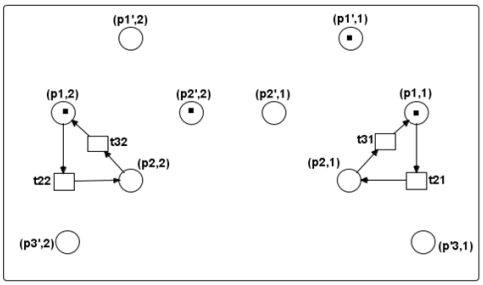


Fig. 4. Transitions and arcs from Rule 3 Fig. 5, Transitions and arcs after Rule 4

$$T^*_{nat} \coloneqq \bigcup_{i\in\Sigma_{nt}}\{t|t_i \in T_i \wedge t_i is\ an\ object\ autonomous\ transition\}. \quad (19)$$

We define a set F^*_{nat} of arcs of net-token autonomous transitions in N^*as follows:

$$F^*_{nat} = \{(p, i), t) \in$$

$$P_{N^*} \times T^*_{nat}|(p, t) \in F_i > 0\} \cup \{(t, (p.\, i) \in T^*_{nat} \times P_{N^*}|(t, p) \in F_i > 0\}. \quad (20)$$

This is depicted in Fig.5.

Rule 5: *Generate a family of transitions representing synchronisation transitions obtained from the system net and net-tokens. An occurrence of a synchronous firing presumes simultaneous occurrence of a transition $\hat{t} \in \hat{T}$ with a set of transitions given by a binding β in system net, and some net-tokens transitions$(t_1, \dots, t_k) \in \ell$. This can be viewed as a combination of Rule 3 and Rule 4 with the condition that all involved transitions must be an elements in the transition relation ℓ of an ERS.*

Transitions $(t_1, \dots, t_k)$ occur simultaneously with $\hat{t} \in \hat{T}$ of a system net, if $(\hat{t}, (t_i, \dots, t_k)) \in \boldsymbol{\ell}$. We generate synchronisation transitions from an ERS in a P/T-net N^* accordingly. This implies that we will have $|\ell|$ such transitions in N^*. Each of these transitions is composed of a system net transition $\hat{t} \in \hat{T}$, and some transitions of net-tokens that participate in synchronous firing of $\hat{t}$. They are defined as follows.

$$T^*_{sync_i} \coloneqq \bigcup_{i=1}^{k}\{t_{i.\beta_i(x)} = \{\hat{t}, t_1, \dots, t_k\}|x \in w(\hat{t}), \hat{t} \in \hat{T}, t_1 \in T_1, \dots, t_k \in T_k\}. \quad (21)$$

In our example two places $\hat{p}_1$ and $\hat{p}_2$ are marked with one net-token each in the initial marking. We add two transitions $t_1 = \{\{\hat{t}_1, t_{21}, \tau\}$ and $t_2 = \{\hat{t}_1, \tau, t_{22}\}$ annotated with @1 and @2, which is shown in Fig.6. The result of transforming ERS into P/T-net is shown in Fig. 7.

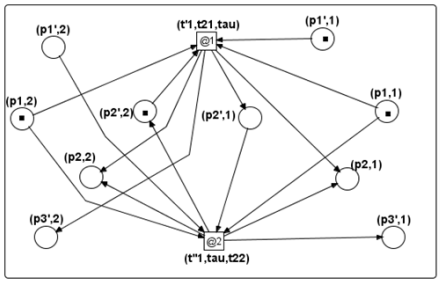


Fig. 6. Synchronous firing transitions and arcs

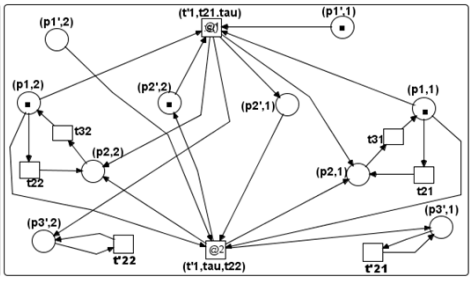


Fig. 7. Result of transforming ERS

5 Isomorphic Properties of the State Spaces

We establish an isomorphism between the states of an ERS and the generated 1-safe P/T-net. Recall that in Rule 2 we defined two separate initial markings for the P/T-net N^*: $M_0^*(\hat{p}, i)$ and $M_0^*(p, i)$. The former is an encoding of markings from the set of places $\hat{P}$ of the system net in an ERS and the latter is an encoding of markings from the set of places P_i of a net-token i. Likewise, we defined three sets of transitions: T_{sat}^*, T_{nat}^*, and $T_{sync_i}^*$ from Rule 3, Rule 4 and Rule 5 respectively in N^*. In the following, we define some mappings from the P/T-net to and ERS.

Definition 5.1 *A mapping $\hat{f}$ maps a marking M^* of a P/T-net N^* from the set of places $\hat{P}$ to markings R of a system net of an ERS as follows:*

$$\hat{f}(M^*)(\hat{p}, i) = R(\hat{p}) \; such \; that \; (\hat{p}, i) \in P_{N^*}^* : \hat{p} \in \hat{P} : i \in \mathbb{R} \,. \tag{22}$$

Definition 5.2 *A mapping f maps a marking M^* of a P/T-net N^* from the set of places P_i of net-token i of ERS to a marking M of a net-token of ERS as follows:*

$$f(M^*)(p, i) = M(p) \; such \; that \; (p, i) \in P_{N^*}^* : p \in P_i : i \in \mathbb{R} \,. \tag{23}$$

Definition 5.3 $\hat{g}$ Is a mapping that maps a transition $t'_{\beta_i(x)} \in T_{sat}^*$ of P/T-net N^* to a system-autonomous firing mode $(\hat{t}, \tau) \notin dom(\ell)$ of an ERS as follows:

$$\hat{g}\left(t'_{\beta_i(x)}\right) = (\hat{t}, \tau) \,. \tag{24}$$

where $\beta_i(x)$ is a binding function that binds a variable $x \in w(\hat{t})$ on arcs adjacent to $\hat{t}$ to an object net name.

Definition 5.4 *g is a function that maps a transition $t \in T_{nat}^*$ of P/T-net N^* to an object-autonomous firing mode $(\tau, t_i) \notin dom(\ell)$ of an ERS as follows:*

$$g(t) = (\tau, t_i) \,. \tag{25}$$

Definition 5.5 *g_s is a mapping function that maps a transition $t_{i.\beta_i(x)} \in T_{sync_i}^*$ of P/T-net N^* to a synchronisation firing mode $(\hat{t}, t_1, \ldots, t_k) \in \ell$ of an ERS as follows:*

$$g_s\left(t_{i.\beta_i(x)}\right) = \{(\hat{t}, t_1, \ldots, t_k)\}\,. \tag{26}$$

The following lemmas related to $\widehat{N}$ and N^*constructed by Rules 1 to 5, hold.

Lemma 5.6 *For the initial marking at $\widehat{N}$ level, the following equality holds:*

$$R^0(\hat{p}) = \hat{f}(M_0^*)(\hat{p}, i)\,. \tag{27}$$

Lemma 5.7 *Suppose that $R = \hat{f}(M^*)$ and$(\hat{t}, \tau) = \hat{g}(t'_{\beta_i(x)})$. The following proposition holds:*

$$M^*[t'_{\beta_i(x)} > \Leftrightarrow R[(\hat{t}, \tau) >\,. \tag{28}$$

Lemma 5.8 *Suppose that $R_1 = \hat{f}(M_1^*)$, $M_1^*[t'_{\beta_i(x)} > M_2^*$, and $R_1[\hat{g}\left(t'_{\beta_i(x)}\right) > R_2$. The following equality holds: $R_2 = \hat{f}(M_2^*)$.*

Lemma 5.9 *For the initial marking of the object net, the following holds:*

$$M^0(p) = f(M_0^*)(p, i)\,. \tag{30}$$

Lemma 5.10 *Suppose that $M = f(M^*)$ and$(\tau, t_i) = g(t)$. The following proposition holds:*

$$M^*[g(t) > \Leftrightarrow M[\left((\tau, t_i)\right) >\,. \tag{31}$$

Lemma 5.11 *Suppose that $M_1 = f(M_1^*)$, $M_1^*[t > M_2^*$, and $M_1[g(t) > M_2$. The following equality holds:*

$$M_2 = f(M_2^*)\,. \tag{32}$$

Lemma 5.12 *Suppose that $(R_1, M_1) = f_s(M_1^*)$ and $t_s = g_s\left(t_{i.\beta_i(x)}\right)$. The following proposition holds:*

$$M_1^*[g_s\left(t_{i.\beta_i(x)}\right) > \Leftrightarrow (R_1, M_1)[t_s >\,. \tag{33}$$

Lemma 5.13 *Suppose$(R_1, M_1) = f_s(M_1^*)$, $M_1^*[t_{i.\beta_i(x)} > M_2^*$ and $(R_1, M_1)[g_s\left(t_{i.\beta_i(x)}\right) > (R_2, M_2)$.*

The following equality holds:

$$(R_2, M_2) = f_s(M_2^*)\,. \tag{34}$$

From the above Lemmas, the following theorem holds.

Theorem 5.14 Let RS be a 1-safe ERS. Let also N*be a 1-safe P/T-net obtained from RS by the set of transformation Rules 1 to 5 above. Then state spaces of RS and N* are isomorphic.

Proof: Lemmas5.6 and 5.9 defines a one-to-one mapping between the initial markings of the 1-safe P/T-net $N^*$and the initial marking in RS. From Lemma 5.7 a system-autonomous firing mode $(\hat{t}, \tau)$ is enabled in a marking (R, M) if, and only if, the corresponding transition $t'_{\beta_i(x)}$ is enabled in the corresponding marking M^*. Also from Lemma 5.10 an object-autonomous firing mode (τ, t_i) is enabled in a marking

(R, M) *if, and only if, the corresponding transition* t *is enabled in the corresponding marking* M^*. *Again, from Lemma 5.12 a synchronous firing mode* $(\hat{t}, t_1, \ldots, t_k)$ *is enabled in a marking* (R, M) *if, and only if, the corresponding transition* $t_{i.\beta_i(x)}$ *is enabled in the corresponding* M^*. *Finally from Lemmas 5.8, 5.11 and 5.13, the generated markings in the 1-safe P/T-net can be mapped to the generated markings in the RS.* □

Thus we have shown that every ERS can be transformed to behaviourally equivalent 1-safe P/T-net. Hence the standard analysis techniques for 1-safe P/T-net can be applied for ERS.

6 Conclusion

While general elementary object systems (EOS) come with some constraints that limit their expressiveness for automatic verification purposes, in this paper a modification that relaxes these constraints was given: *elementary reference-net systems, ERS*. Also, we proposed a set of rules for transforming ERS to behaviourally equivalent 1-safe P/T nest. Furthermore, we established an important relationship between the isomorphic properties of state spaces of 1-safe ERS and 1-safe P/T net. Among such results are the established Lemmas, and the proof of a theorem which relates the state space of 1-safe P/T nets 1-safe ERS. The definition of elementary reference-net system, ERS, targets practical relevance and the use of a partial order (unfolding) approach for dynamic analysis of EOS. In future work, we aim to compare an unfolding of the transformed 1-safe P/T to a direct unfolding of a 1-safe ERS without computing an intermediate expansion.

References

Köhler, M. and Heitmann, F., 2009. On the expressiveness of communication channels for object nets. *Fundamenta Informaticae*, *93*(1-3), pp.205-219.

Köhler, M. and Rölke, H., 2004. Properties of object Petri nets. In Applications and Theory of Petri Nets 2004 (pp. 278-297). Springer Berlin Heidelberg.

Lomazova, I.A. and Schnoebelen, P., 1999, July. Some decidability results for nested Petri nets. In Perspectives of System Informatics (pp. 208-220). Springer Berlin Heidelberg.

Lomazova, I.A. and Ermakova, V.O., 2016 Verification of Nested Petri Nets Using an Unfolding Approach.

Miyamoto, T. and Horiguchi, K., 2013. Modular reachability analysis of Petri nets for multiagent systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 43(6), pp.1411-1423.

Valk, R., 1991. Modelling concurrency by task/flow EN systems. In 3rd Workshop on Concurrency and Compositionality (Vol. 191).

Valk, R., 2003. Object Petri nets: Using the nets-within-nets paradigm, Advanced Course on Petri Nets 2003 (J. Desel, W. Reisig, G. Rozenberg, Eds.), 3098.

Appendix A: Proof of Theorem 3.10

Proof. Let RS be a safe ERS. Let$m := |\hat{P}|$and $n := max\{|P_i| \mid (i, (P_i.T_i, F_i), m_i) \in \mathcal{N}\}$ be the number of system net places and the maximum number of places present in an object net, respectively.

By definition of safe ERS each net token is 1-safe and hence there are at most 2^n different markings a net-token may have. By definition of safe ERS each system net place is either marked or unmarked with a net-token with one of these markings, thus there are up to $(1 + 2^n)^m$ different markings of RS, i.e. $|R(RS)| \leq (1 + 2^n)^m$. □

Appendix B: Proof of Lemma 5.6

Proof: An initial marking of a system net in an ERS can be expressed by $R^0 = R^0(\hat{p}), \forall \hat{p} \in \hat{P}$. *By Rule 2,* $(\hat{p}, i) \in P^*_{N^*}$ *in the P/T-net has one token in the corresponding initial marking* $M^*_0(\hat{p}, i)$, *therefore* $M^*_0(\hat{p}, i) = R^0(\hat{p})$.

From Def. 5.1, $\hat{f}(M^*_0)(\hat{p}, i)$ *becomes* $\hat{f}(M^*_0)(\hat{p}, i) = R^0(\hat{p}) = R^0(\hat{p})$ □

Appendix C: Proof of Lemma 5.7

Proof: (⇒) *Suppose that* $t'_{\beta_i(x)} \in T^*_{sat}$ *is a transition that represents an autonomous transition in the P/T- net then* $(\hat{t}, \tau) \in \hat{T}$ *is a corresponding transition in the system net. From* $M^*[t'_{\beta_i(x)} >$ *and Def. 2.3, each place has at least* $W^*_{sat}((\hat{p}, i), t'_{\beta_i(x)})$ *tokens namely for each place* $(\hat{p}, i) \in P^*_{N^*}$, *the following inequality holds:*

$$M^*\big((\hat{p}, i)\big) \geq W^*_{sat}\left((\hat{p}, i), t'_{\beta_i(x)}\right). \tag{35}$$

Since $R = \hat{f}(M^*)$, *the number of token in place* $(\hat{p}, i)$ *equals the number of tokens in place* $\hat{p} \in \hat{P}$ *of a system net* $\hat{N}$:

$$M^*\big((\hat{p}, i)\big) = R(\hat{p}). \tag{36}$$

From Rule 3, the weight of the arc from $(\hat{p}, i)$ *to* $t'_{\beta_i(x)}$ *equals number of variables on the arc from* $\hat{p}$ *to* $\hat{t}$ *under the binding* β:

$$W^*_{sat}\left((\hat{p}, i), t'_{\beta_i(x)}\right) = \beta\big(w(\hat{p}, \hat{t})\big). \tag{37}$$

From (35), (36) & (37), for each place $\hat{p} \in \hat{P}$ *the following holds:*

$$R(\hat{p}) \geq \beta\big(w(\hat{p}, \hat{t})\big). \tag{38}$$

From Def. 3.5, $R[(\hat{t}, \tau) >$.

(⇐)*(38) holds since* $R[(\hat{t}, \tau) >$; *(36) & (37) also hold. Therefore, (35) holds. From Def. 2.3,* $M^*[t'_{\beta_i(x)} >$

Appendix D: Proof of Lemma 5.8

Proof: From Def. 2.3, the number of tokens in place $(\hat{p}, i)$ *in a successor marking* M_2^* *is expressed as follows:*

$$M_2^*(\hat{p}, i) = M_1^*(\hat{p}, i) - W_{sat}^*\left((\hat{p}, i), t'_{\beta_i(x)}\right) + W_{sat}^*\left(t'_{\beta_i(x)}, (\hat{p}, i)\right). \quad (39)$$

Since $R_1 = \hat{f}(M_1^*)$*, (30) holds. Similarly to (31), it holds that*

$$W_{sat}^*\left(t'_{\beta_i(x)}, (\hat{p}, i)\right) = \beta\big(w(\hat{t}, \hat{p})\big). \quad (40)$$

Therefore: $M_2^*(\hat{p}, i) = R_1(\hat{p}) - \beta\big(w(\hat{p}, \hat{t})\big) + \beta\big(w(\hat{t}, \hat{p})\big)$ *. (See Def. 3.5&* 36) (41)

Finally it holds that $R_2 = \hat{f}(M_2^*)$ *because (41) holds for each place.* □

Appendix E: Proof of Lemma 5.9

Proof: An initial marking of an object net in an ERS can be expressed by $M^0 = M^0(p), \forall p \in P_i,\ i \in \mathbb{R}$ *hold. Rule 2 says that place* $(p, i) \in P_{N^*}^*$ *in the P/T-net has one token in the corresponding initial marking* $M_0^*(p, i)$*, therefore* $M_0^*(p, i) = M^0(p)$.

From Def. 5.2, $f(M_0^*)(p, i)$ *becomes* $f(M_0^*)(p, i) = M^0(p)$ □

Appendix F: Proof of Lemma 5.10

Proof: (⇒) *Suppose that* $t \in T_{nat}^*$ *is a transition that represents an autonomous transition in the P/T- net then* $(\tau, t_i) \in T_i$ *is a corresponding transition in the object net. From* $M^*[t >$ *and the Def. 2.3, each place has at least* $W_{nat}^*((p, i), t)$ *tokens namely for each place* $(p, i) \in P_{N^*}^*$*, the following inequality holds:*

$$M^*\big((p, i)\big) \geq W_{nat}^*\big((p, i), t\big). \quad (42)$$

Since $M = f(M^*)$*, the number of tokens in*(p, i) *equals the number of tokens in* $p \in P_i$ *of an object net* N_i*:*

$$M^*\big((p, i)\big) = M(p). \quad (43)$$

From Rule 4, the weight of the arc from (p, i) *to* t *equals the weight of the arc from* p_i *to* t_i

$$W_{nat}^*\big((p, i), t\big) = W_i(p_i, t_i). \quad (44)$$

From (40) and (41), for each place $p \in P_i$ *the following inequality holds:*

$$M(p) \geq W_i(p_i, t_i). \quad (45)$$

From Def. 4.6, $M[(\tau, t_i) >$.

(⇐)*(45) holds since* $M[(\tau, t_i) >$*; (43) & (44) also hold. Therefore, (42) holds. From Def.2.3,* $M^*[t >$. □

Appendix G: Proof of Lemma 5.11

Proof: From Def. 2.3.2, the number of tokens in place (p, i) *in a successor marking* M_2^* *is expressed as follows:*

$$M_2^*(p,i) = M_1^*(p,i) - W_{nat}^*\big((p,i),t\big) + W_{nat}^*\big(t,(p,i)\big)\,. \tag{46}$$

Since $M_1 = f(M_1^*)$*, (43) holds. Similarly to (44), it holds that*

$$W_{nat}^*\big(t,(p,i)\big) = W_i(p_i,t_i)\,. \tag{47}$$

Therefore, the following equation holds:

$$M_2^*(p,i) = M_1(p_i) - W_i(p_i,t_i + W_i(t_i,p_i) = M_2^*(p,i) \text{ (See Def. 3.6)} \tag{48}$$

Finally it holds that $M_2 = f(M_2^*)$ *because (46) holds for each place.* □

Appendix H: Proof of Lemma 5.12

Proof: (⇒) *For* $\hat{t}$*, it can be proved in a similar way to Lemma 5.7 that*

$$\forall \hat{p} \in {}^\bullet\hat{t}\colon R(\hat{p}) \geq \beta\big(w(\hat{t},\hat{p})\big)\,. \tag{49}$$

For $(t_1,\dots,t_k)$ *it can be proven in a similar to Lemma 5.10 for each net-token transition* $t_i \in T_i$ *that*

$$\forall p_i \in {}^\bullet t_i\colon M_1(p_i) \geq W_i(p_i,t_i)\,. \tag{50}$$

From Rule 5, and equations (48) and (49) it holds that $(R_1, M_1)[t_s >$.

(⇐) *For* $t_{i.\beta_i(x)} \in T_{sync_i}^*$ *which is added in Rule 5, it can be shown that in a similar way to Lemma 5.7 that*

$$\forall (\hat{p},i) \in {P'}_{N^*}\colon M_1^*\big((\hat{p},i)\big) \geq W^*\big((\hat{p},i),\hat{t}\big)\,. \tag{51}$$

Similarly, it can be shown from Lemma 5.10 for $t_i \in T_i$ *that participate in* $t_{i.\beta_i(x)} \in T_{sync_i}^*$ *that*

$$\forall (p_i,i) \in P_{N^*}\colon M_1^*(p_i,i) \geq W_{nat}^*(p_i,t_i). \tag{52}$$

The action $(\hat{t},t_1,\dots,t_k)$ *share no input places by assumption in Rule 1. From Def. 2.3, (51) & (52):* $M_1^*[t_{i.\beta_i(x)} >$. □

Appendix I: Proof of Lemma 5.13

Proof: It can be proved in a similar way to Lemma 5.8 and 5.11 by Def. 2.3, and Rules 3 & 4. □