Local state refinement on Elementary Net Systems: an approach based on morphisms

Luca Bernardinello, Elisabetta Mangioni, and Lucia Pomello

Dipartimento di Informatica Sistemistica e Comunicazione,
Università degli studi di Milano - Bicocca,
Viale Sarca, 336 - Edificio U14 - I-20126 Milano, Italia
mangioni@disco.unimib.it

Abstract. In the design of concurrent and distributed systems, modularity and refinement are basic conceptual tools. We propose a notion of refinement/abstraction of local states for a basic class of Petri Nets, associated with a new kind of morphisms. The morphisms, from a refined system to an abstract one, associate suitable subnets to abstract local states. The main results concern behavioural properties preserved and reflected by the morphisms. In particular, we focus on the conditions under which reachable markings are preserved or reflected, and the conditions under which a morphism induces a bisimulation between net systems.

Keywords: Elementary Net Systems, morphisms, local state refinement

1 Introduction

Refinement and composition of modules are among the basic conceptual tools of a system designer. Several formal approaches are available. One of the main challenges consists in developing languages and methods allowing to derive properties of the refined system from properties of the abstract one.

We propose an approach based on Petri nets, where the refinement of a model is supported by so-called α-morphisms on the class of Elementary Net Systems. We focus on the refinement of local states. Given a net N_2, interpreted as an abstract description of a system, the local states of N_2 are replaced by subnets, giving a new net, say N_1, so that there is an α-morphism from N_1 to N_2.

Using morphisms to formalize the relation between a refined net and a more abstract one is not new. Most approaches, in Petri net theory, are based on transition refinement and, less frequently, on place refinement; for a survey, see [5]. Another survey paper, [9], describes a set of techniques which allow to refine transitions in Place/transition nets, so that the relation between the abstract net and its refinement is given by a morphism. There, the emphasis is on refinement rules that preserve specific behavioural properties, within the wider context of general transformation rules on nets.

A very general class of morphisms, interpreted as abstraction of system requirements, with less focus on strict preservation of behavioural properties, is defined in [6].

The approach we present in this paper is similar in spirit to the refinement operation proposed in [8]. In that approach, refinement is defined on transition systems, but is strictly related to refinement of local states in nets, through the notion of region.

α-morphisms can be seen as a special case of the morphisms introduced by Winskel in [13], as it will be formally shown in Section 5. Other morphisms introduced in the literature on the same line of Winskel morphisms, are the ones given in [12] and [1].

Our approach is motivated by the attempt to define a refinement operation preserving behavioural properties on the basis of structural and only local behavioural constraints. The additional restrictions, with respect to general morphisms, aim, on one hand, to capture typical features of refinements, and on the other hand to ensure that some behavioural properties of the abstract model still hold in the refined model.

Moreover, in [2], we use α-morphisms as a means supporting a composition operator defined through an interface, following the same approach proposed in [4].

In the rest of this section, the main ideas of refinement and related morphisms are explained by means of a simple example. In Section 2 we collect preliminary definitions related to Petri nets which are used in the rest of the paper. Section 3 contains the definition of α-morphisms and the main results of the paper: in particular, we show that reachable markings are preserved, we characterize the local conditions under which reachable markings are reflected, i.e.: under which the counterimage of reachable markings are reachable markings, and such that morphisms induce a bisimulation between the related net systems. In Section 5 we compare α-morphisms with Winskel's morphisms. Finally, in Section 6 we discuss some critical issues in our approach and suggest possible developments.

Most proofs are given in an extended version of the present paper [3].

1.1 An example

The example presented in this section aims at explaining, informally, how α-morphisms support refinement of local states in Elementary Net Systems. The morphism maps nodes of a refined system, N_1, on a more abstact one, N_2.

The Elementary Net System shown in Fig. 1 represents an abstract view of the interaction between a student and an University secretariat office. A student may ask the office either to emit an English proficiency certificate or to admit her to the final exam. Note that, at this level of abstraction, the model does not distinguish a positive answer from a negative one. Suppose that the local state inspect_request corresponds to the actual inspection of the request by a Faculty board, which delivers the decision to the secretariat.

We might want to refine formal_check, in order to distinguish two cases: positive answer and negative answer.

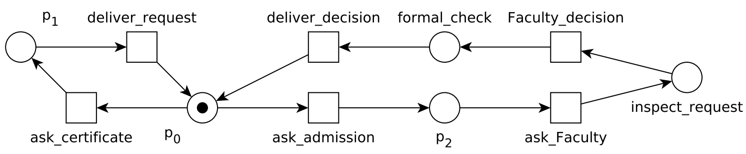


Fig. 1: Abstract view (N_2)

The actual decision has been taken in state inspect_request, so the refinement of formal_check requires splitting the event Faculty_decision, thus reflecting the choice between the two answers. The result of the refinement is shown in Fig. 2,

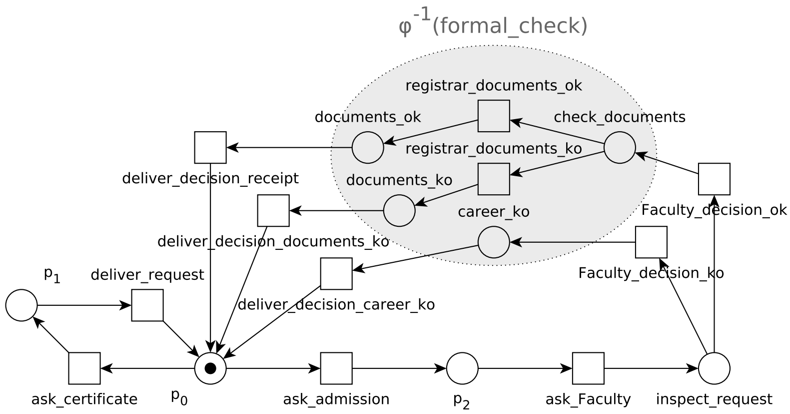


Fig. 2: Refined model (N_1)

where the subnet refining formal_check is enclosed in a shaded oval. Note that the operation has required also splitting the outgoing transitions, in order to reflect the alternative outcomes.

2 Preliminary definitions

In this section, we recall the basic definitions of net theory, in particular Elementary Net Systems [11], and bisimulation [7].

We will use the symbol $\downarrow$ to denote the restriction of a function on a subset of its domain.

2.1 Petri Nets

In net theory, models of distributed systems are based on objects called nets which specify local states, local transitions and the relations among them. A *net* is a triple $N = (B, E, F)$, where B is a set of *conditions* or local states, E is a set of *events* or transitions such that $B \cap E = \emptyset$ and $F \subseteq (B \times E) \cup (E \times B)$ is the *flow relation*.

We adopt the usual graphical notation: conditions are represented by circles, events by boxes and the flow relation by arcs. The set of elements of a net will be denoted by $X = B \cup E$; we allow nets with isolated elements.

The *preset* of an element $x \in X$ is ${}^\bullet x = \{y \in X | (y, x) \in F\}$; the *postset* of x is $x^\bullet = \{y \in X | (x, y) \in F\}$; the *neighbourhood* of x is given by ${}^\bullet x^\bullet = {}^\bullet x \cup x^\bullet$. These notations are extended to subsets of elements in the usual way.

For any net N we denote the *in-elements* of N by ${}^\bigcirc N = \{x \in X_N : {}^\bullet x = \emptyset\}$ and the *out-elements* of N by $N^\bigcirc = \{x \in X_N : x^\bullet = \emptyset\}$.

A net is *simple* if for all $x, y \in X$, if ${}^\bullet x = {}^\bullet y$ and $x^\bullet = y^\bullet$, then $x = y$.

A net $N' = (B', E', F')$ is a *subnet* of $N = (B, E, F)$ if $B' \subseteq B, E' \subseteq E$, and $F' = F \cap ((B' \times E') \cup (E' \times B'))$. Given a subset of elements $A \subseteq X$, we say that $N(A)$ is the *subnet of N identified* by A if $N(A) = (B \cap A, E \cap A, F \cap (A \times A))$.

A *State Machine* is a connected net such that each event e has exactly one input condition and exactly one output condition: $\forall e \in E, |{}^\bullet e| = |e^\bullet| = 1$.

Elementary Net (EN) Systems are a basic system model in net theory. An *Elementary Net System* is a quadruple $N = (B, E, F, m_0)$, where (B, E, F) is a net such that B and E are finite sets, self-loops are not allowed, isolated elements are not allowed, and the *initial marking* is $m_0 \subseteq B$.

The elements in the initial marking are interpreted as the conditions which are true in the initial state.

A subnet of an EN System N identified by a subset of conditions A and all its pre and post events, $N(A \cup {}^\bullet A^\bullet)$, is a *Sequential Component* of N if $N(A \cup {}^\bullet A^\bullet)$ is a State Machine and if it has only one token in the initial marking.

An EN System is *covered* by Sequential Components if every condition of the net belongs to at least a Sequential Component. In this case we say that the system is *State Machine Decomposable (SMD)*.

The behaviour of EN Systems is defined through the firing rule, which specifies when an event can occur, and how event occurrences modify the holding of conditions, i.e. the state of the system.

Let $N = (B, E, F, m_0)$ be an EN System, $e \in E$ and $m \subseteq B$. The event e is *enabled* at m, denoted $m\,[e\rangle$, if ${}^\bullet e \subseteq m$ and $e^\bullet \cap m = \emptyset$; the occurrence of e at m leads from m to m', denoted $m\,[e\rangle\, m'$, iff $m' = (m \setminus {}^\bullet e) \cup e^\bullet$.

Let ϵ denote the empty word in E^*. The firing rule is extended to sequences of events by setting $m\,[\epsilon\rangle\, m$ and $\forall e \in E, \forall w \in E^*, m\,[ew\rangle\, m' = m\,[e\rangle\, m''[w\rangle m''$; w is called *firing sequence*.

A subset $m \subseteq B$ is a *reachable marking* of N if there exists a $w \in E^*$ such that $m_0\,[w\rangle\, m$. The *set of all reachable markings* of N is denoted by $[m_0\rangle$.

An EN System is *contact-free* if $\forall e \in E, \forall m \in [m_0\rangle$: ${}^\bullet e \subseteq m$ implies $e^\bullet \cap m = \emptyset$. An EN System covered by Sequential Components is contact-free. An event is called *dead* at a marking m if it is not enabled at any marking reachable from m. A reachable marking m is called *dead* if no event is enabled at m. An Elementary Net System is *deadlock-free* if no reachable marking is dead.

2.2 Unfoldings

The semantics of an EN System can be given as its *unfolding*. The unfolding is an acyclic net, possibly infinite, which records the occurrences of its elements in all possible executions.

Definition 1. *Let $N = (B, E, F)$ be a net, and let $x, y \in X$. We say that x and y are in* conflict*, denoted by $x \#_N y$, if there exist two distinct events $e_x, e_y \in E$ such that $e_x F^* x$, $e_y F^* y$, and ${}^\bullet e_x \cap {}^\bullet e_y \neq \emptyset$.*

Definition 2. *An occurrence net is a net $N = (B, E, F)$ satisfying:*

1. *if $e_1, e_2 \in E, e_1{}^\bullet \cap e_2{}^\bullet \neq \emptyset$ then $e_1 = e_2$;*
2. *F^* is a partial order,*
3. *for any $x \in X, \{y : yF^*x\}$ is finite;*
4. *$\#_N$ is irreflexive,*
5. *the minimal elements with respect to F^* are conditions.*

A branching process of N is an occurrence net whose elements can be mapped to the elements of N.

Definition 3. *Let $N = (B, E, F, m_0)$ be an EN System, and $\Sigma = (P, T, G)$ be an occurrence net. Let $\pi : P \cup T \to B \cup E$ be a map.*
The pair (Σ, π) is a branching process of N if:

- *$\pi(P) \subseteq B$, $\pi(T) \subseteq E$;*
- *π restricted to the minimal elements of Σ is a bijection on m_0;*
- *for each $t \in T$, π restricted to ${}^\bullet t$ is injective and π restricted to $t^\bullet$ is injective;*
- *for each $t \in T$, $\pi({}^\bullet t) = {}^\bullet(\pi(t))$ and $\pi(t^\bullet) = ({}^\bullet \pi(t))$.*

The unfolding of an EN System N, denoted by *Unf*(N), is the maximal branching process of N, namely the unique branching process such that any other branching process of N is isomorphic to a subnet of *Unf*(N). The map associated to the unfolding will be denoted u and called *folding*.

2.3 Bisimulations

Bisimulation relations have been introduced as equivalence notions with respect to event observation [7]. We define the observability of events of a system by using a labelling function which associates the same label to different events, when viewed as equal by an observer, and the label τ to unobservable events.

Definition 4. *Let $N = (B, E, F, m_0)$ be an EN System, $l : E \to L \cup \{\tau\}$ be a labelling function where L is the alphabet of observable actions and $\tau \notin L$ the unobservable action. Let ϵ denote the empty word both of E^* and L^*. The function l is extended to a homomorphism $l : E^* \to L^*$ in the following way:*

$$l(\epsilon) = \epsilon$$

$$\forall e \in E, \forall w \in E^*, l(ew) = \begin{cases} l(e)l(w) & \textit{if } l(e) \neq \tau \\ l(w) & \textit{if } l(e) = \tau \end{cases}$$

The pair (N, l) *is called* Labelled *EN System.*
Let $m, m' \in [m_0\rangle$ *and* $a \in L \cup \{\epsilon\}$ *then:*

– *a is enabled at m, denoted* $m\,(a\rangle$*, iff* $\exists w \in E^* : l(w) = a$ *and* $m\,[w\rangle$*;*
– *if a is enabled at m, then the occurrence of a can lead from m to m', denoted* $m\,(a\rangle\, m'$*, iff* $\exists w \in E^* : l(w) = a$ *and* $m\,[w\rangle\, m'$*.*

We define weak bisimulation as a relation between reachable markings of Labelled EN Systems [10].

Definition 5. *Let* $N_i = (B_i, E_i, F_i, m_0^i)$ *be an EN System for* $i = 1, 2$*, with the labelling function* $l_i : E_i \to L \cup \{\tau\}$*. Then* (N_1, l_1) *and* (N_2, l_2) *are* weakly bisimilar*, denoted* $(N_1, l_1) \approx (N_2, l_2)$*, iff* $\exists r \subseteq [m_0^1\rangle \times [m_0^2\rangle$ *such that:*

– $(m_0^1, m_0^2) \in r$*;*
– $\forall (m_1, m_2) \in r, \forall a \in L \cup \{\epsilon\}$ *it holds*

$$\forall m_1' : m_1\,(a\rangle\, m_1' \Rightarrow \exists m_2' : m_2\,(a\rangle\, m_2' \wedge (m_1', m_2') \in r$$

and (vice versa)

$$\forall m_2' : m_2\,(a\rangle\, m_2' \Rightarrow \exists m_1' : m_1\,(a\rangle\, m_1' \wedge (m_1', m_2') \in r$$

Such a relation r is called weak bisimulation.

For short in the rest of the paper we will use the term *bisimulation* instead of *weak bisimulation.*

3 A class of morphisms

In this section we present the formal definition of α-morphisms for State Machine Decomposable Elementary Net Systems (SMD-EN Systems), and discuss some of their properties, particularly with respect to the preservation of both structural and behavioural properties.

We start by defining a more general class of morphisms, and then present the more specific restrictions.

Definition 6. *Let* $N_i = (B_i, E_i, F_i, m_0^i)$ *be a SMD-EN System, for* $i = 1, 2$*. An ω-morphism from N_1 to N_2 is a total surjective map* $\varphi : X_1 \to X_2$ *such that:*

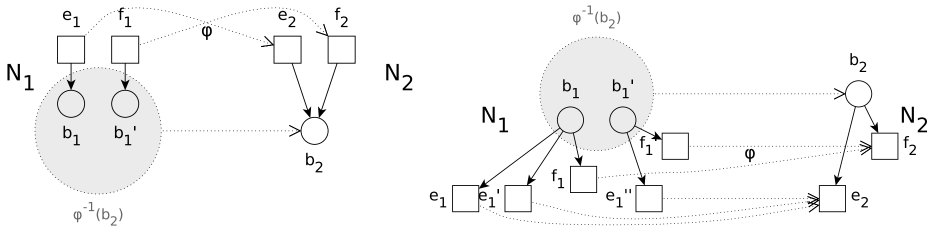
1. $\varphi(B_1) = B_2$*;*
2. $\varphi(m_0^1) = m_0^2$*;*
3. $\forall e_1 \in E_1$*, if* $\varphi(e_1) \in E_2$*, then* $\varphi({}^\bullet e_1) = {}^\bullet\varphi(e_1)$ *and* $\varphi(e_1{}^\bullet) = \varphi(e_1)^\bullet$*;*
4. $\forall e_1 \in E_1$*, if* $\varphi(e_1) \in B_2$*, then* $\varphi({}^\bullet e_1{}^\bullet) = \{\varphi(e_1)\}$*;*

We require that the map is total and surjective because N_1 refines the abstract model N_2, and any abstract element must be related to its refinement.

In particular, a subset of nodes can be mapped on a single condition $b_2 \in B_2$; in this case, we will call *bubble* the subnet identified by this subset, and denote it by $N_1(\varphi^{-1}(b_2))$; if more than one element is mapped on b_2, we will say that b_2 is *refined* by φ.

Definition 7. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be a SMD-EN System, for $i = 1, 2$. An α-morphism from N_1 to N_2 is an ω-morphism satisfying*

5. $\forall b_2 \in B_2$
  (a) $N_1(\varphi^{-1}(b_2))$ *is an acyclic net;*
  (b) $\forall b_1 \in {}^{\bigcirc}N_1(\varphi^{-1}(b_2)),\ \varphi({}^\bullet b_1) \subseteq {}^\bullet b_2$ *and* $({}^\bullet b_2 \neq \emptyset \Rightarrow {}^\bullet b_1 \neq \emptyset)$*;*
  (c) $\forall b_1 \in N_1(\varphi^{-1}(b_2))^{\bigcirc},\ \varphi(b_1{}^\bullet) = b_2{}^\bullet$*;*
  (d) $\forall b_1 \in \varphi^{-1}(b_2) \cap B_1,$
  $(b_1 \notin {}^{\bigcirc}N_1(\varphi^{-1}(b_2)) \Rightarrow \varphi({}^\bullet b_1) = \{b_2\})$ *and* $(b_1 \notin N_1(\varphi^{-1}(b_2))^{\bigcirc} \Rightarrow \varphi(b_1{}^\bullet) = \{b_2\})$*;*
  (e) $\forall b_1 \in \varphi^{-1}(b_2) \cap B_1$*, there is a sequential component* N_{SC} *of* N_1 *such that* $b_1 \in B_{SC}$ *and* $\varphi^{-1}({}^\bullet b_2{}^\bullet) \subseteq E_{SC}$.



(a) Pre events of an in-condition (b) Post events of an out-condition

Fig. 3: Pre and post event of a bubble

As we can see in Fig. 3a and 3b, in-conditions and out-conditions have different constraints, 5b and 5c respectively. As required by 5c, we do not allow that choices, which are internal to a bubble, constrain a final marking of that bubble: i.e., each out-condition of the bubble must have the same choices of the condition it refines. Instead, pre-events do not need this strict constraint (5b): hence it is sufficient only that pre-events of any in-condition are mapped on a subset of the pre-events of the condition it refines. For example, in this particular case, we know that the choice between e_1 and f_1 of Figure 3a is made before the bubble, and this is implied also by the requirement 5e) on sequential components. Moreover, the conditions that are internal to a bubble must have pre-events and post-events which are all mapped to the refined condition b_2, as required by 5d.

By requirement 5e, events in the neighbourhood of a bubble are not concurrent, as their images. Within a bubble, there can be concurrent events; however, post events are in conflict, and firing one of them will empty the bubble, as shown in Lemma 1 below.

The α-morphisms are closed by composition, the identity function on X is an α-morphism, and the composition is associative. Hence, the family of SMD-EN Systems together with α-morphisms forms a category.

The partition of elements of N_1 induced by an α-morphism $\varphi : N_1 \to N_2$ defines the structure of a net:

Definition 8. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be a SMD-EN System, for $i = 1, 2$. Let φ be an α-morphism from N_1 to N_2.*

Then φ defines an equivalence relation on X_1, where the equivalence class of $x \in X_1$ is $[x] = \{y \in X_1 | \ \varphi(y) = \varphi(x)\}$.

The quotient *of N_1 with respect to α is $N_1/\varphi = (B_1/\varphi, E_1/\varphi, F_1/\varphi, m_0^1/\varphi)$, where*

- $B_1/\varphi = \{[x] : x \in X_1, \varphi(x) \in B_2\}$;
- $E_1/\varphi = \{[x] : x \in X_1, \varphi(x) \in E_2\}$;
- $F_1/\varphi = \{([x], [y]) : x, y \in X_1, x \neq y, \exists (x, y) \in F_1\}$;
- $m_0^1/\varphi = \{[x] : x \in m_0^1\}$.

By a simple verification [3], the quotient of N_1, N_1/φ, is a SMD-EN System isomorphic to N_2.

4 Properties preserved and reflected by α-morphisms

Since we consider SMD-EN Systems, it is natural to ask whether α-morphisms preserve and reflect sequential components. Let φ be an α-morphism from N_1 to N_2. We know that, if a condition b_2 belongs to a sequential component, then also its pre- and post-events belong to the same sequential component. Hence, if b_2 is refined by a bubble $N_1(\varphi^{-1}(b_2))$, by the requirement 5e) of α-morphisms any condition of the bubble belongs to a sequential component containing any event in $\varphi^{-1}({}^\bullet b_2{}^\bullet)$. This allows one to say that the sequential components of N_2 are reflected by φ, in the sense that the inverse image of a sequential component is covered by sequential components.

Lemma 1. *Let $\varphi : N_1 \to N_2$ be an α-morphism.*

Let N_{SC2} be a sequential component of N_2. Then $\varphi^{-1}(N_{SC2})$ is covered by sequential components, each one containing all the inverse image of the neighbourhood of each condition of N_{SC2}.

Sequential components are not preserved, as we can see in Fig. 4. The sequential component of N_1 generated by $\{\varphi^{-1}(b_1), b_{5-1}, b_{6-1}\}$ is such that its image $\{b_1, b_5, b_6\}$ is not a sequential component of N_2.

The idea driving our interpretation of bubble is that the subnet corresponding to a condition "behaves" in the same way as the condition it refines. In a SMD-EN System, each condition at any time can be true or false. It is not possible that

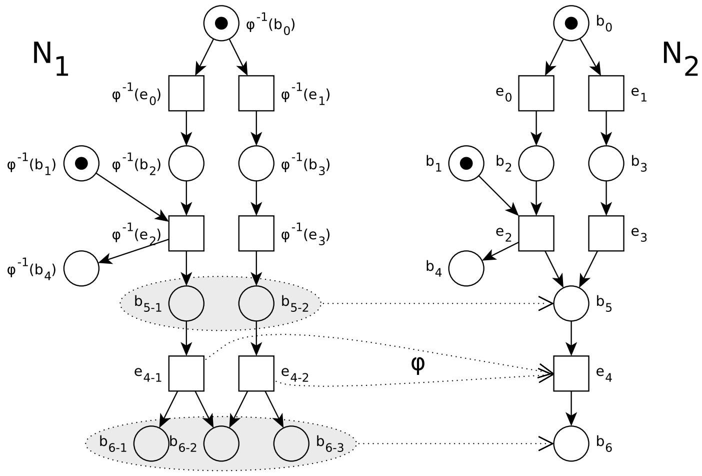


Fig. 4: Two SMD-EN Systems related by an α-morphism

this condition is partially true or partially false; hence, also the bubble should behave like this. The next lemma states that firing an output event of a bubble empties the bubble, and that no input event of a bubble is enabled whenever a token is inside the bubble.

Lemma 2. *Let $\varphi : N_1 \to N_2$ be an α-morphism. Then:*

1. *Let $e_1 \in E_1, b_2 \in B_2$: $e_1 \in \varphi^{-1}(b_2{}^\bullet)$; $m_1, m_1' \in [m_0^1\rangle$: $m_1 [e_1\rangle m_1'$, then $m_1' \cap \varphi^{-1}(b_2) = \emptyset$.*
2. *Let $e_1 \in E_1, b_2 \in B_2$: $e_1 \in \varphi^{-1}({}^\bullet b_2)$; $m_1, m_1' \in [m_0^1\rangle$: $m_1 [e_1\rangle m_1'$ then $m_1 \cap \varphi^{-1}(b_2) = \emptyset$.*

Proof. Take a marking m_1 in which a condition $b_1 \in \varphi^{-1}(b_2)$ is marked.

We know by Def. 7, point 5e) that there exists a sequential component SC of N_1 such that $b_1 \in B_{SC}$ and $\varphi^{-1}({}^\bullet b_2{}^\bullet) \subseteq E_{SC}$.

1. By contradiction, take $e_1 \in \varphi^{-1}(b_2{}^\bullet)$ such that $b_1 \notin {}^\bullet e_1$ and $m_1 [e_1\rangle$; hence all its preconditions are marked. Since SC contains e_1, one of its preconditions belongs to SC as well as b_1, this is a contradiction because the sequential component has only one token.
2. By contradiction, take $e_1 \in \varphi^{-1}({}^\bullet b_2)$ such that $m_1 [e_1\rangle$; hence all its preconditions are marked. Since SC contains e_1, one of its preconditions belongs to SC as well as b_1, and this is a contradiction because the sequential component has only one token.

□

Our morphisms can be seen like a special case of Winskel morphisms [13], as we shall prove in Section 5. Then, since Winskel morphisms preserve reachable markings, also α-morphisms do, as stated in the following.

Proposition 1. *Let $\varphi : N_1 \to N_2$ be an α-morphism.*
Then if $m_1 \in \left[m_0^1\right\rangle$ and $m_1\left[e\right\rangle m_1'$ then $\varphi(m_1) \in \left[m_0^2\right\rangle$ and

- *if $\varphi(e) \in E_2$ then $\varphi(m_1)\left[\varphi(e)\right\rangle \varphi(m_1')$ else*
- *(if $\varphi(e) \in B_2$ then) $\varphi(m_1) = \varphi(m_1')$.*

As for other morphisms in the literature, α-morphisms do not reflect reachable markings. This happens either when a condition is refined by a subnet leading to a block before reaching a marking enabling out-events, or whenever the refinements of conditions "interfere" with each other so that, even if in each bubble a "final" local marking is reached, the global marking doesn't enable any event. The second case is shown in Fig. 5: any event in each bubble can fire, but N_1 has two deadlocks: $\{p3, p6\}$ and $\{p4, p5\}$. The two above cases suggest to require

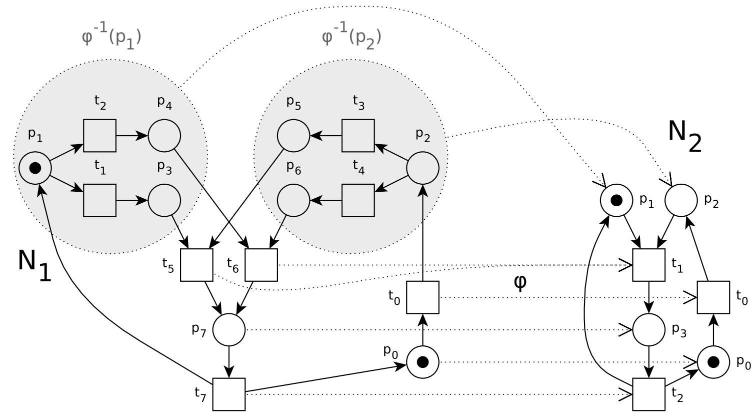


Fig. 5: An α-morphism.

both that any condition is refined by a subnet such that, when a final marking is reached, this one enables events which correspond to the post-events of the refined condition; and also that different refinements do not "interfere" with each other. The non interference is guaranteed when any event of N_2 has at most a unique condition in its neighbourhood that is properly refined in N_1.

In order to reflect the reachable markings we have to introduce local behavioural constraints and this by considering the unfolding of subnets related to the bubbles. Then, we need to define the following auxiliary construction. Given an α-morphism $\varphi : N_1 \to N_2$, and a condition $b_2 \in B_2$ with its refinement $N_1(\varphi^{-1}(b_2))$, we define two new SMD-EN Systems. The first one, denoted $S_1(b_2)$, contains (a copy of) the subnet $N_1(\varphi^{-1}(b_2))$, its pre and post-events in E_1 and two new conditions: b_1^{in}, which is pre of all the pre-events, and b_1^{out}, which is post of all the post-events. The initial marking of $S_1(b_2)$ will be $\{b_1^{in}\}$. The second system, denoted $S_2(b_2)$ contains b_2, its pre- and post-events and two new conditions: b_2^{in}, which is pre of all the pre-events, and b_2^{out}, which is post of all the post-events. The initial marking of $S_2(b_2)$ will be $\{b_2^{in}\}$.

In Fig. 6 and 7 we show the two systems $S_1(b_2)$ and $S_2(b_2)$ for the nets showed in the initial example (Fig. 1 and 2), in Section 1, with $b_2 = \mathsf{formal\_check}$.

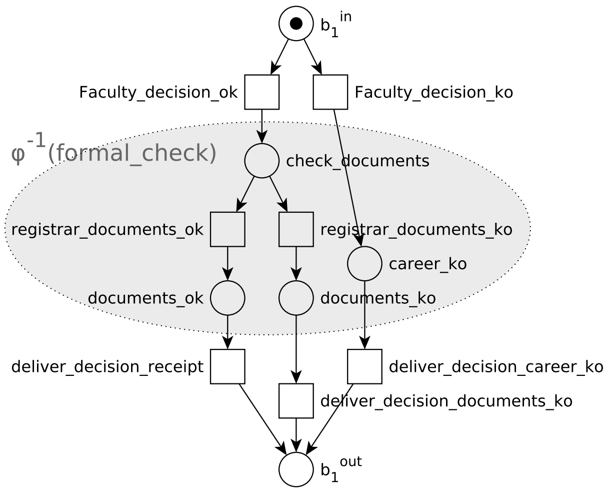


Fig. 6: $S_1(\mathsf{formal\_check})$ of Fig. 2.

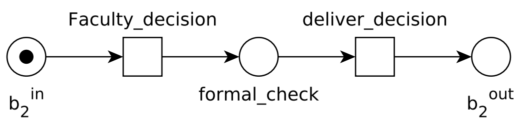


Fig. 7: $S_2(\mathsf{formal\_check})$ of Fig. 1.

Definition 9. *Let $\varphi : N_1 \to N_2$ be an α-morphism and $b_2 \in B_2$.*

Construct the SMD-EN Systems, $S_1(b_2) = (B_{S1}, E_{S1}, F_{S1}, m_0^{S1})$ and $S_2(b_2) = (B_{S2}, E_{S2}, F_{S2}, m_0^{S2})$ in this way:

$$B_{S1} = \begin{cases} (\varphi^{-1}(b_2) \cap B_1) \cup \{b_1^{out}\} & \textit{if } {}^\bullet b_2 = \emptyset \\ (\varphi^{-1}(b_2) \cap B_1) \cup \{b_1^{in}\} & \textit{if } b_2{}^\bullet = \emptyset \\ (\varphi^{-1}(b_2) \cap B_1) \cup \{b_1^{in}, b_1^{out}\} & \textit{otherwise} \end{cases}$$

$E_{S1} = (\varphi^{-1}(b_2) \cap E_1) \cup \varphi^{-1}({}^\bullet b_2) \cup \varphi^{-1}(b_2{}^\bullet)$;

$F_{S1} = (F_1 \cap ((B_{S1} \cup E_{S1}) \times (E_{S1} \cup B_{S1}))) \cup F_{S1}^{in} \cup F_{S1}^{out}$, *where*

$F_{S1}^{in} = \{(b_1^{in}, e) : e \in \varphi^{-1}({}^\bullet b_2)\}$ *and*

$F_{S1}^{out} = \{(e, b_1^{out}) : e \in \varphi^{-1}(b_2{}^\bullet)\}$;

$$m_0^{S1} = \begin{cases} m_0^1 \cap \varphi^{-1}(b_2) & \textit{if } {}^\bullet b_2 = \emptyset \\ \{b_1^{in}\} & \textit{otherwise} \end{cases}$$

$$B_{S2} = \begin{cases} \{b_2, b_2^{out}\} & \textit{if } {}^\bullet b_2 = \emptyset \\ \{b_2, b_2^{in}\} & \textit{if } b_2{}^\bullet = \emptyset \\ \{b_2, b_2^{in}, b_2^{out}\} & \textit{otherwise} \end{cases}$$

$E_{S2} = {}^\bullet b_2{}^\bullet$*;*

$F_{S2} = (F_2 \cap ((B_{S2} \cup E_{S2}) \times (E_{S2} \cup B_{S2}))) \cup F_{S2}^{in} \cup F_{S2}^{out}$*, where* $F_{S2}^{in} = \{(b_2^{in}, e) : e \in {}^\bullet b_2\}$ *and* $F_{S2}^{out} = \{(e, b_2^{out}) : e \in b_2{}^\bullet\}$*;*

$$m_0^{S2} = \begin{cases} m_0^2 \cap \{b_2\} & \textit{if } {}^\bullet b_2 = \emptyset \\ \{b_2^{in}\} & \textit{otherwise} \end{cases}$$

Define φ^S as a map from $S_1(b_2)$ to $S_2(b_2)$, which restricts φ to the elements of $S_1(b_2)$, and extends it with $\varphi^S(b_1^{in}) = b_2^{in}$ and $\varphi^S(b_1^{out}) = b_2^{out}$.

Note that $S_1(b_2)$ and $S_2(b_2)$ are SMD-EN Systems and that φ^S is an α-morphism.

Let $\varphi : N_1 \to N_2$ be an α-morphism and $\varphi^S : S_1(b_2) \to S_2(b_2)$ as in Def. 9. By using φ^S, consider two labelling functions l_1 and l_2 such that the events in E_{S2} are all observable, i.e.: l_2 is the identity function, and the invisible events of $S_1(b_2)$ are the ones mapped to conditions, i.e.:

$$\forall e \in E_{S1} : l_1(e) = \begin{cases} \varphi^S(e) & \text{if } \varphi^S(e) \in E_{S2} \\ \tau & \text{otherwise} \end{cases}$$

Let $\mathit{Unf}(S_1(b_2))$ be the unfolding of $S_1(b_2)$ with $u : \mathit{Unf}(S_1(b_2)) \to S_1(b_2)$ folding function. The following lemma shows that, if the map, $\varphi^S \circ u$, obtained composing φ^S with u is an α-morphism, then $S_1(b_2)$ and $S_2(b_2)$ are bisimilar.

Lemma 3. *Let $\varphi : N_1 \to N_2$ be an α-morphism, and φ^S as in Def. 9. Let $\mathit{Unf}(S_1(b_2))$ be the unfolding of $S_1(b_2)$ with u folding function. If $\varphi^S \circ u$ is an α-morphism from $\mathit{Unf}(S_1(b_2))$ to $S_2(b_2)$, then $r = \{(m_1, \varphi^S(m_1)) : m_1 \in [m_0^{S1}\rangle\}$ is a bisimulation, and $(S_1(b_2), l_1)$ and $(S_1(b_2), l_2)$ are bisimilar.*

In case the morphism corresponds to the refinement of a marked condition, we ask all the tokens of the corresponding bubble to be into in-conditions which are post-conditions of a pre-event, if it exists. System N_1 is then called *well marked* with respect to φ.

Definition 10. *Let $\varphi : N_1 \to N_2$ be an α-morphism. System N_1 is* well marked *with respect to φ if for each $b_2 \in B_2$ one of the following conditions hold:*

- $\varphi^{-1}(b_2) \cap m_0^1 = \emptyset$ *or*
- *if* ${}^\bullet b_2 \neq \emptyset$ *then there is* $e_1 \in \varphi^{-1}({}^\bullet b_2)$ *such that* $\varphi^{-1}(b_2) \cap m_0^1 = e_1{}^\bullet$ *or*
- *if* ${}^\bullet b_2 = \emptyset$ *then* $\varphi^{-1}(b_2) \cap m_0^1 = {}^\circ\varphi^{-1}(b_2)$

The following proposition states a set of conditions under which reachable markings are reflected by α-morphisms.

Proposition 2. *Let $\varphi : N_1 \to N_2$ be an α-morphism such that N_1 is well marked w.r.t. φ and $\varphi^S \circ u$ be an α-morphism from $\mathit{Unf}(S_1(b_2))$ to $S_2(b_2)$ then, for all $m_2 \in [m_0^2\rangle$, there is $m_1 \in [m_0^1\rangle$ such that $\varphi(m_1) = m_2$.*

Proof. We will actually show a slightly stronger property, namely that m_1 can be chosen so that its intersection with the set of conditions in the bubble refining b_2 only contains elements in $(N_1(\varphi^{-1}(b_2)))^{\bigcirc}$. The proof is by induction on the length of a firing sequence σ from m_0^2 to m_2.

Suppose $|\sigma| = 0$. Then $m_2 = m_0^2$. By definition, $\varphi(m_0^1) = m_0^2$. If $b_2 \notin m_0^2$, then $m_0^1 \cap \varphi^{-1}(b_2) = \emptyset$. If $b_2 \in m_0^2$, then we use Lemma 3 to reach in N_1 a marking in the bubble of b_2 that contains only out-conditions, and we are done.

Suppose now $|\sigma| = n+1$. Then we can write $\sigma = \sigma_1 e_2$, with $m_0^2[\sigma_1\rangle m_1^2[e_2\rangle m_2$. By the induction hypothesis, there is $m_1^1 \in [m_0^1\rangle$ such that $\varphi(m_1^1) = m_1^2$ and $m_1^1 \cap \varphi^{-1}(b_2) \subseteq (N_1(\varphi^{-1}(b_2)))^{\bigcirc}$.

Since φ is surjective, there is at least one event in E_1 that φ maps on e_2. If $b_2 \notin {}^\bullet e_2$, then there exists $e_1 \in \varphi^{-1}(e_2)$ such that $m_1^1\,[e_1\rangle$. If $b_2 \in {}^\bullet e_2$, by Lemma 3 there exists $e_1 \in \varphi^{-1}(e_2)$ such that $m_1^1\,[e_1\rangle$. $\square$

Let $N_i = (B_i, E_i, F_i, m_0^i)$ be a SMD-EN System for $i = 1, 2$ and let $\varphi : N_1 \to N_2$ be an α-morphism. By using φ, the labelling functions are defined such that E_2 are all observable, i.e.: l_2 is the identity function, and the invisible events of N_1 are the ones mapped to conditions, i.e.:

$$\forall e \in E_1 : l_1(e) = \begin{cases} \varphi(e) & \text{if } \varphi(e) \in E_2 \\ \tau & \text{otherwise} \end{cases}$$

From Prop. 1 and Prop. 2, it then follows that N_1 and N_2 are bisimilar.

Proposition 3. *Let $\varphi : N_1 \to N_2$ be an α-morphism such that N_1 is well marked and $\varphi^S \circ u$ is an α-morphism from $Unf(S_1(b_2))$ to $S_2(b_2)$ then, (N_1, l_1) and (N_2, l_2) are bisimilar $(N_1, l_1) \approx (N_2, l_2)$.*

Prop. 2 and Prop. 3 are stated in the case in which only one condition is refined, but they can be generalized to multiple refinements, provided that in the neighbourhood of each event of N_2 there is, at most, one refined condition. The examples in Fig. 5 show why this constraint is required.

5 Relations with Winskel morphisms

Let us now study the relation between ω-morphisms and Winskel morphisms, as defined in [13].

A Winskel morphism from N_1 to N_2 is a pair (η, β) with $\eta : E_1 \to_* E_2$ partial function and $\beta : B_1 \to B_2$ finitary multirelation such that $\beta(m_0^1) = m_0^2$ and $\forall e \in E : {}^\bullet(\eta(e)) = \beta({}^\bullet e)$ and $(\eta(e))^\bullet = \beta(e^\bullet)$. Note that if $\eta(e)$ is undefined, $\beta({}^\bullet e)$ and $\beta(e^\bullet)$ should be the empty set.

Given an ω-morphism from N_1 to N_2 we associate to it a Winskel morphism. This is possible by adding or deleting conditions to N_1, if needed. These conditions are *representations* of the abstract conditions refined in N_1. The obtained net is *canonical* with respect to φ as in the following definition.

Definition 11. *Let $\varphi : X_1 \to X_2$ be an ω-morphism from N_1 to N_2. N_1 is* canonical *with respect to φ if every bubble, $\varphi^{-1}(b_2)$ with $b_2 \in B_2$, contains one condition, $b_1 \in \varphi^{-1}(b_2) \cap B_1$, that satisfies the following constraints:*

- $b_1 \in m_0^1 \Leftrightarrow b_2 \in m_0^2$;
- ${}^{\bullet}b_1 = \varphi^{-1}({}^{\bullet}b_2)$;
- $b_1{}^{\bullet} = \varphi^{-1}(b_2{}^{\bullet})$.

We call that condition b_1 representation *of b_2, denoted $r_{N_1}(b_2)$.*

If N_1 is not canonical, it is always possible to construct its unique canonical version, $N_1^{\mathcal{C}}$, by adding the missing representations, and marking them as their images, or by deleting the multiple ones. The corresponding morphism, $\varphi^{\mathcal{C}}$, coincides with φ, plus the mapping of the new conditions on the corresponding conditions of N_2. It is easy to verify that the canonical version of a system, with respect to an ω-morphism to another SMD-EN Systems, is unique up to isomorphisms.

Proposition 4. *$\varphi^{\mathcal{C}}$ is an ω-morphism from $N_1^{\mathcal{C}}$ to N_2.*

Take $N_1^{\mathcal{C}}$, N_2 and $\varphi^{\mathcal{C}}$. Now, restrict $\varphi^{\mathcal{C}}$ to all the nodes of $N_1^{\mathcal{C}}$ that are not in a bubble $\varphi^{-1}(b_2)$, but for $r_{N_1}(b_2)$, for some $b_2 \in B_2$ and call it $(\varphi^{\mathcal{C}})^{rep}$.

Proposition 5. *$((\varphi^{\mathcal{C}})^{rep} \downarrow E_1^{\mathcal{C}}, (\varphi^{\mathcal{C}})^{rep} \downarrow B_1^{\mathcal{C}})$ is a Winskel morphism.*

Any α-morphism is an ω-morphism. Adding to N_1 the representation of each condition does not modify the behaviour, because of the constraint on sequential components. Hence, the result stated here hold for α-morphisms. In this sense, we consider them as a special case of Winskel morphisms.

6 Conclusions

We have presented a notion of morphism for a basic class of Petri nets with the aim of supporting refinement/abstraction of local states. The morphism, in fact, formalizes the relation between a refined net system and an abstract one, by replacing local states of the target net system with subnets. The main idea is that if one starts with an abstract model with some required behavioural properties, then, by refining local states with subnets respecting some constraints, the refined net system will maintain the required behavioural properties. Indeed, the main results concern behavioural properties preserved and reflected by the morphisms. In particular, reachable markings are preserved, and we have characterized some conditions under which reachable markings are reflected, and under which the morphisms induce a bisimulation between net systems. Since bisimulation preserves deadlock freeness, this implies for example that, starting from a deadlock-free abstract system it is possible to refine it obtaining a system which is still deadlock-free. The constraints in order to preserve/reflect behavioural properties are structural and behavioural, where the behavioural ones are only local. On this morphism in [2], we have defined a notion of composition based on interface in the line of [4]. For what concerns future work, we plan to study the constraints under which this morphism can be defined for P/T nets and Coloured nets.

Acknowledgments Work partially supported by MIUR.

References

1. Marek A. Bednarczyk and Andrzej M. Borzyszkowski. On concurrent realization of reactive systems and their morphisms. In Hartmut Ehrig, Gabriel Juhás, Julia Padberg, and Grzegorz Rozenberg, editors, *Unifying Petri Nets*, volume 2128 of *Lecture Notes in Computer Science*, pages 346–379. Springer, 2001.
2. Luca Bernardinello, Elisabetta Mangioni, and Lucia Pomello. Composition of elementary net systems based on α-morphisms. In Proc. Workshop Componet 2012, Hamburg 2012.
3. Luca Bernardinello, Elisabetta Mangioni, and Lucia Pomello. Local state refinement on elementary net systems: an approach based on morphisms. Internal report (2012), available at `http://www.mc3.disco.unimib.it/pub/bmp2012-def.pdf`.
4. Luca Bernardinello, Elena Monticelli, and Lucia Pomello. On preserving structural and behavioural properties by composing net systems on interfaces. *Fundam. Inform.*, 80(1-3):31–47, 2007.
5. Wilfried Brauer, Robert Gold, and Walter Vogler. A survey of behaviour and equivalence preserving refinements of Petri nets. *Advances in Petri Nets 1990*, pages 1–46, 1991.
6. Jörg Desel and Agathe Merceron. Vicinity respecting homomorphisms for abstracting system requirements. *Transactions on Petri Nets and Other Models of Concurrency*, 4:1–20, 2010.
7. Robin Milner. *Communication and concurrency.* Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1989.
8. Mogens Nielsen, Grzegorz Rozenberg, and P. S. Thiagarajan. Elementary transition systems and refinement. *Acta Inf.*, 29(6/7):555–578, 1992.
9. Julia Padberg and Milan Urbásek. Rule-based refinement of Petri nets: A survey. In Hartmut Ehrig, Wolfgang Reisig, Grzegorz Rozenberg, and Herbert Weber, editors, *Petri Net Technology for Communication-Based Systems*, volume 2472 of *Lecture Notes in Computer Science*, pages 161–196. Springer, 2003.
10. Lucia Pomello, Grzegorz Rozenberg, and Carla Simone. A survey of equivalence notions for net based systems. In Grzegorz Rozenberg, editor, *Advances in Petri Nets: The DEMON Project*, volume 609 of *Lecture Notes in Computer Science*, pages 410–472. Springer, 1992.
11. Grzegorz Rozenberg and Joost Engelfriet. Elementary net systems. In Wolfgang Reisig and Grzegorz Rozenberg, editors, *Petri Nets*, volume 1491 of *Lecture Notes in Computer Science*, pages 12–121. Springer, 1996.
12. Walter Vogler. Executions: A new partial-order semantics of Petri nets. *Theor. Comput. Sci.*, 91(2):205–238, 1991.
13. Glynn Winskel. Petri nets, algebras, morphisms, and compositionality. *Inf. Comput.*, 72(3):197–238, 1987.