UNIVERSITÀ DEGLI STUDI DI MILANO–BICOCCA
SCUOLA DI DOTTORATO DI SCIENZE
DOTTORATO IN INFORMATICA - XXIV CICLO

MODULARITY FOR SYSTEM MODELLING AND ANALYSIS

Tesi di Dottorato di:
Elisabetta MANGIONI
Matr. Nr. 025776

Supervisor: prof. Lucia POMELLO
Supervisor: dott. Luca BERNARDINELLO
Tutor: prof. Giorgio DE MICHELIS

Desidero ringraziare Lucia per l'aiuto e l'incoraggiamento datomi durante gli anni universitari.
Sono grata a Luca per la vicinanza e le infinite consulenze sulla teoria e su LaTeX.
Sono riconoscente a Carlo per avermi fatto vivere un esperienza al JRC di Ispra e per essermi stato amico.
Un grazie anche al prof. De Michelis, che mi ha sempre spronata ad andare avanti e a dare il meglio.
Sono grata alla mia famiglia per aver accettato la mia scelta di fare un dottorato anche senza avere una borsa di studio.
Un grazie ed un abbraccio a tutti i miei amici per il loro contributo, specialmente i miei compagni di pappa Iade, Ema e tutti gli amici passati dal SITI 3.
Un saluto a Marco "Coso" Mascheroni che mi ha sopportata durante tutto il suo dottorato :-)
Infine, questa tesi non sarebbe stata scritta senza la carica che l'amore di Claudio mi ha dato. Quindi la dedico a te, che sei la mia vita.

Contents

Chapter 1

Introduction

The domain of this thesis is concurrency theory and formal models of distributed systems. In particular, we work in the fields of modularity and compositionality. We model the system structure by Petri Nets, in particular Elementary Net Systems, and system behaviour by Transition Systems or Occurrence Nets. A Petri Net is a particular graph, whose nodes are of two kinds: local states and local transformations. The first one represents a local part of the state of the system; a local transformation models the effects of the occurrence of an action that modifies the state of the system. Elementary Net Systems are a basic model of Petri Nets in which every local state is a boolean condition. Transition Systems model the global states and the global transformations of a system. Occurrence Nets are a particular kind of Petri Nets that represent the unfolding of an Elementary Net System. The representation of the behaviour of the system is expressed in the same formal notation as its structure. Here, each element records the occurrence of an element of the Elementary Net System. On Occurrence Nets, it is natural to define relations between elements, such as concurrency, conflict and causality.

We work with morphisms: a theoretical tool used to represent formal relations between models. The relation modelled can be a transformation, an abstraction, a refinement or other. Here, we focus on refinement/abstraction. One of the main challenges consists in developing languages and methods allowing to derive properties of the refined system from properties of the abstract system. Starting from some notions of morphisms already defined in the literature (Winskel morphisms [45] [33], N-morphisms [31] and $\widehat{N}$-morphisms [38] [6]), we study the possibility of varying or restricting these definitions so to preserve and reflect structural and behavioural properties of the related systems. Our main contribution in this part is the definition of α-morphisms, which preserve reachable markings. 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. Indeed, we characterize the local additional restrictions, with respect to general morphisms, that 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, like the reflection of reachable markings and that α-morphisms induce a bisimulation between the related Net systems. In order to define a structural morphism able to preserve and reflect behavioural properties, it is natural to search also a behavioural morphism that formalises this goal. As we already said, we consider both Occurrence Nets and Transition Systems to represent the behaviour of systems modelled by Elementary Net Systems. Clearly it is possible to see an Occurrence Net as an Elementary Net System, putting a token in each initial place of the Net. So, it is possible to use the morphisms already defined also on Occurrence Nets. We can use the concurrency, conflict and causality relations to obtain simpler morphisms on Occurrence Nets such that the same results obtained for Elementary Net Systems still hold. In dealing with morphisms on Elementary Transition Systems, we first recall G-morphisms [31], a behaviour preserving morphism, and $\widehat{G}$-morphisms [38], that differ from the former in interpreting the morphism as a refinement of the codomain system. Our contribution is the definition of a more restrictive version of $\widehat{G}$-morphisms, called Γ-morphisms, that take into account also the relations between states and transitions. Γ-morphisms do not allow to map pairs of dependent events into pair of independent events. Moreover, we want to relate morphisms between Elementary Net Systems with morphisms between their associated behavioural models and vice versa, in order to obtain more behavioural properties relating only structural models.

In the development of distributed systems a central role is played by formal tools supporting various aspects of modularity such as compositionality. There is a lot of interest in how to combine models because it makes the analysis of models simpler and more structured. The use of products in a suitable category of Nets as a way to model composition by synchronization has been studied by several authors. One of this works, similar to ours, proposed by Fabre [18], applies to Safe Nets and is built on the notion of pullback. A survey paper by Padberg [34] describes a way to compose Nets using morphisms and pushouts. There, the emphasis is on refinement rules that preserve specific behavioural properties, within the wider context of general transformation rules on Nets. Winskel [45] defines composition as a product in a category built on his morphisms. Following the approach proposed in [38] and in [3], the basic idea consists in composing two different refinements of a common abstract view, obtaining a new model which describes the system comprising the details of both operands, while complying to the same abstract view. The rules for identifying elements of the components are expressed by means of morphisms towards another model, called interface. The interface can be seen as an abstraction of the whole system, shared by the components or, alternatively, it can be interpreted as the specification of the communication protocol. In this case, each operand can be seen as made of the actual, local, component, and of an interface to the rest of the system. The composed system is made by local parts corresponding to each component and a global part corresponding to the interaction between the components. The composed system results to be related to both the components and the interface by means of morphisms, and the resulting diagram is commutative. Our contribution is the adaptation of this procedure to α-morphisms, so that the results obtained for these morphisms can be used in composition. Using α-morphisms we are able to obtain a composed system that is bisimilar to one of the components, if the other component respects the behavioural constraint local to each refinement of the interface.

How could a system designer use these results in practice? One way would consist in defining a set of Net transformations that he or she may use in refining a system model. Such transformations should be consistent with a suitable class of morphisms in the following sense: the result of applying a Net transformation should map onto the initial more abstract model. Our contribution consists on showing two examples of this kind of Net transformations.

The theoretical framework constituted by the composition guided by morphisms and interface is suitable to be used in the field of information flows and visibility. In this part of the research we assume to have a system divided in a hidden part (called the high part or the *defender*) and an observable part (called the low part or the *attacker*). The observer knows the structure of the whole system, but he is able to observe only the observable part. The observer can see the state of a part of the system, and observing this, it is able to derive that one event has occurred. We want to understand if the observer is able to infer some information on the local states of the hidden part. Starting with Moore [30], a lot of interest was in the study of the possibility to infer the state of a hidden part of a system. We aim at a structural characterization of the hidden internal states of a system that become visible after its interaction with a defined subsystem. We assume to have a high-level system that wants to keep secret its internal local states from a low-level system interacting with the high-level component through an interface. Basically, we explore the consequences of a proposal originally made by Busi and Gorrieri for defining non-interference properties. The new part of our proposal is that we use the local validity of conditions as observable properties and we focus on structural properties. Our contribution here is in changing the point of view of the attacker: he is not able to observe events, but only the modification of the local states. Defining a new kind of observability on states, we obtain results on the visibility of conditions of the defender that the attacker is able to infer using invariant properties that concern conditions of the defender and of the interface. We also define a classification of systems related to the idea of visibility.

The thesis will be structured as follows: in Chapter 2 we present the basic definitions we will use. In Chapter 3 we present the morphisms on the three kinds of models we consider, the categories defined and the relations between some of them. In Chapter 4 we present the work on the set of well formed Nets used for transformations and in Chapter 5 we present the work on composition guided by morphisms. Then, in Chapter 6 we present our work on observability and visibility. Finally, in Chapter 7 we expose conclusions and we explore the possible developments of this thesis.

Chapter 2

Basic definitions

2.1 Preliminary definitions

In this section we will recall the main definitions and notions that will be used in the rest of the thesis.

We then present Elementary Net Systems, a basic type of Petri Nets, and two different models of the behaviour of an Elementary Net System: Occurrence Nets, another kind of Petri Nets, and Elementary Transition Systems, a kind of Finite State Automata.

It is possible to use indifferently vectors and characteristic functions: if $\mathbf{v}$ is a vector $x \in \mathbf{v} \Leftrightarrow \mathbf{v}(x) \neq 0$.

Given a vector, we will use the symbol $\downharpoonright$ to denote the restriction of the object on a part of its components.

2.2 Categories, objects, and morphisms

In this section we recall some basic notions from *Category theory*.

The notion of function is one of the most fundamental in mathematics and science. Category theory [1] [44] is the algebra of functions; the main operation on functions is taken to be composition. A category is an abstract structure: a collection of objects together with a collection of arrows between them.

2.2.1 Categories

The following definitions are taken from [1] and [44] with some adaptations. We begin by giving the formal definition.

Definition 1. *A* category $\mathcal{C}$ *consists of a set of* objects *(called* $\mathbf{obj}\ (\mathcal{C})$*) and a set of* morphisms *or arrows. The objects are denoted*

$$A, B, C, ..., X, Y, ...$$

and the morphisms are denoted

$$f, g, h, ...\alpha, \beta, \gamma, ...$$

Further:

- *each morphism has a designated* domain *and* codomain *in* $\mathbf{obj}\ (\mathcal{C})$.

  When the domain of f *is* A *we write* $\mathbf{dom}\ (f) = A$.

  When the codomain of f *is* B *we write* $\mathbf{cod}\ (f) = B$.

  When $\mathbf{dom}\ (f) = A$ *and* $\mathbf{cod}\ (f) = B$ *we write* $f : A \to B$*;*

- *given any object* A *there is a designated* identity *morphism* $1_A : A \to A$*;*

- *given two morphisms* $f : A \to B$ *and* $g : B \to C$*, we define* $g \circ f : A \to C$ *as the* composite *morphism;*

- *the data above is required to satisfy the following:*

  Identity laws: *if* $f : A \to B$ *then* $1_B \circ f = f$ *and* $f \circ 1_A = f$*;*

  Associative law: *if* $f : A \to B, g : B \to C$ *and* $h : C \to D$ *then* $h \circ (g \circ f) = (h \circ g) \circ f : A \to D$*.*

In a category $\mathcal{C}$, given two objects A and B, the collection of all morphisms f such that $f : A \to B$ is denoted by $\mathcal{C}[A, B]$.

Let us define isomorphism between objects and categories.

Definition 2. *An arrow* $\alpha : A \to B$ *in a category for which there exists another arrow* $\alpha^{-1} : B \to A$ *such that*

$$\alpha \circ \alpha^{-1} = 1_B$$

$$\alpha^{-1} \circ \alpha = 1_A$$

is called an isomorphism.

If there is an isomorphism α from A to B we say that A and B are isomorphic objects, and we write $A \cong B$.

Definition 3. *Let* $\mathcal{A}$ *and* $\mathcal{B}$ *be categories.*

An isomorphism *from* $\mathcal{A}$ *to* $\mathcal{B}$ *is a bijection* Φ *from the objects and arrows of* $\mathcal{A}$ *to the objects and arrows of* $\mathcal{B}$*, respectively, such that:*

- Φ *preserves domains and codomains: if* $f : A_1 \to A_2$ *in* $\mathcal{A}$ *then* $\Phi(f) : \Phi(A_1) \to \Phi(A_2)$ *in* $\mathcal{B}$*,*

- Φ *preserves composition: if* $f : A_1 \to A_2$ *and* $g : A_2 \to A_3$ *in* $\mathcal{A}$ *then* $\Phi(g \circ f) = \Phi(g) \circ \Phi(f)$ *in* $\mathcal{B}$*,*

- Φ *preserves identities: if* 1_A *is an identity in* $\mathcal{A}$ *then* $\Phi(1_A) = 1_{\Phi(A)}$ *in* $\mathcal{B}$*.*

If there is an isomorphism Φ from $\mathcal{A}$ to $\mathcal{B}$ we say that $\mathcal{A}$ and $\mathcal{B}$ are isomorphic categories, and we write $\mathcal{A} \cong \mathcal{B}$. It is possible to think of an isomorphism as renaming the objects and arrows because isomorphic categories differ only in the names of the objects and arrows.

An important tool in the practice of Category Theory is the use of diagrams for representing equations. In a diagram a morphism $f : A \to B$ is drawn as an arrow labelled f from object A to object B. A diagram *commutes* if the composition of the morphism along any path between two fixed objects is equal.

Finally, let us define what is a subcategory.

Definition 4. *A category* $\mathcal{B}$ *is a* subcategory *of a category* $\mathcal{A}$*, if*

- $\mathbf{obj}\ (\mathcal{B}) \subseteq \mathbf{obj}\ (\mathcal{A})$*;*

- $\forall A, B \in \mathbf{obj}\ (\mathcal{B}), \mathcal{B}[A, B] \subseteq \mathcal{A}[A, B]$*;*

- *composition and identities in* $\mathcal{B}$ *coincide with those of* $\mathcal{A}$*.*

A subcategory is full *if* $\forall A, B \in \mathbf{obj}\ (\mathcal{B}), \mathcal{B}[A, B] = \mathcal{A}[A, B]$.

A full subcategory is fully determined by its collection of objects.

2.2.2 Functors

If a transformation F between two categories $\mathcal{A}$ and $\mathcal{B}$ must map the categorical structure of $\mathcal{A}$ to that of $\mathcal{B}$, it must take objects and morphisms of $\mathcal{A}$ to objects and morphisms of $\mathcal{B}$; moreover, it must preserve domain, codomain, identities and composition. Such a transformation $\mathsf{F} : \mathcal{A} \to \mathcal{A}$ is called a functor.

Definition 5. *If* $\mathcal{A}$ *and* $\mathcal{B}$ *are categories then a* functor *from* $\mathcal{A}$ *to* $\mathcal{B}$ *consists of two functions, one on objects and one on morphisms; the former is denoted*

$$\mathsf{F}_{obs} : \mathbf{obj}\ (\mathcal{A}) \to \mathbf{obj}\ (\mathcal{B})$$

and, for each pair of objects A_1*,* A_2 *of* $\mathcal{A}$*,*

$$\mathsf{F}_{A_1,A_2} : \mathcal{A}[A_1, A_2] \to \mathcal{B}[\mathsf{F}_{obs}(A_1), \mathsf{F}_{obs}(A_2)]$$

satisfying

$$\mathsf{F}_{A,A}(1_A) = 1_{\mathsf{F}_{obs}(A)}$$

$$\mathsf{F}_{A_1,A_3}(\beta \circ \alpha) = \mathsf{F}_{A_2,A_3}(\beta) \circ \mathsf{F}_{A_1,A_2}(\alpha) \textit{ if } A_1 \xrightarrow{\alpha} A_2 \xrightarrow{\beta} A_3$$

Note that we usually denote all the functions $\mathsf{F}_{obs}, \mathsf{F}_{A_1,A_2}$ by the symbol F.

2.2.3 Pullback and pushout

We now introduce the notion of pullback.

Definition 6. *Given two arrows $f : B \to A$ and $g : C \to A$ with common codomain A, the* pullback *of (f, g) is an object P and a couple of arrows $p_B : P \to B$, $p_C : P \to C$, such that:*

- $f \circ p_B = g \circ p_C : P \to A$*;*
- *for every other triple $(Q, q_B : Q \to B, q_C : Q \to C)$ such that $f \circ q_B = g \circ q_C$, there exists a unique arrow $u : Q \to P$ such that $p_B \circ u = q_B$, and $p_C \circ u = q_C$.*

$$\begin{tikzcd}
Q \arrow[dr, "u"] \arrow[drr, bend left, "q_C"] \arrow[ddr, bend right, "q_B"'] & & \\
& P \arrow[r, "p_C"'] \arrow[d, "p_B"] & C \arrow[d, "g"] \\
& B \arrow[r, "f"'] & A
\end{tikzcd}$$

The notion of pushout is dual to that of pullback.

Definition 7. *Given two arrows $f : A \to B$ and $g : A \to C$ with common domain A, the* pushout *of (f, g) is an object P and a couple of arrows $i_B : B \to P$, $i_C : C \to P$, such that:*

- $i_B \circ f = i_C \circ g : A \to P$*;*
- *for every other triple $(Q, j_B : B \to Q, j_C : C \to Q)$ such that $j_B \circ f = j_C \circ g$, there exists a unique arrow $u : P \to Q$ such that $u \circ i_B = j_B$, and $u \circ i_C = j_C$.*

$$\begin{tikzcd}
A \arrow[r, "g"] \arrow[d, "f"'] & C \arrow[d, "i_C"'] \arrow[ddr, bend left, "j_C"] & \\
B \arrow[r, "i_B"] \arrow[drr, bend right, "j_B"'] & P \arrow[dr, "u"] & \\
& & Q
\end{tikzcd}$$

2.3 Elementary Net Systems

Petri Nets were introduced by Carl Adam Petri [36] as a basic model of general systems. In this section, we recall the basic definitions of Net theory. For a detailed introduction to Net theory, see [40].

In Net theory, models of distributed systems are based on objects called Nets which specify local states, local transitions and the relations among them.

Definition 8. *A* Net *is a triple* $N = (B, E, F)$*, where:*

- B *is a finite set of* local states*;*
- E *is a finite set of* local transformations*;*
- $B \cap E = \emptyset$*;*
- $F \subseteq (B \times E) \cup (E \times B)$ *is the* flow relation.

The set of nodes of a Net will be denoted by $X = B \cup E$; we allow the empty Net and Nets with isolated nodes. In the following, when we add an index to a Net, also its components are identified by this index: $N_i = (B_i, E_i, F_i)$.

A Net can be represented as a bipartite graph. We adopt the usual graphical notation: local states are represented by circles, local transformations by boxes and the flow relation by arcs.

A local state $b \in B$ is a *precondition* of $e \in E$ if $(b, e) \in F$; it is a *postcondition* of e if $(e, b) \in F$. The *preset* of an node $x \in X$ is defined by ${}^\bullet x = \{y \in X \mid (y, x) \in F\}$; the *postset* of x is given by $x^\bullet = \{y \in X \mid (x, y) \in F\}$; the *neighbourhood* of x is given by ${}^\bullet x^\bullet = {}^\bullet x \cup x^\bullet$. These notations are extended to sets of nodes in the usual way.

A local state x is the *complement* of a local state y if ${}^\bullet x = y^\bullet$ and $x^\bullet = {}^\bullet y$. The complement of x, if it exists, will be denoted by x'.

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

A Net $N = (B, E, F)$ is *B-simple* iff for each $x, y \in B$, $({}^\bullet x = {}^\bullet y \wedge x^\bullet = y^\bullet) \Rightarrow x = y$; N is *E-simple* iff for each $x, y \in E$, $({}^\bullet x = {}^\bullet y \wedge x^\bullet = y^\bullet) \Rightarrow x = y$; finally, N is *simple* if it is both $B-$ and $E-$simple.

A Net is T*-restricted* when $\forall e \in E, {}^\bullet e \neq \emptyset \neq e^\bullet$.

Let us define a subnet of a Net generated by a subset of nodes.

Definition 9. *A Net* $N' = (B', E', F')$ *is a* subnet *of a Net* $N = (B, E, F)$ *if* $B' \subseteq B$*,* $E' \subseteq E$*, and* $F' = F \cap ((B' \times E') \cup (E' \times B'))$*.*

Given a subset of nodes $H \subseteq B$*, we say that* N_H *is the* subnet *of* N generated *by* H *if* $N_H = (H, {}^\bullet H^\bullet, F \cap ((H \times {}^\bullet H^\bullet) \cup ({}^\bullet H^\bullet \times H))$*.*

Given a subset of nodes $K \subseteq E$, we say that N_K is the subnet of N generated *by K if $N_K = ({}^\bullet K^\bullet, K, F \cap (({}^\bullet K^\bullet \times K) \cup (K \times {}^\bullet K^\bullet))$.*

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

The structure of a Net can be represented by a matrix M called the incidence matrix.

Definition 10. *The* incidence matrix *of a Net $N = (B, E, F)$ is the matrix M with $|B|$ rows (one for each local state) and $|E|$ columns (one for each local transformation).*

Its (k, j) node is:

$$M(k,j) = \begin{cases} -1 & \textit{if } (b_k, e_j) \in F \\ 0 & \textit{if } (b_k, e_j) \notin F \wedge (e_j, b_k) \notin F \\ 1 & \textit{if } (e_j, b_k) \in F \end{cases}$$

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

Let us now define Elementary Net Systems [41]. Whereas a Net describes the structure of a system, an Elementary Net System adds to this the specification of an initial global state. A global state is a set of local states, and is a snapshot of the system at a given time. Moreover, a local transformation is called *event* and a local state is called *condition*. The events are actions that change some local states of the system. In Elementary Net Systems local states are interpreted as boolean conditions.

Definition 11. *An* Elementary Net System *is a quadruple $N = (B, E, F, m_0)$, where (B, E, F) is a simple Net such that:*

- *self-loops are not allowed: $\forall e \in E, \forall p, q \in B : (p, e), (e, q) \in F \Rightarrow p \neq q$;*
- *isolated nodes are not permitted: $\mathbf{dom}\ (F) \cup \mathbf{cod}\ (F) = X$;*
- *the* initial marking *is $m_0 \subseteq B$.*

In general, a marking (o case) is a subset of conditions that are true at a given time. If $m \subseteq B$ is a marking and $b \in m$, we will say that there is a token in b.

The behaviour of Elementary Net 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.

Definition 12. *Let $N = (B, E, F, m_0)$ be an Elementary Net System, let $e \in E$ and $m \subseteq B$.*

1. *e is* enabled *(or e has* concession*) at m, denoted $m\,[e\rangle$, if ${}^{\bullet}e \subseteq m$ and $e^{\bullet} \cap m = \varnothing$.*

2. *If e is enabled at m, e can occur. Its occurrence brings the Net System from state m to a new state m', denoted by $m\,[e\rangle\,m'$, iff $m' = (m \setminus {}^{\bullet}e) \cup e^{\bullet}$; e is also called a sequential step from m to m'.*

3. *Let ϵ denote the empty word in E^*. The firing rule is extended to sequences of events by*
$$m\,[\epsilon\rangle\,m$$
and
$$\forall e \in E, \forall w \in E^*, m\,[ew\rangle\,m' \Leftrightarrow m\,[e\rangle\,m''[w\rangle m'$$
ew and w are then called firing sequences. *The* set of firing sequences *of N is the set $\mathsf{FS}(N) = \{w \in E^* \mid m_0\,[w\rangle\}$.*

4. *$m \subseteq B$ is a* reachable marking *of N if there exists a $w \in \mathsf{FS}(N)$ with $m_0\,[w\rangle\,m$. The* set of all reachable markings*, or* state space*, of N is denoted by $[m_0\rangle$.*

The sequential behaviour of Elementary Net Systems can be described by marking sequences and transition systems.

Definition 13. *A* marking sequence *ms of N is a sequence*

$$ms = m_1 \ldots m_n : \exists e_1, \ldots e_{n-1} \in E, m_1\,[e_1\rangle\,m_2 \ldots m_{n-1}\,[e_{n-1}\rangle\,m_n$$

We will call MS the set of all marking sequences starting from the initial marking.

Definition 14. *The* marking graph *(or* reachability graph*) of an Elementary Net System N is the triple $MG(N) = ([m_0\rangle, E, T)$, where $T = \{(m, e, m') \mid m, m' \in [m_0\rangle \wedge e \in E \wedge m\,[e\rangle\,m'$.*

Different Elementary Net Systems can have isomorphic marking graphs. In this family of systems, there is a model that is maximal in the number of conditions. This Elementary Net System is called *saturated.*

A set of events $U \subseteq E$ may occur concurrently, i.e. is a *step*, at a marking m, denoted $m\,[U\rangle\,m'$, if they are pairwise independent, i.e., $\forall e_1, e_2 \in U : e_1 \neq e_2$ implies: $({}^{\bullet}e_1 \cup e_1{}^{\bullet}) \cap ({}^{\bullet}e_2 \cup e_2{}^{\bullet}) = \varnothing$, and each one of them is enabled at m. The new marking m' is obtained from m by the occurrence of each event in U.

An Elementary Net System is *1-live* if every event can fire in, at least, one reachable marking: $\forall e \in E$, $\exists m \in [m_0\rangle : m[e\rangle$. 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.

Definition 15. *An Elementary Net System $N = (B, E, F, m_0)$ is said to be* contact-free *iff* $\forall m \in [m_0\rangle, \forall e \in E, {}^\bullet e \subseteq m \Rightarrow e^\bullet \cap m = \varnothing$.

A subnet of an Elementary Net 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 Elementary Net System is *covered* by sequential components if every condition of the Net belongs to at least one sequential component. In this case we say that the system is *State Machine Decomposable (SMD)*.

Intuitively, a State Machine decomposable Net System models a system composed of interacting sequential parts.

If an Elementary Net System is covered by sequential components then it is contact-free.

Some properties of an Elementary Net System can be studied through the incidence matrix and its invariants. An S-invariant [42] associates positive weights to conditions so that the weighted sum of tokens is the same in all reachable markings.

Definition 16. *Let N be an Elementary Net System and let M be its incidence matrix.*

A vector $\mathbf{I} : B \to \mathbb{N}$ *is an S-*invariant *iff it is a solution of:* $\mathbf{I}^T \circ M = \mathbf{0}$.

T-invariants allow to identify firing sequences that reproduce a marking.

Definition 17. *Let N be an Elementary Net System and let M be its incidence matrix.*

A vector $\mathbf{J} : T \to \mathbb{N}$ *is a T-*invariant *iff it is a solution of:* $M \circ \mathbf{J} = \mathbf{0}$.

An S-invariant is *basic* iff its coefficients are in $\{0, 1\}$. An S-invariant is *monomarked* iff it is basic and exactly one condition corresponding to a 1 in the invariant belongs to the initial marking m_0.

2.3.1 Bisimulations for Elementary Net Systems

We consider now an equivalence notion [39], [46] and [35] that is based on the observability of sequences of events. Initially, bisimulation has been defined in the field of Transition Systems. The idea is that two systems are bisimilar if they allow the same set of actions in related states. If we take into account the possibility that some actions of the systems are invisible to an observer, the corresponding notion is called weak bisimilarity, which will be used in the following.

Since the behaviour of Elementary Net Systems is modeled by Transition Systems, bisimilarity has been defined also for these models.

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. In order to capture the behaviour that can be obtained through system observation, it is necessary to define a new transition rule which takes into account only the images of observable events.

Definition 18. *Let* $N = (B, E, F, m_0)$ *be an Elementary Net 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 in both* 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 *Elementary Net System.*

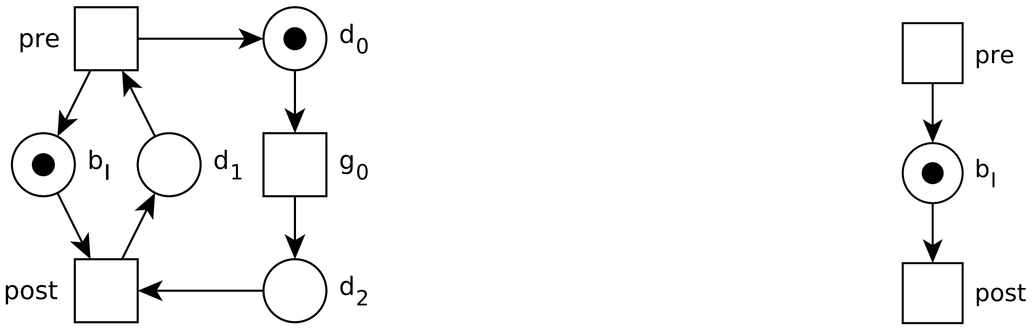
Let $m, m' \in [m_0\rangle$ *and* $a \in L \cup \{\epsilon\}$ *then:*

- 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* $m\,[w\rangle\, m'$*.*

Bisimulation relations have been introduced as equivalence notions with respect to event observation [29]. We define weak bisimulation as a relation between reachable markings of Labelled Elementary Net Systems. The initial markings must be related. Moreover, if one system is in a marking m and evolves to another marking m' with a sequence a of observable actions, it has to be possible for the other system, that is in a marking c bisimilar to m ($c \approx^{BIS} m$), to evolve by means of a to a new marking c' so that $c' \approx^{BIS} m'$ and vice versa.

Definition 19. *Let* $N_i = (B_i, E_i, F_i, m_0^i)$ *be an Elementary Net 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:*

- $(m_0^1, m_0^2) \in r$*;*



(a) N_1 (b) N_2

Figure 2.1: Two Nets

- $\forall (m_1, m_2) \in r, \forall a \in L \cup \{\epsilon\}$ *it holds*

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

and (vice versa)

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

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.*

As an example, consider the systems N_1 and N_2 of Fig. 2.1. The observable actions are the ones on E_2. As labelling function for N_1 consider a l_1 that maps each event on the correspondent one in E_2 but for g_0 that is mapped on τ. As labelling function for N_2 take the identity function. Using the mapping $(\{b_I, d_0\}, \{b_I\}), (\{b_I, d_2\}, \{b_I\}), (\{d_1\}, \varnothing)$, these two systems are bisimilar. To better understand the concept of the new transition rule, note that we can write $\{b_I, d_0\} \langle post \rangle \{d_1\}$ because we have $\{g_0, post\} \in E_2^*$ such that $l_2(\{g_0, post\}) = post$ and $\{b_I, d_0\} [\{g_0, post\}\rangle \{d_1\}$.

2.3.2 Occurrence Nets

Given a Net N, if F^* is a partial order (the Net is acyclic), we can define other interesting relations [2] [7] [16] [22] [37].

Causality coincide with F^* and can be characterised as the least transitive relation $<_N$ over X such that if $x \in {}^\bullet y$ then $x <_N y$ and if $x \in y^\bullet$ then $y <_N x$. We denote by $\leq_N$ the reflexive closure of $<_N$. Informally, $x <_N y$ means that the Net contains a path with at least one arc leading from x to y. For any $x \in X$ we are now able to define its *past*, $\lfloor x \rfloor = \{y \in X : y \leq_N x\}$, and its *future*, $\lceil x \rceil = \{y \in X : x \leq_N y\}$. For $x, y \in X$, $x \leq y$, $[x, y]$ denotes the closed interval between x and y: $[x, y] = \{z \in X \,|\, x \leq z \leq y\}$; $]x, y[$ denotes the open interval between x and y: $]x, y[= \{z \in X \,|\, x < z < y\}$. We will also use the relation **li** defined as $\leq \cup \geq$, where $\geq$ is the inverse of $\leq$.

Let us proceed with the idea of conflict: x and y are in conflict if the Net contains two paths leading to x and y which start at the same place b and immediately diverge (although later on they can converge again).

Definition 20. *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 $e_x, e_y \in E$, $e_x \neq e_y$, such that $e_x \leq x$, $e_y \leq y$, and ${}^\bullet e_x \cap {}^\bullet e_y \neq \emptyset$.*

Two elements, x and y, are *concurrent*, denoted by x **co** y, indicating that x and y may occur at the same time in some reachable marking, if they neither causally depend on nor conflict with each other, defined as: x **co** y iff $\neg(x \#_N y)$ and $\neg(x \leq_N y)$ and $\neg(y \leq_N x)$.

We often drop the subscript N for the defined relations.

A subset of nodes $X \subseteq B$ pairwise concurrent will be called a *co-set*: $\forall x, y \in X, x$ **co** y. A co-set formed by elements of B will be called a *B-co-set*. A maximal co-set with respect to set inclusion is called a *cut*.

Occurrence Nets are basically acyclic Nets where each condition is generated by at most one event.

Definition 21. *An Occurrence Net is a Net N satisfying:*

1. *every condition is generated by at most one event: $\forall e_1, e_2 \in E$, if $e_1{}^\bullet \cap e_2{}^\bullet \neq \emptyset$ then $e_1 = e_2$;*

2. *the Net is acyclic, or, equivalently, the causal relation $\leq$ is a partial order;*

3. *each nodes is finitely preceded: $\lfloor x \rfloor$ is finite for any $x \in X$. This implies that $\forall x, y \in X : |[x, y]| < \infty$.*

4. *no node is in conflict with itself: $\#_N$ is irreflexive,*

5. *the minimal elements with respect to $\leq_N$ form a B-co-set. This set is the implicitly associated initial marking.*

It is easy to see that any two nodes of an Occurrence Net are either in causal, conflict, or concurrency relation.

A run represents a possible execution, where conflicts have been solved.

Definition 22. *A* run *R of an Occurrence Net N is a set of events satisfying the two following properties:*

- *R is causally left-closed: $\forall e_1, e_2 \in E : e_1 \in R \wedge e_2 \leq e_1 \Rightarrow e_2 \in R$,*
- *R is conflict-free: $\forall e_1, e_2 \in R : \neg(e_1 \# e_2)$.*

We impose that the Nets we consider are *T-restricted*, as defined in the previous section.

For any subset A of elements of an Occurrence Net $N = (B, E, F)$, by $\min(A)$ we denote the minimal elements of A with respect to the causal relation $\leq$, i.e. the elements that have an empty preset, as $\min(A) = \{x \in A : {}^\bullet x \cap A = \varnothing\}$, and by $\max(A)$ the maximal elements of A, i.e. the elements that have an empty postset, as $\max(A) = \{x \in A : x^\bullet \cap A = \varnothing\}$. When we consider the set X of nodes of a Net, $\min(X)$ and $\max(X)$ consist of conditions, since we consider T-restricted Nets.

Let us define a subnet of an Occurrence Net generated by a subset of elements.

Definition 23. *Let $N = (B, E, F)$ be an Occurrence Net and let $A \subseteq X$.*

We define $N(A)$ as the Net generated by the nodes of A plus the neighbourhood of the events of A. Let $B_A = (A \cap B) \cup {}^\bullet(A \cap E)^\bullet$ and $E_A = A \cap E$:

$$N(A) = (B_A, E_A, F \cap (A \times A))$$

It is easy to see that a subnet of an Occurrence Net is an Occurrence Net.

We are now ready to define the *unfolding* of an Elementary Net System. Let us start with an informal definition. Consider an Elementary Net System N with its initial marking m_0. It can be “unfolded” into labelled Occurrence Nets in an operational way. Take the initial marking of N. Then, add all the events enabled and their postconditions. Continue in this way, creating a new copy of a node each time you need to add it to the Occurrence Net. It is possible to stop at any time, so creating different Occurrence Nets. The nodes of the Occurrence Net are labelled with the conditions and events of the Net N. The labelled Occurrence Nets obtained through unfolding of Nets are called processes. The unfolding process can be stopped at different times yielding different processes, however there is a unique, usually infinite, process obtained by unfolding “as much as possible”. This process is called the unfolding of the Net System. Clearly, this process can be infinite, generating an Occurrence Net that is infinite.

Hence, a process of N is an Occurrence Net whose elements can be mapped to the elements of N such that the requirements in the following definition are satisfied.

Definition 24. *Let $N = (B, E, F, m_0)$ be an Elementary Net System, and $N_\Sigma = (B_\Sigma, E_\Sigma, F_\Sigma)$ be an Occurrence Net (potentially infinite). Let $\pi : X_\Sigma \to X$ be a map.*

The pair (N_Σ, π) is a process *of N if:*

- *π preserves the nature of nodes: $\pi(B_\Sigma) \subseteq B$, $\pi(E_\Sigma) \subseteq E$;*
- *N_Σ "starts" at the minimal elements of N:*
  π restricted to $\min(X_\Sigma)$ is a bijection on m_0;
- *for each $e \in E_\Sigma$, π restricted to ${}^\bullet e$ is injective and π restricted to $e^\bullet$ is injective;*
- *π preserves the environments of transitions:*
  for each $e \in E_\Sigma$, $\pi({}^\bullet e) = {}^\bullet(\pi(e))$ and $\pi(e^\bullet) = (\pi(e))^\bullet$.

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

2.4 Elementary Transition Systems

The theory of Elementary Transition Systems and regions has been developed in category context in [31]. Transition Systems consist of states and transitions. Every state represents a global system state and every transition links global states. Usually Transition Systems are based on actions which may be viewed as labelled events. We will consider only finite models.

Definition 25. *A* Transition System *is a quadruple $TS = (S, E, T, s_0)$, where*

- *S is a non-empty and finite set of* states,
- *E is a finite set of* events*, actions or labels,*
- *$T \subseteq S \times E \times S$ is the* transition relation*: a set of labelled edges or transitions,*
- *$s_0 \in S$ is the* initial state.

Let $TS = (S, E, T, s_0)$ be a Transition System. When TS is clear from the context we will often write $s \xrightarrow{e} s'$ instead of $(s, e, s') \in T$. An event e is enabled at the state s (denoted $s \xrightarrow{e}$) if there exists a state s' such that $s \xrightarrow{e} s'$.

From now on Transition Systems will be assumed to satisfy the following axioms:

(A1) loopfree: $s \xrightarrow{e} s' \Rightarrow s \neq s'$,

(A2) no multiple arcs: $s \xrightarrow{e_1} s' \wedge s \xrightarrow{e_2} s' \Rightarrow e_1 = e_2$,

(A3) reduced: $\forall e \in E, \exists s, s' \in S : s \xrightarrow{e} s'$,

(A4) reachable: $\forall s \in S \setminus s_0, \exists e_0, e_1, \dots e_{n-1} \in E \wedge \exists p_0, p_1, \dots p_n \in S : p_0 = s_0, p_n = s \wedge p_i \xrightarrow{e_i} p_{i+1}, 0 \leqslant i < n$.

A region is a subset of states whose border is crossed in a uniform way by transitions labelled with the same label.

Definition 26. *Let $TS = (S, E, T, s_0)$ be a Transition System.*
Then $r \subseteq S$ is a region *of TS iff the following two conditions are satisfied:*

- $(s \xrightarrow{e} s' \in T \ \wedge \ s \in r \ \wedge \ s' \notin r) \Rightarrow (\forall s_1 \xrightarrow{e} s'_1 \in T : s_1 \in r \ \wedge \ s'_1 \notin r)$
- $(s \xrightarrow{e} s' \in T \ \wedge \ s \notin r \ \wedge \ s' \in r) \Rightarrow (\forall s_1 \xrightarrow{e} s'_1 \in T : s_1 \notin r \ \wedge \ s'_1 \in r)$

S and $\varnothing$ are particular regions called trivial regions.

Let R_{TS} denote the set of (non trivial) regions of TS, and for each $s \in S$ let $R_s = \{r \,|\, s \in r \in R_{TS}\}$ denote the set of non trivial regions containing s.

It is possible to define pre and post-regions of an event.

Definition 27. *Let $TS = (S, E, T, s_0)$ be a Transition System.*
Then the pre *and* post-regions *of an event are defined in the following sense:*

$$\forall e \in E, {}^{\circ}e = \{r \in R_{TS} \,|\, \exists s \xrightarrow{e} s' \in T, s \in r \wedge s' \notin r\}$$

$$\forall e \in E, e^{\circ} = \{r \in R_{TS} \,|\, \exists s \xrightarrow{e} s' \in T, s \notin r \wedge s' \in r\}$$

Proposition 1. *Let $TS = (S, E, T, s_0)$ be a Transition System.*

- *$r \subseteq S$ is a region iff $\overline{r} = S - r$ is a region;*
- *$\forall e \in E, e^{\circ} = \{\overline{r} \,|\, r \in {}^{\circ}e\}$;*
- *$s \xrightarrow{e} s', {}^{\circ}e = R_s - R_{s'}$ and $e^{\circ} = R_{s'} - R_s$.*

  Consequently ${}^{\circ}e \subseteq R_s$ and $e^{\circ} \cap R_s = \varnothing$ and $R_{s'} = (R_s - {}^{\circ}e) \cup e^{\circ}$.

Let us define a particular subtype of Transition Systems, that respects two constraints on regions.

Definition 28. *The Transition System $TS = (S, E, T, s_0)$ is* Elementary *if it satisfies also these two regional axioms:*

(A5) *state separation:* $\forall s, s' \in S, R_s = R_{s'} \Rightarrow s = s'$;

(A6) *forward closure:* $\forall s \in S, \forall e \in E, {}^{\circ}e \subseteq R_s \Rightarrow s \xrightarrow{e}$.

The behaviour of Elementary Net Systems can be described by marking graphs, which can be characterized as a subclass of Transition Systems. The marking graph of an Elementary Net System is an Elementary Transition System (see [31]).

Chapter 3

Morphisms

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 or composed system from properties of the abstract system or the components.

In this chapter we present different types of morphisms for refinement/abstraction. These can also be used to relate two subsystems to a common interface in order to properly compose the subsystems, as we will show in the next chapter.

Here, we present some already defined morphism and we define some new morphisms for Elementary Net Systems (structural models), Occurrence Nets and Elementary Transition Systems (behavioural models). At the end of the chapter we present the relations between some of the categories introduced.

3.1 Elementary Net Systems

Using morphisms to formalize relations between a refined Net system and a more abstract one is widely used in the literature. Most approaches, in Petri Net theory, are based on transition refinement and, less frequently, on place refinement; for a survey, see [10]. Another survey paper, [34], 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 [15]. An attempt to define abstractions based on morphisms which preserve both structural and behavioural properties is described in [24] for Coloured Petri Nets. These morphisms are consistent with an operation of composition of nets.

In [32] a refinement operation is proposed on Transition Systems, however is strictly related to refinement of local states in Nets, through the notion of region.

In this section, we start introducing some notions of morphisms already defined in literature: Winskel morphisms [45] [33], N-morphisms [31] and $\widehat{N}$-morphisms [38] [6]. We study the possibility of varying or restricting these definitions so to preserve and reflect properties of the related systems. We start working on $\widehat{N}$-morphisms forbidding to relate dependent elements to concurrent ones. Next, we work on morphisms similar to the one of Winskel, introducing the idea of subnet mapped on a single node. On this line, in Section 3.1.7, we present one main results in this area: the definition of α-morphisms, and we show that reachable markings are preserved. Moreover, we characterize the local conditions under which reachable markings are reflected, and such that α-morphisms induce a bisimulation between the related Net systems.

3.1.1 Winskel morphisms

Winskel morphisms are a very basic kind of morphisms and are defined in [45] for general Net and in [33] for basic types of Net. These are behaviour preserving morphisms, to be thought of as kinds of simulations.

Vogler [43] and Bednarczyk [27] defined the same variation of these morphisms in two different period. However, their morphisms are more general than the Winskel ones, hence their are not able to have other properties preserved and reflected.

Definition 29. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be a contact-free EN System, for $i = 1, 2$. A Winskel morphism is a pair $(\beta, \eta) : N_1 \to N_2$, where:*

- *$\beta \subseteq B_1 \times B_2$ and $\beta^{-1} : B_2 \to^* B_1$ is a partial function;*
- *$\eta : E_1 \to^* E_2$ is a partial function;*
- *$\beta(m_0^1) = m_0^2$;*
- *if $\eta(e_1)$ is undefined, then $\beta({}^\bullet e_1) = \varnothing = \beta(e_1{}^\bullet)$;*
- *if $\eta(e_1) = e_2$, then $\beta({}^\bullet e_1) = {}^\bullet e_2$ and $\beta(e_1{}^\bullet) = e_2{}^\bullet$.*

Note that this kind of morphisms does not permit the classical folding, as is illustrated in Fig. 3.1.

Winskel morphisms preserve reachable markings, as stated in the next proposition [33].

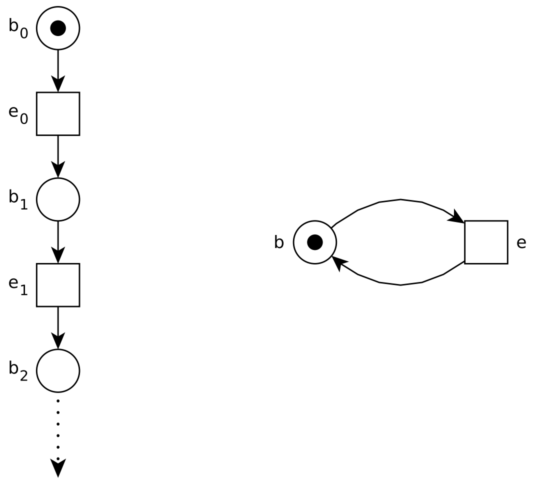


Figure 3.1: Two Nets without a Winskel morphism

Proposition 2. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be an EN System, for $i = 1, 2$. Suppose $(\beta, \eta) : N_1 \to N_2$ is a Winskel morphism.*

- *If $m_1 [e_1\rangle m_1'$ in N_1 and $\eta(e_1) \in E_2$ then $\beta(m_1) [\eta(e_1)\rangle \beta(m_1')$ in N_2.*
- *If $m_1 [e_1\rangle m_1'$ in N_1 and $\eta(e) \in B_2$ then $\beta(m_1) = \beta(m_1')$ in N_2.*
- *If ${}^\bullet e_1{}^\bullet \cap {}^\bullet e_1'{}^\bullet = \varnothing$ in N_1 then ${}^\bullet(\eta(e_1))^\bullet \cap {}^\bullet(\eta(e_1'))^\bullet = \varnothing$ in N_2.*

The Wisnkel morphisms are closed by composition, the identity function is a Winskel morphism, and the composition is associative. Hence, the family of Elementary Net Systems together with Winkel morphisms forms a category denoted $\mathcal{N}$ [33].

3.1.2 N-morphisms

Nielsen, Rozenberg and Thiagarajan [31] introduced a particular kind of morphisms, N-morphisms, that can be seen like a behaviour preserving transformations hence corresponding to a form of partial simulation. N-morphisms are a modified form of Winskel morphisms presented in the previous section. The main difference between them is, firstly, that Winskel morphisms demand the initial cases to be correspondent while Nielsen, Rozenberg and Thiagarajan weakened this assumption since they do not wish to permit isolated elements in the Nets. The other difference is that they do not require the Net to be contact-free whereas Winskel morphisms do.

Definition 30. *Let $N_i = (B_i, E_i, F_i, m_0)$ be an Elementary Net System for $i = 1, 2$. An N-morphism from N_1 to N_2 is a pair (β, η), where:*

1. *$\beta \subseteq B_1 \times B_2$ and $\beta^{-1} : B_2 \to^* B_1$ is a partial function;*

2. *$\eta : E_1 \to^* E_2$ is a partial function;*

3. *$\forall (b_1, b_2) \in \beta : b_1 \in m_0^1 \Leftrightarrow b_2 \in m_0^2$;*

4. *if $\eta(e_1)$ is undefined, then $\beta({}^\bullet e_1) = \varnothing = \beta(e_1{}^\bullet)$;*

5. *if $\eta(e_1) = e_2$, then $\beta({}^\bullet e_1) = {}^\bullet e_2$ and $\beta(e_1{}^\bullet) = e_2{}^\bullet$.*

N-morphisms are behaviour preserving, as stated in the next proposition [31].

Proposition 3. *Let $N_i = (B_i, E_i, F_i, m_0)$ be an Elementary Net System for $i = 1, 2$ and let $(\beta, \eta) : N_1 \to N_2$ be an N-morphism between them. Let $f_\beta : [m_0^1\rangle \to 2^{B_2}$, be given by $\forall m \in [m_0^1\rangle, f_\beta(m) = \beta(m) \cup (m_0^2 - \beta(m_0^1))$ then*

- *$\forall m \in [m_0^1\rangle, f_\beta(m) \in [m_0^2\rangle$,*
- *suppose $m\,[e\rangle\, m'$ then $f_\beta(m) = f_\beta(m')$ in case $\eta(e)$ is undefined, otherwise, $f_\beta(m)\,[\eta(e)\rangle\, f_\beta(m')$.*

In some sense, the morphisms are guided by the mapping on the events, as is explained in the next proposition [31].

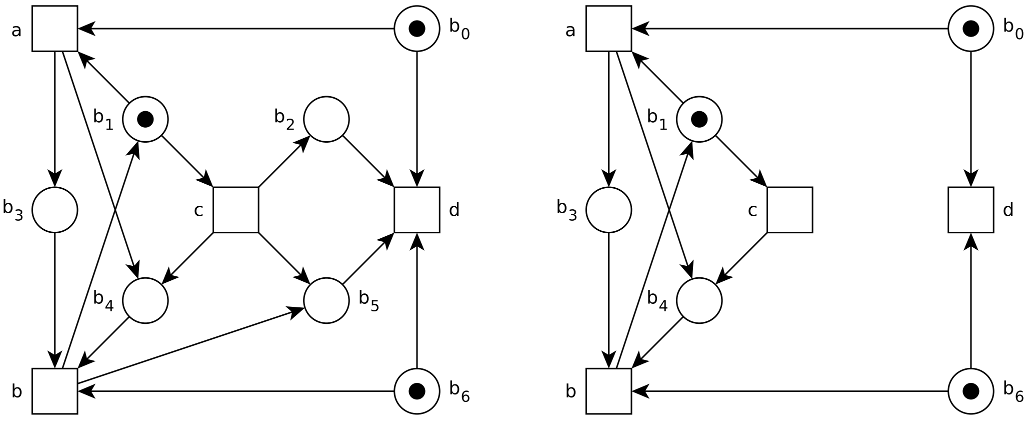
Proposition 4. *Let (β_1, η_1) and (β_2, η_2) be a pair of N-morphisms from N_1 to N_2 where $N_i = (B_i, E_i, F_i, m_0^i)$ are Elementary Net Systems for $i = 1, 2$. If $\eta_1 = \eta_2$ then $\beta_1 = \beta_2$.*

The N-morphisms are closed by composition; the identity function $1_N = (id_B, id_E)$ is an N-morphisms where $id_B : B \to B$ and $id_E : E \to E$ are the (total) identity functions; the composition is associative. Hence, the family of Elementary Net Systems together with N-morphisms forms a category denoted $\mathcal{ENS}$ [33].

3.1.3 $\widehat{N}$-morphisms

Bernardinello, Pomello et al. studied a more restricted version of N-morphisms: $\widehat{N}$-morphism. These morphisms are introduced in [38] and studied in [6].

The basic idea is that N_1 can be seen like a refinement of N_2, so it has to maintain all the conditions and the events of N_2 but it can add other behaviour adding conditions and events. It is very important to take in mind that also this kind of morphisms allow to relax some constraints. Instead of N-morphisms, $\widehat{N}$-morphisms require η to be surjective and β^{-1} to be a total and injective function, that is equivalent to require β to be a partial, injective and surjective function. The



(a) N_1

(b) N_2

Figure 3.2: An example of $\widehat{N}$-morphism

totality of β^{-1} assures that every condition of N_2 must have a counterimage in N_1; the surjectivity of η assures that every event of N_2 can be splitted into more than one event in N_1 but have to be part of the refined Petri Net. $\widehat{N}$-morphisms set constraints on the pre and post conditions of an event but nothing is said about the relation of the conditions which are not in the domain of β.

Definition 31. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be Elementary Net Systems for $i = 1, 2$.*

An $\widehat{N}$-morphism from N_1 to N_2 is an N-morphism (β, η) with the following restrictions:

1. *$\beta^{-1} : B_2 \to B_1$ is a total and injective function. Note that this is equivalent to say that $\beta : B_1 \to^* B_2$ is a partial, injective and surjective function;*

2. *η is surjective.*

$\widehat{N}$-morphisms allow refining local states and adding constraints between events but they do not allow to delete events and conditions of N_2. Fig. 3.2 shows an example of $\widehat{N}$-morphism (elements with the same names are related by the maps β and η). As we can see N_1 has more constraints than N_2.

The $\widehat{N}$-morphisms are closed by composition; the identity function $1_N = (id_B, id_E)$ is an $\widehat{N}$-morphisms where $id_B : B \to B$ and $id_E : E \to E$ are the (total) identity functions; the composition is associative. Hence, the family of Elementary Net Systems together with $\widehat{N}$-morphisms forms a category denoted $\widehat{\mathcal{ENS}}$. Note that $\widehat{\mathcal{ENS}}$ is a subcategory of $\mathcal{ENS}$.

As we have seen before, $\widehat{N}$-morphism can be seen like a refinement/abstraction [38].

Proposition 5. *Let N_1 and N_2 be Elementary Net Systems and (β, η) be an $\widehat{N}$-morphism from N_1 to N_2. Let N_1' be the subnet of N_1 generated by the set of conditions $B_1' = \beta_i^{-1}(B_2)$, and let $simp(N_1')$ be obtained from N_1 by event simplification. Then $simp(N_1')$ is isomorphic to N_2.*

$\widehat{N}$-morphisms are a special kind of N-morphisms so also them are "behaviour-preserving" in a slightly different sense.

Proposition 6. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be Elementary Net Systems for $i = 1, 2$ and let $(\beta, \eta) : N_1 \to N_2$ be an $\widehat{N}$-morphism. Let $f_\beta : [m_0^1\rangle \to 2^{B_2}$, be given by $\forall m \in [m_0^1\rangle, f_\beta(m) = \beta(m)$ and $\forall m \in [m_0^2\rangle, f_\beta^{-1}(m) = \{m_1 \in [m_0^1\rangle : m_1 \supset \beta^{-1}(m)\}$. Hold also that:*

- *$\forall m \in [m_0^1\rangle, f_\beta(m) \in [m_0^2\rangle$,*
- *suppose $m\,[e\rangle\,m'$ then $f_\beta(m) = f_\beta(m')$ in case $\eta(e)$ is undefined, otherwise, $f_\beta(m)\,[\eta(e)\rangle\,f_\beta(m')$.*

Proof. By Prop. 3 we know that $\forall m \in [m_0^1\rangle, f_\beta(m) = \beta(m) \cup (m_0^2 - \beta(m_0^1))$.

The constraint on the surjectivity of β assure that $\beta(m_0^1) = m_0^2$, so $\forall m \in [m_0^1\rangle, f_\beta(m) = \beta(m)$ and we can also write $\forall m \in [m_0^2\rangle, f_\beta^{-1}(m) = \{m_1 \in [m_0^1\rangle : m_1 \supset \beta^{-1}(m)\}$. ◇

As shown in [6], $\widehat{N}$-morphisms preserve some properties on invariants, as stated in the next theorems.

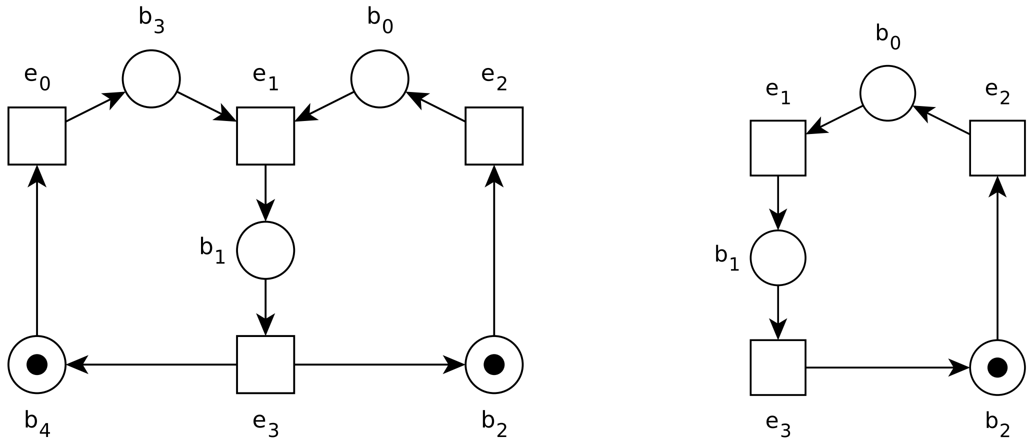
S-invariants are reflected, that is: for each S-invariant of N_2 there is a corresponding one in N_1.

Theorem 1. *For $i = 1, 2$, let $N_i = (B_i, E_i, F_i, m_0^i)$ be an Elementary Net System, M_i its incidence matrix and let $(\beta, \eta) : N_1 \to N_2$ be an $\widehat{N}$-morphism. Let M_1 be ordered so that we put rows corresponding to conditions in the range of β^{-1} in the first $|B_2|$ positions of the incidence matrix of N_1. If $\mathbf{I}_2 = (\alpha_1\alpha_2 \ldots \alpha_{|B_2|})$, with $\alpha_j \in \mathbb{N}$, is an S-invariant of N_2, then $\mathbf{I}_1 = (\alpha_1\alpha_2 \ldots \alpha_{|B_2|} \underbrace{0 \ldots 0}_{|B_1|-|B_2|})$ is an S-invariant of N_1.*

As we can see in Fig. 3.3, $I_1 = (01011)$ is an S-invariant of N_1, while the vector $I_2 = (010)$, created from I_1 by deleting values related to the places without an image in the right Net, is not an S-invariant of N_2.

T-invariants are preserved by $\widehat{N}$-morphisms.

Theorem 2. *For $i = 1, 2$, let $N_i = (B_i, E_i, F_i, m_0^i)$ be an Elementary Net System, M_i its incidence matrix (ordered as seen before); let $(\beta, \eta) : N_1 \to N_2$ be an $\widehat{N}$-morphism and let $\tau_1 : E_1 \to \mathbb{N}$. If $\mathbf{J_1^T} = (\tau_1(e_1)\tau_1(e_2) \ldots \tau_1(e_n))$ is a T-invariant for N_1, then $\mathbf{J_2^T} = (\tau_2(t_1)\tau_2(t_2) \ldots \tau_2(t_m))$ is a T-invariant for N_2, with $\tau_2(t_i) = \sum_{e_j \in \eta^{-1}(t_i)} \tau_1(e_j)$ for all $t_i \in E_2$.*



(a) N_1

(b) N_2

Figure 3.3: Two Nets related by an $\widehat{N}$-morphism

3.1.4 Π-morphisms

$\widehat{N}$-morphisms are too much permissive relating Nets. As we have seen in the previous section, they allow to add constraint that are not present in the second Net, hence breaking the idea that the first Net is a refinement of the second one.

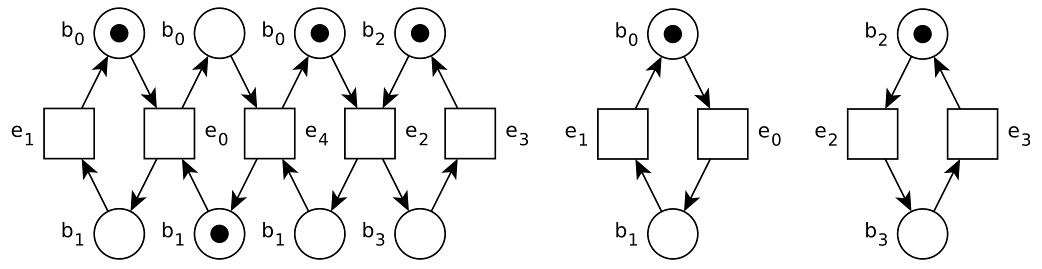
Let us start defining Π-morphisms [26], a subclass of $\widehat{N}$-morphisms.

Definition 32. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be Elementary Net Systems for $i = 1, 2$. Let (β, η) be $\widehat{N}$-morphism from N_1 to N_2. Let G_i =$\mathbf{dom}$ (η_i) the set of mapped events, and $D_i = \{b \in B_i | b \notin {}^\bullet(E_i \setminus G_i)^\bullet\}$ the set of conditions with all neighbours mapped by the morphism. Let us define $reduced(N_1)_{(\beta,\eta)} = (D_i, G_i, F_i \cap ((D_i \times G_i) \cup (G_i \times D_i)), m_0^i \cap D_i)$.*

A Π-morphism from N_1 to N_2 is an $\widehat{N}$-morphism (β, η), with the additional constraint that $reduced(N_1)_{(\beta,\eta)} \sim N_2$, that is $reduced(N_1)_{(\beta,\eta)}$ is isomorphic to N_2.

With this morphism we do not allow to add direct constraints between events of N_2. But it is still possible to add a constraint if we encode it in a path containing events not mapped. For example, N_1 in Fig. 3.4 has a path from e_0 to e_2 while in N_2 the two events are independent (elements with the same names are related by a Π-morphism).

Proposition 7. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be Elementary Net Systems for $i = 1 \ldots 3$. Let (β_i, η_i), with $i = 1, 2$, be Π-morphisms from N_i to N_{i+1}. The function $(\beta, \eta) : N_1 \to N_3$ $(\beta, \eta) = (\beta_2, \eta_2) \circ (\beta_1, \eta_1)$ where $\beta = \beta_2 \circ \beta_1$ and $\eta = \eta_2 \circ \eta_1$ is a Π-morphism.*



(a) N_1 (b) N_2

Figure 3.4: An example of Π-morphism

Proof. We know that (β, η) is an $\widehat{N}$-morphism, we have to prove that it satisfies the additional constraint that characterize Π-morphisms. We know that $N_1^r = reduced(N_1)_{(\beta_1,\eta_1)} \sim N_2$ and $reduced(N_2)_{(\beta_2,\eta_2)} \sim N_3$. From which $reduced(N_1)_{(\beta,\eta)}$ it is equivalent to $reduced(reduced(N_1)_{(\beta_1,\eta_1)})_{(\beta_2,\eta_2)} \sim reduced(N_2)_{(\beta_2,\eta_2)} \sim N_3$. ◇

The Π-morphisms are closed by composition; the identity function $1_N = (id_B, id_E)$ is a Π-morphisms where $id_B : B \to B$ and $id_E : E \to E$ are the (total) identity functions; the composition is associative. Hence, the family of Elementary Net Systems together with Π-morphisms forms a category denoted $\mathcal{ENS}_\Pi$.

3.1.5 ρ-morphisms

Consider the Reachability Graphs of the two given Nets N_1 and N_2. These are Transition Systems and, as we will show in the next section, they are related by morphisms as well as Elementary Net Systems. We want a morphism between Nets that assure the surjectivity between the Reachability Graphs, and Π-morphisms do not give us this assurance.

We now define morphisms different from the others previously seen, ρ-morphisms [26]. ρ-morphisms are a subtype of the one defined in [15]. Let us consider, from now on, only contact-free Nets.

Definition 33. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be T-restricted Elementary Net Systems $i = 1, 2$.*

A ρ-morphisms from N_1 to N_2 is a surjective mapping $\rho : X_1 \to X_2$, such that:

1. *for every edge $(x, y) \in F_1$ it holds:*

   - $(x,y) \in F_1 \cap (B_1 \times E_1) \Rightarrow (\rho(x), \rho(y)) \in F_2 \cap (B_2 \times E_2) \vee \rho(x) = \rho(y)$
   - $(x,y) \in F_1 \cap (E_1 \times B_1) \Rightarrow (\rho(x), \rho(y)) \in F_2 \cap (E_2 \times B_2) \vee \rho(x) = \rho(y)$

2. $\forall b_1 \in B_1, b_1 \in m_0^1 \Leftrightarrow \rho(b_1) \in m_0^2 \wedge \nexists\, b_1' \in B_1, \rho(b_1') = \rho(b_1)$*: every condition in the initial marking of the refined Net has to be the only one mapped in an initial condition of the abstract Net.*

Note that ρ defines an equivalence relation on X_1 and the equivalence class of a node $x \in X_1$ is $[x] = \{y \in X_1 | \rho(y) = \rho(x)\}$.

Note also that if a condition (event) x is mapped to an event (condition) y then $\rho({}^\bullet x \cup x^\bullet) = \{y\}$: this correspond in some sense to Def. 30, item 4. The difference is that in N-morphisms it is not recorded where each undefined element should be mapped. So it is possible to have a sequence of nodes that are not all "implicitly" mapped on the same node. For this reason, this morphism does not allow to add new constraints between nodes of N_2.

Also, note that $\forall (x,y) \in F_1 s.t. \rho(x) \neq \rho(y) : \rho(x) \in B_2 \Leftrightarrow x \in B_1 \wedge \rho(y) \in B_2 \Leftrightarrow y \in B_1$.

Finally, note that Def. 33, item 1 implies that the environment of each node must be preserved or, at least, must implode in the node itself: $\rho(x_1) = x_2 \Rightarrow \rho({}^\bullet x_1) = {}^\bullet x_2 \cup x_2$ and $\rho(x_1) = x_2 \Rightarrow \rho(x_1{}^\bullet) = x_2{}^\bullet \cup x_2$.

Proposition 8. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be Elementary Net Systems for $i = 1 \ldots 3$. Let ρ_i, with $i = 1, 2$, be ρ-morphisms from N_i to N_{i+1}. The function $\rho : N_1 \to N_3$ $\rho = \rho_2 \circ \rho_1$ is a ρ-morphism.*

Proof.

- We show the first part on arcs between conditions and events, the proof on arcs between events and conditions is quite identical:

  $\forall (x,y) \in F_1 \cap (B_1 \times E_1)$ there are two possible cases:

  - $\rho_1(x) = \rho_1(y)$: hence $\rho_2(\rho_1(x)) = \rho_2(\rho_1(y))$;
  - $(\rho_1(x), \rho_1(y)) \in F_2 \cap (B_2 \times E_2)$. We still have two possible cases:
    - $\rho_2(\rho_1(x)) = \rho_2(\rho_1(y))$;
    - $(\rho_2(\rho_1(x)), \rho_2(\rho_1(y))) \in F_3 \cap (B_3 \times E_3)$.

- Let us take a condition b_1 of B_1 such that $b_1 \in m_0^1$. Then, we know by definition that b_2 is an initial condition. Moreover, we also know by definition that $\nexists\, b_1' \in B_1, \rho(b_1') = \rho(b_1)$, hence in the equivalence class of b_1 there is only one condition: b_1 itself. Moreover, in the equivalence class of b_1 there is only one node: b_1 itself. By contradiction, assume that e_1 is in the equivalence class of b_1. Since the Net is T-restricted, e_1 must have at least one pre condition and one post condition, and b_1 cannot be the two of them, because we work with Elementary Net Systems. Hence, by definition, the other condition must be in the equivalence class as well, and this is a contradiction.

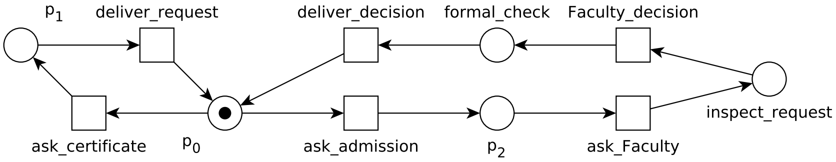


Figure 3.5: Abstract view

Now, take b_2 and follow exactly the same reasoning: in the equivalence class of b_2 there is only one nodes: b_2 itself.

Hence, $\rho(b_1) \in m_0^3 \wedge \nexists\, b_1' \in B_1, \rho(b_1') = \rho(b_1)$.

◊

3.1.6 ω-morphisms

The morphisms presented here allow to define a very general kind of refinement. We allow to refine conditions of a Net substituting them with subnets. Hence, when en event is mapped on a condition, also its environment should be mapped on the same condition. On the other hand, when it is mapped on an event it should have a corresponding environment. We do not impose particular constraints on each subnet mapped on a single condition.

An example

The example presented here aims at explaining, informally, how ω-morphisms support refinement of local states in Elementary Net Systems. The morphisms map nodes of a refined system on a more abstact one.

The Elementary Net System shown in Fig. 3.5 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.

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.

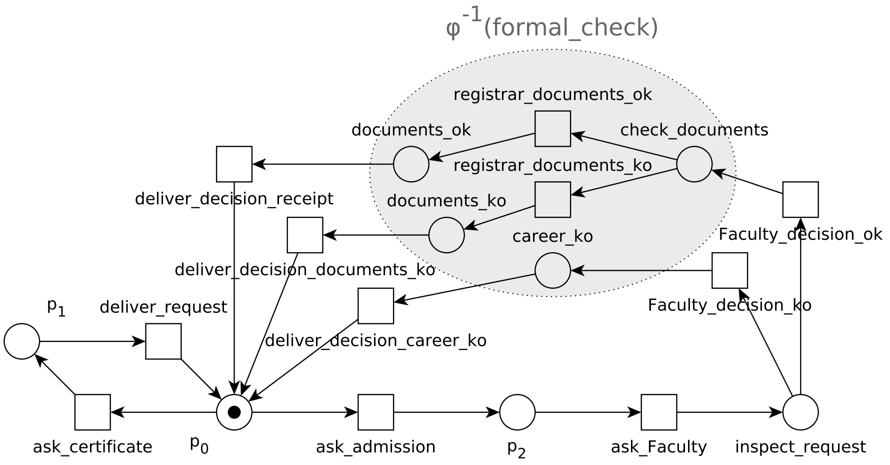


Figure 3.6: Refined model

The result of the refinement is shown in Fig. 3.6, where the subnet refining formal_check is enclosed in a shaded circle. Note that the operation has required also splitting the outgoing transitions, in order to reflect the alternative outcomes.

Definitions

We present here the formal definition of ω-morphisms [5] for State Machine Decomposable Elementary Net Systems (SMD-EN Systems).

Definition 34. *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 $\varphi : X_1 \rightarrow X_2$ 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 $\varphi({}^\bullet e_1{}^\bullet) = \{\varphi(e_1)\}$.*

Let us use the example shown in Fig. 3.7 to explain the constraints we use.

We require that the map is total and surjective because N_1 refines the abstract model N_2 and the map specifies the relation of any abstract element with its refinement. That relation is denoted by labels such that them identify the same node or each node x_{ij} of the refined Net is mapped on x_i in the abstract Net.

In particular, a subset of nodes can be mapped on a single condition $b_2 \in B_2$; in this case, we call *bubble* the subnet identified by this subset, $N_1(\varphi^{-1}(b_2))$; if

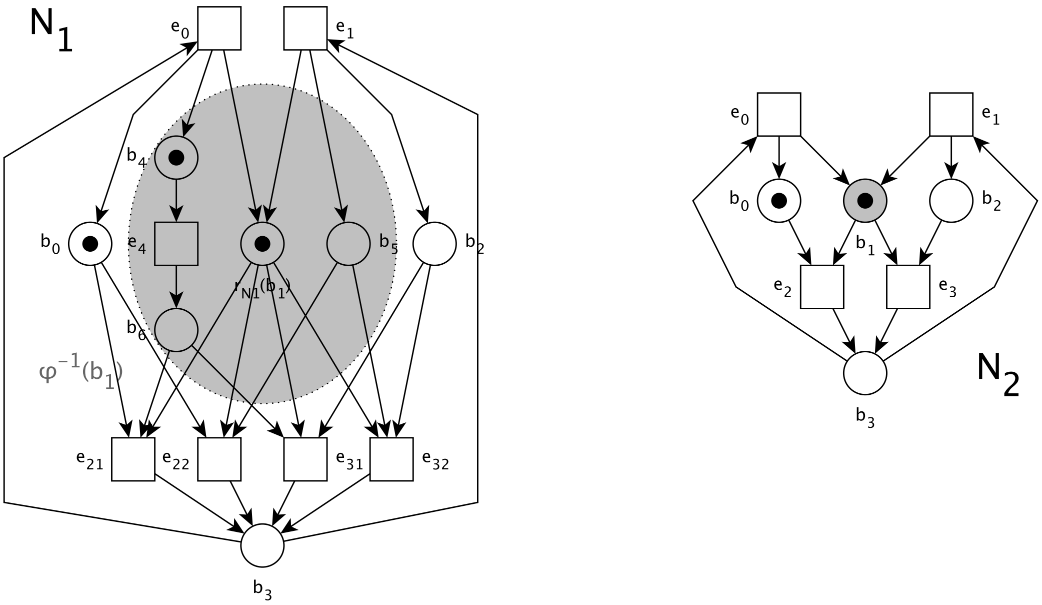


Figure 3.7: An example of ω-morphism

more than one element is mapped on b_2, we say that b_2 is *refined* by φ. In the example we can see that the subnet closed in a gray oval is the bubble of b_1, then b_1 is refined by φ.

Note that Def. 34 point 2 assures that all conditions in the initial marking of N_1 are in the bubbles of the conditions in the initial marking of N_2 and that each mapped condition can be refined by a subnet with more than one token.

The last constraints are on events: when an event is external to a bubble it is mapped on an event and its environment is preserved by φ, when it is internal to a bubble, its environment is internal too.

So far we deal only with structural constraints. However, as we know, the initial marking of a system has a big impact on its behaviour. Another important constraint we impose is on the initial marking: it has to be made only by in-conditions of the bubbles and it has to be reachable in some run of the system.

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 35. *Let $\varphi : N_1 \to N_2$ be an ω-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:*

- $\varphi^{-1}(b_2) \cap m_0^1 = \varnothing$ *or*
- *if ${}^\bullet b_2 \neq \varnothing$ 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* ${}^\bullet b_2 = \varnothing$ *then* $\varphi^{-1}(b_2) \cap m_0^1 = {}^{\bigcirc}\varphi^{-1}(b_2)$

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

Proposition 9. *Let* $N_i = (B_i, E_i, F_i, m_0^i)$ *be a SMD-EN System for* $i = 1 \dots 3$*. Let* φ_i*, with* $i = 1, 2$*, be an* ω*-morphism from* N_i *to* N_{i+1}*.*

The map $\varphi : N_1 \to N_3$*,* $\varphi = \varphi_2 \circ \varphi_1$ *is an* ω*-morphism.*

The proof is a simple verification.

The partition of the nodes of N_1 induced by an ω-morphism $\varphi : N_1 \to N_2$ can be lifted to a Net structure: the set of nodes mapped to a place b becomes a place, while the set of nodes mapped to an event e becomes an event; the flow relation is defined in the obvious way.

Definition 36. *Let* $N_i = (B_i, E_i, F_i, m_0^i)$ *be an SMD-EN System, for* $i = 1, 2$*.*

Let φ *be an* ω*-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* ω *is* $N_1/\varphi = (B_1/\varphi, E_1/\varphi, F_1/\varphi, m_0^1/\varphi)$*, where*

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

The resulting Net is isomorphic to N_2.

Proposition 10. *The quotient of* N_1*,* N_1/φ*, is an SMD-EN System isomorphic to* N_2*.*

Proof. Given the totality of the ω-morphism, it determines a partition of the nodes of N_1 and given the surjectivity of the α-morphism we have that the nodes of the quotient are exactly the same of N_2.

1. Every arrow of F_1/φ is present in F_2: note that the arrows remained are not the ones between nodes of the same equivalence class. So in F_1/φ there are only arrows between nodes belonging to different equivalence classes. Let us take one of these arrows: $(x_1, y_1) \in F_1/\varphi$ hence $(x_1, y_1) \in F_1$ and one of the two nodes is an event and the other is a condition. For Def. 34 point 4 we know that the event is mapped on an event, so for point 3 we know that $\varphi({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi(e_1{}^\bullet) = e_2{}^\bullet$. Hence in N_2 we have an arrow between the two nodes.

2. Every arrow of F_2 is present in F_1/φ: let us take one of these arrows: $(x_2, y_2) \in F_2$ and one of the two nodes is an event and the other is a condition. For the surjectivity of the ω-morphism we know that at least an event of N_1 is mapped on the event, and for Def. 34, point 3 we know that $\varphi({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi(e_1{}^\bullet) = e_2{}^\bullet$. Hence in N_1, for each inverse image of the event, we have at least an inverse image of the other node in the neighbourhood of the event.

$\diamond$

Given a ω-morphism from N_1 to N_2, we identify particular conditions of N_1, that make *canonical* the Net.

Definition 37. *Let $\varphi : X_1 \to X_2$ be an ω-morphism from N_1 to N_2. Given a condition $b_2 \in B_2$, a condition $b_1 \in \varphi^{-1}(b_2) \cap B_1$ is said to be the* representation *of b_2, denoted $r_{N_1}(b_2)$, iff:*

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

By definition of representation and by Def. 34 we get the following result.

Proposition 11. *For every representation $b_1 = r_{N_1}(b_2)$, $\varphi({}^\bullet b_1) = {}^\bullet b_2$ and $\varphi(b_1{}^\bullet) = b_2{}^\bullet$.*

A system is canonical with respect to a morphism if it contains a single representation for each condition of the abstract Net.

Definition 38. *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 for each $b_2 \in B_2$, there exists a unique $b_1 \in \varphi^{-1}(b_2) \cap B_1$ that is a representation of 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.

Note that, adding these conditions we, potentially, change the behaviour of the Net, as we can see in Fig. 3.8 adding the representation of b_1. Note also that these conditions constrain the behaviour of the Net, so we can say that between the case graphs of $N_1^{\mathcal{C}}$ and N_1 there is a G-morphism, as defined in Def. 48.

The set of all the representation of the system N_1 is denoted by $R_1^{\mathcal{C}}$. 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.

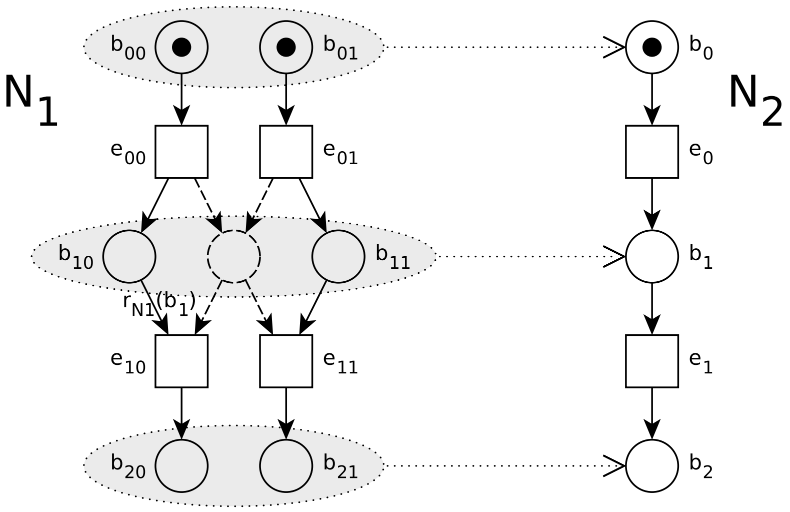


Figure 3.8: An example of ω-morphism

Proposition 12. *$\varphi^{\mathcal{C}}$ is an ω-morphism from $N_1^{\mathcal{C}}$ to N_2.*

Proof. The defined map is a total surjective function from $N_1^{\mathcal{C}}$ to N_2 by construction.

We have to prove all the constraints:

1: $\varphi^{\mathcal{C}}(B_1) = B_2$: given by construction;

2: $\varphi^{\mathcal{C}}(m_0^1) = m_0^2$: given by construction;

3: let $e_1 \in E_1$ and let $e_2 \in E_2$ such that $\varphi^{\mathcal{C}}(e_1) = e_2$. The pre and post events of every new condition have a pre or post condition that is mapped on the same condition of the second Net, hence $\varphi^{\mathcal{C}}({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi^{\mathcal{C}}(e_1{}^\bullet) = e_2{}^\bullet$;

4: let $e_1 \in E_1$ and let $b_2 \in B_2$ be such that $\varphi^{\mathcal{C}}(e_1) = b_2$: this item is not modified in $\varphi^{\mathcal{C}}$.

◇

In order to study the relations between a condition and its refinement, we need to define the following auxiliary construction. Given an ω-morphism $\varphi : N_1 \to N_2$, and a condition $b_2 \in B_2$ with its refinement $\varphi^{-1}(b_2)$, we define two new EN Systems. The first one, denoted $S_1(b_2)$, contains (a copy of) the refinement, 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 $S_1(b_2)$ is $\{b_1^{in}\}$ or, if there are no pre events, the initial marking of the bubble in N_1. The second system, denoted $S_2(b_2)$ contains b_2, its pre- and post-events and two new

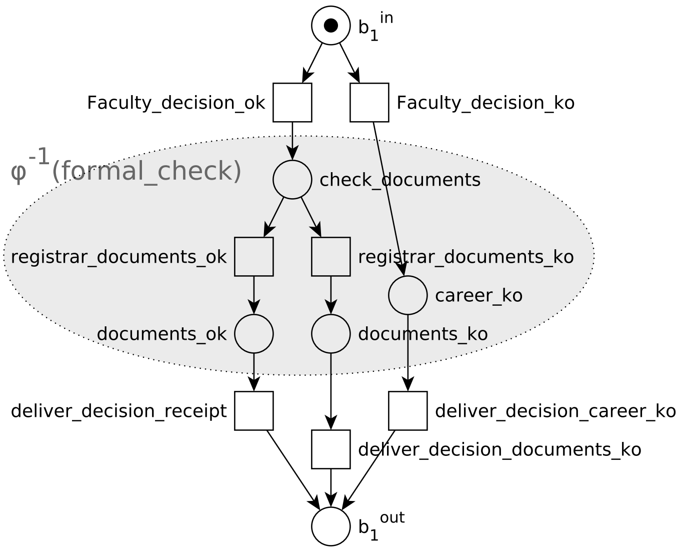


Figure 3.9: $S_1(\textsf{formal\_check})$ of Fig. 3.6.

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 $S_2(b_2)$ is $\{b_2^{in}\}$ or, if there are no pre-events, the initial marking of b_2. Note that $S_2(b_2)$ is an SMD-EN System.

Definition 39. *Let $\varphi : N_1 \to N_2$ be an ω-morphism and $b_2 \in B_2$.*

Construct two 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:

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

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

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

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

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

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

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

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

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

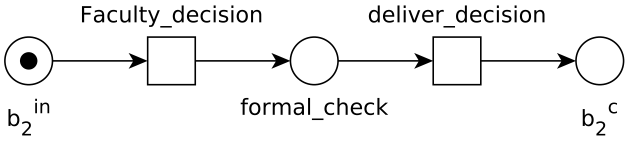


Figure 3.10: S_2(formal_check) of Fig. 3.5.

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

In Fig. 3.9 and 3.10 we show the two systems $S_1(b_2)$ and $S_2(b_2)$ for the Nets showed in the initial example with b_2 = formal_check.

Given an ω-morphism φ from N_1 to N_2, we can define a new mapping, φ^S, from $S_1(b_2)$ to $S_2(b_2)$, by restricting φ to the elements of $S_1(b_2)$, and extending it with $\varphi^S(b_1^{in}) = b_2^{in}$ and $\varphi^S(b_1^{out}) = b_2^{out}$. It is easy to see that this is still an ω-morphism.

Relations with other approaches

The ω-morphisms here defined are related to other more general morphisms as we explain in the next paragraphs.

Relations with Winskel morphisms Given an ω-morphism from N_1 to N_2 we associate to it a Winskel morphism, as defined in Def. 29, from a net, obtained by transforming N_1, to N_2. This is done taking the canonical version of N_1, $N_1^{\mathcal{C}}$, and the corresponding morphism $\varphi^{\mathcal{C}}$. This is then divided in two morphisms, one on the events and one on the conditions. The one on the conditions is restricted only to the representations.

Proposition 13. $(\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2), \varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))$ *is a Winskel morphism.*

Proof. We have to prove that the pair $(\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2), \varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))$ respects the constraints of a Winskel morphism. That is:

- $\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2)$:

  $\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2)$ is a partial injective and surjective function from $B_1^{\mathcal{C}}$ to B_2 for Def. 34, point 1 and for the canonicity of the Net. Its inverse is a total function from B_2 to $B_1^{\mathcal{C}}$, and that is more than what we want to prove;

- $\varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2)$:

  $\varphi^{\mathcal{C}} : X_1^{\mathcal{C}} \to X_2$ is a total surjective function, $\varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2)$ is a partial surjective function for Def. 34, point 1, and that is more than what we want to prove;

- $(\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2))(m_0^1) = m_0^2$: this is given by Def. 34, point 2;
- $\forall e_1 \in E_1$ there are two possibilities:
  - $(\varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))(e_1)$ is undefined (so, also its preset is undefined): this is equivalent to say that $\varphi(e_1) = b_2 \in B_2$, hence for Def. 34, point 4 we have that $\varphi({}^\bullet e_1{}^\bullet) = b_2$. Hence ${}^\bullet e_1{}^\bullet \in \varphi^{-1}(b_2)$. Hence these conditions are not mapped by $\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2)$, so $(\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2))({}^\bullet e) = \varnothing$.

    The proof for the postset is almost identical;
  - $(\varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))(e_1) = e_2$: hence it is equivalent to say that $\varphi(e_1) = e_2$. For Def. 34, point 3 we have that $\varphi({}^\bullet e_1) = {}^\bullet(\varphi(e_1))$. Moreover, we know that for each condition in the preset of e_1 that is in a bubble, we have also the representation as precondition of e_1.

    ${}^\bullet((\varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))(e_1)) = {}^\bullet(\varphi(e_1)) = \varphi({}^\bullet e_1) = (\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2))({}^\bullet e_1)$.

    The proof for the postset is almost identical.

◇

Relations with $\widehat{N}$-morphisms The second type of relation we consider are with $\widehat{N}$-morphisms, as defined in Def. 31.

Given an ω-morphism from N_1 to N_2 we associate to it an $\widehat{N}$-morphism. This is possible taking the canonical version of N_1, $N_1^{\mathcal{C}}$, and the corresponding morphism $\varphi^{\mathcal{C}}$. This is then divided in two morphisms, one on the events and one on the conditions. The one on the conditions is restricted only to the representations.

Proposition 14. *$(\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2), \varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))$ is an $\widehat{N}$-morphism.*

Proof. We have to prove that the pair $(\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2), \varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))$ respects the constraints of an $\widehat{N}$-morphism.

That is:

- $\varphi^{\mathcal{C}} : X_1^{\mathcal{C}} \to X_2$ is a total surjective function; $\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2)$ is a partial injective and surjective function for Def. 34, point 1 and for the canonicity of the Net. Its inverse is a total and injective function;
- $\varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2)$ is a partial surjective function for Def. 34;
- let $e_1 \in E_1^{\mathcal{C}}$ such that $(\varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))(e_1)$ is undefined, this is equivalent to say that $\varphi(e_1) \in B_2$, hence for Def. 34, point 4 we have that $\varphi({}^\bullet e_1{}^\bullet) = \{\varphi(e_1)\}$, hence ${}^\bullet e_1{}^\bullet \in N_1(\varphi^{-1}(\varphi(e_1)))$, hence these conditions are not mapped by $\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2)$, and this is what we want to prove;

- let $e_1 \in E_1^{\mathcal{C}}, e_2 \in E_2$ such that $(\varphi^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_2))(e_1) = e_2$: hence $\varphi(e_1) = e_2$. For Def. 34, point 3 we have that $\varphi({}^\bullet e_1) = {}^\bullet e_2$ (and $\varphi(e_1{}^\bullet) = e_2{}^\bullet$).

  Let $b_2 \in B_2$ such that $b_2 \in (\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2))({}^\bullet e_1)$, hence there is a representation $b_1 \in B_1$ such that $b_1 \in {}^\bullet e_1$ and $(\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2))(b_1) = b_2$.

  For Def. 37 we have that $\varphi({}^\bullet b_1) = {}^\bullet b_2$ and $\varphi(b_1{}^\bullet) = b_2{}^\bullet$, hence $b_2 \in {}^\bullet e_2$.

  On the other direction, let $b_2 \in B_2$ such that $b_2 \in {}^\bullet e_2$, hence for the surjectivity of the function there is a representation $b_1 \in B_1$ such that $(\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2))(b_1) = b_2$. For Def. 37 we have that $b_1 \in {}^\bullet e_1$.

  The proof for the postset is almost identical

- $\forall (b_1, b_2) \in (\varphi^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_2)) : [b_1 \in m_0^1 \Leftrightarrow b_2 \in m_0^2]$: this is given by Def. 34, point 2 and by the totality and surjectivity.

◊

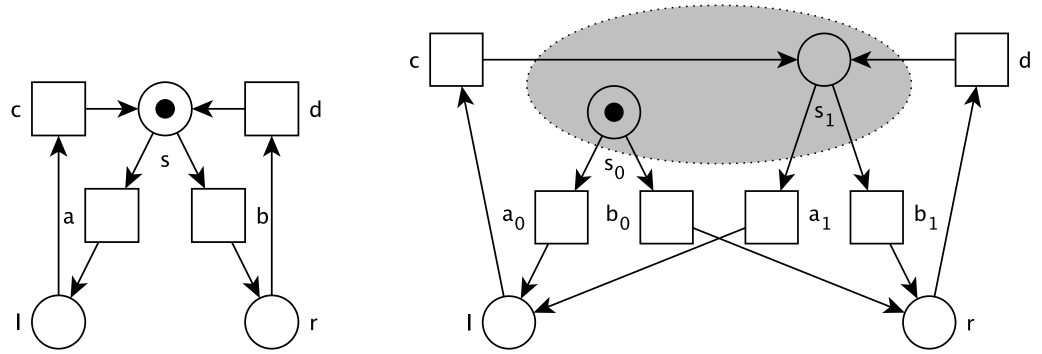
3.1.7 α-morphisms

In this section we present the formal definition of α-morphisms [5], a subclass of ω-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.

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.

The approach we present here is similar in spirit to the refinement operation proposed in [32]. 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.

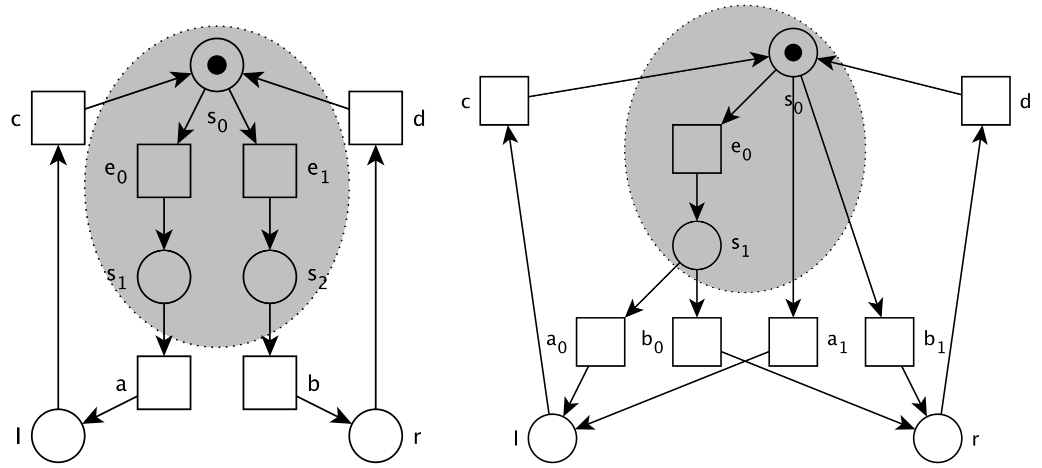
We require that a bubble does not contain an initialization part; in Fig. 3.11b we can see a refinement of the Net of Fig. 3.11a in which the bubble contains an initialization part that will be executed only once. Moreover, each final marking of the bubble must have all the possibilities the abstract condition has (for a counterexample see Fig. 3.12a). We also do not want that a token can exit (enter) from (in) the bubble before the bubble reach is end (after the bubble is already started) and you can see a counterexample in Fig. 3.12b. Finally, we require that all the pre and post-events of a bubble must be part of the same sequential component; a counterexample is shown in Fig. 3.13.



(a) An Elementary Net System

(b) Part of the bubble is not generated by one of the pre-events of the bubble

Figure 3.11: A Net and one of its refinements



(a) Each final marking of the bubble has only part of the post-events of the abstract condition

(b) The flow can exit from a condition that is not final in the bubble

Figure 3.12: Two refinements of the Net of Fig. 3.11a

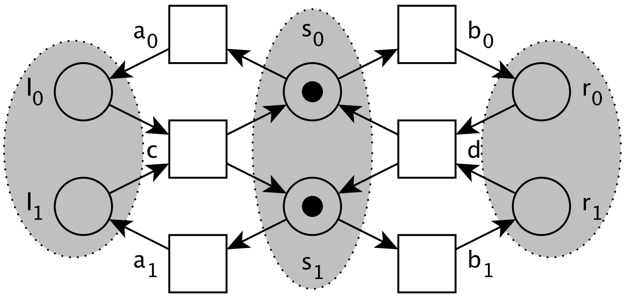


Figure 3.13: A refinements of the Net of Fig. 3.11a in which does not exist a sequential component that contains all the pre and post events of the bubble of s

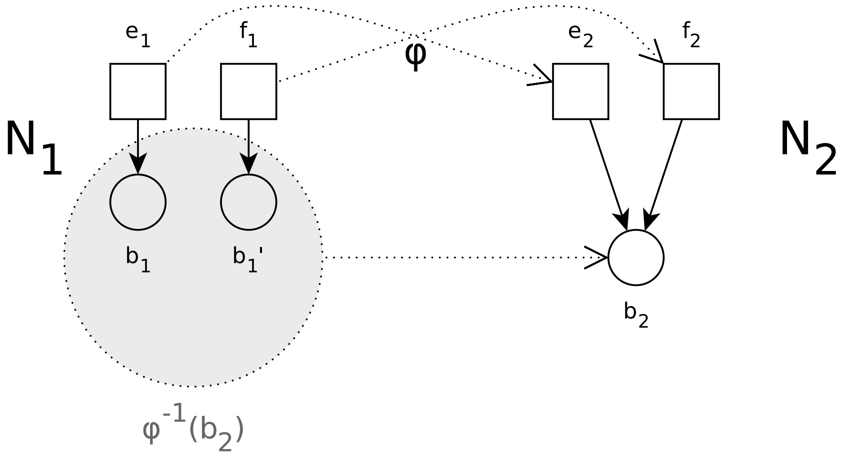


Figure 3.14: Pre events of an in-condition

Definition 40. *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) $\forall b_1 \in {}^{\circ}N_1(\varphi^{-1}(b_2)), \varphi({}^{\bullet}b_1) \subseteq {}^{\bullet}b_2$ *and* $({}^{\bullet}b_2 \neq \varnothing \Rightarrow {}^{\bullet}b_1 \neq \varnothing)$*;*

(c) $\forall b_1 \in N_1(\varphi^{-1}(b_2))^{\circ}, \varphi(b_1{}^{\bullet}) = b_2{}^{\bullet}$*;*

(d) $\forall b_1 \in \varphi^{-1}(b_2) \cap B_1$,
$(b_1 \notin {}^{\circ}N_1(\varphi^{-1}(b_2)) \Rightarrow \varphi({}^{\bullet}b_1) = \{b_2\})$ *and* $(b_1 \notin N_1(\varphi^{-1}(b_2))^{\circ} \Rightarrow \varphi(b_1{}^{\bullet}) = \{b_2\})$*;*

(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* $\varphi^{-1}({}^{\bullet}b_2{}^{\bullet}) \subseteq E_{SC}$.

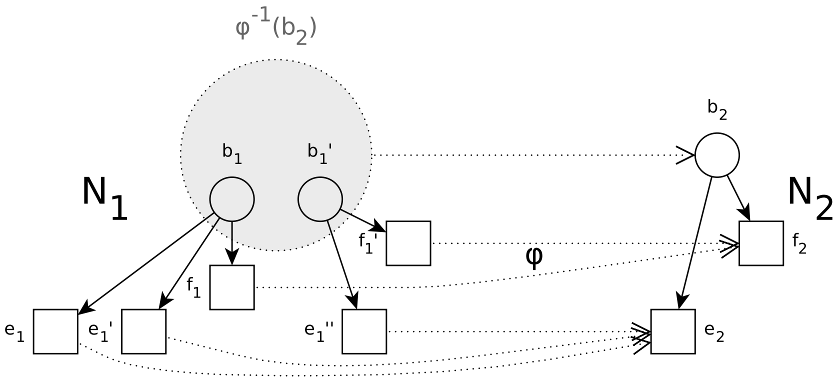


Figure 3.15: Post events of an out-condition

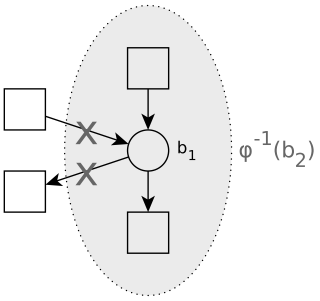


Figure 3.16: Constraints on an internal condition

As we show also in Fig. 3.1.7 and 3.1.7, 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 (even if these are only formal choices). Instead, pre-events do not need this strict constraint (5b). For example, in this particular case, we know that the choice between e_1 and f_1 of Fig. 3.1.7 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, see also Fig. 3.16.

By constraint 5e, the events in the neighbourhood of a bubble, as well as their images, cannot be concurrent. However, within a bubble there can be concurrent events. By the combined effect of 5a-5e, in any execution, when a post-event of a bubble fires, in the next marking no local state within the bubble will be marked.

Note that cycles outside the bubbles are preserved and reflected by the morphism: this is given by the finiteness of a Petri Net and by the constraints on the environment of a node.

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 denoted $\mathcal{ENS}_\alpha$.

Proposition 15. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be a SMD-EN System for $i = 1 \dots 3$. Let φ_i, with $i = 1, 2$, be an α-morphism from N_i to N_{i+1}.*

The map $\varphi : N_1 \to N_3$, $\varphi = \varphi_2 \circ \varphi_1$ is an α-morphism.

Proof. We know by Prop. 9 that φ is an ω-morphism, so we have to prove the additional items of the α-morphism (Def. 40):

5: let $b_3 \in B_3$, by definition $N_1(\varphi^{-1}(b_3)) = N_1(\varphi^{-1}(b_3)) = N_1(\varphi_1^{-1}(\varphi_2^{-1}(b_3)))$. $b_1 \in N_1(\varphi^{-1}(b_3))$, hence $\exists b_2 \in B_2 : \varphi_1(b_1) = b_2 \wedge \varphi_2(b_2) = b_3$.

5b: let $b_1 \in {}^{\bigcirc}N_1(\varphi^{-1}(b_3))$, hence $b_1 \in {}^{\bigcirc}N_1(\varphi_1^{-1}(b_2))$.

We want to prove that $b_2 \in {}^{\bigcirc}N_2(\varphi_2^{-1}(b_3))$. By contradiction, let $e_2 \in {}^\bullet b_2$ and $\varphi_2(e_2) = b_3$. For Def. 40, point 5b ${}^\bullet b_1 \neq \emptyset$, then $\exists e_1 \in E_1$ such that $e_1 \in {}^\bullet b_1$. Given that $b_2 \notin {}^{\bigcirc}N_2(\varphi_2^{-1}(b_3))$, then for Def. 40, point 5d $\varphi_2({}^\bullet b_2) = \{b_3\}$. For Def. 34, point 3 we know that $\varphi_1(e_1) \in {}^\bullet b_2$, then $\varphi(e_1) = b_3$ but this is a contradiction.

For Def. 40, point 5b:

- $\varphi_2({}^\bullet b_2) \subseteq {}^\bullet b_3$ and if ${}^\bullet b_3 \neq \emptyset$ then ${}^\bullet b_2 \neq \emptyset$ and
- $\varphi_1({}^\bullet b_1) \subseteq {}^\bullet b_2$ and if ${}^\bullet b_2 \neq \emptyset$ then ${}^\bullet b_1 \neq \emptyset$.

Then we have $\varphi({}^\bullet b_1) = \varphi_2(\varphi_1({}^\bullet b_1)) \subseteq \varphi_2({}^\bullet b_2) \subseteq {}^\bullet b_3$, and if ${}^\bullet b_3 \neq \emptyset$ then ${}^\bullet b_2 \neq \emptyset$ then ${}^\bullet b_1 \neq \emptyset$;

5c: let $b_1 \in N_1(\varphi^{-1}(b_3))^{\bigcirc}$, hence $b_1 \in N_1(\varphi_1^{-1}(b_2))^{\bigcirc}$. Given that φ_1 is an α-morphism, $\varphi_1(b_1{}^\bullet) = b_2{}^\bullet$.

Now, we want to prove that $b_2 \in N_2(\varphi_2^{-1}(b_3))^{\bigcirc}$. By contradiction, let $e_2 \in b_2{}^\bullet$ and $\varphi_2(e_2) = b_3$. Given that φ_1 is an α-morphism, $\exists e_1 \in E_1$, such that $\varphi_1(e_1) = e_2$ and $e_1 \in b_1{}^\bullet$ but this is a contradiction since $b_1 \in N_1(\varphi^{-1}(b_3))^{\bigcirc}$. Given that φ_2 is an α-morphism, $\varphi_2(b_2{}^\bullet) = b_3{}^\bullet$. Then $\varphi(b_1{}^\bullet) = \varphi_2(\varphi_1(b_1{}^\bullet)) = \varphi_2(b_2{}^\bullet) = b_3{}^\bullet$;

5d: let us start whit $b_1 \in N_1(\varphi^{-1}(b_3)) \cap B_1$ and $b_1 \notin {}^{\bigcirc}N_1(\varphi^{-1}(b_3))$.

Hence $\exists e_1 \in E_1 : e_1 \in {}^\bullet b_1 \wedge \varphi(e_1) = b_3$.

We want to show that each pre-event of b_1 is in the bubble. By contradiction, assume that $\exists e_1' \in E_1 : e_1' \in {}^\bullet b_1 \wedge \varphi(e_1') \neq b_3$. This implies that $\varphi_1(e_1') \neq b_2$, hence $\exists e_2' \in E_2 \wedge \exists e_3' \in E_3 : \varphi(e_1') = \varphi_2(\varphi_1(e_1')) = \varphi_2(e_2') = e_3' \wedge e_2' \in {}^\bullet b_2 \wedge e_3' \in {}^\bullet b_3$.

There are two cases:

- $b_2 \notin {}^{\bigcirc}N_2(\varphi^{-1}(b_3))$, then for Def. 40, point 5d $\varphi_2({}^\bullet b_2) = \{b_3\}$ and this is a contradiction;
- $b_2 \in {}^{\bigcirc}N_2(\varphi^{-1}(b_3))$ then there are two cases:
  - $\varphi_1(e_1) \in B_2$, then for Def. 34, point 4 $\varphi_1(e_1{}^\bullet) = \varphi_1(e_1)$, hence $\varphi_1(e_1) = b_2$ and then $b_1 \notin {}^{\bigcirc}N_1(\varphi^{-1}(b_2))$. Then for Def. 40, point 5d $\varphi_1({}^\bullet b_1) = \{b_2\}$, hence $\varphi_1(e_1') = b_2$ and this is a contradiction;
  - $\varphi_1(e_1) = e_2$, then for Def. 34, point 3 $\varphi_1(e_1{}^\bullet) = e_2{}^\bullet \wedge b_2 \in e_2{}^\bullet \wedge \varphi_2(e_2) \neq b_3$ because b_2 is an in-condition in the bubble of b_3. But then $\varphi(e_1) = \varphi_2(\varphi_1(e_1)) = \varphi_2(e_2) \neq b_3$ and this is a contradiction.

For the conditions of the bubble that are not out-conditions the proof is symmetrical;

5e: we want to prove that there exists a sequential component N_{SC} of N_1 such that $b_1 \in B_{SC}$ and $\varphi^{-1}({}^\bullet b_3{}^\bullet) \subseteq E_{SC}$.

Take a sequential component of N_3 that contains b_3. Using Lemma 2 construct one sequential component of N_2 containing b_2. Using the same Lemma construct one sequential component of N_1 containing b_1.

◇

Given that any α-morphism is an ω-morphism, the constructions and results stated for ω-morphisms hold for α-morphisms. Note also that adding to N_1 the representation of each condition does not modify the behaviour, because of the constraint on sequential components. In this situation the representations, redundant with respect to the behaviour, correspond to abstractions of subnets.

We have proved in the previous section that $\varphi^{\mathcal{C}}$ is an ω-morphism from $N_1^{\mathcal{C}}$ to N_2. Here, we need to prove that, if φ is an α-morphism, then $\varphi^{\mathcal{C}}$ is also an α-morphism, as needed in Section 5.1.2.

Proposition 16. *Let $\varphi : N_1 \to N_2$ be an α-morphism, then $\varphi^{\mathcal{C}}$ is an α-morphism from $N_1^{\mathcal{C}}$ to N_2.*

Proof. We know that $\varphi^{\mathcal{C}}$ is an ω-morphism, so we have to prove only the additional constraints of an α-morphism:

5: let $b_2 \in B_2$, take $N_1((\varphi^{\mathcal{C}})^{-1}(b_2))$, then:

5a: $N_1((\varphi^{\mathcal{C}})^{-1}(b_2))$ is an acyclic Net because is not modified in $\varphi^{\mathcal{C}}$;

5b: let $b_1 \in {}^{\bigcirc}N_1((\varphi^{\mathcal{C}})^{-1}(b_2))$: the only condition we have to check is the representation and by Prop. 11 we know that $\varphi({}^\bullet b_1) = {}^\bullet b_2$;

5c: let $b_1 \in N_1((\varphi^{\mathcal{C}})^{-1}(b_2))^{\bigcirc}$: the only condition we have to check is the representation and by Prop. 11 we know that $\varphi(b_1{}^\bullet) = b_2{}^\bullet$;

5d: let $b_1 \in (\varphi^{\mathcal{C}})^{-1}(b_2) \cap B_1$,
$(b_1 \notin {}^{\bigcirc}N_1((\varphi^{\mathcal{C}})^{-1}(b_2) \Rightarrow \varphi^{\mathcal{C}}({}^\bullet b_1) = \{b_2\})$ and $(b_1 \notin N_1((\varphi^{\mathcal{C}})^{-1}(b_2))^{\bigcirc} \Rightarrow \varphi^{\mathcal{C}}(b_1{}^\bullet) = \{b_2\})$: this item is not modified in $\varphi^{\mathcal{C}}$;

5e: $\forall b_1 \in \varphi^{-1}(b_2) \cap B_1$, there is a sequential component N_{SC} of N_1 such that $b_1 \in B_{SC}$ and $\varphi^{-1}({}^\bullet b_2{}^\bullet) \subseteq E_{SC}$: the only condition we have to check is the representation toghether with all the pre and post-events of the bubble. Take the sequential component that contain one of the other conditions of the bubble, delete all the nodes internal to the bubble and add the representation: clearly this is a sequential component.

◇

Note that dealing with α-morphisms, the systems $S_1(b_2)$ and $S_2(b_2)$ are SMD-EN Systems and that φ^S is an α-morphism.

Properties preserved and reflected by α-morphisms

The idea driving our interpretation of a 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 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 1. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be a SMD-EN System, for $i = 1, 2$.*
Let $\varphi : N_1 \to N_2$ be an α-morphism. Then:

1. *no input event of a bubble is enabled whenever a token is inside the bubble:*

   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 $m_1 \cap \varphi^{-1}(b_2) = \emptyset$.

2. *firing an output event of a bubble empties the bubble:*

   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 $m_1' \cap \varphi^{-1}(b_2) = \emptyset$.

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

We know by Def. 40, point 5e) that there exists a sequential component N_{SC} of N_1 such that $b_1 \in B_{SC}$ and $\varphi^{-1}({}^\bullet b_2{}^\bullet) \subseteq E_{SC}$.

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 N_{SC} contains e_1, one of its preconditions belongs to N_{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 N_{SC} contains e_1, one of its preconditions belongs to N_{SC} as well as b_1, and this is a contradiction because the sequential component has only one token.

◇

We consider SMD-EN Systems, then 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 2. *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}.

Proof. Let us assume that there is a unique condition of N_{SC2}, b_2, that is refined by the morphism.

It is easy to see that $\varphi^{-1}(N_{SC2})$ is a subnet of N_1, and that it is isomorphic to N_{SC2} except for b_2 and its neighbourhood.

Take $b_1 \in \varphi^{-1}(b_2) \cap B_1$. For Def. 40, point 5e we know that there is a sequential component N_{SC1} of N_1 such that $b_1 \in B_{SC1}$ and $\varphi^{-1}({}^\bullet b_2{}^\bullet) \subseteq E_{SC1}$.

Now build up a sequential component generated by $(B_{SC_1} \cap \varphi^{-1}(b_2)) \cup \varphi^{-1}(B_{SC_2} \setminus \{b_2\})$.

This procedure can be easily extended to the refinement of multiple conditions by applying it to a single condition each time. ◇

Sequential components are not preserved, as we can see in Fig. 3.17. 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.

Reflection of sequential components implies reflection of S-invariants.

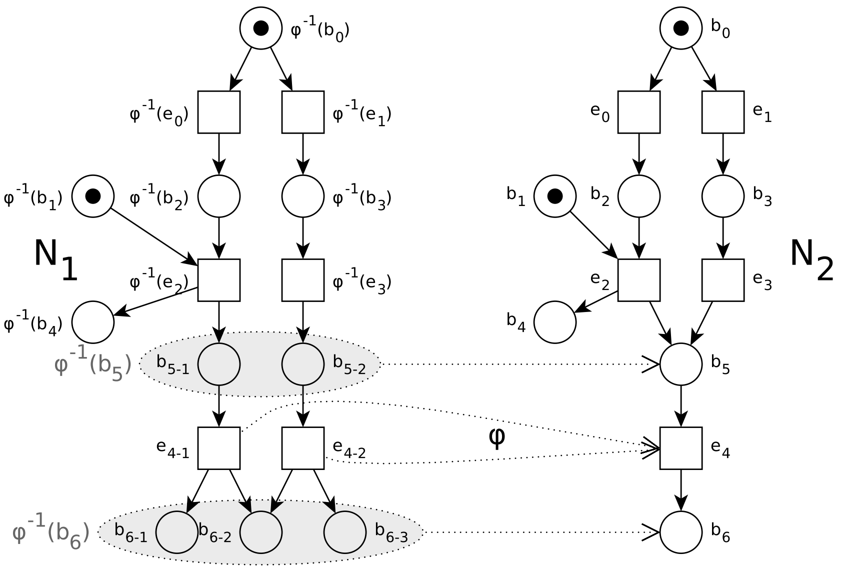


Figure 3.17: Two SMD-EN Systems related by an α-morphism

Our morphisms can be seen like a special case of Winskel morphisms [45] and defined for basic types of Net in [33], as we shall prove in Section 3.1.7. Then, since Winskel morphisms preserve reachable markings, also α-morphisms do, as stated in the following proposition.

Proposition 17. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be an EN System, for $i = 1, 2$. Suppose $\varphi : N_1 \to N_2$ is an α-morphism.*

- *If $m_1 [e\rangle m_1'$ in N_1 and $\varphi(e) \in E_2$ then $\varphi(m_1) [\varphi(e)\rangle \varphi(m_1')$ in N_2.*
- *If $m_1 [e\rangle m_1'$ in N_1 and $\varphi(e) \in B_2$ then $\varphi(m_1) = \varphi(m_1')$ in N_2.*
- *If ${}^\bullet e_1{}^\bullet \cap {}^\bullet e_1'{}^\bullet = \emptyset$ in N_1 then ${}^\bullet(\eta(e_1))^\bullet \cap {}^\bullet(\eta(e_1'))^\bullet = \emptyset$ in N_2.*

As for other morphisms in the literature, α-morphisms do not reflect reachable markings. This fact can be caused by three main cases.

The first one happens when a condition is refined by a subnet leading to a block before reaching a marking enabling out-events, as we can see in Fig. 3.18.

The second case happens when a condition of the bubble has "formally" the same possibilities of the refined condition, but in fact some of this are dead or not fireable, as we can see in Fig. 3.19, event e_{12} and e_{21}.

The third case deals with the situation in which the refinements of conditions "interfere" with each others so that, even if in each bubble a "final" local marking is reached, the global marking doesn't enable any event. That case is shown in

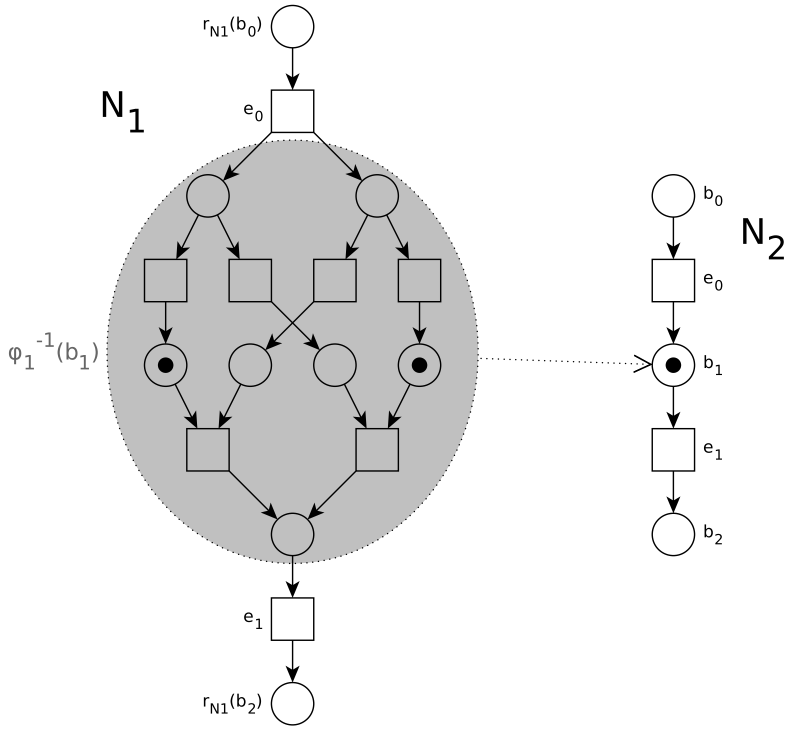


Figure 3.18: Two SMD-EN Systems related by an α-morphism.

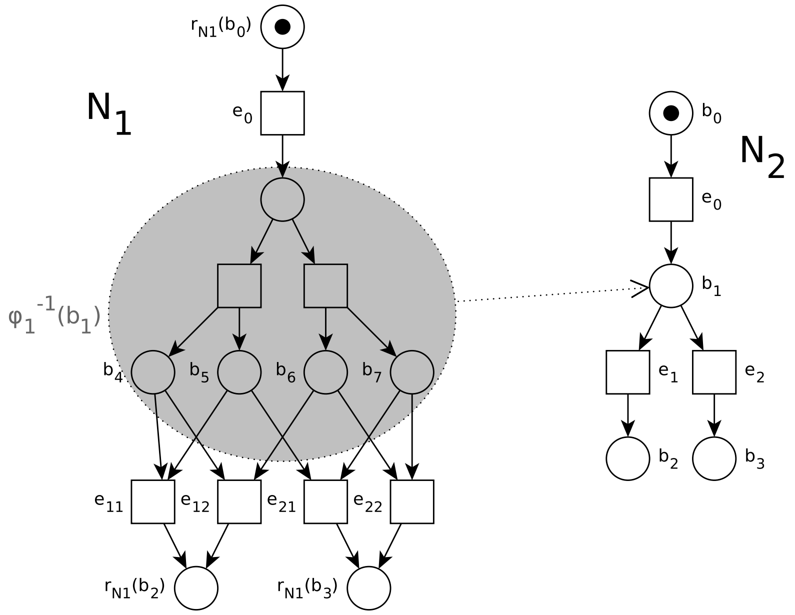


Figure 3.19: Two SMD-EN Systems related by an α-morphism.

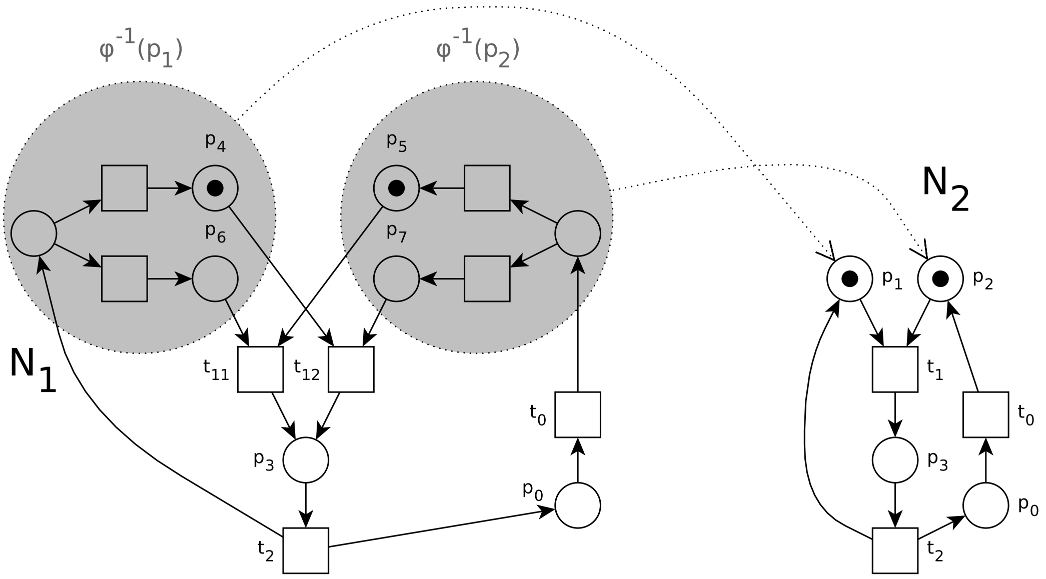


Figure 3.20: Two SMD-EN Systems related by an α-morphism.

Fig. 3.20: any event in each bubble can fire, but N_1 has two deadlocks: $\{p3, p6\}$ and $\{p4, p5\}$.

The three above cases suggest to require 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" each other. The first and second requirement is guaranteed by switching to unfolding, 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.

Then, let us deal with the unfolding of each bubble: if the map between the unfolding of $S_1(b_2)$ and $S_2(b_2)$ is an α-morphism, then we are sure that when a final marking is reached, this one enables events which correspond to the post-events of the refined condition.

Let $\varphi : N_1 \rightarrow N_2$ be an α-morphism and $\varphi^S : S_1(b_2) \rightarrow S_2(b_2)$ as in Def. 39. 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 folding function, $u : \mathit{Unf}(S_1(b_2)) \rightarrow S_1(b_2)$. The following lemma shows that, if the map, $\varphi^S \circ u$, obtained composing

φ^S with the folding 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. 39. Let 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 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.*

Proof. Since φ^S is an α-morphism, Prop. 17 assures that $S_2(b_2)$ simulates $S_1(b_2)$. Then, we need only to prove that $S_1(b_2)$ simulates $S_2(b_2)$.

We prove that r is a bisimulation between $(S_1(b_2), l_1)$ and $(S_2(b_2), l_2)$. The reachable markings of $S_2(b_2)$ are $\{\{b_2^{in}\}, \{b_2\}, \{b_2^{out}\}\}$, let us discuss the three set of markings separately:

- the initial marking of $S_2(b_2)$ is $m_0^{S2} = \{b_2^{in}\}$ and it is related to the initial marking of $S_1(b_2)$, $m_0^{S1} = \{b_1^{in}\}$.

  There are two possible cases:

  - $\{b_2^{in}\}\,[\epsilon\rangle\,\{b_2^{in}\}$: in $S_1(b_2)$ it is not possible to fire one of the pre-events of the bubble, that are the one enabled in the initial marking, because they are all labelled, so it is only possible to fire the empty word and remain in the initial marking,
  - $\{b_2^{in}\}\,[a\rangle\,\{b_2\}$: for the surjectivity of the α-morphism, in $S_1(b_2)$ there is, at least, one event mapped on a, let us call it a_1. For Def. 34, point 3, a_1 has an environment corresponding to the one of a, hence $\{b_1^{in}\}\,[a_1\rangle\,\{m_1\}$ with $\varphi^S(m_1) = b_2$. After this firing, all the events internal to the bubble can freely fire because each one is mapped on b_2, hence for Def. 34, point 4 the new marking is again related to $\{b_2\}$. It is not possible that a post-event of the bubble fires, because in that case the visible action is not a;

- let $(m_1, \{b_2\}) \in r$ such that $m_1 \subseteq \varphi^{-1}(b_2)$.

  There are two possible cases:

  - $\{b_2\}\,[\epsilon\rangle\,\{b_2\}$: this part of the proof is equivalent to the last part of the previous item,
  - $\{b_2\}\,[a\rangle\,\{b_2^{out}\}$: we prove $m_1\,(a\rangle\,\{b_1^{out}\}$ by induction on the distance between one of the initial marking of the bubble and m_1.

    base $\exists e_1 \in S_1(b_2) : {}^\bullet e_1 = b_1^{in} \wedge e_1{}^\bullet = m_1$.

    Note that m_1 is generated, in the unfolding, by an event in conflict with all the other pre-events of the bubble, hence all its future is completely disjoint from the rest of the unfolding of the bubble. Def. 40, point

5c assure that in its future there will be, at least, one event for each post-events of b_2, hence it is possible to fire one event mapped on a,

induction let m_1 be a marking internal to the bubble such that $m_1 \left[a\right\rangle$, let $m_1', m_1 \left[e_1\right\rangle m_1'$, be such that $\neg(m_1' \left[a\right\rangle)$. Hence e_1 is in conflict with all the events with label a. Thus all the future of e_1 is in conflict with all the events with label a. This is a contradiction because the morphism from the unfolding to $S_2(b_2)$ assure that each run ends in b_1^{out} and Def. 40, point 5c assure that each out-condition of the bubble should have a post-event with label a.

- the final marking of $S_2(b_2)$ is $\{b_2^{out}\}$ and it is related to the final marking of $S_1(b_2)$, $\{b_1^{out}\}$. Both are deadlock markings.

◇

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

Proposition 18. *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 Unf$(S_1(b_2))$ to $S_2(b_2)$ then, for all $m_2 \in \left[m_0^2\right\rangle$, there is $m_1 \in \left[m_0^1\right\rangle$ such that $\varphi(m_1) = m_2$.*

Proof. We 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 $m_0^1 \cap \varphi^{-1}(b_2) = \varnothing$. 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 $m_0^2 \left[\sigma_1\right\rangle m_1^2 [e_2\rangle m_2$. By the induction hypothesis, there is $m_1^1 \in \left[m_0^1\right\rangle$ 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 $m_1^1 \left[e_1\right\rangle$. If $b_2 \in {}^\bullet e_2$, by Lemma 3 there exists $e_1 \in \varphi^{-1}(e_2)$ such that $m_1^1 \left[e_1\right\rangle$. ◇

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, two 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. 17 and Prop. 18 follows that N_1 and N_2 are bisimilar.

Proposition 19. *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. 18 and Prop. 19 are stated in the case in which only one condition is refined, but they can be easily 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. 3.20 show why this constraint is required.

Relations with other approaches

The α-morphisms here defined are related to other more general morphisms as we explain in the next paragraphs.

Relations with Winskel morphisms Let us now study the relation between α-morphisms and Winskel morphisms, as introduced in Def. 29.

In the previous section we proved that ω-morphisms can be seen as Winskel morphisms, if the refined system we are dealing with is canonical. An ω-morphism does not assure that a system and his canonical version have an isomorphic case graph, so we are not able to say that ω-morphisms can be seen as a special case of Winskel morphisms.

Any α-morphism is an ω-morphism. In the case of α-morphisms, adding to N_1 some representations of each condition does not modify the behaviour, because of the constraint on sequential components, i.e.: condition 5e of Def. 40. Hence, the result stated here holds for α-morphisms. In this sense, we consider them as a special case of Winskel morphisms.

The converse is not true, as shown in Fig. 3.21 and 3.22, where a Winskel morphism from N_1 to N_2 is given. In the first figure, the morphism shown is not an α one, in the second figure it is easy to see that there is no α-morphism from N_1 to N_2.

If we impose the totality and the surjectivity to Winskel morphisms, we obtain a morphism without a lot of important features of the Winskel one. In the other direction, comparing this to α-morphisms we lost the central feature of bubbles: we can handle only bubble of conditions, loosing the possibility of mapping a subnet on a condition.

Relations with $\widehat{N}$-morphisms The second type of relation we consider are with $\widehat{N}$-morphisms, as defined in Def. 31.

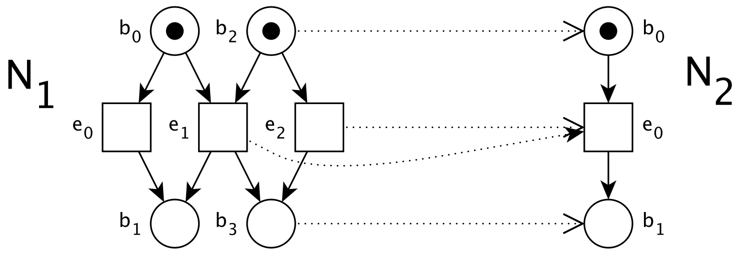


Figure 3.21: An example of Winskel morphism which is not an α-morphism

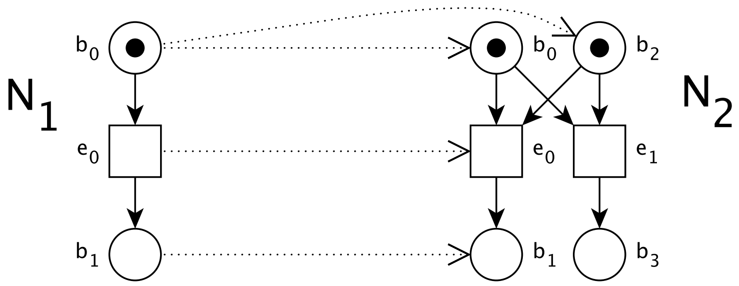


Figure 3.22: An example of Winskel morphism which is not an α-morphism

In the previous section we prove that ω-morphisms can be seen as $\widehat{N}$-morphisms if the refined system we are dealing with is canonical. An ω-morphism do not assure that a system and his canonical version have an isomorphic case graph, so we are not able to say that ω-morphisms can be seen as a special case of $\widehat{N}$-morphisms.

Any α-morphism is an ω-morphism. Adding to N_1 some representations does not modify the behaviour, because of the constraint on sequential components. Hence, the result stated here holds for α-morphisms. By these, we consider α-morphism as a special case of $\widehat{N}$-morphisms.

The converse is not true, as shown in Fig. 3.23, where an $\widehat{N}$-morphism from N_1 to N_2 is given by identical names of elements; it is easy to see that there is no α-morphism from N_1 to N_2, since there is no way to map b_3 and b_5.

3.2 Occurrence Nets

As we have seen in the previous section, using morphisms to formalize the relation between two Nets is widely used in the literature.

Clearly it is possible to see an Occurrence Net as an Elementary Net System, putting a token in each initial place of the Net. So, it is possible to use the morphisms already defined also on Occurrence Nets. We can use the concurrency,

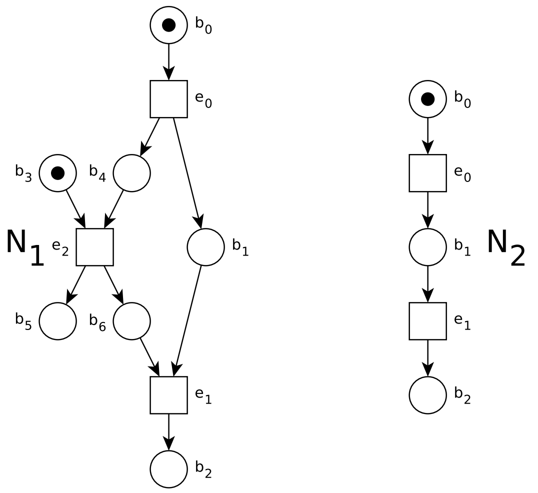


Figure 3.23: An example of $\widehat{N}$-morphism which is not an α-morphism

conflict and causality relations to obtain simpler morphisms on Occurrence Nets such that the same results obtained for Elementary Net Systems, as seen in the previous section, still hold. Moreover, we want to relate morphisms between Elementary Net Systems with morphisms between their Unfoldings and vice versa, so that we are able to obtain more behavioural properties relating only structural models.

In the rest of this section, we present different notion of morphisms on Occurrence Nets and the properties they preserve/reflect.

3.2.1 $\widehat{N_O}$-morphisms

Let us define a morphism on Occurrence Nets taking advantage of the relations of this kind of Net.

Definition 41. *Let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2$.*

An $\widehat{N_O}$-morphism from N_1 to N_2 is a map φ such that:

1. *$\varphi : X_1 \rightarrow^* X_2$ is a partial surjective function;*
2. *$x \leq_{N_1} y$, then $\varphi(x) \leq_{N_2} \varphi(y)$,*
3. *$\varphi(B_1) = B_2$;*
4. *if $\varphi(e_1)$ is undefined, then $\varphi({}^\bullet e_1{}^\bullet)$ is undefined;*
5. *if $\varphi(e_1) \in B_2$, then $\forall b \in {}^\bullet e_1{}^\bullet, \varphi(b) = \varphi(e_1)$;*

6. *if* $\varphi(e_1) = e_2$*, then* $\varphi({}^\bullet e_1) = {}^\bullet e_2$ *and* $\varphi(e_1{}^\bullet) = e_2{}^\bullet$ *and* ${}^\bullet e_1{}^\bullet \subseteq \mathbf{dom}\ (\varphi)$*;*
7. $\forall b_2 \in B_2$*, take* $N_1(\varphi^{-1}(b_2))$*, then:*
   - *(a)* $\forall b_2 \notin \max(N_2)$*, then* $|X_{N_1(\varphi^{-1}(b_2))}| < \infty$
   - *(b)* $\forall b \in \min(N_1(\varphi^{-1}(b_2))), \varphi({}^\bullet b) = {}^\bullet b_2$*;*
   - *(c)* $\forall b \in N_1(\varphi^{-1}(b_2)) : b \notin \max(N_1(\varphi^{-1}(b_2)))$*, then* $\varphi(b^\bullet) = b_2$*;*
   - *(d)* $\forall b \in \max(N_1(\varphi^{-1}(b_2))), \varphi(b^\bullet) = b_2{}^\bullet$*;*
   - *(e)* $\forall b \in \max(N_1(\varphi^{-1}(b_2))), \forall e_1 \in b^\bullet, \exists C \subseteq B_1$*:*
     C is a cut of N_1 and $b \in C$ and $C \cap N_1(\varphi^{-1}(b_2)) \subseteq \max(N_1(\varphi^{-1}(b_2)))$ *and* $C \cap \max(N_1(\varphi^{-1}(b_2))) \subseteq {}^\bullet e_1$.

$\widehat{N_O}$-morphisms allow refining local states with a subnet, they allow to map two different events in one event only if they are concurrent or in conflict. So we can see N_1 as a more detailed version of N_2, where we have refined conditions with bubbles.

In the rest of the section we state properties on $\widehat{N_O}$-morphisms. In the following let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2$ and let $\varphi : N_1$, then N_2 be an $\widehat{N_O}$-morphism.

If a bubble is not infinite, then it is always possible to find a path from a nodes internal to the bubble to a maximal node.

Proposition 20. *Let us take* $N_1(\varphi^{-1}(b_2))$ *with* $b_2 \in B_2$.
$|X_{N_1(\varphi^{-1}(b_2))}| < \infty$*, then* $\forall x \in X_{N_1(\varphi^{-1}(b_2))}, \exists y \in \max(N_1(\varphi^{-1}(b_2))) : x \leq_{N_1} y$*.*

Proof. Let $x \in X_{N_1(\varphi^{-1}(b_2))}$, we have:

- $x \in \max(N_1(\varphi^{-1}(b_2)))$: take $y = x$, then $x \leq_{N_1} x$;
- $x \notin \max(N_1(\varphi^{-1}(b_2)))$: then $\exists z \in X_{N_1(\varphi^{-1}(b_2))}$ and $z \in x^\bullet$ and we should continue until we find a condition that is maximal in the bubble. We know that this maximal condition should exists because the bubble is finite.

◇

Let us show which kind of properties $\widehat{N_O}$-morphisms preserve and reflect. Note that causality is preserved by definition. Moreover, causality is, in some sense, reflected.

Proposition 21. *Let us take* $x_2, y_2 \in X_2, x_2 \leq_{N_2} y_2$*, then* $\exists x_1, y_1 \in X_1 : \varphi(x_1) = x_2$ *and* $\varphi(y_1) = y_2$ *and* $x_1 \leq_{N_1} y_1$*.*

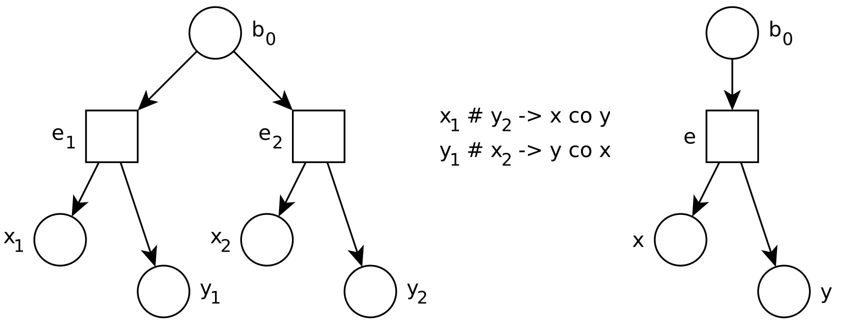


Figure 3.24: An example of $\widehat{N_O}$-morphism

Proof. We prove that by induction on the length of the interval between x_2 and y_2.

base case : $|\,]x_2, y_2[\,| = 0$ hence $x_2 \in {}^\bullet y_2$ and we have two different situation:

- $x_2 \in E_2$ and $y_2 \in B_2$: let us take $y_1 \in \min(N_1(\varphi^{-1}(y_2)))$, for Def. 41, point 7b we know that $\varphi({}^\bullet y_1) = {}^\bullet y_2$ hence $\exists x_1 \in E_1 : x_1 \in {}^\bullet y_1$ and $\varphi(x_1) = x_2$;
- $x_2 \in B_2$ and $y_2 \in E_2$: for Def. 41, point 7a we know that $N_1(\varphi^{-1}(x_2))$ is finite, so it has at least a maximal condition. Let us take $x_1 \in \max(N_1(\varphi^{-1}(x_2)))$, for Def. 41, point 7d we know that $\varphi(x_1{}^\bullet) = x_2{}^\bullet$ hence $\exists y_1 \in E_1 : y_1 \in x_1{}^\bullet$ and $\varphi(y_1) = y_2$.

induction step : $|\,]x_2, z_2[\,| = n$ and $\exists x_1, z_1 \in X_1 : \varphi(x_1) = x_2$ and $\varphi(z_1) = z_2$ and $x_1 \leq_{N_1} z_1$ now add the $n+1$ step: $z_2 \in {}^\bullet y_2$. There are two different situation:

- $z_2 \in E_2$ and $y_2 \in B_2$: for Def. 41, point 6 we know that $\varphi(z_1{}^\bullet) = z_2{}^\bullet$ hence $\exists y_1 \in B_1 : y_1 \in z_1{}^\bullet$ and $\varphi(y_1) = y_2$;
- $z_2 \in B_2$ and $y_2 \in E_2$: for Def. 41, point 7a we know that $N_1(\varphi^{-1}(z_2))$ is finite, so it has at least a maximal condition. For Prop. 20 we know that $\exists v_1 \in \max(N_1(\varphi^{-1}(z_2))) : z_1 \leq_{N_1} v_1$. For Def. 41, point 7d we know that $\varphi(v_1{}^\bullet) = z_2{}^\bullet$ hence $\exists y_1 \in E_1 : y_1 \in v_1{}^\bullet$ and $\varphi(y_1) = y_2$.

◇

Conflict is not preserved, not even weakly ($\# \cup \mathbf{id}$). Fig. 3.24 shows an example of $\widehat{N_O}$-morphism, where the map is given by the names. As we can see, in N_1 the nodes in conflict are $(e_1, e_2), (e_1, x_2), (e_1, y_2), (x_1, e_2), (x_1, x_2), (x_1, y_2), (y_1, e_2), (y_1, x_2), (y_1, y_2)$; in N_2 there are not nodes in conflict. However, as an example, x_1 is mapped on x and y_2 is mapped on y and these two nodes are concurrent.

Now we state some closure properties of the bubbles created by the morphism.

Each node internal to a bubble, in particular not minimal (maximal), has a pre (post) set internal to the bubble.

Proposition 22. *Let us take* $N_1(\varphi^{-1}(b_2))$ *with* $b_2 \in B_2$.
Let $x \in X_{N_1(\varphi^{-1}(b_2))}$, *if* $x \notin \min(N_1(\varphi^{-1}(b_2)))$, *then* $\forall y \in {}^\bullet x, \varphi(y) = b_2$.

Proof. Let $x \in X_{N_1(\varphi^{-1}(b_2))}$ and $x \notin \min(N_1(\varphi^{-1}(b_2)))$. We have:

- $x \in B_1$: because N_1 is an Occurrence Net $\exists ! e_1 \in N_1 : e_1 = {}^\bullet x$ but since x is not minimal in the bubble, $e_1 \in N_1(\varphi^{-1}(b_2))$ hence $\varphi(e_1) = b_2$;
- $x \in E_1$: for Def. 41, point 5 we have $\forall b \in {}^\bullet x, \varphi(b) = b_2$.

◇

Proposition 23. *Let us take* $N_1(\varphi^{-1}(b_2))$ *with* $b_2 \in B_2$.
Let $x \in X_{N_1(\varphi^{-1}(b_2))}$, *if* $x \notin \max(N_1(\varphi^{-1}(b_2)))$, *then* $\forall y \in x^\bullet, \varphi(y) = b_2$.

Proof. Let $x \in X_{N_1(\varphi^{-1}(b_2))}$ and $x \notin \max(N_1(\varphi^{-1}(b_2)))$. We have:

- $x \in B_1$: for Def. 41, point 7c we have $\varphi(x^\bullet) = b_2$; we know also that, if $\exists e_1 \in x^\bullet$ s.t. $\varphi(e_1)$ is undefined, then $\varphi({}^\bullet e_1{}^\bullet) = \varnothing$ and this is a contraddiction;
- $x \in E_1$: for Def. 41, point 5 we have $\forall b \in x^\bullet, \varphi(b) = b_2$.

◇

$\widehat{N_O}$-morphisms preserves and reflects minimal conditions.

Proposition 24. *Let* $b_1 \in B_1$ *such that* $b_1 \in \min(N_1)$ *and* $\varphi(b_1) = b_2$, *then* $b_2 \in \min(N_2)$.

Proof. By contraddiction, let $e_2 \in {}^\bullet b_2$. Given that $b_1 \in \min(N_1)$, we know also that $b_1 \in \min(N_1(\varphi^{-1}(b_2)))$. Then, for Def. 41, point 7b we know that $\varphi({}^\bullet b_1) = {}^\bullet b_2$ but this is a contraddiction because $b_1 \in \min(N_1)$ hence ${}^\bullet b_1 = \varnothing$. ◇

Proposition 25. *Let* $b_1 \in B_1$ *such that* $\varphi(b_1) = b_2$ *and* $b_2 \in \min(N_2)$, *then* $\varphi(\lfloor b_1 \rfloor) = b_2$.

Proof. By contraddiction, let $x \in \lfloor b_1 \rfloor : \varphi(x) \neq b_2$ and $\exists y \in x^\bullet : \varphi(y) = b_2$. x cannot be a condition for Def. 41, point 5 so it should be an event.

There are three possibilities:

- $\varphi(x)$ is undefined: but it is impossible because its post conditions should not be mapped and one of them is mapped on b_2;

- $\varphi(x) = b_2' \neq b_2$: but it is impossible because its post conditions should be mapped on the same condition and one of them is mapped on b_2;
- $\varphi(x) = e_2$: we know that $y \in x^\bullet$ and $\varphi(y) = b_2$, then for Def. 41 point 6 we have $b_2 \in {e_2}^\bullet$ but it is impossible because $b_2 \in \min(N_2)$.

◇

$\widehat{N_O}$-morphisms preserves and reflects maximal conditions.

Proposition 26. *Let $b_1 \in B_1$ such that $b_1 \in \max(N_1)$ and $\varphi(b_1) = b_2$, then $b_2 \in \max(N_2)$.*

Proof. By contraddiction, let $e_2 \in {b_2}^\bullet$. Given that $b_1 \in \max(N_1)$, we know also that $b_1 \in \max(N_1(\varphi^{-1}(b_2)))$. Then, for Def. 41, point 7d we know that $\varphi({b_1}^\bullet) = {b_2}^\bullet$ but this is a contraddiction because $b_1 \in \max(N_1)$ hence ${b_1}^\bullet = \varnothing$. ◇

Proposition 27. *Let $b_1 \in B_1$ such that $\varphi(b_1) = b_2$ and $b_2 \in \max(N_2)$, then $\varphi(\lceil b_1 \rceil) = b_2$.*

Proof. By contraddiction, let $x \in \lceil b_1 \rceil : \varphi(x) \neq b_2$ and $\exists y \in {}^\bullet x : \varphi(y) = b_2$. x cannot be a condition for Def. 41, point 5 so it should be an event.

There are three possibilities:

- $\varphi(x)$ is undefined: but it is impossible because its pre conditions should not be mapped and one of them is mapped on b_2;
- $\varphi(x) = b_2' \neq b_2$: but it is impossible because its pre conditions should be mapped on the same condition and one of them is mapped on b_2;
- $\varphi(x) = e_2$: we know that $y \in {}^\bullet x$ and $\varphi(y) = b_2$, then for Def. 41 point 6 we have $b_2 \in {}^\bullet e_2$ but it is impossible because $b_2 \in \max(N_2)$.

◇

3.2.2 $\overbrace{N_O}$-morphisms

Let us define another morphism on Occurrence Nets that it is stricter than the previous one.

Definition 42. *Let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2$.*

An $\overbrace{N_O}$-morphism from N_1 to N_2 is a map φ such that:

1. *$\varphi : X_1 \to^* X_2$ is a partial surjective function;*

2. *$x \leq_{N_1} y$, then $\varphi(x) \leq_{N_2} \varphi(y)$,*

3. *x $\mathbf{co}_{N_1}$ y, then $\varphi(x)$ $\mathbf{co}_{N_2}$ $\varphi(y)$ or $\varphi(x) = \varphi(y)$,*

4. *$\varphi(B_1) = B_2$;*

5. *if $\varphi(e_1)$ is undefined, then $\varphi({}^\bullet e_1{}^\bullet)$ is undefined;*

6. *if $\varphi(e_1) \in B_2$, then $\varphi({}^\bullet e_1{}^\bullet) = \varphi(e_1)$ and ${}^\bullet e_1{}^\bullet \subseteq \mathbf{dom}\ (\varphi)$;*

7. *if $\varphi(e_1) = e_2$, then $\varphi({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi(e_1{}^\bullet) = e_2{}^\bullet$ and ${}^\bullet e_1{}^\bullet \subseteq \mathbf{dom}\ (\varphi)$;*

8. *$\forall b_2 \in B_2$, take $N_1(\varphi^{-1}(b_2))$, then:*

   (a) *$\forall b_2 \notin \max(N_2)$, then $|X_{N_1(\varphi^{-1}(b_2))}| < \infty$;*
   (b) *$\forall b \in \min(N_1(\varphi^{-1}(b_2))), \varphi({}^\bullet b) = {}^\bullet b_2$;*
   (c) *$\forall b \in N_1(\varphi^{-1}(b_2)) : b \notin \max(N_1(\varphi^{-1}(b_2)))$, then $\varphi(b^\bullet) = b_2$;*
   (d) *$\forall b \in \max(N_1(\varphi^{-1}(b_2))), \varphi(b^\bullet) = b_2{}^\bullet$;*

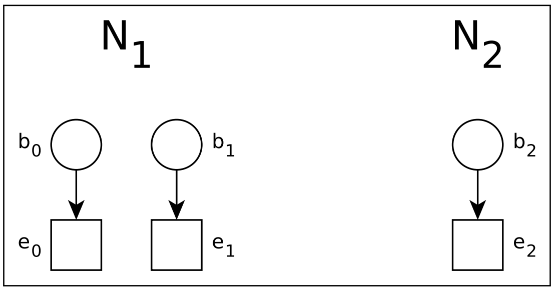
The only difference between $\overbrace{N_O}$-morphisms and $\widehat{N_O}$-morphisms is that $\overbrace{N_O}$-morphisms ask for the co-*preservation* while $\widehat{N_O}$-morphisms constrain on the relation between maximal places of each bubble and its post-events.

In the rest of the section we state properties on $\overbrace{N_O}$-morphisms.

$\overbrace{N_O}$-morphisms implies $\widehat{N_O}$-morphisms.

Proposition 28. *Let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2$ and let $\varphi : N_1 \to N_2$ be an $\overbrace{N_O}$-morphism. φ is an $\widehat{N_0}$-morphisms.*

Proof. We have to prove that x $\mathbf{co}_{N_1}$ y, then $\varphi(x)$ $\mathbf{co}_{N_2}$ $\varphi(y)$ or $\varphi(x) = \varphi(y)$ implies $\forall b_2 \in B_2, \forall b \in \max(N_1(\varphi^{-1}(b_2))), \forall e_1 \in b^\bullet, \exists C \subseteq B_1 : C$ is a *cut* of N_1 and $b \in C$ and $C \cap N_1(\varphi^{-1}(b_2)) \subseteq \max(N_1(\varphi^{-1}(b_2)))$ and $C \cap \max(N_1(\varphi^{-1}(b_2))) \subseteq {}^\bullet e_1$.



Let us take a $b_2 \in B_2 : b_2 \notin \max(N_2)$, hence there is an $e_2 \in E_2$ such that $e_2 \in b_2{}^\bullet$. Let us take $b_0 \in \max(N_1(\varphi^{-1}(b_2))$, then for Def. 42, point 8d there is an $e_0 \in E_1$ such that $e_0 \in b_0{}^\bullet$ and $\varphi(e_0) = e_2$.

By contradiction, suppose that there exists no cut of N_1 such that $b_0 \in C$ and $C \cap N_1(\varphi^{-1}(b_2)) \subseteq \max(N_1(\varphi^{-1}(b_2)))$ and $C \cap \max(N_1(\varphi^{-1}(b_2))) \subseteq {}^\bullet e_1$. So, it must exists a $b_1 \in N_1(\varphi^{-1}(b_2))$ such that b_1 **co** b_0 and $b_1 \in \max(N_1(\varphi^{-1}(b_2)))$ and $b_1 \notin {}^\bullet e_0$. Then, for Def. 42, point 8d we know that $\exists e_1 \in E_1$ and $e_1 \in b_1{}^\bullet$ and $\varphi(e_1) = e_2$.

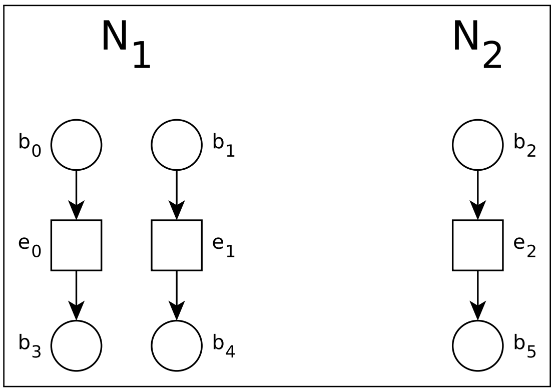
Now, we can say that b_0 $\mathbf{co}_{N_1}$ e_1 (and also b_1 $\mathbf{co}_{N_1}$ e_0). But this it is a contradiction because $\varphi(b_0) = b_2 \leq_{N_I} e_2 = \varphi(e_1)$ but the $\overbrace{N_O}$-morphism is **co**-preserving. ◇

In the following let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2$ and let $\varphi : N_1 \to N_2$ be an $\overbrace{N_O}$-morphism.

The set of events that are mapped on the same event is a #-set.

Proposition 29. *Let $e_2 \in E_2$, then $\varphi^{-1}(e_2)$ is a #-set.*

Proof. Let us take $e_2 \in E_2$, $e_0, e_1 \in E_1 : \varphi(e_0) = \varphi(e_1) = e_2$.



For Def. 42, point 7 we know that $\varphi({}^\bullet e_0) = \varphi({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi(e_0{}^\bullet) = \varphi(e_1{}^\bullet) = e_2{}^\bullet$ and ${}^\bullet e_0{}^\bullet \subseteq \mathbf{dom}\ (\varphi)$ and ${}^\bullet e_1{}^\bullet \subseteq \mathbf{dom}\ (\varphi)$.

By contradiction, there are two cases:

- e_0 **li** e_1: assume that $e_0 \leq e_1$. Let us take $]e_0, e_1[$. It is impossible that $\varphi(]e_0, e_1[)$ is a single condition b, because in that case $b \in {}^\bullet e_2$ and $b \in e_2{}^\bullet$ and this is impossible. So, there must be an event $e \in]e_0, e_1[: \varphi(]e_0, e[) = b_5$ and $\varphi(]e, e_1[) = b_2$ and $\varphi(e) \neq e_2$. Moreover, $\varphi(e)$ cannot be undefined, because in that case its neighbourhood must be undefined, but the neighbourhood of e_0 and e_1 must not. For the **li**-preservation we have that $e_0 <_{N_1} e <_{N_1} e_1$, then $\varphi(e_0) = e_2 \leq_{N_2} \varphi(e) \leq_{N_2} e_2 = \varphi(e_1)$ and this is impossible.

- e_0 **co** e_1: there must be an $b_0 \in E_1 : b_0 \in {}^\bullet e_0$. Let $\varphi(b_0) = b_2$, for Def. 42, point 7 we know that $b_2 \in {}^\bullet e_2$. Clearly, b_0 **co** e_1 but $\varphi(b_0) = b_2 \leq_{N_2} \varphi(e_1)$ and this is impossible.

◊

A run is mapped on a run.

Proposition 30. *Let $R_1 \subseteq X_1$ be a run of N_1; then $\varphi(R_1)$ is a run of N_2.*

Proof. This is given by the fact that a run is a clique of **li** ∪ **co** and an $\overbrace{N_O}$-morphism is **li**-preserving and **co**-preserving. ◊

Let us now define the composite morphism.

Proposition 31. *Let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1 \ldots 3$. Let φ_i, with $i = 1, 2$, be an $\overbrace{N_O}$-morphism from N_i to N_{i+1}.*

The map $\varphi : N_1 \to N_3$ defined as $\varphi = \varphi_2 \circ \varphi_1$ is an $\overbrace{N_O}$-morphism.

Proof. We have to prove all the conditions of an $\overbrace{N_O}$-morphism:

1: $\varphi : X_1 \to^* X_3$ is a partial surjective function: given by the composition of two partial surjective functions;

2: $x \leq_{N_1} y$: given by the composition of two monotone functions;

3: x $\mathbf{co}_{N_1}$ y, there are two possibilities:

- $\varphi_1(x)$ $\mathbf{co}_{N_2}$ $\varphi_1(y)$, there are two cases:
  - $\varphi_2(\varphi_1(x))$ $\mathbf{co}_{N_3}$ $\varphi_2(\varphi_1(y))$ or
  - $\varphi_2(\varphi_1(x)) = \varphi_2(\varphi_1(y))$;
- $\varphi_1(x) = \varphi_1(y)$ hence $\varphi_2(\varphi_1(x)) = \varphi_2(\varphi_1(y))$;

4: $\varphi(B_1) = B_3$: given by the composition;

5: let $\varphi(e_1)$ is undefined, there are three cases:

- $\varphi_1(e_1)$ is undefined then $\varphi_1({}^\bullet e_1) = \emptyset = \varphi_1(e_1{}^\bullet)$ and $\varphi_2(\emptyset) = \emptyset$;
- $\varphi_1(e_1) = b_2$, then $\varphi_1({}^\bullet e_1) = b_2 = \varphi_1(e_1{}^\bullet)$ and $\varphi_2(b_2)$ is undefined;
- $\varphi_1(e_1) = e_2$, then $\varphi_1({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi_1(e_1{}^\bullet) = e_2{}^\bullet$ and $\varphi_2(e_2)$ is undefined then $\varphi_2({}^\bullet e_2) = \emptyset = \varphi_2(e_2{}^\bullet)$;

6: let $\varphi(e_1) \in B_3$, there are two cases:

- $\varphi_1(e_1) = b_2$, then $\varphi_1({}^\bullet e_1{}^\bullet) = b_2$ and ${}^\bullet e_1{}^\bullet \subseteq$**dom** (φ_1) and $\varphi_2(b_2) = b_3$;

- $\varphi_1(e_1) = e_2$, then $\varphi_1({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi_1(e_1{}^\bullet) = e_2{}^\bullet$ and ${}^\bullet e_1{}^\bullet \subseteq$**dom** (φ_1) and $\varphi_2(e_2) = b_3$, then $\varphi_2({}^\bullet e_2{}^\bullet) = b_3$;

7: let $\varphi(e_1) = e_3$, then $\exists e_2 \in E_2 : \varphi(e_1) = \varphi_2(\varphi_1(e_1)) = \varphi_2(e_2) = e_3$.

$\varphi_1(e_1) = e_2$, then $\varphi_1({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi_1(e_1{}^\bullet) = e_2{}^\bullet$ and ${}^\bullet e_1{}^\bullet \subseteq$**dom** (φ_1).

$\varphi_2(e_2) = e_3$, then $\varphi_2({}^\bullet e_2) = {}^\bullet e_3$ and $\varphi_2(e_2{}^\bullet) = e_3{}^\bullet$ and ${}^\bullet e_2{}^\bullet \subseteq$**dom** (φ_2).

By these, we have $\varphi({}^\bullet e_1) = \varphi_2(\varphi_1({}^\bullet e_1)) = \varphi_2({}^\bullet e_2) = {}^\bullet e_3$ and $\varphi(e_1{}^\bullet) = \varphi_2(\varphi_1(e_1{}^\bullet)) = \varphi_2(e_2{}^\bullet) = e_3{}^\bullet$.

By contraddiction, let $b_1 \in B_1, b_1 \in {}^\bullet e_1{}^\bullet : b_1 \notin$**dom** (φ). Then it should be that $\varphi_1(b_1)$ is undefined but this is a contradiction because we know that ${}^\bullet e_1{}^\bullet \subseteq$**dom** (φ_1) or that $\varphi_1(b_1) = b_2 \in B_2$ such that $b_2 \in {}^\bullet e_2{}^\bullet$ and $\varphi_2(b_2)$ is undefined but this is a contradiction because we know that ${}^\bullet e_2{}^\bullet \subseteq$**dom** (φ_2).

8: Let $b_3 \in B_3$, and take $N_1(\varphi^{-1}(b_3))$.

Let $b_1 \in N_1(\varphi^{-1}(b_3))$ hence $\exists b_2 \in B_2 : \varphi_1(b_1) = b_2$ and $\varphi_2(b_2) = b_3$.

8a: $b_3 \notin \max(N_3)$ hence $|X_{N_2(\varphi_2^{-1}(b_3))}| < \infty$. Moreover $\exists e_3 \in E_3 : b_3 \in {}^\bullet e_3$. For Def. 42, point 8d $\forall b_2 \in \max(N_2(\varphi_2^{-1}(b_3))), \varphi(b_2{}^\bullet) = b_3{}^\bullet$ and this means that these conditions are not maximal in N_2. Hence $|X_{N_1(\varphi_1^{-1}(b_2))}| < \infty$, then $N_1(\varphi^{-1}(b_3))$ is the sum of finite set, that is a finite set: $|X_{N_1(\varphi^{-1}(b_3))}| < \infty$;

8b: let $b_1 \in \min(N_1(\varphi^{-1}(b_3)))$, then for Prop. 24 we know that $b_2 \in \min(N_2(\varphi_2^{-1}(b_3)))$, and then for Def. 42, point 8b we have $\varphi_2({}^\bullet b_2) = {}^\bullet b_3$.

Given that $b_1 \in \min(N_1(\varphi^{-1}(b_3)))$ it easy to see that $b_1 \in \min(N_1(\varphi_1^{-1}(b_2)))$, then for Def. 42, point 8b we have $\varphi_1({}^\bullet b_1) = {}^\bullet b_2$.

Hence $\varphi({}^\bullet b_1) = \varphi_2(\varphi_1({}^\bullet b_1)) = \varphi_2({}^\bullet b_2) = {}^\bullet b_3$.

8c: let $b_1 \in N_1(\varphi^{-1}(b_3))$ such that $b_1 \notin \max(N_1(\varphi^{-1}(b_3)))$. Hence $\exists e_1 \in E_1 : e_1 \in b_1{}^\bullet$ and $\varphi(e_1) = b_3$.

By contradiction, assume that $\exists e_1' \in E_1 : e_1 \in b_1{}^\bullet$ and $\varphi(e_1) \neq b_3$. For Def. 42, point 5 we know that this event is in the domain of the function. This implies that $\exists e_2' \in E_2$ and $\exists e_3' \in E_3 : \varphi(e_1') = \varphi_2(\varphi_1(e_1')) = \varphi_2(e_2') = e_3'$ and For Def. 42, point 7 we have that $e_2' \in b_2{}^\bullet$ and $e_3' \in b_3{}^\bullet$.

There are two possibilities:

- $b_2 \notin \max(N_2(\varphi_2^{-1}(b_3)))$, then for Def. 42, point 8c $\varphi_2(b_2{}^\bullet) = b_3$, then $\varphi_2(e_2') = b_3$ and this is a contradiction;
- $b_2 \in \max(N_2(\varphi_2^{-1}(b_3)))$ then, for Prop. 27 we know that $\varphi_1([b_1]\cap N_1(\varphi^{-1}(b_3))) = b_2$. Hence, $\varphi_1(e_1) = b_2$. Hence, $b_1 \notin \max(N_1(\varphi_1^{-1}(b_2)))$.

Hence, for Def. 42, point 8c we know that $\varphi(b_1{}^\bullet) = b_2$, hence $\varphi_1(e_1') = b_2$ but this is a contradiction.

8d: let $b_1 \in \max(N_1(\varphi^{-1}(b_3)))$. Then, for Prop. 26, we know that $b_2 \in \max(N_1(\varphi_2^{-1}(b_3)))$, hence $\varphi_2(b_2{}^\bullet) = b_3{}^\bullet$.

Since $b_1 \in \max(N_1(\varphi^{-1}(b_3)))$ it is easy to see that $b_1 \in \max(N_1(\varphi_1^{-1}(b_2)))$, hence $\varphi_1(b_1{}^\bullet) = b_2{}^\bullet$.

Then we have $\varphi(b_1{}^\bullet) = \varphi_2(\varphi_1(b_1{}^\bullet)) = \varphi_2(b_2{}^\bullet) = b_3{}^\bullet$.

$\diamondsuit$

3.2.3 θ-morphisms

Let us define another morphism on Occurrence Nets that it is the total version of the previous one.

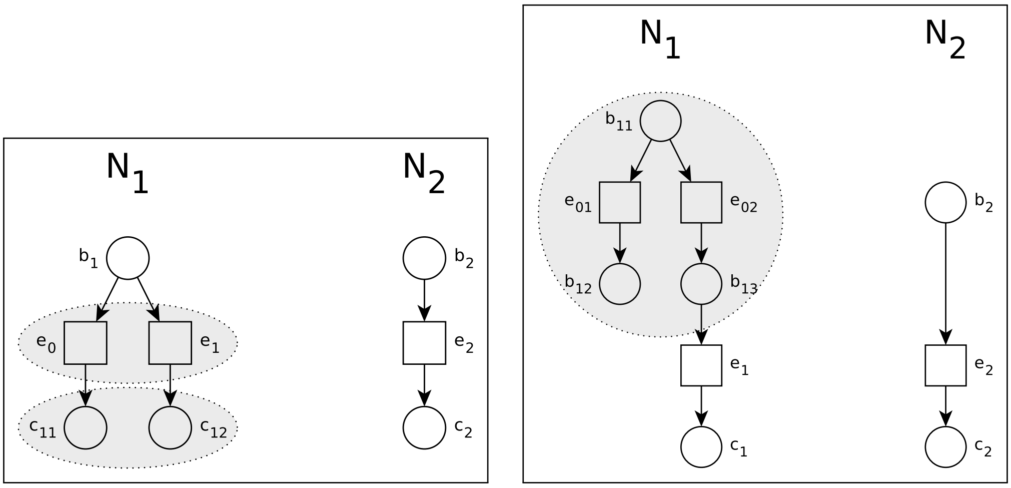
Definition 43. *Let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2$.*

a θ-morphism from N_1 to N_2 is an $\overbrace{N_O}$-morphism with the additional restriction that $\varphi : X_1 \to X_2$ is a total surjective function.

Let us rewrite the complete definition of θ-morphisms.

Definition 44. *Let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2$.*
a θ-morphism from N_1 to N_2 is is a map φ such that:

1. *$\varphi : X_1 \to X_2$ is a total surjective function;*
2. *$x \leq_{N_1} y$, then $\varphi(x) \leq_{N_2} \varphi(y)$;*
3. *$x \ \mathbf{co}_{N_1} \ y$, then $\varphi(x) \ \mathbf{co}_{N_2} \ \varphi(y)$ or $\varphi(x) = \varphi(y)$;*
4. *$\varphi(B_1) = B_2$;*
5. *if $\varphi(e_1) \in B_2$, then $\varphi({}^\bullet e_1{}^\bullet) = \varphi(e_1)$;*
6. *if $\varphi(e_1) = e_2$, then $\varphi({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi(e_1{}^\bullet) = e_2{}^\bullet$;*
7. *$\forall b_2 \in B_2$, take $N_1(\varphi^{-1}(b_2))$, then:*
   - *(a) $\forall b_2 \notin \max(N_2)$, then $|X_{N_1(\varphi^{-1}(b_2))}| < \infty$;*
   - *(b) $\forall b \in \min(N_1(\varphi^{-1}(b_2))), \varphi({}^\bullet b) = {}^\bullet b_2$;*
   - *(c) $\forall b \in N_1(\varphi^{-1}(b_2)) : b \notin \max(N_1(\varphi^{-1}(b_2)))$, then $\varphi(b^\bullet) = b_2$;*
   - *(d) $\forall b \in \max(N_1(\varphi^{-1}(b_2)), \varphi(b^\bullet) = b_2{}^\bullet$.*



(a)

(b)

Figure 3.25: Examples of θ-morphisms

li and **co** $\cup$ **id** are preserved by definition of the morphism.

The map $\varphi = \{(b_1, b_2), (e_0, e_2), (e_1, e_2), (c_{11}, c_2), (c_{12}, c_2)\}$ between N_1 and N_2 shown in Fig. 3.25a is a θ-morphism. As we can see $\#$ is not preserved: $c_{11} \# e_1$ but $\varphi(c_{11}) = c_2$ **li** $e_2 = \varphi(e_1)$.

The map $\varphi = \{(b_{11}, b_2), (e_{01}, b_2), (e_{02}, b_2), (b_{12}, b_2), (b_{13}, b_2), (e_1, e_2), (c_1, c_2)\}$ between N_1 and N_2 shown in Fig. 3.25b is a θ-morphism. Note that **co** does not imply point 7a of Def. 44.

We assume now that the Occurrence Nets we deal with are finite. We are then able to define the morphism in a more compact way.

Definition 45. *Let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2$.*

A θ-morphism from N_1 to N_2 is a map φ such that:

1. *$\varphi : X_1 \to X_2$ is a total surjective function;*

2. *$x \leq_{N_1} y$, then $\varphi(x) \leq_{N_2} \varphi(y)$;*

3. *x **co**$_{N_1}$ y, then $\varphi(x)$ **co**$_{N_2}$ $\varphi(y)$ or $\varphi(x) = \varphi(y)$;*

4. *$\varphi(B_1) = B_2$;*

5. *if $\varphi(e_1) \in B_2$, then $\varphi({}^\bullet e_1{}^\bullet) = \varphi(e_1)$;*

6. *if $\varphi(e_1) = e_2$, then $\varphi({}^\bullet e_1) = {}^\bullet e_2$ and $\varphi(e_1{}^\bullet) = e_2{}^\bullet$;*

7. *$\forall b_2 \in B_2$, take $N_1(\varphi^{-1}(b_2))$, then:*

(a) $\forall b \in \min(N_1(\varphi^{-1}(b_2))), \varphi({}^\bullet b) = {}^\bullet b_2$*;*

(b) $\forall b \in N_1(\varphi^{-1}(b_2)) : b \notin \max(N_1(\varphi^{-1}(b_2)))$*, then* $\varphi(b^\bullet) = b_2$*;*

(c) $\forall b \in \max(N_1(\varphi^{-1}(b_2))), \varphi(b^\bullet) = {b_2}^\bullet$.

As we stated before, the existence of a morphism between two Nets leads to the recognition of bubbles. Moreover, it is possible to partition every bubble into sub-bubbles, each associated to one of the events that are mapped on the unique pre event of the refined condition. Let us define in a more formal way bubbles and sub-bubbles.

Definition 46. *Let* $N_i = (B_i, E_i, F_i)$ *be an Occurrence Net for* $i = 1, 2$ *and let* $\varphi : N_1 \to N_2$ *be a* θ*-morphism.*

For each condition $b_2 \in B_2$ *the* bubble *of* b_2 *is given by the counterimage of* b_2*:* $N_1(\varphi^{-1}(b_2))$.

The representation *of* b_2*, denoted* $r_{N_1}(b_2)$*, is a condition* b_1 *of* N_1 *that respect the following constraint:* $b_1 \in \min(N_1(\varphi^{-1}(b_2))) \cap \max(N_1(\varphi^{-1}(b_2)))$.

For each condition $b_2 \in B_2$ *that is not minimal in* N_2 *and for each* $e_1 \in \varphi^{-1}({}^\bullet b_2)$ *the* sub-bubble *of* b_2 *associated to* e_1 *is given by the subnet of the bubble of* b_2 *that is in the future of* e_1*:* $N_1((\varphi^{-1}(b_2)) \cap \lceil e_1 \rceil)$.

As we saw before, a set of events mapped on the same event is a $\#$-set: by this, we infer that every sub-bubble is disjoint from the others and that dividing a bubble in sub-bubbles is like partitioning the bubble.

Let us now define the composite morphism.

Proposition 32. *Let* $N_i = (B_i, E_i, F_i)$ *be an Occurrence Net for* $i = 1 \ldots 3$*. Let* φ_i*, with* $i = 1, 2$*, be a* θ*-morphism from* N_i *to* N_{i+1}*.*

The map $\varphi : N_1 \to N_3$ *with* $\varphi = \varphi_2 \circ \varphi_1$ *is a* θ*-morphism.*

The proof follow by the proof of composition of $\overbrace{N_O}$-morphisms, Prop. 31.

An Occurrence Net is canonical with respect to a morphism if it contains a single representation for each condition of the abstract Net.

Definition 47. *Let* $N_i = (B_i, E_i, F_i)$ *be an Occurrence Net for* $i = 1, 2$ *and let* $\varphi : N_1$*, then* N_2 *be a* θ*-morphism.*

N_1 *is* canonical *with respect to* φ *if for each* $b_2 \in B_2$*, there exists a unique* b_1 *in each sub-bubble that is a representation of* 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 or by deleting the multiple ones. It is easy to verify that the canonical version of a system, with respect to an θ-morphism to another Occurrence Net, is unique up to isomorphisms.

We list here an algorithm to do this:

Algorithm 1. $B = B_1, F = F_1; \varphi^{\varphi} = \varphi$

```
$\forall b_2 \in B_2$
    $\forall e_1 \in \varphi^{-1}({}^{\bullet}b_2)$    (note that $e_1 \in E_1 \cup$ the initial event, the one that "generate" the Occurrence Net)
        if $\nexists\, b_1 \in B_1 : b_1 \in (\min(N_1((\varphi^{-1}(b_2)) \cap \lceil e_1 \rceil)) \cap \max(N_1((\varphi^{-1}(b_2)) \cap \lceil e_1 \rceil)))$ then
            $B + = b_{2(e_1)}$
            if $e_1 \in E_1$ then
                $F + = (e_1, b_{2(e_1)})$
            $\varphi^{\varphi} + = (b_{2(e_1)}, b_2)$
            $\forall e_p \in (\max(N_1((\varphi^{-1}(b_2)) \cap \lceil e_1 \rceil)))^{\bullet}$
                $F + = (b_{2(e_1)}, e_p)$
```

The corresponding morphism, $\varphi^{\mathcal{C}}$, coincides with φ, plus the mapping of the new conditions on the corresponding conditions of N_2.

Proposition 33. *$\varphi^{\mathcal{C}}$ is a θ-morphism from $N_1^{\mathcal{C}}$ to N_2.*

Proof. We have to prove all the constraints:

1: $\varphi^{\mathcal{C}} : X_1 \to X_2$ is a total surjective function by construction;

2: $x \leq_{N_1} y$, then $\varphi^{\mathcal{C}}(x) \leq_{N_2} \varphi^{\mathcal{C}}(y)$: every representation we add is resuming an "hidden" relation of dependency between the pre event of a sub-bubble and its post events;

3: $x\ \mathbf{co}_{N_1}\ y$, then $\varphi^{\mathcal{C}}(x)\ \mathbf{co}_{N_2}\ \varphi^{\mathcal{C}}(y)$ or $\varphi^{\mathcal{C}}(x) = \varphi^{\mathcal{C}}(y)$: every representation we add is **co** with the other elements of its sub-bubble and both are mapped on the same condition. By this we preserve the same **co** relations;

4: $\varphi^{\mathcal{C}}(B_1) = B_2$: given by construction;

5: let $e_1 \in E_1$ and let $b_2 \in B_2$ such that $\varphi^{\mathcal{C}}(e_1) = b_2$: this item is not modified in $\varphi^{\mathcal{C}}$.

6: let $e_1 \in E_1$ and let $e_2 \in E_2$ such that $\varphi^{\mathcal{C}}(e_1) = e_2$: the pre and post events of every new condition have a pre or post condition that is mapped on the same condition of the second Net, hence $\varphi^{\mathcal{C}}({}^{\bullet}e_1) = {}^{\bullet}e_2$ and $\varphi^{\mathcal{C}}(e_1{}^{\bullet}) = e_2{}^{\bullet}$;

7: $\forall b_2 \in B_2$, take $N_1((\varphi^{\mathcal{C}})^{-1}(b_2))$, then:

7a: let $b \in \min(N_1((\varphi^{\mathcal{C}})^{-1}(b_2))), \varphi^{\mathcal{C}}({}^{\bullet}b) = {}^{\bullet}b_2$: given by construction;

7b: let $b \in N_1((\varphi^{\mathcal{C}})^{-1}(b_2)) : b \notin \max(N_1((\varphi^{\mathcal{C}})^{-1}(b_2)))$, then $\varphi^{\mathcal{C}}(b^{\bullet}) = b_2$: not modified in this new mapping;

7c: let $b \in \max(N_1((\varphi^{\mathcal{C}})^{-1}(b_2))), \varphi^{\mathcal{C}}(b^{\bullet}) = b_2{}^{\bullet}$: given by construction.

◊

3.3 Elementary Transition Systems

Using morphisms to formalize the relation between two Systems is widely used in the literature, also if the Systems are represented by Transition Systems.

We start recalling G-morphisms [31], a behaviour preserving morphism between Elementary Transition Systems. We recall then $\widehat{G}$-morphisms [38], that differ from the former asking for the surjectivity on states and transitions. This is required to interpret the morphism as a refinement of the codomain system. We define a more restrictive version of $\widehat{G}$-morphisms, called Γ-morphisms, that take in to account also the relations between states and transitions. Γ-morphisms do not allow to map pairs of dependent events into pair of independent events. Moreover, we want to relate morphisms between Elementary Net Systems with morphisms between the associated Elementary Transition Systems and vice versa, so that we are able to obtain more behavioural properties relating only structural models.

In the rest of this section, we present different notion of morphisms on Elementary Transition Systems and the properties they preserve/reflect.

3.3.1 G-morphisms

Relations between Elementary Transition Systems have been studied in [31] and can be expressed by G-morphisms that bind systems preserving their behaviour.

Definition 48. *Let $TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$.*

A G-morphism from TS_1 to TS_2 is a pair (f, g), where $f : S_1 \to S_2$, and $g : E_1 \to^* E_2$ is a partial function, such that:

1. *$f(s_0^1) = s_0^2$;*
2. *if $g(e_1)$ is undefined, then $\forall (s, e_1, s') \in T_1, f(s) = f(s')$;*
3. *if $\exists e_2 \in E_2 : g(e_1) = e_2$, then $\forall (s, e_1, s') \in T_1, \exists (f(s), e_2, f(s')) \in T_2$.*

The idea is that TS_2 is capable of ”partially simulating” TS_1 as specified by f. If the event e_1 is mapped on the event e_2, TS_2 simulate TS_1 executing this event when the first system execute e_1. The simulation is partial means that some events of TS_1 is not seen by TS_2, then if $(s, e, s') \in T_1$ and e fires in TS_1, TS_2 does not change its state: $f(s) = f(s')$. Moreover, all the occurrences of an event should be simulated in an uniform manner.

Note that the map on states determines the map on events.

Proposition 34. *Let TS_1 and TS_2 be two Elementary Transition Systems and (f, g) and (f', g') two G-morphisms from TS_1 to TS_2 such that $g = g'$.*

Then $f = f'$.

A basic property of G-morphisms is that they preserve regions in the sense that the inverse image of a region of TS_2 is a region in TS_1. The inverse image of a region r_2 of TS_2 is a pre-region (post-region) of an event e_1 iff e_1 is in the domain of g and r_2 is a pre-region (post-region) of the image of e_1.

Proposition 35. *Let $TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$ and (f, g) be a G-morphism from TS_1 to TS_2.*

If we take $r_2 \subseteq S_2$ region of TS_2, then $f^{-1}(r_2)$ is a region in TS_1.

Furthermore, for every $e_1 \in E_1, f^{-1}(r_2) \in {}^\circ e_1 (e_1{}^\circ)$ iff $\exists e_2 \in E_2, g(e_1) = e_2$ and $r_2 \in {}^\circ e_2 (e_2{}^\circ)$, respectively.

It is possible to define the composition of two G-morphisms in the usual way.

Proposition 36. *Let $TS_i = (S_i, E_i, T_i, s_0^i)$ be Elementary Transition Systems for $i = 1 \ldots 3$. Let (f_i, g_i) be a G-morphism from TS_i to TS_{i+1} for $i = 1, 2$.*

The function $(f, g) : TS_1 \to TS_3$ $(f, g) = (f_2, g_2) \circ (f_1, g_1)$ where $f = f_2 \circ f_1$ and $g = g_2 \circ g_1$ is a G-morphism.

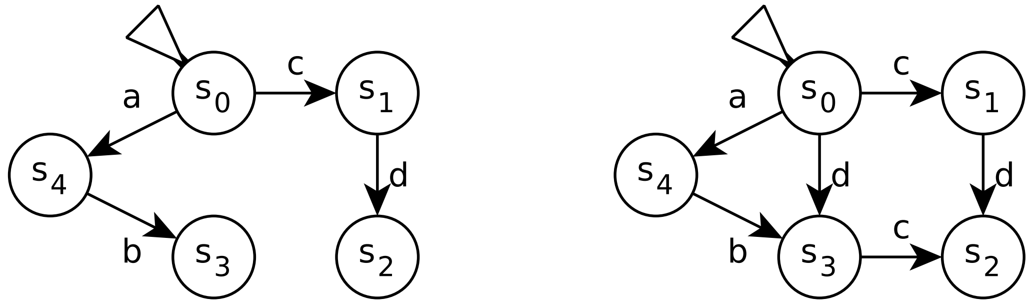
Let $\mathcal{ETS}$ denote the category whose objects are Elementary Transition Systems and whose arrows are G-morphisms. For each object $TS = (S, E, T, s_0)$ let $1_{TS} = (id_S, id_E)$ be the identity morphism where $id_S : S \to S$ and $id_E : E \to E$ are the (total) identity functions. For $(f_1, g_1) : TS_1 \to TS_2$ and $(f_2, g_2) : TS_2 \to TS_3$ take the composition of these two G-morphisms.

3.3.2 $\widehat{G}$-morphisms

In [38] has been defined a more restrictive version of G-morphism: $\widehat{G}$-morphism. These morphisms differ from the original one by the fact that they require surjectivity on states and transitions. This is required to interpret the morphism as a refinement of the codomain system.

Definition 49. *Let $TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$.*

A $\widehat{G}$-morphism from TS_1 to TS_2 is a G-morphisms (f, g), with the additional constraint that $f : S_1 \to S_2$ is surjective, and $g : E_1 \to^* E_2$ is a surjective partial function.



(a) TS_1 (b) TS_2

Figure 3.26: Two Elementary Transition Systems related by a $\widehat{G}$-morphisms

The idea is that TS_1 can be seen as a refinement of TS_2, so it has to maintain the structure of TS_2 but it should add other behaviours refining states of the system. It is very important to take in mind that this kind of morphism allows also to relax some constraints. The surjectivity (and the absence of the injectivity) of f and g assures that every state and every event of TS_2 should be splitted into more than one element in TS_1 but have to be part of the refined Elementary Transition System. Constraints 2 and 3 of Def. 48 assure that every occurrence of the same event in TS_1 have to be mapped in the same way. Nothing is said about the multiple occurrences of one event in TS_2 and this can lead to the relax of contraints between TS_1 and TS_2.

As we see in Fig. 3.26 the maps given by identical labels are a $\widehat{G}$-morphism between TS_1 and TS_2. The events c and d are present in TS_2 twice. As we see, TS_1 has more constraints than TS_2: c need to fire first than d instead in TS_2 they are independent.

It is possible to define the composition of two $\widehat{G}$-morphisms in the usual way.

Proposition 37. *Let $TS_i = (S_i, E_i, T_i, s_0^i)$ be Elementary Transition Systems for $i = 1\dots3$. Let (f_i, g_i) be a $\widehat{G}$-morphism from TS_i to TS_{i+1} for $i = 1, 2$.*

The function $(f, g) : TS_1 \to TS_3$ $(f, g) = (f_2, g_2) \circ (f_1, g_1)$ where $f = f_2 \circ f_1$ and $g = g_2 \circ g_1$ is a $\widehat{G}$-morphism.

Proof. We know that (g, f) is a G-morphism, we have to prove that it satisfies the additional constraints that characterize a $\widehat{G}$-morphism:

- $f : S_1 \to S_3$ is surjective: given by the composition of two surjective functions,

- $g : E_1 \to^* E_3$ is a surjective partial function: given by the composition of two surjective partial functions.

◇

Let $\widehat{\mathcal{ETS}}$ denote the category whose objects are Elementary Transition Systems and whose arrows are $\widehat{G}$-morphisms. For each object $TS = (S, E, T, s_0)$ let $1_{TS} = (id_S, id_E)$ be the identity morphism where $id_S : S \to S$ and $id_E : E \to E$ are the (total) identity functions. For $(f_1, g_1) : TS_1 \to TS_2$ and $(f_2, g_2) : TS_2 \to TS_3$ take the composition of these two $\widehat{G}$-morphisms.

Proposition 38. *$\widehat{\mathcal{ETS}}$ is a subcategory of $\mathcal{ETS}$.*

Proof. As required in Def. 4:

- $Ob_{\widehat{\mathcal{ETS}}} = Ob_{\mathcal{ETS}}$,
- $\forall TS_1, TS_2 \in Ob_{\widehat{\mathcal{ETS}}}, \widehat{\mathcal{ETS}}[TS_1, TS_2] \subseteq \mathcal{ETS}[TS_1, TS_2]$ because all $\widehat{G}$-morphisms are G-morphisms but the contrary does not hold,
- composition and identities in $\widehat{\mathcal{ETS}}$ are the same that the ones in $\mathcal{ETS}$.

◇

3.3.3 Γ-morphisms

$\widehat{G}$-morphisms are too much permissive relating Elementary Transition Systems. As we have seen in the previous section, they allow to remove constraints to couple of events making them independent while they are sequential in the refined system. Let us now define a more restrictive version of $\widehat{G}$-morphisms.

Definition 50. *Let $TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$.*

A Γ-morphism from TS_1 to TS_2 is a $\widehat{G}$-morphisms (f, g), with the additional constraint that $\forall (s_2, e_2, s_2') \in T_2, \exists (s_1, e_1, s_1') \in T_1$ so that $s_1 \in f_1^{-1}(s_2), e_1 \in g_1^{-1}(e_2), s_1' \in f_1^{-1}(s_2')$.

This new requirement binds multiples occurrences of one event in TS_2 with events of TS_1.

As we see in Fig. 3.27 the maps $f = \{(s_0, s_0), (s_5, s_0), (s_1, s_1), (s_6, s_1), (s_2, s_2), (s_7, s_2), (s_3, s_3), (s_8, s_3), (s_4, s_2)\}$ and g given by identical names are a Γ-morphism between TS_1 and TS_2. The event t_1 is not present in TS_1. As we see, TS_1 does not have more or less constraints than TS_2: it has only new behaviours.

The partition of the nodes of TS_1 induced by a Γ-morphism from TS_1 to TS_2 can be lifted to a graph structure: the class of nodes mapped to a node s becomes a node, while the class of events mapped to an event e becomes an event; the flow relation is defined in the obvious way.

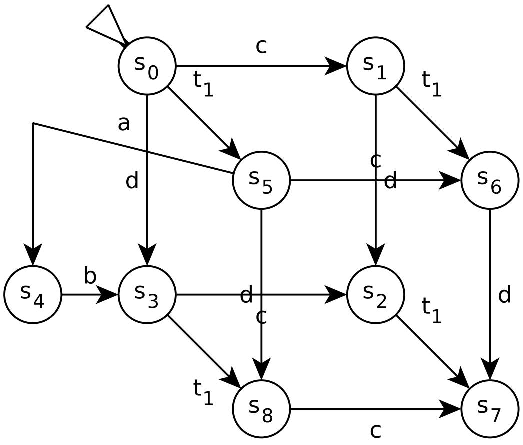


Figure 3.27: An Elementary Transition System, TS_1, related to TS_2, Fig. 3.26b, by a Γ-morphisms

Definition 51. *Let $TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$. Let (f, g) be a Γ-morphism from TS_1 to TS_2. Then f defines an equivalence relation on S_1, where the equivalence class of $s \in S_1$ is $[s] = \{s' \in S_1 | f(s') = f(s)\}$. Also g defines an equivalence relation on E_1, where the equivalence class of $e \in E_1$ is $[e] = \{e' \in E_1 | g(e') = g(e)\}$.*

The quotient *of TS_1 with respect to Γ is $TS_1/(f, g) = (S_1/f, E_1/g, T_1/(f, g), [s_0^1])$, where*

- $S_1/f = \{[s] : s \in S_1\}$,
- $E_1/g = \{[e] : e \in E_1, e \in \mathbf{dom}\ (g)\}$,
- $T_1/(f, g) = \{([s], [e], [s']) : s, s' \in S_1, e \in E_1, [s] \neq [s'], \exists (s, e, s') \in T_1\}$.

The resulting system is isomorphic to TS_2.

Proposition 39. *The quotient of TS_1, $TS_1/(f, g)$, is an Elementary Transition System isomorphic to TS_2.*

Proof. Given the surjectivity of the Γ-morphism we have that the nodes and the events of the quotient are exactly the same of TS_2.

1. Every arrow of $TS_1/(f, g)$ is present in TS_2: note that the arrow remained are not the ones between nodes of the same equivalence class and not the ones labelled by events undefined. These events lead the states they bind to one state of TS_2. So in $TS_1/(f, g)$ there are only arrows with, as labels, events mapped by g. Let us take one of these arrows: $([s], [e], [s']) \in T_1/(f, g)$ hence $(s, e, s') \in T_1$. For Def. 48 point 3 we know that $(f(s), g(e), f(s')) \in T_2$.

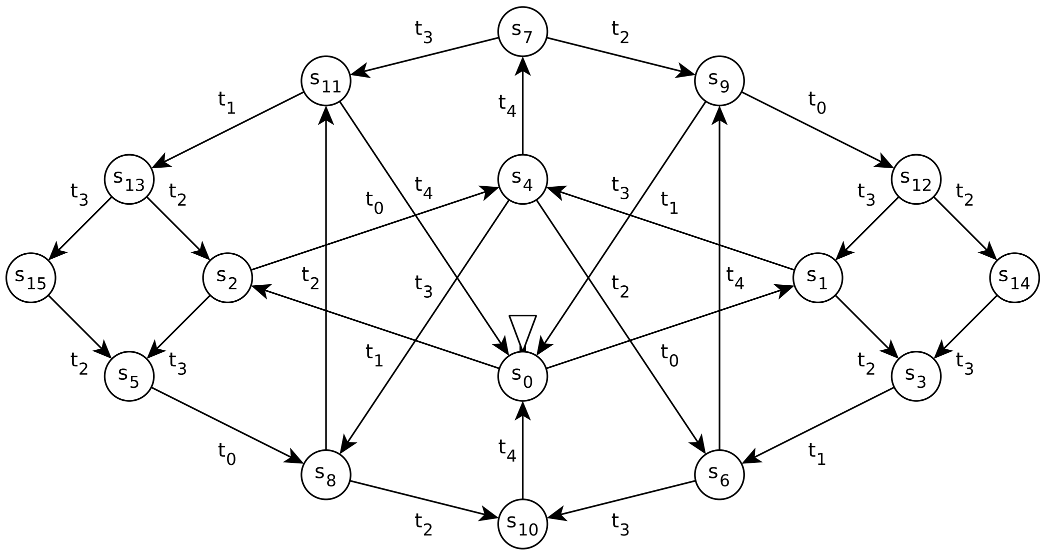


Figure 3.28: TS_1

2. Every arrow of TS_2 is present in $TS_1/(f,g)$: by definition of Γ-morphism $\forall(s_2,e_2,s_2') \in T_2, \exists(s_1,e_1,s_1') \in T_1$ so that $s_1 \in f^{-1}(s_2), e_1 \in g^{-1}(e_2), s_1' \in f^{-1}(s_2')$ hence there is $([s_1],[e_1],[s_1']) \in T_1/(f,g)$.

$\diamond$

Note that this is not given by $\widehat{G}$-morphisms and g-morphisms, and an example is shown in Fig. 3.26.

It is possible to define the composition of two Γ-morphisms in the usual way.

Proposition 40. *Let $TS_i = (S_i,E_i,T_i,s_0^i)$ be Elementary Transition Systems for $i = 1\dots3$. Let (f_i,g_i) be a Γ-morphism from TS_i to TS_{i+1} for $i = 1,2$.*

The function $(f,g) : TS_1 \to TS_3$ $(f,g) = (f_2,g_2) \circ (f_1,g_1)$ where $f = f_2 \circ f_1$ and $g = g_2 \circ g_1$ is a Γ-morphism.

Proof. We know that (g,f) is a $\widehat{G}$-morphism, we have to prove that it satisfies the additional constraints that characterize a Γ-morphism.

Let us take a $(s_3,e_3,s_3') \in T_3$ we know that $\exists(s_2,e_2,s_2') \in T_2$ so that $s_2 \in f_2^{-1}(s_3), e_2 \in g_2^{-1}(e_3), s_2' \in f_2^{-1}(s_3')$. We know also that $\exists(s_1,e_1,s_1') \in T_1$ so that $s_1 \in f_1^{-1}(s_2), e_1 \in g_1^{-1}(e_2), s_1' \in f_1^{-1}(s_2')$. So it is proved. $\diamond$

Let $\mathcal{ETS}_\Gamma$ denote the category whose objects are Elementary Transition Systems and whose arrows are Γ-morphisms. For each object $TS = (S,E,T,s_0)$ let $1_{TS} = (id_S, id_E)$ be the identity morphism where $id_S : S \to S$ and $id_E : E \to E$ are

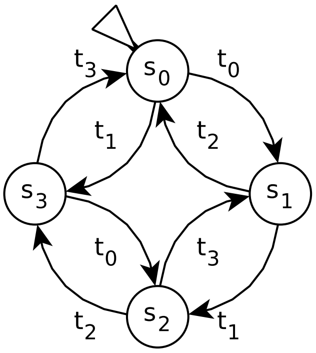


Figure 3.29: TS_2

the (total) identity functions. For $(f_1, g_1) : TS_1 \to TS_2$ and $(f_2, g_2) : TS_2 \to TS_3$ take the composition of these two Γ-morphisms.

Proposition 41. *$\mathcal{ETS}_\Gamma$ is a subcategory of $\widehat{\mathcal{ETS}}$.*

Proof. As required in Def. 4:

- $Ob_{\mathcal{ETS}_\Gamma} = Ob_{\widehat{\mathcal{ETS}}}$,

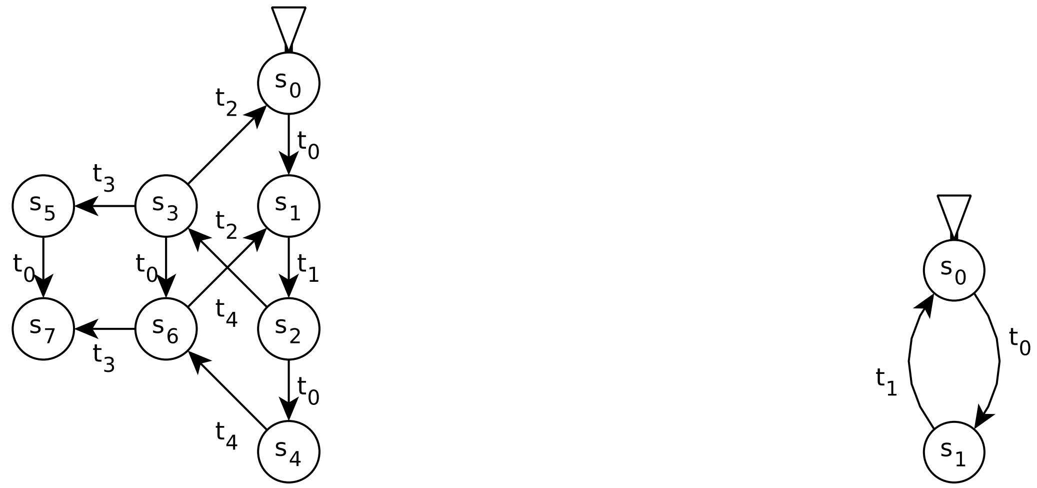
- $\forall TS_1, TS_2 \in Ob_{\mathcal{ETS}_\Gamma}, \mathcal{ETS}_\Gamma [TS_1, TS_2] \subseteq \widehat{\mathcal{ETS}} [TS_1, TS_2]$ because all Γ-morphisms are $\widehat{G}$-morphisms but the contrary does not hold,

- composition and identities in $\mathcal{ETS}_\Gamma$ are the same that the ones in $\widehat{\mathcal{ETS}}$.

$\diamondsuit$

It is although true that this new constraint does not assure that the two Elementary Transition System have exactly the same sets of concurrent events as we see, for example, in Fig. 3.28 and 3.29. The maps $f = \{(s_0, s_0), (s_1, s_1), (s_2, s_3), (s_3, s_0), (s_4, s_2), (s_5, s_0), (s_6, s_3), (s_7, s_2), (s_8, s_1), (s_9, s_3), (s_{10}, s_0), (s_{11}, s_1), (s_{12}, s_2), (s_{13}, s_2), (s_{14}, s_3), (s_{15}, s_1)\}$ and g given by identical names of events constitute a Γ-morphism between TS_1 and TS_2. For example in s_{15} there must start a concurrent square t_1, t_2.

Moreover, the refined Elementary Transition System can reach a deadlock, while the abstract one cannot, as we see in Fig. 3.30. The maps $f = \{(s_0, s_0), (s_1, s_1), (s_2, s_0), (s_3, s_0), (s_4, s_1), (s_5, s_0), (s_6, s_1), (s_7, s_1)\}$ and g given by identical names of events constitute a Γ-morphism between TS_1 and TS_2. As we see, state s_7 of TS_1 is a deadlock.



(a) TS_1 (b) TS_2

Figure 3.30: An example of Γ-morphism

3.4 Relation between the categories introduced

In this section, we relate the categories we introduced in the previous part of this chapter. We recall that N-morphisms correspond to G-morphisms. Then we prove that $\widehat{G}$-morphisms imply $\widehat{N}$-morphisms but the contrary does not hold. On the other hand, α-morphisms imply $\widehat{G}$-morphisms.

3.4.1 From Elementary Net Systems to Elementary Transition Systems

Nielsen, Rozenberg, and Thiagarajan defined in [31] a functor from $\mathcal{ENS}$ to $\mathcal{ETS}$, denoted by $\mathbf{H}$, which coincides with the computation of the case graph of a Net.

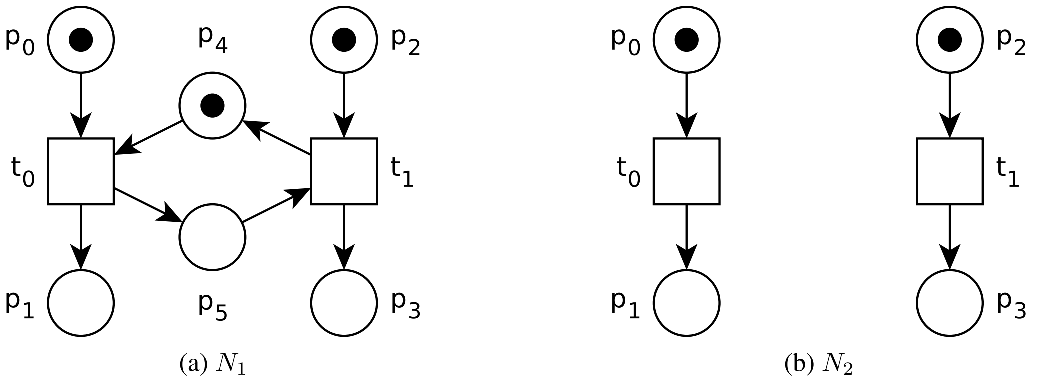
Let $N \in \mathcal{ENS}, N = (B, E, F, m_0)$ be an Elementary Net System, the *Elementary Transition System associated with* N is its reachability graph TS_N. The model obtained is an Elementary Transition System.

We have also to associate to morphisms of $\mathcal{ENS}$ morphisms of $\mathcal{ETS}$ [31].

Definition 52. *Let* $N_i \in \mathcal{ENS}, N_i = (B_i, E_i, F_i, m_0^i)$ *be an Elementary Net Systems for* $i = 1, 2$.

Let $\mathbf{H}$ *be a map which assigns to each object* N_i*, the Elementary Transition System associated with* N_i*.*

Furthermore, $\mathbf{H}$ *assigns to each arrow* $(\beta, \eta) : N_1 \to N_2$ *in* $\mathcal{ENS}$ *the pair* (f_β, η)*, where* $f_\beta : [m_0^1\rangle \to [m_0^2\rangle$*, given by* $\forall m_1 \in [m_0^1\rangle, f_\beta(m_1) = \beta(m_1) \cup (m_0^2 - \beta(m_0^1))$.



(a) N_1 (b) N_2

Figure 3.31: An example of $\widehat{N}$-morphism

Note that f_β defined above is the same that the function defined in Prop. 3. The map obtained by $\mathbf{H}$ on an N-morphism is a G-morphism [31].

Proposition 42. *Let $N_i \in \mathcal{ENS}$, $N_i = (B_i, E_i, F_i, m_0^i)$ be an Elementary Net Systems for $i = 1, 2$ and let (β, η) be an N-morphism from N_1 to N_2.*

The map (f_β, η), constructed as specified in Definition 52, is a G-morphism from $\mathbf{H}(N_1)$ to $\mathbf{H}(N_2)$.

$\mathbf{H} : \mathcal{ENS} \to \mathcal{ETS}$ is a functor.

Let us show that the functor $\mathbf{H}$ does not necessarily map an $\widehat{N}$-morphism to a $\widehat{G}$-morphism. For example, in Fig. 3.31 and Fig. 3.32 we see two Elementary Net Systems (the $\widehat{N}$-morphism relates elements with the same label) and their reachability graphs: no state of TS_1 can be mapped on s_2.

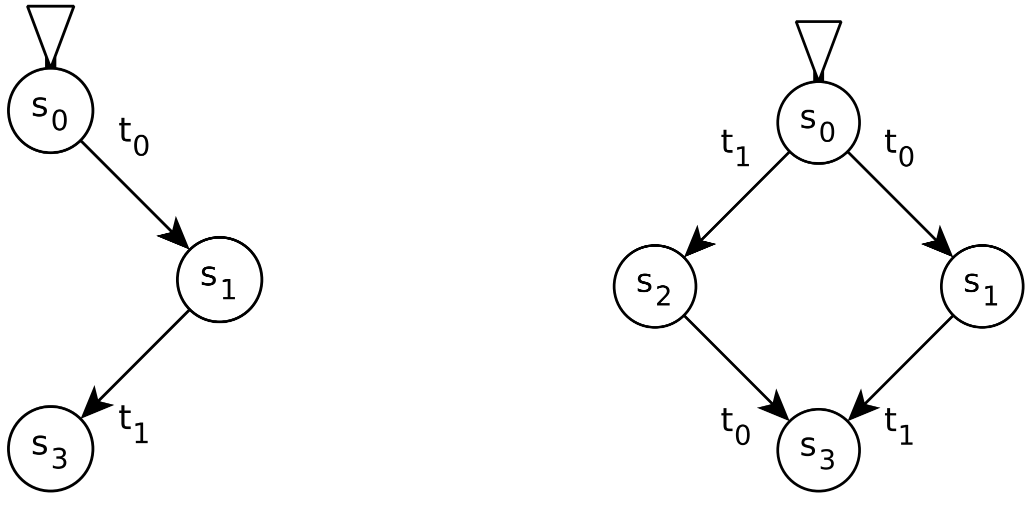
Let us show that the functor $\mathbf{H}$ does not necessarily map a Π-morphism to a $\widehat{G}$-morphism. For example, take the Elementary Net System of Fig. 3.33a and the one of Fig. 3.31b. The map $\beta = \{(p_0, p_0), (p_1, p_1), (p_8, p_2), (p_9, p_3)\}$ and the map $\eta = \{(t_0, t_0), (t_2, t_1)\}$ constitute a Π-morphism between N_1 and N_2. In Fig. 3.33b and 3.32b we see the reachability graphs associated with Elementary Net Systems mentioned before. The functor create the map $f = \{(s_0, s_0), (s_1, s_2), (s_2, s_2), (s_3, s_3)\}$. As we see, (f, η) does not constitute a $\widehat{G}$-morphism between TS_1 and TS_2.

We have to associate to φ-morphism morphisms of $\mathcal{ETS}$.

Definition 53. *Let $N_i \in \mathcal{ENS}_\alpha$, $N_i = (B_i, E_i, F_i, m_0^i)$ be an Elementary Net Systems for $i = 1, 2$.*

Let $\mathbf{H}$ be a map which assigns to each object N_i its reachability graph.

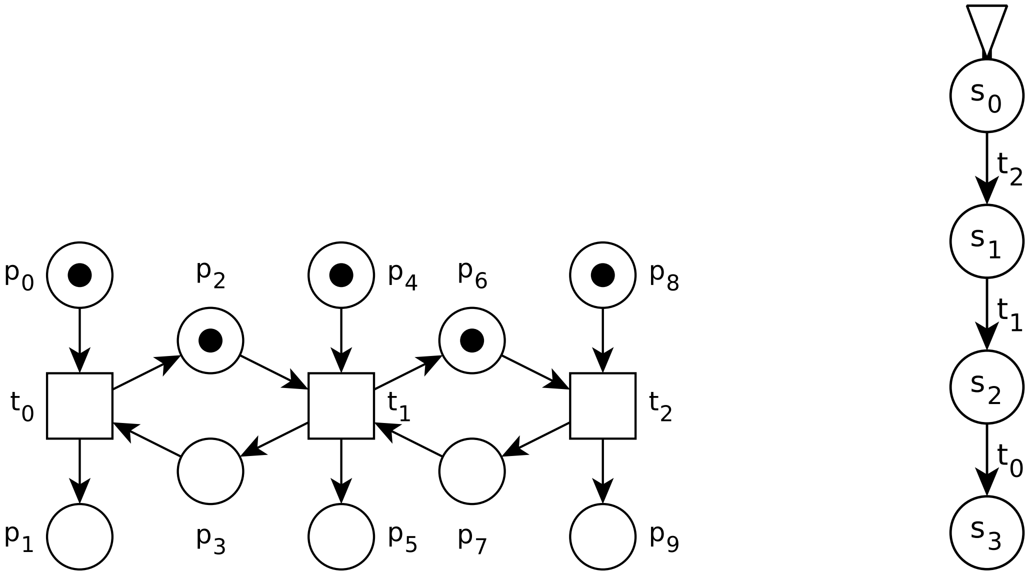
Furthermore, $\mathbf{H}$ assigns to each arrow $\varphi : N_1 \to N_2$ in $\mathcal{ENS}_\alpha$ the pair (f_φ, g_φ), where $f_\varphi : [m_0^1\rangle \to [m_0^2\rangle$ given by $\forall m_1 \in [m_0^1\rangle, f_\varphi(m_1) = \varphi(m_1) \cap B_2$ and $g_\varphi : E_1 \to^* E_2$ given by $\forall e_1 \in E_1 s.t. \varphi(e_1) \in E_2, g_\varphi(e_1) = \varphi(e_1)$.



(a) TS_1

(b) TS_2

Figure 3.32: The reachability graphs of Elementary Net Systems of Fig. 3.31



(a) N_1

(b) TS_1

Figure 3.33: An Elementary Net System and its reachability graph

The map obtained by **H** on a φ-morphism is a $\widehat{G}$-morphism.

Proposition 43. *Let $N_i \in \mathcal{ENS}_\alpha, N_i = (B_i, E_i, F_i, m_0^i)$ be an Elementary Net Systems for $i = 1, 2$ and let φ be a φ-morphism from N_1 to N_2.*

The map (f_φ, g_φ), constructed as specified in Definition 53, is a $\widehat{G}$-morphism from $\mathbf{H}(N_1)$ *to* $\mathbf{H}(N_2)$*.*

Proof. To prove the thesis we have to argue that all the condition of a $\widehat{G}$-morphism are satisfied. We know that a φ-morphism is an $\widehat{N}$-morphism, which is an N-morphism. As we have seen before, (f_φ, g_φ) is a G-morphism, so we need to prove only the additional requirements of a $\widehat{G}$-morphism.

The functions $f_\varphi : S_1 \to S_2$ and $g_\varphi : E_1 \to^* E_2$ are surjective by definition. ◇

The map $\mathbf{H} : \mathcal{ENS}_\alpha \to \widehat{\mathcal{ETS}}$ is a functor since it is immediate to see that it preserve composition and identity.

3.4.2 From Elementary Transition Systems to Elementary Net Systems

Nielsen, Rozenberg, and Thiagarajan defined in [31] a functor from $\mathcal{ETS}$ to $\mathcal{ENS}$, denoted by **J**, that gives a procedure of synthesis which, given an Elementary Transition System, builds an Elementary Net System whose case graph is isomorphic to the Transition System.

We have to associate to every object of $\mathcal{ETS}$ objects of $\mathcal{ENS}$ [31].

Definition 54. *Let $TS \in \mathcal{ETS}, TS = (S, E, T, s_0)$ be an Elementary Transition System.*

The Elementary Net System associated with TS *is defined as* $N_{TS} = (R_{TS}, E, F_{TS}, R_{s_0})$ *where* $F_{TS_i} = \{(r, e) | r \in R_{TS_i} \wedge e \in E \wedge r \in {}^\circ e\} \cup \{(e, r) | r \in R_{TS_i} \wedge e \in E \wedge r \in e^\circ\}$.

The model obtained is an Elementary Net System saturated and, hence, contact-free.

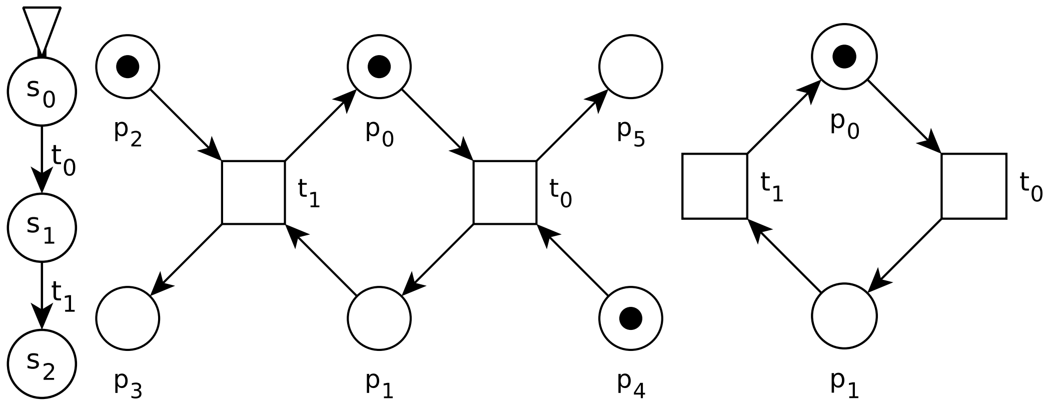
We have also to associate to morphisms of $\mathcal{ETS}$ morphisms of $\mathcal{ENS}$ [31].

Definition 55. *Let $TS_i \in \mathcal{ETS}, TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$.*

Let **J** *be a map which assigns to each object TS_i the Elementary Net System associated with TS_i.*

Furthermore, **J** *assigns to each arrow $(f, g) : TS_1 \to TS_2$ in $\mathcal{ETS}$ the pair (β, g), where $\beta \subseteq R_{TS_1} \times R_{TS_2}$, given by $(r_1, r_2) \in \beta \Leftrightarrow f^{-1}(r_2) = r_1$*

The map obtained by **J** on a G-morphism is an N-morphism.



(a) TS_1 (b) N_1 (c) N_2

Figure 3.34: An Elementary Transition System, two Elementary Net Systems: one associated to it and one to the System of Fig. 3.30b

Proposition 44. *Let $TS_i \in \mathcal{ETS}$, $TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$ and let (f, g) be a G-morphism from TS_1 to TS_2.*

The map (β, g), constructed as specified in Definition 55, is an N-morphism from $\mathbf{J}(TS_1)$ to $\mathbf{J}(TS_2)$.

$\mathbf{J} : \mathcal{ETS} \to \mathcal{ENS}$ is a functor.

We construct now a functor from $\widehat{\mathcal{ETS}}$ to $\widehat{\mathcal{ENS}}$ using the map specified in Definition 55.

The map obtained by $\mathbf{J}$ on a $\widehat{G}$-morphism is an $\widehat{N}$-morphism.

Proposition 45. *Let $TS_i \in \widehat{\mathcal{ETS}}$, $TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$ and let (f, g) be a $\widehat{G}$-morphism from TS_1 to TS_2.*

The map (β, g), constructed as specified in Definition 55, is an $\widehat{N}$-morphism from $\mathbf{J}(TS_1)$ to $\mathbf{J}(TS_2)$.

Proof. To prove the thesis we have to argue that all the condition of an $\widehat{N}$-morphism are satisfied. Nielsen, Rozenberg, and Thiagarajan proved that $(\beta, g) = J((f, g))$ is an N-morphism from $J(TS_1)$ to $J(TS_2)$, so we need to prove only the additional requirements of an $\widehat{N}$-morphism.

The function $g : E_1 \to^* E_2$ is surjective by definition.

By definition $\beta \subseteq R_{TS_1} \times R_{TS_2}$ and $(r_1, r_2) \in \beta$ iff $f^{-1}(r_2) = r_1$, hence β^{-1} is a function. The fact that f is surjective assure that f^{-1} exists $\forall r_2 \in R_{TS_2}$, hence β^{-1} is total. We have to prove injectivity. By contradiction, let $r_2, r_2' \in R_{TS_2}, r_2 \neq r_2'$, and let $r_1 \in R_{TS_1}$ such that $\beta^{-1}(r_2) = f^{-1}(r_2) = r_1 = f^{-1}(r_2') = \beta^{-1}(r_2')$. Assume that $\exists s_2 \in r_2 \setminus r_2'$. Since f is surjective, $\exists s_1 \in S_1 | f^{-1}(s_2) = s_1$. We know also that $s_1 \in f^{-1}(r_2) = r_1 = f^{-1}(r_2')$. Since f is total $\exists s_2' \in r_2' | f(s_1) = s_2'$ and this is a contradiction because function f cannot assign to s_1 both s_2 and s_2'.

For the case $\exists s_2 \in r_2' \setminus r_2$ the prove is similar. $\diamondsuit$

The map $\mathbf{J} : \widehat{\mathcal{ETS}} \to \widehat{\mathcal{ENS}}$ is a functor given that it is immediate to see that it preserves composition and identity.

Since $\mathcal{ETS}_\Gamma$ is a subcategory of $\widehat{\mathcal{ETS}}$, the previously defined functor $\mathbf{J}$ binds also $\mathcal{ETS}_\Gamma$ with $\widehat{\mathcal{ENS}}$.

Let us show that the functor $\mathbf{J}$ does not assure that, if there is a Γ-morphism between two Elementary Transition Systems, there is a Π-morphism between the Elementary Net Systems associated with them. For example, take the Elementary Transition System of Fig. 3.34a and the one of Fig. 3.30b. The map $f = \{(s_0, s_0), (s_1, s_1), (s_2, s_0)\}$ and the map given by identical names of events constitute a Γ-morphism between the two. In Fig. 3.34b and 3.34c we see the Elementary Net Systems associated with the Elementary Transition Systems mentioned before. $\mathbf{J}$ create the map $\beta = \{(p_1, p_1), (p_0, p_0)\}$. As we see, (β, g) do not constitute a Π-morphism between N_1 and N_2.

Chapter 4

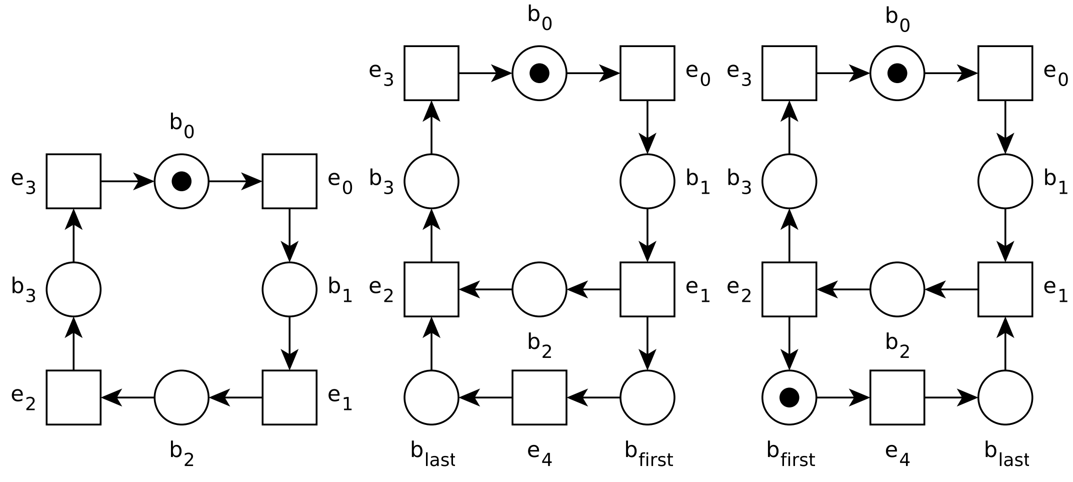
Nets transformations and morphisms

The results and notions presented in the previous chapter are a theoretical basis supporting methods for modular development. From a practical viewpoint, a designer prefer to use a set of Net transformations in order to refine a Net. In this chapter, starting from $\widehat{N}$-morphism, we will try to define such transformation instead of constraining the morphism. Formally, refining a Net with these transformation, there will be an $\widehat{N}$-morphism from the refined Net to the abstract one and a Γ-morphism between the corresponding reachability graphs.

Here we present two examples of such transformations as a first step in this direction. Esparza and Silva in [17] defined three kinds of structures in Place Transition Nets and they proved results on desirable properties by using these structures. The first refinement we present is based on one of them, called handle, and consists in adding to the Net a path refining a single condition relating two events. The second one is a live Net synchronized on one event of the original net.

Definition 56. *Let $N_1 = (B_1, E_1, F_1, m_0^1)$ be an Elementary Net System. Let us take two events e_1, e_1' in N_1 such that there exist a condition b_1 connecting the two events: $b_1 \in e_1{}^\bullet \wedge b_1 \in {}^\bullet e_1'$. Condition b_1 is connected only to e_1 and e_1'.*

A handle *of N_1 is an Elementary Net System $N_h = (B_h, E_h, F_h, m_0^h)$, with $E_h \cap E_1 = \{e_1, e_1'\}$ and $B_h \cap B_1 = \emptyset$, consisting of a directed path, containing at least one event different from e_1 with e_1', connecting e_1 with e_1'. If the path is in the same direction of the connection in N_1 and b_1 is (not) marked one (no) condition of the handle has to be marked. If the path is in the opposite direction of the connection in N_1 and b_1 is (not) marked no (one) condition of the handle has to be marked.*



(a) N_1 (b) N_2 (c) N_3

Figure 4.1: A Net N_1, the net N_2 obtained by adding in N_1 a handle between e_1 and e_2 in the same direction of b_2 and the net N_3 obtained by adding in N_1 a handle between e_1 and e_2 in the opposite direction of b_2

We can see examples of handle in Fig. 4.1 and 4.2.

Let us call b_{first} the first condition of the handle and b_{last} the last one. We start showing some properties on the marking of the handle. Note that the handle is a path that contains only one token. If there is a path from the event e_1 (e_1') to e_1' (e_1) through b_1 and the handle start in e_1 (e_1') and ends in e_1' (e_1) we will say that the handle is directed as b_1.

Lemma 4. *Let $N_1 = (B_1, E_1, F_1, m_0^1)$ be an Elementary Net System. Let N_h be a handle directed as b_1. Let $N_2 = (B_2, E_2, F_2, m_0^2)$ be the net constructed by synchronizing N_1 and N_h on the two common events e_1 and e_1': $N_2 = (B_1 \cup B_h, E_1 \cup E_h, F_1 \cup F_h, m_0^1 \cup m_0^h)$.*

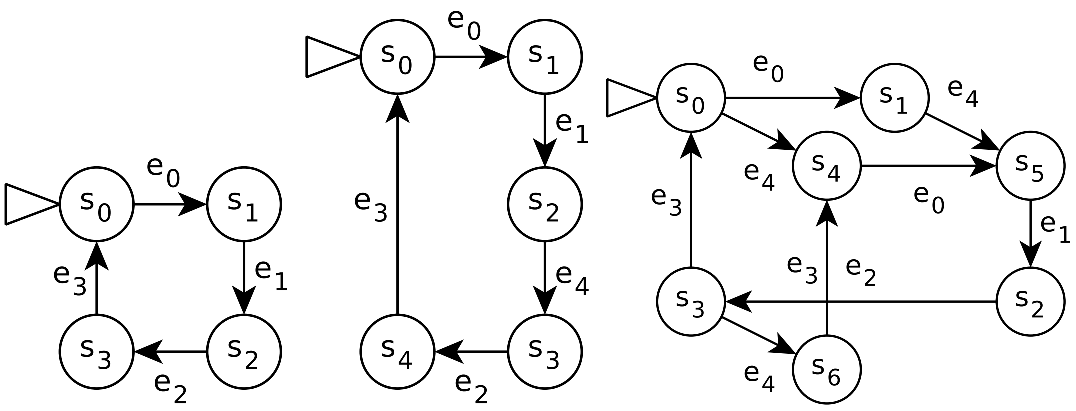
For all $m_2 \in [m_0^2\rangle$, the following holds: $m \cap B_h \neq \varnothing$ if, and only if, $b_1 \in m_2$ and, in that case, $|m \cap B_h| = 1$.

Proof. b_1 is marked in the initial condition iff one condition of the handle is marked.

b_1 becomes un-marked only when e_1' fires, and e_1' consumes a token also from b_{last}, hence all the conditions of the handle are un-marked after that firing.

b_1 becomes marked only when e_1 fires, and e_1 produces a token also in b_{first}, hence one condition of the handle is marked after that firing. ◇

Lemma 5. *Let $N_1 = (B_1, E_1, F_1, m_0^1)$ be an Elementary Net System. Let N_h be a handle not directed as b_1. Let $N_2 = (B_2, E_2, F_2, m_0^2)$ be the net constructed*



(a) **H** (N_1) (b) **H** (N_2) (c) **H** (N_3)

Figure 4.2: Reachability Graphs of Nets of Fig. 4.1

by synchronizing N_1 and N_h on the two common events e_1 and e'_1: $N_2 = (B_1 \cup B_h, E_1 \cup E_h, F_1 \cup F_h, m_0^1 \cup m_0^h)$.

For all $m_2 \in [m_0^2\rangle$, the following holds: $m \cap B_h \neq \emptyset$ if, and only if, $b_1 \notin m_2$ and, in that case, $|m \cap B_h| = 1$.

Proof. b_1 is marked in the initial condition iff all conditions of the handle are not marked,

b_1 becomes un-marked only when e'_1 fires, and e'_1 produces a token also in b_{first}, hence one condition of the handle is marked after that firing.

b_1 becomes marked only when e_1 fires, and e_1 consumes a token also from b_{last}, hence all the conditions of the handle are un-marked after that firing. ◇

Now we prove that from a Net enriched with a handle to the original Net there is an $\widehat{N}$-morphism.

Theorem 3. *Let $N_1 = (B_1, E_1, F_1, m_0^1)$ be an Elementary Net System. Let $N_2 = (B_2, E_2, F_2, m_0^2)$ be the net constructed by synchronizing N_1 and a handle N_h on the two common events e_1 and e'_1: $N_2 = (B_1 \cup B_h, E_1 \cup E_h, F_1 \cup F_h, m_0^1 \cup m_0^h)$.*

The pair of functions (β, η) given by the identity functions from N_2 to N_1, restricted to the nodes of N_1, is an $\widehat{N}$-morphism from N_2 to N_1.

Proof. We have to prove all the constraints of $\widehat{N}$-morphisms (see Def. 30 and 31):

31.1: β^{-1} is total injective since β is the identity function and $B_1 \subseteq B_2$,

31.2: η is a partial surjective function because all events of N_1 are in N_2,

30.3: given that β is the identity function and that new conditions which are marked in the initial state are not in the domain of β, we have

$$\forall(b_2, b_1) \in \beta : b_2 \in m_0^2 \Leftrightarrow b_1 \in m_0^1$$

30.4: take an event e_2 such that $\eta(e_2)$ is undefined. This implies that e_2 is in the handle, and all the handle (but for e_1 and e_1') is not mapped, hence also the pre and the post of e_2 are not mapped,

30.5: take an event of N_2 in the domain of η. This event is not in the handle, hence it is present also in N_1. For all the events but e_1, e_1' the proof that the neighbourhood is preserved is trivial.

Events e_1 and e_1' have one new neighbour in N_2, but these conditions are not mapped by β so the neighbourhood is preserved also for e_1 and e_1'.

◇

The following is one of the major results of this chapter: from the reachability graph of the Net enriched with a handle to the reachability graph of the original Net there is a Γ-morphism. To show this fact, we will use the functor **H**, as defined in Def. 52. This shows that this transformation consistently reflects on the behaviour of the Net.

Theorem 4. *Let $N_1 = (B_1, E_1, F_1, m_0^1)$ be an Elementary Net System. Let $N_2 = (B_2, E_2, F_2, m_0^2)$ be the net constructed synchronizing N_1 and a handle N_h on the two common events e_1 and e_1': $N_2 = (B_1 \cup B_h, E_1 \cup E_h, F_1 \cup F_h, m_0^1 \cup m_0^h)$.*

The pair of functions $\mathbf{H}(\beta, \eta)$, with (β, η) given by the identity functions between N_2 and N_1 restricted to the nodes of N_1, is a Γ-morphism from $\mathbf{H}(N_2)$ to $\mathbf{H}(N_1)$.

Proof. We know by Theorem 3 that (β, η) is an $\widehat{N}$-morphism from N_2 to N_1. Hence we know that there is a G-morphism between $\mathbf{H}(N_2)$ and $\mathbf{H}(N_1)$, so we need first to prove the additional constraints of $\widehat{G}$-morphisms:

- it can be proved by induction on the reachable states that $f_\beta : [m_0^2\rangle \to [m_0^1\rangle$ is a surjective total function,
- $\eta : E_2 \to^* E_1$ is a surjective partial function by construction.

Now we need to prove only the additional constraint of Γ-morphisms. We have to prove that each arrow in N_1 has a corresponding arrow in N_2. Let us take $s_1 \in [s_0^1\rangle$. We know that there exists a set of states in $\mathbf{H}(N_2)$ that are mapped on s_1. Now, take an event $e \in E_1$ such that $(s_1, e, s_1') \in T_1$.

There are three possibilities:

- $e \neq e_1, e_1'$: we know that there is an arrow (s_2, e, s_2') such that $f_\beta(s_2) = s_1$ and $f_\beta(s_2') = s_1'$ given that we have not changed the neighbourhood of e in N_2,
- $e = e_1$: hence $b_1 \notin s_1$. Hence no (one) condition of the handle is marked in s_1. Hence there is an arrow labelled with the event e_1 (after some other arrows labelled with events of the handle, there is an arrow labelled with the event e_1) that leads to a state s_2' containing b_1 and b_{first} (not containing b_{last}). Hence, s_2' is related to s_1',
- $e = e_1'$: hence $b_1 \in s_1$. Hence one (no) condition of the handle is marked in s_1. Hence, after some other arrows labelled with events of the handle, there is an arrow labelled with the event e_1' (there is an arrow labelled with the event e_1') that leads to a state s_2' not containing b_1 and b_{last} (containing b_{first}). Hence, s_2' is related to s_1';

◇

Let us now define the second transformation.

Definition 57. *Let $N_1 = (B_1, E_1, F_1, m_0^1)$ be an Elementary Net System. Let us take one event e_1 in N_1.*

An aquarium *of N_1 is a live Elementary Net System $N_a = (B_a, E_a, F_a, m_0^a)$, with $E_a \cap E_1 = \{e_1\}$ and $B_a \cap B_1 = \varnothing$.*

We can see an example of aquarium in Fig. 4.3.

Now we prove that from a Net enriched with an aquarium to the original Net there is an $\widehat{N}$-morphism.

Theorem 5. *Let $N_1 = (B_1, E_1, F_1, m_0^1)$ be an Elementary Net System. Let $N_2 = (B_2, E_2, F_2, m_0^2)$ be the net constructed by synchronizing N_1 and an aquarium N_a on the common event e_1: $N_2 = (B_1 \cup B_a, E_1 \cup E_a, F_1 \cup F_a, m_0^1 \cup m_0^a)$.*

The pair of functions (β, η) given by the identity functions from N_2 to N_1, restricted to the nodes of N_1, is an $\widehat{N}$-morphism from N_2 to N_1.

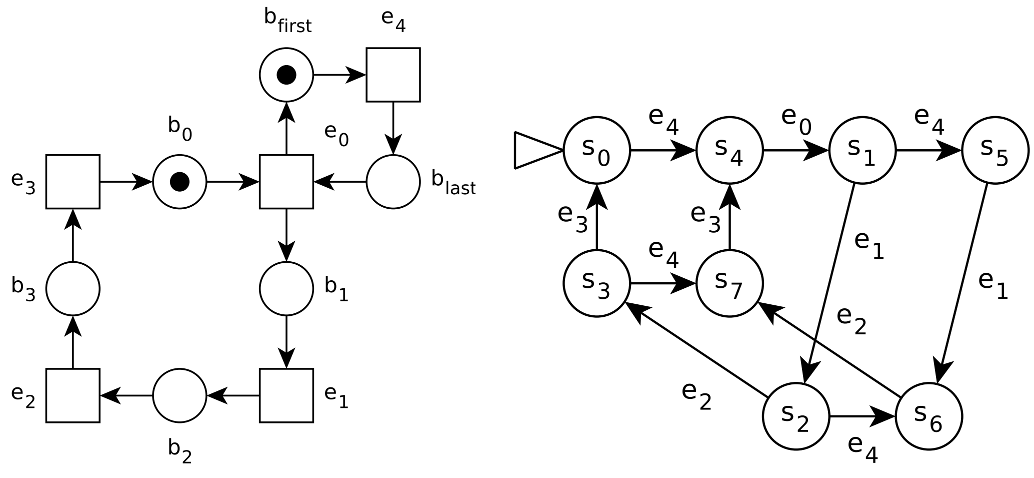
Proof. We have to prove all the constraints of $\widehat{N}$-morphisms:

31.1: β^{-1} is total injective since β is the identity function and $B_1 \subseteq B_2$,

31.2: η is a partial surjective function because all events of N_1 are in N_2,

30.3: given that β is the identity function and that new conditions which are marked in the initial state are not in the domain of β, we have

$$\forall (b_2, b_1) \in \beta : b_2 \in m_0^2 \Leftrightarrow b_1 \in m_0^1$$



(a) N_4 (b) $\mathbf{H}(N_4)$

Figure 4.3: The net N_4 obtained by adding in N_1 of Fig. 4.1a an aquarium on e_0 (note that it is also a loop) and its Reachability Graph

30.4: take an event e_2 such that $\eta(e_2)$ is undefined. This implies that e_2 is in the aquarium, and all the aquarium (but for e_1) is not mapped, hence also the pre and the post of e_2 are not mapped,

30.5: take an event of N_2 in the domain of η. This event is not in the aquarium, hence it is present also in N_1. For all the events but e_1 the proof that the neighbourhood is preserved is trivial.

Events e_1 have new neighbours in N_2, but these conditions are not mapped by β so the neighbourhood is preserved also for e_1 and e_1'.

◇

The following is another results of this chapter: from the reachability graph of the Net enriched with an aquarium to the reachability graph of the original Net there is a Γ-morphism.

Theorem 6. *Let* $N_1 = (B_1, E_1, F_1, m_0^1)$ *be an Elementary Net System. Let* $N_2 = (B_2, E_2, F_2, m_0^2)$ *be the net constructed synchronizing* N_1 *and an aquarium* N_a *on the common event* e_1*:* $N_2 = (B_1 \cup B_a, E_1 \cup E_a, F_1 \cup F_a, m_0^1 \cup m_0^a)$.

The pair of functions $\mathbf{H}(\beta, \eta)$*, with* (β, η) *given by the identity functions between* N_2 *and* N_1 *restricted to the nodes of* N_1*, is a* Γ*-morphism from* $\mathbf{H}(N_2)$ *to* $\mathbf{H}(N_1)$.

Proof. We know by Theorem 5 that (β, η) is an $\widehat{N}$-morphism from N_2 to N_1. Hence we know that there is a G-morphism between $\mathbf{H}(N_2)$ and $\mathbf{H}(N_1)$, so we need first to prove the additional constraints of $\widehat{G}$-morphisms:

- it can be proved by induction on the reachable states that $f_\beta : [m_0^2\rangle \rightarrow [m_0^1\rangle$ is a surjective total function,
- $\eta : E_2 \rightarrow^* E_1$ is a surjective partial function by construction,

Now we need to prove only the additional constraint of Γ-morphisms. We have to prove that each arrow in N_1 has a corresponding arrow in N_2. Let us take $s_1 \in [s_0^1\rangle$. We know that there exists a set of states in **H** (N_2) that are mapped on s_1. Now, take an event $e \in E_1$ such that $(s_1, e, s_1') \in T_1$.

There are two possibilities:

- $e \neq e_1, e_1'$: we know that there is an arrow (s_2, e, s_2') such that $f_\beta(s_2) = s_1$ and $f_\beta(s_2') = s_1'$ given that we have not changed the neighbourhood of e in N_2,
- $e = e_1$: we know by the liveness of the aquarium that there are a set of arrows that leads to a state s_2 (still mapped on s_1) in which start an arrow labelled with the event e_1. It lead to a state s_2' that contains the post conditions of e_1 in N_1 plus the ones of the aquarium, hence it is mapped on s_1'.

$\diamondsuit$

The results of this section form a basis upon which one can construct a set of Net transformations to be used by a designer. The final aim along this line of research is to define a complete collection of Net transformations which guarantee the existence of a Γ-morphism from the refined Net to the abstract one.

Chapter 5

Composition

In the development of distributed systems a central role is played by formal tools supporting various aspects of modularity such as compositionality, refinement and abstraction. Several formal approaches are available. One of the main challenges consists in developing languages and methods allowing to derive properties of the refined or composed system from properties of the components. There is a lot of interest in how to combine models because it makes the analysis of models simpler and more structured.

Following the approach proposed in [38] and in [3], the basic idea consists in composing two different refinements of a common abstract view, obtaining a new model which describes the system comprising the details of both operands, while complying to the same abstract view.

The rules for identifying elements of the models being composed are expressed by means of morphisms towards another model, called interface. The interface can be seen as an abstraction of the whole system, shared by the components or, alternatively, it can be interpreted as the specification of the communication protocol. In this case, each operand can be seen as made of the actual, local, component, and of an interface to the rest of the system. The composed system is made by local parts corresponding to each component and a global part corresponding to the interaction between the components. The composed system results to be related to both the components and the interface by means of morphisms, and the resulting diagram is commutative.

The use of products in a suitable category of Nets as a way to model composition by synchronization has been studied by several authors. One of this works, similar to ours, proposed by Fabre [18], applies to Safe Nets and is built on the notion of pullback.

A survey paper, [34], describes a way to compose Nets using morphisms and pushouts. There, the emphasis is on refinement rules that preserve specific behavioural properties, within the wider context of general transformation rules on Nets.

Winskel introduced a new kind of morphism in [45] and defined its composition using products in the corresponding category.

The chapter is structured as follows. We start considering systems modelled by Elementary Net Systems, then we skip to Occurrence Nets and to Elementary Transition Systems.

5.1 Elementary Net Systems

5.1.1 $\widehat{N}$-morphisms

We recall an operation of composition defined by Pomello and Bernardinello in [38]. The starting point is a set of three Elementary Net Systems; one of them, N_I, plays the role of an interface between the other two, N_1 and N_2. The composition is driven by a pair of $\widehat{N}$-morphisms, (β_1, η_1) and (β_2, η_2), respectively from N_1 to N_I, and from N_2 to N_I. We can see N_I also as the protocol of the interaction between them. In that sense, it is important that the morphisms are surjective, because each system has to respect the protocol entirely. The composition of these two systems is given by the union of a local part of each system and a common part corresponding to the protocol. All the definitions and results of this section are taken from [38].

Definition 58. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be an Elementary Net System for $i = 1, 2$, $N_I = (B_I, E_I, F_I, m_0^I)$ be an Elementary Net System and let $(\beta, \eta) : N_i \to N_I$ be an $\widehat{N}$-morphism. Let D_i denote the domain of the binary relation β_i, $D_i = \{b \in B_i | \beta_i(b) \neq \varnothing\}$, and G_i denote the domain of the partial function η_i, $G_i = \mathbf{dom}\ (\eta_i)$.*

We define $N_1\langle N_I\rangle N_2 = N = (B, E, F, m_0)$ as follows:

1. *$B = (B_1 \setminus D_1) \cup (B_2 \setminus D_2) \cup B_I$,*

2. *$E = (E_1 \setminus G_1) \cup (E_2 \setminus G_2) \cup E_{sync}$,*
   where $E_{sync} = \{\langle e_1, e_2\rangle | e_1 \in G_1, e_2 \in G_2, \eta_1(e_1) = \eta_2(e_2)\}$,

3. *F is defined by the following clauses:*

   (a) $\forall b \in (B_i \setminus D_i), \forall e \in (E_i \setminus G_i), i = 1, 2$ we have

$$(b, e) \in F \Leftrightarrow (b, e) \in F_i$$

$$(e, b) \in F \Leftrightarrow (e, b) \in F_i$$

(b) $\forall b \in (B_i \setminus D_i), \forall e \in G_i, \forall e_j \in G_{3-i}$ *and* $e_s = \langle e, e_j \rangle$ *if* $i = 1$ *or* $e_s = \langle e_j, e \rangle$ *if* $i = 2$ *we have*

$$(b, e_s) \in F \Leftrightarrow e_s \in E, (b, e) \in F_i$$

$$(e_s, b) \in F \Leftrightarrow e_s \in E, (e, b) \in F_i$$

(c) $\forall b \in B_I, \forall e = \langle e_1, e_2 \rangle \in E_{sync}$ *we have*

$$(b, e) \in F \Leftrightarrow (\beta_1^{-1}(b), e_1) \in F_1, (\beta_2^{-1}(b), e_2) \in F_2$$

$$(e, b) \in F \Leftrightarrow (e_1, \beta_1^{-1}(b)) \in F_1, (e_2, \beta_2^{-1}(b)) \in F_2$$

4. $m_0 = (m_0^1 \setminus D_1) \cup (m_0^2 \setminus D_2) \cup m_0^I$.

From this construction it follows immediately that $N = N_1 \langle N_I \rangle N_2$ *as defined above is an Elementary Net Systems. Moreover, the Net system N maps onto* N_1 *and* N_2.

The idea that guides this composition is that the morphisms identify the conditions of the interface in each component. Therefore, the events that modify each local copy of a common condition must be synchronized. If one of these conditions changes its state, it is because one of the neighbouring events is fired. These events must be given by the synchronisation of corresponding local events. Hence, the composed Net is given by the local conditions and events of the two components plus the conditions of the interface and the synchronized events.

The following statement define the natural relations between the composed Net and its components.

Definition 59. *Define the pair* (β_i', η_i')*, with* $\beta_i' \subseteq B \times B_i$ *and* $\eta_i' : E \to E_i$ *as follows:*

- $\beta_i' = \{(b, b) | b \in B_i \setminus D_i\} \cup \{(b, \beta_i^{-1}(b)) | b \in B_I\}$,
- $\forall e \in E_1 \setminus G_1 : \eta_1'(e) = e, \eta_2'(e) =$ *undefined,*
- $\forall e \in E_2 \setminus G_2 : \eta_1'(e) =$ *undefined*$, \eta_2'(e) = e,$
- $\forall \langle e_1, e_2 \rangle \in E : \eta_i'(\langle e_1, e_2 \rangle) = e_i.$

As shown in [38], the diagram formed by the $\widehat{N}$-morphisms between the interface, the two components, and the composed Net commutes.

Theorem 7. *The pair (β'_i, η'_i) is an $\widehat{N}$-morphism from $N = N_1\langle N_I\rangle N_2$ to $N_i, i = 1, 2$ and the following diagram commutes.*

$$\begin{tikzcd}
& N_I & \\
N_1 \arrow[ur, "\beta_1{,}\eta_1"] & & N_2 \arrow[ul, "\beta_2{,}\eta_2"'] \\
& N \arrow[ul, "\beta'_1{,}\eta'_1"] \arrow[ur, "\beta'_2{,}\eta'_2"'] &
\end{tikzcd}$$

From the previous commutative diagram and from Prop. 5 it follows that N contains N_1, N_2 and N_I as subnets, possibly with some elements duplicated. However, as discussed in [3], the operation is not a pullback in $\mathcal{ENS}$.

As shown in [6], this operation preserves some properties. Let N_I, N_i be Elementary Net Systems for $i = 1, 2$ and let (β_i, η_i) be an $\widehat{N}$-morphism from N_i to N_I. Let $N = N_1\langle N_I\rangle N_2$ be the composition of N_1 and N_2 using (β_i, η_i). Let (β'_i, η'_i) be the $\widehat{N}$-morphism from N to N_i created by the composition operation. We can say that:

n1 the composition is associative;

n2 *if the components reflect the sequences of the interface*, the composed Net reflects the sequences of the two components;

n3 *if one component is weakly bisimilar to the interface*, then the composed Net is weakly bisimilar to the other component.

5.1.2 α-morphisms

Given that α-morphisms preserve and reflect more properties than $\widehat{N}$-morphisms (see Section 3.1.7), we want to use them to drive a composition in a way similar to the one introduced in the previous section [4].

A simple example of the composition guided by α-morphisms is shown in Fig. 5.1. We have an interface, N_I, that is a simple sequence of two operations and three local states. Each component refines the same condition, b_1, with a condition bordered subnet related to events mapped on the pre and post events of b_1. The composed Net, $N_1\langle N_I\rangle N_2$, contains the two subnets local to the components, but for the condition representing b_1 that is taken only once; the rest of the Net, not refined by the components, is taken as it is.

To correctly relate all the systems involved in the composition, it is necessary to work with a canonical systems. Hence, starting from a pair of systems that we want to compose, it is always possible to build up their canonical versions with

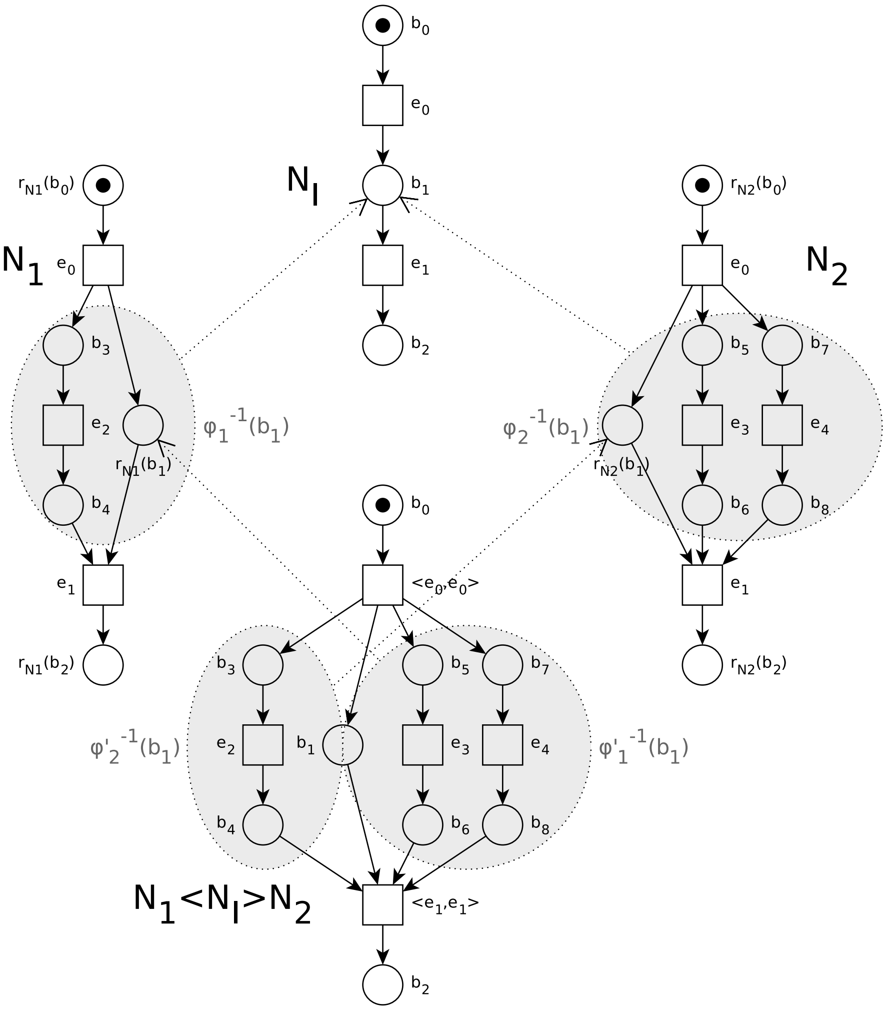


Figure 5.1: An example of composition based on α-morphisms

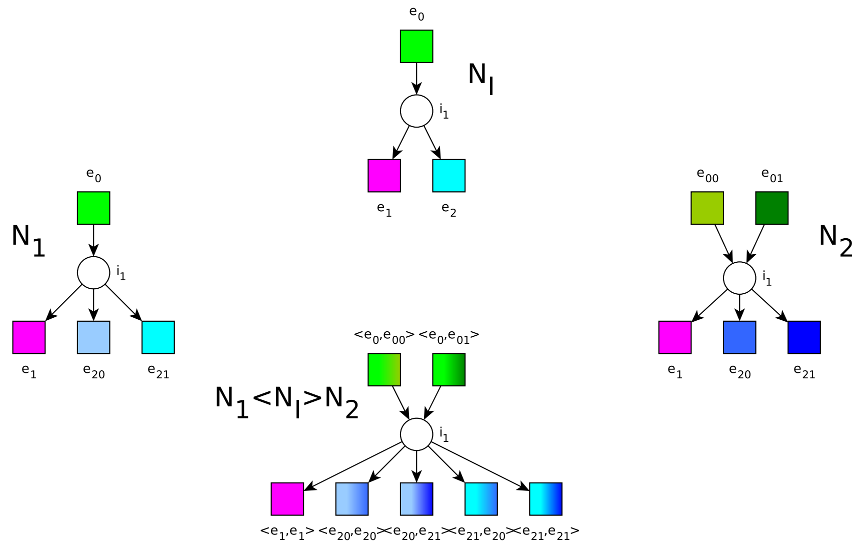


Figure 5.2: How to create the environment of an identified condition

respect to the α-morphisms and to use these systems to construct the composed Net.

$$\begin{tikzcd}
N_1 \arrow[r, "\varphi_1"] \arrow[d, rightsquigarrow] & N_I & N_2 \arrow[l, "\varphi_2"'] \arrow[d, rightsquigarrow] \\
N_1^{\mathbb{C}} \arrow[ur, "\varphi_1^{\mathbb{C}}"] & & N_2^{\mathbb{C}} \arrow[ul, "\varphi_2^{\mathbb{C}}"']
\end{tikzcd}$$

The crucial point in the definition concerns the choice of synchronizing events. Suppose that the morphisms onto the interface maps bubbles A_1 and A_2 to the same local state b (where A_i is taken in N_i). Then, the representations of A_1 and A_2 are local states which are identified as b in composing the two Nets. This implies that any event in N_1 which puts a token in the representation of A_1 must be synchronized with any event doing the same in the representation of A_2, as we can see in Fig. 5.2. This explains the definition of the sets E_{sync}, below.

Definition 60. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be an SMD-EN System for $i = 1, 2, I$. Let φ_i, with $i = 1, 2$, be an α-morphism from N_i to N_I. Let N_i be canonical with respect to φ_i.*

For each condition b_I of the interface, we define its bubble in the composed system:

$$\begin{aligned}
\mathit{Bubble}(b_I) \;=\; & ((\varphi_1^{-1}(b_I) \cap B_1 \setminus \{r_{N_1}(b_I)\}) \cup \{b_I\} \cup (\varphi_2^{-1}(b_I) \cap B_2 \setminus \{r_{N_2}(b_I)\}), \\
& (\varphi_1^{-1}(b_I) \cap E_1) \cup (\varphi_2^{-1}(b_I) \cap E_2),
\end{aligned}$$

$$F_{N_1(\varphi_1^{-1}(b_I)\setminus\{r_{N_1}(b_I)\})} \cup F_{N_2(\varphi_2^{-1}(b_I)\setminus\{r_{N_2}(b_I)\})})$$

and its connection to the rest of the Net, $F(b_I) = {}^\bullet F(b_I) \cup F^\bullet(b_I)$.
Let $e = \langle e_1, e_2\rangle \in \bigcup_{e_I \in {}^\bullet b_I} E_{sync}(e_I)$,

$$\begin{array}{rcl} {}^\bullet F(b_I) & = & \{(e,b) : b \in {}^\bigcirc\mathit{Bubble}(b_I), (e_1,b) \in F_1\} \cup \\ & & \{(e,b_I)\} \cup \\ & & \{(e,b) : b \in {}^\bigcirc\mathit{Bubble}(b_I), (e_2,b) \in F_2\} \end{array}$$

Let $e = \langle e_1, e_2\rangle \in \bigcup_{e_I \in b_I^\bullet} E_{sync}(e_I)$,

$$\begin{array}{rcl} F^\bullet(b_I) & = & \{(b,e) : b \in \mathit{Bubble}(b_I)^\bigcirc, (b,e_1) \in F_1\} \cup \\ & & \{(b_I,e)\} \cup \\ & & \{(b,e) : b \in \mathit{Bubble}(b_I)^\bigcirc, (b,e_2) \in F_2\} \end{array}$$

Synchronized events are given by synchronizing two events mapped on the same event of the interface:

$$E_{sync}(e_I) = \{e = \langle e_1, e_2\rangle : e_1 \in E_1, e_2 \in E_2, \varphi_1(e_1) = e_I = \varphi_2(e_2)\}$$

We define the composed Net $N = N_1\langle N_I\rangle N_2 = (B, E, F, m_0)$ *as*

$$B = \bigcup_{b_I \in B_I} B_{\mathit{Bubble}(b_I)}$$

$$E = \left(\bigcup_{e_I \in E_I} E_{sync}(e_I)\right) \cup \left(\bigcup_{b_I \in B_I} E_{\mathit{Bubble}(b_I)}\right)$$

$$F = \bigcup_{b_I \in B_I} \left(F(b_I) \cup F_{\mathit{Bubble}(b_I)}\right)$$

By construction, $N = N_1\langle N_I\rangle N_2$ as defined above is an Elementary Net System.

The composition maintains sequential components of the components.

Proposition 46. *Let* $N_i = (B_i, E_i, F_i, m_0^i)$ *be an Elementary Net System for* $i = 1, 2, I$. *Let* φ_i, *with* $i = 1, 2$, *be an* α*-morphism from* N_i *to* N_I. *Let* N_i *be canonical with respect to* φ_i. *Let* $N = N_1\langle N_I\rangle N_2 = (B, E, F, m_0)$.

For each sequential component of N_i, *there is a corresponding sequential component of* N.

Proof. Take a sequential component N_{SC} of N_i. For each $b_i \in B_{SC}$:

- if b_i is the representation of a condition of the interface $b_I \in B_I$, that is $b_i = r_{N_1}(b_I)$, then take $b_I \in B$,
- else take $b_i \in B$.

It's easy to see that these conditions, with their pre and post-events, are a sequential component of N. ◇

Hence, the composed Net is covered by sequential components. To see this, take a condition of the composed Net. This condition belongs to one of the components of the system, then it belongs also to a sequential component in that component, and the sequential components are maintained by the composition.

We now define a map from N onto N_1 and N_2.

Definition 61. *Define $\varphi'_i : N \to N_i$ as follows, for each $x \in X$:*

$$\varphi'_i(x) = \begin{cases} x, & \textit{if } x \in X_i \\ r_{N_i}(x), & \textit{if } x \in B_I \\ r_{N_i}(\varphi_{3-i}(x)), & \textit{if } x \in B_{3-i} \\ e_i, & \textit{if } x = \langle e_1, e_2 \rangle \\ r_{N_i}(\varphi_{3-i}(x)), & \textit{if } x \in E_{3-i} \end{cases}$$

Theorem 8. *The map φ'_i is an α-morphism from $N = N_1 \langle N_I \rangle N_2$ to $N_i, i = 1, 2$.*

Proof. $\varphi'_i : X \to X_i$ is a total surjective function by construction.

Let $x, y \in X, e \in E$,

1: $\varphi'_i(B) = B_i$: take $b \in B$; there are three cases:

- $b \in B_i$, hence $\varphi'_i(b) = b$,
- $b \in B_I$, hence $\varphi'_i(b) = r_{N_i}(b)$,
- $b \in B_{3-i}$, hence $\varphi'_i(b) = r_{N_i}(b)$;

2: $\varphi'_i(m_0) = m_0^i$: given by construction;

3: let $\varphi'_i(e) \in E_i$; there are two cases:

- $e \in E_i$: this means that e is an event in a bubble of N_i and the construction respects its pre and post conditions and all the arcs;
- $e = \langle e_1, e_2 \rangle$, hence $\varphi_i(e_i) = e_I$. Let us start with preconditions.

  Take $b \in {}^\bullet e$, then for Def. 34, points 1 $\exists b_i \in B_i : \varphi'_i(b) = b_i \wedge \exists b_I \in B_I : \varphi_i(b_i) = b_I$; if $(b, e) \in F$ there are two cases:

- $b_i \in \text{Bubble}(b_I)^{\bigcirc}$ and $(b_i, e_i) \in F_i$,
- $b \in B_I$ or $b_i \in \text{Bubble}(b_I)^{\bigcirc}$ and $(b_i, e_{3-i}) \in F_{3-i}$, hence $\varphi'_i(b) = r_{N_i}(b_I)$, hence $(r_{N_i}(b_I), e_i)$.

In the other direction, take $b_i \in {}^\bullet e_i$; then for Def. 34 there is a condition of N mapped on it. For construction, there are that $b_i \in \text{Bubble}(b_I)^{\bigcirc}$, and it can be a representation or not. If it is not a representation, $b_i \in B$, $\varphi'_i(b_i) = b_i$ and $(b_i, e) \in F$. If it is a representation, $b_I \in B$, $\varphi'_i(b_I) = b_i$ and $(b_I, e) \in F$.

The proof for post-conditions is analogous;

4: $\varphi'_i(e) = r_{N_i}(b_I) \in B_i$, hence it was in a bubble of b_I in N_2: $e \in E_{3-i}$ and $\varphi_{3-i}(e) = b_I \in B_I$, hence by construction also ${}^\bullet e^\bullet$ is in that bubble: $\varphi'_i({}^\bullet e^\bullet) = r_{N_i}(b_I)$;

5: take $b_i \in B_i$, $N(\varphi'^{-1}_i(b_i))$ and $b_I = \varphi_i(b_i) \in B_I$.

If b_i is not a representation in N_i, by construction its bubble in N consists in the condition itself alone: in that case all the constraints are easily verified.

If b_i is a representation in N_i ($b_i = r_{N_i}(b_I)$), by construction, its bubble in N is made by b_I plus the bubble of b_I in the other component. For b_I, the proof is exactly as we stated before. That bubble is clearly acyclic. The composition rebuilds the same relations between elements in the bubble of the other component, respecting constraint 5d. It creates the Cartesian product of events of N_1 and N_2 mapped on the same event of N_I and, consequently, it creates an arc between all these copies and the neighbouring conditions, respecting constraints 5b and 5c.

We now prove, for representation b_i, the constraint 5e on the conditions in the bubble of the other component, $b \in B_{3-i}$. Let $b \in \varphi'^{-1}_i(b_i) \cap B$, such that $b \notin B_I$.

Let N_{SC_i} be a sequential component of N_i containing b_i. Clearly, this sequential component contains also its pre and post events. Given that b_i is a representation, these are exactly all the events in the inverse image of pre and post events of b_I.

Let $N_{SC_{3-i}}$ be a sequential component of N_{3-i} containing b and all the events in the inverse image of pre and post events of b_I.

Take a sequential component generated by all the conditions of N_{SC_i} but for b_i plus the conditions of $N_{SC_{3-i}}$ that are in the bubble of b_I. That sequential component contains all the events in the neighbourhood of these conditions, hence also all the events in the inverse image of pre and post events of b_i.

◇

The diagram formed by the α-morphisms between the interface, the two components, and the composed Net commutes.

Proposition 47. *The following diagram commutes.*

$$\begin{tikzcd}
 & N_I & \\
N_1^{\mathbb{C}} \arrow[ur, "\varphi_1^{\mathbb{C}}"] & & N_2^{\mathbb{C}} \arrow[ul, "\varphi_2^{\mathbb{C}}"'] \\
 & N_1^{\mathbb{C}}\langle N_I\rangle N_2^{\mathbb{C}} \arrow[ul, "\varphi'_1"] \arrow[ur, "\varphi'_2"'] &
\end{tikzcd}$$

Proof. We have to prove that, for every elements $x \in X_N : \varphi_1^{\mathbb{C}}(\varphi'_1(x)) = \varphi_2^{\mathbb{C}}(\varphi'_2(x))$. The elements of the composed Net are of three kinds:

elements local to the components : take $x \in X$ such that $x \in X_i$. Hence there is a condition of the interface, $b_I \in B_I$, such that $\varphi_i^{\mathbb{C}}(x) = b_I$. Hence there is a representation of b_I in the other component $r_{N_{3-i}}(b_I)$.

$\varphi_i^{\mathbb{C}}(\varphi'_i(x)) = \varphi_i^{\mathbb{C}}(x) = b_I = \varphi_{3-i}^{\mathbb{C}}(r_{N_{3-i}}(b_I)) = \varphi_{3-i}^{\mathbb{C}}(\varphi'_{3-i}(x))$;

representation conditions: take $x \in B_I$. Hence there is a representation of x in the two components $r_{N_i}(x)$ and $r_{N_{3-i}}(x)$.

$\varphi_i^{\mathbb{C}}(\varphi'_i(x)) = \varphi_i^{\mathbb{C}}(r_{N_i}(x)) = x = \varphi_{3-i}^{\mathbb{C}}(r_{N_{3-i}}(x)) = \varphi_{3-i}^{\mathbb{C}}(\varphi'_{3-i}(x))$;

synchronized events: take $x \in E$ such that $x = \langle e_1, e_2\rangle$. Hence $\varphi_1^{\mathbb{C}}(e_1) = e_I = \varphi_2^{\mathbb{C}}(e_2)$ with $e_I \in E_I$.

$\varphi_1^{\mathbb{C}}(\varphi'_1(\langle e_1, e_2\rangle)) = \varphi_1^{\mathbb{C}}(e_1) = e_I = \varphi_2^{\mathbb{C}}(e_2) = \varphi_2^{\mathbb{C}}(\varphi'_2(\langle e_1, e_2\rangle))$.

◇

By construction we get the following result:

Proposition 48. *The system $N = N_1\langle N_I\rangle N_2$ is canonical with respect to φ'_1 and to φ'_2.*

The result of the composition can not be seen as the pullback, as shown in Fig. 5.1. It is easy to see the α-morphisms from N_i to N_I and from $N_1\langle N_I\rangle N_2$ to N_i. If we build up a new diagram in which we substitute $N_1\langle N_I\rangle N_2$ with N_2, it is possible to build up α-morphisms from N_2 to N_i. But it is not possible to build up an α-morphism from N_2 to $N_1\langle N_I\rangle N_2$, hence the resulting Net from the composition operation is not a pullback. In this category it is not possible to find the pullback, due to the fact that the morphisms are surjective [25].

It is still an open problem whether, in general, the diagram of a composition operation is a pushout.

This operation, essentially, coincides with composition of Nets based on $\widehat{N}$-morphisms.

Proposition 49. *Let $N_i = (B_i, E_i, F_i, m_0^i)$ be an SMD-EN System for $i = 1, 2, I$. Let φ_i, with $i = 1, 2$, be an α-morphism from N_i to N_I. Let N_i be canonical with respect to φ_i. Let $N^\alpha = N_1\langle N_I\rangle^\alpha N_2 = (B, E, F, m_0)$ be the composition of N_1 and N_2 using φ_1 and φ_2. Let φ_i' be the α-morphism from N to N_i created by the composition operation.*

Now, consider the $\widehat{N}$-morphism $(\varphi_i^{\mathcal{C}} \cap (R_i^{\mathcal{C}} \times B_I), \varphi_i^{\mathcal{C}} \cap (E_i^{\mathcal{C}} \times E_I))$. Let $N^{\widehat{N}} = N_1\langle N_I\rangle^{\widehat{N}} N_2 = (B, E, F, m_0)$ be the composition of N_1 and N_2 using $(\varphi_1^{\mathcal{C}} \cap (R_1^{\mathcal{C}} \times B_I), \varphi_1^{\mathcal{C}} \cap (E_1^{\mathcal{C}} \times E_I))$ and $(\varphi_2^{\mathcal{C}} \cap (R_2^{\mathcal{C}} \times B_I), \varphi_2^{\mathcal{C}} \cap (E_2^{\mathcal{C}} \times E_I))$. Let (β_i', η_i') be the $\widehat{N}$-morphism from N to N_i created by the composition operation.

The systems N^α and $N^{\widehat{N}}$ are isomorphic, $\beta_i' = \varphi_i' \cap (R^{\mathcal{C}} \times B_i)$ and $\eta_i' = \varphi_i' \cap (E \times E_i)$.

From results in Sections 3.1.7 and 3.1.6 we can derive a property valid for composition based on α-morphisms. We know that, if N_1 is weakly bisimilar to N_I then N is weakly bisimilar to N_2. By Prop. 19 we can infer weak bisimilarity between N_1 and N_I. This property is based on an α-morphism from a well marked N_1 to N_I plus a check on the final markings of each bubble, non interferent, using the unfolding. These constraints are either structural or locally behavioural, while, in the case of $\widehat{N}$-morphisms, checking bisimilarity must be made globally. Fig. 5.3 shows an example in which N_1 and N_2 are weakly bisimilar to N_I. Hence $N_1\langle N_I\rangle N_2$ is weakly bisimilar to N_1, N_2 and N_I.

Algorithms

The following algorithm builds up the composed system starting from canonical components.

Algorithm 2. $B = \varnothing; E = \varnothing; F = \varnothing; \varphi = \varnothing; \varphi_1' = \varnothing; \varphi_2' = \varnothing$

First, create the synchronized events:

```
$\forall e_I \in E_I$
  $\forall e_1 \in (\varphi_1^{\mathbb{C}})^{-1}(e_I)$
    $\forall e_2 \in (\varphi_2^{\mathbb{C}})^{-1}(e_I)$
      $E+ = \langle e_1, e_2\rangle$
      $\varphi_1'+ = (\langle e_1, e_2\rangle, e_1)$
```

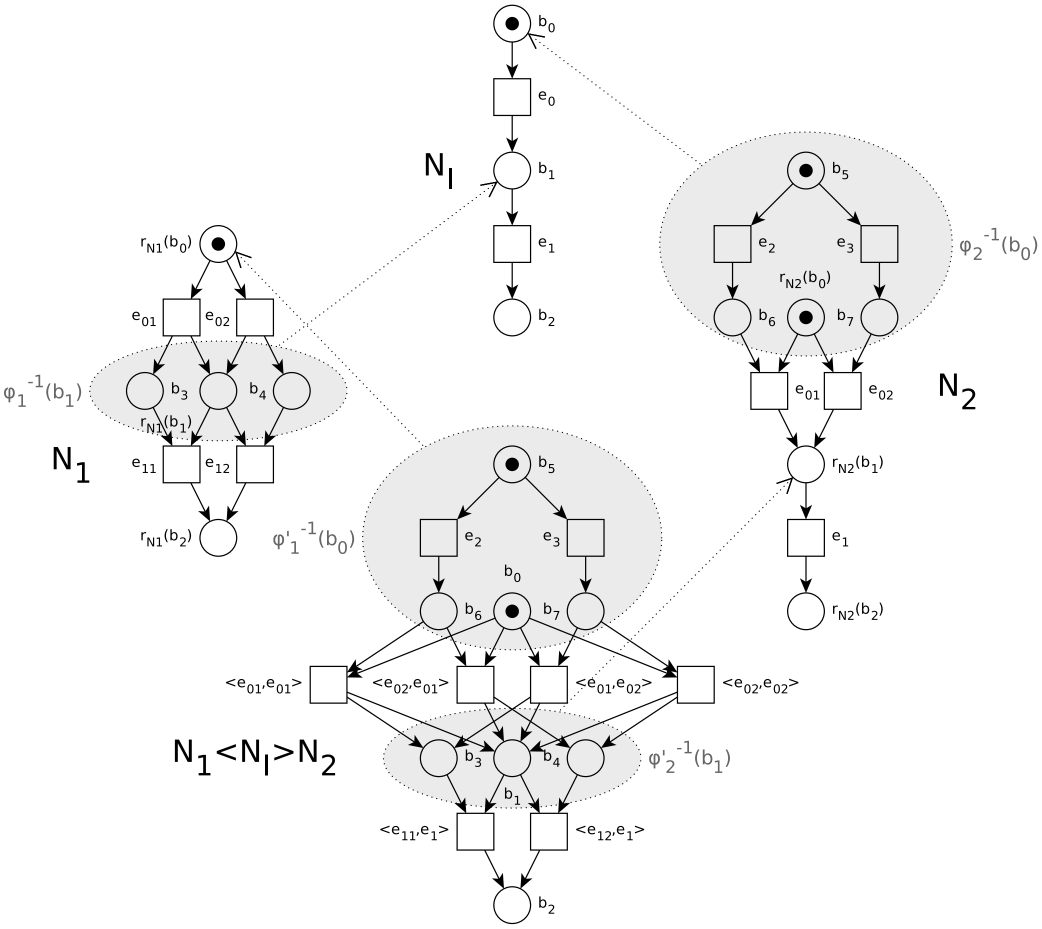


Figure 5.3: An example of composition based on α-morphisms

```
    $\varphi_2'+ = (\langle e_1, e_2 \rangle, e_2)$
    $\varphi+ = (\langle e_1, e_2 \rangle, e_I)$
```

Then, create the conditions, the bubbles and the arcs:

```
$\forall b_I \in B_I$
   $Pre_1 = {}^{\bullet}({}^{\bigcirc}N_1(\varphi_1^{-1}(b_I)))$
   $Pre_2 = {}^{\bullet}({}^{\bigcirc}N_2(\varphi_2^{-1}(b_I)))$
   $Post_1 = (N_1(\varphi_1^{-1}(b_I))^{\bigcirc})^{\bullet}$
   $Post_2 = (N_2(\varphi_2^{-1}(b_I))^{\bigcirc})^{\bullet}$
   $r_1 = {}^{\bigcirc}N_1(\varphi_1^{-1}(b_I)) \cap N_1(\varphi_1^{-1}(b_I))^{\bigcirc}$
   $r_2 = {}^{\bigcirc}N_2(\varphi_2^{-1}(b_I)) \cap N_2(\varphi_2^{-1}(b_I))^{\bigcirc}$
   *addCondition*$(b_I, Pre_1, Pre_2, Post_1, Post_2, r_1, r_2)$
   *if* $|N_1(\varphi_1^{-1}(b_I))| > 1$ *then*
      *addBubble*$(b_I, 1, N_1(\varphi_1^{-1}(b_I)), Pre_2, Post_2, r_2)$
   *if* $|N_2(\varphi_2^{-1}(b_I))| > 1$ *then*
      *addBubble*$(b_I, 2, N_2(\varphi_2^{-1}(b_I)), Pre_1, Post_1, r_1)$
```

where we use the following sub-algorithms:

Algorithm 3. addCondition$(b_I, Pre_1, Pre_2, Post_1, Post_2, r_1, r_2)$:

```
$B+ = b_I$
$\varphi_1'+ = (b_I, r_1)$
$\varphi_2'+ = (b_I, r_2)$
$\varphi+ = (b_I, b_I)$
$\forall p_1 \in Pre_1$
   $\forall p_2 \in Pre_2$
      *if* $\langle p1, p2 \rangle \in E$ *then*
         $F+ = (\langle p_1, p_2 \rangle, b_I)$
$\forall q_1 \in Post_1$
   $\forall q_2 \in Post_2$
      *if* $\langle q1, q2 \rangle \in E$ *then*
         $F+ = (b_I, \langle q_1, q_2 \rangle)$
```

Algorithm 4. addBubble$(b_I, \text{net}, \text{bubble}, Pre_{other}, Post_{other}, r)$:

```
$\forall b \in {}^{\bigcirc}$*bubble* $\setminus$ *bubble*$^{\bigcirc}$
   $B+ = b$
   $\varphi_{net}'+ = (b, b)$
   $\varphi_{3-net}'+ = (b, r)$
   $\varphi+ = (b, b_I)$
   $Pre = {}^{\bullet}b$
   $\forall p_1 \in Pre$
      $\forall p_2 \in Pre_{other}$
```

```
        if $\langle p1, p2\rangle \in E$ then
            $F += (\langle p_1, p_2\rangle, b)$
    $\forall x \in b^\bullet \cap bubble$
        $addNodeBubble(b_I, b, x, Net, bubble, Post_{other}, r)$
```

Algorithm 5. addNodeBubble(b_I, ante, y, Net, bubble, $Post_{other}$, r):

```
if $y \notin X$ then
    $X += y$
    $\varphi'_{net} += (y, y)$
    $\varphi'_{3-net} += (y, r)$
    $\varphi += (y, b_I)$
    $Post = y^\bullet$
    $\forall x \in Post \cap bubble$
        $addNodeBubble(b_I, y, x, Net, bubble, Post_{other}, r)$
    if $y \in bubble^\bigcirc$
        $\forall q_1 \in Post$
            $\forall q_2 \in Post_{other}$
                if $\langle q1, q2\rangle \in E$ then
                    $F += (y, \langle q_1, q_2\rangle)$
$F += (ante, y)$
```

5.2 Occurrence Nets

We now define an operation of composition for Occurrence Nets. This operation composes two Occurrence Nets, N_1 and N_2, with respect to a third Occurrence Net N_I. The composition is driven by a pair of θ-morphisms, φ_1 and φ_2, respectively from N_1 to N_I, and from N_2 to N_I. In this way, N_1 and N_2 can be seen as refinement of conditions of N_I using bubbles. We can interpret this as two components and a protocol of interaction between them.

We impose that the subsystems and the interface are simple Nets. To obtain the correct relations between the composed system, the two subsystems and the interface system, it is necessary that the two subsystems are canonical with respect to their morphisms.

Definition 62. *Let $N_i = (B_i, E_i, F_i)$ be an Occurrence Net for $i = 1, 2, I$. Let φ_i, with $i = 1, 2$, be a θ-morphism from N_i to N_I. Let N_i be canonical with respect to φ_i.*

Synchronized events are given by synchronizing two events mapped on the same event of the interface:

$$E_{sync}(e_I) = \{e = \langle e_1, e_2\rangle : e_1 \in E_1, e_2 \in E_2, \varphi_1(e_1) = e_I = \varphi_2(e_2)\}$$

For each condition b_I of the interface, we define its bubble in the composed system and its connection to the rest of the Net.

- *if* $b_I \in \min(N_I)$ *then*

$$\begin{aligned}\textit{Bubble}(b_I) &= ((\varphi_1^{-1}(b_I) \cap B_1 \setminus \{r_{N_1}(b_I)\}) \cup \{b_I\} \cup (\varphi_2^{-1}(b_I) \cap B_2 \setminus \{r_{N_2}(b_I)\}),\\ &\quad (\varphi_1^{-1}(b_I) \cap E_1) \cup (\varphi_2^{-1}(b_I) \cap E_2),\\ &\quad F_{N_1(\varphi_1^{-1}(b_I)\setminus\{r_{N_1}(b_I)\})} \cup F_{N_2(\varphi_2^{-1}(b_I)\setminus\{r_{N_2}(b_I)\})})\end{aligned}$$

Let $e = \langle e_1, e_2\rangle \in \bigcup_{e_I \in b_I^\bullet} E_{sync}(e_I)$,

$$\begin{aligned}F(b_I) &= \{(b,e) : b \in \max(\textit{Bubble}(b_I)), (b, e_1) \in F_1\} \cup\\ &\quad \{(b_I, e)\} \cup\\ &\quad \{(b,e) : b \in \max(\textit{Bubble}(b_I)), (b, e_2) \in F_2\}\end{aligned}$$

- *otherwise*
Bubble$(b_I) = \bigcup_{e \in E_{sync}({}^\bullet b_I)} SB(b_I, e)$, *where* $e = \langle e_1, e_2\rangle$*:*

$$\begin{aligned}SB(b_I, e) &= (((\varphi_1^{-1}(b_I) \cap B_1 \setminus \{r_{N_1}(b_I)\}) \cap \lceil e_1\rceil) \cup \{b_{I,e}\} \cup\\ &\quad ((\varphi_2^{-1}(b_I) \cap B_2 \setminus \{r_{N_2}(b_I)\}) \cap \lceil e_2\rceil),\\ &\quad (\varphi_1^{-1}(b_I) \cap E_1 \cap \lceil e_1\rceil) \cup (\varphi_2^{-1}(b_I) \cap E_2 \cap \lceil e_2\rceil),\\ &\quad F_{N_1(\varphi_1^{-1}(b_I)\setminus\{r_{N_1}(b_I)\})\cap\lceil e_1\rceil} \cup F_{N_2(\varphi_2^{-1}(b_I)\setminus\{r_{N_2}(b_I)\})\cap\lceil e_2\rceil})\end{aligned}$$

The arcs are defined as $F(b_I) = \bigcup_{e \in E_{sync}({}^\bullet b_I)} F(b_I, e)$, *where* $F(b_I, e) = {}^\bullet F(b_I, e) \cup F^\bullet(b_I, e)$

$$^\bullet F(b_I, e) = \{(e, b) : b \in \min(SB(b_I, e))\}$$

Let $f = \langle f_1, f_2\rangle \in \bigcup_{f_I \in b_I^\bullet} E_{sync}(f_I)$,

$$\begin{aligned}F^\bullet(b_I, e) &= \{(b, f) : b \in \max(SB(b_I, e)), (b, f_1) \in F_1, e_1 \le f_1, e_2 \le f_2\} \cup\\ &\quad \{(b_{I,e}, f), e_1 \le f_1, e_2 \le f_2\} \cup\\ &\quad \{(b, f) : b \in \max(SB(b_I, e)), (b, f_2) \in F_2, e_1 \le f_1, e_2 \le f_2\}\end{aligned}$$

We define the composed Net $N = N_1\langle N_I\rangle N_2 = (B, E, F)$ *as*

$$B = \bigcup_{b_I \in B_I} B_{\textit{Bubble}(b_I)}$$

$$E = \left(\bigcup_{e_I \in E_I} E_{sync}(e_I) \right) \cup \left(\bigcup_{b_I \in B_I} E_{Bubble(b_I)} \right)$$

$$F = \bigcup_{b_I \in B_I} \left(F(b_I) \cup F_{Bubble(b_I)} \right)$$

By construction, $N = N_1\langle N_I \rangle N_2$ as defined above is an Occurrence Net. We now define a map from N onto N_1 and N_2.

Definition 63. *Define $\varphi'_i : N \to N_i$ as follows, for each $x \in X$:*

$$\varphi'_i(x) = \begin{cases} x, & \textit{if } x \in X_i \\ b_{I,e_i}, & \textit{if } x = b_{I,\langle e_1,e_2 \rangle} \in B_I \\ b_{I,e_i}, & \textit{if } x \in B_{3-i} \textit{ and } x \in SB(b_{i,e_{3-i}}) \textit{ and } e \in \lfloor x \rfloor = \langle e_1, e_2 \rangle \\ e_i, & \textit{if } x = \langle e_1, e_2 \rangle \\ b_{I,e_i}, & \textit{if } x \in E_{3-i} \textit{ and } x \in SB(b_{i,e_{3-i}}) \textit{ and } e \in \lfloor x \rfloor = \langle e_1, e_2 \rangle \end{cases}$$

Theorem 9. *The map φ'_i is a θ-morphism from $N = N_1\langle N_I \rangle N_2$ to $N_i, i = 1, 2$.*

Proof. Let $x, y \in X, e, f \in E$,

1: $\varphi'_i : X \to X_i$ is a total surjective function by construction;

2: $x \leq_N y$: for every elements mapped on themselves the causality relation is weakly preserved, hence $\varphi'_i(x) \leq_{N_i} \varphi'_i(y)$. The elements of the other subnet are mapped on a representation and this is enough because it is present also in the composed Net;

3: $x \ \mathbf{co}_N \ y$: for every elements mapped on themselves the concurrency relation is preserved, hence $\varphi'_i(x) \ \mathbf{co}_{N_2} \ \varphi'_i(y)$ or $\varphi'_i(x) = \varphi'_i(y)$. The elements of the other subnet are mapped on a representation and this is enough because it is present also in the composed Net;

4: $\varphi'_i(B) = B_i$: take $b \in B$; there are two cases:

- $b \in B_i$, hence $\varphi'_i(b) = b$,
- $b \notin B_i$, hence $\varphi'_i(b) = r_{N_i}(\varphi_{3-i}(b))$;

5: $\varphi'_i(e) = r_{N_i}(b_I) \in B_i$, hence it was in a bubble of b_I in N_{3-i}: $e \in E_{3-i}$ and $\varphi_{3-i}(e) = b_I \in B_I$, hence by construction also ${}^\bullet e^\bullet$ is contained in that bubble: $\varphi'_i({}^\bullet e^\bullet) = r_{N_i}(b_I)$;

6: let $\varphi'_i(e) \in E_i$; there are two cases:

- $e \in E_i$: this means that e is an event in a bubble of N_i and the construction respects its pre and post conditions and all the arcs;
- $f = \langle f_1, f_2 \rangle$, hence $\varphi_i(f_i) = f_I \in E_I$. Let us start with preconditions. Take $b \in {}^\bullet f$, then for Def. 45, points 4 $\exists b_i \in B_i : \varphi'_i(b) = b_i \wedge \exists b_I \in B_I : \varphi_i(b_i) = b_I$; if $(b, f) \in F$ there are two cases:
  - $b \in B_i$ and $b_i \in \max(SB(b_I, e))$ and $(b_i, f_i) \in F_i$,
  - $b \notin B_i$, hence $\varphi'_i(b) = r_{N_i}(b_I)$, hence $(r_{N_i}(b_I), f_i) \in F_i$.

  In the other direction, take $b_i \in {}^\bullet f_i$, then by Def. 45 there is a condition of N mapped on it. By construction, we have that $b_i \in \max(\text{Bubble}(b_I))$, and it can be a representation or not. If it is not a representation, $b_i \in B$, $\varphi'_i(b_i) = b_i$ and $(b_i, f) \in F$. If it is a representation, $b_I \in B$, $\varphi'_i(b_I) = b_i$ and $(b_I, f) \in F$.

  The proof for post-conditions is analogous;

7: take $b_i \in B_i$, $N((\varphi'_i)^{-1}(b_i))$ and $b_I = \varphi_i(b_i) \in B_I$.

If b_i is not a representation in N_i, by construction its bubble in N consists in the condition itself alone: in that case all the constraints are easily verified.

If b_i is a representation in N_i ($b_i = r_{N_i}(b_I)$), by construction, its bubble in N is made by b_I plus the bubble of b_I in the other component. For b_I, the proof is exactly as we stated before. The composition creates the Cartesian product of events of N_1 and N_2 mapped on the same event of N_I and, consequently, it creates an arc between all these copies and the neighbouring conditions, respecting constraints 7a and 7c. It rebuilds the same relations between elements in the bubble of the other component, respecting constraint 7b.

◇

The diagram formed by the θ-morphisms between the interface, the two components, and the composed Net commutes.

Proposition 50. *The following diagram commutes.*

$$\begin{tikzcd}
 & N_I & \\
N_1^{\mathbb{C}} \arrow[ur, "\varphi_1^{\mathbb{C}}"] & & N_2^{\mathbb{C}} \arrow[ul, "\varphi_2^{\mathbb{C}}"'] \\
 & N_1^{\mathbb{C}} \langle N_I \rangle N_2^{\mathbb{C}} \arrow[ul, "\varphi'_1"] \arrow[ur, "\varphi'_2"'] &
\end{tikzcd}$$

Proof. We have to prove that, for every element $x \in X_N : \varphi_1^{\mathbb{C}}(\varphi_1'(x)) = \varphi_2^{\mathbb{C}}(\varphi_2'(x))$. The elements of the composed Net are of three kinds:

elements local to the components : take $x \in X$ such that $x \in X_i$. Hence there is a condition of the interface, $b_I \in B_I$, such that $\varphi_i^{\mathbb{C}}(x) = b_I$. Hence there is a representation of b_I in the other component $r_{N_{3-i}}(b_I)$.
$\varphi_i^{\mathbb{C}}(\varphi_i'(x)) = \varphi_i^{\mathbb{C}}(x) = b_I = \varphi_{3-i}^{\mathbb{C}}(r_{N_{3-i}}(b_I)) = \varphi_{3-i}^{\mathbb{C}}(\varphi_{3-i}'(x))$;

representation conditions: take $x \in B_I$. Hence there is a representation of x in the two components $r_{N_i}(x)$ and $r_{N_{3-i}}(x)$.
$\varphi_i^{\mathbb{C}}(\varphi_i'(x)) = \varphi_i^{\mathbb{C}}(r_{N_i}(x)) = x = \varphi_{3-i}^{\mathbb{C}}(r_{N_{3-i}}(x)) = \varphi_{3-i}^{\mathbb{C}}(\varphi_{3-i}'(x))$;

synchronized events: take $x \in E$ such that $x = \langle e_1, e_2 \rangle$. Hence $\varphi_1^{\mathbb{C}}(e_1) = e_I = \varphi_2^{\mathbb{C}}(e_2)$ with $e_I \in E_I$.
$\varphi_1^{\mathbb{C}}(\varphi_1'(\langle e_1, e_2 \rangle)) = \varphi_1^{\mathbb{C}}(e_1) = e_I = \varphi_2^{\mathbb{C}}(e_2) = \varphi_2^{\mathbb{C}}(\varphi_2'(\langle e_1, e_2 \rangle))$.

◇

By construction we get the following result:

Proposition 51. *The system $N = N_1 \langle N_I \rangle N_2$ is canonical with respect to φ_1' and to φ_2'.*

5.3 Elementary Transition Systems

5.3.1 $\widehat{G}$-morphisms

We recall an operation of composition defined by Pomello and Bernardinello in [38]. The starting point is a set of three Elementary Transition Systems; one of them, TS_I, plays the role of an interface between the other two, TS_1 and TS_2. The composition is driven by a pair of $\widehat{G}$-morphisms, (f_1, g_1) and (f_2, g_2), respectively from TS_1 to TS_I, and from TS_2 to TS_I. We can see TS_I also as the protocol of the interaction between them. In that sense, it is important that the morphisms are surjective, because each system has to respect the protocol entirely. The composition of these two systems is given by the union of a local part of each system and a common part corresponding to the protocol.

Definition 64. *Let $TS_i = (S_i, E_i, T_i, s_0^i)$ be an Elementary Transition System for $i = 1, 2$, $TS_I = (S_I, E_I, T_I, s_0^I)$ be an Elementary Transition System and let $(f, g) : TS_i \to TS_I$ be a $\widehat{G}$-morphism. Let L_i denote the set of events which are in E_i and not in the domain of the partial function g_i, $L_i = \{e \in E_i : g_i(e) = undefined\}$;*

and let H denote the set of pairs of events $\langle e_1, e_2\rangle$ which are mapped by the two morphisms on the same event of TS_I, $H = \{\langle e_1, e_2\rangle : g_1(e_1) = g_2(e_2)\}$.

We define $TS_1\langle TS_I\rangle TS_2 = TS = (S, E, T, s_0)$ as follows:

1. *$S = \{(s_1, s_2) \in S_1 \times S_2 : f_1(s_1) = f_2(s_2)\}$,*
2. *$E = L_1 \cup L_2 \cup H$,*
3. *$((s_1, s_2), e, (s'_1, s'_2)) \in T$ iff one of the following clauses holds:*
   - *(a) $(s_1, e_1, s'_1) \in T_1 \wedge (s_2, e_2, s'_2) \in T_2 \wedge e = \langle e_1, e_2\rangle \in H$,*
   - *(b) $(s_1, e, s'_1) \in T_1, s_2 = s'_2 \wedge e \in L_1$,*
   - *(c) $s_1 = s'_1, (s_2, e, s'_2) \in T_2 \wedge e \in L_2$,*
4. *$s_0 = (s^1_0, s^2_0)$.*

From this construction it follows immediately that $TS = TS_1\langle TS_I\rangle TS_2$ as defined above is a Transition System.

The reachable part of the composed Transition System is an Elementary Transition System [38].

Definition 65. *Define the pair (f'_i, g'_i), with $f'_i \subseteq S \times S_i$ and $g'_i : E \to^* E_i$ as follows:*

- *f'_i is the projection of an element of S into $S_i, i = 1, 2$: $f'_i = \{((s_1, s_2), s_i) : s_i \in S_i\}$,*
- *$\forall e \in L_1 : g'_1(e) = e, g'_2(e) =$ undefined,*
- *$\forall e \in L_2 : g'_1(e) =$ undefined$, g'_2(e) = e$,*
- *$\forall \langle e_1, e_2\rangle \in H : \eta'_i(\langle e_1, e_2\rangle) = e_i$.*

As shown in [38], the diagram created by the $\widehat{G}$-morphisms between the interface, the two components, and the composed system commutes.

Theorem 10. *The pair (f'_i, g'_i) is a $\widehat{G}$-morphism from $TS = TS_1\langle TS_I\rangle TS_2$ to $TS_i, i = 1, 2$ and the following diagram commutes.*

$$\begin{tikzcd}
 & TS_I & \\
TS_1 \arrow[ur, "{(f_1,g_1)}"] & & TS_2 \arrow[ul, "{(f_2,g_2)}"'] \\
 & TS \arrow[ul, "{(f'_1,g'_1)}"] \arrow[ur, "{(f'_2,g'_2)}"'] &
\end{tikzcd}$$

However, as discussed in [3], the operation is not a pullback in $\mathcal{ETS}$.

5.3.2 Γ-morphisms

We want to use Γ-morphisms here defined to drive the composition introduced in Def. 64.

The diagram created by the Γ-morphisms between the interface, the two components, and the composed system commutes.

Theorem 11. *The pair* (f'_i, g'_i) *as defines in Def. 65 is a* Γ*-morphism from* $TS = TS_1\langle TS_I\rangle TS_2$ *to* $TS_i, i = 1, 2$ *and the following diagram commutes.*

$$\begin{tikzcd}
 & TS_I & \\
TS_1 \arrow[ur, "{(f_1,g_1)}"] & & TS_2 \arrow[ul, "{(f_2,g_2)}"'] \\
 & TS \arrow[ul, "{(f'_1,g'_1)}"] \arrow[ur, "{(f'_2,g'_2)}"'] &
\end{tikzcd}$$

Proof. It has already been proved in the previous section that (f'_i, g'_i) is a $\widehat{G}$-morphism. We need to prove only that $\forall(s_i, e_i, s'_i) \in T_i, \exists(s, e, s') \in T$ so that $s \in (f'_i)^{-1}(s_i), e \in (g'_i)^{-1}(e_i), s' \in (f'_i)^{-1}(s'_i)$.

Let us take $(s_1, e_1, s'_1) \in T_1$ (for arrows of TS_2 the proof is identical, up to indexes). There are two cases:

- $e_1 \in L_1$: so e_1 is not mapped by g_1 and this implies that $\exists s_I \in S_I : f_1(s_1) = f_1(s'_1) = s_I$. For the surjectivity of f_2 we know that $\exists s_2 \in S_2 : f_2(s_2) = s_I$ and by construction of S we know that $\exists(s_1, s_2), (s'_1, s_2) \in S$ and by construction of T we know that $\exists((s_1, s_2), e_1, (s'_1, s_2)) \in T$;

- $\exists e_2 \in E_2 : \langle e_1, e_2\rangle \in H$: this implies that $\exists e_I \in E_I : g_1(e_1) = g_2(e_2) = e_I$. The Γ-morphism between TS_1 and TS_I assures that $\exists(f_1(s_1), e_I, f_1(s'_1)) \in T_I$. The Γ-morphism between TS_2 and TS_I assures that $\exists(s_2, e_2, s'_2) \in T_2 \wedge s_2 \in f_2^{-1}(f_1(s_1)), s'_2 \in f_2^{-1}(f_1(s'_1))$. By construction of S we know that $\exists(s_1, s_2), (s'_1, s'_2) \in S$. By construction of T we know that $((s_1, s_2), \langle e_1, e_2\rangle, (s'_1, s'_2)) \in T$.

The diagram commutes by definition of the composed Transition System. ◇

Chapter 6

Observability

The theoretical framework constituted by the composition guided by morphisms and interface is suitable to be used in the study of information flows and visibility.

In this chapter we assume to have a system divided in a hidden part (called the high part or the *defender*) and an observable part (called the low part or the *attacker*). The observer knows the structure of the whole system, but he is able to observe only the observable part. The observer can see the state of a part of the system, and observing this, it is able to derive that one event is fired. We want to understand if the observer is able to infer some information on the local states of the hidden part.

A lot of interest was in the study of the possibility to infer the state of a hidden part of a system. Let us cite some of the main works present in the literature.

Moore [30] considers sequential machines with a finite number of states, a finite number of possible input symbols, and a finite number of possible output symbols. He investigates what kinds of conclusions about the internal conditions of the machine it is possible to draw from external experiments.

The experimenter chooses the finite sequence of input symbols he puts into the machine, either a fixed sequence, or one in which each symbol depends on the previous output symbols. There will be a sequence of output symbols and, possibly, a conclusion which the experimenter emits. That conclusion depend only on which experiment is being performed and what the sequence of output symbols was.

There is a second kind of experiment in which the experimenter has access to several copies of the same machine, each of which is initially in the same state. The experimenter can send different sequences of inputs to each of these copies, and receive from each one the corresponding output sequence.

In each of these two kinds of experiments the experimenter is a human who is trying to learn the answer to some question about the nature of the machine or its initial state.

There is an artificial restriction that is imposed on the action of the experimenter. He is not allowed to open up the machine and look at the parts to see what they are and how they are interconnected. At any rate, we always impose this artificial restriction that the machines under consideration are always just what are sometimes called "black boxes", described in terms of their inputs and outputs, but no information on the internal construction can be gained.

We aim at a structural characterization of the hidden internal states of a system that become visible after its interaction with a defined subsystem. We assume to have a high-level system that wants to keep secret its internal local states from a low-level system interacting with the high-level component through an interface.

Basically, we explore the consequences of a proposal originally made by Busi and Gorrieri for defining non-interference properties. The newly part of our proposal is that we use the local validity of conditions as observable properties and we focus on structural properties.

The general context of our study is known today as non-interference in the literature. The notions of opacity and interference between subsystems have been originally defined formally for process algebras [20].

One of the first definitions of opacity is given in [28]. Mazaré wants to hide a piece of information from an intruder. He says that the verification of a protocol should include a way of formalizing the information that were leaked and that the intruder could guess. In his work he assumes that the intruder has a passive view of a protocol session in which two agents exchange encrypted messages. He defines an opaque property as a property for which there exist two possible sessions of the protocol such that in one the property is true whereas in the other it is not, and it is impossible for the intruder to differentiate from these two sessions seeing only their messages.

The work of Sutherland is reviewed in [47]. It is a theory of information flow based on logical deduction, which he intended as a means of facing the security problem. The broad theme of Sutherland's work is that in a secure computer system the users or processes at low security levels should not be able to deduce with certainty anything about the activities of the high users or processes. We can say that the information flows from a high user to a low one, if what the low user is able to see is strictly related to what the high user sees. He call these notion non-deductibility.

Bryans, Koutny and Ryan [11] use the notion of non-deducibility due to Sutherland and a variant of this idea: the notion of opacity. Whereas non-interference tries to capture the complete absence of information flow, opacity is specific to a particular item of information. Thus, for example, the value of a variable said v, is deemed to be opaque for a particular run of a protocol if the adversary is unable to deduce its value from the observations and deductions available to him during the run. The adversary is able to observe the local states of a low-level part of the system as well as actions. For the protocol to satisfy such a requirement it must be the case that, for any alternative value of v, there is another possible run of the protocol that gives rise to observations by the adversary that are indistinguishable from the original observations. As standard in these cases, they assume that the adversary has full knowledge of the construction of the system. This is in effect a worst case assumption. The authors extend the notion of opacity to general systems modelled by Petri Nets with weighted arcs. They also define different kinds of opacity. They show that other concepts commonly used in the formal security community, like anonymity, non-interference and downgrading of a channel, can be modelled with this approach. They extend opacity to Transition Systems and give flexible definition of the adversary's observational capabilities. Since the majority of opacity problems are undecidable, they define an approximation of opacity that is decidable under certain constraints.

Information Flow is a concept widely used but with a weak formal definition. There have been several attempts to formalize it, as in [9]. Boudol works on developing "security-minded" programming languages. He shows that secure information flow property is guaranteed by a standard security type system, and that, for a simple language, it is strictly stronger than non-interference. With non-interference he means a property stating that "variety in a secret input should not be conveyed to public output". He exposes two reasons why non-interference does not provide him with an appropriate semantical setting to use: one is that it does not easily account for dynamic manipulations of the security policy, and the second is that it does not rely on an intuitive notion of a security error that could be used to explain why a program is faulty. Non-interference does not formalize the intuitive notion of secure information flow, which is, that "no execution results in a flow unless this is allowed by the information flow policy". But, to make this definition precise, it is necessary to give a formal meaning to "execution results in a flow". That is, it has to give an information-flow-aware semantics to programs. He uses lattice of security levels in which "objects" - information containers - of a system are labelled by security levels, and information is allowed to flow from one object to another if the source object has a lower confidentiality level than the target one. Moreover, he shows that this notion of secure information flow allows him to give natural semantics to various security-minded programming constructs, including declassification.

In the context of Petri Nets, Busi and Gorrieri [12] applied the notion of non-interference to Elementary Net Systems, as we will see in next section, and Best, Darondeau and Gorrieri [8] extended recently the results to unbounded P/T Systems.

In these latter works, non-interference is basically defined as language equivalence. The equivalent languages are, respectively, the one generated by the restriction of the system to the low-level component alone, and the language generated by the composition of the low-level component with any high-level component.

The definition of non interference in terms of languages forces at considering events as basic observable entities, but this is partly in contradiction with the traditional view of events in Nets as entities observable only indirectly, via the modifications of their pre- and post-conditions.

We consider as basic observables entities the local properties of systems represented by conditions and we call the property we describe visibility. In terms of visibility, two interacting systems can be seen as defender and attacker. The defender offers a service to the environment and wants to keep secret part of its local states. The attacker uses the service of the defender and tries to get information about its internal local states.

In some way, our definition is similar to the one in [39], but our idea is that, even if we can see only a subset of the conditions of the system, we can observe not only the cases completely observable, but also a part of the other cases.

6.1 Observability of states in Petri Nets

We consider systems as divided in a high part and a low one. The high one should be hidden to the low part. *Non-interference* has been defined in the literature as a property based on some observational semantics: the high part of a system is non-interfering with the low part if whatever is done at the high level produces no visible effect on the low part of the system.

Busi and Gorrieri bring this approach in the field of Petri Nets [12]; in their work, security properties are based on the dynamics of systems: all their definitions use one (or more) equivalence check(s). Hence, non-interference checking is as difficult as equivalence checking, a well-studied hard problem in concurrency theory. They analyse systems, modeled by safe P/T nets, that can perform two kinds of actions: high level actions, representing the interaction of the system with high level users, and low level actions, representing the interaction with low level users. They want to verify if the interplay between the high user and the high part of the system can affect the view of the system as observed by a low user. They assume that the observer knows the structure of the system, and they check if, in spite of this, he is not able to infer the behavior of the high user by observing the low view of an execution of the system. They define properties characterizing the security of systems:

- *Strong Nondeterministic Non-Interference* (SNNI) is a trace-based property, that intuitively says that a system is secure if what the low part can see does not depend on what the high level part sees

$$N \approx_{tr}^{\Lambda} N \setminus H$$

where $\approx_{tr}^{\Lambda}$ is the trace equivalence as sees by the low user and $N \setminus H$ is the system without the high events.

- *Nondeducibility on Composition* (NDC) is a trace-based property and says that the low view of a system N in isolation is not to be altered when considering each potential interaction of N with the high users of the external environment

  $$\forall \text{ high-level Net } K : N \setminus H \approx_{tr}^{\Lambda} (N \mid K) \setminus (H \setminus H_K)$$

  where $N \mid K$ is the parallel composition of N and K.

- *Bisimulation SNNI* (BSNNI) is similar to SNNI but use a kind of bisimulation that considers low-view traces of the systems

  $$N \approx_{bis}^{\Lambda} N \setminus H \qquad \text{BSNNI} \subseteq \text{SNNI}$$

  where $\approx_{bis}^{\Lambda}$ is the weak bisimulation equivalence on the events of the low user.

- *Bisimulation NDC* (BNDC)

  $$\forall \text{ high-level Net } K : N \setminus H \approx_{bis}^{\Lambda} (N \mid K) \setminus (H \setminus H_K)$$

- *Strong BNDC* (SBNDC) is an alternative characterization of BNDC which is practically checkable

  $$\begin{array}{lcl} \forall m \in [m_0\rangle, \forall h \in H & : & m\,[h\rangle\, m' \Rightarrow \exists \text{ low-view bisimulation} \\ & & \text{R: } N \rightarrow N \setminus H \text{ s.t. } (m, m') \in \text{R} \end{array}$$

To recognize if a system has one of these properties they define two other kinds of properties. These properties permits to check if the system contains some condition that flows information between high and low users.

- A condition s of N such that $s^\bullet \cap L = \emptyset$ is a *potentially causal condition* if it link a high event to a low one, ${}^\bullet s \cap H = \emptyset$. A potentially causal condition s is a *causal condition* if it is marked in the initial marking and there is an event sequence that contains two of its low post events, if $m_0(s) > 0$ then there exists an event sequence $t_1 \dots t_n$ and $i < n$ s.t. $t_i, t_n \in s^\bullet \cap L$.

  A condition s of N such that $s^\bullet \cap L = \emptyset$ is a *conflict condition* if it is a precondition of an high event, $s^\bullet \cap H = \emptyset$.

  N is *Place Based Non-Interference* (PBNI) if, for all s $\in$ S, s is neither a causal condition nor a conflict condition.

- Causal region and conflict region are defined in a similar way. N is *Region-Based Non-Interference* (RBNI) if, for all regions $r \in Reg(MG(N))$, r is neither a causal region nor a conflict region. If N is RBNI then N is also PBNI. N is RBNI iff $Sat(MG(N))$ is PBNI.

These two properties, PBNI and RBNI, are structural because no notion of observational equivalence is considered in their definition; however, to be precise, the definition of RBNI requires an exploration of the state space (marking graph), hence it is in some sense a behavioural property.

The main results of Busi and Gorrieri [12] are:

- N is SNNI iff N is NDC,
- if N is BNDC then N is BSNNI,
- N is BNDC iff N is SBNDC,
- if N has no causal conditions then N is SNNI,
- if N is PBNI then N is SBNDC,

These concepts have been implemented in a software tool [21].

6.2 Visibility

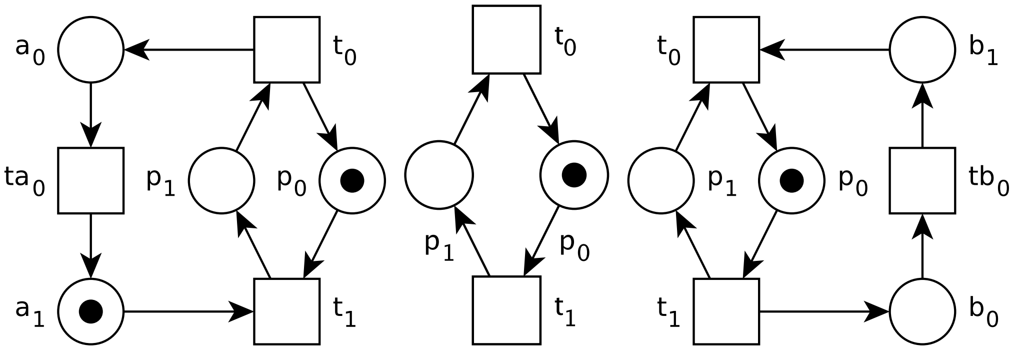
In our approach we consider an Elementary Net System, $N = N_D\langle N_I\rangle N_A = (B, E, F, m_0)$, made by two subsystems. The *defender*, $N_D = (B_D, E_D, F_D, m_0^D)$, is a high-level system that offers a service to the environment through an interface. The *attacker*, $N_A = (B_A, E_A, F_A, m_0^A)$, is a low-level system that wants to use the service and wants to infer something on the defender system or wants to control it. Let $(\beta_i, \eta_i) : N_i \to N_I$ and $(\gamma_i, \delta_i) : N \to N_i$ be $\widehat{N}$-morphisms that connect the systems.

We assume that the defender wants to take hidden part of his local conditions. We do not want that the attacker infer something about that conditions of the defender. In our approach the observer (the attacker) is able to see only a part of the system: the part of the composed system that mirrors itself and the interface [19].

As an example, consider the three Elementary Net Systems shown in Fig. 6.1.

We compose the Net N_1 and N_2 using the interface N_I. The label suggest the correspondence given by the morphisms; the resulting Net is shown in Fig. 6.2.

We want to know if a modification of the internal state of the defender can affect the view of the system as observed by the observer. We assume that the



(a) N_1 (b) N_I (c) N_2

Figure 6.1: The two Net to be composed through the Net interface

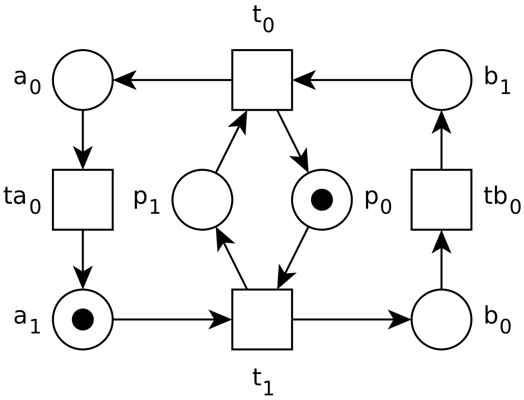


Figure 6.2: The composed Net

observer knows the structure of the system, and we want to know if he is not able to infer the internal state of the defender by observing how the execution of the system changes the state of the part of the system he is able to observe.

The non-interference properties we want to define use the notion of observability of low conditions of a system, i.e., what can be observed of a system from the point of view of the observer.

We can now be more precise about what the attacker can infer about the validity of conditions of the whole system.

Definition 66. *The* attacker-view *of a marking m of the system N is the restriction of the marking on the conditions of N_A and N_I:*

$$\forall m \in [m_0\rangle\,, m_{\upharpoonright_{I\cup A}} = m \cap (B_A \cup B_I)$$

In general, the attacker is able to distinguish only subsets of markings of the composed system.

Definition 67. *We say that two distinct markings $m, m' \in [m_0\rangle$ are* attacker-view equivalent *if $m_{\upharpoonright_{I\cup A}} = m'_{\upharpoonright_{I\cup A}}$.*

A marking $m \in [m_0\rangle$ is distinguishable *by the attacker if $\nexists m' \in [m_0\rangle : m_{\upharpoonright_{I\cup A}} = m'_{\upharpoonright_{I\cup A}}$.*

The attacker has a complete distinguishability *of the markings of the whole system if:*

$$\forall m, m' \in [m_0\rangle\,, m_{\upharpoonright_{I\cup A}} = m'_{\upharpoonright_{I\cup A}} \Rightarrow m = m'$$

The interesting cases are those in which there is no complete distinguishability. We define as follows the conditions visible or invisible to the attacker.

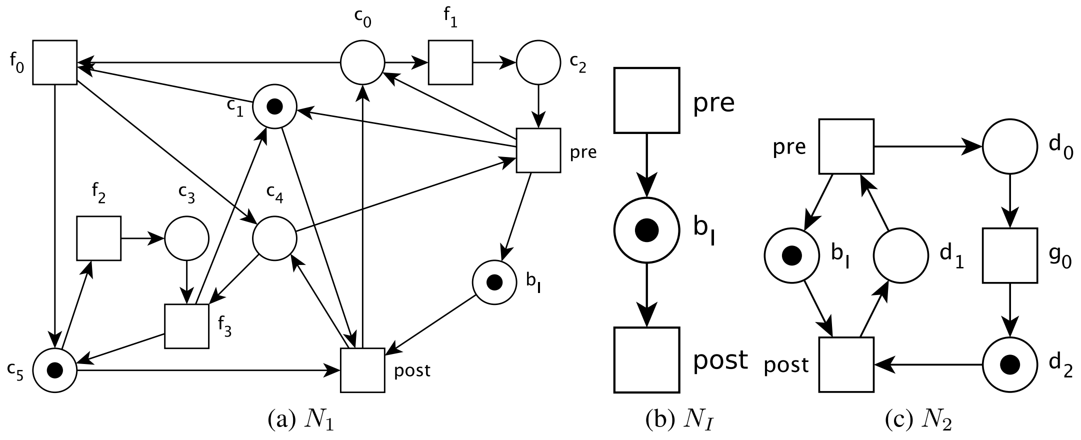
Definition 68. *A condition $p \in B_D \setminus B_I$ is* invisible at a marking *$m_A \in [m_0^A\rangle$ by an attacker N_A in isolation iff*

$$\exists\, m, m' \in [m_0\rangle : m(p) = 0 \wedge m'(p) = 1 \wedge m_{\upharpoonright_{I\cup A}} = m'_{\upharpoonright_{I\cup A}} = m_A$$

Condition $p \in B_D \setminus B_I$ is invisible *by N_A iff p is invisible for every $m_A \in [m_0^A\rangle$. If a condition is not invisible then we say that it is visible.*

We call $S_D \subseteq B_D \setminus B_I$ the set of invisible conditions computed as in the procedure reported below for *an* attacker N_A, in the system $N = N_D\langle N_I\rangle N_A$.

We call $S_D^* \subseteq B_D \setminus B_I$ the set of invisible conditions by *all* attacking Net Systems N_A, in the system $N = N_D\langle N_I\rangle N_A$.



(a) N_1 (b) N_I (c) N_2

Figure 6.3: Two Nets to be composed through the Net interface

6.2.1 Invisible conditions

To determine which conditions are in S_D we follow this procedure:

- partition the reachable markings of the composed system according to the markings of the attacker;
- for each marking of the attacker, compute the invisible conditions and
- compute the intersection of the sets of invisible conditions above.

Since the computation of all the markings of a Petri Net is exponential, to find the set of invisible conditions is an exponential computation too.

Let us explain this procedure by means of the example of Fig. 6.3. The morphisms from the Nets in Fig. 6.3a and 6.3c to the one in Fig. 6.3b are given by identical names; the composed Net is shown in Fig. 6.4.

We use the markings of the composed system, shown in Table 6.1, and of the attacker, Table 6.2, to compute S_D. Starting by the markings of the attacker N_2, let us partition the markings of the composed system in sets of undistinguishable markings as in Table 6.2. The same Table lists also the conditions invisible by each marking of the attacker; the conditions invisible for N_2 are $\{c_{0N3}, c_{2N3}\}$, given by the intersection of all of the computed S_D sets.

To compute S^*_D we deal with every possible attacker compatible with the interface N_I with respect to the composition operation. We conjecture that the conditions invisible by the interface (or to an attacker isomorphic to the interface) allow to infer an upper bound to the set S^*_D. The cases in which the attacker is bisimilar to the interface are discussed below.

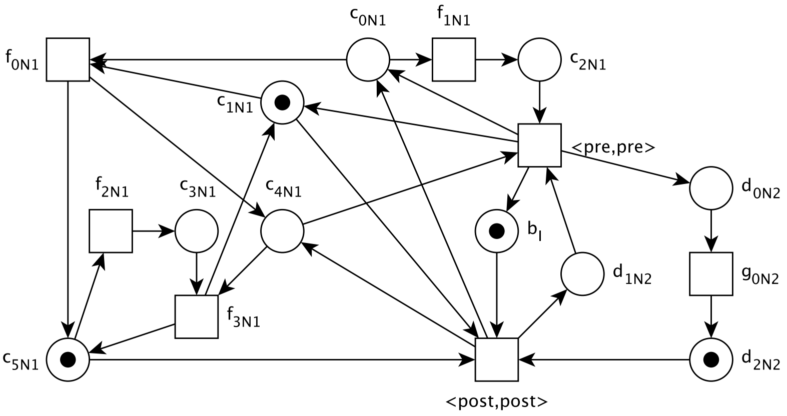


Figure 6.4: The composition of the Nets of Fig. 6.3

	c_{0N3}	c_{1N3}	c_{2N3}	c_{3N3}	c_{4N3}	c_{5N3}	b_I	d_{0N4}	d_{1N4}	d_{2N4}
S_0	0	1	0	0	0	1	1	0	0	1
S_1	1	0	0	0	1	0	0	0	1	0
S_2	0	1	0	1	0	0	1	0	0	1
S_3	0	0	1	0	1	0	0	0	1	0
S_4	1	1	0	0	0	0	1	1	0	0
S_5	1	1	0	0	0	0	1	0	0	1
S_6	0	1	1	0	0	0	1	1	0	0
S_7	0	0	0	0	1	1	1	1	0	0
S_8	0	1	1	0	0	0	1	0	0	1
S_9	0	0	0	0	1	1	1	0	0	1
S_{10}	0	0	0	1	1	0	1	1	0	0
S_{11}	0	0	0	1	1	0	1	0	0	1
S_{12}	0	1	0	0	0	1	1	1	0	0
S_{13}	0	1	0	1	0	0	1	1	0	0

Table 6.1: Reachable states of system $N_1\langle N_I 2\rangle N_2$ of Fig. 6.4

	b_I	d_0	d_1	d_2	possible markings of the composed system	conditions invisible
S_{0A}	1	0	0	1	S_0, S_2, S_5, S_8, S_9, S_{11}	$\{c_{0N3}, c_{1N3}, c_{2N3}, c_{3N3}, c_{4N3}, c_{5N3}\}$
S_{1A}	0	0	1	0	S_1, S_3	$\{c_{0N3}, c_{2N3}\}$
S_{2A}	1	1	0	0	S_4, S_6, S_7, S_{10}, S_{12}, S_{13}	$\{c_{0N3}, c_{1N3}, c_{2N3}, c_{3N3}, c_{4N3}, c_{5N3}\}$

Table 6.2: Reachable states of system N_2 of Fig. 6.3c

	a_0	a_1	p_0	p_1	b_0	b_1	$\mathbf{I}\cdot m_0$
$\mathbf{I}_1$	0	0	1	1	0	0	1
$\mathbf{I}_2$	1	1	0	1	0	0	1
$\mathbf{I}_3$	0	0	1	0	1	1	1
$\mathbf{I}_4$	1	1	0	0	1	1	1

(a) $N_1\langle N_I\rangle N_2$

	p_0	p_1	$\mathbf{I}\cdot m_0$
$\mathbf{I}_1^I$	1	1	1

(b) N_I

	a_0	a_1	p_0	p_1	$\mathbf{I}\cdot m_0$
$\mathbf{I}_1^a$	0	0	1	1	1
$\mathbf{I}_2^a$	1	1	0	1	1

(c) N_1

	p_0	p_1	b_0	b_1	$\mathbf{I}\cdot m_0$
$\mathbf{I}_1^b$	1	1	0	0	1
$\mathbf{I}_3^b$	1	0	1	1	1

(d) N_2

Table 6.3: The invariants of the Nets of Fig. 6.1 and 6.2

6.2.2 Invariants

We focus now on the study of what we can infer using invariant properties.

We see in Table 6.3 the invariants of the Nets of Fig. 6.1 and 6.2. Each row represent an invariant on the conditions of the net and its last value is the number of token the invariant contains. We see that the S-invariant $\mathbf{I}_1^I$ is reflected in $\mathbf{I}_1^a, \mathbf{I}_1^b, \mathbf{I}_1$, the S-invariant $\mathbf{I}_2^a$ is reflected in $\mathbf{I}_2$ and $\mathbf{I}_3^b$ is reflected in $\mathbf{I}_3$. $\mathbf{I}_4$ is not preserved in N_1 and N_2.

Looking at the invariants of the composed Net we can infer something on the marking of the subsystems without directly observe their local states.

For example, take the initial marking of $N_1\langle N_I\rangle N_2$

$$m_0 = (011000)$$

and the invariant

$$\mathbf{I}_2 = (110100)$$

Now, project m_0 on $m_{0\downharpoonright_{I\cup A}}$, the marking observable by N_2:

$$m_{0\downharpoonright_{I\cup A}} = (1000)$$

Which is the simpler hypothesis that N_2 could make on the marking of $N_1\langle N_I\rangle N_2$? It could hypothesize that in all the conditions that he is not able to observe there are no tokens. Let us call this “operator of extension” $ext(m_i) : B_i \to B$, this operator puts a zero for all the elements that were cancelled by the projection operator, in the original position:

$$ext(m_{0\downharpoonright_{I\cup A}}) = (001000)$$

Now, do the product:

$$\mathbf{I}_2^T \bullet ext(m_{0\downharpoonright_{I\cup A}}) = \begin{pmatrix}1\\1\\0\\1\\0\\0\end{pmatrix} \bullet (001000) = 0$$

but N_2 knows that this product gives 1. So, N_2 infer that in one of the 2 new elements of $ext(m_{0\downharpoonright_{I\cup A}})$ (the first two) there must be 1. N_2 hypothesizes that the true marking of $N_1\langle N_I\rangle N_2$ can be either (011000) or (101000). N_2 has gained information through the use of the invariants and the *attacker-view* of a marking.

Table 6.4 presents all the possible inferences we can do using the invariants in case of partial observation of N_2. The cell colored in green are components of the invariants.

Definition 69. *For $i = D, A, I$, let $N_i = (B_i, E_i, F_i, m_0^i)$ and $N = N_D\langle N_I\rangle N_A = (B, E, F, m_0)$ be Elementary Net Systems and let $(\gamma_i, \delta_i) : N \to N_i$ be an $\widehat{N}$-morphism. Let*

- *$\mathfrak{I}_b^D$ be the set of all the basic invariants that contain local conditions of N_D,*
- *$\mathfrak{I}_b^{A\cup I}$ be the set of all the basic invariants that contain conditions of N_A,*
- *$\mathfrak{I}_b^\star$ be the set of all the basic invariants that contain conditions of N_D and N_A, in other words the basic invariants concerning N_D and visible by the attacker:*

$$\mathfrak{I}_b^\star = \mathfrak{I}_b^D \cap \mathfrak{I}_b^{A\cup I}$$

We are interested in all the invariants $\mathbf{I} \in \mathfrak{I}_b^\star$ and we can see these invariants as composed of three parts:

$$\mathbf{I} = \mathbf{I}_{\downharpoonright_D} \cup \mathbf{I}_{\downharpoonright_I} \cup \mathbf{I}_{\downharpoonright_A}$$

Note that, in every invariant, $\mathbf{I}_{\downharpoonright_I}$ or $\mathbf{I}_{\downharpoonright_A}$ shall be equal to $\underline{0}$ because these invariants can only concern N_D or be invariants of both subnets, created in the composition (and that do not concern the interface).

For a marking m of the composed system we are able to infer some information about the validity of some defender's conditions in the following way:

- $(\exists \mathbf{I} \in \mathfrak{I}_b^\star, \|m_{\downharpoonright_A} \cdot \mathbf{I}_{\downharpoonright_A}\|_1 + \|m_{\downharpoonright_I} \cdot \mathbf{I}_{\downharpoonright_I}\|_1 < \|\mathbf{I} \cdot m_0\|_1) \Rightarrow \exists c \in I_{\downharpoonright_D} : m(c) > 0$
- $(\exists \mathbf{I} \in \mathfrak{I}_b^\star, \|m_{\downharpoonright_A} \cdot \mathbf{I}_{\downharpoonright_A}\|_1 + \|m_{\downharpoonright_I} \cdot \mathbf{I}_{\downharpoonright_I}\|_1 = \|\mathbf{I} \cdot m_0\|_1) \Rightarrow \forall c \in I_{\downharpoonright_D} : m(c) = 0$

	a_0	a_1	p_0	p_1	b_0	b_1	Product result
Marking m_0 of $N_1\langle N_I\rangle N_2$	0	1	1	0	0	0	
m_0 observed from N_2	0	0	1	0	0	0	
$\mathbf{I}_2$	0	0	0	0	0	0	0
$\mathbf{I}_4$	0	0	0	0	0	0	0

(a)

	a_0	a_1	p_0	p_1	b_0	b_1	Product result
Marking m_1 in $N_1\langle N_I\rangle N_2$	0	0	0	1	1	0	
m_1 observed from N_2	0	0	0	1	1	0	
$\mathbf{I}_2$	0	0	0	1	1	0	1
$\mathbf{I}_4$	0	0	0	1	1	0	1

(b)

	a_0	a_1	p_0	p_1	b_0	b_1	Product result
Marking m_2 in $N_1\langle N_I\rangle N_2$	0	0	0	1	0	1	
m_2 observed from N_2	0	0	0	1	0	1	
$\mathbf{I}_2$	0	0	0	1	0	1	1
$\mathbf{I}_4$	0	0	0	1	0	1	1

(c)

	a_0	a_1	p_0	p_1	b_0	b_1	Product result
Marking m_3 in $N_1\langle N_I\rangle N_2$	1	0	1	0	0	0	
m_3 observed from N_2	0	0	1	0	0	0	
$\mathbf{I}_2$	0	0	1	0	0	0	0
$\mathbf{I}_4$	0	0	1	0	0	0	0

(d)

Table 6.4: Example of markings of $N_1\langle N_I\rangle N_2$

In the Net of Fig. 6.2 the interesting invariants are $\mathfrak{I}_b^\star = \{\mathbf{I}_2, \mathbf{I}_4\}$. We see in Table 6.4a that N_2 infers that a_0 or a_1 is marked.

Therefore the attacker is able to make assertions on the possible states the whole system is in. However, as we have seen above, the attacker is able to make assertions only on certain conditions of the defender. This way the attacker is able to construct a range of possible markings of the whole system.

In the above example N_2 hypothesizes that the original marking is (011000) or (101000).

But in a real system the set of possible markings is larger and also is too difficult to construct the set of reachable markings. Checking the reachability of a marking is NP-complete, while a sufficient condition for non reachability of a given marking $m \in S$ is non existence of $\sigma' \in \mathbb{Z}^{|T|}$ such that $C \cdot \sigma' = m - m_0$, which is polynomial time [42]. Using this remark, the attacker can reject some of the possible markings, in the best case remaining with only one possible marking.

We can also assert that under certain constraints the attacker is always able to block the defender choosing not to fire some event. For example, in the system shown in Fig. 6.2, the attacker is able to decide to not fire the event f_0. So, when, in the composed system, the event t_1 fires, the attacker, with its decision of not doing an action, blocks the whole system.

Is it possible to decide how much a defender is dependent or independent on its interface? In a very simple way we can decide if a system is dependent on its interface in the following way:

Definition 70. *Let $b, c \in B$; we say that b* weakly covers *c if it exists a basic invariant $\mathbf{I}$ that contains b and c.*

A condition $b \in S$ weakly covers *a set of conditions C if it weakly covers each condition $c_i \in C$.*

If $b \in B_I$ weakly covers all the conditions of the defender, B_D, we say that the defender is weakly dependent *from the interface.*

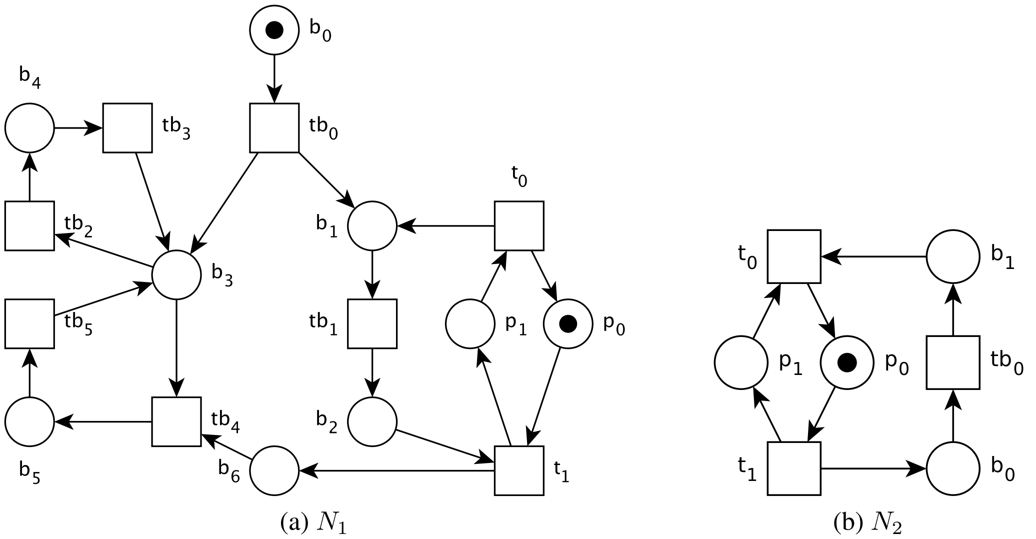
If we restrict the above definitions using only monomarked invariants, we use the word cover.

Let $S_{\notin} \subseteq B_D$ be the set of all the conditions of the defender not covered by conditions of the interface:

$$S_{\notin} = \{p \in B_D : \nexists b \in B_I, b \text{ covers } p\}$$

In the Net of Fig. 6.2, as we see from the invariants shown in Table 6.3c, we say that N_1 depends from the interface through p_1.

In Fig. 6.5 we see a Net, 6.5a, that is not covered by any condition of the interface and, so, that is not dependent from the interface.



(a) N_1

(b) N_2

Figure 6.5: Two Nets to be composed through the Net interface shown in Fig. 6.3b

p_0	p_1	b_0	b_1	b_2	b_3	b_4	b_5	b_6	$\mathbf{I} \cdot m_0$
0	0	1	0	0	1	1	1	0	1
1	0	1	1	1	0	0	0	0	1
1	1	0	0	0	0	0	0	0	1

(a) Invariants of the Net in Fig. 6.5a

p_0	p_1	b_0	b_1	$\mathbf{I} \cdot m_0$
0	1	1	1	1
1	1	0	0	1

(b) Invariants of the Net in Fig. 6.5b

Table 6.5: The invariants of the Nets of the Fig. 6.5

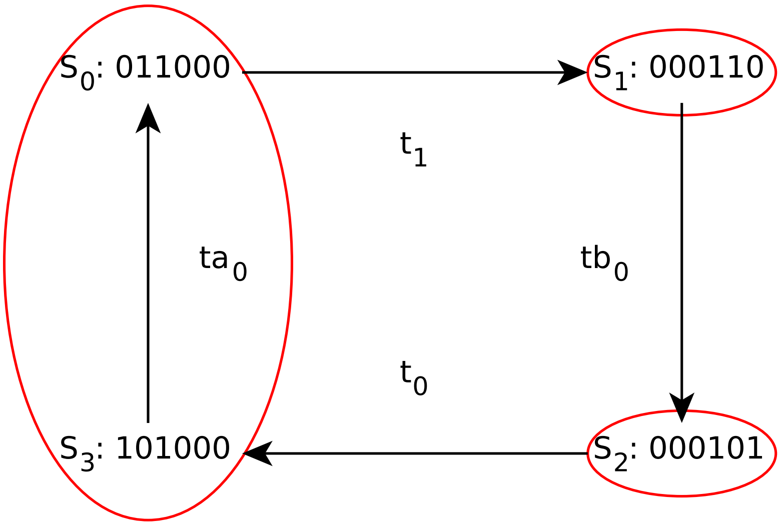


Figure 6.6: The reachability graph of the Net of Fig. 6.2 with the observability of the attacker

The dependence condition is sufficient to assert that there exists an attacker able to block the defender, however we don't know if it necessary. And, more important, is the contrary true? If a Net is not dependent on the interface is that Net independent? Is it impossible to block an independent Net?

We conjecture that it is not possible to block a non-dependent Net. This is because, informally, the attacker is able to block the interface but in this case this is not sufficient to block the defender. How can we formally prove this aspect?

Proposition 52. *For $i = D, A, I$, let $N_i = (B_i, E_i, F_i, m_0^i)$ and $N = N_D\langle N_I\rangle N_A = (B, E, F, m_0)$ be Elementary Net System and let $(\gamma_i, \delta_i) : N \to N_i$ be an $\widehat{N}$-morphism. Let G_i denote the domain of the partial function η_i.*

If there is a reachable marking $m_b \in [m_0\rangle$ that is distinguishable for the attacker and that enables only events local to the attacker

$$\forall e \in E | m_b [e\rangle, e \notin ((E_1 \setminus G_1) \cup E_{sync})$$

then we say that the attacker blocks *the whole system.*

We also check this condition in a graphical way by using the reachability graph. We have to modify the graph in order to underline the observability of the attacker, as we see in Fig. 6.6.

We see that N_2 blocks the system in the marking S_1 not firing tb_1.

It is possible for a defender to expose an interface that do not permits the creation of unwanted invariants? With this composition it is impossible to generate

c_0	c_1	c_2	c_3	c_4	c_5	b_I	$\mathbf{I} \cdot m_0$
0	1	0	0	1	0	0	1
1	0	1	1	0	1	0	1

Table 6.6: The invariants of the Nets of Fig. 6.3a

b_0	b_I	b_1	b_2	$\mathbf{I} \cdot m_0$
1	1	1	1	1

Table 6.7: The invariants of the Nets of Fig. 6.7a

new T-invariants in the composition. As we see in Theorem 1, all the invariants of the composed Net are reflected in invariants of the subnets. So with this composition we only resolve global conflicts in local way.

Now we show that, even if a condition of the defender is not covered by a condition of the interface, it is possible that this condition is visible, that is $S_D \neq S_{\not c}$.

The invariants of the Net in Fig. 6.3a are listed in Table 6.6. As we see, no one of the conditions of N_1 are in an invariant with the only condition of the interface, so $S_{\not c} = \{c_0, c_1, c_2, c_3, c_4, c_5\}$ so how can be possible that one of these condition is visible by the attacker?

Nevertheless, consider all the markings of the attacker, N_2, listed in Table 6.2 and the markings of the composed system, listed in Table 6.1. The condition c_4 of the defender, that is in $S_{\not c}$, is visible because in the marking $S1_A$ the attacker is sure that there is a token in c_4 because there are no markings of the composed system in which c_4 is not marked and such that this marking is seen as $S1_A$ by the attacker.

So, now we know that $S_{\not c} \neq S_D$ and that $S_{\not c} \nsubseteq S_D$.

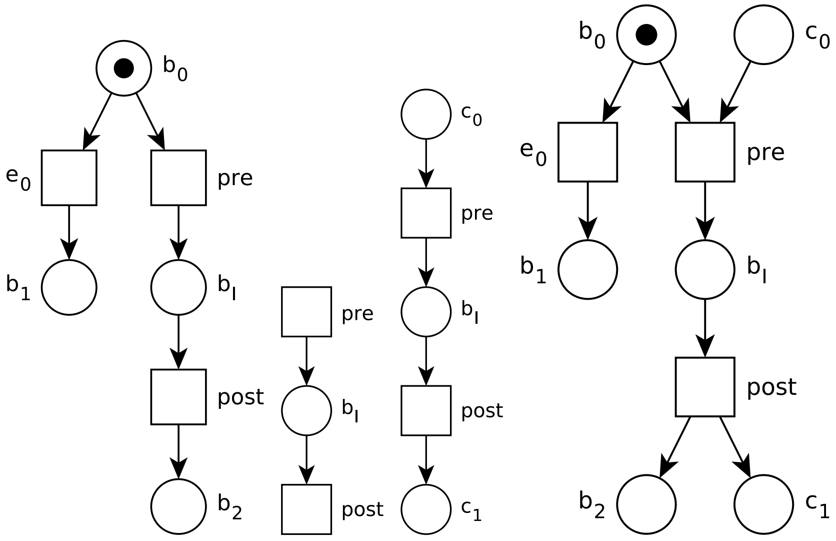
Let us show you another example. In Fig. 6.7 you see the defender (6.7a), the attacker (6.7c) and the interface (6.7b).

The morphisms from the Nets in Fig. 6.7a and 6.7c to the one in Fig. 6.7b are given by identical names; the composed Net is shown in Fig. 6.7d.

The invariants of 6.7a are listed in Table 6.7. As we see, all the conditions of N_1 are in an invariant with the only condition of the interface, so $S_{\not c} = \phi$ and how can be possible that one of these condition is invisible by the attacker?

Nevertheless, consider the only marking of the attacker, N_2, $c_0 = 0, b_I = 0, c_1 = 0$, and the markings of the composed system, listed in Table 6.8. The conditions b_0 and b_1 of the defender, that are not in $S_{\not c}$, are invisible because the only marking of the attacker correspond to all the markings of the composed Net and in these markings b_0 and b_1 are once marked and once not.

Now we are able to say that $S_D \nsubseteq S_{\not c}$.



(a) N_1 (b) N_I (c) N_2 (d) $N_1\langle N_I\rangle N_2$

Figure 6.7: Two Nets to be composed through the Net interface and the resulting Net

	b_0	b_1	b_2	b_I	c_0	c_1
$S0$	1	0	0	0	0	0
$S1$	0	1	0	0	0	0

Table 6.8: The markings of the Nets of Fig. 6.7d

6.2.3 Invisible and visible conditions: results

Let us now prove the central result. We define a necessary constraint for a defined attacker N_A such that a condition of the defender is not in S_D. This happens when a condition of the defender is in a monomarked invariant with a condition of the interface. In this case, it is possible to construct an attacker (isomorphic to the interface itself) with a marking in which that condition is visible.

Theorem 12. *Let N_D, N_I be bisimilar Elementary Net Systems, and $(\beta_D, \eta_D) : N_D \to N_I$ an $\widehat{N}$-morphism. If N_I is 1-live and $b \in B_D \setminus \beta_D^{-1}(B_I), i \in \beta_D^{-1}(B_I)$ satisfies $b, i \in \mathbf{I_D}$ with $\mathbf{I_D}$ monomarked S-invariant of N_D, then b is visible by each attacker bisimilar to the interface.*

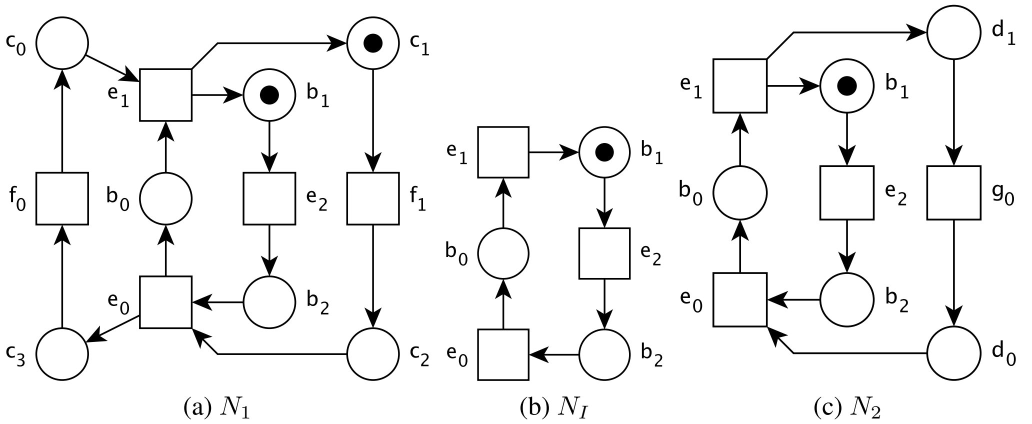
Proof. Consider an attacker isomorphic to the interface, $N_A = N_I$. Given that we consider each attacker bisimilar to the interface, if we prove that this result holds for the interface, it holds for all these attackers too.

Since S-invariants are reflected, $\mathbf{I_D}$ is an invariant of the composed Net (that in this case is isomorphic to N_D). So, if we reach a marking m in which $m(i) = 1$ then we are sure that $m(b) = 0$ and then b is visible. If $m_0(i) = 1$ this is the marking we are looking for. Suppose $m_0(i) = 0$. Since N_I is an Elementary Net System, $\beta_D(i)$ is not isolated. If ${}^\bullet\beta_D(i) = \varnothing$, then $\beta_D(i)$ should have at least a post-event. In this case this post-event is dead while N_I is 1-live by hypothesis. So, the preset of $\beta_D(i)$ is not empty. Given that N_I is 1-live, an event in the preset of $\beta_D(i)$ fires at some reachable case. Let us call $u \in E_I^*$ a sequence of events such that $m_0^I\,[u\rangle\, m_1^I$ and $m_1^I(\beta_D(i)) = 1$. From the assumption that $N_D \approx N_I$ with the labelling function $h : E_D \to E_I \cup \{\tau\}$ we deduce that $\exists w \in E_D^* : h(w) = u, m_0^D\,[w\rangle\, m_1^D, m_1^D(i) = 1$. ◇

The Theorem does not state conditions of bisimilarity between the attacker and the interface. Nevertheless, an attacker not bisimilar to the interface is of no interest since it can introduce some limitations of behaviour of the composed system and hide to itself some visible parts of the defender.

As an example, in Fig. 6.8 (where the $\widehat{N}$-morphisms are implicitly defined by the identical labels on conditions and events), the attacker is not bisimilar to the interface and event $\langle e_0, e_0\rangle$ of the composed system is dead. Conditions c_3 and c_4 are visible by the attacker, as we see in Fig. 6.9 and Tables 6.10 and 6.9. Instead, if we modify the initial marking for the attacker N_2 by adding a token in condition d_1, the attacker becomes bisimilar to the interface. In this case, conditions c_1 and c_2 of N_1 become visible together with c_3 and c_4.

The explicit request in the Theorem for a defender bisimilar to the interface is motivated by the fact that the interface is the protocol of interaction of the defender with the other systems. Consequently, it is reasonable to expect that the defender



(a) N_1 (b) N_I (c) N_2

Figure 6.8: Two Elementary Net Systems to be composed through the interface N_I

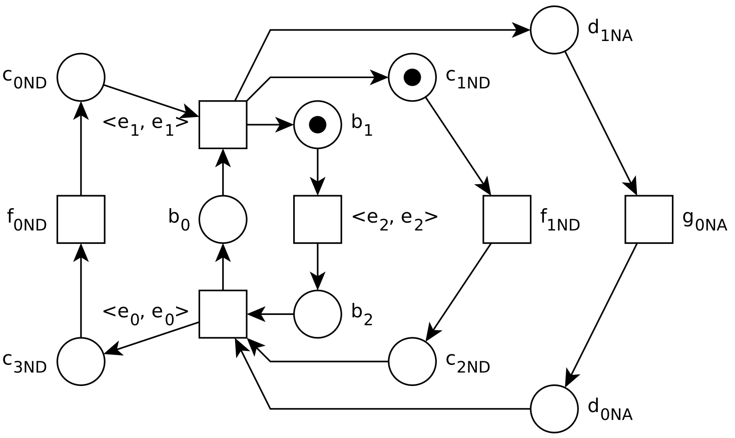


Figure 6.9: The composition of the Elementary Net Systems of Fig. 6.8

	b_0	b_1	b_2	d_0	d_1	possible markings of the composed system	invisible conditions
S_{0A}	0	1	0	0	0	S_0, S_2	$\{c_{1ND}, c_{2ND}\}$
S_{1A}	0	0	1	0	0	S_1, S_3	$\{c_{1ND}, c_{2ND}\}$

Table 6.9: Reachable states of system N_1 of Fig. 6.8a

	b_0	b_1	b_2	c_{0ND}	c_{1ND}	c_{2ND}	c_{3ND}	d_{0NA}	d_{1NA}
S_0	0	1	0	0	1	0	0	0	0
S_1	0	0	1	0	1	0	0	0	0
S_2	0	1	0	0	0	1	0	0	0
S_3	0	0	1	0	0	1	0	0	0

Table 6.10: Reachable states of system $N_1\langle N_I\rangle N_2$ of Fig. 6.9

respects its own contract with the environment. The request for a live interface is reasonable as well for the same motivation. Finding an S-invariant containing a condition of the interface and a condition local to the defender is necessary to establish a channel that brings information from the local part of the defender to a part shared with the attacker. Computing the minimal invariants of a Net is an NP-complete problem [14], nevertheless, several tools compute it. For instance CPN-AMI, GreatSPN, mist2, Petruchio, Platform Independent Petri Net Editor, PNetLab, ProM framework.

6.2.4 Measuring visibility

In this section, we sketch a first attempt to give a measure of the uncertainty related to visibility. Intuitively, visible or invisible conditions are opposite ends of some kind of *spectrum* of visibility and, in Def. 68, we do not weight the relative persistence of the invisible condition p in marking m or m'.

For example, in Table 6.2, attacker case S_{0A}, condition b_{0N3} is more frequently un-marked than marked. Consequently, we could consider b_{0N3} as a random variable whose average information content - persistence in a given local state - depends on the chosen marking of the attacker.

Traditionally, entropy is a measure of the uncertainty associated with a random variable. Consequently, a measure of the uncertainty of the marking for a given defender condition in a given attacker marking can be given, as usual in information science, using Shannon's entropy:

the entropy H of a discrete random variable $X = \{x_1, ..., x_n\}$ with p denoting the probability mass function of X is $H(X) = -\sum_{i=1}^{n} p(x_i)\log_2 p(x_i)$.

For example, with reference to Table 6.2, let us calculate the entropy of b_{0N3} seen as variable with possible values in $\{0, 1\}$ with respect to the attacker marking S_{0A}. Marking S_{0A} "covers" $\{S_0, S_2, S_5, S_8, S_9, S_{11}\}$ and, with reference to Table 6.1, we can divide this set in two subsets: one in which $b_{0N3} = 0$, $\{S_0, S_2, S_8, S_9, S_{11}\}$, and one with $b_{0N3} = 1$, $\{S_5\}$. By plain computation of the relative frequencies of persistence in a state, the entropy is $H(b_{0N3}) = -\sum_{i=1}^{2} p(x_i)\log_2 p(x_i) =$

$-5/6\log_2 5/6 - 1/6\log_2 1/6 = 0,65$. So b_{0N3} in S_{0A} is invisible at 65%.

6.3 Classes of systems

Definition 71. *The* attacker-view *of a marking sequence $ms = m_1 \dots m_n$ of the system N is the sequence of the attacker-view of every marking $m_i, 1 \le i \le n$ of ms, if this view is different from the previous one:*

$$\epsilon_{\downharpoonright_{I\cup A}} = \epsilon$$

$$ms_{\downharpoonright_{I\cup A}} = \begin{cases} \{m_1 \dots m_{n-1}\}_{\downharpoonright_{I\cup A}} m_{n\downharpoonright_{I\cup A}} & \textit{if } m_{n\downharpoonright_{I\cup A}} \neq m_{n-1\downharpoonright_{I\cup A}} \\ \{m_1 \dots m_{n-1}\}_{\downharpoonright_{I\cup A}} & \textit{otherwise} \end{cases}$$

Definition 72. *Two marking sequences $ms, ms' \in MS$ are* attacker-view equivalent *if $ms_{\downharpoonright_{I\cup A}} = ms'_{\downharpoonright_{I\cup A}}$.*

A marking sequence $ms \in MS$ is distinguishable *by the attacker if $\nexists ms' \in MS : ms_{\downharpoonright_{I\cup A}} = ms'_{\downharpoonright_{I\cup A}}$.*

Definition 73. *The attacker has a complete* distinguishability *of the marking sequences of the whole system if:*

$$\forall ms, ms' \in MS, ms_{\downharpoonright_{I\cup A}} = ms'_{\downharpoonright_{I\cup A}} \Rightarrow ms = ms'$$

Definition 74. *We say that N is* attacker-view equivalent *to N_A, denoted by $N \sim N_A$, iff $[m_0\rangle_{\downharpoonright_{I\cup A}} = [m_0^A\rangle$. In this case we say that N is* Nondeterministic Non-Visible *(NNV for short).*

We say that N is strong attacker-view equivalent *to N_A, denoted by $N \approx N_A$, iff $MS_{\downharpoonright_{I\cup A}} = MS_A$. In this case we say that N is* Strong Nondeterministic Non-Visible *(SNNV for short)*

Intuitively, the property Strong Nondeterministic Non-Visible says that a system is secure if what the attacker see does not depend on the fact that it is composed with the defender.

Now, take $N_D \approx^{BIS} N_I$ with r_D as bisimulation function

$$r_D = \{(m_D, m_I) : m_{D\downharpoonright_I} = m_I\}$$

and let E_I be a set of labels, with the label functions:

$$l_I \text{ is the identity function}$$

$$l_D = \eta_D \cup \{\forall e_D | \eta_D(e_D) = \text{ undefined }, (e_D, \tau)\}$$

then the Theorem 4.5 in [6] states that $N \approx^{BIS} N_A$ with r as bisimulation function

$$r = \{(m, m_A) : m_{\downharpoonright_{I \cup A}} = m_A\}$$

taking E_A as the set of labels, with the label functions:

$$l_A \text{ is the identity function}$$

$$l = \delta_A \cup \{\forall e | \delta_A(e) = \text{ undefined }, (e, \tau)\}$$

Theorem 13. *If $N_D \approx^{BIS} N_I$, N is NNV for every N_A.*

Proof.

- $[m_0\rangle_{\downharpoonright_{I \cup A}} \supseteq [m_0^A\rangle$?
  the existence of the bisimulation between N and N_A implies that

$$\forall m_A \in \left[m_0^A\right\rangle, \exists m \in [m_0\rangle : (m, m_A) \in r \Rightarrow m_{\downharpoonright_{I \cup A}} = m_A$$

- $[m_0\rangle_{\downharpoonright_{I \cup A}} \subseteq [m_0^A\rangle$?
  the existence of the bisimulation between N and N_A implies that

$$\forall m \in [m_0\rangle, \exists m_A \in \left[m_0^A\right\rangle : (m, m_A) \in r \Rightarrow m_{\downharpoonright_{I \cup A}} = m_A$$

◇

Theorem 14. *If $N_D \approx^{BIS} N_I$, N is SNNV for every N_A.*

Proof.

- $MS_{\downharpoonright_{I \cup A}} \supseteq MS_A$?
  by induction on the length of the marking sequence:

  base $\epsilon_{\downharpoonright_{I \cup A}} = \epsilon$

  induction step let us take a marking sequence $ms_A^n \in MS_A : ms_A^n = ms_A^{n-1} m_n^A$, by hypothesis $\exists ms^i \in MS : ms^i_{\downharpoonright_{I \cup A}} = ms_A^{n-1}, i \geq n-1$. Now, take the event $e_A \in E_A : m_{n-1}^A [e_A\rangle m_n^A$ and take the last marking of ms^i: $m_i, m_{i \downharpoonright_{I \cup A}} = m_{n-1}^A$; the bisimulation states that

$$\exists m \in [m_0\rangle, \exists v \in E^*, l_A(v) = e_A : m_i [v\rangle m, (m, m_n^A) \in r \Rightarrow m_{\downharpoonright_{I \cup A}} = m_n^A$$

  Assume that $v = e_1 \dots e_k e_A e_{k+1} \dots e_j$, with $e_z \in E_D \setminus G_D, z = 1 \dots j$ (otherwise the label function map the event in E_A). The construction of the composed Net assure that these events are pre or post only of local conditions of N_D, and so they do not change the projection of the marking.

  So, $ms_A^n = ms_A^{n-1} m_n^A = m_{i \downharpoonright_{I \cup A}} m_{\downharpoonright_{I \cup A}} = ms_{\downharpoonright_{I \cup A}}$.

- $MS_{\downharpoonright_{I\cup A}} \subseteq MS_A$?
  by induction on the length of the marking sequence:

  base $\epsilon_{\downharpoonright_{I\cup A}} = \epsilon$

  induction step let us take a marking sequence $ms^n \in MS : ms^n = ms^{n-1}m_n$, by hypothesys, we know that $\exists ms^i_A \in MS_A : ms^{n-1}_{\downharpoonright_{I\cup A}} = ms^i_A, i \leq n-1$. Now, take the event $e \in E : m_{n-1}\left[e\right\rangle m_n$, this event can be:

  - $e \in E_D \setminus G_D$ (the labelling function does not map it): the construction of the composed Net assure that this event are pre or post only of local conditions of N_D, and so it do not change the projection of the marking

$$m_{n\downharpoonright_{I\cup A}} = m_{n-1\downharpoonright_{I\cup A}} = m^A_i$$

$$ms^n_{\downharpoonright_{I\cup A}} = ms^{n-1}_{\downharpoonright_{I\cup A}} = ms^i_A$$

  - $e \in E \setminus (E_D \setminus G_D)$ (the labelling function does map it): the bisimulation states that

$$\exists m^A_{i+1} \in \left[m^A_0\right\rangle : m^A_i\left[e\right\rangle m^A_{i+1}, (m_n, m^A_{i+1}) \in r \Rightarrow m_{n\downharpoonright_{I\cup A}} = m^A_{i+1}$$

$$ms^n_{\downharpoonright_{I\cup A}} = ms^{n-1}_{\downharpoonright_{I\cup A}} m_{n\downharpoonright_{I\cup A}} = ms^i_A m^A_{i+1} = ms^{i+1}_A$$

◇

6.4 Final remarks on Observability

We aimed at defining structurally the notion of *visibility* between composed subsystems in order to isolate the unwanted information flows between a hypothetical *defender* system and an *attacker* system whose interactions are coordinated by an *interface*. In the context of information science, our work is naturally placed in the field of *non-interference* as reported in the introduction.

We managed to use traditional tools in the study of Petri Nets like *invariants*, for the definition of the properties of our interest. In the context of this work we did not use T-invariants because they are more related to the concept of controlling the defender than to the concept of visibility. We reached a preliminary result in a direction worth to be explored further. Next steps will be in the direction of a finer characterization of the statistical dependence between the subsystems, in proving the conjecture concerning the dependence between all the possible *attackers* and the *interface*, and in using different α-morphisms for the definition of the composition in order to avoid the use of bisimilarity relations in the proofs.

Chapter 7

Conclusions

In this thesis, we take inspiration from morphisms already presented in the literature to define new morphisms for the refinement of systems. In particular, we focus on the refinement on local states and choose, as reference model, Elementary Net Systems. The morphism we define, called α-morphism, relies mainly on structural constraints; the only exceptions are based on the local behaviours of subnets. With this definition, α-morphisms preserve reachable markings and reflect sequential components, meaning that the inverse image of a sequential component is a subnet of the refined Net covered by sequential components. By imposing additional behavioural constraints on the refining subnet and its environment, the α-morphisms reflect behaviour and induce a bisimulation between the refined Net and the abstract one. A natural development of this part consists in defining and studying categories related to the new morphisms, and functors relating these categories. These functors would set a correspondence between a structural view and a behavioural view of concurrent systems. In a different direction, we plan to define and study morphisms analogous to α-morphisms for more general classes of Petri Nets, such as Place Transition or High level Nets.

From a more practical point of view, the results summarised so far can be used as theoretical basis upon which to build a set of tools for system designers. In this thesis we present a couple of examples in the form of simple Net transformations that guarantee the existence of morphisms from the refined Net to the original one. The final target is a set of complete transformations for a given kind of morphism.

A notion of *visibility* related to information flow in a distributed system has been studied by several authors. We applied to this field the idea of composition presented in this thesis. We consider a system made of an attacker and a defender interacting through an interface. The defender wants to keep secrets some information represented by its local conditions. We assume that the attacker is not able to directly observe the local state of the defender, however it knows its structure.

In this field we define a new kind of observability, related to conditions. We obtain a first result based on invariant properties of the model, that states the conditions under which some local states of the defender become visible to the attacker. The results presented here are stated in terms of $\widehat{N}$-morphisms. We plan to explore the applicability of α-morphisms. This would allow to relax some behavioural constraints.

Bibliography

[1] Andrea Asperti and Giuseppe Longo. *Categories, Types, And Structures: An Introduction to Category Theory for the Working Computer Scientist*. Foundations of Computer Science. M.I.T. Press, 1991.

[2] Paolo Baldan, Stefan Haar, and Barbara König. Distributed Unfolding of Petri Nets. In Luca Aceto and Anna Ingólfsdóttir, editors, *FoSSaCS*, volume 3921 of *Lecture Notes in Computer Science*, pages 126–141. Springer, 2006.

[3] Marek A. Bednarczyk, Luca Bernardinello, Benoît Caillaud, Wieslaw Pawlowski, and Lucia Pomello. Modular System Development with Pullbacks. In Wil M. P. van der Aalst and Eike Best, editors, *ICATPN*, volume 2679 of *Lecture Notes in Computer Science*, pages 140–160. Springer, 2003.

[4] Luca Bernardinello, Elisabetta Mangioni, and Lucia Pomello. Composition of Elementary Net Systems based on α-morphisms. In Köhler-Bußmeier [23], pages 87–102.

[5] Luca Bernardinello, Elisabetta Mangioni, and Lucia Pomello. Local State Refinement on Elementary Net Systems: an Approach Based on Morphisms. In Lawrence Cabac, Michael Duvigneau, and Daniel Moldt, editors, *Petri Nets and Software Engineering. International Workshop, PNSE'12, Hamburg, Germany, June 25-26, 2012. Proceedings*, volume 851 of *CEUR Workshop Proceedings*, pages 138–152. CEUR-WS.org, 2012.

[6] Luca Bernardinello, Elena Monticelli, and Lucia Pomello. On Preserving Structural and Behavioural Properties by Composing Net Systems on Interfaces. *Fundamenta Informaticae*, 80(1-3):31–47, 2007.

[7] Eike Best and César Fernández C. *Nonsequential processes: a Petri net view*. EATCS monographs on theoretical computer science. Springer-Verlag, 1988.

[8] Eike Best, Philippe Darondeau, and Roberto Gorrieri. On the Decidability of Non Interference over Unbounded Petri Nets. In Konstantinos Chatzikokolakis and Véronique Cortier, editors, *SecCo*, volume 51 of *EPTCS*, pages 16–33, 2010.

[9] Gérard Boudol. Secure Information Flow as a Safety Property. In Degano et al. [13], pages 20–34.

[10] 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.

[11] Jeremy W. Bryans, Maciej Koutny, and Peter Y. A. Ryan. Modelling Opacity Using Petri Nets. *Electronic Notes Theoretical Computer Science*, 121:101–115, 2005.

[12] Nadia Busi and Roberto Gorrieri. A Survey on Non-interference with Petri Nets. In Jörg Desel, Wolfgang Reisig, and Grzegorz Rozenberg, editors, *Lectures on Concurrency and Petri Nets*, volume 3098 of *Lecture Notes in Computer Science*, pages 328–344. Springer, 2003.

[13] Pierpaolo Degano, Joshua D. Guttman, and Fabio Martinelli, editors. *Formal Aspects in Security and Trust, 5th International Workshop, FAST 2008, Malaga, Spain, October 9-10, 2008, Revised Selected Papers*, volume 5491 of *Lecture Notes in Computer Science*. Springer, 2009.

[14] Jörg Desel. Basic Linear Algebraic Techniques for Place or Transition Nets. In Reisig and Rozenberg [40], pages 257–308.

[15] 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.

[16] Javier Esparza, Stefan Römer, and Walter Vogler. An Improvement of McMillan's Unfolding Algorithm. *Formal Methods in System Design*, 20(3):285–310, 2002.

[17] Javier Esparza and Manuel Silva. Circuits, handles, bridges and nets. In Grzegorz Rozenberg, editor, *Applications and Theory of Petri Nets*, volume 483 of *Lecture Notes in Computer Science*, pages 210–242. Springer, 1989.

[18] Eric Fabre. On the Construction of Pullbacks for Safe Petri Nets. In S. Donatelli and P.S. Thiagarajan, editors, *ICATPN*, volume 4024 of *Lecture Notes in Computer Science*, pages 166–180. Springer, 2006.

[19] Carlo Ferigato and Elisabetta Mangioni. Inference of Local Properties in Petri Nets Composed through an Interface. In Köhler-Bußmeier [23], pages 71–84.

[20] Riccardo Focardi and Roberto Gorrieri. Classification of Security Properties (Part I: Information Flow). In Riccardo Focardi and Roberto Gorrieri, editors, *FOSAD*, volume 2171 of *Lecture Notes in Computer Science*, pages 331–396. Springer, 2000.

[21] Simone Frau, Roberto Gorrieri, and Carlo Ferigato. Petri Net Security Checker: Structural Non-interference at Work. In Degano et al. [13], pages 210–225.

[22] Jonathan Hayman and Glynn Winskel. The unfolding of general Petri nets. In Ramesh Hariharan, Madhavan Mukund, and V. Vinay, editors, *FSTTCS*, volume 2 of *LIPIcs*, pages 223–234. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2008.

[23] Michael Köhler-Bußmeier, editor. *Joint Proceedings of the 5th International Workshop on Logics, Agents, and Mobility (LAM'12), the 1st International Workshop on Petri Net-based Security (WooPS'12), and the 2nd International Workshop on Petri Nets Compositions (CompoNet'12), Hamburg, Germany, June 25-26, 2012*, volume 853 of *CEUR Workshop Proceedings*. CEUR-WS.org, 2012.

[24] Charles Lakos. On the Abstraction of Coloured Petri Nets. In Pierre Azéma and Gianfranco Balbo, editors, *ICATPN*, volume 1248 of *Lecture Notes in Computer Science*, pages 42–61. Springer, 1997.

[25] Saunders Mac Lane. *Categories for the working mathematician.* Springer-Verlag, New York, 1971.

[26] Elisabetta Mangioni. Morphisms for composition on interfaces. Poster at ICATPN 2011 Newcastle (International Conference on Application and Theory of Petri Nets).

[27] 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.

[28] Laurent Mazaré. Using unification for opacity properties. In *In Proceedings of the Workshop on Issues in the Theory of Security (WITS)*, pages 165–176, 2004.

[29] Robin Milner. *Communication and concurrency*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1989.

[30] Edward F. Moore. Gedanken Experiments on Sequential Machines. In Claude Elwood Shannon and John McCarthy, editors, *Automata Studies*, volume 34 of *Annals of mathematics studies*, pages 129–153. Princeton University Press, 1956.

[31] Mogens Nielsen, Grzegorz Rozenberg, and P. S. Thiagarajan. Elementary Transition Systems. *Theoretical Computer Science*, 96(1):3–33, 1992.

[32] Mogens Nielsen, Grzegorz Rozenberg, and P. S. Thiagarajan. Elementary Transition Systems and Refinement. *Acta Informatica*, 29(6/7):555–578, 1992.

[33] Mogens Nielsen and Glynn Winskel. Petri Nets and Bisimulation. *Theoretical Computer Science*, 153(1&2):211–244, 1996.

[34] 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.

[35] David Michael Ritchie Park. Concurrency and Automata on Infinite Sequences. In Peter Deussen, editor, *Theoretical Computer Science*, volume 104 of *Lecture Notes in Computer Science*, pages 167–183. Springer, 1981.

[36] Carl Adam Petri. Concepts of Net Theory. In *MFCS*, pages 137–146. Mathematical Institute of the Slovak Academy of Sciences, 1973.

[37] Carl Adam Petri. Concurrency. In Wilfried Brauer, editor, *Advanced Course: Net Theory and Applications*, volume 84 of *Lecture Notes in Computer Science*, pages 251–260. Springer, 1975.

[38] Lucia Pomello and Luca Bernardinello. Formal Tools for Modular System Development. In Jordi Cortadella and Wolfgang Reisig, editors, *ICATPN*, volume 3099 of *Lecture Notes in Computer Science*, pages 77–96. Springer, 2004.

[39] 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.

[40] Wolfgang Reisig and Grzegorz Rozenberg, editors. *Lectures on Petri Nets I: Basic Models, Advances in Petri Nets, the volumes are based on the Advanced Course on Petri Nets, held in Dagstuhl, September 1996*, volume 1491 of *Lecture Notes in Computer Science*. Springer, 1998.

[41] Grzegorz Rozenberg and Joost Engelfriet. Elementary Net Systems. In Reisig and Rozenberg [40], pages 12–121.

[42] Manuel Silva, Enrique Teruel, and José Manuel Colom. Linear Algebraic and Linear Programming Techniques for the Analysis of Place or Transition Net Systems. In Reisig and Rozenberg [40], pages 309–373.

[43] Walter Vogler. Executions: A New Partial-Order Semantics of Petri Nets. *Theoretical Computer Science*, 91(2):205–238, 1991.

[44] Robert Frank Carslaw Walters. *Categories and computer science*. Cambridge University Press, Cambridge, 1992.

[45] Glynn Winskel. Petri Nets, Algebras, Morphisms, and Compositionality. *Inf. Computer*, 72(3):197–238, 1987.

[46] Glynn Winskel. Topics in Concurrency Lecture Notes, 2009.

[47] J. Todd Wittbold and Dale M. Johnson. Information Flow in Nondeterministic Systems. In *IEEE Symposium on Security and Privacy*, pages 144–161, 1990.