# Elementary Transition Systems and Refinement

M. Nielsen G. Rozenberg P.S. Thiagarajan

March 1991

# Contents

# 0 Introduction

Elementary transition systems were introduced in [NRT] as a model of distributed computations. Their main asset is that they are just transition systems – with a rich and well-established theory – which satisfy a few additional axioms. Fundamental notions such as conflict and concurrency from net theory and the theory of event structures can be easily carried over to this model. This was proved in [ER] by establishing a formal link between elementary transition systems (ets's) and a basic model of net theory called elementary net systems. It was shown that – up to "isomorphism" – elementary transition systems are exactly the class of transition systems (called case graphs) that explicate the operational behaviour of elementary net systems. In [NRT] this link was lifted to a categorical framework by equipping both elementary transition systems and elementary net systems with behaviour preserving morphisms. After extending the two maps established in [ER] (taking elementary transition systems to elementary net systems and vice versa) to two functors, a number of strong results were proved concerning the properties of these two functors. All these results support the view that an elementary transition system is basically an abstract version of an elementary net system.

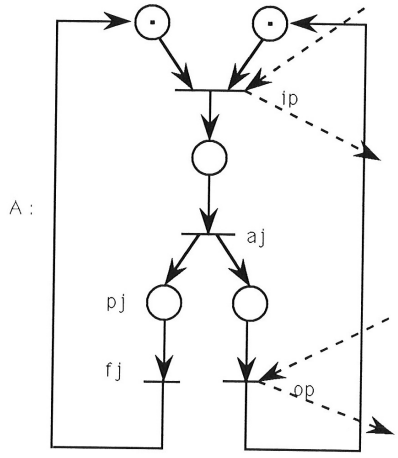
It turns out that this more abstract representation has many advantages over net systems in certain kinds of theoretical studies. In particular, elementary transition systems allow simple definitions of non-deterministic choice and parallel composition following the lines of Winskel [W]. We will not discuss here how various ccs-like operations can be defined over ets's. Instead we shall concentrate on the more difficult and interesting task of providing ets's with refinement operations. There seems to be two natural types of such operations, – one over the local states (called regions) and the other over local transitions (called events). In this paper we concentrate on local state refinement.

In the next section we discuss an example to bring out the main motivations underlying our refinement operations. In Section 2 we provide a brief introduction to elementary transition systems. In the subsequent two sections we propose a local state refinement operation and develop some of its properties. In the concluding section we discuss related work and issues concerning future work.

# 1 Motivating Examples

Let us take as a first motivating example the net version of the cyclic scheduler studied in [M]. The example consists of a number of individual agents performing jobs for the environment, and communicating internally to ensure a certain pattern in their joint job performance. An individual agent behaves as follows: first it gets permission (from another agent in the scheduler) to accept an incoming job followed by acceptance of an incoming job, followed by independently finishing the job and granting some other agent permission to accept a job from the environment. For details w.r.t. the desired behavioral properties of the cyclic schedule we refer to [M].

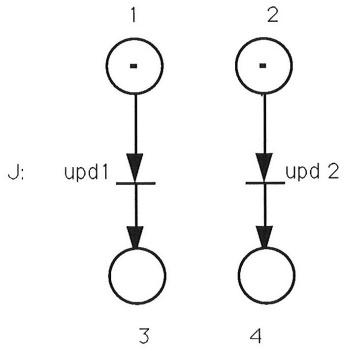
In net terms an agent is described in [M] as follows: Suppose we wish to




events:
ip -- incomming permission
aj -- accept job
fj -- finish job
op -- outgoing permission

conditions
pj -- performing job

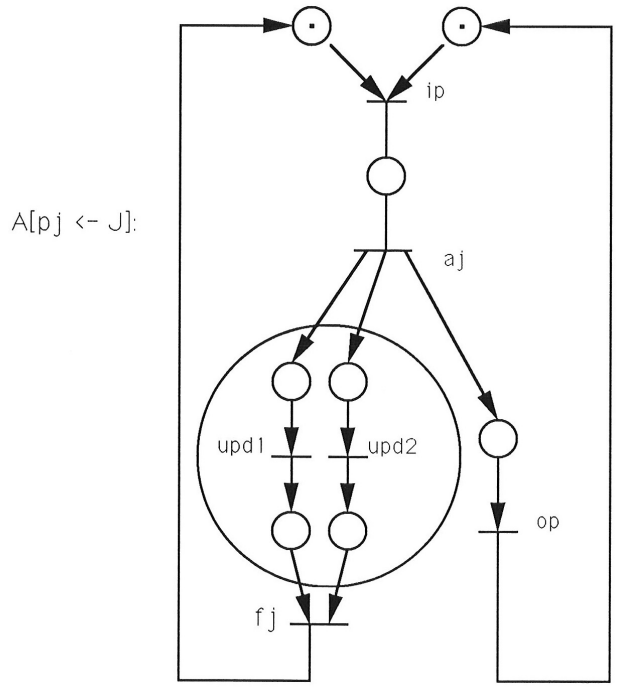
include in this description of the behaviour of an agent, a description of how a job is performed. Imagine that performing a job consists of two independent updates of variables, as represented by



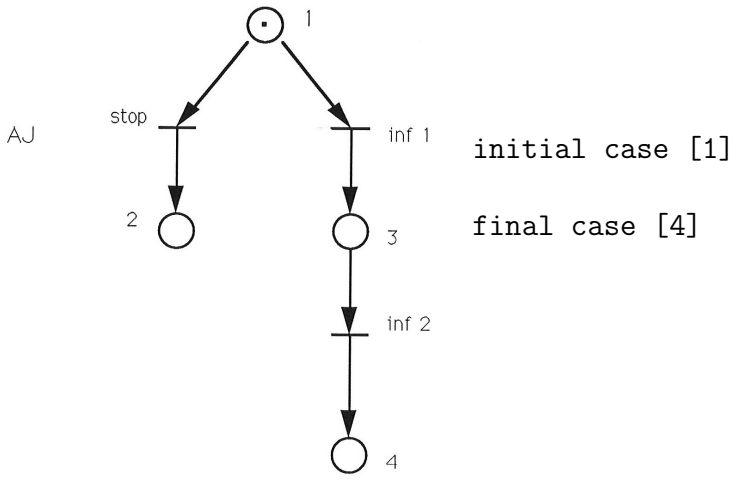

```
initial case [1, 2]

final case [3, 4]
(job done)
```

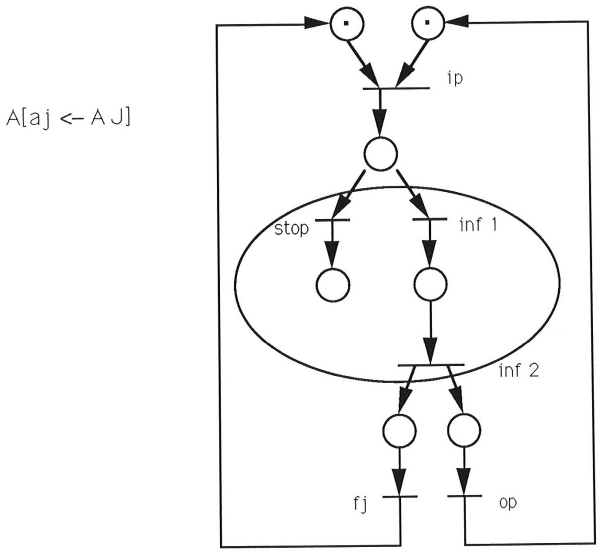
Intuitively, we need to modify $A$, by refining the condition $p_j$ by a copy of $J$, hooking it up appropriately with the pre- and postevents of $p_j$. We would expect such a refinement to produce




Imagine instead we would like to include in $A$ a more detailed description of what actually happens when a job is accepted. It might be that this could either be an error message from the environment telling the agent to stop computing or the sequential acceptance of two pieces of information related to the job, as represented by

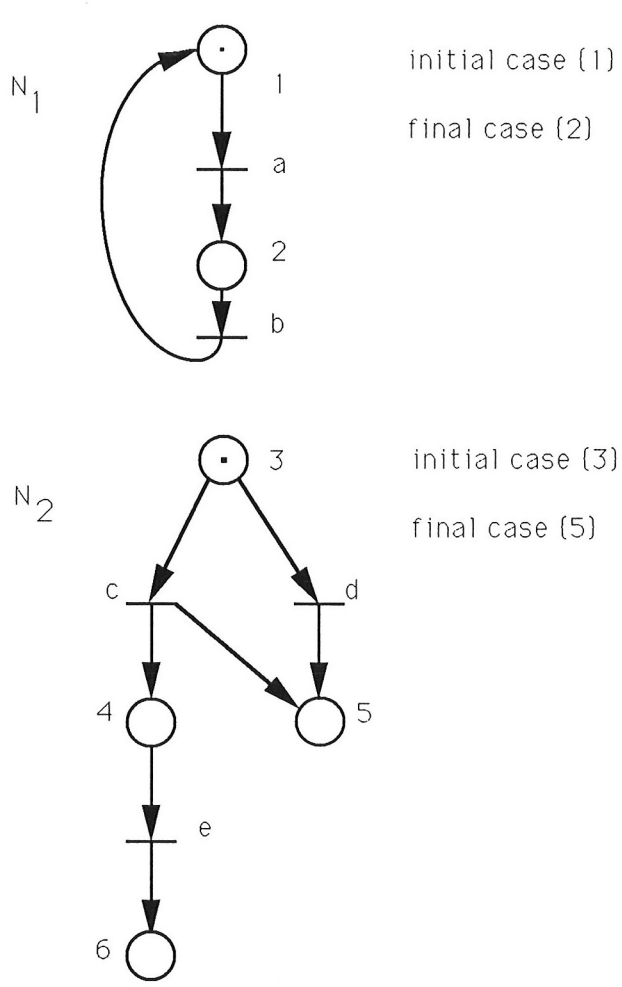



What we need is to modify $A$, by refining the event $aj$. We would expect such a refinement to produce

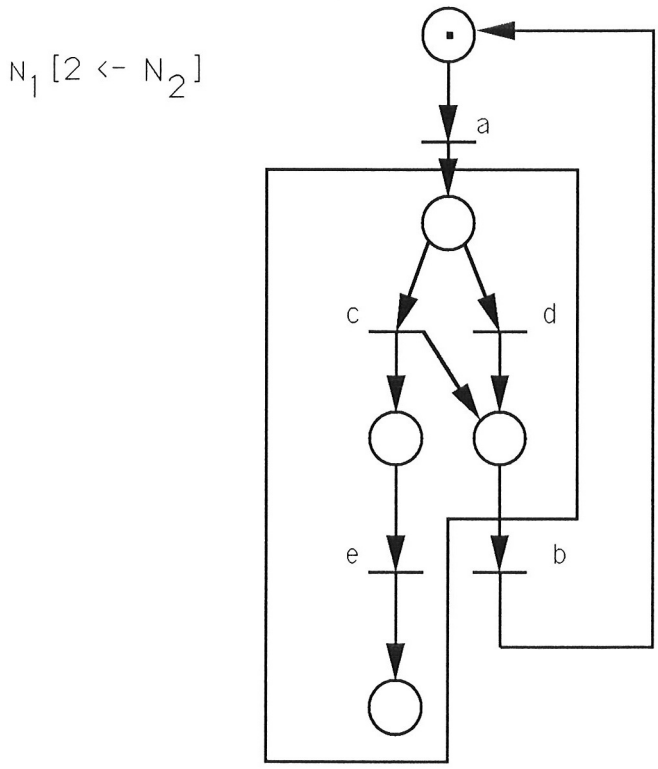



It is easy to come up with formal syntactic definitions of (local) state and event refinement for ens's capturing the intuitions from this example. Many such definitions may be found in the literature [K,V], and we shall present our version in this paper. However, as pointed out in [K] one would like any such syntactic notions to be supported by methods of reasoning about the

behaviour of the refined system in terms of the behaviours of the component systems in the refinement (compositional reasoning). This looks intuitively to be the case with our (non formalized!) notions from the above example, but let us consider another example.




Following the intuition from the previous example we would expect $N_1$ with condition "2" refined by $N_2$ to look as




However, behaviourally this net has the firing sequence $acb$ in which $N_2$ has been entered (by $a$) **and** left (by $b$), and yet after this firing sequence the net is in a state in which part of $N_2$ (the event $e$) is firable. So, behaviourally a holding of condition 2 in $N_1$ is *not* simply replaced by a complete behaviour of $N_2$ in $N_1[2 \leftarrow N_2]$ – our intended intuition behind the notion of local state refinement. Also, one sees by this example, that a "too" simple approach to syntactic condition refinement may produce a net with contact even though the two component nets ($N_1$ and $N_2$) are contact free.

The reader should be convinced that the kind of phenomenon illustrated by Example 1.2 makes behavioural compositional reasoning extremely difficult. It is easy to produce an example illustrating that one gets into the same kind of problem with a naive approach to event refinement.

One "solution" to these problems is suggested in [K] where a *dynamic* substitution of an event by a subnet is introduced, involving a fundamental change in the definition of the firing rule. Or one may impose certain restrictions

on the class of nets/refinements one allows with the purpose of obtaining behavioural compositionality, e.g. [V]. This paper may be seen to be suggesting another simple (and in the case of local state refinements very attractive) "solution". This paper tries to give formal arguments for the view that nets are basically too concrete to support naturally a behavioural notion like refinement. As an attractive alternative, elementary transition systems will be shown to have a simple notion of syntactic (local) state refinement, which **does** allow compositional reasoning at the level of behaviours. Also, if one wishes to stay within the framework of nets, we argue strongly in the following that one should work only with canonical versions of net systems (the so-called saturated net systems), in which the problems illustrated above disappear completely, without changing basic principles like firing rules in any way.

# 2 Elementary Transition Systems

Elementary transition systems are transition systems that satisfy a number of additional requirements.
A *transition system* in the present context is a 5-tuple $TS = (S, E, T, in, fin)$ where

- $S$ is a *non-empty* set of *states*
- $E$ is a set of *events*
- $T \subseteq S \times E \times S$ is a set of (labelled) *transitions*
- $in, fin \in S$ is the *initial* and *final* state respectively.

An elementary transition system is a transition system which will be required to satisfy six properties. A few of these properties are imposed for convenience. Others are imposed to reflect the fact that these transition systems "correspond" to elementary net systems (see [NRT]). Four of these properties can be stated straightaway.

**(A1)** $\forall e \in E.\ \exists (s, e, s') \in T.$

**(A2)** $\forall s \in S.\ \exists s_0, s_1, \ldots, s_n \in S$ and $\exists e_0, e_1, \ldots e_{n-1} \in E$ such that $in = s_0, s_n = s$ and $(s_i, e_i, s_{i+1}) \in T$ for $0 \leq i < n$.

**(A3)** $\forall (s, e, s') \in T.[s \neq s']$

**(A4)** $\forall (s, e_1, s_1)(s, e_2, s_2) \in T.[s_1 = s_2 \Rightarrow e_1 = e_2].$

(A1) and (A2) demand that there be no "redundant" events and states respectively. The more crucical axioms (A3) and (A4) rule out self-loops and multiple-arcs. Stated differently, (A3) demands that each event occurrence should result in *some* change in the system state. (A4) demands that every pair of states can be connected by at most one event occurence.
For stating the remaining two requirements, we need the important notion of a **region**.

## Definition 2.1

Let $TS = (S, E, T, in, fin)$ be a transition system. A **region** of $TS$ is a subset $r \subseteq S$ of states satisfying:

$\forall (s_0, e, s_0'), (s_1, e, s_1') \in T.$
(i) $s_0 \in r$ and $s_0' \notin r \Rightarrow s_1 \in r$ and $s_1' \notin r$
(ii) $s_0 \notin r$ and $s_0' \in r \Rightarrow s_1 \notin r$ and $s_1' \in r$.

□

Thus a region is a subset $r$ of states for which if **one** $e$-transition enters/leaves $r$ then **all** $e$-transitions enter/leave $r$. For an event $e$ we mean of course by an $e$-transition, a transition of the form $(s, e, s')$. We will say that an event $e$ is **crossing** the region $r$ in case every $e$-transition is leaving or every $e$-transition is entering $r$.

Let $TS = (S, E, T, in\ , fin)$ be a transition system. Then it is easy to see that both $\emptyset$ and $S$ are regions of $TS$. They are called the **trivial** regions. We will let $R_{TS}$ denote the set of non-trivial regions of $TS$. For $s \in S$, we will use $R_s$ to denote the set of regions containing $s$. Formally:

$$\forall s \in S. R_s = \{r \in R_{TS} \mid s \in r\}.$$

Finally, we shall use ${}^\circ e$ and $e^\circ (e \in E)$ as notation for the set of **pre-regions** and **post-regions** of $e$. Formally:

$$\begin{array}{lrcl} \forall e \in E. & {}^\circ e & = & \{r \in R_{TS} \mid \exists (s, e, s') \in T.\ s \in r \wedge s' \notin r\} \\ & e^\circ & = & \{r \in R_{TS} \mid \exists (s, e, s') \in T.\ s \notin r \wedge s' \in r\} \end{array}$$

Some useful properties of regions – which were shown in [ER] and [NRT] – are the following

## Proposition 2.2

Let $TS = (S, E, T, in, fin)$ be a transition system. Then

(i) $r \subseteq S$ is a region iff $\bar{r} = S - r$ is a region.

(ii) $\forall e \in E.\ e^\circ = \{\bar{r} \mid r \in^\circ e\}$.

(iii) $\forall (s, e, s') \in T.\ R_s - R_{s'} =^\circ e$ and $R_{s'} - R_s = e^\circ$ and consequently $R_{s'} = (R_s -^\circ e) \cup e^\circ$.

□

The last two properties we shall impose on our transition systems may now be formulated.

(A5) $\forall s, s' \in S.\ [R_s = R_{s'} \Rightarrow s = s']$.

(A6) $\forall s \in S\ \forall e \in E.\ [{}^\circ e \subseteq R_s \Rightarrow s \xrightarrow{e}]$.

The notation $s \xrightarrow{e}$ stands for the fact that $e$ is *enabled* at $s$. We say that the event $e$ is enabled at the state $s$ iff there exists a state $s'$ such that $(s, e, s') \in T$.

## Definition 2.3

An *elementary transition system* is a transition system which satisfies the axioms $(A1)$ through $(A6)$ stated above. □

It is easy to check that the transition system shown in Fig. 2.1. is elementary. The convention we have used in this diagram to decorate the initial and final state will be followed through the rest of the paper.

$$\{\{in, a\}, \{in, b\}, \{a, fin\}, \{b, fin\}\}$$

is the set of regions of this transition system. $\{a, fin\}$ is a preregion of 3 and a postregion of 1. The transition system shown in Fig. 2.2.a. is not elementary because it does not fulfill $(A5)$ ($R_a = R_b = R_c$). The transition system shown in Fig. 2.2.b. is not elementary because it does not fulfill $(A6)$ (at the state $b$ w.r.t. the event 2).

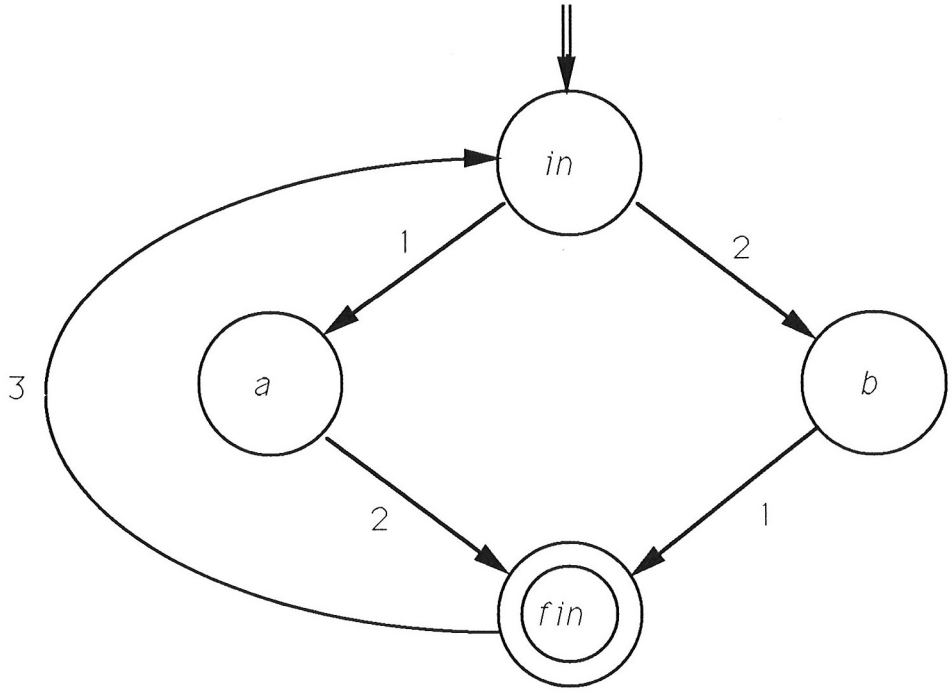



Fig. 2.1

We shall finish this section by quickly bringing out the relationship established in [NRT] between elementary transition systems and elementary net systems. For detailed definitions and explanation, we refer the reader to [NRT]. Given our present purposes, it will be convenient to adopt the following notion of elementary net systems.

## Definition 2.4

An *elementary net system* is a 5-tuple $N = (B, E, F, c_{in}, c_{fin})$ where

- $(B, E, F)$ is a simple net called the underlying net of $N$.
- $c_{in} \subseteq B$ is the *initial case* of $N$.
- $c_{fin} \in C_N$ is the *final case* of $N$, where $C_N$ denotes the set of cases of $N$ reachable (sequentially) from the initial case of $N$. □

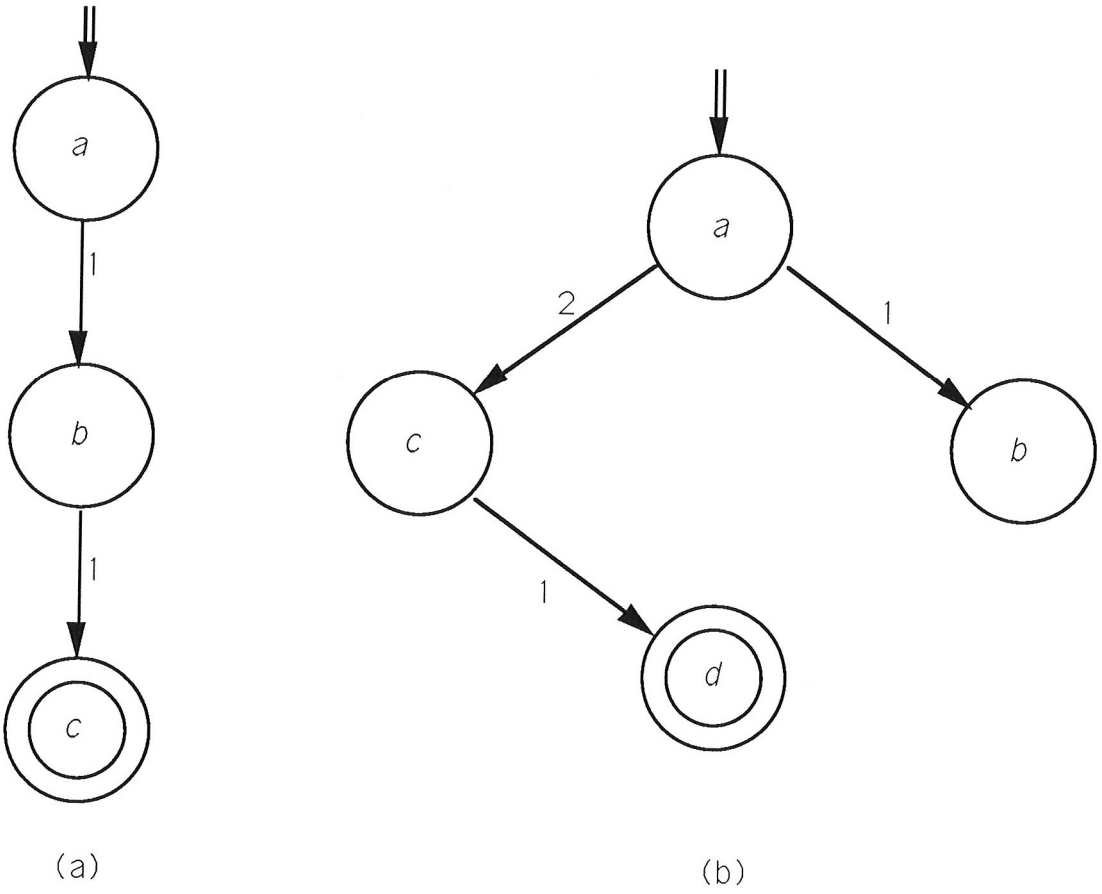



Fig. 2.2

In [NRT] both elementary net systems and elementary transition systems were equipped with behaviour-preserving morphisms called $N$-morphisms and $G$-morphisms respectively. These notions can be transported to the present setting as follows.

Let $N_i = (B_i, E_i, F_i, c^i_{in}, c^i_{fin}), i = 1, 2$ be a pair of elementary net systems. An $N$-morphism from $N_1$ to $N_2$ is a pair $(\beta, \eta)$ where $\beta \subseteq B_1 \times B_2$ is a binary relation and $\eta : E_1 \to E_2$ is a partial function such that:

(i) $\beta^{-1}$ is a partial function from $B_2$ to $B_1$.

(ii) $\forall (b_1, b_2) \in \beta.\ b_1 \in c^1_{in}$ iff $b_2 \in c^2_{in}$.

(iii) $c^2_{\mathit{fin}} = \beta(c^1_{\mathit{fin}}) \cup (c^2_{in} - \ \beta(c^1_{in}))$.

(iv) If $\eta(e_1)$ is undefined then $\beta({}^\bullet e_1) = \emptyset = \beta(e_1^\bullet)$

(v) If $\eta(e_1) = e_2$ then $\beta({}^\bullet e_1) = {}^\bullet e_2$ and $\beta(e_1^\bullet) = e_2^\bullet$.

□

Let $\mathcal{ENS}$ denote the category whose objects are elementary net systems and whose arrows are $N$-morphisms with the obvious notions of identity arrows and composition.

Turning now to elementary transition systems, $G$-morphisms are conveniently defined in the present set-up as follows.

Let $TS_i = (S_i, E_i, T_i, \mathit{in}_i, \mathit{fin}_i), i = 1, 2$ be a pair of elementary transition systems. Then a *G-morphism* from $TS_1$ to $TS_2$ is a map $f : S_1 \to S_2$ which satisfies:

(i) $f(\mathit{in}_1) = \mathit{in}_2$ and $f(\mathit{fin}_1) = \mathit{fin}_2$.

(ii) $\forall\ (s, e_1, s') \in T_1$. $[f(s) = f(s')$ or there exists $e_2 \in E_2$ such that $(f(s), e_2, f(s')) \in T_2]$.

(iii) If $(s, e_1, s') \in T_1$ and $(f(s), e_2, f(s')) \in T_2$ then $(f(s_1), e_2, f(s'_1)) \in T_2$ for every $(s_1, e_1, s'_1) \in T_1$.

Let $\mathcal{ETS}$ denote the category whose objects are elementary transition systems and whose arrows are $G$-morphisms with obvious notions of identities and composition. In [NRT] two functors $J$ and $H$ with $J$ going from $\mathcal{ETS}$ to $\mathcal{ENS}$ and $H$ going $\mathcal{ENS}$ to $\mathcal{ETS}$ were constructed and it was shown $J$ and $H$ form an adjunction (correflection) with $J$ as a leftadjoint. To be precise, the objects considered were slightly different, in that final states (for elementary transition systems) and final cases (for elementary net systems) were not taken into account. However, it is easy to verify that the adjunction result cited above goes through in the presence of final states and final cases.

In the present paper what will be of immediate interest is the manner in which the functors $J$ and $H$ operate on the objects. For an elementary net system $N = (B, E, F, c_{in}, c_{fin})$, $H(N) = (C_N, E_N, T_N, c_{in}, c_{fin})$ where $(C_N, E_N, T_N, c_{in})$, is the *case graph* (sometimes called the *sequential* case graph) of $N$. For an elementary transition system $TS = (S, E, T, in, fin)$, $J(TS)$ is given by:

$$J(TS) = (R_{TS}, E, F_{TS}, R_{in}, R_{fin}) \text{ where}$$

$$F_{TS} = \{(r, e) \mid r \in^\circ e\} \cup \{(e, r) \mid r \in e^\circ\}.$$

The important observation here is that when viewing ets's as nets (via the functor $J$) regions play the role of conditions (local states).

The adjunction (co-reflection) result of [NRT] then at once implies that every elementary transition system $TS$ is $G$-isomorphic to $H \circ J(TS)$. In addition, this leades to a canonical representation of elementary net systems. We will say that an elementary net system $N$ is *saturated* iff there exists an elementary transition system $TS$ such that $N$ is $N$-isomorphic to $J(TS)$. From the functorial nature of $J$ and $H$, it follows that for an elementary net system $N$, $J \circ H(N)$ is saturated. It seems natural to view $J \circ H(N)$ as a canonical representation $N$. One of our aims will be to demonstrate that canonical representations of elementary net systems are the proper objects to work with if one is interested in local state refinement operations. We conclude this section with a few examples. In Fig. 2.3 we have shown four elementary transition systems and in Fig. 2.4 the $J$-images of these transition systems. Final states/cases have been suppressed for convenience in these figures, and in Fig. 2.4 only selected conditions are annotated by the regions they represent.

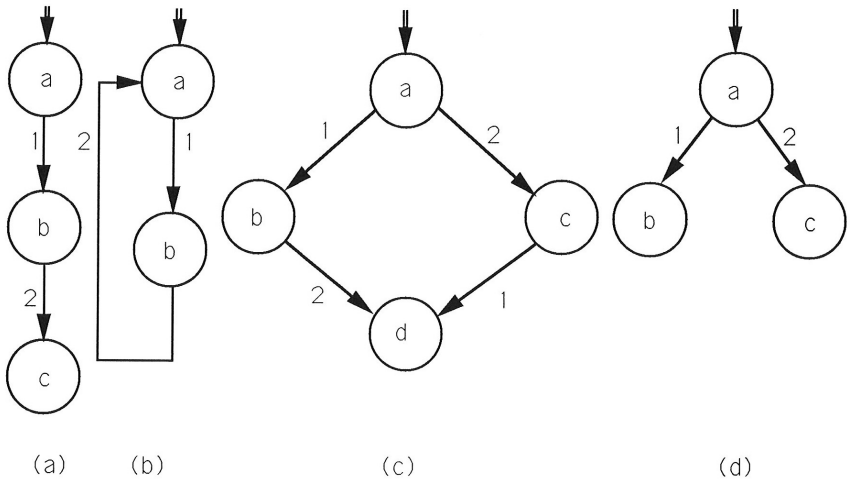



Fig. 2.3

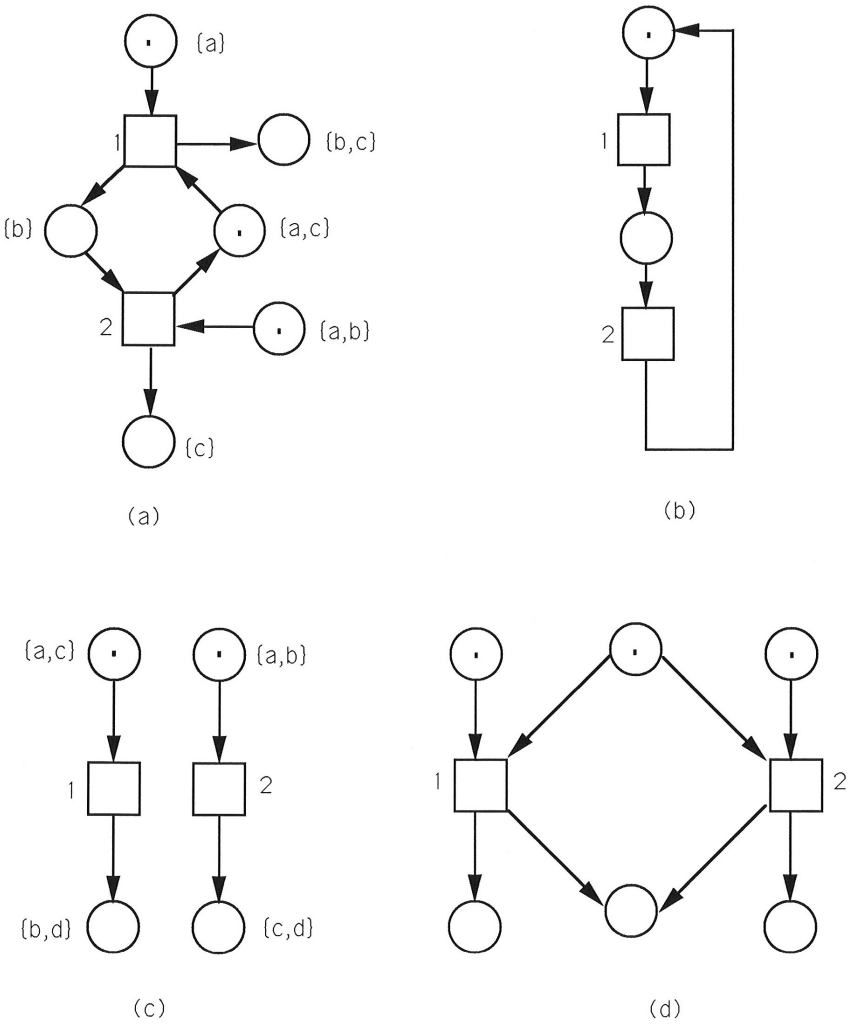



Fig. 2.4

# 3 State Refinement for $ETS$

Following the intuition from the introduction and the formal definition of ets's in the previous section, it seems natural to look for a formal definition of local state refinement on an ets in terms of a region refinement. Intuitively given one ets, $TS_1$, and a non-trivial region $r$ of $TS_1$, refining $r$ by some other ets, $TS_2$, should have the effect that any "holding" of $r$ (i.e. any "visit" to $r$) should behaviourally give rise to a *complete* behaviour of $TS_2$, i.e. a behaviour of $TS_2$ from its initial to its final state. Also, following our intuition this behaviour should only replace the "holding" of $r$, i.e. the behaviour of $TS_1$ within $r$ should otherwise be unaffected. We propose the following definition.

## Definition 3.1

Let $TS_1 = (S_1, E_1, T_1, in_1, fin_1)$ and $TS_2 = (S_2, E_2, T_2, in_2, fin_2)$ be two ets's with disjoint sets of states and events, and let $r_1$ be a non-trivial region of $TS_1$. Define **the refinement of $r_1$ in $TS_1$ by $TS_2$,** denoted $TS_1[r_1 \leftarrow TS_2]$ as the following structure $TS = (S, E, T, in, fin)$ where

$S = (S_1 - r_1) \cup r_1 \times S_2$.

$E = E_1 \cup E_2$.

T is the minimal subset of $S \times E \times S$ such that:

| | | | |
|---|---|---|---|
| i) | for every $(s_1, e_1, s_1') \in T_1$, | | |
| | i1) if $s_1 \notin r_1, s_1' \notin r_1$ | then | $(s_1, e_1, s_1') \in T$ |
| | i2) if $s_1 \notin r_1, s_1' \in r_1$ | then | $(s_1, e_1, (s_1', in_2)) \in T$ |
| | i3) if $s_1 \in r_1, s_1' \notin r_1$ | then | $((s_1, fin_2), e_1, s_1') \in T$ |
| | i4) if $s_1 \in r_1, s_1' \in r_1$ | then for every | $s_2 \in S_2$ |
| | | | $((s_1, s_2), e_1, (s_1', s_2)) \in T$ |
| ii) | for every $(s_2, e_2, s_2') \in T_2$ | | |
| | for every $s_1 \in r_1$ | | $((s_1, s_2), e_2, (s_1, s_2')) \in T$ |

$$in = \begin{cases} in_1 & \text{if } \ in_1 \notin r_1 \\ (in_1, in_2) & \text{if } \ in_1 \in r_1 \end{cases}$$

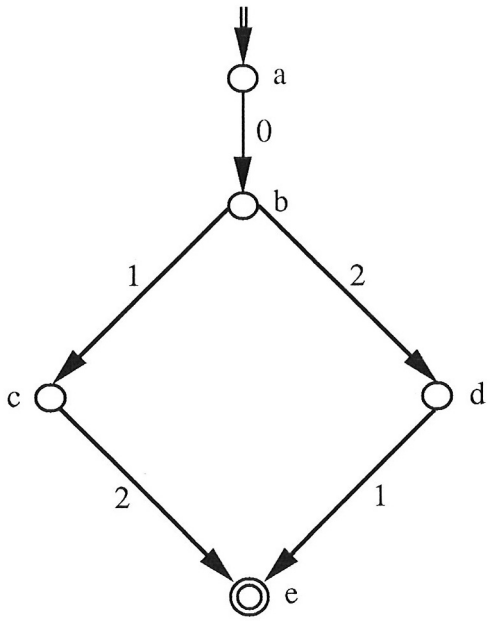
$$fin = \begin{cases} fin_1 & \text{if} \quad fin_1 \notin r_1 \\ (fin_1, fin_2) & \text{if} \quad fin_2 \in r_1 \end{cases}$$

□

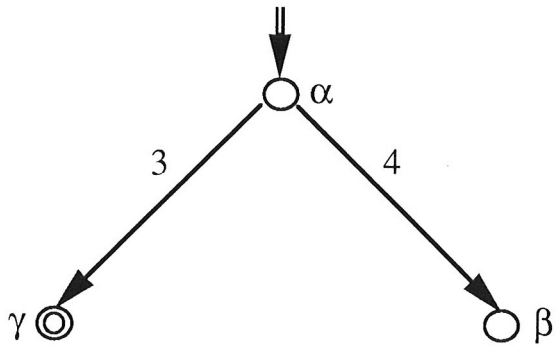
The different clauses in the definition of $T$ represent the behaviour of $TS$ in terms of the behaviours of $TS_1$ and $TS_2$. Outside the area $r_1 \times S_2$, the transition system $TS$ behaves like $TS_1$ (i1). Whenever $TS_1$ enters $r_1$, the transition system $TS$ enters the area $r_1 \times S_2$ (i2) and a copy of $TS_2$ is initiated to begin one of its computations. Within this "common area" $TS$ can move independently according to the moves of $TS_1$ internal to $r_1$ (i4) or according to moves from $TS_2$ (ii). $TS$ leaves the area $r_1 \times S_2$ whenever $TS_1$ leaves $r_1$ **and** $TS_2$ has finished a computation (i3).

## Example 3.2

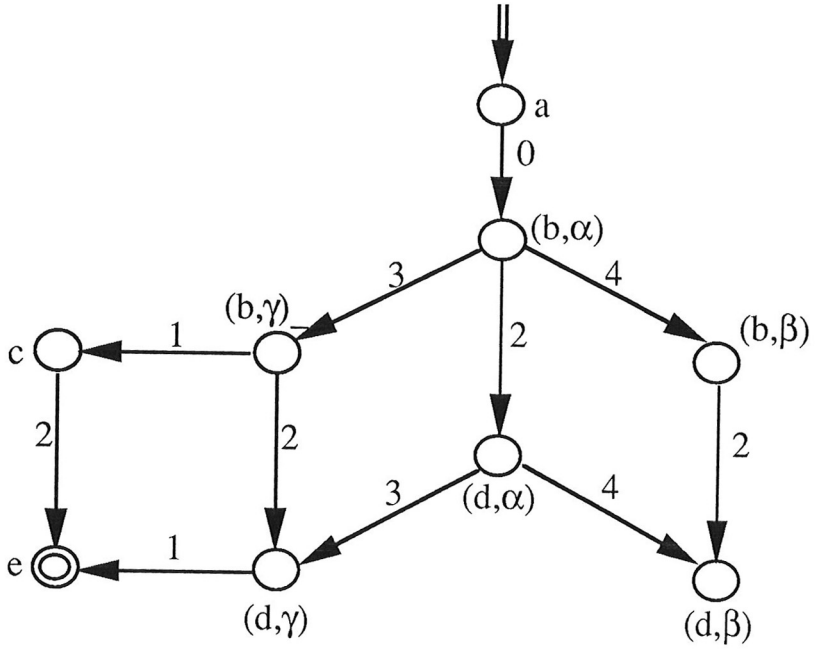
Let $TS_1$ be the following ets with initial state $a$, final state $e$, events $\{0, 1, 2\}$, and let $r_1$ be the region $\{b, d\}$.



Let $TS_2$ be the following ets with initial state $\alpha$, final state $\gamma$ and events $\{3, 4\}$.




According to Definition 3.1 $TS_1[r_1 \leftarrow TS_2]$ is the following transition system.




$TS_1[r_1 \leftarrow TS_2]$ as defined in Definition 3.1 is obviously a transition system, but is it also elementary? Before we prove that this is the case, it will be convenient to state a few lemmas providing us with some of the regions of $TS_1[r_1 \leftarrow TS_2]$.

## Lemma 3.3

Let $TS_1, TS_2, r_1$, and $TS_1[r_1 \leftarrow TS_2] = TS$ be as in Definition 3.1. Then for every $\hat{r} \in R_{TS_1}$

$$r = (\hat{r} - r_1) \cup ((r_1 \cap \hat{r}) \times S_2) \in R_{TS}.$$

Moreover, for every $e \in E = E_1 \cup E_2$, $e$ is entering/leaving $r$ in $TS$ iff $e \in E_1$ and $e$ is entering/leaving $\hat{r}$ in $TS_1$.

**Proof** Obvious from the definition of $TS_1[r_1 \leftarrow TS_2]$. □

## Lemma 3.4

Let $TS_1, TS_2, r_1$ and $TS_1[r_1 \leftarrow TS_2] = TS$ be as in Definition 3.1. Then for every $r_2 \in R_{TS_2}, r_1 \times r_2 \in R_{TS}$. Moreover, for every $e \in E = E_1 \cup E_2$, $e$ is entering/leaving $r_1 \times r_2$ iff

either $e \in E_1$ and $e$ is entering/leaving $r_1$
or $e \in E_2$ and $e$ is entering/leaving $r_2$

**Proof** From the definition of $TS$ in Definition 3.1 there are only two possibilities of an event entering $r_1 \times r_2$:

1. if $(s_1, e_1, s_1') \in T_1$ and $s_1 \notin r_1, s_1' \in r_1$, then if furthermore $in_2 \in r_2$ we have $(s_1, e_1, (s_1', in_2))$ as a transition entering $r_1 \times r_2$ in $TS$. Since $r_1$ is a region of $TS_1$ we see that any $e_1$-occurrence in $T$ must be of this particular form, and hence any $e_1$-occurrence is also entering $r_1 \times r_2$. Notice, that this argument makes essential use of the fact that an ets has a unique initial state!

2. if $(s_2, e_2, s_2') \in T_2$ and $s_2 \notin r_2, s_2' \in r_2$, then for every $s_1 \in r_1$, we have $((s_1, s_2), e_2, (s_1, s_2'))$ as a transition entering $r_1 \times r_2$ in $TS$. Since $r_2$ is a region, we see that any $e_2$-transition must be of this particular form, and hence any $e_2$-transition is also entering $r_1 \times r_2$.

Similar arguments apply in the case where an event is assumed to leave $r_1 \times r_2$. Here, it is essential that we work with ets's with one unique final state! $\square$

## Theorem 3.5

Let $TS_1, TS_2, r_1$ and $TS_1, [r_1 \leftarrow TS_2] = TS$ be as in Definition 3.1. Then $TS$ is an Elementary Transition System.

**Proof** $TS$ is clearly a transition system satisfying properties $(A1) - -(A4)$. So, let us prove that $TS$ also satisfies properties $(A5)$ and $(A6)$.

Given two states $s \neq s'$ in $S = (S_1 - r_1) \cup (r_1 \times S_2)$ we must show that there exists a region in $TS$ containing one and not the other of the two states. We consider the following cases

1. $s, s' \in S_1 - r_1$

   Take any region $r_1'$ of $TS_1$ such that $s \notin r_1', s' \in r_1'$ (at least one such region must exist since $TS_1$ is an ets). From Lemma 3.3 it now follows that

   $$r = (r_1' - r_1) \cup ((r_1' \cap r_1) \times S_2)$$

   is a region of $TS$, clearly containing $s'$ and not $s$, i.e., $r \in R_{s'}, r \notin R_s$.

2. $s \in S_1 - r_1$ , $s' \in r_1 \times S_2$

   Applying Lemma 3.4 to the region $r_2 = S_2$ of $TS_2$ it follows that $r_1 \times S_2$ is a region of $TS$ containing $s'$ and not $s$, i.e.,
   $r_1 \times S_2 \in R_{s'}$ , $r_1 \times S_2 \notin R_s$.

3. $s, s' \in r_1 \times S_2$

   Let $s = (x, y)$ and $s' = (x', y')$ where $x, x' \in r_1$. Since $s \neq s'$ we must have either $x \neq x'$ or $y \neq y'$. Let us look at the two cases separately.

   $x \neq x'$ Take any region $r_1'$ of $TS_1$ containing $x'$ but not $x$ (at least one such region exists, since $TS_1$ is an *ets*. Then it follows from Lemma 3.3 that

$$r = (r'_1 - r_1) \cup ((r'_1 \cap r_1) \times S_2)$$

is a region containing $s' = (x', y')$ but not $s = (x, y)$, i.e., $r \in R'_s, r \notin R_s$.

$y \neq y'$ Take any region $r_2$ of $TS_2$ such that $y \in r_2$ , $y' \notin r_2$ (some such region must exist since $TS_2$ is an ets). It follows now from Lemma 3.4 that $r_1 \times r_2$ is a region of $TS$ containing $s = (x, y)$ but not $s' = (x', y')$, i.e., $r_1 \times r_2 \in R_s,\ r_1 \times r_2 \notin R_{s'}$.

Thus $TS$ satisfies $(A5)$. We move now to verify $(A6)$.

Let $s \in S$ and $e \in E$, and assume that $e$ is not enabled at $s$. We have to show that ${}^\circ e \not\subseteq R_S$.

Consider four cases:

1. $s \in S_1 - r_1$ and $e \in E_1$.

   From Definition 3.1 it follows that $e$ is not enabled at $s$ in $TS_1$. Hence we know (since $TS_1$ is an ets) that there exists a region $r'_1$ of $TS_1$ such that

   $$r'_1 \in {}^\circ e \wedge r'_1 \notin R_s$$

   From Lemma 3.3 it now follows that $r = (r'_1 - r_1) \cup ((r'_1 \cap r_1) \times S_2)$ is a pre-region of $e$ in $TS$ which does not contain $s$.

2. $s \in S_1 - r_1$ and $e \in E_2$.

   Let $(s_2, e, s'_2)$ be any e-transition of $TS_2$, and let $r_2$ be a region containing $s_2$ and not $s'_2$ (at least one exists since $TS_2$ is an ets). Clearly $r_2 \in {}^\circ e$ in $TS_2$. Then from Lemma 3.4 it follows that $r_1 \times r_2$ is a pre-region of $e$ in $TS$ not containing $s$.

3. $s = (x, y) \in r_1 \times S_2$ and $e \in E_1$.

   From the definition of $TS$ it follows that

   either (a) $e$ is not enabled at $x$ in $TS_1$,
   or (b) for some $x' \in S_1 - r_1,\ (x, e, x') \in T_1$ but $y \neq fin_2$.

In case a) it follows from arguments like in case 1) above using Lemma 3.3 that a region may be constructed in $TS$ which is a pre-region of $e$ not containing $s$.

In case (b) take any region $r_2$ of $TS_2$ such that $y \notin r_2$ and $fin_2 \in r_2$. It follows from Lemma 3.4 that $r_1 \times r_2$ is a region of $TS$ such that $(x, fin_2) \in r_1 \times r_2$ and $(x, y) \notin r_1 \times r_2$. From Definition 3.1 it follows that $((x, fin_2), e, x') \in T$, and hence $r_1 \times r_2 \in {}^\circ e$; but since also $r_1 \times r_2 \notin R_{(x,y)}$ we have $(x, y) \notin r_1 \times r_2$.

4. $s = (x, y) \in r_1 \times S_2$ and $e \in E_2$.

   Then $e$ is not enabled at $y$ in $TS_2$. Since $TS_2$ is an ets we have that there exists a region $r_2$ of $TS_2$ such that

   $$r_2 \in {}^\circ e \text{ and } r_2 \notin R_y \text{ in } TS_2.$$

   If we apply Lemma 3.4 to $r_2$ we get a region of $TS$ which is a pre-region of $e$ not containing $s$.

□

# 4 Properties of State Refinement for $ETS$

In this section we shall state and prove a few results in support of our notion of state refinement. These results will establish that the state refinement operation defined here can be studied in terms of $G$-morphisms between elementary transition systems. We first recall the notion of $G$-morphisms.

**Definition 4.1** Let $TS_i = (S_i, E_i, T_i, in_i, fin_i)$ for $i = 1, 2$ be a pair of elementary transition systems. A *$G$-morphism* from $TS_1$ to $TS_2$ is a map $f : S_1 \rightarrow S_2$ which satisfies:

(i) $f(in_1) = in_2$ and $f(fin_1) = fin_2$

(ii) $\forall\ (s, e_1, s') \in T_1$. [$f(s) = f(s')$ or there exists $e_2 \in E_2$ such that $(f(s), e_2, f(s')) \in T_2$.]

(iii) If $(s, e_1, s') \in T_1$ and $(f(s), e_2, f(s')) \in T_2$ then $(f(s_1), e_2, f(s'_1)) \in T_2$ for every $(s_1, e_1, s'_1) \in T_1$.

The $G$-morphism $f : TS_1 \rightarrow TS_2$ defined above induces a unique partial function denoted $\eta_f$ from $E_1$ to $E_2$ given by:

$$\forall\, e_1 \in E_1.\ \eta_f(e_1) = \begin{cases} e_2, \text{ if } \exists (s, e_1, s') \in T_1 \text{ such that } (f(s), e_2, f(s')) \in T_2 \\ \text{undefined, otherwise.} \end{cases}$$

A simple but useful observation from [NRT] concerning $G$-morphisms is that a $G$-morphism is completely determined by the partial function over events that it induces.

**Proposition 4.2** Let $f_1$ and $f_2$ be two $G$-morphisms from $TS_1$ to $TS_2$ where $TS_1$ and $TS_2$ are two elementary transition systems. Then $f_1 = f_2$ iff $\eta_{f_1} = \eta_{f_2}$. □

Yet another basic property of $G$-morphisms (see, e.g., [ER] or [NRT]) is that they preserve regions in the following sense.

**Proposition 4.3** Let $TS_1 = (S_i, E_i, T_i, in_i, fin_i)$, $i = 1, 2$ be a pair of elementary transition systems and $f : TS_1 \to TS_2$ a $G$-morphism. Suppose $r_2$ is a region of $TS_2$. Then $f^{-1}(r_2)$ is a region of $TS_1$. Moreover for every $e_1 \in E_1$, it is the case that $f^{-1}(r_2)$ is a pre-region/post-region of $e_1$ in $TS_1$ iff $\eta_f(e_1)$ is defined **and** $r_2$ is a pre-region/post-region of $\eta_f(e_1)$ in $TS_2$. $\square$

Let $TS_1, r_1, TS_2$ and $TS = TS_1[r_1 \leftarrow TS_2]$ be as in Definition 3.1. Then our first result states that in $TS$, the behaviour of $TS_1$ is left unchanged if we "suppress" the behaviour of $TS_2$. To state this precisely we shall make use of the notion of firing sequences. Let $TS = (S, E, T, in, fin)$ be an elementary transition system. (Actually the notion of firing sequences can be defined in terms of general transition systems). Then $FS$, the set of firing sequences of $TS$ is the least subset of $E^*$ given inductively by:

(i) $\lambda \in FS$ and $in[\![\lambda > in$
($\lambda$ is the null sequence)

(ii) suppose $\rho \in FS$ and $in[\![\rho > s$ and $(s, e, s') \in T$. Then $\rho e \in FS$ and $in[\![\rho e > s'$.

Next suppose $f : TS_1 \to TS_2$ is a $G$-morphism with $TS_i = (S_i, E_i, T_i, in_i, fin_i)$, $i = 1, 2$. Then the partial function $\eta_f : E_1 \longrightarrow_* E_2$ induced by $f$ extends uniquely to a total function $\eta_f^*$ from $FS_1$ to $FS_2$ where $FS_i$ is the set of firing sequences of $TS_i$. This extension is given by

(i) $\eta_f^*(\lambda) = \lambda$

(ii) $\eta_f^*(\rho e) = \begin{cases} \eta_f^*(\rho)\eta_f(e), & \text{if } \eta_f(e) \text{is defined} \\ \eta_f^*(\rho), & \text{otherwise} \end{cases}$

By abuse of notation we will often write $\eta_f^*$ as $\eta_f$.

**Theorem 4.4** Let $TS_1, r_1, TS_2$ and $TS = TS_1[r_1 \leftarrow TS_2]$ be as in Definition 3.1. Let $f : S \to S_1$ be given by (recall that $S = (S_1 - r_1) \cup (r_1 \times S_2)$):

$$\forall s \in S.\ f(s) = \begin{cases} s, & \text{if } s \in S_1 - r_1 \\ x, & \text{if } s = (x, y) \in r_1 \times S_2. \end{cases}$$

Then the following statements hold.

(i) $f$ is a $G$-morphism from $TS$ to $TS_1$.

(ii) $\eta_f : E \rightarrow_* E_1$ satisfies:

$$\forall e \in E.\ \eta_f(e) = \begin{cases} e, & \text{if } e \in E_1 \\ \text{undefined}, & \text{otherwise.} \end{cases}$$

(iii) $FS_1 = \{\eta_f(\rho) \mid \rho \in FS\}$ where $FS_1$ is the set of firing sequences of $TS_1$ and $FS$ is the set of firing sequences of $TS$.

**Proof** Follows easily from the definitions. □

Thus as promised, the behaviour of $TS$ is precisely that of $TS_1$ provided we "blank out" completely the behaviour of $TS_2$. A similar result does not hold in general for $TS_2$ in relation to $TS$ when we blank out the behaviour of $TS_1$. But this is only because $TS_2$ may be "restarted" several times in $TS_1[r_1 \leftarrow TS_2]$ (see example after next theorem).

**Theorem 4.5** Let $TS_1, r_1, TS_2$ and $TS = TS_1[r_1 \leftarrow TS_2]$ be as in Definition 3.1. Assume further $in_2 = fin_2$. Let $f : S \rightarrow S_2$ be given by:

$$\forall s \in S.\ f(s) = \begin{cases} in_2, & \text{if } s \in S_1 - r_1 \\ y, & \text{if } s = (x, y) \in r_1 \times S_2. \end{cases}$$

Then the following statements hold.

(i) $f$ is a $G$-morphism from $TS$ to $TS_2$.

(ii) $\eta_f : E \rightarrow_* E_2$ satisfies:

$$\forall e \in E.\ \eta_f(e) = \begin{cases} e, & \text{if } e \in E_2 \\ \text{undefined}, & \text{otherwise.} \end{cases}$$

(iii) $FS_2 = \{\eta_f(\rho) \mid \rho \in FS\}$, where $FS_2$ is the set of firing sequences of $TS_2$ and, $FS$ is the set of firing sequences of $TS$.

**Proof:** Follows again from the definition. However, one must use the fact that $in_2 = fin_2$ to prove that $f$ is a $G$-morphism. □

Here is an example which shows that in general the above result does not hold.

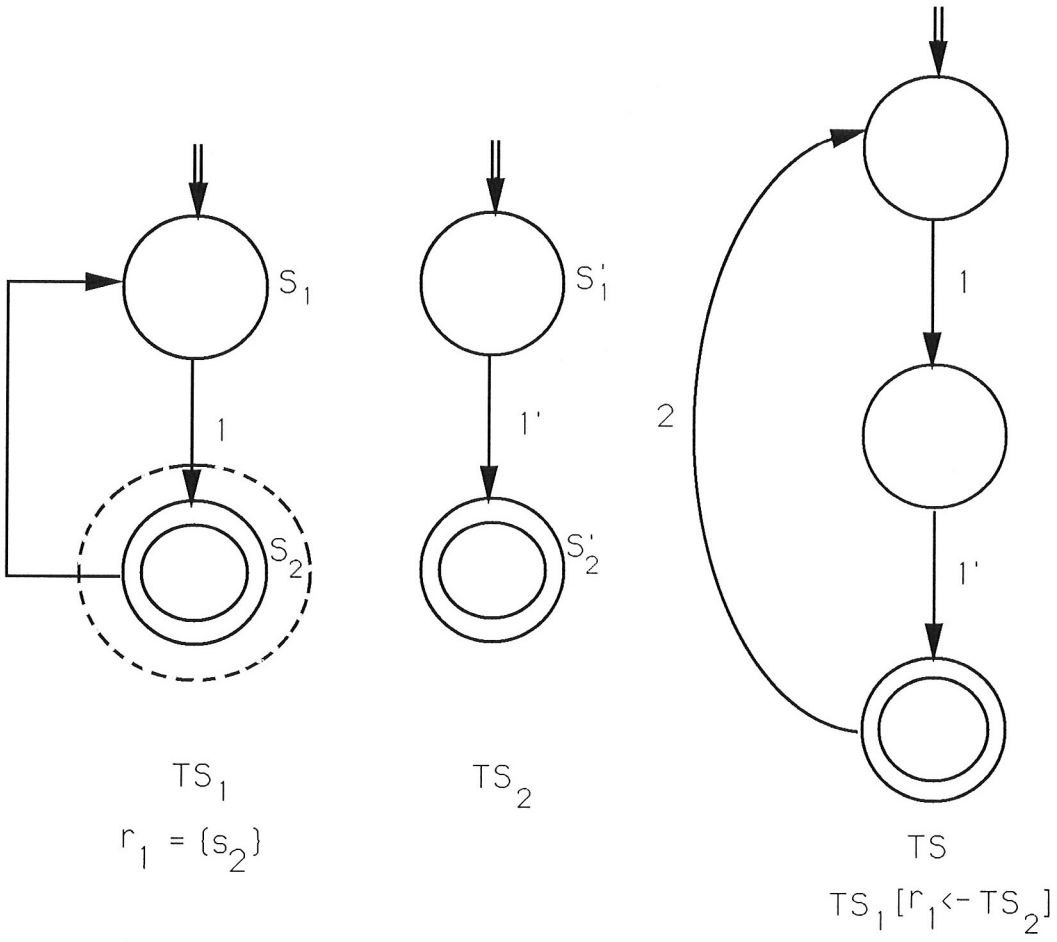



Fig 4.1

Then clearly there can be no non-trivial $G$-morphism from $TS$ to $TS_2$ let alone a $G$-morphism $g$ with the property $FS_2 = \eta_g(FS)$.

Our next result states that our notion of state refinement respects $G$-morphisms – in the following sense. Suppose $TS_2'$ is simulated by $TS_2$ modulo some $G$-morphism $f_2$. Then for any $TS_1$ and a region $r_1$ of $TS_1$, one would expect

$TS_1[r_1 \leftarrow TS_2']$ to be simulated by $TS_1[r_1 \leftarrow TS_2]$ modulo a $G$-morphism which respects $f_2$ w.r.t. its effect on the events of $TS_2'$. Similarly if $TS_1'$ is simulated by $TS_1$ modulo some $G$-morphism $f_1$ then for any region $r_1$ of $TS_1$ and any $TS_2$, one would expect $TS_1'[f_1^{-1}(r_1) \leftarrow TS_2]$ to be simulated by $TS_1[r_1 \leftarrow TS_2]$ modulo a $G$-morphism which respects $f_1$ w.r.t. its effect on the events of $TS_1'$. This is indeed so. Rather than stating and proving these results seperately, we combine them into the following.

**Theorem 4.6** Let $TS_1, r_1, TS_2$ and $TS = TS_1[r_1 \leftarrow TS_2]$ be as in Definition 3.1. Let $f_i, i = 1, 2$, be a pair of $G$-morphisms from $TS_i' = (S_i', E_i', T_i', in_i', fin_i')$ to $TS_i$ for $i = 1, 2$. Let $f$ be the function from the states of $TS' = TS_1'[f_1^{-1}(r_1) \leftarrow TS_2'] = (S', E', T', in', fin')$ to the states of $TS = TS_1[r_1 \leftarrow TS_2]$ defined as follows.

$$\forall s' \in S'.\ f(s') = \begin{cases} f_1(s'), & \text{if } s' \in S_1' - f_1^{-1}(r_1) \\ (f_1(x), f_2(y)), & \text{if } s' = (x, y) \in f_1^{-1}(r_1) \times S_2'. \end{cases}$$

Then the following statements hold:

(i) $f$ is a $G$-morphism from $TS'$ to $TS$.

(ii) $\eta_f$ satisfies:

$$\forall e' \in E'.\ \eta_f(e') = \begin{cases} \eta_{f_1}(e'), & \text{if } e' \in E_1' \\ \eta_{f_2}(e'), & \text{if } e' \in E_2'. \end{cases}$$

(iii) Let $FS'$ denote the set of firing sequences of $TS'$. Then

$$\begin{aligned} \forall \rho \in FS'.\ \eta_f(\rho) \restriction E_1 &= \eta_{f_1}(\rho \restriction E_1') \text{ and} \\ \eta_f(\rho) \restriction E_2 &= \eta_{f_2}(\rho \restriction E_2'). \end{aligned}$$

**Proof:** Parts $(ii)$ and $(iii)$ follow easily from $(i)$. This is easy to check. Hence we will just prove $(i)$.

Notice first that by Proposition 4.3 $TS_1'[f_1^{-1}(r_1) \leftarrow TS_2']$ is well-defined. The only non-trivial part of the proof is proving that $f$ as defined is indeed a morphism, so we concentrate on that part of the proof. We split the proof into subcases, according to the five different forms of moves $(s, e, s')$ in $TS'$.

1. $\underline{s, s' \in S_1' - f_1^{-1}(r_1),\ e \in E_1'}$

   1a) $\underline{\eta_{f_1}(e) \text{ defined}}$
   Since $f_1$ is a $G$-morphism we know that $(f_1(s), \eta_{f_1}(e), f_1(s')) = (f(s), \eta_f(e), f(s'))$ is a transition in $TS_1$, and since $f_1(s), f_1(s') \in S_1 - r_1$ we also have this transition in $TS$.

   1b) $\underline{\eta_{f_1}(e) \text{ undefined}}$
   Since $f_1$ is a $G$-morphism we have $f_1(s) = f_1(s')$. From the definition of $f$ it follows $f(s) = f(s')$.

2. $\underline{s \in S_1' - f_1^{-1}(r_1),\ s' = (x, in_2') \in f_1^{-1}(r_1) \times S_2',\ e \in E_1'}$
   By definition we have $(s, e, x) \in T_1'$, and since $f_1(s) \in S_1 - r_1$ and $f_1(x) \in r_1$ we must have $s \neq x$ and hence $\eta_{f_1}(e)$ is defined . Since $f_1$ is a $G$-morphism we also know $(f_1(s), \eta_{f_1}(e), f_1(x)) \in T_1$, and hence from Definition 3.1 $(f_1(s), \eta_{f_1}(e), (f_1(x), in_2)) =$
   $(f(s), \eta_f(e), f(s'))$ is a transition in $TS_1[r_1 \leftarrow TS_2] = TS$.

3. $\underline{s = (x, fin_2') \in f_1^{-1}(r_1) \times S_2',\ s' \in S_1' - f_1^{-1}(r_1) \text{ and } e \in E_1'}$
   By arguments similar to case 2) we must have $\eta_f(e) = \eta_{f_1}(e)$ defined and $(f_1(x), \eta_{f_1}(e), f_1(s')) \in T_1$ where $f_1(x) \in r_1$ and $f_1(s') \in S_1 - r_1$. But then again from Definition 3.1 it follows that
   $((f_1(x), fin_2), \eta_{f_1}(e), f_1(s')) = (f(s), \eta_f(e), f(s'))$ is a transition of $TS$.

4. $\underline{s = (x, y), s' = (x', y) \in f_1^{-1}(r_1) \times S_2',\ e \in E_1'}$
   From Definition 3.1 we have $(x, e, x') \in T_1'$ and $x, x' \in f_1^{-1}(r_1)$.

   4a) $\underline{\eta_{f_1}(e) \text{ is defined}}$
   Since $f_1$ is a $G$-morphism we have $(f_1(x), \eta_{f_1}(e), f_1(x')) \in T_1$ and $(f_1(x), f_1(x') \in r_1$. Hence from Definition 3.1 we also have $((f_1(x), f_2(y)), \eta_{f_1}(e), (f_1(x'), f_2(y)) = (f(s), \eta_f(e), f(s'))$ as a transition of $TS$.

   4b) $\underline{\eta_{f_1}(e) \text{ is undefined}}$
   Since $f_1$ is a $G$-morphism we have $f_1(x) = f_1(x')$, and hence also $f(s) = (f_1(x), f_2(y)) = (f_1(x'), f_2(y)) = f(s')$.

5. $\underline{s = (x, y), s' = (x, y') \in f_1^{-1}(r) \times S_2',\ e \in E_2'}$

This case is treated similarly to case 4.
The rest of the proof is routine and we omit the details. □

Next we would like to show how our notion of state refinement translates to elementary net systems. It turns out that modulo the act of adding "saturating conditions", our notion does indeed translate into the naive notion of condition-refinement that we considered (and rejected!) in Section 1. The key point is that we apply this simple minded condition- refinement operation only to saturated net systems. Recall that the elementary net system $N$ is said to be saturated in case $N$ is $N$-isomorphic to $J(TS)$ for some elementary transition system $TS$. First let us formalize the naive approach to condition-refinement.

**Definition 4.7** Given two elementary net systems
$N_i = (B_i, E_i, F_i, c^i_{in}, c^i_{fin})$, $i = 1, 2$, where the $B_i$'s and $E_i$'s are mutually disjoint sets. Let $b \in B_1$.

Define "$N_1$ *with* $b$ *defined by* $N_2$", notationally $\underline{N_1[b \leftarrow N_2]}$, as the net $N = (B, E, F, c_{in}, c_{fin})$ where

$$
\begin{aligned}
B &= (B_1 - \{b\}) \cup B_2 \\
E &= E_1 \cup E_2 \\
F &= F_1 - (\{b\} \times E_1 \cup E_1 \times \{b\}) \\
&\quad \cup F_2 \\
&\quad \cup \{(e_1, b_2) \mid (e_1, b) \in F_1 \wedge b_2 \in c^2_{in}\} \\
&\quad \cup \{(b_2, e_1) \mid (b, e_1) \in F_1 \wedge b_2 \in c^2_{fin}\} \\
c_{in} &= \begin{cases} c^1_{in} & \text{if } b \notin c^1_{in} \\ (c^1_{in} - \{b\}) \cup c^2_{in} & \text{if } b \in c^1_{in} \end{cases} \\
c_{fin} &= \begin{cases} c^1_{fin} & \text{if } b \notin c^1_{fin} \\ (c^1_{fin} - \{b\}) \cup c^2_{fin} & \text{if } b \in c^1_{fin} \end{cases}
\end{aligned}
$$

□

As we saw earlier this pleasingly simple and intuitive definition does not "work" if applied to arbitary net systems. $N_1$ and $N_2$ might be contact-free but $N_1[b \leftarrow N_2]$ might not be. Even if we choose to ignore this, one would expect to explain the operational behaviour of $N_1[b \leftarrow N_2]$ (i.e. that

of $H(N_1[b \leftarrow N_2]))$ by refining the operational behaviour of $N_1$ (i.e. that of $H(N_1)$) with the help of $H(N_2)$ where naturally the region of $H(N_1)$ that one would expect to refine would be $r_b = \{c \in C_{N_1} \mid b \in c\}$ (known to be a region from [NRT]). In other words, it does not seem unreasonable to demand that $H(N_1[b \leftarrow N_2])$ and $H(N_1)[r_b \leftarrow H(N_2)]$ should be $G$-isomorphic. However, as illustrated earlier this, in general, is not the case. All these problems however disappear if one works only with saturated net systems. We shall first bring this out before putting down the "correct" operation of condition-refinement for saturated net systems.

**Theorem 4.8** Let $N_1 = (B_i, E_i, F_i, c^i_{in}, c^i_{\mathit{fin}})$, $i = 1, 2$ be a pair of saturated net systems with disjoint pairs of conditions and events. Let $b \in B_1$ and $N = N_1[b \leftarrow N_2]$ be as in Definition 4.7. Then $H(N)$ is $G$-isomorphic to $H(N_1)[r_b \leftarrow H(N_2)]$ where $r_b = \{c \in C_{N_1} \mid b \in c\}$.

**Proof** We can assume without loss of generality that

$$TS_i = (S_i, E_i, T_i, in_i, \mathit{fin}_i),$$

$i = 1, 2$ is a pair of elementary transition systems such that $N_i = J(TS_i)$ for $i = 1, 2$. Consequently $B_i = R_{TS_i}$, $c^i_{in} = R_{in_i}$ and $c^i_{\mathit{fin}} = R_{\mathit{fin}_i}$ for $i = 1, 2$. Moreover

$$\begin{aligned} F_i &= \{(r, e) \mid r \in^\circ e \text{ in } TS_i\} \cup \\ &\quad \{(e, r) \mid r \in e^\circ \text{ in } TS_i\} \end{aligned}$$

From the results of [NRT] it also follows that $u_i : S_i \to C_{N_i}$ given by:

$$u_i(s) = R_s \text{ in } TS_i$$

is a $G$-isomorphism from $TS_i$ to $H(N_i)$ for $i = 1, 2$.

We will break the proof up into basically two steps.

Since $b \in B_1$, it is clear that $b$ is a non-trivial region in $TS_1$. Hence it makes sense to consider the elementary transition system

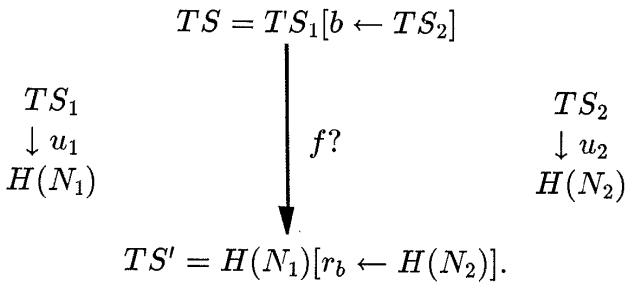
$$TS = TS_1[b \leftarrow TS_2].$$

We will show:

(i) $TS$ is $G$-isomorphic to $H(N_1)[r_b \leftarrow H(N_2)]$.

(ii) $TS$ is $G$-isomorphic to $H(N_1[b \leftarrow N_2])$.

**Proof of** $(i)$ We have the following situation.




Now define the map $f$ from the states of $TS$ to the states of $TS'$ as follows.

$$\forall\ s \in S\ \ f(s) = \begin{cases} u_1(s), \text{if } s \in S_1 - b \\ (u_1(x), u_2(y)), \text{if } s = (x,y) \in b \times S_2. \end{cases}$$

By Theorem 4.6, $f$ is a $G$-morphism from $TS$ to $TS'$ provided $u_1^{-1}(r_b) = b$ which we will now proceed to show.

Suppose $s \in u_1^{-1}(r_b)$. Then there exists $c \in r_b$ such that $u_1(s) = c$. Now $c \in r_b$ implies that $b \in c$ (where $b$ is viewed as a condition and $c$ is viewed as a case of $N_1$). But $u_1(s) = R_s$ and hence $b \in R_s$ implies that $s \in b$ (Here $b$ is viewed as a region of $TS_1$!). Hence $u_1^{-1}(r_b) \subseteq b$.

Now let $s \in b$ in $TS_1$. Then $b \in R_s$ and hence $b \in u_1(s)$. Thus $b$ holds in the case $u_1(s)$ of $N_1$. Consequently $u_1(s) \in r_b$ (in $H(N_1)$). This implies that $s \in u_1^{-1}(r_b)$. Hence $b \subseteq u_1^{-1}(r_b)$ and we are done.

We now wish to show that $f$ is in fact a $G$-isomorphism.

Clearly $f$ viewed as a function from the states of $TS$ to the states of $TS'$ is a bijection because $u_1$ and $u_2$ are $G$-isomorphisms and $S_1 - b$ and $b \times S_2$ are disjoint sets by definition.

From Theorem 4.6 it follows easily that $\eta_f$ is a total function from $E_1 \cup E_2$ to $E_1 \cup E_2$, and moreover it is the identity function.

From the facts that both $f$ (viewed as a map between sets) and $\eta_f$ are bijections, it follows at once that $f$ is indeed a $G$-isomorphism from $TS_1[b \leftarrow TS_2]$ to $H(N_1)[r_b \leftarrow H(N_2)]$.

**Proof of** $(ii)$ We propose the following map $g$ from the states of $TS$ to the states of $H(N_1[b \leftarrow N_2])$.

$$\forall s \in S.\ g(s) = \begin{cases} R_s, \text{if } s \in S_1 - b \\ (R_x - \{b\}) \cup R_y, \text{if } s = (x, y) \in b \times S_2. \end{cases}$$

We first argue that $g$ is well-defined. We can do this by picking $s \in S$ and doing induction on the "distance" of $s$ from $in$, the initial state of $TS$.

Suppose $s = in$. There are two cases to consider. Assume first that $in \in S_1 - b$. Then $in = in_1$ and $b \notin R_{in} = R_{in_1}$. But $R_{in_1} = c^1_{in}$, the initial case of $N_1$ and according to the definition of $N_1[b \leftarrow N_2]$, $b \notin c^1_{in}$ implies that $c^1_{in} = c_{in}$, the initial case of $N_1[b \leftarrow N_2]$. Thus $g(s) \in C_N$.

Now suppose $in \in b \times S_2$. Then $in_1 \in b$ and hence $b \in R_{in_1}$. Then once again by the definition of $N_1[b \leftarrow N_2]$, $c_{in} = (c^1_{in} - \{b\}) \cup c^2_{in}$. But $c^1_{in} = R_{in_1}$ and $c^2_{in} = R_{in_2}$. Hence $g(in) = c_{in}$, the initial case of $C_N$ as required.

Now suppose that $(s, e, s') \in T$ and $g(s) \in C_N$ where $N = N_1[b \leftarrow N_2]$. Depending on the type of this transition (w.r.t. its cross relation with the region $b$ in $TS_1$) there are five possible cases to consider. We just consider one of the cases here to illustrate the kind of arguments that are involved.

**Case 1** $s \in S_1 - b$, $s' = (x, y) \in b \times S_2$ and $e \in E_1$.

Then $b \in e^\circ$ in $TS_1$. By the definition of $N_1$ and $N_2 (N_i = J(TS_i))$, ${}^\bullet e = {}^\circ e$ and $e^\bullet = e^\circ$ (in the respective net systems (where ${}^\bullet e$ and $e^\bullet$ denote the pre-conditions and post-conditions of $e$ in the underlying nets of $N_1$ and $N_2$). For convenience (and to avoid confusion!) let $pre(e)$ and $post(e)$ denote the set of pre-conditions and post-conditions respectively of $e$ in $N = N_1[b \leftarrow N_2]$.

Now by the definition of $TS = TS_1[b \leftarrow TS_2], (s, e, x) \in T_1$. Hence $R_s \xrightarrow{e} R_x$ in $N_1$ (by the results of [NRT]). By the definition of $N$, it follows that

$pre(e) =^\bullet e$ and $post(e) = (e^\bullet - \{b\}) \cup c^2_{in}$. By the induction hypothesis, $g(s) = R_s \in C_N$. Now $pre(e) \subseteq R_s$ because $pre(e) =^\bullet e =^\circ e$. On the other hand, $B_1$ and $B_2$ are required to be disjoint sets and hence $c^2_{in} \cap R_s = \emptyset$. ($R_s \in C_{N_1}$). Since $e^\bullet = e^\circ \cap R_s = \emptyset$, because $e$ is enabled at $R_s$ in $N_1$, we now get $post(e) \cap R_s = \emptyset$ in $N$. Thus $e$ is enabled at $N$. It is now easy to verify that $(R_s - pre(e)) \cup post(e) = (R_x - \{b\}) \cup R_y$ where $R_y = R_{in_2}$. Consequently $g(s') \in C_N$ as required.

The remaining cases can be proved using similar applications of the definitions of $N$ and $TS$.

Now going through the details of the arguments it is also easy to establish the following .

(i) $\forall\, (s, e, s') \in T.\ (g(s), e, g(s')) \in T''$
where $H(N_1[b \leftarrow N_2]) = (S'', E'', T'', in'', fin'')$.

(ii) $\forall\, s \in S$ and $\forall\, e \in E.$ $[(g(s), e, c) \in T''$ implies that there exists $s' \in s$ such that $(s, e, s') \in T$ and $g(s') = c]$

It is then routine to establish – using once again the facts that $u_1$ and $u_2$ are $G$-isomorphisms – the following:

(iii) $g$ is a $G$-morphism

(iv) $g$, viewed as a function from $S$ to $S''$ is a bijection.

(v) $\eta_g$ is a total function from $E$ to $E$, and in fact is the identity function.

These three facts at once leads to the desired conclusion that $g$ is a $G$-isomorphism. □

It is a curious fact that $N = N_1[b \leftarrow N_2]$ can fail to be contact-free although both $N_1$ and $N_2$ are required to be saturated net systems. This however seems to be a pathological case where $N_2$ is the **empty** net system and $N_1$ has two distinct events $e_1$ and $e_2$ such that ${}^\bullet e_1 \cap^\bullet e_2 = \{b\}$ **and** there exists a case $c \in C_{N_1}$ at which both $e_1$ and $e_2$ are enabled! The main idea can be illustrated by an example. Let $TS_1, TS_2$ and $b$ be as indicated.

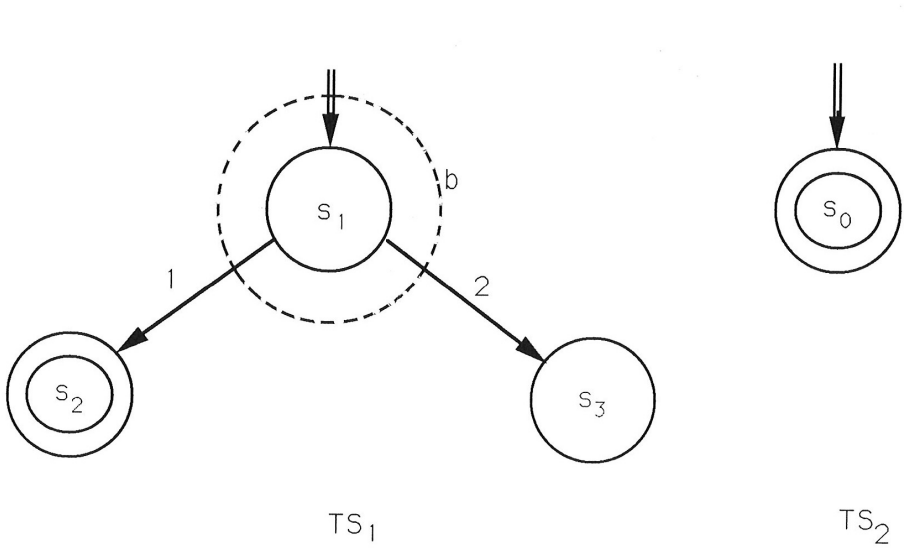



Fig 4.2

Then $TS = TS_1[b \leftarrow TS_2], N_1, N_2$ and $N = N_1[b \leftarrow N_2]$ will be as shown below.

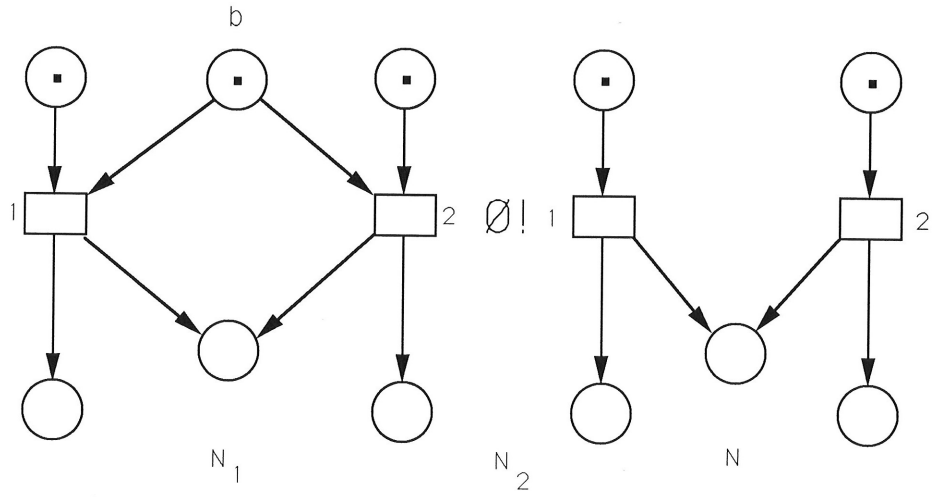



Fig 4.3

Thus $N$ will have contact although $H(N)$ and $TS_1[b \leftarrow TS_2]$ will be $G$-

isomorphic. Thus the "correct" state refinement operation for saturated net systems , in addition to the simple-minded operation specified in Definition 4.7, should "saturate" the resulting object. This motivates the following definition.

**Definition 4.9** Let $N_i = (B_i, E_i, F_i, c^i_{in})$, $i = 1, 2$ be a pair of saturated net systems and $b \in B_1$. Then the (saturated?) **refinement of $b$ in $N_1$ by $N_2$** is denoted as $N_1[\![b \leftarrow N_2]\!] = JoH(N_1[b \leftarrow N_2])$. □

It will be interesting to investigate the translation of our notion of refinement into other behavioural formalisms. We have some preliminary results in this regard w.r.t. firing sequences. Much more however needs to be done even at this level and also w.r.t. more sophisticated notions such as traces (in the sense of Mazurkiewicz; we expect this to be hard), non-sequential processes (we expect to this be easy) and labelled event structure (we expect this to be hard too!).

# Discussion

The model of Elementary Transition Systems was introduced in [ER], [NRT] as an abstraction of Elementary Net Systems – with a formal embedding in terms of a categorical coreflection, keeping behavioural information like causality, concurrency and conflict, but forgetting the concrete programming of a particular behaviour over an event set using conditions. In this paper we have given one example of the advantages of ETS over ENS, – the definition of local state refinement. What we have shown is that the well known problems in understanding within nets the simple notion of syntactic substitution of conditions by (sub)nets behaviourally, – these problems seem to disappear when moving to the more abstract level of ETS. Formally, we have shown that the ETS-version of condition-substitution (Theorem 4.8) does satisfy nice and natural properties, e.g., projection and compositionality results w.r.t. a standard notion of transition system morphisms (Theorems 4.4, 4.5, 4.6). Similar results do *not* hold for nets, – at least not with the simple notion of condition substitution and the corresponding notion of net morphisms.

We see this as only a small but promissing contribution to the understanding of refinement in models for concurrency. Much work needs to be done, e.g., studying the robustness of our results w.r.t. other notions of behaviour, and providing a notion of event-refinement for ETS also accompanied by some theoretical justification.

# Acknowledgements

This work has been part of joint work of ESPRIT Basic Research Actions CEDISYS and DEMON from which support is acknowledged. The third author acknowledges support from the Dutch National Concurrency Project REX sponsored by NFI.

# References


[**ER**] Ehrenfeucht, A. and Rozenberg, G., (1990), Partial 2-structures; Part II: State spaces of concurrent systemes, Acta Informatica, 27, 348-368.

[**K**] Kiehn, A., (1990), Petri Net Systems and their Closure Properties, Lecture Notes in Computer Science, 424, 306-328, Springer Verlag.

[**M**] Milner, R., (1980), A calculus of Communicating Systems, Lecture Notes in Computer Science, 92, Springer Verlag.

[**NRT**] Nielsen, M., Rozenberg, G., Thiagarajan, P. S., (1990), Elementary Transition Systems, Technical Report, PB-310, Computer Science Department, Aarhus University, Denmark.

[**V**] Vogler, W., (1987), Behaviour Preserving Refinement of Petri Nets, Lecture Notes in Computer Science, 246, 82-93, Springer Verlag.

[**W**] Winskel, G., (1987), Event Structures, Lecture Notes in Computer Science, 235, 325-392, Springer Verlag.