UNIVERSITÄT AUGSBURG

Modular Construction of Fast Asynchronous Systems

Lars Jenner

Report 1996-2 Dezember 1996

INSTITUT FÜR INFORMATIK
D-86135 AUGSBURG

Modular Construction of Fast Asynchronous Systems

Lars Jenner *

Institut für Informatik, Universität Augsburg
D-86135 Augsburg, Germany
jenner@uni-augsburg.de

Abstract

A testing scenario in the sense of De Nicola and Hennessy is developed to measure the worst-case efficiency of asynchronous systems using dense time, and it is shown that one can equivalently use discrete time. The resulting testing-preorder is characterized with some kind of refusal traces. Furthermore, the testing-preorder is refined to a precongruence for standard operators known from process algebras. Beside the usual complications with the choice operator, it turns out that even the prefix operation requires a refinement. Finally, the testing-preorder is compared to those gained from similar approaches.

1 Introduction

In the testing approach of [DNH84], reactive systems are compared by embedding them – with a parallel composition operator $\|$ – in arbitrary test environments. One variant of testing (must-testing) considers the worst-case behaviour: a system N performs successfully in an environment O if *every* run of $N \| O$ reaches success, which is signalled by a special action ω. If some system N_1 performs successfully whenever a second system N_2 does, then N_1 is called an implementation of the specification N_2; of course, an implementation may be successful in more environments than specified. This approach only takes into account the functionality of systems, i.e. which actions can be performed. To take also into account the efficiency of systems, we can add a time bound D to our tests and require that every run reaches success within time D [Vog95a]. In this efficiency testing approach, an implementation cannot only be successful in more environments than the specification, it can also be successful faster; i.e. the implementation (or testing) preorder can serve as a faster-than relation.

To apply efficiency testing, we have to measure the duration of a run. This is no problem, if the parallel system $N \| O$ is synchronous, i.e. if all components perform their actions

*This work was supported by the DFG-project 'Halbordnungstesten'.

according to a common global time scale; this case is treated in [Vog95a]. In asynchronous systems, the components work with indeterminate relative speeds. Usually, this is interpreted as: components may idle unnecessarily or actions may take more time than necessary; under this interpretation, the worst-case behaviour is to idle until time D is up and, thus, no test at all is satisfied.

Nevertheless, based on [Vog95b], [JV95] develops a scenario of efficiency testing for asynchronous systems and studies the corresponding faster-than relation. This scenario is based on a different interpretation of asynchronous systems: it is assumed that the components are guaranteed to perform each enabled action within one unit of time; thus, a component does not idle or take a lot of time with its current action; instead all other components may work very fast in comparison. Under this interpretation, the relative speeds of the components are still arbitrary, i.e. we really get a theory for asynchronous systems; this idea goes back to at least [LF81].

The basic variant of [JV95] assumes one unit of *dense* time for activation- and occurrence-time together; this approach seems appealing since it treats places (activation) and transitions (occurrence) of a net on an equal footing; a disadvantage is the technically complicated characterization of the resulting testing preorder.

In the present approach, an action may start some time after activation and it may end some time later, provided the start occurs within one unit of time after activation and the end occurs within another unit of time after the start; note that again, places and transitions of a net are treated on an equal footing. Based on this behaviour, satisfaction of an efficiency test and the corresponding testing preorder are defined, which shares all the nice properties of the approach in [JV95].

Our first main result shows that, analogously to the approach of [JV95], we can replace the modelling with dense time by an equivalent model using discrete time; this makes the testing approach much easier to work with and, in particular, it gives us a finite state space for a finite asynchronous system.

As a second main result, we give a characterization for the testing preorder with some kind of refusal traces. This characterization is less involved than the one developed for the basic approach of [JV95]. A view taken in [JV95] is again useful here: a refusal set consists of actions that are treated correctly in some way.

For the modular construction of and the compositional reasoning about systems, operators known from process algebras are introduced in our Petri net framework. Whereas parallel composition of nets is already essential for the testing scenario, we also consider prefix, choice, restriction, hiding and relabelling. It will turn out as a third main result that the testing preorder has to be refined to get a precongruence for all these operators. Quite interestingly, even for the prefix operation a refinement is necessary, and although we consider a preorder, the condition on stability concerning the choice operator is not only an implication but an equivalence.

To demonstrate that the precongruence is really a sensible faster-than relation, three constructions of a system N' from a system N – introduced in [Vog95b] – are considered, where it is intuitively clear that N and N' should be functionally equivalent, but that N should be faster. As a fourth main result, we show that this is indeed the case in the present approach.

Finally, the present approach is compared with the three variants developed in [JV95]. It turns out that in the present approach two systems are equivalent which should be equivalent intuitevely and are not in the basic approach of [JV95].

In this paper, we use (labelled, safe) Petri nets to model concurrent systems; some basic Petri net notions are defined in Section 2. Asynchronous behaviour with upper time bounds based on dense time is introduced in Section 3 and transformed to a discrete behaviour which gives rise to the same testing preorder. Section 4 gives the characterization, which in particular implies decidability of the testing preorder. In Section 5 the testing preorder is refined to a precongruence for the above mentioned operators and in Section 6, the three constructions of slower systems are discussed. Section 7 contains the comparison of the present approach with the one of [JV95]. Finally, related literature is discussed in the conclusion in Section 8.

2 Basic Notions

In this section, a very brief introduction to Petri nets is given. For further information the reader is referred to e.g. [Pet81, Rei85]. We will deal with safe Petri nets (place/transition-nets) whose transitions are labelled with actions from some infinite alphabet Σ' or with the empty word λ. These actions are left uninterpreted; the labelling only indicates that two transitions with the same label from Σ' represent the same action occurring in different internal situations, while λ-labelled transitions represent internal, unobservable actions. Σ' contains a special action ω, which we will need in our tests to indicate success, and we put $\Sigma = \Sigma' - \{\omega\}$.

Thus, a *labelled Petri net* $N = (S, T, W, l, M_N)$ (or just a *net* for short) consists of finite disjoint sets S of *places* and T of *transitions*, the *weight function* $W : S \times T \cup T \times S \to \{0, 1\}$, the *labelling* $l : T \to \Sigma' \cup \{\lambda\}$, and the *initial marking* $M_N : S \to \{0, 1\}$. When we introduce a net N or N_1, then we assume that implicitly this introduces its components S, T, W, ... or S_1, T_1, ..., etc. If $W(x, y) = 1$, then (x, y) is called an *arc*; for each $x \in S \cup T$, the *preset* of x is ${}^\bullet x = \{y \mid W(y, x) = 1\}$ and the *postset* of x is $x^\bullet = \{y \mid W(x, y) = 1\}$.

- A *multiset* over a set X is a function $\mu : X \to \mathbb{N}_0$. We identify $x \in X$ with the multiset that is 1 for x and 0 everywhere else. A subset Y of X is identified with the multiset that is 1 for $y \in Y$ and 0 everywhere else. For multisets, multiplication with scalars from $\mathbb{N}_0$ and addition is defined elementwise.

- A *marking* is a multiset over S, a *step* is a multiset over T. A step μ is *enabled* under a marking M, denoted by $M[\mu\rangle$, if $\sum_{t \in T} \mu(t) \cdot {}^\bullet t \leq M$. The step is *maximal* if additionally: whenever $M[\mu'\rangle$ and $\mu \leq \mu'$ (transition-wise), then $\mu = \mu'$.

  If $M[\mu\rangle$ and $M' = M + \sum_{t \in \mu} \mu(t) \cdot t^\bullet - \sum_{t \in \mu} \mu(t) \cdot {}^\bullet t$, then we denote this by $M[\mu\rangle M'$ and say that μ can *occur* or *fire* under M yielding the *follower marking* M'. Since transitions are special steps, this also defines $M[t\rangle$ and $M[t\rangle M'$ for $t \in T$.

- This definition of enabling and occurrence can be extended to sequences as usual: a sequence w of steps is *enabled* under a marking M, denoted by $M[w\rangle$, and yields the follower marking M' when *occurring*, denoted by $M[w\rangle M'$, if $w = \lambda$ and $M = M'$ or $w = w'\mu$, $M[w'\rangle M''$ and $M''[\mu\rangle M'$ for some marking M''. If w is enabled under the initial marking, then it is called a *step sequence*, or – in case that $w \in T^*$ – a *firing sequence*.

We can extend the labelling of a net to steps by $l(\mu) = \sum_{t \in T, l(t) \neq \lambda} \mu(t) \cdot l(t)$, where the empty sum equals the empty word. Then we can extend the labelling also to sequences of steps or transitions as usual, i.e. homomorphically; note that internal actions are automatically deleted in the labelling of a sequence. Next, we lift the enabledness and firing definitions to the level of actions:

- A sequence v of multisets over Σ' is *enabled* under a marking M, denoted by $M[v\rangle\rangle$, if there is some w with $M[w\rangle$ and $l(w) = v$. If $M = M_N$, then v is called a *step trace*; if $w \in T^*$, then v is called a *trace*. We call two nets *step equivalent* if they have the same step traces. We call two nets *language equivalent* if they have the same traces.
- For a marking M the set $[M\rangle$ of markings *reachable* from M is defined as $\{M' \mid \exists w \in T^* : M[w\rangle M'\}$. A marking is called *reachable* if it is reachable from M_N. The net is *safe* if $M(s) \leq 1$ for all places s and reachable markings M.
- Two not necessarily distinct transitions t_1 and t_2 are concurrently enabled under some marking M if $M[t_1 + t_2\rangle$. A transition t is *self-concurrent*, if $M[2t\rangle$ for some reachable marking M. An action $a \in \Sigma'$ is *autoconcurrent*, if $M[2a\rangle\rangle$ for some reachable marking M.

General assumption: All nets considered in this paper are safe and without isolated transitions. This implies that all nets in this paper are free of self-concurrency, but it does not exclude autoconcurrency.

For each set A of transitions or actions, A^+ and A^- denote disjoint copies of A whose elements are called *transition* or *action parts* and denoted a^+ resp. a^-, $a \in A$; a^+ will stand for the start of the transition or action a, which only empties the corresponding preset, while a^- indicates the end of the transition or action a, producing the tokens of the corresponding postset. We let $A^\pm = A^+ \cup A^-$. The labelling function l is extended to transition parts by $l(t^+) = l(t)^+$ and $l(t^-) = l(t)^-$ if $l(t) \neq \lambda$ and $l(t^+) = l(t^-) = \lambda$ if $l(t) = \lambda$. Note that we use A^* to denote – as usual – the set of all sequences over A.

Finally, we introduce parallel composition $\|_A$ with synchronization inspired from TCSP. If we combine nets N_1 and N_2 with $\|_A$, then they run in parallel and have to synchronize on actions from A. To construct the composed net, we have to combine each a-labelled transition t_1 of N_1 with each a-labelled transition t_2 from N_2 if $a \in A$.

In the definition of parallel composition, $*$ is used as a dummy element, which is formally combined e.g. with those transitions that do not have their label in the synchronization set A. (We assume that $*$ is not a transition or a place of any net.)

Definition 2.1 *parallel composition of nets*

Let N_1, N_2 be nets, $A \subseteq \Sigma'$. Then the *parallel composition* $N = N_1 \|_A N_2$ *with synchronization* over A is defined by

$$
\begin{aligned}
S &= S_1 \times \{*\} \cup \{*\} \times S_2 \\
T &= \ \ \{(t_1, t_2) \mid t_1 \in T_1, t_2 \in T_2, l_1(t_1) = l_2(t_2) \in A\} \\
&\quad \cup \{(t_1, *) \mid t_1 \in T_1, l_1(t_1) \notin A\} \\
&\quad \cup \{(*, t_2) \mid t_2 \in T_2, l_2(t_2) \notin A\}
\end{aligned}
$$

$$
\begin{aligned}
W((s_1, s_2), (t_1, t_2)) &= \begin{cases} W_1(s_1, t_1) & \text{if } s_1 \in S_1,\, t_1 \in T_1 \\ W_2(s_2, t_2) & \text{if } s_2 \in S_2,\, t_2 \in T_2 \\ 0 & \text{otherwise} \end{cases} \\
W((t_1, t_2), (s_1, s_2)) &= \begin{cases} W_1(t_1, s_1) & \text{if } s_1 \in S_1,\, t_1 \in T_1 \\ W_2(t_2, s_2) & \text{if } s_2 \in S_2,\, t_2 \in T_2 \\ 0 & \text{otherwise} \end{cases} \\
l((t_1, t_2)) &= \begin{cases} l_1(t_1) & \text{if } t_1 \in T_1 \\ l_2(t_2) & \text{if } t_2 \in T_2 \end{cases} \\
M_N &= M_{N_1} \dot\cup M_{N_2}, \text{ i.e. } M_N((s_1, s_2)) = \begin{cases} M_{N_1}(s_1) & \text{if } s_1 \in S_1 \\ M_{N_2}(s_2) & \text{if } s_2 \in S_2 \end{cases}
\end{aligned}
$$

■ 2.1

Parallel composition is an important operator for the modular construction of nets. In the present paper, the main purpose of this operator is to combine a net N with a test net. Designing suitable test nets O and looking at the behaviour of $N \parallel_\Sigma O$, we can get information on the behaviour of N. The net O may also be regarded as an observer of N. For the general approach of testing, see [DNH84].

3 Timed Behaviour of Asynchronous Systems

The first definition of this section describes the asynchronous behaviour of a parallel system. Hence, we assume that the components of the system vary in speed – but we also assume that they are guaranteed to start each enabled action within at most one unit of time and end this action within another unit of time; this upper time bound allows the relative speeds of the components to vary arbitrarily, since we have no lower time bound. Thus, the behaviour we define is truly asynchronous.

Technically speaking, we require that each enabled transition starts firing within time 1 – unless it is disabled within this time – and ends firing within time 1 after its start. For this purpose, we keep track of the remaining time an enabled or firing transition has using a function ρ; $\rho(t)$ is initialized to 1, when t gets enabled and when t starts. Since we distinguish starts and ends of transition firings, we also have a set C of currently firing transitions. As dense time domain we choose the reals, hence we will speak of 2-continuous firing, where 2 indicates the two time units of activation resp. firing time; $\mathbb{R}^+$ is the set of positive real numbers. This approach is very similar to that of [JV95].

When dealing with functions (especially those from transitions to real numbers), we denote a constant function by this constant, possibly indexed by the function's domain.

Definition 3.1 *continuous instantaneous description, continuous firing*

A *continuous instantaneous description CID* of a net is a quadrupel (M, A, C, ρ) consisting of a marking M of N, two sets $A \subseteq T$ and $C \subseteq T$ of *activated* and *current(ly firing) transitions* and a function $\rho : A \cup C \to [0, 1]$ describing the *residual activation* resp. *firing time* of an activated resp. current transition. The *initial CID* is $CID_N = (M_N, A_N, \emptyset, \rho_N)$ with $A_N = \{t \mid M_N[t\rangle\}$ and $\rho_N = 1_{A_N}$.

We write $(M, A, C, \rho)[\varepsilon\rangle_2^c(M', A', C', \rho')$ if one of the following cases applies:

1. $\varepsilon = t^+$, $t \in A$, $M' = M - {}^\bullet t$, $A' = \{t' \mid M'[t'\rangle\}$, $C' = C \cup \{t\}$, $\rho' = \rho|_{(A' \cup C)} \cup 1_{\{t\}}$.
2. $\varepsilon = t^-$, $t \in C$, $M' = M + t^\bullet$, $A' = \{t' \mid M'[t'\rangle\}$, $C' = C - \{t\}$, $\rho' = \rho|_{(A \cup C')} \cup 1_{(A' - A)}$.
3. $\varepsilon = (r)$, $r \in \mathbb{R}^+$, $r \leq \min \rho(A \cup C)$, $M' = M$, $A' = A$, $C' = C$, $\rho' = \rho - r$.

The set $2CFS(N) = \{w \mid CID_N[w\rangle_2^c CID\}$ is the set of *(2c-firable) continuous firing sequences* of N, the set $2CL(N) = \{l(w) \mid w \in 2CFS(N)\}$ is the 2*-continuous language* of N containing the 2*-continuous traces* of N. We let l preserve time steps, i.e. $l((r)) = (r)$.
■ 3.1

Part 3 of this firing rule ensures that every transition that is enabled for one unit of time starts firing within that unit and ends firing within another unit of time, but according to 1 and 2 it may also act faster. Note that due to the lack of self-concurrency, we have $A \cap C = \emptyset$ for all reachable *CID*'s.

Definition 3.2 *action sequence, transition sequence, duration*

For every w in $2CL(N)$ resp. $2CFS(N)$, $\alpha(w)$ is the *sequence* of (plussed or minussed) *action* resp. *transition parts* in w, and $\zeta(w)$ is the *duration*, i.e. the sum of time steps in w.
■ 3.2

To see whether a system N performs successfully in a testing environment O, we have to check that in each run of $N\|_\Sigma O$ the success action ω is performed at some given time R at the latest. To be sure that we have seen everything that occurs up to time R, we only look at runs w with $\zeta(w) > R$.

Definition 3.3 *continuously timed test*

A net is *testable* if none of its transitions is labelled with ω. A *continuously timed test* is a pair (O, R), where O is a net (the *test net*) and $R \in \mathbb{R}_0^+$ (the *real time bound*). A testable net N 2*c-satisfies* a continuously timed test (O, R) (N $must_2^c$ (O, R)), if each $w \in 2CL(N\|_\Sigma O)$ with $\zeta(w) > R$ contains some ω^+. For testable nets N_1 and N_2, we call N_1 a 2*-continuously faster implementation* of N_2, $N_1 \sqsupseteq_2^c N_2$, if N_1 2*c*-satisfies all continuously timed tests that N_2 satisfies:

$$N_1 \sqsupseteq_2^c N_2 \Leftrightarrow (\ \forall (O, R) : N_2\ must_2^c\ (O, R) \Rightarrow N_1\ must_2^c\ (O, R)\ )$$

■ 3.3

Considering the timed testing approach, our aim is now to characterize the slowest firing sequences, for these sequences will decide the success of a timed test (O, R). We will draw the convenient conclusion that we can restrict attention to the discrete sublanguage of the continuous language, i.e. those $v \in \mathit{2CL}$ that contain only discrete time steps of one unit.

Definition 3.4 *2-discrete language, discretely timed tests*

The 2-*discrete language* $\mathit{2DL}(N)$ of a net N is a subset of $\mathit{2CL}(N)$ defined as

$$\mathit{2DL}(N) = \{v \in \mathit{2CL}(N) \,|\, \text{for all time steps } (r) \text{ in } v\text{: } r = 1\}.$$

$\mathit{2DL}(N)$ is also generated by the suitably defined *(2d-firable) 2-discrete firing sequences* $\mathit{2DFS}(N)$. Analogously to Definition 3.3 we define *discretely timed testing*: a *discretely timed test* is a pair (O, D), where O is a net and $D \in \mathbb{N}_0$. A testable net N *2d-satisfies* such a test (O, D), N must_2^d (O, D), if each $v \in \mathit{2DL}(N\|_\Sigma O)$ with $\zeta(v) > D$ contains some ω^+, and define

$$N_1 \sqsupseteq_2^d N_2 \Leftrightarrow (\, \forall (O, D) : N_2 \ \mathit{must}_2^d \ (O, D) \Rightarrow N_1 \ \mathit{must}_2^d \ (O, D)\,)$$

■ 3.4

We now show that for every $w \in \mathit{2CFS}$ we can find a $v \in \mathit{2DFS}$ that has the same action sequence but is discrete in its time steps and slower. The sequence v is constructed from w by letting one time unit pass in v whenever the cumulated time in w exceeds the next natural number.

Lemma 3.5

For a net N there is for each $w \in \mathit{2CFS}(N)$ a $v \in \mathit{2DFS}(N)$ with $\alpha(v) = \alpha(w)$ and $\zeta(v) \geq \zeta(w)$.

Proof: We will construct for each $w \in \mathit{2CFS}(N)$ a $v \in \mathit{2DFS}(N)$ with $\alpha(v) = \alpha(w)$ and $\zeta(v) \geq \zeta(w)$; furthermore, we will show that for CID_w and CID_v reached after w and v we have $\rho_v + \zeta(v) - \zeta(w) \geq \rho_w$. Note that, as a consequence of $\alpha(v) = \alpha(w)$, CID_v and CID_w coincide in their M-, C- and A-component. The proof is by induction on $|w|$, where for $w = \lambda$ we can choose $v = \lambda$. Hence, assume that for $w \in \mathit{2CFS}(N)$ we have constructed $v \in \mathit{2DFS}(N)$ as required and consider $w' = w\varepsilon \in \mathit{2CFS}(N)$. We denote the CID's reached after w' and the corresponding v' by $\mathit{CID}_{w'}$ and $\mathit{CID}_{v'}$.

If $\varepsilon \in T^{\pm}$ then $v' = v\varepsilon \in \mathit{2DFS}(N)$ with $\alpha(v') = \alpha(v\varepsilon) = \alpha(w\varepsilon) = \alpha(w')$ and $\zeta(v') = \zeta(v\varepsilon) = \zeta(v) \geq \zeta(w) = \zeta(w\varepsilon) = \zeta(w')$. The residual times $\rho_{w'}$ and $\rho_{v'}$ coincide with ρ_w and ρ_v or, for the newly activated transitions resp. the started transition, are both equal 1 and $1 + \zeta(v') - \zeta(w') = 1 + \zeta(v) - \zeta(w) \geq 1$.

Now let $\varepsilon = (r)$. If $r \leq \zeta(v) - \zeta(w)$ we choose $v' = v$; obviously, $\alpha(v') = \alpha(v')$ and $\zeta(v') = \zeta(v) \geq r + \zeta(w) = \zeta(w')$. Furthermore $\rho_{v'} + \zeta(v') - \zeta(w') = \rho_v + \zeta(v) - \zeta(w) - r \geq \rho_w - r = \rho_{w'}$. If on the other hand $r > \zeta(v) - \zeta(w)$, we choose $v' = v(1)$. Since $\rho_v + \zeta(v) - \zeta(w) \geq \rho_w \geq r > \zeta(v) - \zeta(w)$, we have $\rho_v > 0$ and $\rho_v = 1$ by $v \in \mathit{2DFS}(N)$; thus, the time step (1) is enabled after v and $v' = v(1) \in \mathit{2DFS}(N)$ with $\alpha(v') = \alpha(w')$. Furthermore, $\zeta(v') = \zeta(v) + 1 \geq \zeta(w) + r = \zeta(w')$ and $\rho_{v'} + \zeta(v') - \zeta(w') = \zeta(v) + 1 - \zeta(w) - r = \rho_v + \zeta(v) - \zeta(w) - r \geq \rho_w - r = \rho_{w'}$. ■ 3.5

Before comparing discrete and continuous testing, we note that additionally we can require a 2-discrete firing sequence to start with a time step.

Lemma 3.6

For each $v \in$ *2DFS*(N) there is a $v' \in$ *2DFS*(N) that starts with a (1)-time-step and satisfies $\alpha(v') = \alpha(v)$ and $\zeta(v') \geq \zeta(v)$.

Proof: Let $v = v_1(1)v_2(1)v_3$, where v_1 and v_2 contain no time-step; the treatment of this case also shows how a v with no or only one time-step can be treated. Let $\mathit{CID}_N[v_1(1)v_2\rangle_2^c \mathit{CID}_1$ $[(1)\rangle_2^c \mathit{CID}_2$.

Obviously, $\mathit{CID}_N[(1)\rangle_2^c$. Since the *CID*'s encountered along $v_1(1)v_2$ coincide with those along $(1)v_1v_2$ in their M-, A- and C-parts, we get furthermore $\mathit{CID}_N[(1)v_1v_2\rangle_2^c \mathit{CID}_1'$ by Definition 3.1 1 and 2.

Assume that $\rho_1'(t) = 0$ for some $t \in A_1' \cup C_1' = A_1 \cup C_1$. The ρ-value of such a t must have been decreased by the initial (1)-step, i.e. t was initially enabled and neither started nor disabled during v_1v_2; but this implies $\rho_1(t) = 0$ and, since $\mathit{CID}_1[(1)\rangle_2^c$, such a t does not exist. Thus, we get $\mathit{CID}_1'[(1)\rangle_2^c \mathit{CID}_2'$, where CID_2 and CID_2' coincide in their M-, A- and C-parts and $\rho_2' = 0 = \rho_2$, i.e. $\mathit{CID}_2 = \mathit{CID}_2'$. Hence, we can choose $v' = (1)v_1v_2(1)v_3$. ■ 3.6

Theorem 3.7

The relations $\sqsupseteq_2^c$ and $\sqsupseteq_2^d$ coincide.

Proof: For testable nets N_1 and N_2 we show $N_1 \sqsupseteq_2^c N_2 \Leftrightarrow N_1 \sqsupseteq_2^d N_2$.
"$\Rightarrow$": Assume a test (O, D) with $N_1 \ \not{m}\mathit{ust}_2^d\ (O, D)$. Since *2DL*$(N_1\|_\Sigma O) \subseteq$ *2CL*$(N_1\|_\Sigma O)$, we have $N_1 \ \not{m}\mathit{ust}_c\ (O, D)$ and by hypothesis $N_2 \ \not{m}\mathit{ust}_2^c\ (O, D)$. Let $\zeta(w) > D$ for a $w \in$ *2CL*$(N_2\|_\Sigma O)$ that contains no ω^+. Using Lemma 3.5, from w we construct a $v \in$ *2DL*$(N_2\|_\Sigma O)$ with $\zeta(v) \geq \zeta(w) > D$ that contains no ω^+ either and conclude $N_2 \ \not{m}\mathit{ust}_2^d$ (O, D).
"$\Leftarrow$": Assume a test (O, R) with $N_1 \ \not{m}\mathit{ust}_2^c\ (O, R)$. Then there is a $w \in$ *2CL*$(N_1\|_\Sigma O)$ with $\zeta(w) > R$ that contains no ω^+. Using Lemma 3.5, we can find a $v \in$ *2DL*$(N_1\|_\Sigma O)$ with $\zeta(v) > D = \lfloor R \rfloor$ that contains no ω^+, i.e. $N_1 \ \not{m}\mathit{ust}_2^d\ (O, D)$. From $N_1 \sqsupseteq_2^d N_2$ we conclude $N_2 \ \not{m}\mathit{ust}_2^d\ (O, D)$, i.e. there is a $v' \in$ *2DL*$(N_2\|_\Sigma O)$ with $\zeta(v') \geq D + 1 > R$ that contains no ω^+. This v' causes $N_2 \ \not{m}\mathit{ust}_2^c\ (O, R)$. ■ 3.7

The construction of a *2DL*-sequence from a *2CL*-sequence has made it very obvious that several events can occur at the same moment, i.e. without any time passing inbetween. In particular, a long sequence of events where one event causes the next could occur in zero-time. This could be regarded as unrealistic by some readers. In contrast, we could require that between any two events a positive amount of time has to pass. Before we continue our normalization of the 2-continuous language, we demonstrate that this 'non-zero' requirement does not change the testing preorder.

Definition 3.8 *non-zero continuous firing sequences*

A $w \in$ *2CFS*(N) is a *(2nz-firable) 2-non-zero continuous firing sequence* ($w \in$ *2NZCFS*(N) and $l(w) \in$ *2NZCL*(N)), if in w transition parts from $T^\pm$ and time steps (r) alternate. A testable net N *2nz-satisfies* a continuously timed test (O, R) (N must_2^{nz} (O, R)), if each $w \in$ *2NZCL*$(N\|_\Sigma O)$ with $\zeta(w) > R$ contains some ω^+. For testable nets N_1 and N_2 we define

$$N_1 \sqsupseteq_2^{nz} N_2 \Leftrightarrow (\ \forall (O,R) : N_2 \ must_2^{nz} \ (O,R) \Rightarrow N_1 \ must_2^{nz} \ (O,R)\ )$$

■ 3.8

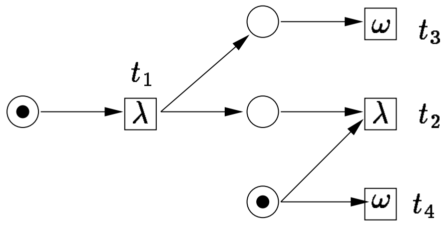

Figure 1:

To show the coincidence of $\sqsupseteq_2^c$ and $\sqsupseteq_2^{nz}$, one could try to prove an analogue to Lemma 3.5; unfortunately, this is not possible (cf. Figure 1): consider a 2-continuous firing sequence $(1)t_1^+t_1^-t_2^+(1)$, where t_2 has to start at time 1 to disable transition t_4. When we try to satisfy the non-zero requirement without changing the transition sequence, t_1^- has to occur *before* time 1 in order to start t_2^+ in time. But now t_3 has to start before time 2; hence, we cannot find a suitable sequence of duration 2. But the following, slightly weaker lemma suffices:

Lemma 3.9

Let $w \in \mathit{2CFS}(N)$ with $\zeta(w) > 0$ and $\delta > 0$. Then there exists some $w' \in \mathit{2NZCFS}(N)$ with $\alpha(w') = \alpha(w)$ and $\zeta(w) - \zeta(w') < \delta$.

Proof: We may assume $\delta < 1$. By Lemma 3.5 and Lemma 3.6, we can assume that in w only (1) occurs as time step and that w starts with (1). We proceed by induction on $|w|$, showing at the same time that for *CID* and *CID'* reached after w and w' we have $\rho - \rho' < \delta - \zeta(w) + \zeta(w')$ and $\rho' > 0$. Note that as a consequence of $\alpha(w') = \alpha(w)$, *CID* and *CID'* coincide in their M-, C- and A-component.

The base case is $w = (1)$; choose $w' = (1 - \frac{\delta}{2}) \in \mathit{2NZCFS}(N)$. Obviously, $\alpha(w') = \alpha(w)$ and $\zeta(w) - \zeta(w') = \frac{\delta}{2} < \delta$; furthermore, $\rho = 0$ and $\rho' = \frac{\delta}{2}$, hence $\rho' > 0$ and $\rho - \rho' = -\frac{\delta}{2} < \delta - \zeta(w) + \zeta(w')$.

Assume we have constructed w and w' with ρ and ρ' as required and $w\varepsilon \in \mathit{2CFS}(N)$. If $\varepsilon = (1)$, we have $\rho = 1$, i.e. $\rho' > 1 - \delta + \zeta(w) - \zeta(w')$; we choose $\gamma > 1 - \delta + \zeta(w) - \zeta(w')$ less than the minimal value of ρ'. Thus, (γ) is an allowable time step after w', i.e. $w'(\gamma) \in \mathit{2NZCFS}(N)$ with $\alpha(w'(\gamma)) = \alpha(w(1))$. Furthermore, $\zeta(w(1)) - \zeta(w'(\gamma)) = \zeta(w) + 1 - \zeta(w') - \gamma < \delta$ by the lower bound on γ. Finally, for the residual times ρ_1 after $w(1)$ and ρ_1' after $w'(\gamma)$, we have $\rho_1' = \rho' - \gamma > 0$ and $\rho_1 - \rho_1' = -\rho_1' < 0 < \delta - \zeta(w(1)) + \zeta(w'(\gamma))$.

If ε is a transition part, we choose $\gamma > 0$ less than the minimal values of ρ' and $\rho' - \rho + \delta - \zeta(w) + \zeta(w')$. Then, $w'(\gamma)\varepsilon \in \mathit{2NZCFS}(N)$ with $\alpha(w'(\gamma)\varepsilon) = \alpha(w\varepsilon)$ and $\zeta(w\varepsilon) - \zeta(w'(\gamma)\varepsilon) = \zeta(w) - \zeta(w') - \gamma < \zeta(w) - \zeta(w') < \delta$. Finally, for the residual times ρ_1 after $w\varepsilon$ and ρ_1' after $w'(\gamma)\varepsilon$, we have that ρ_1' has value $1 > 0$ for the newly activated transitions resp. newly started transition or the same value as $\rho' - \gamma > 0$ and that $\rho_1 - \rho_1'$ has value $1 - 1 = 0 < \delta - \zeta(w\varepsilon) + \zeta(w'(\gamma)\varepsilon)$ or the value of $\rho - (\rho' - \gamma) < \delta - \zeta(w) + \zeta(w')$ by choice of γ, and $\delta - \zeta(w) + \zeta(w') < \delta - \zeta(w\varepsilon) + \zeta(w'(\gamma)\varepsilon)$. ■ 3.9

Theorem 3.10

The relations $\sqsupseteq_2^c$ and $\sqsupseteq_2^{nz}$ coincide.

Proof: For testable nets N_1 and N_2 we show $N_1 \sqsupseteq_2^c N_2 \Leftrightarrow N_1 \sqsupseteq_2^{nz} N_2$.
"$\Rightarrow$": Assume a test (O, R) with $N_1 \not\mathit{must}_2^{nz}\ (O, R)$. From $\mathit{2NZCL}(N_1\|_\Sigma O) \subseteq \mathit{2CL}(N_1\|_\Sigma O)$ we conclude $N_1 \not\mathit{must}_2^{c}\ (O, R)$ and by hypothesis $N_2 \not\mathit{must}_2^{c}\ (O, R)$. For a $w \in \mathit{2CL}(N_2\|_\Sigma O)$ with $\zeta(w) > R$ that contains no ω^+ let $\delta = \zeta(w) - R$. Using Lemma 3.9, we find a $w' \in \mathit{2NZCL}(N_2\|_\Sigma O)$ with $\alpha(w') = \alpha(w)$ and $\zeta(w') > \zeta(w) - \delta > R$ that contains no ω^+ either, and we conclude $N_2 \not\mathit{must}_2^{nz}\ (O, R)$.
"$\Leftarrow$": Assume a test (O, R) with $N_1 \not\mathit{must}_2^{c}\ (O, R)$. As above, Lemma 3.9 yields $N_1 \not\mathit{must}_2^{nz}$ (O, R) and by hypothesis $N_2 \not\mathit{must}_2^{nz}\ (O, R)$. Again from $\mathit{2NZCL}(N_2\|_\Sigma O) \subseteq \mathit{2CL}(N_2\|_\Sigma O)$ we conclude $N_2 \not\mathit{must}_2^{c}\ (O, R)$. ■ 3.10

Our aim is now to normalize the 2-discrete language *2DL* to a simpler language *2L*. Starting from *2L*, it will be easier to find a characterization for the testing preorder $\sqsupseteq_2^c$. We will write the time steps (1) as σ and assume, using Lemma 3.6, that all sequences start with a σ; the initial σ is left implicit, i.e. it will actually be omitted. The behaviour inbetween two σ's is called a *round*.

On the level of 2-discrete firing sequences, we have three different kinds of firing events within a round. Firstly, there are transitions that fire in zero-time, indicated by a t^+ and – within the same round – the next corresponding t^-. In the simple language we are going to define, these events will simply be expressed by t in place of the t^+, omitting the t^-, for starting and ending of the transition occur at the same time. Secondly, there are transitions that start but will only end in the next round, indicated by a t^+ not followed by the corresponding t^- in the same round. We adopt these t^+ in the simple language. Thirdly, there are transitions that have started one round before and are ending in the present round, indicated by a t^- not preceded by the corresponding t^+ in the present round. In the simple language we omit these t^-, for this event is completely described by the corresponding t^+ one round before and the following σ. We impose an ordering between the different types of events within a round, i.e. all t will occur before the t^+. The sequence of the t^+ corresponds to a step of transitions that are firing during the following σ; so our firing rule in fact allows a step μ followed by σ and we can omit the set C of current transitions in the instantaneous description. To have a linear notation, we will write a step μ as a sequence of t^+. Finally, we can resign the residual time function ρ as it has only values in $\{0, 1\}$; we replace it by a set U of urgent transitions containing those transitions with $\rho(t) = 0$.

Definition 3.11 *instantaneous description*

An *instantaneous description ID* of a net is a tuple (M, U) consisting of a marking M of N and a set U of *urgent transitions*. The initial *ID* ist $ID_N = (M_N, U_N)$ with $U_N = \{t \mid M_N[t\rangle\}$.

We write $(M, U)[\varepsilon\rangle_2(M', U')$ if one of the following cases applies:

1. $\varepsilon = t \in T$, $M[t\rangle M'$, $U' = U \setminus ({}^\bullet t)^\bullet$
2. $\varepsilon = \mu\sigma$, $\mu \subseteq T$, $M[\mu\rangle M'$, $U \setminus ({}^\bullet \mu)^\bullet = \emptyset$, $U' = \{t \mid (M - {}^\bullet\mu)[t\rangle\}$

In case 2, the step μ will often be written as the sequence of its plussed elements. (More precisely as one of these sequences.) Especially, it can be the empty set yielding an empty sequence.

The set $2FS(N) = \{w \mid ID_N[w\rangle_2 ID\}$ is the set of *(2-firable) 2-firing sequences* of N, the set $2L(N) = \{l(w) \mid w \in 2FS(N)\}$ is the *2-language* of N containing the *2-traces* of N. As in Definition 3.1, we let l preserve time steps, i.e. $l(\sigma) = \sigma$ and $l(\mu) \in \mathcal{M}(\Sigma')$ is a (finite) multiset of actions from Σ'. We extend $\zeta(w)$ to elements of $2FS$ and $2L$ in the obvious way, i.e. $\zeta(w)$ is the number of σ's in w.

The behaviour inbetween two $\sigma's$ is called a *round*. In a round of the form $t_1t_2\dots\mu$, the t_i *start* and *end* in this round, while the transitions in μ start in the present round and end in the next.

A testable net N *satisfies* a *discretely timed test* (O, D), N *must*$_2$ (O, D), if each $w \in 2L(N\|_\Sigma O)$ with $\zeta(w) \geq D$ contains some ω, and define

$$N_1 \sqsupseteq_2 N_2 \Leftrightarrow (\ \forall (O, D) : N_2\ must_2\ (O, D) \Rightarrow N_1\ must_2\ (O, D)\,)$$

■ 3.11

The initial set U_N contains all initially activated transitions as we assume an ('invisible') (1)-time-step at the beginning of the sequence. When defining satisfaction of a test, we consider sequences w with $\zeta(w) \geq D$, because due to the invisible (1)-time-step these are the sequences with $\zeta(w) > D$ from the *2DL*-point of view. The condition $U \setminus ({}^\bullet\mu)^\bullet = \emptyset$ ensures that all remaining urgent transitions are started or deactivated by the step. Time passes during the step, i.e. between the start and the end of the step; therefore, transitions that are enabled after the start, i.e. under $M - {}^\bullet\mu$, are urgent after the end.

Theorem 3.12

The relations $\sqsupseteq_2^c$ and $\sqsupseteq_2$ coincide.

Proof: By Theorem 3.7, we have to show that $\sqsupseteq_2^d$ and $\sqsupseteq_2$ coincide. Since these relations are based on the same tests, it suffices to show that a testable net N *must*$_2^d$ (O, D) iff it *must*$_2$ (O, D). For this, in turn, it suffices to show that, for a net N and $D \in \mathbb{N}_0$, there exists some $w \in 2DFS(N)$ with $\zeta(w) > D$ not containing the start of an ω-transition iff there exists some $v \in 2FS(N)$ with $\zeta(v) \geq D$ not containing an ω-transition. We may assume that w ends with (1) and v with σ, since further transition parts or transitions do not make w or v last longer; by Lemma 3.6, we may further assume that w starts with (1).

We observe some possible transformations for w: if a round of w has the form $w_1\varepsilon t^- w_2$ with $\varepsilon \in T^\pm$ and $\varepsilon \neq t^+$, we can replace it by $w_1 t^- \varepsilon w_2$ getting a 2d-firing sequence that reaches the same *CID* after this round and in the end; similarly, we can change $t^+\varepsilon$ to εt^+ for $\varepsilon \in T^\pm$ with $\varepsilon \neq t^-$. Hence, we may assume that each round of d has the form $w_i^- w_i w_i^+$, where w_i^- consists of transition ends, w_i has the form $t_1^+t_1^-t_2^+t_2^- \dots t_n^+t_n^-$, and w_i^+ consists of transition starts.

Let $w = (1)w_1^- w_1 w_1^+(1)\dots w_n^- w_n w_n^+(1) \in 2DFS(N)$ be of this form; then the transitions in w_i^+ must end firing in the next round, i.e. w_i^+ consists of the same transitions as w_{i+1}^- for $i = 1, \dots, n-1$, and we have $w_1^- = \lambda$. For w we construct $v =$

$v_1\mu_1\sigma \ldots v_n\mu_n\sigma$ as follows: v_i is w_i with each pair $t_j^+t_j^-$ replaced by t_j; μ_i consists of the transitions listed in w_i^+. Vice versa, from $v = v_1\mu_1\sigma \ldots v_n\mu_n\sigma \in \mathit{2FS}(N)$ we construct $w = (1)w_1^- w_1 w_1^+(1) \ldots w_n^- w_n w_n^+(1)$ by: w_i is v_i with each t_j replaced by $t_j^+t_j^-$; w_i^+ and w_{i+1}^- list the transitions in μ_i as starts, as ends resp. Since $\zeta(w) = n+1 > D$ iff $\zeta(v) = n \geq D$, it remains to show that, for these constructions, w is 2d-firable iff v is 2-firable.

For this proof, we use the notation given by

$$\mathit{CID}_N[(1)w_1^-\rangle_2^c \mathit{CID}_1[w_1\rangle_2^c \mathit{CID}_1'[w_1^+\rangle_2^c \mathit{CID}_1''[(1)w_2^-\rangle_2^c \mathit{CID}_2 \ldots \mathit{CID}_n'[w_n^+\rangle_2^c \mathit{CID}_n''[(1)\rangle_2^c$$

and

$$\mathit{ID}_N = \mathit{ID}_1[v_1\rangle_2 \mathit{ID}_1'[\mu_1\sigma\rangle_2 \mathit{ID}_2 \ldots \mathit{ID}_n'[\mu_n\sigma\rangle_2.$$

Obviously, the M-parts are transformed in the same way by w and v, i.e. the M-parts of CID_i and ID_i coincide (and are both denoted M_i by our convention anyway) and also the M-parts of CID_i' and ID_i' (denoted M_i'). Additionally to the firability of w and v, we show by induction that $C_i = \emptyset$ and U_i consists of those $t \in A_i$ with $\rho_i(t) = 0$, while $\rho_i(t) = 1$ for $t \in A_i - U_i$. This is true for $i = 1$; so we now assume it for i.

Enabledness of w_i and v_i only depends on M_i, so one is enabled if the other is; obviously, $C_i' = \emptyset$ since $C_i = \emptyset$. Firing v_i, a transition t is removed from U_i if it is fired or disabled; hence, either $t \notin A_i'$ or t is enabled again with ρ-value 1. Hence, $U_i' = \{t \in A_i' \mid \rho_i'(t) = 0\}$. Now $\mathit{CID}_i'[w_i^+\rangle_2^c \mathit{CID}_i''[(1)\rangle_2^c$ iff the transitions in w_i^+ form the enabled step μ_i such that no transition in $A_i'' \subseteq A_i'$ has ρ_i''-value 0 iff $M_i'[\mu_i\rangle_2$ and $U_i' \setminus ({}^\bullet\mu_i)^\bullet = \emptyset$ (since $A_i'' = A_i' \setminus ({}^\bullet\mu_i)^\bullet$ and $\rho_i''|_{A_i''} = \rho_i'|_{A_i''}$) iff $\mathit{ID}_i'[\mu_i\sigma\rangle_2$. By the form of w, it is obvious that $\mathit{CID}_i'[w_i^+(1)w_{i+1}^-\rangle_2^c$ iff $\mathit{CID}_i'[w_i^+(1)\rangle_2^c$ for $i < n$.

It remains to relate CID_{i+1} and ID_{i+1} for $i < n$. As remarked, the M-parts coincide, and by the form of w we have $C_{i+1} = \emptyset$. All transitions in $A_i'' = \{t \mid (M_i' - {}^\bullet\mu_i)[t\rangle\} = U_{i+1}$ have ρ_i''-value 1, hence ρ_{i+1}-value 0; all transitions in $A_{i+1} - A_i''$ are newly activated by w_{i+1}^-, hence they have ρ_{i+1}-value 1. Thus, we are done. ■ 3.12

4 Characterization of the Testing Preorder

Our aim is now to characterize the testing-preorder $\sqsupseteq_2$. In the classical case [DNH84], this is done by the failure semantics which contains pairs (w, X) where w is an executable action sequence and X is a set of actions that can be refused by the system in the state reached after w. Sometimes, the characterization also needs this refusal information in intermediate states occurring during execution of the sequence, yielding a refusal trace semantics [Phi87]. To understand our characterization of $\sqsupseteq_2$, an unusual view of failure semantics proposed in [JV95] seems again appropriate: if (w, X) is a failure pair, w is a partial run of the system, i.e. the system is (possibly) stopped prematurely; but the actions in X are treated correctly when the system is stopped, since they are not possible at this stage. What we need to characterize $\sqsupseteq_2$ is a kind of refusal trace semantics which gives information on correctly treated actions.

Instead of the σ, we use a set X of correctly treated actions to indicate a time-step. The set X contains actions that are not urgent when the time-step occurs, i.e. are treated properly concerning the condition $U \setminus ({}^\bullet\mu)^\bullet = \emptyset$. Internal actions always have to be treated properly.

Definition 4.1 *refusal firing sequences*

For instantaneous descriptions (M, U) and (M', U') we write $(M, U)[\varepsilon\rangle_2^r(M', U')$ if one of the following cases applies:

1. $\varepsilon = t \in T,\ M[t\rangle M',\ U' = U \setminus ({}^\bullet t)^\bullet$
2. $\varepsilon = \mu X,\ \mu \subseteq T,\ X \subseteq \Sigma',\ M[\mu\rangle M',\ U' = \{t \mid (M - {}^\bullet\mu)[t\rangle\},$
   $\forall t \in U \setminus ({}^\bullet\mu)^\bullet : l(t) \notin X \cup \{\lambda\}$

The initial *ID* is $ID_N = (M_N, U_N)$ with $U_N = \{t \mid M_N[t\rangle\}$. The corresponding sequences are called *(2r-firable) 2-refusal firing sequences*, their set is denoted by *2RFS*(N). *2RT*$(N) = \{l(w) \mid w \in$ *2RFS*$(N)\}$ is the set of 2-*refusal traces* where $l(\mu X) = l(\mu)X$. If $ID[w\rangle_2^r ID'$, we write $ID[l(w)\rangle\rangle_2^r ID'$. To have a linear notation, μ will be written as a sequence of its plussed elements. This carries over to the level of 2-refusal traces. ∎ 4.1

It is not hard to see that the *2RT*-semantics is more detailed than the *2L*-semantics.

Proposition 4.2

For nets N_1 and N_2, *2RT*$(N_1) \subseteq$ *2RT*(N_2) implies *2L*$(N_1) \subseteq$ *2L*(N_2).

Proof: To obtain *2L*(N) from *2RT*(N) take those sequences in which all parts μX satisfy $X = \Sigma'$ by replacing $\mu\Sigma'$ by $\mu\sigma$. ∎ 4.2

Now we want to show that the *2RT*-semantics induces a congruence for parallel composition; for this, we define $\|_A$ for 2-refusal traces. When composing u and v to w, actions from A are merged, while others are interleaved. Steps must coincide on the synchronized actions from A while actions from $\Sigma' \setminus A$ are added up. A combined transition (t_1, t_2) of some $N_1\|_A N_2$ is enabled, if t_1 is enabled in N_1 and t_2 is enabled in N_2; hence (t_1, t_2) is urgent only if t_1 and t_2 are urgent. In w, actions from A are treated correctly concerning the condition $U \setminus ({}^\bullet\mu)^\bullet = \emptyset$ if they are treated correctly in u or v, while the others have to be treated correctly in both, u and v.

Definition 4.3 *shuffle of traces w.r.t. A*

Let $u, v \in (\Sigma' \cup (\mathcal{M}(\Sigma') \times \mathcal{P}(\Sigma')))^*$, $A \subseteq \Sigma'$. Then $u \|_A v$ is the set of all $w \in (\Sigma' \cup (\mathcal{M}(\Sigma') \times \mathcal{P}(\Sigma')))^*$ such that for some n $u = u_1 \dots u_n$, $v = v_1 \dots v_n$, $w = w_1 \dots w_n$ and for $i = 1, \dots, n$ one of the following cases applies:

1. $u_i = v_i = w_i \in A$
2. $u_i = w_i \in (\Sigma' - A)$ and $v_i = \lambda$
3. $v_i = w_i \in (\Sigma' - A)$ and $u_i = \lambda$
4. $u_i, v_i, w_i \in (\mathcal{M}(\Sigma') \times \mathcal{P}(\Sigma'))$, $u_i = p_1 X_1$, $v_i = p_2 X_2$, $w_i = pX$,
   $\forall a \in A :\ p_1(a) = p_2(a) = p(a),\quad \forall a \in (\Sigma' - A) :\ p(a) = p_1(a) + p_2(a),$
   $X \subseteq ((X_1 \cup X_2) \cap A) \cup (X_1 \cap X_2)$

∎ 4.3

Note that any refusal trace can formally be enriched by 'inserting' $\lambda's$ at any place, i.e. there is no need for underlying λ-labelled transitions.

Definition 4.4 *A-Combination of ID's*

Let N_1, N_2 be nets, $A \subseteq \Sigma'$, and $N = (N_1 \|_A N_2)$. Let ID, ID_1, ID_2 be reachable instantaneous descriptions of N, N_1, N_2, respectively. Then $ID = (M, U)$ is the *A-combination* of $ID_1 = (M_1, U_1)$ and $ID_2 = (M_2, U_2)$ if

$$\begin{array}{rcl} M((s_1,*)) & = & M_1(s_1) \text{ for } s_1 \in S_1 \\ M((*,s_2)) & = & M_2(s_2) \text{ for } s_2 \in S_2 \\ U & = & ((U_1 \times \{*\}) \cup (U_1 \times U_2) \cup (\{*\} \times U_2)) \cap T \end{array} \qquad \blacksquare\, 4.4$$

The reason for the last equation is again that a synchronized transition is urgent iff both its components are urgent. The following technical lemma is essential for the proof that we have defined $\|_A$ appropriately for refusal traces. Here $proj_i$ denotes the projection onto the i-th component; we assume that $proj_1(*, t_2)$ and $proj_2(t_1, *)$ are undefined for all t_1, t_2 and that in this case statements like $proj_i(t) \notin U_i$ are false, as they violate an implicit definedness. For a set μ, $proj_i(\mu)$ is the set of all defined $proj_i(t)$ with $t \in \mu$.

Lemma 4.5

Let N_1, N_2 be nets, $A \subseteq \Sigma'$, and $N = (N_1 \|_A N_2)$. Let $ID_1 = (M_1, U_1)$, $ID_2 = (M_2, U_2)$ and $ID = (M, U)$ be reachable discrete instantaneous descriptions of N_1, N_2, N, respectively, such that ID is the A-combination of ID_1 and ID_2.

1. If $ID[\varepsilon\rangle_2^r$ in N according to Definition 4.1 1. or 2., then there are ε_1, ε_2 such that $ID_1[\varepsilon_1\rangle_2^r$ in N_1, $ID_2[\varepsilon_2\rangle_2^r$ in N_2 and one of the following cases applies:
   (a) $\varepsilon = (t_1, t_2)$, $\varepsilon_1 = t_1$, $\varepsilon_2 = t_2$, $l_1(t_1) = l_2(t_2) \in A$
   (b) $\varepsilon = (t_1, *)$, $\varepsilon_1 = t_1$, $\varepsilon_2 = \lambda$, $l_1(t_1) \notin A$
   (c) Analogously for $\varepsilon = (*, t_2)$
   (d) $\varepsilon = \mu X$, $\varepsilon_1 = \mu_1 X_1$, $\varepsilon_2 = \mu_2 X_2$,
   $\mu_1 = proj_1(\mu)$, $\mu_2 = proj_2(\mu)$,
   $X \subseteq ((X_1 \cup X_2) \cap A) \cup (X_1 \cap X_2)$
2. Let $ID_1[\varepsilon_1\rangle_2^r$ and $ID_2[\varepsilon_2\rangle_2^r$ according to Definition 4.1 1. or 2.
   (a) If $\varepsilon_1 = t_1$, $\varepsilon_2 = t_2$, $l_1(t_1) = l_2(t_2) \in A$, then $ID[\varepsilon\rangle_2^r$ with $\varepsilon = (t_1, t_2)$.
   (b) If $\varepsilon_1 = t_1$, $\varepsilon_2 = \lambda$, $l_1(t_1) \notin A$, then $ID[\varepsilon\rangle_2^r$ with $\varepsilon = (t_1, *)$.
   (c) Analoguosly for $\varepsilon_2 = t_2$, $l_2(t_2) \notin A$
   (d) If $\varepsilon_1 = \mu_1 X_1$ and $\varepsilon_2 = \mu_2 X_2$, then $ID[\varepsilon\rangle_2^r$ for all $\varepsilon = \mu X$ with
   $\mu \subseteq T$, $proj_1(\mu) = \mu_1$, $proj_2(\mu) = \mu_2$, both injective,
   $X \subseteq ((X_1 \cup X_2) \cap A) \cup (X_1 \cap X_2)$

Furthermore in both cases, if for these ε, ε_1, ε_2 we have that $ID[\varepsilon\rangle_2^r ID'$, $ID_1[\varepsilon_1\rangle_2^r ID_1'$, $ID_2[\varepsilon_2\rangle_2^r ID_2'$, then ID' is the A-combination of ID_1' and ID_2'.

Proof: 1. Cases (a)-(c) are straightforward but technically expensive. E.g. for (a) we get with Definition 4.4: $M[(t_1, t_2)\rangle M'$ implies $M_1[t_1\rangle M_1'$ and $M_2[t_2\rangle M_2'$ with $M' = M_1' \times \{*\} \cup \{*\} \times M_2'$ and
$U' = U \setminus ({}^\bullet(t_1, t_2))^\bullet = U \setminus (({}^\bullet t_1 \times \{*\})^\bullet \cup (\{*\} \times {}^\bullet t_2)^\bullet) =$
$U \setminus ((({}^\bullet t_1)^\bullet \times \{*\}) \cup (({}^\bullet t_1)^\bullet \times T_2) \cup (T_1 \times ({}^\bullet t_2)^\bullet) \cup (\{*\} \times ({}^\bullet t_2)^\bullet)) =$

$((U_1 \times \{*\}) \setminus ((^\bullet t_1)^\bullet \times \{*\}) \cup (U_1 \times U_2) \setminus (((^\bullet t_1)^\bullet \times T_2) \cup (T_1 \times (^\bullet t_2)^\bullet)) \cup (\{*\} \times U_2) \setminus (\{*\} \times (^\bullet t_2)^\bullet)) \cap T =$
$((U_1 \setminus (^\bullet t_1)^\bullet) \times \{*\} \cup ((U_1 \times U_2) \setminus ((^\bullet t_1)^\bullet \times T_2) \cap (U_1 \times U_2) \setminus (T_1 \times (^\bullet t_2)^\bullet)) \cup \{*\} \times (U_2 \setminus (^\bullet t_2)^\bullet)) \cap T =$
$((U_1 \setminus (^\bullet t_1)^\bullet) \times \{*\} \cup ((U_1 \setminus (^\bullet t_1)^\bullet) \times U_2 \cap U_1 \times (U_2 \setminus (^\bullet t_2)^\bullet)) \cup \{*\} \times (U_2 \setminus (^\bullet t_2)^\bullet)) \cap T =$
$((U_1 \setminus (^\bullet t_1)^\bullet) \times \{*\} \cup (U_1 \setminus (^\bullet t_1)^\bullet) \times (U_2 \setminus (^\bullet t_2)^\bullet) \cup \{*\} \times (U_2 \setminus (^\bullet t_2)^\bullet)) \cap T =$
$((U_1' \times \{*\}) \cup (U_1' \times U_2') \cup (\{*\} \times U_2')) \cap T$,
such that ID' is the A-combination of ID_1' and ID_2'.

In case (d), for $\varepsilon = \mu X$ we have that the corresponding steps $proj_i(\mu)$ can be started under the ordinary firing rule in the N_i, as $^\bullet proj_i(\mu) = proj_i(^\bullet\mu)$; furthermore $proj_i(\mu)^\bullet = proj_i(\mu^\bullet)$ holds.

Assume $\exists t_1 \in U_1 \setminus (^\bullet\mu_1)^\bullet : l_1(t_1) = \lambda$. As λ is not synchronized, we have $(t_1, *) \in U$ and $^\bullet t_1 \cap {}^\bullet\mu_1 = \emptyset$ yields $^\bullet t_1 \times \{*\} \cap {}^\bullet\mu_1 \times \{*\} = {}^\bullet(t_1,*) \cap {}^\bullet\mu = \emptyset$; so $t = (t_1, *) \in U \setminus (^\bullet\mu)^\bullet \wedge l(t) = \lambda$ which is a contradiction to Definition 4.1; the same argument holds for $t_2 \in U \setminus (^\bullet\mu_2)^\bullet$. We choose X_1, X_2 maximal, i.e. $X_i = \Sigma' - l(U_i \setminus (^\bullet\mu_i)^\bullet)$, $i = 1, 2$. Thus μ_1 and μ_2 can occur.

We now show the required inclusion for X. Firstly, let $a \in X$. For $a \in A$ assume $a \notin ((X_1 \cup X_2) \cap A)$, i.e. $a \notin X_1$ and $a \notin X_2$: $\forall i = 1,2\, \exists t_i :\ l_i(t_i) = a \wedge t_i \in U_i \wedge t_i \notin (^\bullet\mu_i)^\bullet$. By Definition 2.1 and Definition 4.4 we conclude that there is a $t = (t_1, t_2)$ in N with $l(t) = a$, $t \in U$ and $t \notin (^\bullet\mu)^\bullet$, as $^\bullet t \cap {}^\bullet\mu = ((^\bullet t_1 \times \{*\}) \cup (\{*\} \times {}^\bullet t_2)) \cap ((^\bullet\mu_1 \times \{*\}) \cup (\{*\} \times {}^\bullet\mu_2)) = ((^\bullet t_1 \times \{*\} \cap (^\bullet\mu_1 \times \{*\})) \cup ((\{*\} \times {}^\bullet t_2) \cap (\{*\} \times {}^\bullet\mu_2)) = ((^\bullet t_1 \cap {}^\bullet\mu_1) \times \{*\}) \cup (\{*\} \times (^\bullet t_2 \cap {}^\bullet\mu_2)) = (\emptyset \times \{*\}) \cup (\{*\} \times \emptyset) = \emptyset$. We get the contradiction $a \notin X$. Now assume $a \in \Sigma' - A$ and $a \notin (X_1 \cap X_2)$. Without loss of generality, let $a \notin X_1$. Then $\exists t_1 :\ l_1(t_1) = a \ \wedge\ t_1 \in U_1 \ \wedge\ t_1 \notin (^\bullet\mu_1)^\bullet$. By a similar argument as above, we get $\exists t = (t_1, *) \in T :\ l(t) = a \ \wedge\ t \in U \ \wedge\ t \notin (^\bullet\mu)^\bullet$. Again we have the contradiction $a \notin X$.

A transition t is in U' iff it is enabled by $M - {}^\bullet\mu$, i.e. one of the following cases applies:

(a) $t = (t_1, *) \in T$ and t_1 is enabled by $M_1 - {}^\bullet\mu_1$, i.e. $t_1 \in U_1'$.
(b) Analogously for $t = (*, t_2)$.
(c) $t = (t_1, t_2) \in T$ and t_1 is enabled by $M_1 - {}^\bullet\mu_1$ and t_2 is enabled by $M_2 - {}^\bullet\mu_2$, i.e. $t_1 \in U_1'$ and $t_2 \in U_2'$.

We conclude, that ID' is again the A-combination of ID_1' and ID_2'.

2. Cases (a)-(c) are similar to those in 1. In case (d), assume there is a $\mu \subseteq T$ with $proj_1(\mu) = \mu_1$, $proj_2(\mu) = \mu_2$ and both projections are injective. Then μ is enabled by ID in N, as $^\bullet\mu = proj_1(^\bullet\mu) \times \{*\} \cup \{*\} \times proj_2(^\bullet\mu) = {}^\bullet proj_1(\mu) \times \{*\} \cup \{*\} \times {}^\bullet proj_2(\mu) = {}^\bullet\mu_1 \times \{*\} \cup \{*\} \times {}^\bullet\mu_2$ and μ_1, μ_2 are enabled in N_1, N_2 respectively; suppose we omit the injectivity, e.g. (t_1, t_2) and (t_1, t_2') are elements of μ; then μ cannot be enabled as the nets are safe and t_1 is not enabled twice in N_1.

   Finally we have to check the correcteness of X. Let $a \in (X_1 \cup X_2) \cap A$ and assume $a \in X$ were not possible. Then $\exists t = (t_1, t_2) \in U :\ {}^\bullet t \cap {}^\bullet\mu = \emptyset \wedge l(t) = a$. But then we have $t_1 \in U_1 \wedge {}^\bullet t_1 \cap {}^\bullet\mu_1 = \emptyset \wedge l_1(t_1) = a \wedge t_2 \in U_2 \wedge {}^\bullet t_2 \cap {}^\bullet\mu_2 = \emptyset \wedge l_2(t_2) = a$, so $a \notin X_1$ and $a \notin X_2$, a contradiction. Let $a \in X_1 \cap X_2$, $a \notin A$ and assume $a \in X$ is not allowed. Then $\exists t = (t_1, *) \in U :\ {}^\bullet t \cap {}^\bullet\mu = \emptyset \wedge l(t) = a$ or $\exists t = (*, t_2) \in U :$

${}^\bullet t \cap {}^\bullet \mu = \emptyset \wedge l(t) = a$. But then we also have $\exists t_1 \in U_1 : {}^\bullet t_1 \cap {}^\bullet \mu_1 = \emptyset \wedge l_1(t_1) = a$ or $\exists t_2 \in U_2 : {}^\bullet t_2 \cap {}^\bullet \mu_2 = \emptyset \wedge l_2(t_2) = a$, i.e. $a \notin X_1$ or $a \notin X_2$, again a contradiction. μX may occur in N.

By similar arguments as in 1. we conclude that ID' is again the A-combination of ID'_1 and ID'_2.

■ 4.5

We are now ready to state the congruence result of *2RT*-semantics.

Theorem 4.6

For nets N_1 and N_2 and $A \subseteq \Sigma'$ we have

$$2RT(N_1 \|_A N_2) = \bigcup \{u_1 \|_A u_2 \mid u_1 \in 2RT(N_1),\ u_2 \in 2RT(N_2)\}.$$

Proof: Let $N = N_1 \|_A N_2$.

"$\subseteq$":

Let $u \in 2RT(N)$. Then there is a $w \in 2RFS(N)$ with $l(w) = u$. We perform induction on the length of w and show that if $ID_N[w\rangle_2^r ID$ then there are $w_1 \in 2RFS(N_1)$ and $w_2 \in 2RFS(N_2)$ such that $u = l(w) \in (l_1(w_1) \|_A l_2(w_1))$ and if $ID_{N_1}[w_1\rangle_2^r ID_1$ and $ID_{N_2}[w_2\rangle_2^r ID_2$ then ID is the A-combination of ID_1 and ID_2.

For $w = \lambda$ we choose $w_1 = w_2 = \lambda$ such that $l(w) \in (l_1(w_1) \|_A l_2(w_2))$ and $ID = ID_N$ is the A-combination of $ID_1 = ID_{N_1}$ and $ID_2 = ID_{N_2}$.

Let $w' = w\varepsilon$ and $ID[\varepsilon\rangle_2^r ID'$, where ID is reached after w . Then one of the following cases applies:

1. $\varepsilon = t = (t_1, t_2)$, $l(t) = a \in A$. So $u' = ua$ and by Lemma 4.5.1.(a) there are $\varepsilon_1 = t_1$ and $\varepsilon_2 = t_2$ with $l_1(t_1) = l_2(t_2) = a \in A$, $ID_1[\varepsilon_1\rangle_2^r ID'_1$, $ID_2[\varepsilon_2\rangle_2^r ID'_2$ and ID' is the A-combination of ID'_1 and ID'_2. We get $l_1(w'_1) = l_1(w_1 t_1) = l_1(w_1)a$ and $l_2(w'_2) = l_2(w_2 t_2) = l_2(w_2)a$ and by Definition 4.3.1., from $u \in (l_1(w_1) \|_A l_2(w_2))$ we conclude $u' = ua \in (l_1(w_1)a \|_A l_2(w_1)a) = (l_1(w'_1) \|_A l_2(w'_2))$.
2. $\varepsilon = t = (t_1, *)$, $l(t) = a \notin A$. So $u' = ua$ and by Lemma 4.5.1.(b) there are $\varepsilon_1 = t_1$ and $\varepsilon_2 = \lambda$ with $l_1(t_1) = a \notin A$, $ID_1[\varepsilon_1\rangle_2^r ID'_1$, $ID_2[\varepsilon\rangle_2^r ID'_2 = ID_2$ and ID' is the A-combination of ID'_1 and ID'_2. We get $l_1(w'_1) = l_1(w_1 t_1) = l_1(w_1)a$ and $l_2(w'_2) = l_2(w_2)$ and by Definition 4.3.2., from $u \in (l_1(w_1) \|_A l_2(w_2))$ we conclude $u' = ua \in (l_1(w_1)a \|_A l_2(w_2)) = (l_1(w'_1) \|_A l_2(w'_2))$.
3. Analogously for $\varepsilon = (*, t_2)$ with Definition 4.3.3. and Lemma 4.5.1.(c).
4. $\varepsilon = \mu X$, so $u' = ul(\mu)X$ and by Lemma 4.5.1.(d) there are $\varepsilon_1 = \mu_1 X_1$ and $\varepsilon_2 = \mu_2 X_2$ with $ID_1[\varepsilon_1\rangle_2^r ID'_1$, $ID_2[\varepsilon_2\rangle_2^r ID'_2$ such that ID' is the A-combination of ID'_1 and ID'_2. From $\mu_1 = proj_1(\mu)$ and $\mu_2 = proj_2(\mu)$ we conclude $\forall a \in A : l_1(\mu_1)(a) = l_2(\mu_2)(a) = l(\mu)(a)$ and $\forall a \in \Sigma' - A : l(\mu)(a) = l_1(\mu_1)(a) + l_2(\mu_2)(a)$. Finally, we have $X \subseteq ((X_1 \cup X_2) \cap A) \cup (X_1 \cap X_2)$. By Definition 4.3.4., from $u \in (l_1(w_1) \|_A l_2(w_2))$ we conclude $u' = ul(\mu)X \in (l_1(w_1)l_1(\mu_1)X_1) \|_A (l_2(w_2)l_2(\mu_2)X_2) = (l_1(w'_1) \|_A l_2(w'_2))$.

"$\supseteq$":

We show that for all w_1, w_2 with $ID_{N_1}[w_1\rangle_2^r ID_1$ and $ID_{N_2}[w_2\rangle_2^r ID_2$, for all $u \in l_1(w_1) \|_A l_2(w_2)$

there is a $w \in \mathit{2RFS}(N)$ with $l(w) = u$ and if $ID_N[w\rangle_2^r ID$ then ID is the A-combination of ID_1 and ID_2. We perform induction on the sum of lengths of w_1 and w_2.

For $|w_1| + |w_2| = 0$ we have $l_1(w_1) = l_2(w_2) = \lambda$, so $l_1(w_1)\|_A l_2(w_2) = \{\lambda\}$ and $u = \lambda$ has the underlying firing sequence $w = \lambda \in \mathit{2RFS}(N)$. We also have that $ID = ID_N$ is the A-combination of $ID_1 = ID_{N_1}$ and $ID_2 = ID_{N_2}$. Now we distinguish several cases:

1. $w_1 = w_1' t_1$ with $l_1(t_1) = \lambda$. Then $l_1(w_1) = l_1(w_1')$ and for $u \in l_1(w_1')\|_A l_2(w_2)$, by induction hypothesis there is a w in $\mathit{2RFS}(N)$ with $l(w) = u$. As λ is not synchronized, we have that $(t_1, *) \in T$ can fire iff t_1 can fire in N_1 and conclude, that if $ID_N[w'\rangle_2^r ID[(t_1,*)\rangle_r ID'$ and $ID_{N_1}[w_1'\rangle_2^r ID_1[t_1\rangle_2^r ID_1'$ and $ID_{N_2}[w_2\rangle_2^r ID_2 = ID_2'$ then by Lemma 4.5.2.(b) ID' is the A-combination of ID_1' and ID_2'.
2. Analogouosly for $w_2 = w_2' t_2$ with $l_2(t_2) = \lambda$.
3. Not 1. or 2., but $u = u'a$ and $a \in A$. Then by Definition 4.3.1. $w_1 = w_1' t_1$ and $w_2 = w_2' t_2$ with $l_1(t_1) = l_2(t_2) = a$ and $ID_1[t_1\rangle_2^r ID_1'$ and $ID_2[t_2\rangle_2^r ID_2'$. By Lemma 4.5.2.(a) there is $t = (t_1, t_2) \in T$ such that $ID[t\rangle_2^r ID'$ and ID' is the A-combination of ID_1' and ID_2', i.e. as we have a $w' \in \mathit{2RFS}(N)$ with $l(w') = u'$ we now get a $w = w't \in \mathit{2RFS}(N)$ such that $l(w) = u'a$.
4. Not 1. or 2., but $u = u'a$ and $a \notin A$. Then by Definition 4.3.2. and 3., we must have $w_1 = w_1' t_1$ with $l_1(t_1) = a$ or $w_2 = w_2' t_2$ with $l_2(t_2) = a$. Now by Lemma 4.5.2.(b) and (c) we have $t = (t_1, *)$ resp. $t = (*, t_2)$ such that $ID[t\rangle_2^r ID'$ and ID' is the A-combination of ID_1' and ID_2', i.e. $w = w'(t_1, *)$ resp. $w = w'(*, t_2)$, $w \in \mathit{2RFS}(N)$ and $l(w) = u'a$.
5. Not 1. or 2., but $u = u'pX$. Then by Definition 4.3.4., we must have $w_1 = w_1' \mu_1 X_1$ and $w_2 = w_2' \mu_2 X_2$. We construct μ as follows: For all $t_1 \in \mu_1$, if $l_1(t_1) \in \Sigma' - A$ then we put $(t_1, *)$ in μ. The same applies analogously for all $t_2 \in \mu_2$. For all $a \in A$ combine each a-labelled transition $t_1 \in \mu_1$ with an a-labelled transition $t_2 \in \mu_2$. Let all these combined transitions (t_1, t_2) be elements of μ. By Definition 4.3.4 and this construction, we have $l_1(\mu_1)|_A = l_2(\mu_2)|_A = l(\mu)|_A$ and $l(\mu)|_{\Sigma'-A} = l_1(\mu_1)|_{\Sigma'-A} + l_2(\mu_2)|_{\Sigma'-A}$, i.e. $\mathit{proj}_1(\mu) = \mu_1$, $\mathit{proj}_2(\mu) = \mu_2$, both injective and $l(\mu) = p$. Finally, we have $X \subseteq ((X_1 \cup X_2) \cap A) \cup (X_1 \cap X_2)$. So by Lemma 4.5.2.(d), $ID[\mu X\rangle_2^r ID'$ and ID' is the A-combination of ID_1' and ID_2', i.e. $w = w'\mu X$, $w \in \mathit{2RFS}(N)$ and $l(w) = u'pX$.

■ 4.6

With this result we are now able to characterize the testing-preorder.

Theorem 4.7

Let N_1 and N_2 be testable nets. Then $N_1 \sqsupseteq_2 N_2$ if and only if $\mathit{2RT}(N_1) \subseteq \mathit{2RT}(N_2)$.

Proof:
"if": Let (O, D) be a timed test. Then $\mathit{2RT}(N_1) \subseteq \mathit{2RT}(N_2)$ implies $\mathit{2L}(N_1\|_\Sigma O) \subseteq \mathit{2L}(N_2\|_\Sigma O)$ by Theorem 4.6 and Proposition 4.2. Thus, if N_1 fails the test due to some $w \in \mathit{2L}(N_1\|_\Sigma O)$, then so does N_2.
"only if": In this proof upper indices are used; e.g. a_1^2 is an item with two indices

in the following and *not* the string a_1a_1. We assume $N_1 \sqsupseteq_2 N_2$ and take some $w = a_1^1 \dots a_{n_1}^1 b_1^{1+} \dots b_{m_1}^{1+} X^1 \dots a_1^L \dots a_{n_L}^L b_1^{L+} \dots b_{m_L}^{L+} X^L \in \mathit{2RT}(N_1)$, where L, $m_i, n_i \in \mathbb{N}_0$. (All discrete refusal traces of N_1 can be extended to end with a set, hence it is enough to consider traces of this form.) We may assume that $X^j \subseteq l_1(T_1) \cup l_2(T_2)$, i.e. X^j is finite ($j = 1, \dots, L$), since $\mathit{2RT}(N)$ is closed under addition and removal of actions that do not appear in N at all to resp. from the X-sets. We construct a test (O, D) that a net fails if and only if it has w as discrete refusal trace. Then N_1 fails (O, D), hence N_2 does and we are done. We define O as follows. See Figure 2 for the case $w = ab^+\{x\}d\emptyset$.

$$
\begin{aligned}
S_O \quad = \quad & \{s_i^j \mid j = 1, \dots, L+1;\ i = 0, 1, 2\} \cup \{s_1^{L+2}\} \\
& \cup \{s_{ai}^j \mid j = 1, \dots, L;\ i = 1, \dots, n_j + 1\} \\
& \cup \{s_{rx}^j \mid j = 1, \dots, L;\ x \in X^j\} \\
& \cup \{s_{bi1}^j, s_{bi2}^j \mid j = 1, \dots, L;\ i = 1, \dots, m_j\}
\end{aligned}
$$

$$
\begin{aligned}
T_O \quad = \quad & \{t_i^j \mid j = 1, \dots, L+1;\ i = 0, 1, 2\} \cup \{t_1^{L+2}\} \\
& \cup \{t_{ai}^j \mid j = 1, \dots, L;\ i = 1, \dots, n_j\} \\
& \cup \{t_{rx}^j \mid j = 1, \dots, L;\ x \in X^j\} \\
& \cup \{t_{bi}^j, t_{bi1}^j, t_{bi2}^j \mid j = 1, \dots, L;\ i = 1, \dots, m_j\}
\end{aligned}
$$

O has arcs for the following pairs:

(s_0^j, t_0^j), $j = 1, \dots, L+1$;
(t_0^j, s_0^{j+1}), $j = 1, \dots, L$;
(t_0^j, s_1^{j+1}), $j = 1, \dots, L+1$;
(t_0^j, s_2^j), $j = 1, \dots, L+1$;
(s_1^j, t_1^j), $j = 1, \dots, L+2$;
(s_2^j, t_2^j), $j = 1, \dots, L+1$;
(s_1^j, t_2^j), $j = 1, \dots, L+1$;

(t_0^j, s_{a1}^j), $j = 1, \dots, L-1$;
(s_{ai}^j, t_{ai}^j), $j = 1, \dots, L$; $i = 1, \dots, n_j$;
$(t_{ai}^j, s_{a(i+1)}^j)$, $j = 1, \dots, L$; $i = 1, \dots, n_j$;
$(s_{a(n_j+1)}^j, t_2^j)$, $j = 1, \dots, L$;

(t_0^j, s_{rx}^{j+1}), $j = 1, \dots, L-1$; $x \in X^j$;
(s_{rx}^j, t_{rx}^j), $j = 1, \dots, L$; $x \in X^j$;
(s_{rx}^j, t_2^{j+1}), $j = 1, \dots, L$; $x \in X^j$;

(t_0^j, s_{bi1}^{j+1}), $j = 1, \dots, L-1$; $i = 1, \dots, m_j$;
(s_{bi1}^j, t_{bi}^j), $j = 1, \dots, L$; $i = 1, \dots, m_j$;
(s_{bi1}^j, t_{bi1}^j), $j = 1, \dots, L$; $i = 1, \dots, m_j$;
(t_{bi}^j, s_{bi2}^j), $j = 1, \dots, L$; $i = 1, \dots, m_j$;
(s_{bi2}^j, t_{bi2}^j), $j = 1, \dots, L$; $i = 1, \dots, m_j$;
(s_{bi2}^j, t_2^{j+2}), $j = 1, \dots, L-1$; $i = 1, \dots, m_j$;

Initially, the places s_0^1, s_1^1 and s_{rx}^1 with $x \in X^1$ and s_{bi1}^1 with $i = 1, \dots, m_1$ are marked. The labelling is as follows:

$l_O(t_0^j) = l_O(t_2^j) = \lambda$; $j = 1, \dots, L+1$;
$l_O(t_1^j) = \omega$; $j = 1, \dots, L+2$;

$l_O(t^j_{ai}) = a^j_i$; $j = 1, \dots, L$; $i = 1, \dots, n_j$;
$l_O(t^j_{rx}) = x$; $j = 1, \dots, L$; $x \in X^j$;
$l_O(t^j_{bi}) = b^j_i$; $j = 1, \dots, L$; $i = 1, \dots, m_j$;
$l_O(t^j_{bi1}) = l_O(t^j_{bi2}) = \omega$; $j = 1, \dots, L$; $i = 1, \dots, m_j$.

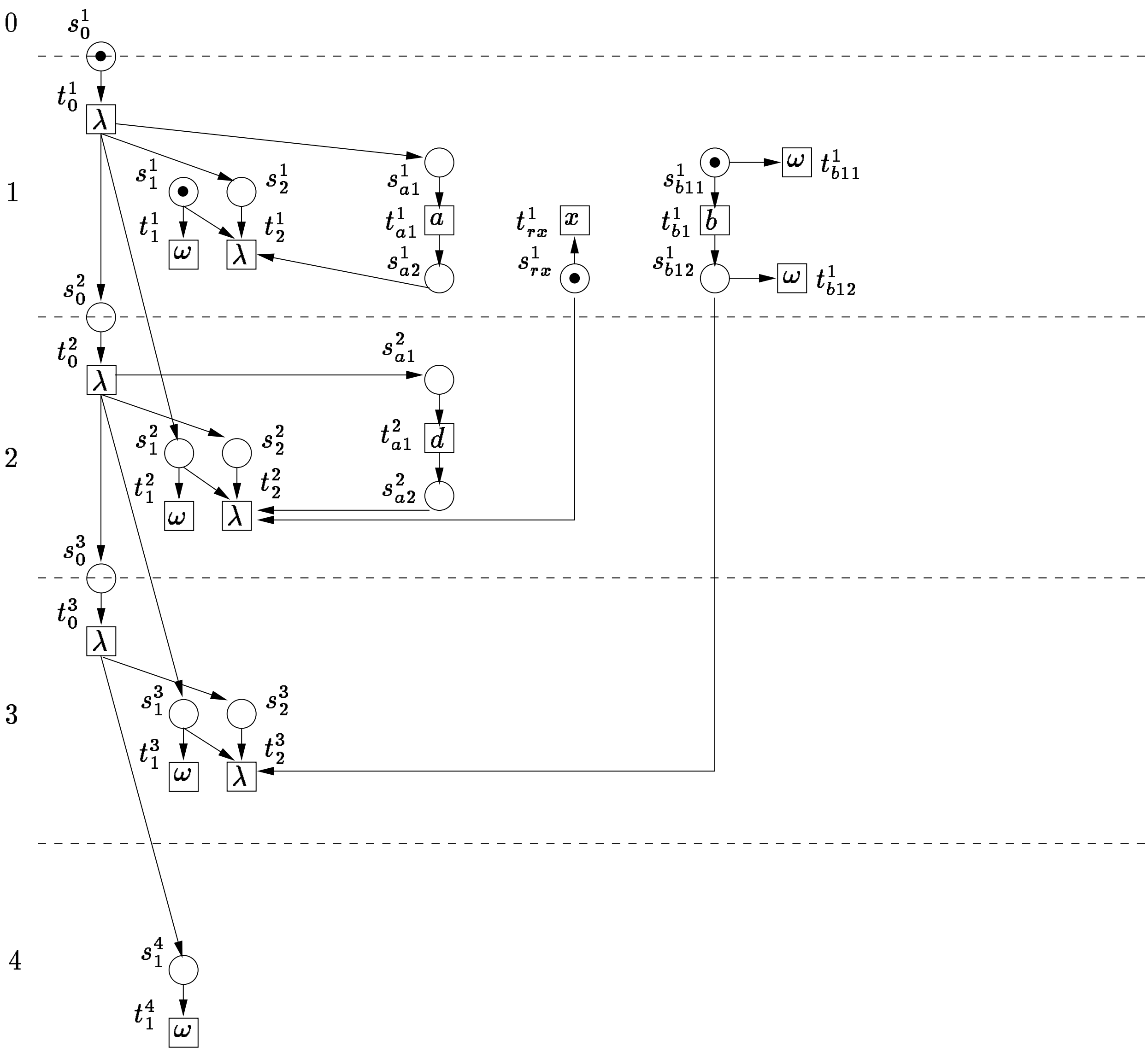

Figure 2: test net O

The subnet consisting of the s^j_i, t^j_i with $i = 0, 1, 2$ for $j = 1, \dots, L+1$ and s_1^{L+2}, t_1^{L+2} acts as a clock. It ends with an ω-transition (t_1^{L+2}), and in order to fail the test, the clock must proceed as slow as possible but still respect the firing discipline, i.e it must work with a fixed speed. N_1 will fail the test for $D = L + 1$, i.e. $L + 1$ rounds with $L + 1$ σ's occur, not counting the inital implicit σ, in the following called 0-th σ.

We now describe how such a failing trace must look like. First, consider the sequence of the s^j_0, t^j_0 with $j = 1, \dots, L+1$ finished by s_1^{L+2}, t_1^{L+2}. Before the $(L+1)$-th σ occurs, t_1^{L+2} must not be urgent, i.e. t_0^{L+1} must end firing after the L-th σ. Inductively, t^j_0 must end firing after the $(j-1)$-th σ, i.e. in the j-th round. t^1_0 is initially activated and urgent after the 0-th σ, i.e. in the first round. The same applies for t_1^1, and in order to fail the test, t_1^1 must be deactivated by the start of t_2^1 before the first σ, i.e. in the first round. Therefore, t_0^1 must end in the first round, thereby activating t_0^2 and t_1^2, which become urgent in the second round. Inductively, t_0^j must end firing and t_2^j must start firing before the j-th σ, i.e. in the j-th round. Altogether, t_0^j must fire instantaneously in the j-th round and t_2^j must start firing in the j-th round for $j = 1, \ldots, L+1$.

The t_{ai}^j are sequenced inbetween the end of t_0^j and the start of t_2^j, and by the above argument, they all must fire in zero time in the j-th round.

The t_{bi1}^j are activated concurrently by the end of t_0^{j-1} which occurs one round before. Hence, in the j-th round the t_{bi1}^j are urgent and the t_{bi}^j must start firing in the j-th round at the latest in order to deactivate the t_{bi1}^j. The ends of the t_{bi}^j activate the t_{bi2}^j which are urgent one round later, but will only be deactivated by t_2^{j+2}. So the t_{bi}^j must end firing not before round $j+1$. Thus, the t_{bi}^j must start in the j-th round and must end in round $j+1$. For $j = L$, the t_{bi2}^L will not be deactivated, the t_{bi}^L must end firing in round $L+1$ and in this case the t_{bi2}^L can be avoided in the first $L+1$ rounds. As the t_{bi}^j are urgent in the test net in round j, they must be synchronized with non-urgent partners in the tested net. We conclude that the tested net must be able to perform the b_i^{j+} in round j.

The t_{rx}^j are also activated concurrently by the end of t_0^{j-1} and are urgent in round j. On the other hand, the tokens on the s_{rx}^j are needed for the firing start of t_2^{j+1} one round later, so if there are synchronization partners for the t_{rx}^j in the tested net, they must not be urgent when the time step occurs, i.e. the tested net must be able to perform a time step X^j with $x \in X^j$.

We conclude that N_1 can fail the test by performing w, so N_2 must be able to fail the test; we see, that the test can only be failed by performing w and conclude $w \in \mathit{2RT}(N_2)$. ■ 4.7

Corollary 4.8

The $\mathit{2RT}$-semantics is fully abstract w.r.t. $\mathit{2L}$ and parallel composition of nets, i.e. it gives the coarsest congruence for parallel composition that respects $\mathit{2L}$-equivalence. $\sqsupseteq_2$ is a precongruence for parallel composition.

Proof: follows from Proposition 4.2, Theorem 4.6 and Theorem 4.7. Theorem 4.6 and Proposition 4.2 show that $\mathit{2RT}$-equivalence is a congruence that respects $\mathit{2L}$-equivalence. If $\mathit{2RT}(N_1) \neq \mathit{2RT}(N_2)$, then the proof of Theorem 4.7 exhibits a test net O such that $\mathit{2L}(N_1 \|_\Sigma O) \neq \mathit{2L}(N_2 \|_\Sigma O)$. (If N_1 or N_2 contain the special action ω, then its rôle in O must be played by some other action a not occuring in N_1 or N_2; consider $\mathit{2L}(N_i \|_{\Sigma' - \{a\}} O)$ in this case.) ■ 4.8

Theorem 4.7 essentially reduces $\sqsupseteq_2$ to an inclusion of regular languages; the only small problem is that the refusal sets X can be arbitrarily large, but when comparing N_1 and N_2 it is obviously sufficient to draw these sets from the finite set $l_1(T_1) \cup l_2(T_2)$. Thus, $\sqsupseteq_2$ is in particular decidable, which is not obvious from the start, where we have an infinite (even uncountable) state space according to Definition 3.1.

In the literature, similar results exist that reduce an infinite state space arising from the use of dense time to a finite one, starting with [AD94]; but as far as I know, they are not applicable to our setting.

5 Test-based Precongruences for Prefix and Choice

In this section, operators for the modular construction of systems known from process algebras are introduced in our Petri net framework. Whereas parallel composition was already treated in Section 4, we now also consider prefix, choice, relabelling, hiding and restriction.

Definition 5.1 *prefix*

Let N be a net. For $a \in \Sigma' \cup \{\lambda\}$ the *a-prefix* $a.N$ of N is obtained by removing all tokens, adding a new marked place s and a new a-labelled transition t with $^\bullet t = \{s\}$ and $t^\bullet = M_N$. ■ 5.1

Quite surprisingly, the testing preorder $\sqsupseteq_2$ is not a precongruence for prefix, as the example in Figure 3 shows.

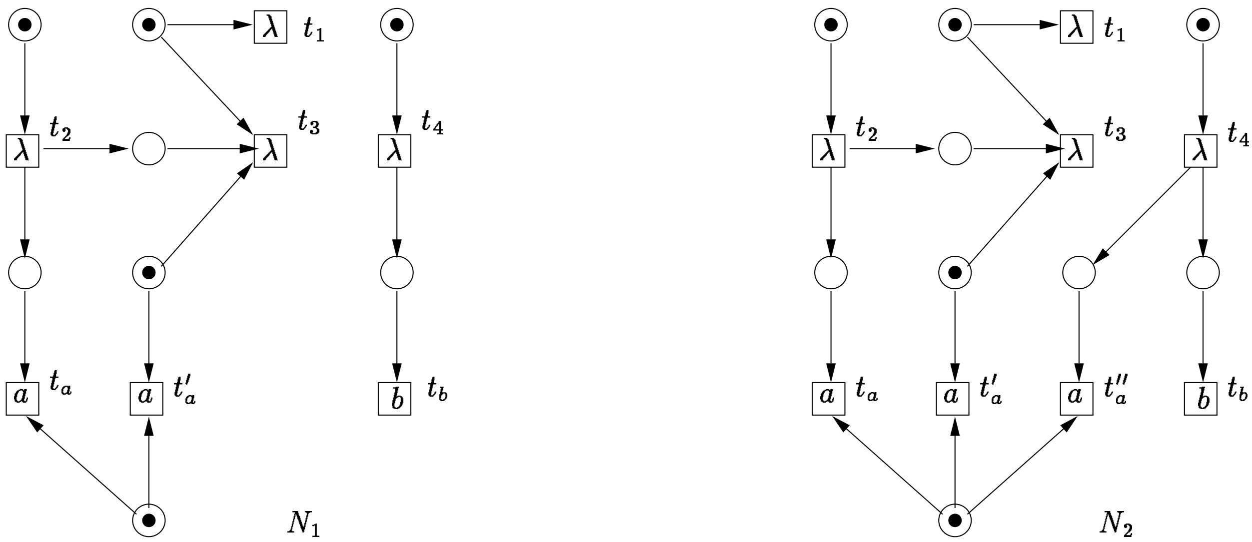

Figure 3:

We first argue that $\mathit{2RT}(N_1) = \mathit{2RT}(N_2)$, i.e. in particular $N_1 \sqsupseteq_2 N_2$. In both nets, t'_a is initially urgent, but can be deactivated by t_2t_3 such that a can be refused at the first time step. As t_1 is initially urgent, too, it has to be fired or deactivated by firing of t_3. If t_1 were fired, t'_a could never be deactivated and a could never be refused. Firing of t_2 has enabled t_a in both nets, which is urgent after the first time step and cannot be deactivated, such that a cannot be refused any longer. In N_2, t''_a can be activated before the first time step by firing t_4 instantaneously, but it is urgent not before the first time step, such that a can indeed be refused at the first time step in N_2, but not longer. We conclude $\mathit{2RT}(N_1) = \mathit{2RT}(N_2)$ and $N_1 \sqsupseteq_2 N_2$. Now we compare $c.N_1$ and $c.N_2$, where in both nets t_c may be the additional c-labelled transition. We have $l_1(t_ct_4t_b\Sigma t_2t_3\Sigma) = cb\Sigma\Sigma \in \mathit{2RT}(c.N_1) \setminus \mathit{2RT}(c.N_2)$, since t_a is not urgent before the first time step and occurrence of b in $c.N_2$ before the first time step implies enabledness of t''_a before and urgency of t''_a after the first time step, such that a cannot be refused at the second time step in $c.N_2$. We conclude $c.N_1 \not\sqsupseteq_2 c.N_2$.

After some thought one could assume that the initial time step might be the reason for this behaviour, since if we start from the initial ID $(M_N, \emptyset)$, the nets in Figure 3 are not refusal-trace-equivalent. We now show that this is indeed the case in general.

Definition 5.2

For a net N let $2RFS^\bullet(N)$ be the set of all 2-refusal firing sequences of N generated by Definition 4.1, where the initial ID is $ID^\bullet_N = (M_N, \emptyset)$. Define $2RT^\bullet(N) = \{l(w) \mid w \in 2RFS^\bullet(N)\}$ and for testable nets N_1 and N_2, $N_1 \geq^\bullet_2 N_2 \Leftrightarrow 2RT^\bullet(N_1) \subseteq 2RT^\bullet(N_2)$. ■ 5.2

Theorem 5.3

For nets N_1 and N_2, $2RT^\bullet(N_1) \subseteq 2RT^\bullet(N_2)$ implies $2RT(N_1) \subseteq 2RT(N_2)$, i.e. $N_1 \geq^\bullet_2 N_2$ implies $N_1 \sqsupseteq_2 N_2$.

Proof: To obtain $2RT(N)$ from $2RT^\bullet(N)$ take those sequences u from $2RT^\bullet(N)$ that start with a Σ and remove this Σ. Obviously, all sequences of $2RT(N)$ are gained, since $ID^\bullet_N[\Sigma\rangle\rangle^r_2 ID_N$. We have to treat the case that the underlying 2-refusal firing sequence w does not start with Σ, i.e. $u = l(w)$ and w starts $\imath\jmath\Sigma$ where $\imath$ is a sequence of internal transitions and $\jmath$ is a set of internal transitions. We only look at the general case $w = \imath\jmath\Sigma v\mu X w'' \in 2RFS^\bullet(N)$ where v is a sequence and μ is a set of transitions.

Analogously to the proof of Lemma 3.6, we show that if $ID^\bullet_N[\imath\jmath\Sigma v\rangle^r_2 ID_1[\mu X\rangle^r_2 ID_2$ then $ID^\bullet_N[\emptyset\Sigma\rangle^r_2 ID_N[\imath\bar{\jmath}v\rangle^r_2 ID'_1[\mu X\rangle^r_2 ID'_2$, where $\bar{\jmath}$ is an arbitrary sequentialisation of $\jmath$ and $ID'_2 = ID_2$; hence, $w' = \imath\bar{\jmath}v\mu X w'' \in 2RFS(N)$, $\Sigma l(w') = l(w) = u$ and $l(w') \in 2RT(N)$.

Obviously, $ID^\bullet_N[\emptyset\Sigma\rangle^r_2 ID_N$ by Definition 4.1 part 2. As M_N enables $\imath\jmath v$ we also have $ID_N[\imath\bar{\jmath}v\rangle^r_2 ID'_1$, and we have $M'_1 = M_1$ by Definition 4.1 part 1 and 2.

Assume there exists a $t \in U'_1 \setminus ({}^\bullet\mu)^\bullet$ with $l(t) \in X \cup \{\lambda\}$. This t must have become urgent after the initial time step, i.e. t was initially enabled and neither fired nor disabled during $\imath\bar{\jmath}v$; but this implies $t \in U_1 \setminus ({}^\bullet\mu)^\bullet$ too, and, since $ID_1[\mu X\rangle^r_2$, such a t does not exist. Thus, we get $ID'_1[\mu X\rangle^r_2 ID'_2$ with $M'_2 = M_2$ and $U'_2 = \{t \mid (M'_1 - {}^\bullet\mu_2)[t\rangle\} = \{t \mid (M_1 - {}^\bullet\mu_2)[t\rangle\} = U_2$, i.e. $ID'_2 = ID_2$. ■ 5.3

Before we show that $\geq^\bullet_2$ is indeed a precongruence for prefix, we remark that $\geq^\bullet_2$ is also a precongruence for for parallel composition.

Theorem 5.4

$2RT^\bullet$-equivalence is a congruence and $\geq^\bullet_2$ is a precongruence for parallel composition of nets.

Proof: Analogously to the proof of Theorem 4.6, where we did not need to consider the inital time-step of $2RT$-semantics. ■ 5.4

Theorem 5.5

$2RT^\bullet$-equivalence is a congruence and $\geq^\bullet_2$ is a precongruence for prefix.

Proof: Let N be a net and $a \in \Sigma'$. Then $2RT^\bullet(a.N)$ is the set of all prefixes of elements from

$$\{X_1 \dots X_n \,|\, n \in \mathbb{N}_0,\, X_1 \subseteq \Sigma,\, X_2 \dots X_n \subseteq \Sigma - \{a\}\} \circ \{a,\, a^+X \,|\, X \subseteq \Sigma\} \circ 2RT^\bullet(N)$$

where $\circ$ is concatenation of languages, and $2RT^\bullet(\lambda.N)$ is the set of all prefixes of elements from

$$\{X_1 \dots X_n \,|\, n \in \{0,1,2\},\, X_1 \dots X_n \subseteq \Sigma\} \circ 2RT^\bullet(N).$$

Initially, in $a.N$ only the additional a-labelled transition is activated, i.e. a $u \in 2RT^\bullet(a.N)$ may start with an arbitrary number of time steps, where at the first time step all actions, and at the following time steps all actions except a may be refused. Finally, the a may occur either instantaneously or in the form a^+X, where by X again all actions may be refused. In both cases $ID_N^\bullet$ is reached, from where all refusal traces from $2RT^\bullet(N)$ are possible.

Initially, in $\lambda.N$ only the additional λ-labelled transition is activated, i.e. a $u \in 2RT^\bullet(\lambda.N)$ may start with a time step, at which all actions may be refused. Now, the additional λ-labelled transition must occur either instantaneously or during another time step, at which again all actions may be refused. In both cases $ID_N^\bullet$ is reached, from where all refusal traces from $2RT^\bullet(N)$ are possible. ■ 5.5

Corollary 5.6

$\geq_2^\bullet$ is fully abstract w.r.t. prefix and $\sqsupseteq_2$.

Proof: By and Theorem 5.3 Theorem 5.5, we have to show that $\geq_2^\bullet$ is the coarsest precongruence for prefix that respects $\sqsupseteq_2$, i.e. $a.N_1 \sqsupseteq_2 a.N_2 \Rightarrow N_1 \geq_2^\bullet N_2$ for some $a \in \Sigma'$. Now $a.N_1 \sqsupseteq_2 a.N_2$ implies $2RT(a.N_1) \subseteq 2RT(a.N_2)$ and $2RT(a.N)$ is the set of all prefixes of elements from

$$\{X_1 \dots X_n \,|n \in \mathbb{N}_0,\, X_1 \dots X_n \subseteq \Sigma - \{a\}\} \circ \{a,\, a^+X \,|\, X \subseteq \Sigma\} \circ 2RT^\bullet(N)$$

Take $u \in 2RT^\bullet(N_1)$; then $au \in 2RT(a.N_1) \subseteq 2RT(a.N_2)$; from the form of the elements of $2RT(a.N_2)$, we see that $u \in 2RT^\bullet(N_2)$, i.e. $2RT^\bullet(N_1) \subseteq 2RT^\bullet(N_2)$ and $N_1 \geq_2^\bullet N_2$. ■ 5.6

We now come to the definition of a choice operator for nets. As already argued in [GV87], we have to perform a root-unwinding before composing two nets.

Definition 5.7 *root-unwinding*

Let N be a net; then the *root-unwinding* $\tilde{N}$ of N is defined as follows. Let $S_c = \{s \in S \,|\, M_N(s) = 1 \wedge {}^\bullet s \neq \emptyset\} \subseteq S$ be the set of initially marked places with nonempty preset, and let $S_c' = \{s' \,|\, s \in S_c\}$ be a copy of this set. Define $\tilde{S} = S \cup S_c'$ and $M_{\tilde{N}} = M_N|_{S-S_c} \cup 0_{S_c} \cup 1_{S_c'}$ and $\tilde{T} = \{t_R \,|\, \emptyset \subseteq R \subseteq S_c \cap {}^\bullet t\}$, such that ${}^\bullet t_R = ({}^\bullet t - R) \cup \{s' \in S_c' \,|\, s \in R\}$, $t_R^\bullet = t^\bullet$ and $\tilde{l}(t_R) = l(t)$. ■ 5.7

We expect a net N and its root-unwinding $\tilde{N}$ to be $2RT^\bullet$-equivalent. In order to prove this, it is helpful to use the following forward simulations.

Definition 5.8 *2RT•-forward simulation*

For nets N_1 and N_2, a relation $\mathcal{S}$ between some *ID*'s of N_1 and some of N_2 is a *2RT•-(forward) simulation* from N_1 to N_2 if the following hold:

1. $(ID^\bullet_{N_1}, ID^\bullet_{N_2}) \in \mathcal{S}$
2. If $(ID_1, ID_2) \in \mathcal{S}$ and $ID_1[t\rangle^r_2 ID'_1$ or $ID_1[\mu X\rangle^r_2 ID'_1$, then for some ID'_2 with $(ID'_1, ID'_2) \in \mathcal{S}$ we have $ID_2[l_1(t)\rangle\rangle^r_2 ID'_2$ or $ID_2[l_1(\mu)X\rangle\rangle^r_2 ID'_2$. Observe that these moves from ID_2 to ID'_2 may involve sequences of internal transitions.

■ 5.8

The following theorem is straightforward; compare e.g. [LV95] for a similar result and a survey on the use of simulations.

Theorem 5.9

If there exists a *2RT•*-simulation from N_1 to N_2, then $\mathit{2RT}^\bullet(N_1) \subseteq \mathit{2RT}^\bullet(N_2)$, i.e. $N_1 \geq^\bullet_2 N_2$. ■ 5.9

Lemma 5.10

Let N be a net and $\tilde{N}$ its root-unwinding. Then $\tilde{N}$ is safe and $\mathit{2RT}^\bullet(\tilde{N}) = \mathit{2RT}^\bullet(N)$.

Proof: Let $ID = (M, U)$ and $\tilde{ID} = (\tilde{M}, \tilde{U})$ be reachable *ID*'s of N, $\tilde{N}$ resp. We let $(M, \tilde{M}) \in \mathcal{M}$ if $\forall s \in S - S_c : \tilde{M}(s) = M(s)$ and $\forall s \in S_c : \tilde{M}(s) + \tilde{M}(s') = M(s)$. For a given pair $(M, \tilde{M}) \in \mathcal{M}$ we define a bijection $\tau : T \to \tilde{T}$ by $\tau(t) = t_R$ with $R = \{s \in S_c \cap {}^\bullet t \mid \tilde{M}(s') = 1\}$. Obviously, $\tilde{l}(\tau(t)) = l(t)$. Finally, we let $(ID, \tilde{ID}) \in \mathcal{B}$ if $(M, \tilde{M}) \in \mathcal{M}$ and $\tau(U) = \tilde{U}$.

We show that $(ID^\bullet_N, ID^\bullet_{\tilde{N}}) \in \mathcal{B}$ and if $(ID, \tilde{ID}) \in \mathcal{B}$ then
i) if $ID[\varepsilon\rangle\rangle^r_2 ID'$ then $\exists \tilde{ID}' : \tilde{ID}[\varepsilon\rangle\rangle^r_2 \tilde{ID}' \wedge (ID', \tilde{ID}') \in \mathcal{B}$ and
ii) if $\tilde{ID}[\varepsilon\rangle\rangle^r_2 \tilde{ID}'$ then $\exists ID' : ID[\varepsilon\rangle\rangle^r_2 ID' \wedge (ID', \tilde{ID}') \in \mathcal{B}$,
i.e. $\mathcal{B}$ is a *2RT•*-simulation from N to $\tilde{N}$ and $\mathcal{B}^{-1}$ a *2RT•*-simulation from $\tilde{N}$ to N. ($\mathcal{B}$ is a bisimulation between N and $\tilde{N}$.) The safety of $\tilde{N}$ follows from the totality of $\mathcal{B}^{-1}$, the safety of N and the definition of $\mathcal{M}$.

By definition we have $\forall s \in S - S_c : M_{\tilde{N}}(s) = M_N(s)$ and $\forall s \in S_c : M_{\tilde{N}}(s) = 0 \wedge M_{\tilde{N}}(s') = 1 = M_N(s)$, hence $(M_N, M_{\tilde{N}}) \in \mathcal{M}$ and since $U_N = \tau(U_N) = \emptyset = U_{\tilde{N}}$ we have $(ID^\bullet_N, ID^\bullet_{\tilde{N}}) \in \mathcal{B}$.

Now let $(ID, \tilde{ID}) \in \mathcal{B}$. We first show some properties.

1. $M[t\rangle M'$ if and only if $\tilde{M}[\tau(t)\rangle \tilde{M}'$ and in this case $(M', \tilde{M}') \in \mathcal{M}$:
Let $\tau(t) = t_R$; then $s \in {}^\bullet t \cap (S - S_c) \Leftrightarrow s \in {}^\bullet t_R \cap (S - S_c)$ and $s \in {}^\bullet t \cap S_c \Leftrightarrow (s \notin R \wedge s \in {}^\bullet t_R \cap S_c) \vee (s \in R \wedge s' \in {}^\bullet t_R \cap S'_c)$; from this we can deduce $M[t\rangle$ iff $\tilde{M}[\tau(t)\rangle$.
Let $s \in (S - S_c)$; then $s \in M' \Leftrightarrow s \in (M - {}^\bullet t + t^\bullet) \Leftrightarrow s \in (\tilde{M} - {}^\bullet t_R + t_R^\bullet) \Leftrightarrow s \in \tilde{M}'$, since $M(s) = \tilde{M}(s)$, ${}^\bullet t \cap (S - S_c) = {}^\bullet t_R \cap (S - S_c)$ and $t^\bullet = t_R^\bullet$. We have to show $\forall s \in S_c : M(s) - {}^\bullet t(s) + t^\bullet(s) = \tilde{M}(s) - {}^\bullet t_R(s) + t_R^\bullet(s) + \tilde{M}(s') - {}^\bullet t_R(s') + t_R^\bullet(s')$. Since $M(s) = \tilde{M}(s) + \tilde{M}(s')$, $t^\bullet(s) = t_R^\bullet(s)$ and $t_R^\bullet(s') = 0$, this can be reduced to $\forall s \in S_c : {}^\bullet t(s) = {}^\bullet t_R(s) + {}^\bullet t_R(s')$; now $\forall s \in (S_c - R) : {}^\bullet t(s) = {}^\bullet t_R(s) \wedge {}^\bullet t_R(s') = 0$ and $\forall s \in R : {}^\bullet t(s) = {}^\bullet t_R(s') = 1 \wedge {}^\bullet t_R(s) = 0$ by definition of ${}^\bullet t_R$; we conclude $(M', \tilde{M}') \in \mathcal{M}$.

2. Assume $\tilde{M}[t_R\rangle$ and $\tilde{M}[t_{R'}\rangle$ for some t and $R \neq R'$; then without loss of generality, there exists $s \in R' \setminus R$ with $\tilde{M}(s) = 1$ since $s \in {}^\bullet t_R$ and $\tilde{M}(s') = 1$ since $s \in {}^\bullet t_{R'}$, hence $\tilde{M}(s) + \tilde{M}(s') \neq M(s) \leq 1$ as N is safe, a contradiction to $(M, \tilde{M}) \in \mathcal{M}$.

3. Properties 1. and 2. imply that t is enabled in N if and only if $\tau(t) = t_R$ is enabled in $\tilde{N}$, and if t_R is enabled, then there is no $R' \neq R$ such that $t_{R'}$ is enabled.

4. For transitions $t, t' \in T$ we have ${}^\bullet t \cap {}^\bullet t' = \emptyset \Leftrightarrow {}^\bullet \tau(t) \cap {}^\bullet \tau(t') = \emptyset$:
Let $\tau(t) = t_R$; first let $s \in S - S_c$; then $s \in {}^\bullet t \Leftrightarrow s \in {}^\bullet t_R$; now let $s \in S_c$; If $s' \notin \tilde{M}$ then $s \in {}^\bullet t \Leftrightarrow s \in {}^\bullet t_R$ and $s' \notin {}^\bullet t_R$; if $s' \in \tilde{M}$ then $s \in {}^\bullet t \Leftrightarrow s' \in {}^\bullet t_R$ and $s \notin {}^\bullet t_R$.

5. If $M[t\rangle M'$ and $\tilde{M}[\tau(t)\rangle \tilde{M}'$ and $U' = U \setminus ({}^\bullet t)^\bullet$ and $\tilde{U}' = \tilde{U} \setminus ({}^\bullet \tau(t))^\bullet$, then $\tau'(U') = \tilde{U}'$:
Property 4. implies $t' \in U' \Leftrightarrow t' \in U \setminus ({}^\bullet t)^\bullet \Leftrightarrow t' \in U \wedge {}^\bullet t' \cap {}^\bullet t = \emptyset \Leftrightarrow \tau(t') \in \tilde{U} \wedge {}^\bullet \tau(t) \cap {}^\bullet \tau(t') = \emptyset \Leftrightarrow \tau(t') \in \tilde{U} \setminus ({}^\bullet \tau(t))^\bullet \Leftrightarrow \tau(t') \in \tilde{U}'$; furthermore, in this case t' is enabled under M' and $\tau(t')$ is enabled under $\tilde{M}'$, hence property 3. implies $\tau(t') = \tau'(t')$.

6. $M[\mu\rangle M'$ if and only if $\tilde{M}[\tau(\mu)\rangle \tilde{M}'$ and in this case $(M', \tilde{M}') \in \mathcal{M}$:
follows by repeated application of property 1.

7. If $M[\mu\rangle M'$ and $\tilde{M}[\tau(\mu)\rangle \tilde{M}'$ and $U' = \{t \mid (M - {}^\bullet \mu)[t\rangle\}$ and $\tilde{U}' = \{\tilde{t} \mid (\tilde{M} - {}^\bullet \tau(\mu))[\tilde{t}\rangle\}$ then $\tau'(U') = \tilde{U}'$:
Properties 3. and 4. imply $t \in U' \Leftrightarrow M[t\rangle \wedge {}^\bullet t \cap {}^\bullet \mu = \emptyset \Leftrightarrow \tilde{M}[\tau(t)\rangle \wedge {}^\bullet \tau(t) \cap {}^\bullet \tau(\mu) = \emptyset \Leftrightarrow \tau(t) \in \tilde{U}'$; again, t is enabled under M' and $\tau(t)$ is enabled under $\tilde{M}'$, hence property 3. implies $\tau(t) = \tau'(t)$.

8. $l(U \setminus ({}^\bullet \mu)^\bullet) = \tilde{l}(\tilde{U} \setminus ({}^\bullet \tau(\mu))^\bullet)$:
$t \in U \setminus ({}^\bullet \mu)^\bullet \Leftrightarrow \tau(t) \in \tilde{U} \setminus ({}^\bullet \tau(\mu))^\bullet$ by repeated application of property 5. (noting that $\tau(t) = \tau'(t)$ for the concerned transitions)and $l(t) = \tilde{l}(\tau(t))$.

Now let $\varepsilon = a \in \Sigma' \cup \{\lambda\}$. Then $ID[\varepsilon\rangle\rangle_2^r ID'$ implies $\tilde{ID}[\varepsilon\rangle\rangle_2^r \tilde{ID}'$ and $(ID', \tilde{ID}') \in \mathcal{B}$ by Definition 4.1 and properties 1. and 5., and vice versa.

If $\varepsilon = pX$, then $ID[\varepsilon\rangle\rangle_2^r ID'$ implies $\tilde{ID}[\varepsilon\rangle\rangle_2^r \tilde{ID}'$ and $(ID', \tilde{ID}') \in \mathcal{B}$ by Definition 4.1 and properties 6., 7. and 8, and vice versa. ■ 5.10

As in [GV87], we define the choice between two nets as follows.

Definition 5.11 *choice*

Let N_1, N_2 be nets and $\tilde{N}_1$, $\tilde{N}_2$ their root-unwindings; then the *choice (sum)* $N = N_1 + N_2$ of N_1 and N_2 is defined as follows:

$$\begin{aligned} S &= \{s_1 \in \tilde{S}_1 \mid M_{\tilde{N}_1}(s_1) = 0\} \cup \{s_2 \in \tilde{S}_2 \mid M_{\tilde{N}_2}(s_2) = 0\} \\ &\quad \cup \{(s_1, s_2) \in \tilde{S}_1 \times \tilde{S}_2 \mid M_{\tilde{N}_1}(s_1) = M_{\tilde{N}_2}(s_2) = 1\} \\ T &= \tilde{T}_1 \cup \tilde{T}_2 \end{aligned}$$

$$
\begin{aligned}
W(s,t) &= \begin{cases} \tilde{W}_1(s_1,t_1) & \text{if } s = s_1 \in \tilde{S}_1 \text{ or } s = (s_1,s_2),\ t = t_1 \in \tilde{T}_1 \\ \tilde{W}_2(s_2,t_2) & \text{if } s = s_2 \in \tilde{S}_2 \text{ or } s = (s_1,s_2),\ t = t_2 \in \tilde{T}_2 \\ 0 & \text{otherwise} \end{cases} \\
W(t,s) &= \begin{cases} \tilde{W}_1(t_1,s_1) & \text{if } s = s_1 \in \tilde{S}_1,\ t = t_1 \in \tilde{T}_1 \\ \tilde{W}_2(t_2,s_2) & \text{if } s = s_2 \in \tilde{S}_2,\ t = t_2 \in \tilde{T}_2 \\ 0 & \text{otherwise} \end{cases} \\
l(t) &= \begin{cases} \tilde{l}_1(t_1) & \text{if } t = t_1 \in \tilde{T}_1 \\ \tilde{l}_2(t_2) & \text{if } t = t_2 \in \tilde{T}_2 \end{cases} \\
M_N(s) &= \begin{cases} 1 & \text{if } s = (s_1,s_2) \\ 0 & \text{otherwise} \end{cases}
\end{aligned}
$$

■ 5.11

Very often, congruences for choice have to consider the (initial) stability of systems defined as follows.

Definition 5.12 *stable*

A net N is *stable*, if no internal transition is initially enabled, i.e. $\{t \in T \mid M_N[t\rangle \wedge l(t) = \lambda\} = \emptyset$. For testable nets N_1 and N_2, we write $N_1 \geq_2 N_2$, if $N_1 \geq_2^\bullet N_2$ and N_2 stable $\Leftrightarrow$ N_1 stable. ■ 5.12

An interesting point is that the condition on the stability is an equivalence although we consider a preorder.

Lemma 5.13

If two nets N_1 and N_2 are stable, then

$$
\begin{aligned}
\mathit{2RT}^\bullet(N_1 + N_2) = \{&X_1 \ldots X_n u \in \mathit{2RT}^\bullet(N_1) \cup \mathit{2RT}^\bullet(N_2) \mid \\
&X_1 \ldots X_n \in \mathit{2RT}^\bullet(N_1) \cap \mathit{2RT}^\bullet(N_2),\ n \in \mathbb{N}_0,\ u \text{ does not start with a set}\}.
\end{aligned}
$$

If N_1 is not stable and N_2 is stable, then

$$\mathit{2RT}^\bullet(N_1 + N_2) = \mathit{2RT}^\bullet(N_1) \cup \{u,\ Xu \in \mathit{2RT}^\bullet(N_2) \mid u \text{ does not start with a set}\}.$$

If neither N_1 nor N_2 is stable, then

$$\mathit{2RT}^\bullet(N_1 + N_2) = \mathit{2RT}^\bullet(N_1) \cup \mathit{2RT}^\bullet(N_2).$$

Proof: Let $N = N_1 + N_2$.

If N_1 and N_2 are stable, then by Definition 5.7 and Definition 5.11 N is stable and initially in N an arbitrary number of time steps $X_1 \ldots X_n$ may occur, at which all actions may be refused that can be initially refused in both components N_1 and N_2. Finally, in N a transition can fire instantaneously or within a step, and since N is stable, this transition is labelled with a visible action and by Definition 5.11 and Lemma 5.10, it makes a decision either for a refusal trace of N_1 or a refusal trace of N_2.

If N_1 is not stable and N_2 is stable, then N is not stable. By Definition 5.7, Definition 5.11 and Lemma 5.10, N can perform any refusal trace of N_1 which may start with maximal one time step (at which all actions – escpecially those from N_2 – may be refused), before an initially activated λ-transition of N_1 must occur and the decision for N_1 is made.

Analogously, N can perform any refusal trace of N_2 that starts with maximal one time step, after which a (visible) action from N_2 must occur in order to deactivate all transitions from N_1 (especially the initially activated λ-transitions) and the decision for N_2 is made.

If both N_1 and N_2 are not stable, then N is not stable and after maximal one time step, one of the initially activated λ-transitions of either N_1 or N_2 must occur, and the decision for N_1 resp. N_2 is made, such that N can perform all refusal traces from N_1 and N_2. ■ 5.13

Theorem 5.14

$\geq_2$ is a precongruence for choice.

Proof: For testable nets N_1, N_1', N_2, N_2' we assume $N_1 \geq_2 N_2 \wedge N_1' \geq_2 N_2'$ and show $N_1 + N_1' \geq_2 N_2 + N_2'$. We distinguish several cases:

1. N_1 stable and N_1' stable. Then $N_1 + N_1'$ stable and by assumption N_2 stable and N_2' stable, i.e. $N_2 + N_2'$ stable. Let $u \in \mathit{2RT}^\bullet(N_1 + N_1')$ by Lemma 5.13 be of the form $X_1 \dots X_n u'$. By assumption, $X_1 \dots X_n \in \mathit{2RT}^\bullet(N_1) \cap \mathit{2RT}^\bullet(N_1') \subseteq \mathit{2RT}^\bullet(N_2) \cap \mathit{2RT}^\bullet(N_2')$ and $u \in \mathit{2RT}^\bullet(N_1) \cup \mathit{2RT}^\bullet(N_1') \subseteq \mathit{2RT}^\bullet(N_2) \cup \mathit{2RT}^\bullet(N_2')$, i.e. $u \in \mathit{2RT}^\bullet(N_2 + N_2')$ and $\mathit{2RT}^\bullet(N_1 + N_1') \subseteq \mathit{2RT}^\bullet(N_2 + N_2')$.

2. N_1 not stable and N_1' stable. Then $N_1 + N_1'$ not stable and by assumption N_2 not stable and N_2' stable, i.e. $N_2 + N_2'$ not stable. Now by Lemma 5.13 and by assumption, $\mathit{2RT}^\bullet(N_1 + N_1') = \mathit{2RT}^\bullet(N_1) \cup \{u,\ Xu \in \mathit{2RT}^\bullet(N_1') \mid u \text{ does not start with a set}\} \subseteq \mathit{2RT}^\bullet(N_2) \cup \{u,\ Xu \in \mathit{2RT}^\bullet(N_2') \mid u \text{ does not start with a set}\} = \mathit{2RT}^\bullet(N_2 + N_2')$.

3. Analogously for N_1 stable and N_1' not stable.

4. N_1 not stable and N_1' not stable. Then $N_1 + N_1'$ not stable and by assumption N_2 not stable and N_2' not stable, i.e. $N_2 + N_2'$ not stable. By Lemma 5.13 and by assumption, $\mathit{2RT}^\bullet(N_1 + N_1') = \mathit{2RT}^\bullet(N_1) \cup \mathit{2RT}^\bullet(N_1') \subseteq \mathit{2RT}^\bullet(N_2) \cup \mathit{2RT}^\bullet(N_2') = \mathit{2RT}^\bullet(N_2 + N_2')$. ■ 5.14

The next Theorem states that we have refined $\geq_2^\bullet$ adequately to deal with the choice operator; in particular, it justifies the $\Leftrightarrow$-requirement for the stability.

Theorem 5.15

$\geq_2$ is fully abstract w.r.t. choice and $\geq_2^\bullet$.

Proof: By Definition 5.12 and Theorem 5.14, we have to show that for any N_1, N_2 : $(\forall N : N_1 + N \geq_2^\bullet N_2 + N) \Rightarrow N_1 \geq_2 N_2$. For given N_1, N_2 assume to the contrary, i.e. $\forall N : N_1 + N \geq_2^\bullet N_2 + N$ but $N_1 \not\geq_2 N_2$; since N might be the empty net, we have $N_1 \geq_2^\bullet N_2$, so the condition on the stability of N_1 and N_2 must be violated, i.e. N_1 stable and N_2 not stable or vice versa.

In the following let N be the net that can only perform one single action $x \in \Sigma' \setminus (l_1(N_1) \cup l_2(N_2))$, i.e. N has one initially marked place with one arc to its only transition, which is labelled with x.

First assume N_1 stable and N_2 not stable; then $\emptyset\emptyset x \in \mathit{2RT}^\bullet(N_1+N) \setminus \mathit{2RT}^\bullet(N_2+N)$, since $N_1 + N$ may still be in its inital marking after two time steps, wheras $N_2 + N$ must have fired at least one of the initially activated internal transitions of N_2, thereby avoiding a following x; now $2RT^\bullet(N_1+N) \not\subseteq 2RT^\bullet(N_2+N)$ is a contradiction to $N_1+N \geq_2^\bullet N_2+N$.

Now assume N_1 not stable and N_2 stable; then $\emptyset\{x\} \in 2RT^\bullet(N_1+N) \setminus 2RT^\bullet(N_2+N)$, since N_1+N may fire one of the initially activated internal transitions of N_1, thereby deactivating x of N, such that x can be refused after the first time step. This is not possible for N_2+N, since there are no internal transitions that can deactivate x. Hence, x is urgent after the first time step, if no visible action has occurred yet; again $2RT^\bullet(N_1+N) \not\subseteq 2RT^\bullet(N_2+N)$ is a contradiction to $N_1+N \geq_2^\bullet N_2+N$. ∎ 5.15

Corollary 5.16

$\geq_2$ is a precongruence for parallel composition of nets and fully abstract w.r.t *2L*-inclusion, parallel composition, prefix and choice.

Proof: Follows from Theorem 5.4, since the parallel composition of two nets is stable iff both nets are stable, and Corollary 4.8, Theorem 5.3, Theorem 5.4, Corollary 5.6 and Theorem 5.15, where we always made only the necessary refinements. ∎ 5.16

Finally, we consider three standard operators.

Definition 5.17 *relabelling, hiding, restriction*

A *relabelling function* is a function $f : \Sigma' \cup \{\lambda\} \to \Sigma' \cup \{\lambda\}$ with $f(\lambda) = \lambda$ and $f(\Sigma') = \Sigma'$. The *relabelling* $N[f]$ of N with relabelling function f is obtained from N by changing the labelling from l to $f \circ l$. *Hiding* $a \in \Sigma'$ in N means changing all labels a to λ; it results in $N \backslash a$. *Restricting* $a \in \Sigma'$ in N means deleting all a-labelled transitions; it results in N/a. ∎ 5.17

Theorem 5.18

$\geq_2$ is a precongruence w.r.t. hiding, relabelling and restriction.

Proof: $2RT^\bullet(N \backslash a)$ can be constructed from those refusal traces in $2RT^\bullet(N)$ where for all steps μX we have $a \in X$; this requirement is necessary to ensure that the new internal actions in $N \backslash a$ are treated correctly. Delete all a and a^+ in these traces and replace the refusal sets by arbitrary subsets (possibly not containing a). For testable nets N_1, N_2 assume $N_1 \geq_2 N_2$. If both nets are not stable, then they will both be not stable after hiding. So assume N_1 and N_2 to be stable. If $N_1 \backslash a$ is not stable, then there must have been an initially activated a-labelled transition in N_1, i.e. $a \in 2RT^\bullet(N_1) \subseteq 2RT^\bullet(N_2)$, and since N_2 is stable, too, there must also have been an initially activated a-labelled transition in N_2, i.e. $N_2 \backslash a$ is not stable, too. If on the other hand $N_2 \backslash a$ is not stable, then there must have been an initially activated a-labelled transition in N_2, i.e. since N_2 is stable, $\Sigma\{a\} \notin 2RT^\bullet(N_2) \supseteq 2RT^\bullet(N_1)$, so there must also have been an initially activated a-labelled transition in stable N_1, i.e. $N_1 \backslash a$ is not stable, too.

For restriction of a, consider those refusal traces that do not contain a or a^+ and add a to some refusal sets (– 'some' including the cases 'none' and 'all'). Restriction does not affect the stability of a net.

For relabelling it is enough to consider those functions that change some a to some b and leave all other actions unchanged. We can construct $\mathit{2RT}(N[f])$ by changing in the refusal traces all a to b and all a^+ to b^+, removing b from those refusal sets that do not also contain a and adding a to 'some' refusal sets. Relabelling does not affect the stability of a net. ■ 5.18

It should be mentioned that already $\sqsupseteq_2$ as all variants considered in [JV95] are precongruences w.r.t. hiding, relabelling and restriction.

6 Further Properties of the $\geq_2$-Preorder

In this section, we will show some properties of $\geq_2$ one might intuitively expect from a faster-than relation. The following constructions are taken from [Vog95b, JV95]; they transform a net in a 'slower' one.

Definition 6.1 *elongation, persistence, ip-sequentialisation*

N' is an *elongation* of N, if it is obtained from N by choosing a transition t, adding a new unmarked place s and a new λ-labelled transition t' with ${}^\bullet t' = \{s\}$ and $t'^\bullet = t^\bullet$ and, finally, redefining $t^\bullet$ by $t^\bullet := \{s\}$.

Call a transition t of N *persistent*, if no reachable marking M with $M[t\rangle$ enables a transition t' with ${}^\bullet t \cap {}^\bullet t' \neq \emptyset$.

N' is a *sequentialisation* of N, if it is obtained from N by choosing two transitions $\dot{t}$ and $\ddot{t}$ and adding a new marked place s to the pre- and postsets of $\dot{t}$ and $\ddot{t}$; N' is an *ip-sequentialisation* if $\ddot{t}$ is internal and persistent. ■ 6.1

One would expect intuitively, that N and $\lambda.N$ exhibit the same behaviour except that $\lambda.N$ might take a bit more time for the additional initialisation; i.e. one would expect that N is faster than $\lambda.N$ and similarly also than any elongation or sequentialisation. It was already argued in [Vog95b] why the parallel execution of two visible actions may sometimes take more time, namely if the two actions block the two copies of a resource which is needed for some other time-critical activity; in this case, the resource is not available for the duration of the two actions – an effect that cannot occur if the actions are durationless.

Theorem 6.2

For a net N let N' be an elongation and N'' be an *ip*-sequentialisation of N. Then $N \geq_2^\bullet N'$, $N \geq_2^\bullet N''$ and $N \geq_2^\bullet \lambda.N$.

Proof: The identity relation is a $\mathit{2RT}^\bullet$-simulation from N to $\lambda.N$. Let t' be the additional λ-transition of $\lambda.N$. Then the first move $ID_N^\bullet[\varepsilon\rangle_2^r ID$ of N with $\varepsilon = t$ or $\varepsilon = \mu X$ is matched by $ID_{\lambda.N}^\bullet[t'\rangle_2^r ID_N^\bullet[\varepsilon\rangle_2^r ID$ in $\lambda.N$.

The identity relation is a $\mathit{2RT}^\bullet$-simulation from N to N'; if t and t' are the transitions involved in constructing N', then t in N is matched by tt' in N'; instantaneous firing of a transition t'' with $t \neq t'' \neq t'$ in N is matched by the same item in N'. If in N a move μX occurs, we simulate this by the same move in N', if $t \notin \mu$ and by the move $\mu X t'$, if $t \in \mu$. In all cases, the markings reached and the sets of urgent transitions coincide in both nets, since the transitions enabled by t are not urgent after μX in N and firing t' does not change the set of urgent transitions, since it does not share a precondition with any other transition.

Let N'' be obtained from N by adding s to the pre- and postsets of $\dot{t}$ and $\ddot{t}$. $\mathcal{S} = \{((M,U),(M \cup \{s\},U')) \mid (M,U)$ is reachable in N, $(M \cup \{s\},U')$ is reachable in N'' and $U' \subseteq U\}$ is a *2RT*$^\bullet$-simulation from N to N''. Obviously, $(ID^\bullet_N, ID^\bullet_{N''}) \in \mathcal{S}$. Let N be in a state (M,U) and N'' in a state $(M \cup \{s\},U')$ with $U' \subseteq U$.

Instantaneous firing of a transition t in N – yielding (M_1,U_1) – is matched by the same item in N'' – yielding $(M_1 \cup \{s\},U_1')$. The $2r$-firability in N'' follows from $M[t\rangle M_1$ in N iff $(M \cup \{s\})[t\rangle(M_1 \cup \{s\})$ in N'' and $U' \subseteq U$ implies $t' \in U_1' \Leftrightarrow t' \in U' \setminus ({}^\bullet t)^\bullet \Rightarrow t' \in U \setminus ({}^\bullet t)^\bullet \Leftrightarrow t' \in U_1$, i.e. $U_1' \subseteq U_1$ again. If, say, $t = \dot{t}$, then additionally $\ddot{t}$ is (possibly) removed from U'; hence in any case $U_1' \subseteq U_1$.

A move μX in N with $\dot{t} \notin \mu$ or $\ddot{t} \notin \mu$ – yielding (M_1,U_1) – is matched by the same item in N'' – yielding $(M_1 \cup \{s\},U_1')$. The $2r$-firability in N'' follows from $M[\mu\rangle M_1$ in N iff $(M \cup \{s\})[\mu\rangle(M_1 \cup \{s\})$ in N'' and $U' \subseteq U$ implies $t' \in U' \setminus ({}^\bullet\mu)^\bullet \Rightarrow t' \in U \setminus ({}^\bullet\mu)^\bullet \Rightarrow l(t') \neq X \cup \{\lambda\}$. Furthermore, if $t' \in U_1' \Leftrightarrow ((M \cup \{s\}) - {}^\bullet\mu)[t'\rangle$, then $(M - {}^\bullet\mu)[t'\rangle \Leftrightarrow t' \in U_1$, and if, say, $\dot{t} \in \mu$, then $\ddot{t} \notin U_1'$; hence in any case $U_1' \subseteq U_1$ again.

If we have a move μX with $\{\dot{t},\ddot{t}\} \subseteq \mu$ in N, we can simulate this in N'' with the move $\mu' X \ddot{t}$ with $\mu' = \mu - \{\ddot{t}\}$. The step $\mu' \subset \mu$ is activated under $M \cup \{s\}$ as μ is activated under M. If $M[\mu\rangle M_1$ in N_1, then $(M \cup \{s\})[\mu'\ddot{t}\rangle(M_1 \cup \{s\})$ in N''. As $\ddot{t}$ is internal, we have $l(\mu X) = l(\mu' X \ddot{t})$. $t' \in U' \setminus ({}^\bullet\mu')^\bullet$ in N'' implies $t' \in U \setminus ({}^\bullet\mu)^\bullet$ in N; as $\ddot{t}$ is persistent (in N), μ' deactivates the same transitions as μ, and $\ddot{t} \notin U' \subseteq U$, since $\ddot{t}$ is internal. So we have $\forall t' \in T : t' \in U' \setminus ({}^\bullet\mu')^\bullet \Rightarrow l(t') \notin X \cup \{\lambda\}$ and $\mu' X$ is $2r$-firable in N''. If $(M \cup \{s\} - {}^\bullet\mu')[t'\rangle$ in N'' then $(M - {}^\bullet\mu)[t'\rangle$ in N as $\ddot{t}$ is persistent (in N) and deactivated by $\mu' X$ in N'', i.e. not urgent after $\mu' X$. The instantaneous firing of $\ddot{t}$ after $\mu' X$ does not change the set of urgent transitions in N'', so we have $U_1' \subseteq U_1$ again. ■ 6.2

Corollary 6.3

For a net N let N' be an elongation and N'' be an *ip*-sequentialisation of N. Then $N \geq_2 N'$, $N \geq_2 N''$ and if N not stable, then $N \geq_2 \lambda.N$.

Proof: Follows from Definition 5.12 and Theorem 6.2, since elongation and *ip*-sequentialisation do not affect stability of a net. ■ 6.3

7 Variants – Transitions without Activation Time or without Duration

For our tests with efficiency for asynchronous systems, we have defined a firing rule in Definition 3.1 where each enabled transition has to start within time 1 (unless it is disabled within this time) and has to end within another unit of time. Occurrence of a transition has two phases: the activation phase lasts from the enabling moment to the start of firing, the firing phase from there to the end of firing. According to Definition 3.1, both phases last at most time 1. Two variants also seem plausible: we could assume that the activation phase is instantaneous and that time is only spent when the transition fires; this is the a-variant.

Or we could assume – as it is often done – that the transition has no duration, i.e. the firing phase is instantaneous, while the activation phase may take up to one unit of time; this is the i-variant.

In [JV95], a similar approach to the present one is taken. There, a basic variant is investigated, which allows up to *one* time unit for activation time *and* firing time *together*; this will be the d-variant in the following; note that the above mentioned a- and i-variants are also special cases of the d-variant. In [JV95], for all three variants testing-preorders ($\sqsupseteq$ for the d-variant, $\sqsupseteq_i$ and $\sqsupseteq_a$) are defined and characterized by sets of appropriate refusal traces (*DRT*, *IRT* and *ART*). One main disadvantage of the d-variant is its technically involved definition of the *DRT*-semantics; the present 2-variant is much easier to handle and the i-variant has the easiest characterization. The following definitions are taken from [JV95].

Definition 7.1 *DRT-semantics*

For instantaneous descriptions (M, U) and (M', U') we write $(M, U)[\varepsilon\rangle_d^r(M', U')$ if one of the following cases applies:

1. $\varepsilon = t \in T,\ M[t\rangle M',\ U' = U \setminus ({}^\bullet t)^\bullet$
2. $\varepsilon = \mu\nu X,\ \mu, \nu \subseteq T,\ M[\mu\rangle M',\ X \subseteq \Sigma'$,
   $\nu \subseteq \mu,\ \nu \cap U = \emptyset,\ \forall t \in \mu :\ l(t) = \lambda \Rightarrow t \in \nu$,
   $\forall t \in U \setminus ({}^\bullet\mu)^\bullet :\ l(t) \notin X \cup \{\lambda\}$,
   $U' = \{t \mid (M - {}^\bullet\mu)[t\rangle\}$

The corresponding sequences are called *discrete refusal firing sequences*, their set is denoted by $DRFS(N)$. $DRT(N) = \{l(w) \mid w \in DRFS(N)\}$ is the set of *discrete refusal traces*. The initial *ID* ist $ID_N = (M_N, U_N)$ with $U_N = \{t \mid M[t\rangle\}$. ■ 7.1

Definition 7.2 *ART-semantics*

For markings M, M' we write $M[\varepsilon\rangle_a^r M'$ if one of the following cases applies:

1. $\varepsilon = t \in T,\ M[t\rangle M'$;
2. $\varepsilon = \mu X,\ \mu \subseteq T,\ X \subseteq \Sigma',\ M[\mu\rangle M',\ \forall t \in T :\ (M - {}^\bullet\mu)[t\rangle \Rightarrow l(t) \notin X \cup \{\lambda\}$

If $M[w\rangle_a^r M'$, we write $M[l(w)\rangle\rangle_a^r M'$. The sets $ARFS(N)$ and $ART(N)$ are defined suitably. ■ 7.2

Definition 7.3 *IRT-semantics*

For *ID*'s (M, U) and (M', U'), we write $(M, U)[\varepsilon\rangle_i^r(M', U')$ if one of the following cases applies:

1. $\varepsilon = t \in T,\ M[t\rangle M',\ U' = U \setminus ({}^\bullet t)^\bullet$
2. $\varepsilon = X,\ X \subseteq \Sigma',\ M = M',\ U' = \{t \mid M[t\rangle\},\ \forall t \in U :\ l(t) \notin X \cup \{\lambda\}$

The initial *ID* ist $ID_N = (M_N, U_N)$ with $U_N = \{t \mid M[t\rangle\}$. If $ID[w\rangle_i^r ID'$, we write $ID[l(w)\rangle\rangle_i^r ID'$.The sets $IRFS(N)$ and $IRT(N)$ are defined suitably. ■ 7.3

It turned out that the d-, a- and i-variant are incomparable in general. Before we compare $\sqsupseteq_2$ with the other three testing preorders $\sqsupseteq$, $\sqsupseteq_i$ and $\sqsupseteq_a$, let us shortly compare it to the classical behaviour notions of traces and step traces. It is obvious that the 2-refusal traces that only use part 1 of Definition 4.1 correspond exactly to the ordinary traces. Hence:

Proposition 7.4

Let N_1 and N_2 be nets with $N_1 \sqsupseteq_2 N_2$. Then every trace of N_1 is a trace of N_2. ■ 7.4

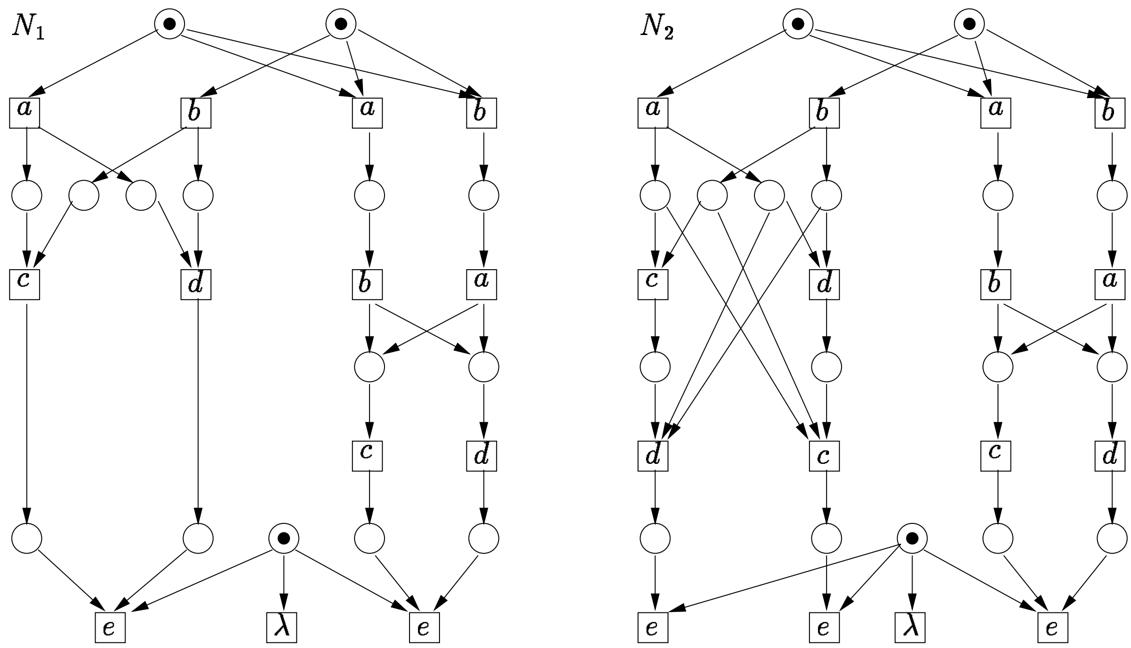

Figure 4: equivalent nets with different step traces

Somewhat surprisingly, the preorder $\geq_2$ (and thereby $\sqsupseteq_2$) is not sensitive to step traces. The nets in Figure 4 are $2RT^\bullet$-equivalent and both not stable, but only N_1 can perform the step trace $\binom{a}{b}\binom{c}{d}e$. The following considerations show the $2RT^\bullet$-equivalence of the nets: note that in both nets after maximal two time steps e has been fired or deactivated by the λ-transition. Since the right parts of N_1 and N_2 are identical and in conflict with the left parts, we only have to make sure that the refusal traces generated by execution of the left parts coincide or can also be generated by the right parts. Any refusal trace of the left parts that does not (after possibly some time steps) start with a step a^+b^+X can also be generated by the right part: if in the left part a and b occur instantaneously in any order, thereby activating concurrent c and d, this can be done by the right part, too, yielding equivalent states in N_1. If the left part of N_2 continues with the step c^+d^+X, then e can be refused at the next time step, but this is possible anyway, since the λ-transition may occur, i.e. we reach equivalent states in N_2, too. Analogous considerations apply, if the left part starts ab^+X or ba^+X. If the left part starts a^+X or b^+X, then b resp. a is urgent after the time step in the left part but not in the simulating right part, such that the right part may possibly refuse more actions than the left part now; this, however, has no effect on the capability to simulate the left part.

Now assume a refusal trace of the left parts to start a^+b^+X. Afterwards in both nets c and d are activated concurrently. Any sequentialisation of them is possible in both nets and can be followed by an e; but if e does not occur before or during the next time step (especially in the case c^+d^+X), then it will be disabled by the λ-transition. We conclude that the refusal traces of the nets coincide.

For the reverse implication, consider the step equivalent nets in Figure 5; they are even process-equivalent, compare e.g. [Vog92, p.18]. But $a\{b\} \in \mathit{2RT}(N_2) \setminus \mathit{2RT}(N_1)$ such that $N_2 \not\sqsupseteq_2 N_1$, yielding $N_2 \not\geq_2 N_1$, too.

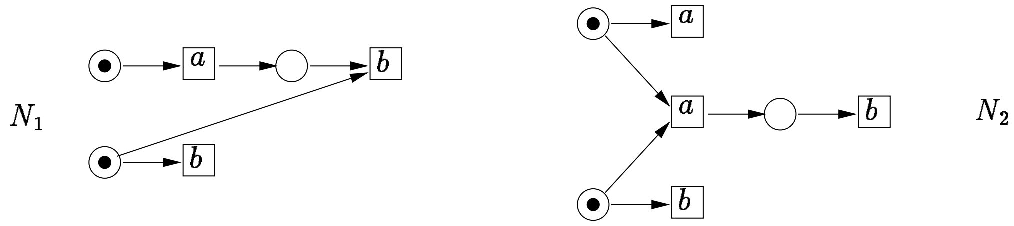

Figure 5: inequivalent nets with the same step traces

As pointed out in [JV95], the nets in Figure 6 are *IRT*- and *ART*-equivalent, but not *DRT*-equivalent, which might be regarded as counterintuitive. In both nets, a and b are activated concurrently and the additional b in N_2 should not make N_2 slower than N_1. But they are $\mathit{2RT}^\bullet$- (and thereby *2RT*-) equivalent.

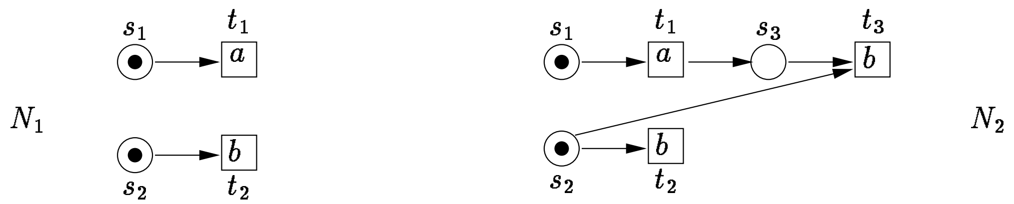

Figure 6: $\mathit{2RT}^\bullet$-, not *DRT*-equivalent nets

By [JV95], the nets in Figure 7 are *DRT*- and *IRT*-equivalent, but they are not *2RT*- (and thereby not $\mathit{2RT}^\bullet$-) equivalent. We have $l_1(t_1t_2^+t_3^+\Sigma\Sigma) = a^+\Sigma\Sigma \in \mathit{2RT}(N_1) \setminus \mathit{2RT}(N_2)$.

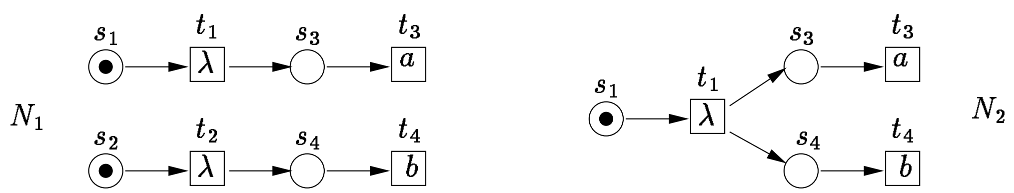

Figure 7: *DRT*-, *IRT*-, not *2RT*-equivalent nets

By [JV95], the nets in Figure 8 are *ART*-equivalent, but they are not *2RT*- (and thereby not $\mathit{2RT}^\bullet$-) equivalent. We have $l_1(t_1t_4\{a\}) = \{a\} \in \mathit{2RT}(N_1) \setminus \mathit{2RT}(N_2)$.

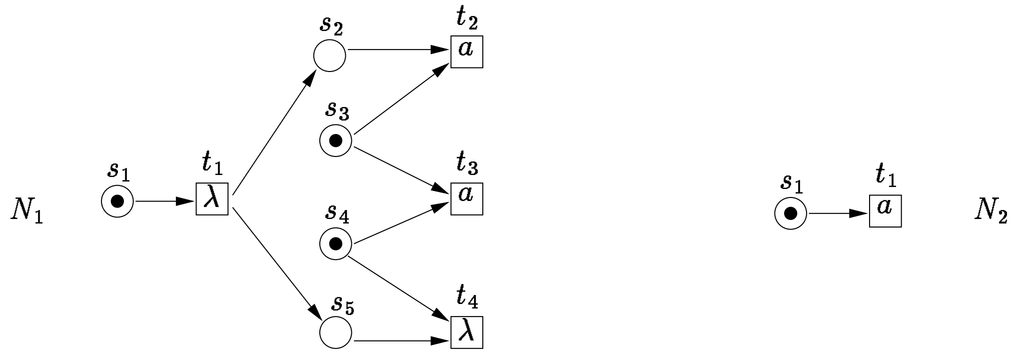

Figure 8: *ART*-, not *2RT*-equivalent nets

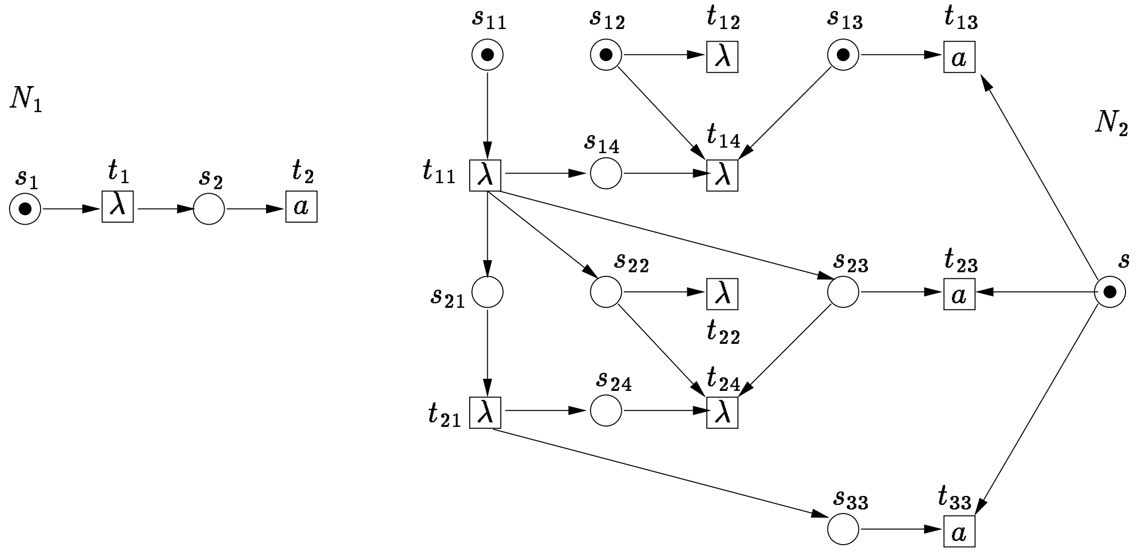

Figure 9: *2RT*$^\bullet$-, not *DRT*-, not *ART*-, not *IRT*-equivalent nets

The nets in Figure 9 are *2RT*$^\bullet$- (and thereby *2RT*-) equivalent and both not stable, but they are neither *DRT*-, nor *ART*-, nor *IRT*-equivalent. The following considerations show the *2RT*$^\bullet$-equivalence of the nets: In both nets, a is the only visible action and after occurrence of one a, all actions may be refused at all following time steps. The essential question is, how long a can be refused. Obviously, $l_1(\Sigma t_1^+ \Sigma\Sigma) = \Sigma\Sigma\Sigma \in \mathit{2RT}^\bullet(N_1)$; now a can not be refused any longer. We show that this trace is also in $\mathit{2RT}^\bullet(N_2)$, and that a can not be refused in N_2 after the third time step. Initially, a-labelled t_{13} is activated in N_2 and becomes urgent after the first Σ; now it can only be deactivated by instantaneous firing of urgent t_{11} and firing of t_{14}, which also disables the now urgent t_{12}. If a-labelled t_{13} is not deactivated this way, it will never be disabled since urgent t_{12} must fire before or during the next time step, and in this case a could not ever be refused again. Instantaneous firing of t_{11} before the second time step has enabled internal t_{21}, internal t_{22} and a-labelled t_{23}, and we are essentially in the same situation as before the first time step, i.e. another Σ may occur, t_{21} has to fire instantaneously and t_{22} must fire in order to deactivate urgent a-labelled t_{23} and urgent internal t_{22}. Now instantaneous firing of t_{21} before the third time step has enalbled

a-labelled t_{33}, which can not be disabled any more and becomes urgent after a third Σ, such that a can not be refused any longer after $\Sigma\Sigma\Sigma \in \mathit{2RT}^{\bullet}(N_2)$.

On the other hand, we have $l_2(t_{11}t_{14}\Sigma t_{21}t_{24}\Sigma) = \Sigma\Sigma \in (\mathit{DRT}(N_2) \cap \mathit{IRT}(N_2)) \setminus (\mathit{DRT}(N_1) \cup \mathit{IRT}(N_1))$ and actually $N_1 \sqsupseteq N_2$ and $N_1 \sqsupseteq_i N_2$. Somewhat surprisingly, we have $l_1(t_1^+\Sigma) \in \mathit{ART}(N_1) \setminus \mathit{ART}(N_2)$ and actually $N_2 \sqsupseteq_a N_1$.

The above examples have shown that, in general, $\geq_2$ and $\sqsupseteq_2$ are incomparable with $\sqsupseteq$, $\sqsupseteq_i$ and $\sqsupseteq_a$ which in turn are in general incomparable as shown in [JV95]. But at least for a special class of nets, we can show two implications.

Lemma 7.5

Let N be a net without internal transitions. Then

$$a_{11} \ldots a_{1n_1}\mu_1 X_1 \ldots a_{L1} \ldots a_{Ln_L}\mu_L X_L \in \mathit{ART}(N)$$

iff

$$a_{11}\emptyset\emptyset \ldots a_{1n_1}\emptyset\emptyset\mu_1 X_1\emptyset\emptyset \ldots a_{L1}\emptyset\emptyset \ldots a_{Ln_L}\emptyset\emptyset\mu_L X_L\emptyset\emptyset \in \mathit{2RT}(N),$$

where $a_{ij} \in \Sigma'$, μ_i a step and $X_i \subseteq \Sigma'$.

Proof: First observe that we can always $2r$-fire $\emptyset\emptyset$, in particular since there are no internal transitions and, hence, $l(t) \notin \emptyset \cup \{\lambda\}$ holds for all t. Furthermore, $2r$-firing $\emptyset\emptyset$ does not change the marking and makes all enabled transitions urgent.

We will show the claim inductively; observe that the sequences start from M_N and (M_N, U_N), where $U_N = \{t \mid M_N[t\rangle\}$. So assume that M and (M, U) with $U = \{t \mid M[t\rangle\}$ are given.

We have $M[t\rangle_a^r M'$ iff $(M, U)[t\emptyset\emptyset\rangle_2^r(M', U')$, where by the above remark $U' = \{t' \mid M'[t'\rangle\}$. Furthermore, $M[\mu X\rangle_a^r M'$ iff $M[\mu\rangle M'$ and $(M - {}^\bullet\mu)[t\rangle \Rightarrow l(t) \notin X$ iff $M[\mu\rangle M'$ and $t \in U \setminus ({}^\bullet\mu)^\bullet \Rightarrow l(t) \notin X$ iff $(M, U)[\mu X\rangle_2^r(M', U'')$ iff, by the above remark, $(M, U)[\mu X\emptyset\emptyset\rangle_2^r(M', U')$, where $U' = \{t' \mid M'[t'\rangle\}$. ■ 7.5

Theorem 7.6

Let N_1 and N_2 be nets without internal transitions. Then $N_1 \sqsupseteq_2 N_2$ implies $N_1 \sqsupseteq_a N_2$ and $N_1 \sqsupseteq_i N_2$.

Proof: For the first part take some $w \in \mathit{ART}(N_1)$. Applying the 'only-if'-part of Lemma 7.5 to w gives some $v \in \mathit{2RT}(N_1) \subseteq \mathit{2RT}(N_2)$, and applying the 'if'-part to $v \in \mathit{2RT}(N_2)$ shows $w \in \mathit{ART}(N_2)$.

For the second part take some $w \in \mathit{IRT}(N_1) \subseteq \mathit{2RT}(N_1) \subseteq \mathit{2RT}(N_2)$. Since there are no internal transitions, an underlying $v \in \mathit{2RFS}(N_2)$ cannot contain any (transition-) steps, i.e. $v \in \mathit{IRFS}(N_2)$ and $w \in \mathit{IRT}(N_2)$, too. ■ 7.6

8 Conclusion

We have developed a testing scenario for the worst-case efficiency of asynchronous systems using *dense* time, following the approach of [Vog95b, JV95], where in [JV95] a basic firing rule and two of its variants are investigated; the two variants turn out to be also variants of the present approach.

We have shown that, in fact, we can equivalently work with discrete time. The resulting testing preorder can be characterized with some kind of refusal traces and the important point is that their definition is significantly less involved than that of the basic variant in [JV95].

We have refined the testing preorder, which is naturally a preorder for parallel composition, to a precongruence for several operators for the modular construction of systems known from process algebras. This allows on the one hand easier and more efficient compositional reasoning about faster-than-properties of systems; on the other hand, it is a first step towards a connection of Petri-net-methods and process-algebra-methods in the area of timed – especially asynchronous – systems.

The testing preorder and its refinement are shown to satisfy some properties which make them attractive as faster-than relations. In general, the present approach is incomparable with the three variants developed in [JV95].

For the comparison with other literature I may refer to the explanations made in [JV95].

References

[AD94] R. Alur and D. Dill. A theory of timed automata. *Theoret. Comput. Sci.*, 126:183–235, 1994.

[DNH84] R. De Nicola and M.C.B. Hennessy. Testing equivalence for processes. *Theoret. Comput. Sci.*, 34:83–133, 1984.

[GV87] R.J. v. Glabbeek and F. Vaandrager. Petri net models for algebraic theories of concurrency. In J.W. de Bakker et al., editors, *PARLE Vol. II*, Lect. Notes Comp. Sci. 259, 224–242. Springer, 1987.

[JV95] L. Jenner and W. Vogler. Fast asynchronous systems in dense time. Technical Report Nr. 344, Inst. f. Mathematik, Univ. Augsburg, 1995. Extended abstract to appear in Proc. ICALP 96.

[LF81] N. Lynch and M. Fischer. On describing the behaviour and implementation of distributed systems. *Theoret. Comput. Sci.*, 13:17–43, 1981.

[LV95] N. Lynch and F. Vaandrager. Forward and backward simulations I: Untimed systems. *Information and Computation*, 121:214–233, 1995.

[Pet81] J.L. Peterson. *Petri Net Theory*. Prentice-Hall, 1981.

[Phi87] I. Phillips. Refusal testing. *Theoret. Comput. Sci.*, 50:241–284, 1987.

[Rei85] W. Reisig. *Petri Nets*. EATCS Monographs on Theoretical Computer Science 4. Springer, 1985.

[Vog92] W. Vogler. *Modular Construction and Partial Order Semantics of Petri Nets*. Lect. Notes Comp. Sci. 625. Springer, 1992.

[Vog95a] W. Vogler. Timed testing of concurrent systems. *Information and Computation*, 121:149–171, 1995.

[Vog95b] W. Vogler. Faster asynchronous systems. In I. Lee and S. Smolka, editors, *CONCUR 95*, Lect. Notes Comp. Sci. 962, 299–312. Springer, 1995.