Temporal Logic and Categories of Petri Nets

Carolyn Brown* and Doug Gurr†
School of Cognitive and Computing Sciences
University of Sussex, Falmer, Brighton, BN1 9QH

Abstract. We present a novel method for proving temporal properties of the behaviour a Petri net. Unlike existing methods, which involve an exhaustive examination of the transition system representing all behaviours of the net, our approach uses morphisms dependent only on the static structure of the net. These morphisms correspond to simulations. We restrict the analysis of dynamic behaviours to particularly simple nets (test nets), and establish temporal properties of a complex net by considering morphisms between it and various test nets. This approach is computationally efficient, and the construction of test nets is facilitated by the graphical representation of nets. The use of category theory permits a natural modular approach to proving properties of nets.

Our main result is the syntactic characterisation of two expressive classes of formulae: those whose satisfaction is preserved by morphisms and those whose satisfaction is reflected.

1 Introduction

Proving properties of the operational behaviour of Petri nets is computationally expensive, as most existing techniques [1] involve an exhaustive examination of the labelled transition system representing all possible markings and behaviours of the net. In this paper we describe a novel technique for proving properties of the behaviour of a Petri net by considering only the static structure of the net. Our approach exploits the simplicity of the graphical presentation of a net: it is sufficiently powerful to prove a wide range of properties but has complexity which is linear in the size of the net.

Our technique builds on our existing results concerning categories of Petri nets. In [2, 3, 4, 5] we studied a category **Net** whose objects are unmarked Petri nets. We proved in [5] that whenever there is a morphism from N to N' in **Net** then subject to a natural condition on the initial markings of the nets, N' can simulate any evolution of N. This result gives rise to a methodology for proving properties of the dynamic behaviour of a net by exhibiting morphisms in **Net**: such morphisms depend only on the static structure of the nets. The method involves constructing a number of simple "test" nets whose behavioural properties can either be inferred by inspection or proved using existing model-checking techniques. These test nets should be small enough that their properties can be established quickly and easily. We then establish properties of a more complex net by exhibiting morphisms between it and the test nets, and using the fact that the image net can always simulate the behaviour of the source net.

Some examples of this technique were given in [3], including proofs of liveness properties and of mutual exclusion properties. It is natural to ask what range of properties our technique can be used to demonstrate. In this paper we prove that our technique is powerful enough to establish properties which cover the full spectrum of Manna and Pnueli's hierarchy of temporal properties [8]. The main advantage of a technique based on the static structure of the net is that the complexity of model-checking is linear in the size of the net. An additional advantage is that the graphical presentation of a simple test net is a great aid to envisaging properties of its behaviour. The advantage of using category theory is that it gives rise to a compositional, modular proof system: this permits a structured approach to proving properties of large nets.

In [15], Winskel considered a category of nets which is essentially a subcategory of $\mathbf{MNet}^+$. He suggested that, informally, morphisms in his category of nets appeared to preserve liveness properties and to reflect safety properties. This judgement was based on the usual description of a safety property as expressing the fact that "something bad never happens" and a liveness property expressing the fact that "something desirable is guaranteed to happen." Our results show that the situation is more complex than this: we give a syntactic characterisations of formulae which are preserved, reflected or respected in a different sense by morphisms. Human insight is needed both in choosing morphisms and in designing suitable, efficient test nets, while checking that we have a morphism and that a test net satisfies a formula can be readily and efficiently automated.

In Section 2 we recall the elementary definitions of Petri net theory and give examples of the proof technique. In Section 3 we generalise the relevant results from [4, 5] and illustrate our approach with some examples. In Section 4 we define a temporal logic $\mathcal{T}$ for describing net behaviours and define a notion of satisfaction of a $\mathcal{T}$ formula by a marked net, and in Section 5 we give a syntactic characterisation of properties which are preserved or reflected by morphisms in our category. This fundamental result shows when we can deduce properties of a complex net from the existence of morphisms between it and test nets satisfying those properties. The check that a pair of functions $\langle f, F\rangle$ is a morphism from N to N' is linear in the size of the nets N and N', and so our technique is relatively efficient.

e-mail: carolynb@cogs.susx.ac.uk †UK Department of Transport

2 Definitions concerning Petri Nets

We recall some elementary definitions of Petri net theory: details may be found in [13].

Definition 1 *A* Petri net*, denoted N, is a 4–tuple $\langle E, B, pre, post\rangle$ where E and B are sets, and pre and post are functions from $E \times B$ to $\mathbb{N}$ which are zero on all but a finite subset of $E \times B$.*

We shall call elements of E *events* and elements of B *conditions*. We shall call *pre* and *post* the pre– and post–condition relations of N respectively. With each of the multirelations *pre* and *post* we associate a function of the same name from E to $B^{\oplus}$ (the free abelian monoid on B, with unit the empty multiset $\emptyset$) defined by

$$pre(e) = \sum_{b \in B} pre(e,b)b \quad \text{and} \quad post(e) = \sum_{b \in B} post(e,b)b.$$

We call $pre(e)$ the pre–condition set and $post(e)$ the post–condition set of e. A *loop* arises if the pre- and post-condition sets of an event intersect non-trivially. A *1-loop* is a loop such that for every $b \in pre(e) \cap post(e)$ we have $pre(e,b) = post(e,b) = 1$. All loops which are not 1-loops are *multi-loops*. We shall only consider the class of nets without multi-loops, which we call **Petri**.

The state of a net is described by a finite multiset over B (that is, a multiset which is zero on all but finitely many $b \in B$), called a *marking*, which indicates which conditions hold, and in what multiplicities. A *marked net* is a pair $\langle M, N\rangle$, where N is a net and M is a marking of N.

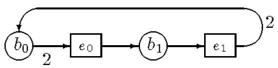
The occurrence of an event, called a firing, transforms the state of the net by consuming its pre–condition set and producing its post–condition set. We say $\langle M, N\rangle$ *enables* $\Sigma n_i e_i$ if the marking M contains the multiset $\Sigma n_i pre(e_i)$. The multiset $\Sigma n_i e_i$ of events, called a *step*, can then fire concurrently. We denote this firing $M \xrightarrow{\Sigma n_i e_i} M - \Sigma n_i pre(e_i) + \Sigma n_i post(e_i)$. We permit identity steps which leave the marking of a net unchanged, but require that a net never fire infinitely many identity steps when a non-empty step is enabled (this requirement may be seen either as a progress assumption or as a fairness assumption). A *step sequence* or *computation* is a possibly infinite sequence of steps $M \xrightarrow{\sigma_0} M_0 \xrightarrow{\sigma_1} \ldots$, sometimes written $\sigma_0 ; \sigma_1 ; \ldots$. Since we can extend any finite computation to an infinite one by repeating a trivial identity step indefinitely, we shall restrict our attention to infinite computations. The set of computations of a net $\langle M, N\rangle$ is denoted by C_N^M. If σ is a computation then $\overline{\sigma}_{k+1}$ denotes

the computation whose ith step is the $(k+i)$th step of σ: thus $\overline{\sigma}_{k+1} = \sigma_{k+1} ; \sigma_{k+2} ; \ldots$.

The finiteness condition on *pre* and *post* ensures that at every point in the evolution of the net, finitely many events are enabled and finitely many conditions are marked. It therefore ensures that the net describes a finitely-branching process.

3 Categories of Nets: extending existing results

In the past [2, 3, 4, 5] we have considered primarily unmarked nets, structural properties of nets and modular specification using categorical constructions on nets. We derived results about a net's behaviour for all initial markings or for those markings meeting a given condition. It is clear that the behavioural properties of a net depend crucially on its initial marking: for example, in the net

$N =$ 

with marking $2b_0$, some event is always enabled and in the course of any step sequence, e_0 is enabled infinitely often. However, the net $\langle b_0, N\rangle$ possesses neither of these properties. In this paper we therefore work with explicit markings, modifying our earlier definitions and results accordingly. (In the notation of Section 4, if $\theta(\alpha_i) = e_i$ for $i = 0, 1$ then $\langle 2b_0, N\rangle \models_\theta \Box\exists x.E(x)$ and $\langle 2b_0, N\rangle \models_\theta \Box\Diamond E(\alpha_0)$ but it is not the case that $\langle b_0, N\rangle \models_\theta \Box\exists x.E(x) \vee \Box\Diamond E(\alpha_0)$).

It is our intention to prove properties of a net N by exhibiting morphisms between N and various test nets T_i. This approach is most efficient if our test nets are small. We can use smaller test nets if, rather than insisting that a morphism from N to N' map events of N to events of N' (as in our earlier work), we allow an event of N to be mapped to a finite computation of N' (as will be done in proving absence of starvation in Section 3.2). With this aim, we now generalise the results of [3, 5]: such a generalisation is somewhat in the spirit of [9].

3.1 *A Category of Nets for proving Temporal Properties*

Intuitively, a computation is either an event (possibly idle) or the parallel or sequential composition of two computations. The parallel composition of computations c and d, written $c + d$, occurs when they can fire simultaneously, consuming $pre(c) + pre(d)$ and producing $post(c) + post(d)$. The sequential composition of c and d, written $c ; d$, occurs when c can fire to reach a marking in which d is enabled. We extend the pre and post-condition relations of a net from events to computations in the evident way. For parallel composition,we define

$$pre(c_0 + c_1) = pre(c_0) + pre(c_1) \quad \text{and} \quad post(c_0 + c_1) = post(c_0) + post(c_1).$$

Defining pre and postcondition relations for sequential composition requires a little care. Note that sequential composition is associative, even though its definition implicitly involves truncated subtraction[1] $\ominus$ which is not in general associative.

$$pre(c_0\,;c_1, b) = \begin{cases} pre(c_0, b) + pre(c_1, b) - post(c_0, b) & \text{if } post(c_0, b) \leq pre(c_1, b) \\ pre(c_0, b) & \text{otherwise} \end{cases}$$

and

$$post(c_0\,;c_1, b) = \begin{cases} post(c_1, b) + post(c_0, b) - pre(c_0, b) & \text{if } pre(c_0, b) \leq post(c_1, b) \\ post(c_1, b) & \text{otherwise.} \end{cases}$$

Suppose we have a function $F\colon B' \to B$ which maps the conditions in a simulating net N' to the conditions in the original net N which they implement. Let M be a marking of N and M' a marking of N'. Whenever M' contains enough resources to implement all the resources marked in M, we expect the simulating net $\langle M', N' \rangle$ to be able to simulate any computation of $\langle M, N \rangle$. This relationship between markings is formalised in the following definition.

Definition 2 *Let F be a function from a set B' to a set B. The relation $F^+ \subseteq B^{\oplus} \times B'^{\oplus}$ is given by*

$$\langle M, M' \rangle \in F^+ \quad \textit{if and only if} \quad MF \leq M',$$

that is, if and only if for each $b' \in B'$ we have $M(Fb') \;\leq\; M'(b')$.

Expressing this definition succinctly as a diagram in **Set**, we have $\langle M, M' \rangle \in F^+$ if and only if

$$\begin{tikzcd} B' \arrow[r, "F"] \arrow[d, "M'"'] \arrow[dr, phantom, "\geq"] & B \arrow[dl, "M"] \\ \mathbb{N} & \end{tikzcd}$$

where we extend the usual ordering $\geq$ on $\mathbb{N}$ pointwise to functions into $\mathbb{N}$.

[1] defined by $m \ominus n = \max\{n - m, 0\}$

We now define a category of marked nets in which morphisms from $\langle M, N \rangle$ to $\langle M', N' \rangle$ map events of a N to computations of N'.

Definition 3 *The category $\mathbf{MNet}^+$ is defined by the following data:*

- *objects are marked nets $\langle M, N \rangle$ where N is an element of* **Petri***,*
- *a morphism from $\langle M, E, B, pre, post \rangle$ to $\langle M', E', B', pre', post' \rangle$ is a pair of functions $\langle f, F \rangle$ with $f\colon E \to E'^+$ and $F\colon B' \to B$ such that $\langle M, M' \rangle \in F^+$ and in* **Set** *we have*

$$\begin{tikzcd} E \times B' \arrow[r, "1 \times F"] \arrow[d, "f \times 1"'] \arrow[dr, phantom, "\leq"] & E \times B \arrow[d, "pre"] \\ E'^+ \times B' \arrow[r, "pre'"'] & \mathbb{N} \end{tikzcd} \quad \textit{and} \quad \begin{tikzcd} E \times B' \arrow[r, "1 \times F"] \arrow[d, "f \times 1"'] \arrow[dr, phantom, "\geq"] & E \times B \arrow[d, "post"] \\ E'^+ \times B' \arrow[r, "post'"'] & \mathbb{N}, \end{tikzcd}$$

  that is, for each $e \in E$ and each $b' \in B'$

$$pre(e, Fb') \geq pre'(fe, b') \quad \text{and} \quad post(e, Fb') \leq post'(fe, b'),$$

- *and composition is function composition in each component.*

Remark 1 *It follows immediately from the above definition that if $\langle f, F \rangle : \langle M, N \rangle \longrightarrow \langle M', N' \rangle$ is a morphism in $\mathbf{MNet}^+$ and $\langle M_1, M_1' \rangle \in F^+$ then $\langle f, F \rangle$ is a morphism from $\langle M_1, N \rangle$ to $\langle M_1', N' \rangle$ in $\mathbf{MNet}^+$.*

Morphisms in $\mathbf{MNet}^+$ are defined on the purely static structure of nets, but capture precisely a notion of simulation between the dynamic behaviours of nets, as the following results show.

Proposition 2 *Let $\langle f, F \rangle$ be a morphism from $\langle M_0, N \rangle$ to $\langle M_0', N' \rangle$ in $\mathbf{MNet}^+$. Then for all $e \in E$, if $M_0 \xrightarrow{e} M_1$ in N then $M_0' \xrightarrow{fe} M_1'$ in N' and $\langle M_1, M_1' \rangle \in F^+$. Furthermore, $\langle f, F \rangle$ is a morphism from $\langle M_1, N \rangle$ to $\langle M_1', N' \rangle$ in $\mathbf{MNet}^+$.*

Proof: For each $b' \in B'$ we have
$$\begin{aligned} M_0'(b') &\geq M_0(Fb') && \text{as } \langle M_0, M_0' \rangle \in F^+ \\ &\geq pre(e, Fb') && \text{as } M_0 \text{ enables } e \\ &\geq pre'(fe, b') && \text{by definition,} \end{aligned}$$

and so M_0' enables fe. Further, for each $b' \in B'$,

$$\begin{aligned} M_1'(b') &= M_0'(b') - pre'(fe, b') + post'(fe, b') \\ &\geq M_0(Fb') - pre(e, Fb') + post(e, Fb') \\ &= M_1(Fb') \end{aligned}$$

and so $\langle M_1, M_1' \rangle \in F^+$. That $\langle f, F\rangle : \langle M_1, N\rangle \to \langle M_1', N'\rangle$ in $\mathbf{MNet}^+$ follows immediately from Remark 1. $\square$

Corollary 3 *Let $\langle f, F\rangle$ be a morphism from $\langle M_0, N\rangle$ to $\langle M_0', N'\rangle$ in $\mathbf{MNet}^+$. For $i \in \{0, \ldots, n\}$ let $\sigma_i = \sum_1^{k_i} n_j e_j$ be a multiset of events of N. Extend f to multisets of events by putting $f(t+s) = f(t)+f(s)$. If $\langle M_0, N\rangle$ enables the computation $M_0 \xrightarrow{\sigma_0} M_1 \xrightarrow{\sigma_1} \cdots M_n$ then $\langle M_0', N'\rangle$ enables the computation $M_0' \xrightarrow{f\sigma_0} M_1' \xrightarrow{f\sigma_1} \cdots M_n'$.*

Proof: Suppose the result does not hold. Let n be the smallest integer such that $\langle M_0, N\rangle$ enables $\sigma_0 ; \sigma_1 ; \ldots \sigma_n$ and $\langle M_0', N'\rangle$ does not enable $f\sigma_0 ; f\sigma_1 ; \ldots f\sigma_n$. Now in N we have $M_0 \xrightarrow{\sigma_0} M_1 \xrightarrow{\sigma_1} ; \ldots \xrightarrow{\sigma_{n-1}} M_n$, and it follows by minimality of n that in N' we have $M_0' \xrightarrow{f\sigma_0} M_1' ; \xrightarrow{f\sigma_1} ; \ldots \xrightarrow{f\sigma_{n-1}} M_n'$. Applying Proposition 2 n times, we see that $\langle M_n, M_n'\rangle \in F^+$ and $\langle f, F\rangle$ is a morphism from $\langle M_n, N\rangle$ to $\langle M_n', N'\rangle$. Since $\langle M_n, N\rangle$ enables σ_n, it follows from Proposition 2 that $\langle M_n', N'\rangle$ enables $f\sigma_n$. But this contradicts our assumption that $\langle M_0', N'\rangle$ does not enable $f\sigma_0 ; f\sigma_1 ; \ldots f\sigma_n$. The result follows. $\square$

Proposition 2 shows that if a pair of markings $\langle M, M'\rangle$ is in F^+, then the net $\langle M', N'\rangle$ can simulate any one–step computation of $\langle M, N\rangle$, in the sense that whenever $\langle M, N\rangle$ enables an event e, $\langle M', N'\rangle$ enables the computation fe. Corollary 3 shows that N' can simulate any computation of N. We say that N' *simulates* N.

Definition 4 *Let $\langle M, N\rangle$ and $\langle M', N'\rangle$ be nets and let $f : E \to E'^+$ and $F : B' \to B$ be functions. Then $\langle M', N'\rangle$* simulates *$\langle M, N\rangle$ (and $\langle f, F\rangle$ is a* simulation*), if and only if $\langle M, M'\rangle \in F^+$ and for all pairs of markings $\langle M_0, M_0'\rangle \in F^+$,*

$$\text{if } M_0 \xrightarrow{e} M_1 \text{ then } M_0' \xrightarrow{fe} M_1' \text{ and } \langle M_1, M_1'\rangle \in F^+.$$

By Corollary 3, every morphism in $\mathbf{MNet}^+$ is a simulation. The converse also holds:

Proposition 4 *Let N and N' be elements of* **Petri** *and let $\langle f, F\rangle$ be a simulation from $\langle M, N\rangle$ to $\langle M', N'\rangle$ which preserves 1-loops, that is,*

$$\text{if } pre(e, Fb') = post(e, Fb') = 1 \text{ then } pre'(fe, b') = post'(fe, b') = 1$$

Then $\langle f, F\rangle : \langle M, N\rangle \longrightarrow \langle M', N'\rangle$ in $\mathbf{MNet}^+$.

Proof: Let $M_0 = pre(e)$ and $M_0' = M_0F$. Then $\langle M_0, M_0'\rangle \in F^+$. Since M_0 enables e and $\langle f, F\rangle$ is a simulation, M_0' enables $f(e)$. Hence for each $b' \in B'$, $pre'(fe, b') \leq M'(b') = M(F(b')) = pre(e, Fb')$.
We now show that for each $b' \in B'$, $post(e, Fb') \leq post'(fe, b')$. Putting $M_1 = post(e)$ and $M_1' = M_0F - pre'(fe) + post'(fe)$, we have $M_0 \xrightarrow{e} M_1$ and $M_0' \xrightarrow{fe} M_1'$. For each $b' \in B'$, $M_1(Fb') = post(e, Fb') \leq pre(e, Fb') - pre'(fe, b') + post'(fe, b')$.
Now, if $post(e, Fb') = 0$ then $post(e, Fb') \leq post'(fe, b')$ and we are done. Otherwise, as N has no multiloops, either $pre(e, Fb') = post(e, Fb') = pre'(fe, b') = post'(fe, b') = 1$ (since $\langle f, F\rangle$ preserves 1-loops) and we are done, or $pre(e, Fb') = 0$. In the latter case $pre'(fe, b') = 0$ since $pre'(fe, b') \leq pre(e, Fb')$, whence $post(e, Fb') \leq 0 - 0 + post'(fe, b')$ as required.
Since $\langle f, F\rangle$ is a simulation, $\langle M, M'\rangle \in F^+$: it follows that $\langle f, F\rangle$ is a morphism from $\langle M, N\rangle$ to $\langle M', N'\rangle$ in $\mathbf{MNet}^+$. $\square$

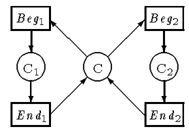
The results of this section are important because they show that, not only do the morphisms of $\mathbf{MNet}^+$ have a meaningful computational interpretation, but further, all simulations between nets without multi-loops are morphisms in $\mathbf{MNet}^+$.

3.2 An Example: proving a safety and a liveness property

We illustrate a proof of a safety property and a liveness property, using an example taken from [11]. Olderog presents the nets N_1 and N_2 below, and wishes to examine the relationship between them. As he says, "Intuitively, N_2 is obtained from N_1 by *abstracting* from the actions NCr_i, Req_i and Out_i, $i = 1, 2$, in N_1, i.e. by transforming them into internal actions τ and then forgetting about the τ's". We shall give a morphism which effects such an abstraction. For simplicity, in the net N_1 (depicted in Figure 1), we have only named those conditions which will be in the image of our morphisms or in the initial marking of N_1.

Given marking C, the net N_2 below forces a choice between the evolutions $Beg_1 ; End_1$ and $Beg_2 ; End_2$:

The net N_2



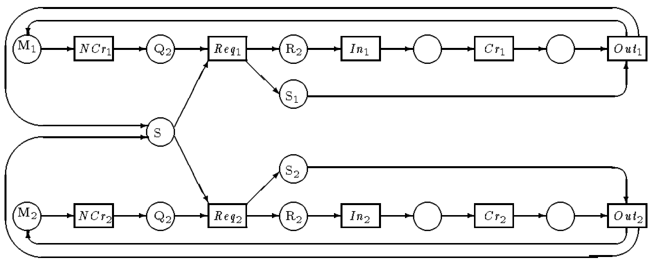


FIGURE 1. *The net N_1: mutual exclusion*

It is readily proved that every behaviour of the net $\langle C, N_2\rangle$ is a sequence of form $Beg_a\,;End_a\,;Beg_b\,;End_b\,;Beg_c\,;End_c\,;\ldots$ where a, b and c range over $\{1,2\}$. We shall add to the net N_2 a trivial event $*$, which has empty pre- and post-condition set. The resultant net $\langle C, N_2 + \bot\rangle$ is the coproduct in $\mathbf{MNet}^+$ of N_2 with the marked net $\bot = \langle\emptyset, \{*\}, \{*\}, 0, 0\rangle$ (where 0 denotes the empty multirelation). There is a morphism $\langle f, F\rangle$ in $\mathbf{MNet}^+$ from $\langle M_1 + M_2 + S, N_1\rangle$ to $\langle C, N_2 + \bot\rangle$ given by:

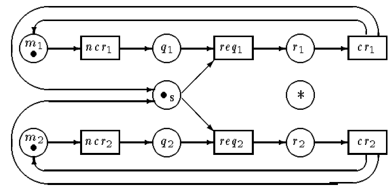
$$
\begin{array}{lll}
f(Req_i) = Beg_i & f(Out_i) = End_i & f(e) = * \text{ for all other events } e\\
F(C) = S & F(C_i) = S_i &
\end{array}
$$

By Corollary 3, the existence of this morphism shows that the net $\langle C, N_2 + \bot\rangle$ can simulate any behaviour of the net $\langle M_1 + M_2 + S, N_1\rangle$. Since the behaviour of the image net is so restricted (indeed, $\langle f, F\rangle$ is minimal in the sense of Definition 11), this proves an important feature of the marked net $\langle M_1 + M_2 + S, N_1\rangle$, that it can never reach a state in which Req_2 can occur if Req_1 has occurred and Out_1 has not. This, together with the analogous property for Req_2, ensures that $\langle M_1 + M_2 + S, N_1\rangle$ preserves mutual exclusion of the behaviours $In_1; Cr_1; Out_1$ and $In_2; Cr_2; Out_2$. This example is particularly simple. Note, however, for any net $\langle M, N\rangle$ intended as a mutual exclusion algorithm, the existence of a morphism from $\langle M, N\rangle$ to $\langle C, N_2 + \bot\rangle$ can be used to demonstrate that $\langle M, N\rangle$ preserves mutual exclusion.

The net $\langle C, N_2\rangle$ describes the behaviour of the shared resource, abstracting away from the competing processes. A different abstraction is

given in the net $\langle m_1 + m_2 + s, N_3\rangle$ below, which describes only the possible states of the processes (critical, requesting entry to the critical region, or neither of these) and how these interact. There is a morphism $\langle g, G\rangle$ in $\mathbf{MNet}^+$ from $\langle m_1 + m_2 + s, N_3\rangle$ to $\langle M_1 + M_2 + S, N_1\rangle$ given by:

$$
\begin{array}{lll}
g(ncr_i) = Ncr_i & g(req_i) = Req_i & g(cr_i) = In_i\,;Cr_i\,;In_i\\
G(M_i) = m_i & G(Q_i) = q_i & G(R_i) = G(S_i) = r_i\\
G(S) = s & G(b) = * \text{ for all other conditions } b \text{ of } N_1 &
\end{array}
$$



The marked net $\langle m_1 + m_2 + s, N_3\rangle$

We shall assume strong fairness in the sense that if any event of N_3 is enabled infinitely often, it occurs infinitely often. Note that $\langle g, G\rangle$ is minimal in the sense of Definition 11 and so preserves strong fairness (see Example 2). Clearly, if q_1 is marked in N_3 but req_1 never occurs, then q_1 is always marked. Also, s is marked infinitely often. Hence req_1 is enabled infinitely often and by strong fairness must occur infinitely often, contradicting the assumption that req_1 never occurs. We deduce that $\langle m_1 + m_2 + s, N_3\rangle$ satisfies a liveness property which might be called "absence of starvation", stating that if a process requests entry to its critical region, it eventually enters it. This property is preserved by $\langle g, G\rangle$ and thus $\langle M_1 + M_2 + S, N_1\rangle$ also satisfies absence of starvation. This small example illustrates two ways in which morphisms reduce the complexity of model-checking: conditions can be identified and computations can be collapsed to single events (r_1 corresponds to both S_1 and R_1 while cr_1 corresponds to $In_1\,;Cr_1\,;Out_1$).

In Section 4, we develop a means of expressing such proofs formally. We define temporal and modal logics which express properties of nets as temporal logic formulae. A net satisfies a formula if its behaviour has the property described by that formula. We show that satisfaction of certain formulae is preserved by morphisms in $\mathbf{MNet}^+$, while satisfaction of other formula is reflected. Suppose that $\langle f, F\rangle$: $\langle M, N\rangle \to \langle M', N'\rangle$ in $\mathbf{MNet}^+$. If $\langle M, N\rangle$ has the property described by ϕ and satisfaction of ϕ

is preserved by morphisms then $\langle M', N'\rangle$ also has the property described by ϕ. If $\langle M', N'\rangle$ has the property described by ψ and satisfaction of ψ is reflected by morphisms then $\langle M, N\rangle$ also has the property described by ψ.

In Section 5.1 we reprove the results of this section in our formal setting. We do this by expressing mutual exclusion and absence of starvation as temporal logic formulae and showing that the existence of the morphisms $\langle f, F\rangle$ and $\langle g, G\rangle$ can be used to prove that $\langle M_1 + M_2 + S, N_1\rangle$ satisfies both properties, without explicitly considering the set of possible behaviours of $\langle M_1 + M_2 + S, N_1\rangle$.

4 A Temporal Logic for Enablement

The main purpose of modal and temporal logics is the specification of complex concurrent systems. A specification is the conjunction of formulae each describing a property required of a system: our technique facilitates the proof that a net satisfies each conjunct in its specification. Classifying properties helps to prevent underspecification: we know, for example, that a full specification must describe both safety and liveness properties. The categorical approach offers a basis for successive refinements (since we can compose morphisms) and for a compositional proof system exploiting structure in our category of processes.

The examples of Section 3.2 gave simple test nets possessing properties of mutual exclusion and absence of starvation, and used morphisms to demonstrate that a more complex net also had these properties. A key point is that we proved properties of the complex net without reference to its dynamic behaviour. We now prove that this technique applies to a large class of properties, which we characterise syntactically in Section 5. In this section we develop a simple modal language $\mathcal{M}$ and temporal language $\mathcal{T}$ for discussing net behaviours. We give interpretations of $\mathcal{M}$ and $\mathcal{T}$ in any marked net, define a notion of satisfaction and demonstrate the expressiveness of our logics. This section formalises the arguments of Section 3.2, and demonstrates the expressive power of the formulae for which our technique can be applied.

Modal logics use modalities to express the effects of events firing. For each step s, the operator $[s]$ means "after every s-step", while its dual $\neg[s]\neg$, abbreviated $\langle s\rangle$, means "after some s-step". We assume disjoint collections of variables (ranged over by $x, x_0, \ldots$) and constants (ranged over by $\alpha, \alpha_0, \alpha_1, \ldots$). A *term* of $\mathcal{M}$ is either a variable, a constant, a multiset of constants or a sequence of two terms. $\mathcal{M}$ is the modal language

given by:

$$\phi ::= \mathtt{tt} \;\Big|\; \neg\phi \;\Big|\; \phi \wedge \phi \;\Big|\; \langle t\rangle\phi \;\Big|\; \forall x.\phi \quad \text{for } t \text{ a closed term and } x \text{ a variable.}$$

We define formulae $\mathtt{ff}$, $\phi \vee \psi$, $\phi \rightarrow \psi$, $\exists x.\phi$, $[t]\phi$ and $\phi \leftrightarrow \psi$ (logical equivalence) in the usual, classical way. The quantifiers $\forall$ and $\exists$ bind variables, and a formula is closed if it has no free variables. Closed terms are ranged over by t. We write $\phi[e/x]$ to stand for ϕ with e substituted for all free occurrences of x, subject to the usual renaming of bound variables. We define an interpretation of an $\mathcal{M}$ formula ϕ in a marked net inductively in terms of an interpretation of the constants α_i which occur in ϕ as computations of the net. An *interpretation* of $\mathcal{M}$ in a marked net $\langle M, N\rangle$ is a partial function θ from the constants α_i of $\mathcal{M}$ to the computations E^+ of N. $dom(\theta)$ denotes the set of constants on which θ is defined. We extend θ homomorphically to closed terms.

Definition 5 *The satisfaction relation $\models_\theta$ between marked nets and closed formulae of $\mathcal{M}$ relative to an interpretation θ of $\mathcal{M}$ in $\langle M, N\rangle$ is defined as follows:*

1 $\langle M, N\rangle \models_\theta \mathtt{tt}$
2 $\langle M, N\rangle \models_\theta \neg\phi$ *iff it is not the case that* $\langle M, N\rangle \models_\theta \phi$
3 $\langle M, N\rangle \models_\theta \phi \wedge \psi$ *iff* $\langle M, N\rangle \models_\theta \phi$ *and* $\langle M, N\rangle \models_\theta \psi$
4 $\langle M, N\rangle \models_\theta \forall x.\phi$ *iff for all* $\alpha \in dom(\theta)$ *we have* $\langle M, N\rangle \models_\theta \phi[\alpha/x]$
5 $\langle M, N\rangle \models_\theta [t]\phi$ *iff whenever* $M \xrightarrow{\theta t} M'$ *we have* $\langle M', N\rangle \models_\theta \phi$.

The satisfaction relation is then determined for the derived operators. For example, we have:

$\langle M, N\rangle \models_\theta \phi \vee \psi$ iff $\langle M, N\rangle \models_\theta \phi$ or $\langle M, N\rangle \models_\theta \psi$
$\langle M, N\rangle \models_\theta \phi \rightarrow \psi$ iff whenever $\langle M, N\rangle \models_\theta \phi$ then $\langle M, N\rangle \models_\theta \psi$
$\langle M, N\rangle \models_\theta \exists x.\phi$ iff $\exists\alpha \in dom(\theta)$ such that $\langle M, N\rangle \models_\theta \phi[\alpha/x]$
$\langle M, N\rangle \models_\theta \langle t\rangle\phi$ iff $\exists M'$ such that $M \xrightarrow{\theta t} M'$ and $\langle M', N\rangle \models_\theta \phi$.

Rules 1 to 4 give satisfaction a standard meaning in the style of Tarski: in particular, they reflect the fact that our logic is classical. The interesting rule is 5, which expresses the interaction of the modal operators with evolution of the net. Thus $\langle M, N\rangle \models_\theta \langle\alpha\rangle\phi$ if M can evolve under $\theta(\alpha)$ to a marking in which ϕ is satisfied. Similarly, $\langle M, N\rangle \models_\theta \exists x.\langle x\rangle\phi$ if it is possible to satisfy ϕ after a computation interpreting some constant.

Let t be a closed term of $\mathcal{M}$. Define $E(t)$ to be the formula $\langle t\rangle\mathtt{tt}$. Then $\langle M, N\rangle \models_\theta E(t)$ exactly when the computation in $\langle M, N\rangle$ which interprets the term t is enabled. It follows from the definition of satisfaction that $\langle M, N\rangle \models_\theta \neg E(t)$ if and only if $\langle M, N\rangle \models_\theta \langle t\rangle \mathrm{ff}$, that is, precisely when the computation interpreting t is not enabled. Observe that if α is interpreted by the identity step id_{nb} then $\langle M, N\rangle \models_\theta E(\alpha)$ whenever the condition b is marked in $\langle M, N\rangle$ with at least n tokens. In general such properties as mutual exclusion or freedom from deadlock can be expressed in terms of the enabling of events. For example, the fact that two events e_0 and e_1 cannot occur concurrently is expressed by the formula $\neg E(\alpha_0 + \alpha_1)$, where α_i is interpreted in $\langle M, N\rangle$ by e_i.

We wish to specify and reason about both the overall behaviour of a net and individual enabled steps: we therefore turn our attention from steps to step sequences, and extend $\mathcal{M}$ to the temporal logic $\mathcal{T}$ by considering the modal formulae which hold on computation paths rather than at individual states. $\mathcal{T}$ is given by:

$$\phi ::= \mathrm{tt} \;\Big|\; \neg\phi \;\Big|\; \phi \wedge \phi \;\Big|\; \forall x.\phi \;\Big|\; [t]\phi \;\Big|\; \Box\phi \quad \text{for } t \text{ a closed term.}$$

Definition 5 *The interpretation of a closed formula ϕ of $\mathcal{T}$ relative to an interpretation θ of $\mathcal{T}$ in a marked net $\langle M, N\rangle$ is a set of step sequences $\sigma = \sigma_0 \,;\, \sigma_1 \,;\, \ldots$ given as follows:*

$\sigma \in [\![\mathrm{tt}]\!]_\theta$ *for any* σ
$\sigma \in [\![\neg\phi]\!]_\theta$ *iff it is not the case that* $\sigma \in [\![\phi]\!]_\theta$
$\sigma \in [\![\phi \wedge \psi]\!]_\theta$ *iff* $\sigma \in [\![\phi]\!]_\theta \cap [\![\psi]\!]_\theta$
$\sigma \in [\![\forall x.\phi]\!]_\theta$ *iff for all* $\alpha \in dom(\theta)$ *we have* $\sigma \in [\![\phi[\alpha/x]]\!]_\theta$
$\sigma \in [\![[t]\phi]\!]_\theta$ *iff whenever there exists* k *such that* $\sigma_0 \,;\, \sigma_1 \,;\, \ldots \,;\, \sigma_k = \theta(t)$ *then* $\overline{\sigma}_{k+1} \in [\![\phi]\!]_\theta$
$\sigma \in [\![\Box\phi]\!]_\theta$ *iff for each* i *we have* $\sigma_i \,;\, \sigma_{i+1} \,;\, \ldots \in [\![\phi]\!]_\theta$.

The satisfaction relation $\models$ between marked nets and closed formulae of $\mathcal{T}$ relative to θ is given by $\langle M, N\rangle \models_\theta \phi$ iff every computation of $\langle M, N\rangle$ is an element of $[\![\phi]\!]_\theta$.

This interpretation gives the usual meaning to the derived operators. Thus $\langle M, N\rangle \models_\theta \Diamond\phi$ precisely when every computation of $\langle M, N\rangle$ eventually satisfies ϕ, while $\langle M, N\rangle \models_\theta \langle t\rangle\phi$ precisely when $\langle M, N\rangle$ can evolve under $\theta(t)$ to $\langle M', N\rangle$ and $\langle M', N\rangle \models_\theta \phi$. We could define $\models_\theta$ relative to certain fairness or liveness assumptions, considering, for example, only those step sequences which are *weakly* or *strongly fair* [7]. In his temporal logic for occurrence nets [14], Reisig restricts attention to behaviours in which no condition ever contains more than one token.

The language $\mathcal{T}$ expresses many interesting properties of nets, both positive (what can be enabled) and negative (what cannot be enabled).

For example, mutual exclusion of events interpreting α_0 and α_1 is expressed by satisfaction of the formula $\Box\neg E(\alpha_0 + \alpha_1)$ while freedom from deadlock is expressed by satisfaction of the formula $\Box\exists x.E(x)$.

In practice, the graphical representation of nets facilitates the creative process of constructing test nets. It appears difficult to find an algorithm which constructs an efficient test net corresponding to a given formula (especially in the case of negation). Each test net can be used to establish a property for many different complex nets, however, which justifies considerable effort in constructing test nets. An efficient (smaller) test net offers savings each time it is used.

This paper aims to demonstrate by means of modal and temporal logic the wide range of properties which our technique can be used to prove. The principal rôle of the logics $\mathcal{M}$ and $\mathcal{T}$ lies in providing a sufficiently powerful language to express the properties which concern us. We do not here explore proof systems, beyond observing that, in addition to the usual proof rules for modal logic [6] and temporal logic [7], the net model satisfies proof rules corresponding to properties of nets, including the evident rules reflecting the following facts

- $\langle M + pre(\theta(t)), N\rangle \models_\theta E(t)$ for any marking M of N,
- if $\langle M, N\rangle \models_\theta E(t_0 \,;\, t_1)$ then $\langle M, N\rangle \models_\theta E(t_0)$ and $\langle M, N\rangle \models_\theta \Diamond E(t_1)$ and
- if $\langle M, N\rangle \models_\theta E(t_0 + t_1)$ then $\langle M, N\rangle \models_\theta E(t_0) \wedge E(t_1)$.

Further rules reflect the interaction between satisfaction and structure in the category $\mathbf{MNet}^+$.

5 The Interaction of the Logics with the Categorical Framework

In this section, we show more precisely how the satisfaction of modal and temporal logic formulae interacts with morphisms and structure in $\mathbf{MNet}^+$. This is necessary for compositional and modular reasoning about the properties satisfied by net behaviours.

We first express the properties we require a net $\langle M, N\rangle$ to satisfy as temporal logic formulae. In general these formulae are either preserved or reflected by morphisms in $\mathbf{MNet}^+$. For each formula ϕ whose satisfaction is preserved, we seek a test net T which is readily shown to satisfy ϕ and which maps to $\langle M, N\rangle$ by morphism $\langle f, F\rangle$ in $\mathbf{MNet}^+$. When we have found suitable T and $\langle f, F\rangle$, we conclude that $\langle M, N\rangle$ satisfies ϕ. Similarly, for each formula ψ whose satisfaction is reflected, we seek a test net T' and a morphism $\langle g, G\rangle$ from $\langle M, N\rangle$ to T'.

Let $\mathcal{L}$ be the sublanguage of the modal language $\mathcal{M}$ without negation or quantification, given by:

$$\phi ::= \mathrm{tt} \;\Big|\; \mathrm{ff} \;\Big|\; \langle t\rangle\phi \;\Big|\; [t]\phi \;\Big|\; \phi\wedge\phi \;\Big|\; \phi\vee\phi \quad \text{for } t \text{ a closed term.}$$

The language $\mathcal{L}$ is of particular interest because, if t is restricted to constant terms, $\mathcal{L}$ characterises strong bisimulation of processes in CCS in the sense that two finitely branching processes are strongly bisimilar if and only if they satisfy the same formulae of $\mathcal{L}$.

Definition 6 *Satisfaction of a formula ϕ of $\mathcal{T}$ is* preserved *by a morphism $\langle f, F\rangle : \langle M, N\rangle \longrightarrow \langle M', N'\rangle$ of $\mathbf{MNet}^+$ if, for any interpretation θ of $\mathcal{T}$ in $\langle M, N\rangle$,*

$$\textit{if } \langle M, N\rangle \models_\theta \phi \textit{ then } \langle M', N'\rangle \models_{f\theta} \phi.$$

Satisfaction of ϕ is reflected *by $\langle f, F\rangle$ if ,for any interpretation θ,*

$$\textit{if } \langle M', N'\rangle \models_{f\theta} \phi \textit{ then } \langle M, N\rangle \models_\theta \phi.$$

We omit mention of the morphism $\langle f, F\rangle$ where a result holds for any morphism in $\mathbf{MNet}^+$, for example, if any morphism preserves ϕ then we say that ϕ is preserved.

Proposition 6 *If ϕ is a formula of $\mathcal{L}$ containing no instance of $[t]$ then ϕ is preserved.*

Proof: We use induction on the structure of ϕ. The base cases are trivial since every marked net satisfies the formula tt and none satisfies ff. The cases of conjunction and disjunction are straightforward: for example, if $\langle M_0, N\rangle \models_\theta \phi_0 \vee \phi_1$ then $\langle M_0, N\rangle \models_\theta \phi_i$ for $i = 0$ or $i = 1$, by definition. By inductive hypothesis, $\langle M_0', N'\rangle \models_\theta \phi_i$ and hence $\langle M_0', N'\rangle \models_\theta \phi_0 \vee \phi_1$.

Now suppose that $\langle M_0, N\rangle \models_\theta \langle t\rangle\phi$. There exists M_1 such that $M_0 \xrightarrow{\theta(t)} M_1$ and $\langle M_1, N\rangle \models_\theta \phi$. But $\langle f, F\rangle$ is a morphism from $\langle M_0, N\rangle$ to $\langle M_0', N'\rangle$ in $\mathbf{MNet}^+$, so $M_0' \xrightarrow{f(\theta(t))} M_1'$ and since (using Proposition 2), $\langle f, F\rangle$ is also a morphism in $\mathbf{MNet}^+$ from $\langle M_1, N\rangle$ to $\langle M_1', N'\rangle$, by inductive hypothesis, $\langle M_1', N'\rangle \models_{f\theta} \phi$. Hence $\langle M_0', N'\rangle \models_{f\theta} \langle t\rangle\phi$, by definition. □

Note that $[t]\phi$ is not preserved: for the net N of Section 3, we have $\langle id, id\rangle : \langle\emptyset, N\rangle \rightarrow \langle 2b_0, N\rangle$ in $\mathbf{MNet}^+$. If $\theta(\alpha) = e_0$ then $\langle\emptyset, N\rangle \models_\theta [\alpha]E(\alpha)$ (since e_0 is not enabled), but $\langle 2b_0, N\rangle \not\models_\theta [\alpha]E(\alpha)$.

Proposition 7 *If ϕ is a formula of $\mathcal{L}$ containing no instance of $\langle t\rangle$ then ϕ is reflected.*

Proof: Again, we use induction on the structure of ϕ. The interesting case is when $\langle M_0', N'\rangle \models_{f\theta} [t]\phi$. Whenever $M_0 \xrightarrow{\theta(t)} M_1$ in N, we know that $M_0' \xrightarrow{f(\theta(t))} M_1'$ in N', and so $\langle M_1', N'\rangle \models_{f\theta} \phi$, by assumption. Now $\langle f, F\rangle : \langle M_1, N\rangle \longrightarrow \langle M_1', N'\rangle$ in $\mathbf{MNet}^+$, and so, by inductive hypothesis, $\langle M_1, N\rangle \models_\theta \phi$. Hence, by definition, $\langle M_0, N\rangle \models_\theta [t]\phi$. □

The above results state that certain safety properties expressible as formulae of $\mathcal{L}$ are preserved by morphisms in $\mathbf{MNet}^+$, while certain liveness properties are reflected. It is important to note that we code up the change of interpretation by replacing θ by $f\theta$. Since the formula ϕ does not change, a single test net satisfying ϕ witnesses the fact that both $\langle M, N\rangle$ and $\langle M', N'\rangle$ satisfy the property described by ϕ. We now generalise these results to our temporal language $\mathcal{T}$.

Definition 8 *Let $\langle f, F\rangle : \langle M, N\rangle \rightarrow \langle M', N'\rangle$ be a morphism in $\mathbf{MNet}^+$. We say that ϕ-*computations are preserved by* $\langle f, F\rangle$ iff*

$$\textit{if } \sigma \in [\![\phi]\!]_\theta \textit{ then } f\sigma \in [\![\phi]\!]_{f\theta}.$$

*We say that ϕ-*computations are reflected by* $\langle f, F\rangle$ iff*

$$\textit{if } f\sigma \in [\![\phi]\!]_{f\theta} \textit{ then } \sigma \in [\![\phi]\!]_\theta.$$

Thus $\langle f, F\rangle$ preserves ϕ-computations iff $f[\![\phi]\!]_\theta \subseteq [\![\phi]\!]_{f\theta}$ and $\langle f, F\rangle$ reflects ϕ-computations iff $f^{-1}[\![\phi]\!]_{f\theta} \subseteq [\![\phi]\!]_\theta$. In this paper we consider preservation and reflection at three levels, illustrated by the cases where

(1) a morphism $\langle f, F\rangle$ preserves (or reflects) ϕ-computations,

(2) a morphism $\langle f, F\rangle$ preserves (or reflects) satisfaction of ϕ and

(3) any morphism of $\mathbf{MNet}^+$ preserves (or reflects) ϕ-computations or ϕ.

In general, we prove results at levels (1) and (2) for an arbitrary morphism $\langle f, F\rangle$, which enables us to deduce that the results hold at level (3). Results at level (2) are weaker than those at level (1). Propositions 9, 10 and 13 below relate the different notions of preservation and reflection.

Proposition 9 *ϕ-computations are reflected iff $\neg\phi$ computations are preserved.*

Proof: Suppose ϕ-computations are preserved and $\langle f, F\rangle$ is a morphism with $f\sigma \in [\![\neg\phi]\!]_{f\theta}$. Then $f\sigma \notin [\![\phi]\!]_{f\theta}$ and, since ϕ-computations are preserved, $\sigma \notin [\![\phi]\!]_\theta$. Thus $\neg\phi$-computations are reflected.

Now suppose that ϕ-computations are reflected and that $\sigma \in [\![\neg\phi]\!]_\theta$. Then $\sigma \notin [\![\phi]\!]_\theta$ and, since ϕ-computations are reflected, $\sigma \notin [\![\phi]\!]_{f\theta}$. Thus $\neg\phi$-computations are preserved. □

In the propositions which follow, it is to be understood that $\langle f, F\rangle : \langle M, N\rangle \longrightarrow \langle M', N'\rangle$.

Proposition 10 *If $\langle f, F\rangle$ reflects ϕ-computations then $\langle f, F\rangle$ reflects ϕ.*

Proof: If $\langle M', N'\rangle \models_{f\theta} \phi$ and σ' is a step sequence of $\langle M', N'\rangle$ then $\sigma' \in [\![\phi]\!]_{f\theta}$. In particular, for every step sequence σ of $\langle M, N\rangle$, $f\sigma \in [\![\phi]\!]_{f\theta}$. Since $\langle f, F\rangle$ reflects ϕ-computations, $\sigma \in [\![\phi]\!]_\theta$ for every step sequence σ of $\langle M, N\rangle$, and so $\langle M, N\rangle \models_\theta \phi$. □

Note that it is not the case that if ϕ-computations are preserved by $\langle f, F\rangle$ then ϕ is preserved by $\langle f, F\rangle$, as $\langle M', N'\rangle$ may enable step sequences which are not in the image of f. We therefore introduce the following slightly weaker notion of preservation of a formula ϕ and ϕ-computations:

Definition 11 *Let $\langle f, F\rangle : \langle M, N\rangle \rightarrow \langle M', N'\rangle$ in $\mathbf{MNet}^+$. We say that $\langle f, F\rangle$ is* minimal *if every step sequence of $\langle M', N'\rangle$ is the image under f of some step sequence of $\langle M, N\rangle$, that is, if $C^{M'}_{N'} \subseteq f(C^M_N)$.*

Definition 12 *A formula ϕ of $\mathcal{T}$ is* minimally preserved *if any minimal morphism $\langle f, F\rangle : \langle M, N\rangle \rightarrow \langle M', N'\rangle$ in $\mathbf{MNet}^+$ preserves ϕ. Similarly, ϕ is* minimally reflected *if any minimal morphism $\langle f, F\rangle$ reflects ϕ.*

Although the definition of a minimal morphism may appear restrictive, in practice it is a natural property to require of an efficient test net, expressing the fact that the test net should contain no redundant behaviour. Note that a morphism $\langle f, F\rangle : \langle M, N\rangle \longrightarrow \langle M', N'\rangle$ is minimal if every event $e' \in E'$ is the image of some event in E. It is evident that if ϕ is preserved (reflected) then ϕ is minimally preserved (reflected).

Proposition 13 *If $\langle f, F\rangle$ preserves ϕ-computations and is minimal then $\langle f, F\rangle$ preserves ϕ.*

Proof: If $\langle M, N\rangle \models_\theta \phi$ then $C^M_N \subseteq [\![\phi]\!]_\theta$. Since $\langle f, F\rangle$ preserves ϕ-computations, $f(C^M_N) \subseteq [\![\phi]\!]_{f\theta}$. Since f is minimal, $C^{M'}_{N'} \subseteq fC^M_N$ and so $\langle M', N'\rangle \models_{f\theta} \phi$. □

Corollary 14 *If ϕ-computations are preserved by every minimal morphism of $\mathbf{MNet}^+$ then ϕ is minimally preserved.* □

We shall show that the preservation and reflection properties of various compound formulae are determined by the preservation and reflection properties of their component formulae. The following lemma, together with Lemmas 21 and 23, provides a starting point for the inductive definition of the set of formulae whose preservation and reflection properties we can readily establish.

Lemma 15 *$\mathtt{tt}$-computations are preserved and reflected, while $\mathtt{tt}$ is preserved and reflected.*
$E(t)$-computations are preserved and $E(t)$ is preserved. Furthermore, $\neg E(t)$ is reflected.

Proof: Preservation and reflection of $\mathtt{tt}$ are immediate. Now suppose $\langle f, F\rangle : \langle M, N\rangle \rightarrow \langle M', N'\rangle$ in $\mathbf{MNet}^+$. Then

$$\begin{aligned} f([\![\mathtt{tt}]\!]_\theta) &= f(C^M_N) \\ &\subseteq C^{M'}_{N'} \qquad \text{by Proposition 2} \\ &= [\![\mathtt{tt}]\!]_{f\theta} \end{aligned}$$

and thus $\mathtt{tt}$-computations are preserved. Similarly, $\mathtt{tt}$-computations are reflected since $f^{-1}(C^{M'}_{N'}) \subseteq C^M_N$.
In the case of preservation of $E(t)$ and reflection of $\neg E(t)$ we appeal to Proposition 2. □

We extend the notion of preservation and reflection of ϕ-computations to open formulae in the usual way: thus for example, $\forall x.\phi$-computations are preserved by $\langle f, F\rangle$ if for every $\alpha \in dom(\theta)$ it is the case that $\langle f, F\rangle$ preserves $\phi[\alpha/x]$-computations.

Proposition 16 *If $\langle f, F\rangle$ preserves ϕ- and ψ-computations then $\langle f, F\rangle$ preserves*

- *$\phi \wedge \psi$-computations and*
- *$\forall x.\phi$-computations.*

Proof:

- Suppose $\sigma \in [\![\phi \wedge \psi]\!]_\theta = [\![\phi]\!]_\theta \cap [\![\psi]\!]_\theta$. Then $\sigma \in [\![\phi]\!]_\theta$ and $\sigma \in [\![\psi]\!]_\theta$ and since $\langle f, F\rangle$ preserves both ϕ- and ψ-computations, $f\sigma \in [\![\phi]\!]_{f\theta}$ and $f\sigma \in [\![\psi]\!]_{f\theta}$, whence $f\sigma \in [\![\phi \wedge \psi]\!]_{f\theta}$. Hence $f[\![\phi \wedge \psi]\!]_\theta \subseteq [\![\phi \wedge \psi]\!]_{f\theta}$ and $\langle f, F\rangle$ preserves $\phi \wedge \psi$-computations.

- Suppose $\sigma \in \llbracket \forall x.\phi \rrbracket_\theta$. Then for each $\alpha \in dom(\theta)$ we have $\sigma \in \llbracket \phi[\alpha/x] \rrbracket_\theta$ and, since $dom(f\theta) = dom(\theta)$ and ϕ-computations are preserved, $f\sigma \in \llbracket \phi[\alpha/x] \rrbracket_{f\theta}$ for each $\alpha \in dom(f\theta)$. Hence $f\sigma \in \llbracket \forall x.\phi \rrbracket_{f\theta}$ and $\forall x.\phi$-computations are preserved.

□

Proposition 17 *If $\langle f, F\rangle$ reflects ϕ- and ψ-computations then $\langle f, F\rangle$ reflects*

– *$\phi \wedge \psi$-computations,*
– *$[t]\phi$-computations,*
– *$\Box\phi$-computations and*
– *$\forall x.\phi$-computations.*

Proof:

- Suppose $f\sigma \in \llbracket \phi \wedge \psi \rrbracket_{f\theta} = \llbracket \phi \rrbracket_{f\theta} \cap \llbracket \psi \rrbracket_{f\theta}$. Then $f\sigma \in \llbracket \phi \rrbracket_{f\theta}$ and $f\sigma \in \llbracket \psi \rrbracket_{f\theta}$ and since both ϕ- and ψ-computations are reflected, $\sigma \in \llbracket \phi \rrbracket_\theta$ and $\sigma \in \llbracket \psi \rrbracket_\theta$, whence $\sigma \in \llbracket \phi \wedge \psi \rrbracket_\theta$. Thus $f^{-1}(\llbracket \phi \wedge \psi \rrbracket_{f\theta}) \subseteq \llbracket \phi \wedge \psi \rrbracket_\theta$ and $\langle f, F\rangle$ reflects $\phi \wedge \psi$-computations.
- Suppose $f\sigma \in \llbracket [t]\phi \rrbracket_{f\theta}$ and $\sigma_0 ; \sigma_1 \ldots \sigma_k = \theta(t)$. Then putting $\sigma' = f\sigma$ we can find l such that $f(\sigma_0 ; \sigma_1 \ldots \sigma_k) = \sigma'_0 ; \sigma'_1 ; \ldots \sigma'_l = f\theta(t)$ and $f(\overline{\sigma}_{k+1}) = \overline{\sigma}'_{l+1}$. Since $\sigma' = f\sigma \in \llbracket [t]\phi \rrbracket_{f\theta}$ we have $\overline{\sigma}'_{l+1} \in \llbracket \phi \rrbracket_{f\theta}$. Since ϕ-computations are reflected, $\overline{\sigma}_{k+1} \in f^{-1}(\overline{\sigma}'_{l+1}) \subseteq \llbracket \phi \rrbracket_\theta$. Hence $\sigma \in \llbracket [t]\phi \rrbracket_\theta$ and $\langle f, F\rangle$ reflects $[t]\phi$-computations.
- Suppose $\sigma' = f\sigma \in \llbracket \Box\phi \rrbracket_{f\theta}$. Now for each k we can find l such that $f(\overline{\sigma}_k) = \overline{\sigma}'_l$ and so $f(\overline{\sigma}_k) \in \llbracket \phi \rrbracket_{f\theta}$. But ϕ-computations are reflected and so $\overline{\sigma}_k \in \llbracket \phi \rrbracket_\theta$. This holds for each k and so $\sigma \in \llbracket \Box\phi \rrbracket_\theta$ and $\Box\phi$-computations are reflected.
- Suppose $f\sigma \in \llbracket \forall x.\phi \rrbracket_{f\theta}$. Then for each $\alpha \in dom(f\theta)$, $f\sigma \in \llbracket \phi[\alpha/x] \rrbracket_{f\theta}$. Since ϕ-computations are reflected and $dom(\theta) = dom(f\theta)$, for each $\alpha \in dom(\theta)$, $\sigma \in \llbracket \phi[\alpha/x] \rrbracket_\theta$ and so $\sigma \in \llbracket \forall x.\phi \rrbracket_\theta$. Hence $f^{-1}\llbracket \forall x.\phi \rrbracket_{f\theta} \subseteq \llbracket \forall x.\phi \rrbracket_\theta$ as required.

□

Corollary 18 *If $\langle f, F\rangle$ preserves ϕ- and ψ-computations then $\langle f, F\rangle$ preserves*

– *$\phi \vee \psi$-computations,*
– *$\langle t\rangle\phi$-computations,*
– *$\Diamond\phi$-computations and*
– *$\exists x.\phi$-computations.*

If $\langle f, F\rangle$ reflects ϕ and ψ-computations then $\langle f, F\rangle$ reflects

– *$\phi \vee \psi$-computations and*
– *$\exists x.\phi$-computations.*

Proof: By Proposition 9, $\langle f, F\rangle$ reflects $\neg\phi$- and $\neg\psi$-computations, and so by Proposition 17, $\langle f, F\rangle$ reflects $(\neg\phi) \wedge (\neg\psi)$-computations. Hence $\langle f, F\rangle$ reflects $\neg(\phi \vee \psi)$-computations. By Proposition 9, $\langle f, F\rangle$ preserves $\phi \vee \psi$-computations.

The other cases are proved analogously. □

Lemma 19
If $\langle f, F\rangle$ preserves ϕ-computations and f is injective then $\langle f, F\rangle$ preserves $[t]\phi$-computations.
If $\langle f, F\rangle$ is minimal and preserves ϕ-computations then $\langle f, F\rangle$ preserves $[t]\phi$.

Proof: Suppose $\langle f, F\rangle : \langle M, N\rangle \longrightarrow \langle M', N'\rangle$ and $\sigma \in \llbracket [t]\phi \rrbracket_\theta$. If $\sigma_0 ; \ldots \sigma_k = \theta t$ it follows that $\overline{\sigma}_{k+1} \in \llbracket \phi \rrbracket_{f\theta}$. Now suppose that $f\sigma_0 ; \ldots f\sigma_k = f\theta t$. Since f is injective, $\sigma_0 ; \ldots \sigma_k = \theta t$ and so $\overline{\sigma}_{k+1} \in \llbracket \phi \rrbracket_\theta$ and, since $\langle f, F\rangle$ preserves ϕ-computations, $f(\overline{\sigma}_{k+1}) \in \llbracket \phi \rrbracket_{f\theta}$. Hence $f\sigma \in \llbracket [t]\phi \rrbracket_{f\theta}$.

Suppose now that $\langle f, F\rangle : \langle M, N\rangle \longrightarrow \langle M', N'\rangle$ is minimal and preserves ϕ-computations, and that $\langle M, N\rangle \models_\theta [t]\phi$. Suppose $\sigma'_0 ; \ldots \sigma'_l = f\theta t$. It suffices to show that $\overline{\sigma}'_{l+1} \in \llbracket \phi \rrbracket_{f\theta}$. By minimality, $\sigma' = f\sigma$ for some $\sigma \in C_N^M$. Hence for some k, $f\sigma_0 ; \ldots \sigma_k = f\theta t$. It follows that $\sigma' = (f\theta t) ; f\overline{\sigma}_{k+1}$. Now $(\theta t) ; \overline{\sigma}_{k+1} \in C_N^M \subseteq \llbracket [t]\phi \rrbracket_\theta$, and so $\overline{\sigma}_{k+1} \in \llbracket \phi \rrbracket_\theta$. Since $\langle f, F\rangle$ preserves ϕ-computations, $f(\overline{\sigma}_{k+1}) \in \llbracket \phi \rrbracket_{f\theta}$ and so $\overline{\sigma}'_{l+1} \in \llbracket \phi \rrbracket_{f\theta}$, as required. □

Corollary 20
If $\langle f, F\rangle$ reflects ϕ-computations and f is injective then $\langle f, F\rangle$ reflects $\langle t\rangle\phi$-computations.
If ϕ is minimally preserved then $[t]\phi$ is minimally preserved.
If ϕ is minimally reflected then $\langle t\rangle\phi$ is minimally reflected.

□

Example 1 *The following formulae are preserved:*

$E(t)$	*$\theta(t)$ is enabled*
$\exists x.E(x)$	*some $\theta(\alpha)$ is enabled*
$E(t) \vee E(t')$	*either $\theta(t)$ or $\theta(t')$ is enabled.*

The following formulae are reflected:

$\neg E(t)$	*$\theta(t)$ is not enabled*
$\Diamond\neg E(t)$	*eventually $\theta(t)$ is disabled*
$\Box\neg E(t)$	*$\theta(t)$ is never enabled*
$\forall x.\neg E(x)$	*no $\theta(\alpha)$ is enabled (relative deadlock).*
$\Box\Diamond\neg E(t)$	*a marking is always reachable in which $\theta(t)$ is disabled.*

The following formulae are minimally preserved:

$\Diamond E(t)$	*$\theta(t)$ is eventually enabled*
$\Diamond\neg E(t)$	*$\theta(t)$ is eventually disabled*
$\neg E(t)$	*$\theta(t)$ is not enabled*
$\Diamond\exists x.E(x)$	*eventually some $\theta(\alpha)$ is enabled*
$\forall x.\neg E(x)$	*no $\theta(\alpha)$ is enabled (relative deadlock)*
$\Box\exists x.E(x)$	*some $\theta(t)$ is always enabled.*

The following formulae are minimally reflected:

$E(t)$	*$\theta(t)$ is enabled*
$\exists x.E(x)$	*some $\theta(\alpha)$ is enabled*
$\Box\exists x.E(x)$	*some $\theta(t)$ is always enabled.*

There are many more examples of formulae whose properties we can deduce from the results presented above. A selection is given in Example 2.

A common situation is illustrated by the following lemma:

Lemma 21 *Let I index the set $\{t_i \mid f\theta(t_i) = f\theta(t)$. If $f\sigma \in [\![E(t)]\!]_{f\theta}$ then $\sigma \in \bigcup_{i \in I} [\![E(t_i)]\!]_{\theta}$ and whenever $\langle M', N' \rangle \models_{f\theta} E(t)$ it is the case that $\langle M, N \rangle \models_{\theta} \bigvee_I E(t_i)$.*

Proof: Straightforward $\Box$

Remark 22 *It is an immediate consequence of the previous lemma that if $f\theta t = f\theta t'$ implies that $\theta t = \theta t'$ (and in particular, if f is injective) then $E(t)$-computations are minimally reflected and so $E(t)$ is minimally reflected.*

It is not in general the case that $\Box\phi$ is preserved or that $\Box\phi$-computations are preserved, even by a minimal morphism. For example, returning to the net N illustrated at the start of Section 3, the identity morphism $\langle id, id \rangle$ maps $\langle b_0, N \rangle$ to $\langle 2b_0, N \rangle$ but $\langle b_0, N \rangle \models_{\theta} \Box\neg E(\alpha_0)$ and $\langle 2b_0, N \rangle \not\models_{\mathrm{id}\theta} \Box\neg E(\alpha_0)$. The following lemma establishes a special case in which we can infer properties of a formula $\Box\phi$ from properties of ϕ.

Lemma 23
$\Box\Diamond E(t)$-computations are preserved and $\Box\Diamond E(t)$ is minimally preserved. If $f\theta(t) = f\theta(t')$ implies that $\theta(t) = \theta(t')$ and $\langle f, F \rangle$ is minimal then $\langle f, F \rangle$ reflects $\Box\Diamond E(t)$-computations.

Proof: Suppose $\sigma \in [\![\Box\Diamond E(t)]\!]_{\theta}$. Then for every i there exists j such that $\overline{\sigma}_{i+j} \in [\![E(t)]\!]_{\theta}$. Suppose that $f\sigma \notin [\![\Box\Diamond E(t)]\!]_{f\theta}$. Then there exists some k such that for all l, $\overline{f\sigma}_{k+l} \notin [\![E(t)]\!]_{f\theta}$. It follows that there exists $m \geq k$ such that for all l, $f(\overline{\sigma}_{m+l}) \notin [\![E(t)]\!]_{f\theta}$. Since $E(t)$-computations are preserved, this would imply that we could find some m such that for all l, $\overline{\sigma}_{m+l} \notin [\![E(t)]\!]_{\theta}$, which contradicts our assumption that $\sigma \in [\![\Box\Diamond E(t)]\!]_{\theta}$. Hence $f\sigma \in [\![E(t)]\!]_{f\theta}$.

It follows that $\Box\Diamond E(t)$ is minimally preserved, by Proposition 13.

We now show that $\Box\Diamond E(t)$-computations are minimally reflected. Suppose $f\sigma \in [\![\Box\Diamond E(t)]\!]_{f\theta}$. Then for all i there exists j such that $\overline{f\sigma}_{i+j} \in [\![E(t)]\!]_{f\theta}$. It follows that for all i there exists $k \geq j$ such that $f(\overline{\sigma}_{i+k}) \in [\![E(t)]\!]_{f\theta}$. Since $\langle f, F \rangle$ is minimal, it follows from the proof of Lemma 21 that $\langle f, F \rangle$ reflects $E(t)$. Hence for all i there exists k such that $\overline{\sigma}_{i+k} \in [\![E(t)]\!]_{\theta}$.

$\Box$

Remark 24 *Observe that the proof above still goes through if we replace $E(t)$ by any formula ϕ which is preserved and minimally reflected. We can prove the usual dual results for formulae of the form $\Diamond\Box\phi$.*

If we extend $\mathcal{T}$ with arbitrary disjunctions then we can prove the following proposition:

Proposition 25 *If $\langle f, F \rangle$: $\langle M, N \rangle \rightarrow \langle M', N' \rangle$ is minimal and I indexes $\{t_i \mid f\theta(t_i) = f\theta(t)\}$, then*

if $\langle M', N' \rangle \models_{f\theta} \Box E(t)$ then $\langle M, N \rangle \models_{\theta} \Box \bigvee_I E(t_i)$,

if $\langle M', N' \rangle \models_{f\theta} \Box\Diamond E(t)$ then $\langle M, N \rangle \models_{\theta} \Box\Diamond \bigvee E(t_i)$ and

if $\langle M', N' \rangle \models_{f\theta} \Diamond E(t)$ then $\langle M, N \rangle \models_{\theta} \Diamond \bigvee E(t_i)$.

Proof: Suppose for example that $\langle M', N'\rangle \models_{f\theta} \Box E(t)$. We show that $\langle M, N\rangle \models_\theta \Box\bigvee_I E(t_i)$. In every computation of $\langle M', N'\rangle$ the computation $\theta(t)$ is continuously enabled. By minimality, in every computation of $\langle M, N\rangle$, there is always a computation enabled whose image under f equals $f(\theta t)$. Let I index the set $\{t_i \mid f\theta(t_i) = f\theta(t)\}$. Then $\langle M, N\rangle \models_\theta \Box\bigvee_I E(t_i)$. □

Note that, as in the case of Lemma 21, if $f\theta(t') = f\theta(t)$ implies that $t' = t$ and $\langle f, F\rangle : \langle M, N\rangle \longrightarrow \langle M', N'\rangle$ is minimal with $\langle M', N'\rangle \models_{f\theta} \Box E(t)$ then $\langle M, N\rangle \models_\theta \Box E(t)$.

Proposition 26 *If $\langle f, F\rangle$: $\langle M, N\rangle \to \langle M', N'\rangle$ is minimal and I indexes $\{t_i \mid f\theta(t_i) = f\theta(t)\}$, then*
if $\langle M, N\rangle \models_\theta \Box\Diamond\bigwedge_I \neg E(t_i)$ then $\langle M', N'\rangle \models_{f\theta} \Box\Diamond\neg E(t)$ and
if $\langle M, N\rangle \models_\theta \Diamond\bigwedge_I \neg E(t_i)$ then $\langle M', N'\rangle \models_{f\theta} \Diamond\neg E(t)$.

Proof: Analogous to that of Proposition 25 □

The results of this section together with the proof rules for temporal and modal logic determine a relatively large and expressive class of formulae which are either preserved or reflected by morphisms in $\mathbf{MNet}^+$. These formulae occur at all levels of Manna and Pnueli's hierarchy [7, 8].

Example 2 *The state formulae of $\mathcal{T}$ are those given by $\mathtt{tt} \mid E(t) \mid \phi \wedge \phi \mid \neg\phi$. If ϕ and ψ are state formulae then:*

- *$\Box\phi$ describes a safety property. Many such formulae, including mutual exclusion $\Box\neg E(t_0 + t_1))$, are reflected.*
- *$\Diamond\phi$ describes a termination property, guaranteeing a one-time goal. An example is $\Diamond E(\alpha)$, which is both minimally preserved and minimally reflected.*
- *$\Box\Diamond\phi$ describes a recurrence property or response property. An example is $\Box(E(t_0) \to \Diamond E(t_1))$, which is minimally preserved and minimally reflected.*
- *$\Diamond\Box\phi$ describes a persistence property. As an example, $\Diamond\Box E(t)$ is minimally reflected.*
- *$\Diamond\Box\phi \vee \Box\Diamond\psi$ describes a progress property. An example is $\Box(\Box\Diamond E(t_0) \to \Box\Diamond E(t_1))$ (strong fairness) which is minimally preserved, and furthermore is reflected by minimal morphisms $\langle f, F\rangle$ such that f is injective.*

5.1 *Proving Properties of Nets*

We now outline the formal proofs that the net $\langle M_1 + M_2 + S, N_1\rangle$ of Section 3.2 preserves mutual exclusion and satisfies absence of starvation. These proofs follow our previous reasoning closely. For absence of starvation, we shall assume an invertible interpretation θ in $\langle m_1 + m_2 + s, N_3\rangle$ with inverse η. The fact that s is marked infinitely often is expressed as $\langle m_1 + m_2 + s, N_3\rangle \models_\theta \Box\Diamond E(\eta\, id_s)$. The fact that if q_1 is marked and cr_1 never occurs then q_1 remains marked is expressed as $\langle m_1 + m_2 + s, N_3\rangle \models_\theta (E(\eta\, id_{q_1}) \wedge \neg\Diamond E(\eta\, cr_1)) \to \Box E(\eta\, id_{q_1})$, and similarly for q_2. The assumption of strong fairness implies that $\langle m_1 + m_2 + s, N_3\rangle \models_\theta \Box\Diamond E(\eta\, req_i) \to \Box\Diamond E(\eta\, cr_i)$. We deduce that $\langle m_1 + m_2 + s, N_3\rangle \models_\theta E(\eta\, req_i) \to \Diamond E(\eta\, ncr_i)$ by applying the proof rules of temporal logic. Thus $\langle m_1 + m_2 + s, N_3\rangle$ satisfies absence of starvation. By minimality and injectivity of g, satisfaction of $\neg E(\alpha)$ is preserved and satisfaction of $\Diamond E(\alpha)$ is preserved. Hence satisfaction of $(E(\eta\, req_i) \to \Diamond E(\eta\, ncr_i)) \equiv (\neg E(\eta\, req_i) \vee \Diamond E(\eta\, ncr_i))$ is preserved and the net $\langle M_1 + M_2 + S, N_1\rangle$ satisfies absence of starvation.

For mutual exclusion, putting $\theta(\alpha) = Out_1 + Out_2$ and $\theta(\beta) = Cr_1 + Cr_2$ we have $\langle C, N_2\rangle \models_{f\theta} \Box\neg E(\alpha)$. By Propositions 15 and 17, $\langle S + M_1 + M_2, N_1\rangle \models_\theta \Box\neg E(\alpha)$. Now if $\langle S + M_1 + M_2, N_1\rangle$ were to fire Cr_1 and Cr_2 simultaneously, $Out_1 + Out_2$ would become enabled: that is, $\langle S + M_1 + M_2, N_1\rangle \models_\theta [\beta]E(\alpha)$. We deduce that $\langle S + M_1 + M_2, N_1\rangle$ can never enable $\theta(\beta)$, that is, $\langle S + M_1 + M_2, N_1\rangle$ never enables Cr_1 and Cr_2 simultaneously. Thus entry to the critical regions Cr_1 and Cr_2 is mutually exclusive.

6 Future Work

This paper sketches an approach and presents some preliminary results concerning the applicability of that approach. It remains to establish a suitable proof system for our logic and to consider a logical characterisation of the simulation preorder. An important aspect of future research is the use of structure in our category to modularise proofs. $\mathbf{MNet}^+$ has coproducts (representing choice) and products of a kind (representing parallel composition of processes). There is certainly a relationship between the formulae satisfied by a compound net and the formulae satisfied by its components, which we would like to make precise (compare [15]). Future work will consider the use of relations rather than functions, thus approaching still more closely the simulations of process algebra [10, 12].

References

[1] H. R. Andersen and G. Winskel. Compositional checking of satisfaction. In K. G. Larsen and A. Skou, editors, *Proceedings of the 3rd Workshop on Computer Aided Verification, July 1991, Aalborg*, volume 575 of *LNCS*, 1992.

[2] C. T. Brown. *Linear Logic and Petri Nets: Categories, Algebra and Proof.* PhD thesis, University of Edinburgh, 1990. Technical Report ECS-LFCS-91-128.

[3] C. T. Brown and D. J. Gurr. Refinement and simulation of nets – a categorical characterisation. In K. Jensen, editor, *Proc. 13th International Conference on Applications and Theory of Petri Nets*. Springer–Verlag, 1992. LNCS 616.

[4] C. T. Brown and D. J. Gurr. Timing petri nets categorically. In W. Kuich, editor, *Proc. ICALP*. Springer–Verlag, 1992. LNCS 623.

[5] C. T. Brown, D. J. Gurr, and V. C. V. de Paiva. A linear specification language for petri nets. Technical Report DAIMI PB – 363, DAIMI, Århus University, 1991. to appear in Mathematical Structures in Computer Science.

[6] D. Kozen. Results on the propositional μ-calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[7] Z. Manna and A. Pnueli. The anchored version of the temporal framework. In J.W. de Bakker, W.-P. de Roever, and G. Rozenberg, editors, *Proc. Workshop on Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency*, pages 201–284. LNCS 354, 1988.

[8] Z. Manna and A. Pnueli. A hierarchy of temporal properties. In *Proc. ACM Symposium on Principles of Distributed Computing, Quebec*, 1990.

[9] J. Meseguer and U. Montanari. Petri nets are monoids: A new algebraic foundation for net theory. In *Proc LICS*, 1988.

[10] R. Milner. *Communication and Concurrency*. Prentice Hall, 1989.

[11] E. R. Olderog. *Nets, terms and Formulas*. CUP, 1991.

[12] D. M. R. Park. Concurrency and automata on infinite sequences. 1980. LNCS 104, Springer–Verlag.

[13] W. Reisig. *Petri Nets: an Introduction*. EATCS Monographs on Theoretical Computer Science, Springer–Verlag, 1985.

[14] W. Reisig. Towards a temporal logic for causality and choice in distributed systems. In J.W. de Bakker, W.-P. de Roever, and G. Rozenberg, editors, *Proc. Workshop on Linear Time, Branching Time and Partial Order in Logics and Models for Concurrency*, pages 603–627. LNCS 354, 1988.

[15] G. Winskel. A category of labelled petri nets and compositional proof system. In *Proc LICS*, 1988.