Technische Universität Braunschweig

Institut für Programmierung
und Reaktive Systeme

Informatik Bericht Nr. 2011-10

On Distributability of Petri Nets

On Distributability of Petri Nets[*]

Rob van Glabbeek
NICTA, Sydney, Australia
School of Computer Science and Engineering
Univ. of New South Wales, Sydney, Australia
rvg@cs.stanford.edu

Ursula Goltz   Jens-Wolfhard Schicke-Uffmann
Institute for Programming and Reactive Systems
TU Braunschweig, Germany
goltz@ips.cs.tu-bs.de   drahflow@gmx.de

We formalise a general concept of distributed systems as sequential components interacting asynchronously. We define a corresponding class of Petri nets, called LSGA nets, and precisely characterise those system specifications which can be implemented as LSGA nets up to branching ST-bisimilarity with explicit divergence.

1 Introduction

The aim of this paper is to contribute to a fundamental understanding of the concept of a distributed reactive system and the paradigms of synchronous and asynchronous interaction. We start by giving an intuitive characterisation of the basic features of distributed systems. In particular we assume that distributed systems consist of components that reside on different locations, and that any signal from one component to another takes time to travel. Hence the only interaction mechanism between components is asynchronous communication.

Our aim is to characterise which system specifications may be implemented as distributed systems. In many formalisms for system specification or design, synchronous communication is provided as a basic notion; this happens for example in process algebras. Hence a particular challenge is that it may be necessary to simulate synchronous communication by asynchronous communication.

Trivially, any system specification may be implemented distributedly by locating the whole system on one single component. Hence we need to pose some additional requirements. One option would be to specify locations for system activities and then to ask for implementations satisfying this distribution and still preserving the behaviour of the original specification. This is done in [1]. Here we pursue a different approach. We add another requirement to our notion of a distributed system, namely that its components only allow sequential behaviour. We then ask whether an arbitrary system specification may be implemented as a distributed system consisting of sequential components in an optimal way, that is without restricting the concurrency of the original specification. This is a particular challenge when synchronous communication interacts with concurrency in the specification of the original system. We will give a precise characterisation of the class of distributable systems, which answers in particular under which conditions synchronous communication may be implemented in a distributed setting.

For our investigations we need a model which is expressive enough to represent concurrency. It is also useful to have an explicit representation of the distributed state space of a distributed system, showing in particular the local control states of components. We choose Petri nets, which offer these possibilities and additionally allow finite representations of infinite behaviours. We work within the class of *structural*

[*] This work was partially supported by the DFG (German Research Foundation).
An extended abstract of this paper appeared in L. Birkedal, ed.: Proc. 15th Int. Conf. on Foundations of Software Science and Computation Structures (FoSSaCS 2012), LNCS 7213, Springer, 2012, pp. 331–345, doi:10.1007/978-3-642-2872-9_22.

Technical Report 2011-10
Institut für Programmierung und Reaktive Systeme
Technical University of Braunschweig

conflict nets [7]—a proper generalisation of the class of one-safe place/transition systems, where conflict and concurrency are clearly separated.

For comparing the behaviour of systems with their distributed implementation we need a suitable equivalence notion. Since we think of open systems interacting with an environment, and since we do not want to restrict concurrency in applications, we need an equivalence that respects branching time and concurrency to some degree. Our implementations use transitions which are invisible to the environment, and this should be reflected in the equivalence by abstracting from such transitions. However, we do not want implementations to introduce divergence. In the light of these requirements we work with two semantic equivalences. *Step readiness equivalence* is one of the weakest equivalences that captures branching time, concurrency and divergence to some degree; whereas *branching ST-bisimilarity with explicit divergence* fully captures branching time, divergence, and those aspects of concurrency that can be represented by concurrent actions overlapping in time. We obtain the same characterisation for both notions of equivalence, and thus implicitly for all notions in between these extremes.

We model distributed systems consisting of sequential components as an appropriate class of Petri nets, called *LSGA nets*. These are obtained by composing nets with sequential behaviour by means of an asynchronous parallel composition. We show that this class corresponds exactly to a more abstract notion of distributed systems, formalised as *distributed nets* [6].

We then consider distributability of system specifications which are represented as structural conflict nets. A net N is *distributable* if there exists a distributed implementation of N, that is a distributed net which is semantically equivalent to N. In the implementation we allow unobservable transitions, and labellings of transitions, so that single actions of the original system may be implemented by multiple transitions. However, the system specifications for which we search distributed implementations are *plain* nets without these features.

We give a precise characterisation of distributable nets in terms of a semi-structural property. This characterisation provides a formal proof that the interplay between choice and synchronous communication is a key issue for distributability.

To establish the correctness of our characterisation we develop a new method for rigorously proving the equivalence of two Petri nets, one of which known to be plain, up to branching ST-bisimilarity with explicit divergence.

2 Basic Notions

In this paper we employ *signed multisets*, which generalise multisets by allowing elements to occur in it with a negative multiplicity.

Definition 1 Let X be a set.

- A *signed multiset* over X is a function $A\colon X \rightarrow \mathbb{Z}$, i.e. $A \in \mathbb{Z}^X$.
  It is a *multiset* iff $A \in \mathbb{N}^X$, i.e. iff $A(x) \geq 0$ for all $x \in X$.
- $x \in X$ is an *element of* a signed multiset $A \in \mathbb{N}^X$, notation $x \in A$, iff $A(x) \neq 0$.
- For signed multisets A and B over X we write $A \leq B$ iff $A(x) \leq B(x)$ for all $x \in X$;
  $A \cup B$ denotes the signed multiset over X with $(A \cup B)(x) := \max(A(x), B(x))$,
  $A \cap B$ denotes the signed multiset over X with $(A \cap B)(x) := \min(A(x), B(x))$,
  $A + B$ denotes the signed multiset over X with $(A + B)(x) := A(x) + B(x)$,
  $A - B$ denotes the signed multiset over X with $(A - B)(x) := A(x) - B(x)$, and
  for $k \in \mathbb{N}$ the signed multiset $k \cdot A$ is given by $(k \cdot A)(x) := k \cdot A(x)$.
- The function $\emptyset\colon X \rightarrow \mathbb{N}$, given by $\emptyset(x) := 0$ for all $x \in X$, is the *empty* multiset over X.

- If A is a signed multiset over X and $Y \subseteq X$ then $A \upharpoonright Y$ denotes the signed multiset over Y defined by $(A \upharpoonright Y)(x) := A(x)$ for all $x \in Y$.
- The cardinality $|A|$ of a signed multiset A over X is given by $|A| := \sum_{x \in X} |A(x)|$.
- A signed multiset A over X is *finite* iff $|A| < \infty$, i.e., iff the set $\{x \mid x \in A\}$ is finite.
  We write $A \in_f \mathbb{Z}^X$ or $A \in_f \mathbb{N}^X$ to indicate that A is a finite (signed) multiset over X.
- Any function $f : X \to \mathbb{Z}$ or $f : X \to \mathbb{Z}^Y$ from X to either the integers or the signed multisets over some set Y extends to the finite signed multisets A over X by $f(A) = \sum_{x \in X} A(x) \cdot f(x)$.

Two signed multisets $A\colon X \to \mathbb{Z}$ and $B\colon Y \to \mathbb{Z}$ are *extensionally equivalent* iff $A \upharpoonright (X \cap Y) = B \upharpoonright (X \cap Y)$, $A \upharpoonright (X \setminus Y) = \emptyset$, and $B \upharpoonright (Y \setminus X) = \emptyset$. In this paper we often do not distinguish extensionally equivalent signed multisets. This enables us, for instance, to use $A + B$ even when A and B have different underlying domains. A multiset A with $A(x) \in \{0,1\}$ for all x is identified with the set $\{x \mid A(x) = 1\}$. A signed multiset with elements x and y, having multiplicities -2 and 3, is denoted as $-2 \cdot \{x\} + 3 \cdot \{y\}$.

We consider here general labelled place/transition systems with arc weights. Arc weights are not necessary for the results of the paper, but are included for the sake of generality.

Definition 2 Let Act be a set of *visible actions* and $\tau \notin \text{Act}$ be an *invisible action*. Let $\text{Act}_\tau := \text{Act} \stackrel{\bullet}{\cup} \{\tau\}$. A (*labelled*) *Petri net* (*over* Act_τ) is a tuple $N = (S, T, F, M_0, \ell)$ where
- S and T are disjoint sets (of *places* and *transitions*),
- $F : (S \times T \cup T \times S) \to \mathbb{N}$ (the *flow relation* including *arc weights*),
- $M_0 : S \to \mathbb{N}$ (the *initial marking*), and
- $\ell : T \to \text{Act}_\tau$ (the *labelling function*).

Petri nets are depicted by drawing the places as circles and the transitions as boxes, containing their label. Identities of places and transitions are displayed next to the net element. When $F(x,y) > 0$ for $x,y \in S \cup T$ there is an arrow (*arc*) from x to y, labelled with the *arc weight* $F(x,y)$. Weights 1 are elided. When a Petri net represents a concurrent system, a global state of this system is given as a *marking*, a multiset M of places, depicted by placing $M(s)$ dots (*tokens*) in each place s. The initial state is M_0.

To compress the graphical notation, we also allow universal quantifiers of the form $\forall x.\phi(x)$ to appear in the drawing (cf. Figure 4). A quantifier replaces occurrences of x in element identities with all concrete values for which $\phi(x)$ holds, possibly creating a set of elements instead of the depicted single one. An arc of which only one end is replicated by a given quantifier results in a fan of arcs, one for each replicated element. If both ends of an arc are affected by the same quantifier, an arc is created between pairs of elements corresponding to the same x, but not between elements created due to differing values of x.

The behaviour of a Petri net is defined by the possible moves between markings M and M', which take place when a finite multiset G of transitions *fires*. In that case, each occurrence of a transition t in G consumes $F(s,t)$ tokens from each place s. Naturally, this can happen only if M makes all these tokens available in the first place. Next, each t produces $F(t,s)$ tokens in each s. Definition 4 formalises this notion of behaviour.

Definition 3 Let $N = (S, T, F, M_0, \ell)$ be a Petri net and $x \in S \cup T$.
The multisets ${}^\bullet x,\ x^\bullet : S \cup T \to \mathbb{N}$ are given by ${}^\bullet x(y) = F(y,x)$ and $x^\bullet(y) = F(x,y)$ for all $y \in S \cup T$. If $x \in T$, the elements of ${}^\bullet x$ and $x^\bullet$ are called *pre-* and *postplaces* of x, respectively, and if $x \in S$ we speak of *pre-* and *posttransitions*. The *token replacement function* $[\![\_]\!] : T \to \mathbb{Z}^S$ is given by $[\![t]\!] = t^\bullet - {}^\bullet t$ for all $t \in T$. These functions extend to finite signed multisets as usual (see Definition 1).

Definition 4 Let $N = (S, T, F, M_0, \ell)$ be a Petri net, $G \in \mathbb{N}^T$, G non-empty and finite, and $M, M' \in \mathbb{N}^S$.
G is a *step* from M to M', written $M\ [G\rangle_N\ M'$, iff

- ${}^\bullet G \leq M$ (G is *enabled*) and
- $M' = (M - {}^\bullet G) + G^\bullet = M + [\![G]\!]$.

Note that steps are (finite) multisets, thus allowing self-concurrency, i.e. the same transition can occur multiple times in a single step. We write $M\ [t\rangle_N\ M'$ for $M\ [\{t\}\rangle_N\ M'$, whereas $M[G\rangle_N$ abbreviates $\exists M'.\ M\ [G\rangle_N\ M'$. We may omit the subscript N if clear from context.

In our nets transitions are labelled with *actions* drawn from a set $\mathrm{Act} \overset{\bullet}{\cup} \{\tau\}$. This makes it possible to see these nets as models of *reactive systems* that interact with their environment. A transition t can be thought of as the occurrence of the action $\ell(t)$. If $\ell(t) \in \mathrm{Act}$, this occurrence can be observed and influenced by the environment, but if $\ell(t) = \tau$, it cannot and t is an *internal* or *silent* transition. Transitions whose occurrences cannot be distinguished by the environment carry the same label. In particular, since the environment cannot observe the occurrence of internal transitions at all, they are all labelled τ.

The labelling function ℓ extends to finite multisets of transitions $G \in \mathbb{Z}^T$ by $\ell(G) := \sum_{t \in T} G(t) \cdot \{\ell(t)\}$. For $A, B \in \mathbb{Z}^{\mathrm{Act}_\tau}$ we write $A \equiv B$ iff $\ell(A)(a) = \ell(B)(a)$ for all $a \in \mathrm{Act}$, i.e. iff A and B contain the same (numbers of) visible actions, allowing $\ell(A)(\tau) \neq \ell(B)(\tau)$. Hence $\ell(G) \equiv \emptyset$ indicates that $\ell(t) = \tau$ for all transitions $t \in T$ with $G(t) \neq 0$.

Definition 5 Let $N = (S, T, F, M_0, \ell)$ be a Petri net.

- The set $[M_0\rangle_N$ of *reachable markings of* N is defined as the smallest set containing M_0 that is closed under $[G\rangle_N$, meaning that if $M \in [M_0\rangle_N$ and $M\ [G\rangle_N\ M'$ then $M' \in [M_0\rangle_N$.
- N is *one-safe* iff $M \in [M_0\rangle_N \Rightarrow \forall s \in S.\ M(s) \leq 1$.
- The *concurrency relation* $\smile\ \subseteq T^2$ is given by $t \smile u \Leftrightarrow \exists M \in [M_0\rangle.\ M[\{t\}+\{u\}\rangle$.
- N is a *structural conflict net* iff for all $t, u \in T$ with $t \smile u$ we have ${}^\bullet t \cap {}^\bullet u = \emptyset$.

We use the term *plain nets* for Petri nets where ℓ is injective and no transition has the label τ, i.e. essentially unlabelled nets.

This paper first of all aims at studying finite Petri nets: nets with finitely many places and transitions. However, our work also applies to infinite nets with the properties that ${}^\bullet t \neq \emptyset$ for all transitions $t \in T$, and any reachable marking (a) is finite, and (b) enables only finitely many transitions. Henceforth, we call such nets *finitary*. Finitariness can be ensured by requiring $|M_0| < \infty \wedge \forall t \in T.\, {}^\bullet t \neq \emptyset \wedge \forall x \in S \cup T.\, |x^\bullet| < \infty$, i.e. that the initial marking is finite, no transition has an empty set of preplaces, and each place and transition has only finitely many outgoing arcs.

3 Semantic Equivalences

In this section, we give an overview on some semantic equivalences for reactive systems. Most of these may be defined formally for Petri nets in a uniform way, by first defining equivalences for transition systems and then associating different transition systems with a Petri net. This yields in particular different non-interleaving equivalences for Petri nets.

Definition 6 Let $\mathfrak{Act}$ be a set of *visible actions* and $\tau \notin \mathfrak{Act}$ be an *invisible action*. Let $\mathfrak{Act}_\tau := \mathfrak{Act} \overset{\bullet}{\cup} \{\tau\}$. A *labelled transition system* (LTS) (*over* $\mathfrak{Act}_\tau$) is a triple $\mathfrak{L} = (\mathfrak{S}, \mathfrak{T}, \mathfrak{M}_0)$ with

- $\mathfrak{S}$ a set of *states*,
- $\mathfrak{T} \subseteq \mathfrak{S} \times \mathfrak{Act}_\tau \times \mathfrak{S}$ a *transition relation*
- and $\mathfrak{M}_0 \in \mathfrak{S}$ the *initial state*.

Given an LTS $(\mathfrak{S}, \mathfrak{T}, \mathfrak{M}_0)$ with $\mathfrak{M}, \mathfrak{M}' \in \mathfrak{S}$ and $\alpha \in \mathfrak{Act}_\tau$, we write $\mathfrak{M} \xrightarrow{\alpha} \mathfrak{M}'$ for $(\mathfrak{M}, \alpha, \mathfrak{M}') \in \mathfrak{T}$. We write $\mathfrak{M} \xrightarrow{\alpha}$ for $\exists \mathfrak{M}'.\ \mathfrak{M} \xrightarrow{\alpha} \mathfrak{M}'$ and $\mathfrak{M} \not\xrightarrow{\alpha}$ for $\nexists \mathfrak{M}'.\ \mathfrak{M} \xrightarrow{\alpha} \mathfrak{M}'$. Furthermore, $\mathfrak{M} \xrightarrow{(\alpha)} \mathfrak{M}'$ denotes

$\mathfrak{M} \xrightarrow{\alpha} \mathfrak{M}' \vee (\alpha = \tau \wedge \mathfrak{M} = \mathfrak{M}')$, meaning that in case $\alpha = \tau$ performing a τ-transition is optional. For $a_1 a_2 \cdots a_n \in \mathfrak{Act}^*$ we write $\mathfrak{M} \xRightarrow{a_1 a_2 \cdots a_n} \mathfrak{M}'$ when

$$\mathfrak{M} \Longrightarrow\xrightarrow{a_1}\Longrightarrow\xrightarrow{a_2}\Longrightarrow \cdots \Longrightarrow\xrightarrow{a_n}\Longrightarrow \mathfrak{M}'$$

where $\Longrightarrow$ denotes the reflexive and transitive closure of $\xrightarrow{\tau}$. A state $\mathfrak{M} \in \mathfrak{S}$ is said to be *reachable* iff there is a $\sigma \in \mathfrak{Act}^*$ such that $\mathfrak{M}_\mathrm{o} \xRightarrow{\sigma} \mathfrak{M}$. The set of all reachable states is denoted by $[\mathfrak{M}_\mathrm{o}\rangle$. In case there are $\mathfrak{M}_i \in [\mathfrak{M}_\mathrm{o}\rangle$ for all $i \geq 1$ with $\mathfrak{M}_1 \xrightarrow{\tau} \mathfrak{M}_2 \xrightarrow{\tau} \cdots$ the LTS is said to display *divergence*.

Many semantic equivalences on LTSs that in some way abstract from internal transitions are defined in the literature; an overview can be found in [4]. On divergence-free LTSs, the most discriminating semantics in the spectrum of equivalences of [4], and the only one that fully respects the branching structure of related systems, is *branching bisimilarity*, proposed in [10].

Definition 7 Two LTSs $(\mathfrak{S}_1, \mathfrak{T}_1, \mathfrak{M}_{\mathrm{o}1})$ and $(\mathfrak{S}_2, \mathfrak{T}_2, \mathfrak{M}_{\mathrm{o}2})$ are *branching bisimilar* iff there exists a relation $\mathscr{B} \subseteq \mathfrak{S}_1 \times \mathfrak{S}_2$—a *branching bisimulation*—such that, for all $\alpha \in \mathfrak{Act}_\tau$:

1. $\mathfrak{M}_{\mathrm{o}1} \mathscr{B} \mathfrak{M}_{\mathrm{o}2}$;
2. if $\mathfrak{M}_1 \mathscr{B} \mathfrak{M}_2$ and $\mathfrak{M}_1 \xrightarrow{\alpha} \mathfrak{M}_1'$ then $\exists \mathfrak{M}_2^\dagger, \mathfrak{M}_2'$ such that $\mathfrak{M}_2 \Longrightarrow \mathfrak{M}_2^\dagger \xrightarrow{(\alpha)} \mathfrak{M}_2'$, $\mathfrak{M}_1 \mathscr{B} \mathfrak{M}_2^\dagger$ and $\mathfrak{M}_1' \mathscr{B} \mathfrak{M}_2'$;
3. if $\mathfrak{M}_1 \mathscr{B} \mathfrak{M}_2$ and $\mathfrak{M}_2 \xrightarrow{\alpha} \mathfrak{M}_2'$ then $\exists \mathfrak{M}_1^\dagger, \mathfrak{M}_1'$ such that $\mathfrak{M}_1 \Longrightarrow \mathfrak{M}_1^\dagger \xrightarrow{(\alpha)} \mathfrak{M}_1'$, $\mathfrak{M}_1^\dagger \mathscr{B} \mathfrak{M}_2$ and $\mathfrak{M}_1' \mathscr{B} \mathfrak{M}_2'$.

Branching bisimilarity *with explicit divergence* [10, 8], is a variant of branching bisimilarity that fully respects the diverging behaviour of related systems. Since in this paper we mainly compare systems of which one admits no divergence at all, the definition simplifies to the requirement that the other system may not diverge either.

One of the semantics reviewed in [4] that respects branching time and divergence only to a small extent, is *readiness equivalence*, proposed in [13].

Definition 8 Let $\mathfrak{L} = (\mathfrak{S}, \mathfrak{T}, \mathfrak{M}_\mathrm{o})$ be an LTS, $\sigma \in \mathfrak{Act}^*$ and $X \subseteq \mathfrak{Act}$. $\langle \sigma, X \rangle$ is a *ready pair* of $\mathfrak{L}$ iff

$$\exists \mathfrak{M}.\ \mathfrak{M}_\mathrm{o} \xRightarrow{\sigma} \mathfrak{M} \wedge \mathfrak{M} \overset{\tau}{\not\longrightarrow} \wedge X = \{a \in \mathfrak{Act} \mid \mathfrak{M} \xrightarrow{a}\}.$$

We write $\mathfrak{R}(\mathfrak{L})$ for the set of all ready pairs of $\mathfrak{L}$.
Two LTSs $\mathfrak{L}_1$ and $\mathfrak{L}_2$ are *readiness equivalent* iff $\mathfrak{R}(\mathfrak{L}_1) = \mathfrak{R}(\mathfrak{L}_2)$.

As indicated in [5], see in particular the diagram on Page 317 (or 88), equivalences on LTSs have been ported to Petri nets and other causality respecting models of concurrency chiefly in five ways: we distinguish *interleaving semantics*, *step semantics*, *split semantics*, *ST-semantics* and *causal semantics*. Causal semantics fully respect the causal relationships between the actions of related systems, whereas interleaving semantics fully abstract from this information. Step semantics differ from interleaving semantics by taking into account the possibility of multiple actions to occur simultaneously (in *one step*); this carries a minimal amount of causal information. ST-semantics respect causality to the extent that it can be expressed in terms of the possibility of durational actions to overlap in time. They are formalised by executing a visible action a in two phases: its start a^+ and its termination a^-. Moreover, terminating actions are properly matched with their starts. Split semantics are a simplification of ST-semantics in which the matching of starts and terminations is dropped.

Interleaving semantics on Petri nets can be formalised by associating to each net $N = (S, T, F, M_0, \ell)$ the LTS $(\mathfrak{S}, \mathfrak{T}, M_0)$ with $\mathfrak{S}$ the set of markings of N and $\mathfrak{T}$ given by

$$M_1 \xrightarrow{\alpha} M_2 :\Leftrightarrow \exists t \in T.\ \alpha = \ell(t) \wedge M_1\ [t\rangle\ M_2.$$

Here we take $\mathfrak{Act} := \mathrm{Act}$. Now each equivalence on LTSs from [4] induces a corresponding interleaving equivalence on nets by declaring two nets equivalent iff the associated LTSs are. For example, *interleaving branching bisimilarity* is the relation of Definition 7 with the $\mathfrak{M}$'s denoting markings, and the α's actions from Act_τ.

Step semantics on Petri nets can be formalised by associating another LTS to each net. Again we take $\mathfrak{S}$ to be the markings of the net, and $\mathfrak{M}_\mathrm{o}$ the initial marking, but this time $\mathfrak{Act}$ consists of the *steps* over Act, the non-empty, finite multisets A of visible actions from Act, and the transition relation $\mathfrak{T}$ is given by

$$M_1 \xrightarrow{A} M_2 :\Leftrightarrow \exists\, G \in_f \mathbb{N}^T.\, A = \ell(G) \wedge M_1\ [G\rangle\ M_2$$

with τ-transitions defined just as in the interleaving case. In particular, the step version of readiness equivalence would be the relation of Definition 8 with the $\mathfrak{M}$'s denoting markings, the a's steps over Act, and the σ's sequences of steps. However, variations in this type of definition are possible. In this paper, following [6], we employ a form of step readiness semantics that is a bit closer to interleaving semantics: σ is a sequence of single actions, whereas the menu X of possible continuations after σ is a set of steps.

Definition 9 Let $N = (S,T,F,M_0,\ell)$ be a Petri net, $\sigma \in \mathrm{Act}^*$ and $X \subseteq \mathbb{N}^{\mathrm{Act}}$. $\langle \sigma, X\rangle$ is a *step ready pair* of N iff

$$\exists M. M_0 \overset{\sigma}{\Longrightarrow} M \wedge M \overset{\tau}{\not\longrightarrow} \wedge X = \{A \in \mathbb{N}^{\mathrm{Act}} \mid M \xrightarrow{A}\}.$$

We write $\mathscr{R}(N)$ for the set of all step ready pairs of N.
Two Petri nets N_1 and N_2 are *step readiness equivalent*, $N_1 \approx_{\mathscr{R}} N_2$, iff $\mathscr{R}(N_1) = \mathscr{R}(N_2)$.

Next we propose a general definition on Petri nets of ST-versions of each of the semantics of [4]. Again we do this through a mapping from nets to a suitable LTS. An *ST-marking* of a net (S,T,F,M_0,ℓ) is a pair $(M,U) \in \mathbb{N}^S \times T^*$ of a normal marking, together with a sequence of transitions *currently firing*. The *initial* ST-marking is $\mathfrak{M}_\mathrm{o} := (M_0, \varepsilon)$. The elements of $\mathrm{Act}^\pm := \{a^+, a^{-n} \mid a \in \mathrm{Act},\ n > 0\}$ are called *visible action phases*, and $\mathit{Act}_\tau^\pm := \mathrm{Act}^\pm \mathbin{\dot\cup} \{\tau\}$. For $U \in T^*$, we write $t \in^{(n)} U$ if t is the n^{th} element of U. Furthermore U^{-n} denotes U after removal of the n^{th} transition.

Definition 10 Let $N = (S,T,F,M_0,\ell)$ be a Petri net, labelled over Act_τ.
The *ST-transition relations* $\xrightarrow{\eta}$ for $\eta \in \mathrm{Act}_\tau^\pm$ between ST-markings are given by
$(M,U) \xrightarrow{a^+} (M',U')$ iff $\exists t \in T.\, \ell(t) = a \wedge M[t\rangle \wedge M' = M - {}^\bullet t \wedge U' = Ut$.
$(M,U) \xrightarrow{a^{-n}} (M',U')$ iff $\exists t \in^{(n)} U.\, \ell(t) = a \wedge U' = U^{-n} \wedge M' = M + t^\bullet$.
$(M,U) \xrightarrow{\tau} (M',U')$ iff $M \xrightarrow{\tau} M' \wedge U' = U$.

Now the ST-LTS associated to a net N is $(\mathfrak{S}, \mathfrak{T}, \mathfrak{M}_\mathrm{o})$ with $\mathfrak{S}$ the set of ST-markings of N, $\mathfrak{Act} := \mathrm{Act}^\pm$, $\mathfrak{T}$ as defined in Definition 10, and $\mathfrak{M}_\mathrm{o}$ the initial ST-marking. Again, each equivalence on LTSs from [4] induces a corresponding ST-equivalence on nets by declaring two nets equivalent iff their associated LTSs are. In particular, *branching ST-bisimilarity* is the relation of Definition 7 with the $\mathfrak{M}$'s denoting ST-markings, and the α's action phases from $\mathrm{Act}_\tau^\pm$. We write $N_1 \approx^\Delta_{bSTb} N_2$ iff N_1 and N_2 are branching ST-bisimilar with explicit divergence.

ST-bisimilarity was originally proposed in [9]. It was extended to a setting with internal actions in [17], based on the notion of *weak bisimilarity* of [12], which is a bit less discriminating than branching bisimilarity. The above can be regarded as a reformulation of the same idea; the notion of weak ST-bisimilarity defined according to the recipe above agrees with the ST-bisimilarity of [17].

The next proposition says that branching ST-bisimilarity with explicit divergence is more discriminating than (i.e. *stronger* than, *finer* than, or included in) step readiness equivalence.

Proposition 1 Let N_1 and N_2 be Petri nets. If $N_1 \approx^{\Delta}_{bSTb} N_2$ then $N_1 \approx_{\mathscr{R}} N_2$.

Proof: Suppose $N_1 \approx^{\Delta}_{bSTb} N_2$ and $\langle\sigma,X\rangle \in \mathscr{R}(N_1)$. By symmetry it suffices to show that $\langle\sigma,X\rangle \in \mathscr{R}(N_2)$.

There must be a branching bisimulation $\mathscr{B}$ between the ST-markings of $N_1 = (S_1,T_1,F_1,M_{01},\ell_1)$ and $N_2 = (S_2,T_2,F_2,M_{02},\ell_2)$. In particular, $(M_{01},\varepsilon)\mathscr{B}(M_{02},\varepsilon)$. Let $\sigma := a_1a_2\cdots a_n \in \mathrm{Act}^*$. Then $M_{01} \Longrightarrow\xrightarrow{a_1}\Longrightarrow\xrightarrow{a_2}\Longrightarrow \cdots \Longrightarrow\xrightarrow{a_n}\Longrightarrow M'_1$ for a marking $M'_1 \in \mathbb{N}^{S_1}$ with $X = \{A \in \mathbb{N}^{\mathrm{Act}} \mid M'_1 \xrightarrow{A}\}$ and $M'_1 \overset{\tau}{\not\longrightarrow}$. Hence $(M_{01},\varepsilon) \Longrightarrow\xrightarrow{a_1^+}\xrightarrow{a_1^{-1}}\Longrightarrow\xrightarrow{a_2^+}\xrightarrow{a_2^{-1}}\Longrightarrow \cdots \Longrightarrow\xrightarrow{a_n^+}\xrightarrow{a_n^{-1}}\Longrightarrow (M'_1,\varepsilon)$. Thus, using the properties of a branching bisimulation on the ST-LTSs associated to N_1 and N_2, there must be a marking $M'_2 \in \mathbb{N}^{S_2}$ such that $(M_{02},\varepsilon)\Longrightarrow\xrightarrow{a_1^+}\xrightarrow{a_1^{-1}}\Longrightarrow\xrightarrow{a_2^+}\xrightarrow{a_2^{-1}}\Longrightarrow \cdots \Longrightarrow\xrightarrow{a_n^+}\xrightarrow{a_n^{-1}}\Longrightarrow(M'_2,\varepsilon)$ and $(M'_1,\varepsilon)\mathscr{B}(M'_2,\varepsilon)$. Since $(M'_1,\varepsilon) \overset{\tau}{\not\longrightarrow}$, the ST-marking (M'_1,ε) admits no divergence. As $\approx^{\Delta}_{bSTb}$ respects this property, also (M'_2,ε) admits no divergence, and there must be an $M''_2 \in \mathbb{N}^{S_2}$ with $M''_2 \overset{\tau}{\not\longrightarrow}$ and $(M'_2,\varepsilon) \Longrightarrow (M''_2,\varepsilon)$. Clause 3. of a branching bisimulation gives $(M'_1,\varepsilon)\mathscr{B}(M''_2,\varepsilon)$, and Definition 10 yields $M_{02} \overset{\sigma}{\Longrightarrow} M''_2$.

Now let $B = \{b_1,\dots,b_n\} \in X$. Then $M'_1 \xrightarrow{B}$, so $(M'_1,\varepsilon) \xrightarrow{b_1^+}\xrightarrow{b_2^+} \cdots \xrightarrow{b_m^+}$. Property 2. of a branching bisimulation implies $(M''_2,\varepsilon) \xrightarrow{b_1^+}\xrightarrow{b_2^+} \cdots \xrightarrow{b_m^+}$ and hence $M''_2 \xrightarrow{B}$. Likewise, with Property 3., $M''_2 \xrightarrow{B}$ implies $M'_1 \xrightarrow{B}$ for all $B \in \mathbb{N}^{\mathrm{Act}}$. It follows that $\langle\sigma,X\rangle \in \mathscr{R}(N_2)$. □

In this paper we employ both step readiness equivalence and branching ST-bisimilarity with explicit divergence. Fortunately it will turn out that for our purposes the latter equivalence coincides with its split version (since always one of the compared nets is plain, see Proposition 2).

A *split marking* of a net $N = (S,T,F,M_0,\ell)$ is a pair $(M,U) \in \mathbb{N}^S \times \mathbb{N}^T$ of a normal marking M, together with a multiset of transitions currently firing. The *initial* split marking is $\mathfrak{M}_\mathrm{o} := (M_0,\emptyset)$. A split marking can be regarded as an abstraction from an ST-marking, in which the total order on the (finite) multiset of transitions that are currently firing has been dropped. Let $\mathrm{Act}^{\pm}_{\mathrm{split}} := \{a^+,\, a^- \mid a \in \mathrm{Act}\}$.

Definition 11 Let $N = (S,T,F,M_0,\ell)$ be a Petri net, labelled over Act_τ.

The *split transition relations* $\xrightarrow{\zeta}$ for $\zeta \in \mathrm{Act}^{\pm}_{\mathrm{split}} \stackrel{\bullet}{\cup} \{\tau\}$ between split markings are given by
$(M,U) \xrightarrow{a^+} (M',U')$ iff $\exists t \in T.\, \ell(t) = a \wedge M[t\rangle \wedge M' = M - {}^\bullet t \wedge U' = U + \{t\}$.
$(M,U) \xrightarrow{a^-} (M',U')$ iff $\exists t \in U.\, \ell(t) = a \wedge U' = U - \{t\} \wedge M' = M + t^\bullet$.
$(M,U) \xrightarrow{\tau} (M',U')$ iff $M \xrightarrow{\tau} M' \wedge U' = U$.

Note that $(M,U) \xrightarrow{a^+}$ iff $M \xrightarrow{a}$, whereas $(M,U) \xrightarrow{a^-}$ iff $a \in \ell(U)$. With induction on reachability of markings it is furthermore easy to check that $(M,U) \in [\mathfrak{M}_\mathrm{o}\rangle$ iff $\ell(U) \in \mathbb{N}^{\mathrm{Act}}$ and $M + {}^\bullet U \in [M_0\rangle$.

The split LTS associated to a net N is $(\mathfrak{S},\mathfrak{T},\mathfrak{M}_\mathrm{o})$ with $\mathfrak{S}$ the set of split markings of N, $\mathfrak{Act} := \mathrm{Act}^{\pm}$, $\mathfrak{T}$ as defined in Definition 11, and $\mathfrak{M}_\mathrm{o}$ the initial split marking. Again, each equivalence on LTSs from [4] induces a corresponding split equivalence on nets by declaring two nets equivalent iff their associated LTSs are. In particular, *branching split bisimilarity* is the relation of Definition 7 with the $\mathfrak{M}$'s denoting split markings, and the α's action phases from $\mathrm{Act}^{\pm}_{\mathrm{split}} \stackrel{\bullet}{\cup} \{\tau\}$.

For $\mathfrak{M} = (M,U) \in \mathbb{N}^S \times T^*$ an ST-marking, let $\overline{\mathfrak{M}} = (M,\overline{U}) \in \mathbb{N}^S \times \mathbb{N}^T$ be the split marking obtained by converting the sequence U into the multiset $\overline{U}$, where $\overline{U}(t)$ is the number of occurrences of the transition $t \in T$ in U. Moreover, define $\ell(\mathfrak{M})$ by $\ell(M,U) := \ell(U)$ and $\ell(t_1t_2\cdots t_k) := \ell(t_1)\ell(t_2)\cdots\ell(t_k)$. Furthermore, for $\eta \in \mathrm{Act}^{\pm}_{\tau}$, let $\overline{\eta} \in \mathrm{Act}^{\pm}_{\mathrm{split}} \stackrel{\bullet}{\cup} \{\tau\}$ be given by $\overline{a^+} := a^+$, $\overline{a^{-n}} := a^-$ and $\overline{\tau} := \tau$.

Observation 1 Let $\mathfrak{M},\mathfrak{M}'$ be ST-markings, $\mathfrak{M}^\dagger$ a split marking, $\eta \in \mathrm{Act}^{\pm}_{\tau}$ and $\zeta \in \mathrm{Act}^{\pm}_{\mathrm{split}} \cup \{\tau\}$. Then

- $\mathfrak{M} \in \mathbb{N}^S \times T^*$ is the initial ST-marking of N iff $\overline{\mathfrak{M}} \in \mathbb{N}^S \times \mathbb{N}^T$ is the initial split marking of N;
- if $\mathfrak{M} \xrightarrow{\eta} \mathfrak{M}'$ then $\overline{\mathfrak{M}} \xrightarrow{\overline{\eta}} \overline{\mathfrak{M}'}$;
- if $\overline{\mathfrak{M}} \xrightarrow{\zeta} \mathfrak{M}^\dagger$ then there is a $\mathfrak{M}' \in \mathbb{N}^S \times T^*$ and $\eta \in \mathrm{Act}^{\pm}_{\tau}$ such that $\mathfrak{M} \xrightarrow{\eta} \mathfrak{M}'$, $\overline{\eta} = \zeta$ and $\overline{\mathfrak{M}'} = \mathfrak{M}^\dagger$;
- if $\mathfrak{M} \xrightarrow{(\eta)} \mathfrak{M}'$ then $\overline{\mathfrak{M}} \xrightarrow{\overline{(\eta)}} \overline{\mathfrak{M}'}$;

- if $\overline{\mathfrak{M}} \xrightarrow{(\zeta)} \mathfrak{M}^\dagger$ then there is a $\mathfrak{M}' \in \mathbb{N}^S \times T^*$ and $\eta \in \mathrm{Act}_\tau^\pm$ such that $\mathfrak{M} \xrightarrow{(\eta)} \mathfrak{M}'$, $\overline{\eta} = \zeta$ and $\overline{\mathfrak{M}'} = \mathfrak{M}^\dagger$;
- if $\mathfrak{M} \Longrightarrow \mathfrak{M}'$ then $\overline{\mathfrak{M}} \Longrightarrow \overline{\mathfrak{M}'}$;
- if $\overline{\mathfrak{M}} \Longrightarrow \mathfrak{M}^\dagger$ then there is a $\mathfrak{M}' \in \mathbb{N}^S \times T^*$ such that $\mathfrak{M} \Longrightarrow \mathfrak{M}'$ and $\overline{\mathfrak{M}'} = \mathfrak{M}^\dagger$. □

Lemma 1 Let $N_1 = (S_1, T_1, F_1, M_{01}, \ell)$ and $N_2 = (S_2, T_2, F_2, M_{02}, \ell_2)$ be two nets, N_2 being plain; let $\mathfrak{M}_1, \mathfrak{M}'_1$ be ST-markings of N_1, and $\mathfrak{M}_2, \mathfrak{M}'_2$ ST-markings of N_2. If $\ell(\mathfrak{M}_2) = \ell(\mathfrak{M}_1)$, $\mathfrak{M}_1 \xrightarrow{\eta} \mathfrak{M}'_1$ and $\mathfrak{M}_2 \xrightarrow{(\eta')} \mathfrak{M}'_2$ with $\overline{\eta'} = \overline{\eta}$, then there is an $\mathfrak{M}''_2$ with $\mathfrak{M}_2 \xrightarrow{(\eta)} \mathfrak{M}''_2$, $\ell(\mathfrak{M}''_2) = \ell(\mathfrak{M}'_1)$, and $\overline{\mathfrak{M}''_2} = \overline{\mathfrak{M}'_2}$.

Proof: If $\mathfrak{M} \xrightarrow{\eta} \mathfrak{M}'$ or $\mathfrak{M} \xrightarrow{(\eta)} \mathfrak{M}'$ then $\ell(\mathfrak{M}')$ is completely determined by $\ell(\mathfrak{M})$ and η. For this reason the requirement $\ell(\mathfrak{M}''_2) = \ell(\mathfrak{M}'_1)$ will hold as soon as the other requirements are met.

First suppose η is of the form τ or a^+. Then $\overline{\eta} = \eta$ and moreover $\overline{\eta'} = \overline{\eta}$ implies $\eta' = \eta$. Thus we can take $\mathfrak{M}''_2 := \mathfrak{M}'_2$.

Now suppose $\eta := a^{-n}$ for some $n > 0$. Then $\eta' = a^{-m}$ for some $m > 0$. As $\mathfrak{M}_1 \xrightarrow{\eta}$, the n^{th} element of $\ell(\mathfrak{M}_1)$ must (exist and) be a. Since $\ell(\mathfrak{M}_2) = \ell(\mathfrak{M}_1)$, also the n^{th} element of $\ell(\mathfrak{M}_2)$ must be a, so there is an $\mathfrak{M}''_2$ with $\mathfrak{M}_2 \xrightarrow{(\eta)} \mathfrak{M}''_2$. Let $\mathfrak{M}_2 := (M_2, U_2)$. Then U_2 is a sequence of transitions of which the n^{th} and the m^{th} elements are both labelled a. Since the net N_2 is plain, those two transitions must be equal. Let $\mathfrak{M}'_2 := (M'_2, U'_2)$ and $\mathfrak{M}''{}_2 := (M''_2, U''_2)$. We find that $M''_2 = M'_2$ and $\overline{U''_2} = \overline{U'_2}$. It follows that $\overline{\mathfrak{M}''_2} = \overline{\mathfrak{M}'_2}$. □

Observation 2 If $\mathfrak{M} \Longrightarrow \mathfrak{M}'$ for ST-markings $\mathfrak{M}, \mathfrak{M}'$ then $\ell(\mathfrak{M}') = \ell(\mathfrak{M})$.

Observation 3 If $\ell(\mathfrak{M}_1) = \ell(\mathfrak{M}_2)$ and $\mathfrak{M}_2 \xrightarrow{a^{-n}}$ for some $a \in \mathrm{Act}$ and $n > 0$, then $\mathfrak{M}_1 \xrightarrow{a^{-n}}$.

Observation 4 If $\mathfrak{M} \xrightarrow{a^{-n}} \mathfrak{M}'$ and $\mathfrak{M} \xrightarrow{a^{-n}} \mathfrak{M}''$ for some $a \in \mathrm{Act}$ and $n > 0$, then $\mathfrak{M}'_1 = \mathfrak{M}'_2$.

Proposition 2 Let $N_1 = (S_1, T_1, F_1, M_{01}, \ell)$ and $N_2 = (S_2, T_2, F_2, M_{02}, \ell_2)$ be two nets, N_2 being plain. Then N_1 and N_2 are branching ST-bisimilar (with explicit divergence) iff they are branching split bisimilar (with explicit divergence).

Proof: Suppose $\mathscr{B}$ is a branching ST-bisimulation between N_1 and N_2. Then, by Observation 1, the relation $\mathscr{B}_{\mathrm{split}} := \{(\overline{\mathfrak{M}_1}, \overline{\mathfrak{M}_2}) \mid (\mathfrak{M}_1, \mathfrak{M}_2) \in \mathscr{B}\}$ is a branching split bisimulation between N_1 and N_2.

Now let $\mathscr{B}$ be a branching split bisimulation between N_1 and N_2. Then, using Observation 1, the relation $\mathscr{B}_{\mathrm{ST}} := \{(\mathfrak{M}_1, \mathfrak{M}_2) \mid \ell_1(\mathfrak{M}_1) = \ell_2(\mathfrak{M}_2) \land (\overline{\mathfrak{M}_1}, \overline{\mathfrak{M}_2}) \in \mathscr{B}\}$ turns out to be a branching ST-bisimulation between N_1 and N_2:

1. $\mathfrak{M}_{\mathrm{o}1} \mathscr{B}_{\mathrm{ST}} \mathfrak{M}_{\mathrm{o}2}$ follows from Observation 1, using that $\overline{\mathfrak{M}_{\mathrm{o}1}} \mathscr{B} \overline{\mathfrak{M}_{\mathrm{o}2}}$ and $\ell(\mathfrak{M}_{\mathrm{o}1}) = \ell(\mathfrak{M}_{\mathrm{o}2}) = \varepsilon$.

2. Suppose $\mathfrak{M}_1 \mathscr{B}_{\mathrm{ST}} \mathfrak{M}_2$ and $\mathfrak{M}_1 \xrightarrow{\eta} \mathfrak{M}'_1$. Then $\overline{\mathfrak{M}_1} \mathscr{B} \overline{\mathfrak{M}_2}$ and $\overline{\mathfrak{M}_1} \xrightarrow{\overline{\eta}} \overline{\mathfrak{M}'_1}$. Hence $\exists \mathfrak{M}^\dagger_2, \mathfrak{M}^\ddagger_2$ such that $\overline{\mathfrak{M}_2} \Longrightarrow \mathfrak{M}^\dagger_2 \xrightarrow{(\overline{\eta})} \mathfrak{M}^\ddagger_2$, $\overline{\mathfrak{M}_1} \mathscr{B} \mathfrak{M}^\dagger_2$ and $\overline{\mathfrak{M}'_1} \mathscr{B} \mathfrak{M}^\ddagger_2$. As N_2 is plain, $\mathfrak{M}^\dagger_2 = \overline{\mathfrak{M}_2}$. By Observation 1, using that $\overline{\mathfrak{M}_2} \xrightarrow{(\overline{\eta})} \mathfrak{M}^\ddagger_2$, $\exists \mathfrak{M}'_2, \eta'$ such that $\mathfrak{M}_2 \xrightarrow{(\eta')} \mathfrak{M}'_2$, $\overline{\eta'} = \overline{\eta}$ and $\overline{\mathfrak{M}'_2} = \mathfrak{M}^\ddagger_2$. By Lemma 1, there is an ST-marking $\mathfrak{M}''_2$ such that $\mathfrak{M}_2 \xrightarrow{(\eta)} \mathfrak{M}''_2$, $\ell(\mathfrak{M}''_2) = \ell(\mathfrak{M}'_1)$, and $\overline{\mathfrak{M}''_2} = \overline{\mathfrak{M}'_2} = \mathfrak{M}^\ddagger_2$. It follows that $\mathfrak{M}'_1 \mathscr{B}_{\mathrm{ST}} \mathfrak{M}''_2$.

3. Suppose $\mathfrak{M}_1 \mathscr{B}_{\mathrm{ST}} \mathfrak{M}_2$ and $\mathfrak{M}_2 \xrightarrow{\eta} \mathfrak{M}'_2$. Then $\overline{\mathfrak{M}_1} \mathscr{B} \overline{\mathfrak{M}_2}$ and $\overline{\mathfrak{M}_2} \xrightarrow{\overline{\eta}} \overline{\mathfrak{M}'_2}$. Hence $\exists \mathfrak{M}^\dagger_1, \mathfrak{M}^\ddagger_1$ such that $\overline{\mathfrak{M}_1} \Longrightarrow \mathfrak{M}^\dagger_1 \xrightarrow{(\overline{\eta})} \mathfrak{M}^\ddagger_1$, $\mathfrak{M}^\dagger_1 \mathscr{B} \overline{\mathfrak{M}_2}$ and $\mathfrak{M}^\ddagger_1 \mathscr{B} \overline{\mathfrak{M}'_2}$. By Observation 1, $\exists \mathfrak{M}^*_1$ such that $\mathfrak{M}_1 \Longrightarrow \mathfrak{M}^*_1$ and $\overline{\mathfrak{M}^*_1} = \mathfrak{M}^\dagger_1$. By Observation 2, $\ell(\mathfrak{M}^*_1) = \ell(\mathfrak{M}_1) = \ell(\mathfrak{M}_2)$, so $\mathfrak{M}^*_1 \mathscr{B}_{\mathrm{ST}} \mathfrak{M}_2$. Since N_2 is plain, $\eta \neq \tau$.

   - Let $\eta = a^+$ for some $a \in \mathrm{Act}$. Using that $\overline{\mathfrak{M}^*_1} \xrightarrow{(\overline{\eta})} \mathfrak{M}^\ddagger_1$, by Observation 1 $\exists \mathfrak{M}'_1, \eta'$ such that $\mathfrak{M}^*_1 \xrightarrow{(\eta')} \mathfrak{M}'_1$, $\overline{\eta'} = \overline{\eta}$ and $\overline{\mathfrak{M}'_1} = \mathfrak{M}^\ddagger_1$. It must be that $\eta' = \eta = a^+$ and $\ell(\mathfrak{M}'_1) = \ell(\mathfrak{M}^*_1)a = \ell(\mathfrak{M}_2)a = \ell(\mathfrak{M}'_2)$. Hence $\mathfrak{M}'_1 \mathscr{B}_{\mathrm{ST}} \mathfrak{M}'_2$.

- Let $\eta = a^{-n}$ for some $a \in \mathrm{Act}$ and $n > 0$. By Observation 3, $\exists \mathfrak{M}_1'$ with $\mathfrak{M}_1^* \xrightarrow{\eta} \mathfrak{M}_1'$. By Part 2. of this proof, $\exists \mathfrak{M}_2''$ such that $\mathfrak{M}_2 \xrightarrow{(\eta)} \mathfrak{M}_2''$ and $\mathfrak{M}_1' \mathscr{B}_{\mathrm{ST}} \mathfrak{M}_2''$. By Observation 4 $\mathfrak{M}_2'' = \mathfrak{M}_2'$.

Since the net N_2 is plain, it has no divergence. In such a case, the requirement "with explicit divergence" requires N_1 to be free of divergence as well, regardless of whether split or ST-semantics is in used. □

In this paper we will not consider causal semantics. The reason is that our distributed implementations will not fully preserve the causal behaviour of nets. We will further comment on this in the conclusion.

4 Distributed Systems

In this section, we stipulate what we understand by a distributed system, and subsequently formalise a model of distributed systems in terms of Petri nets.

- A distributed system consists of components residing on different locations.
- Components work concurrently.
- Interactions between components are only possible by explicit communications.
- Communication between components is time consuming and asynchronous.

Asynchronous communication is the only interaction mechanism in a distributed system for exchanging signals or information.

- The sending of a message happens always strictly before its receipt (there is a causal relation between sending and receiving a message).
- A sending component sends without regarding the state of the receiver; in particular there is no need to synchronise with a receiving component. After sending the sender continues its behaviour independently of receipt of the message.

As explained in the introduction, we will add another requirement to our notion of a distributed system, namely that its components only allow sequential behaviour.

Formally, we model distributed systems as nets consisting of component nets with sequential behaviour and interfaces in terms of input and output places.

Definition 12 Let $N = (S, T, F, M_0, \ell)$ be a Petri net, $I, O \subseteq S$, $I \cap O = \emptyset$ and $O^\bullet = \emptyset$.

1. (N, I, O) is a *component with interface* (I, O).
2. (N, I, O) is a *sequential* component with interface (I, O) iff
   $\exists Q \subseteq S \backslash (I \cup O)$ with $\forall t \in T. |{}^\bullet t \upharpoonright Q| = 1 \wedge |t^\bullet \upharpoonright Q| = 1$ and $|M_0 \upharpoonright Q| = 1$.

An input place $i \in I$ of a component $\mathscr{C} = (N, I, O)$ can be regarded as a mailbox of $\mathscr{C}$ for a specific type of messages. An output place $o \in O$, on the other hand, is an address outside $\mathscr{C}$ to which $\mathscr{C}$ can send messages. Moving a token into o is like posting a letter. The condition $o^\bullet = \emptyset$ says that a message, once posted, cannot be retrieved by the component.

A set of places like Q above is called an *S-invariant*. The requirements guarantee that the number of tokens in these places remains constant, in this case 1. It follows that no two transitions can ever fire concurrently (in one step). Conversely, whenever a net is sequential, in the sense that no two transitions can fire in one step, it is easily converted into a behaviourally equivalent net with the required S-invariant, namely by adding a single marked place with a self-loop to all transitions. This modification preserves virtually all semantic equivalences on Petri nets from the literature, including $\approx^{\Delta}_{bSTb}$.

Next we define an operator for combining components with asynchronous communication by fusing input and output places.

Definition 13 Let $\mathfrak{K}$ be an index set.
Let $((S_k,T_k,F_k,M_{0k},\ell_k),I_k,O_k)$ with $k\in\mathfrak{K}$ be components with interface such that $(S_k\cup T_k)\cap(S_l\cup T_l) = (I_k\cup O_k)\cap(I_l\cup O_l)$ for all $k,l\in\mathfrak{K}$ with $k\neq l$ (components are disjoint except for interface places) and $I_k\cap I_l=\emptyset$ for all $k,l\in\mathfrak{K}$ with $k\neq l$ (mailboxes cannot be shared; any message has a unique recipient).
Then the *asynchronous parallel composition* of these components is defined by

$$\Big\|_{i\in\mathfrak{K}}((S_k,T_k,F_k,M_{0k},\ell_k),I_k,O_k) = ((S,T,F,M_0,\ell),I,O)$$

with $S{=}\bigcup_{k\in\mathfrak{K}}S_k,\ T{=}\bigcup_{k\in\mathfrak{K}}T_k,\ F{=}\bigcup_{k\in\mathfrak{K}}F_k,\ M_0{=}\sum_{k\in\mathfrak{K}}M_{0k},\ \ell{=}\bigcup_{k\in\mathfrak{K}}\ell_k$ (componentwise union of all nets), $I{=}\bigcup_{k\in\mathfrak{K}}I_k$ (we accept additional inputs from outside), and $O{=}\bigcup_{k\in\mathfrak{K}}O_k\setminus\bigcup_{k\in\mathfrak{K}}I_k$ (once fused with an input, $o\in O_I$ is no longer an output).

Observation 5 $\|$ is associative.

This follows directly from the associativity of the (multi)set union operator. □

We are now ready to define the class of nets representing systems of asynchronously communicating sequential components.

Definition 14 A Petri net N is an *LSGA net* (a *locally sequential globally asynchronous net*) iff there exists an index set $\mathfrak{K}$ and sequential components with interface $\mathscr{C}_k,\ k\in\mathfrak{K}$, such that $(N,I,O)=\|_{k\in\mathfrak{K}}\mathscr{C}_k$ for some I and O.

Up to $\approx^{\Delta}_{bSTb}$—or any reasonable equivalence preserving causality and branching time but abstracting from internal activity—the same class of LSGA systems would have been obtained if we had imposed, in Definition 12, that I, O and Q form a partition of S and that ${}^\bullet I=\emptyset$. However, it is essential that our definition allows multiple transitions of a component to read from the same input place.

In the remainder of this section we give a more abstract characterisation of Petri nets representing distributed systems, namely as *distributed* Petri nets, which we introduced in [6]. This will be useful in Section 5, where we investigate distributability using this more semantic characterisation. We show below that the concrete characterisation of distributed systems as LSGA nets and this abstract characterisation agree.

Following [1], to arrive at a class of nets representing distributed systems, we associate *localities* to the elements of a net $N=(S,T,F,M_0,\ell)$. We model this by a function $D: S\cup T\rightarrow \text{Loc}$, with Loc a set of possible locations. We refer to such a function as a *distribution* of N. Since the identity of the locations is irrelevant for our purposes, we can just as well abstract from Loc and represent D by the equivalence relation $\equiv_D$ on $S\cup T$ given by $x\equiv_D y$ iff $D(x)=D(y)$.

Following [6], we impose a fundamental restriction on distributions, namely that when two transitions can occur in one step, they cannot be co-located. This reflects our assumption that at a given location actions can only occur sequentially.

In [6] we observed that Petri nets incorporate a notion of synchronous interaction, in that a transition can fire only by synchronously taking the tokens from all of its preplaces. In general the behaviour of a net would change radically if a transition would take its input tokens one by one—in particular deadlocks may be introduced. Therefore we insist that in a distributed Petri net, a transition and all its input places reside on the same location. There is no reason to require the same for the output places of a transition, for the behaviour of a net would not change significantly if transitions were to deposit their output tokens one by one [6].

This leads to the following definition of a distributed Petri net.

Definition 15 [6] A Petri net $N = (S, T, F, M_0, \ell)$ is *distributed* iff there exists a distribution D such that
(1) $\forall s \in S,\ t \in T.\ s \in {}^\bullet t \Rightarrow t \equiv_D s$,
(2) $\forall t, u \in T.\ t \smile u \Rightarrow t \not\equiv_D u$.

A typical example of a net which is not distributed is shown in Figure 1 on Page 13. Transitions t and v are concurrently executable and hence should be placed on different locations. However, both have preplaces in common with u which would enforce putting all three transitions on the same location. In fact, distributed nets can be characterised in the following semi-structural way.

Observation 6 A Petri net is distributed iff there is no sequence $t_0, \dots, t_n$ of transitions with $t_0 \smile t_n$ and ${}^\bullet t_{i-1} \cap {}^\bullet t_i \neq \emptyset$ for $i = 1, \dots, n$. □

We proceed to show that the classes of LSGA nets and distributable nets essentially coincide. That every LSGA net is distributed follows because we can place each sequential component on a separate location. The following two lemmas constitute a formal argument. Here we call a component with interface (N, I, O) distributed iff N is distributed.

Lemma 2 Any sequential component with interface is distributed.

Proof: As a sequential component displays no concurrency, it suffices to co-locate all places and transitions. □

Lemma 3 states that the class of distributed nets is closed under asynchronous parallel composition.

Lemma 3 Let $\mathscr{C}_k = (N_k, I_k, O_k)$, $k \in \mathfrak{K}$, be components with interface, satisfying the requirements of Definition 13, which are all distributed. Then $\|_{k \in \mathfrak{K}} \mathscr{C}_k$ is distributed.

Proof: We need to find a distribution D satisfying the requirements of Definition 15.

Every component $\mathscr{C}_k$ is distributed and hence comes with a distribution D_k. Without loss of generality the codomains of all D_k can be assumed disjoint.

Considering each D_k as a function from net elements onto locations, a partial function D'_k can be defined which does not map any places in O_k, denoting that the element may be located arbitrarily, and behaves as D_k for all other elements. As an output place has no posttransitions within a component, any total function larger than (i.e. a superset of) D'_k is still a valid distribution for N_k.

Now $D' = \bigcup_{k \in \mathfrak{K}} D'_k$ is a (partial) function, as every place shared between components is an input place of at most one. The required distribution D can be chosen as any total function extending D'; it satisfies the requirements of Definition 15 since the D_k's do. □

Corollary 1 Every LSGA net is distributed. □

Conversely, any distributed net N can be transformed in an LSGA net by choosing co-located transitions with their pre- and postplaces as sequential components and declaring any place that belongs to multiple components to be an input place of component N_k if it is a preplace of a transition in N_k, and an output place of component N_l if it is a postplace of a transition in N_l and not an input place of N_l. Furthermore, in order to guarantee that the components are sequential in the sense of Definition 12, an explicit control place is added to each component—without changing behaviour—as explained below Definition 12. It is straightforward to check that the asynchronous parallel composition of all so-obtained components is an LSGA net, and that it is equivalent to N (using $\approx_{\mathscr{R}}$, $\approx^{\Delta}_{bSTb}$, or any other reasonable equivalence).

Theorem 1 For any distributed net N there is an LSGA net N' with $N' \approx^{\Delta}_{bSTb} N$.

Proof: Let $N = (S,T,F,M_0,\ell)$ be a distributed net with a distribution D. Then an equivalent LSGA net N' can be constructed by composing sequential components with interfaces as follows.

For each equivalence class $[x]$ of net elements according to D a sequential component $(N_{[x]}, I_{[x]}, O_{[x]})$ is created. Each such component contains one new and initially marked place $p_{[x]}$ which is connected via self-loops to all transitions in $[x]$. The interface of the component is formed by $I_{[x]} := (S \cap [x])$[1] and $O_{[x]} := ([x] \cap T)^{\bullet} \setminus [x]$. Formally, $N_{[x]} := (S_{[x]}, T_{[x]}, F_{[x]}, M_{0[x]}, \ell_{[x]})$ with

- $S_{[x]} = ((S \cap [x]) \cup O_{[x]} \cup \{p_{[x]}\}$,
- $T_{[x]} = T \cap [x]$,
- $F_{[x]} = F \restriction (S_{[x]} \cup T_{[x]})^2 \cup \{(p_{[x]},t),(t,p_{[x]}) \mid t \in T_{[x]}\}$,
- $M_{0[x]} = (M_0 \restriction [x]) \cup \{p_{[x]}\}$, and
- $\ell_{[x]} = \ell \restriction [x]$.

All components overlap at interfaces only, as the sole places not in an interface are the newly created $p_{[x]}$. The $I_{[x]}$ are disjoint as the equivalence classes $[x]$ are, so $(N',I',O') := \|_{[x]\in(S\cup T)/D}(N_{[x]}, O_{[x]}, I_{[x]})$ is well-defined. It remains to be shown that $N' \approx^{\Delta}_{bSTb} N$. The elements of N' are exactly those of N plus the new places $p_{[x]}$, which stay marked continuously except when a transition from $[x]$ is firing, and never connect two concurrently enabled transitions. Hence there exists a bijection between the ST-markings of N' and N that preserves the ST-transition relations between them, i.e. the associated ST-LTSs are isomorphic. From this it follows that $N' \approx^{\Delta}_{bSTb} N$. □

Observation 7 Every distributed Petri net is a structural conflict net. □

Corollary 2 Every LSGA net is a structural conflict net. □

Further on, we use a more liberal definition of a distributed net, called *essentially distributed*. We will show that up to $\approx^{\Delta}_{bSTb}$ any essentially distributed net can be converted into a distributed net. In [6] we employed an even more liberal definition of a distributed net, which we call here *externally distributed*. Although we showed that up to step readiness equivalence any externally distributed net can be converted into a distributed net, this does not hold for $\approx^{\Delta}_{bSTb}$.

Definition 16 A net $N = (S,T,F,M_0,\ell)$ is *essentially distributed* iff there exists a distribution D satisfying (1) of Definition 15 and
(2′) $\forall t,u \in T.\, t \smile u \wedge \ell(t) \neq \tau \Rightarrow t \not\equiv_D u$.
It is *externally distributed* iff there exists a distribution D satisfying (1) and
(2″) $\forall t,u \in T.\, t \smile u \wedge \ell(t),\ell(u) \neq \tau \Rightarrow t \not\equiv_D u$.

Instead of ruling out co-location of concurrent transitions in general, essentially distributed nets permit concurrency of internal transitions—labelled τ—at the same location. Externally distributed nets even allow concurrency between external and internal transitions at the same location. If the transitions t and v in the net of Figure 1 would both be labelled τ, the net would be essentially distributed, although not distributed; in case only v would be labelled τ the net would be externally distributed but not essentially distributed. Essentially distributed nets need not be structural conflict nets; in fact, *any* net without external transitions is essentially distributed.

The following proposition says that up to $\approx^{\Delta}_{bSTb}$ any essentially distributed net can be converted into a distributed net.

[1] Alternatively, we could take $I_{[x]} := (T \setminus [x])^{\bullet} \cap [x]$.

Proposition 3 For any essentially distributed net N there is a distributed net N' with $N' \approx^{\Delta}_{bSTb} N$.

Proof: The same construction as in the proof of Theorem 1 applies: N' differs from N by the addition, for each location $[x]$, of a marked place $p_{[x]}$ that is connected through self-loops to all transitions at that location. This time there exists a bijection between the *reachable* ST-markings of N' and N that preserves the ST-transition relations between them. This bijection exists because a reachable ST-marking is a pair (M,U) with U a sequence of *external* transitions only; this follows by a straightforward induction on reachability by ST-transitions. From this it follows that $N' \approx^{\Delta}_{bSTb} N$. □

Likewise, up to $\approx_{\mathscr{R}}$ any externally distributed net can be converted into a distributed net.

Proposition 4 [6] For any externally distributed net N there is a distributed net N' with $N' \approx_{\mathscr{R}} N$.

Proof: Again the same construction applies. This time there exists a bijection between the markings of N' and N that preserves the step transition relations between them, i.e. the associated step transition systems are isomorphic. Here we use that the transitions in the associated LTS involve either a multiset of concurrently firing *external* transitions, or a single internal one. From this, step readiness equivalence follows. □

The counterexample in Figure 2 shows that up to $N' \approx^{\Delta}_{bSTb} N$ not any externally distributed net can be converted into a distributed net. Sequentialising the component with actions a, b and τ would disable the execution $\xrightarrow{a^+}\Longrightarrow\xrightarrow{c^+}$.

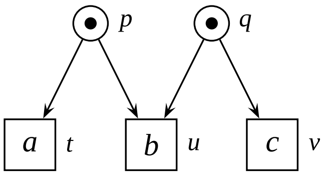

Figure 1: A fully marked M.

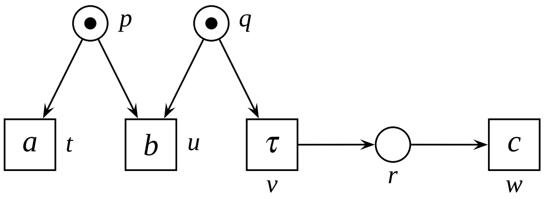

Figure 2: Externally distributed, but not distributable.

Definition 17 Given any Petri net N, the *canonical co-location relation* $\equiv_C$ on N is the equivalence relation on the places and transitions of N *generated* by Condition (1) of Definition 15, i.e. the smallest equivalence relation $\equiv_D$ satisfying (1). The *canonical distribution* of N is the distribution C that maps each place or transition to its $\equiv_C$-equivalence class.

Observation 8 A Petri net that is distributed (resp. essentially or externally distributed) w.r.t. any distribution D, is distributed (resp. essentially or externally distributed) w.r.t. its canonical distribution.

Hence a net is distributed (resp. essentially or externally distributed) iff its canonical distribution D satisfies Condition (2) of Definition 15 (resp. Condition (2′) or (2″) of Definition 16).

5 Distributable Systems

We now consider Petri nets as specifications of concurrent systems and ask the question which of those specifications can be implemented as distributed systems. This question can be formalised as

Which Petri nets are semantically equivalent to distributed nets?

Of course the answer depends on the choice of a suitable semantic equivalence. Here we will answer this question using the two equivalences discussed in the introduction. We will give a precise characterisation of those nets for which we can find semantically equivalent distributed nets. For the negative part of this characterisation, stating that certain nets are not distributable, we will use step readiness equivalence, which is one of the simplest and least discriminating equivalences imaginable that abstracts from internal actions, but preserves branching time, concurrency and divergence to some small degree. As explained in [6], giving up on any of these latter three properties would make any Petri net distributable, but in a rather trivial and unsatisfactory way. For the positive part, namely that all other nets are indeed distributable, we will use the most discriminating equivalence for which our implementation works, namely branching ST-bisimilarity with explicit divergence, which is finer than step readiness equivalence. Hence we will obtain the strongest possible results for both directions and it turns out that the concept of distributability is fairly robust w.r.t. the choice of a suitable equivalence: any equivalence notion between step readiness equivalence and branching ST-bisimilarity with explicit divergence will yield the same characterisation.

Definition 18 A Petri net N is *distributable* up to an equivalence $\approx$ iff there exists a distributed net N' with $N' \approx N$.

Formally we give our characterisation of distributability by classifying which finitary plain structural conflict nets can be implemented as distributed nets, and hence as LSGA nets. In such implementations, we use invisible transitions. We study the concept "distributable" for plain nets only, but in order to get the largest class possible we allow non-plain implementations, where a given transition may be split into multiple transitions carrying the same label.

It is well known that sometimes a global protocol is necessary to implement synchronous interaction present in system specifications. In particular, this may be needed for deciding choices in a coherent way, when these choices require agreement of multiple components. The simple net in Figure 1 shows a typical situation of this kind. Independent decisions of the two choices might lead to a deadlock. As remarked in [6], for this particular net there exists no satisfactory distributed implementation that fully respects the reactive behaviour of the original system. Indeed such M-structures, representing interference between concurrency and choice, turn out to play a crucial rôle for characterising distributability.

Definition 19 Let $N = (S,T,F,M_0,\ell)$ be a Petri net. N has a *fully reachable pure* M iff $\exists t,u,v \in T. {}^\bullet t \cap {}^\bullet u \neq \emptyset \wedge {}^\bullet u \cap {}^\bullet v \neq \emptyset \wedge {}^\bullet t \cap {}^\bullet v = \emptyset \wedge \exists M \in [M_0\rangle. {}^\bullet t \cup {}^\bullet u \cup {}^\bullet v \subseteq M$.

Note that Definition 19 implies that $t \neq u$, $u \neq v$ and $t \neq v$.

We now give an upper bound on the class of distributable nets by adopting a result from [6].

Theorem 2 Let N be a plain structural conflict Petri net. If N has a fully reachable pure M, then N is not distributable up to step readiness equivalence.

Proof: In [6] this theorem was obtained for plain one-safe nets.[2] The proof applies verbatim to plain structural conflict nets as well. □

Since $\approx^\Delta_{bSTb}$ is finer than $\approx_{\mathscr{R}}$, this result holds also for distributability up to $\approx^\Delta_{bSTb}$ (and any equivalence between $\approx_{\mathscr{R}}$ and $\approx^\Delta_{bSTb}$).

In the following, we establish that this upper bound is tight, and hence a finitary plain structural conflict net is distributable iff it has no fully reachable pure M. For this, it is helpful to first introduce macros in Petri nets for reversibility of transitions.

[2] In [6] the theorem was claimed and proven only for plain nets with a fully reachable *visible* pure M; however, for plain nets the requirement of visibility is irrelevant.

5.1 Petri nets with reversible transitions

A *Petri net with reversible transitions* generalises the notion of a Petri net; its semantics is given by a translation to an ordinary Petri net, thereby interpreting the reversible transitions as syntactic sugar for certain net fragments. It is defined as a tuple $(S,T,\Omega,\iota,F,M_0,\ell)$ with S a set of places, T a set of (reversible) transitions, labelled by $\ell : T \to \mathrm{Act} \overset{\bullet}{\cup} \{\tau\}$, Ω a set of *undo interfaces* with the relation $\iota \subseteq \Omega \times T$ linking interfaces to transitions, $M_0 \in \mathbb{N}^S$ an initial marking, and

$$F : (S \times T \times \{\mathit{in}, \mathit{early}, \mathit{late}, \mathit{out}, \mathit{far}\} \to \mathbb{N})$$

the flow relation. When $F(s,t,\mathit{type}) > 0$ for $\mathit{type} \in \{\mathit{in}, \mathit{early}, \mathit{late}, \mathit{out}, \mathit{far}\}$, this is depicted by drawing an arc from s to t, labelled with its arc weight $F(s,t,\mathit{type})$, of the form $\longrightarrow$, $\relbar\!\!\relbar\!\!\!\prec\!\!\!\succ$, $\relbar\!\!\relbar\!\!\leftrightarrow$, $\longleftarrow$, $\leftrightarrow\!\!\relbar\!\!\relbar$, respectively. For $t \in T$ and $\mathit{type} \in \{\mathit{in}, \mathit{early}, \mathit{late}, \mathit{out}, \mathit{far}\}$, the multiset of places $t^{\mathit{type}} \in \mathbb{N}^S$ is given by $t^{\mathit{type}}(s) = F(s,t,\mathit{type})$. When $s \in t^{\mathit{type}}$ for $\mathit{type} \in \{\mathit{in}, \mathit{early}, \mathit{late}\}$, the place s is called a *preplace* of t of type type; when $s \in t^{\mathit{type}}$ for $\mathit{type} \in \{\mathit{out}, \mathit{far}\}$, s is called a *postplace* of t of type type. For each undo interface $\omega \in \Omega$ and transition t with $\iota(\omega,t)$ there must be places $\mathsf{undo}_\omega(t)$, $\mathsf{reset}_\omega(t)$ and $\mathsf{ack}_\omega(t)$ in S. A transition with a nonempty set of interfaces is called *reversible*; the other (*standard*) transitions may have pre- and postplaces of types in and out only—for these transitions $t^{\mathit{in}} = {}^\bullet t$ and $t^{\mathit{out}} = t^\bullet$. In case $\Omega = \emptyset$, the net is just a normal Petri net.

A global state of a Petri net with reversible transitions is given by a marking $M \in \mathbb{N}^S$, together with the state of each reversible transition "currently in progress". Each transition in the net can fire as usual. A reversible transition can moreover take back (some of) its output tokens, and be *undone* and *reset*. When a transition t fires, it consumes $\sum_{\mathit{type} \in \{\mathit{in}, \mathit{early}, \mathit{late}\}} F(s,t,\mathit{type})$ tokens from each of its preplaces s and produces $\sum_{\mathit{type} \in \{\mathit{out}, \mathit{far}\}} F(s,t,\mathit{type})$ tokens in each of its postplaces s. A reversible transition t that has fired can start its reversal by consuming a token from $\mathsf{undo}_\omega(t)$ for one of its interfaces ω. Subsequently, it can take back one by one a token from its postplaces of type far. After it has retrieved all its output of type far, the transition is undone, thereby returning $F(s,t,\mathit{early})$ tokens in each of its preplaces s of type early. Afterwards, by consuming a token from $\mathsf{reset}_\omega(t)$, for the same interface ω that started the undo-process, the transition terminates its chain of activities by returning $F(s,t,\mathit{late})$ tokens in each of its late preplaces s. At that occasion it also produces a token in $\mathsf{ack}_\omega(t)$. Alternatively, two tokens in $\mathsf{undo}_\omega(t)$ and $\mathsf{reset}_\omega(t)$ can annihilate each other without involving the transition t; this also produces a token in $\mathsf{ack}_\omega(t)$. The latter mechanism comes in action when trying to undo a transition that has not yet fired.

Figure 3 shows the translation of a reversible transition t with $\ell(t) = a$ into an ordinary net fragment. The arc weights on the green (or grey) arcs are inherited from the untranslated net; the other arcs have weight 1. Formally, a net $(S,T,\Omega,\iota,F,M_0,\ell)$ with reversible transitions translates into the Petri net containing all places S, initially marked as indicated by M_0, all standard transitions in T, labelled according to ℓ, along with their pre- and postplaces, and furthermore all net elements mentioned in Table 1. Here $T^{\leftarrow}$ denotes the set of reversible transitions in T.

Transition	label	Preplaces	Postplaces	for all
$t \cdot \mathsf{fire}$	$\ell(t)$	t^{in}, t^{early}, t^{late}	$\mathsf{fired}(t)$, $t^{\mathit{out}}, t^{\mathit{far}}$	$t \in T^{\leftarrow}$
$t \cdot \mathsf{undo}_\omega$	τ	$\mathsf{undo}_\omega(t)$, $\mathsf{fired}(t)$	$\rho_\omega(t)$, $\mathsf{take}(f,t)$	$t \in T^{\leftarrow}$, $\iota(\omega,t)$, $f \in t^{\mathit{far}}$
$t \cdot \mathsf{undo}(f)$	τ	$\mathsf{take}(f,t)$, f	$\mathsf{took}(f,t)$	$t \in T^{\leftarrow}$, $f \in t^{\mathit{far}}$
$t \cdot \mathsf{undone}$	τ	$\mathsf{took}(f,t)$	$\rho(t)$, t^{early}	$t \in T^{\leftarrow}$, $f \in t^{\mathit{far}}$
$t \cdot \mathsf{reset}_\omega$	τ	$\mathsf{reset}_\omega(t)$, $\rho_\omega(t)$, $\rho(t)$	t^{late}, $\mathsf{ack}_\omega(t)$	$t \in T^{\leftarrow}$, $\iota(\omega,t)$
$t \cdot \mathsf{elide}_\omega$	τ	$\mathsf{undo}_\omega(t)$, $\mathsf{reset}_\omega(t)$	$\mathsf{ack}_\omega(t)$	$t \in T^{\leftarrow}$, $\iota(\omega,t)$

Table 1: Expansion of a Petri net with reversible transitions into a place/transition system.

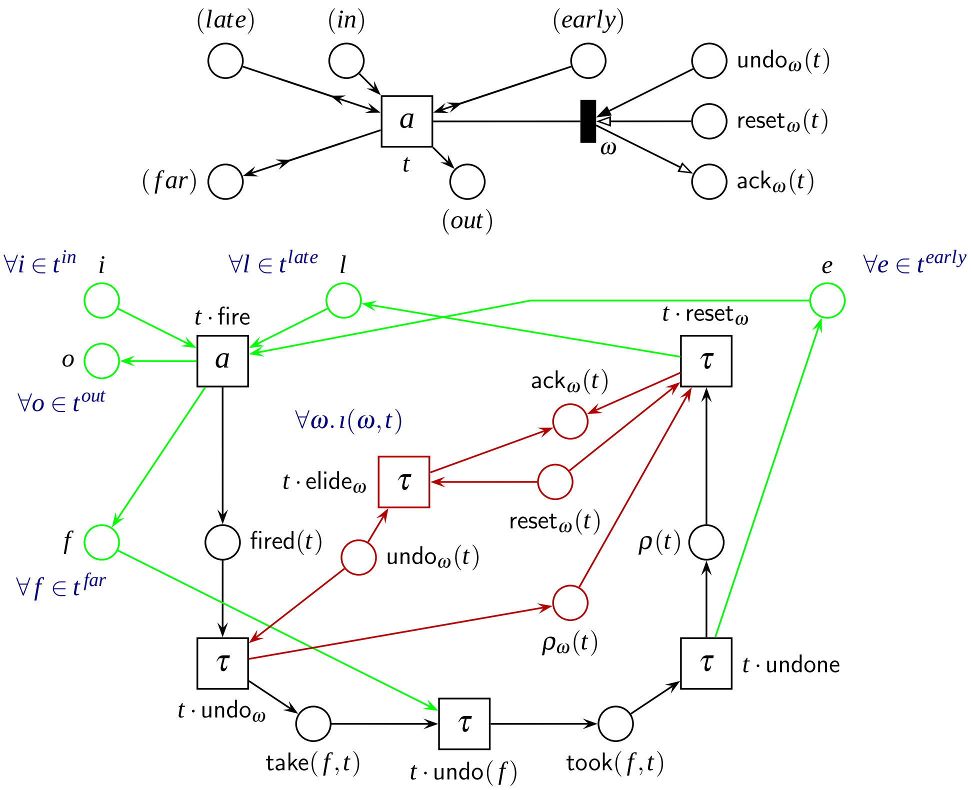

Figure 3: A reversible transition and its macro expansion.

5.2 The conflict replicating implementation

Now we establish that a finitary plain structural conflict net that has no fully reachable pure M is distributable. We do this by proposing the *conflict replicating implementation* of any such net, and show that this implementation is always (a) essentially distributed, and (b) equivalent to the original net. In order to get the strongest possible result, for (b) we use branching ST-bisimilarity with explicit divergence.

To define the conflict replicating implementation of a net $N = (S,T,F,M_0,\ell)$ we fix an arbitrary well-ordering $<$ on its transitions. We let b,c,g,h,i,j,k,l range over these ordered transitions, and write

- $i \# j$ iff $i \neq j \wedge {}^\bullet i \cap {}^\bullet j \neq \emptyset$ (transitions i and j are *in conflict*), and $i \overset{\#}{=} j$ iff $i \# j \vee i = j$,
- $i <^{\#} j$ iff $i < j \wedge i \# j$, and $i \leq^{\#} j$ iff $i <^{\#} j \vee i = j$.

Figure 4 shows the conflict replicating implementation of N. It is presented as a Petri net

$$\mathscr{I}(N) = (S',T',F',\Omega,\iota,M_0',\ell')$$

with reversible transitions. The set Ω of undo interfaces is T, and for $i \in \Omega$ we have $\iota(i,t)$ iff $t \in \Omega_i$, where the sets of transitions $\Omega_i \in \mathbb{N}^{T'}$ are specified in Figure 4. The implementation $\mathscr{I}(N)$ inherits the places of N (i.e. $S' \supseteq S$), and we postulate that $M_0' \upharpoonright S = M_0$. Given this, Figure 4 is not merely an illustration of $\mathscr{I}(N)$—it provides a complete and accurate description of it, thereby defining the conflict replicating implementation of any net. In interpreting this figure it is important to realise that net elements are completely determined by their name (identity), and exist only once, even if they show up multiple times in the figure. For instance, the place $\pi_{h\#j}$ with h=2 and j=5 (when using natural numbers for the transitions in T) is the same as the place $\pi_{j\#l}$ with j=2 and l=5; it is a standard preplace of execute_2^i (for

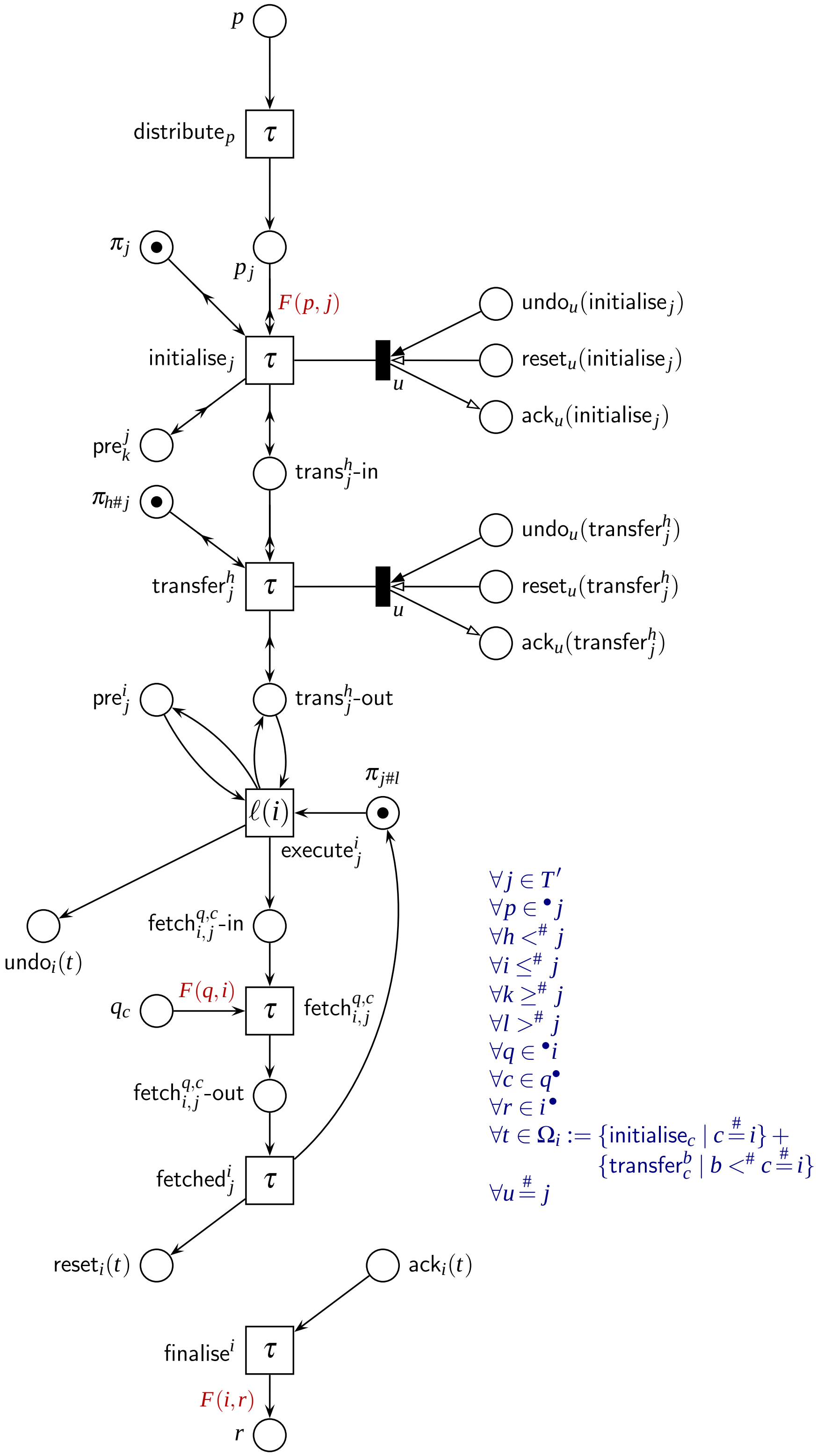

Figure 4: The conflict replicating implementation

all $i \leq^{\#} 2$), a standard postplace of $\mathsf{fetched}^{i}_{2}$, as well as a late preplace of $\mathsf{transfer}^{2}_{5}$. A description of this net after expanding the macros for reversible transitions appears in Table 2 on Page 29.

The rôle of the transitions $\mathsf{distribute}_p$ for $p \in S$ is to distribute a token in p to copies p_j of p in the localities of all transitions $j \in T$ with $p \in {}^\bullet j$. In case j is enabled in N, the transition $\mathsf{initialise}_j$ will become enabled in $\mathscr{I}(N)$. These transitions put tokens in the places pre^{j}_{k}, which are preconditions for all transitions $\mathsf{execute}^{j}_{k}$, which model the execution of j at the location of k. When two conflicting transitions h and j are both enabled in N, the first steps $\mathsf{initialise}_h$ and $\mathsf{initialise}_j$ towards their execution in $\mathscr{I}(N)$ can happen in parallel. To prevent them from executing both, $\mathsf{execute}^{j}_{j}$ (of j at its own location) is only possible after $\mathsf{transfer}^{h}_{j}$, which disables $\mathsf{execute}^{h}_{h}$.

The main idea behind the conflict replicating implementation is that a transition $h \in T$ is primarily executed by a sequential component of its own, but when a conflicting transition j gets enabled, the sequential component implementing j may "steal" the possibility to execute h from the home component of h, and keep the options to do h and j open until one of them occurs. To prevent h and j from stealing each other's initiative, which would result in deadlock, a global asymmetry is built in by ordering the transitions. Transition j can steal the initiative from h only when $h < j$.

In case j is also in conflict with a transition l, with $j < l$, the initiative to perform j may subsequently be stolen by l. In that case either h and l are in conflict too—then l takes responsibility for the execution of h as well—or h and l are concurrent—in that case h will not be enabled, due to the absence of fully reachable pure Ms in N. The absence of fully reachable pure Ms also guarantees that it cannot happen that two concurrent transitions j and k both steal the initiative from an enabled transition h.

After the firing of $\mathsf{execute}^{i}_{j}$ all tokens that were left behind in the process of carefully orchestrating this firing will have to be cleaned up, in order to prepare the net for the next activity in the same neighbourhood. This is the reason for the reversibility of the transitions preparing the firing of $\mathsf{execute}^{i}_{j}$. Hence there is an undo interface for each transition $i \in T'$, cleaning up the mess made in preparation of firing $\mathsf{execute}^{i}_{j}$ for some $j \geq^{\#} i$. Ω_i is the multiset of all transitions t that could possibly have contributed to this. For each of them the undo interface i is activated, by $\mathsf{execute}^{i}_{j}$ depositing a token in $\mathsf{undo}_i(t)$. After all preparatory transitions that have fired are undone, tokens appear in the places p_c for all $p \in {}^\bullet i$ and $c \in p^\bullet$. These are collected by $\mathsf{fetch}^{p,c}_{i,j}$, after which all transitions in Ω_i get a reset signal. Those that have fired and were undone are reset, and those that never fired perform $\mathsf{elide}_i(t)$. In either case a token appears in $\mathsf{ack}_i(t)$. These are collected by $\mathsf{finalise}^{i}$, which finishes the process of executing i by depositing tokens in its postplaces.

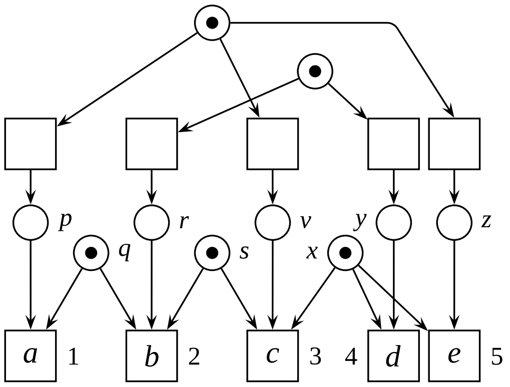

Figure 5: An example net.

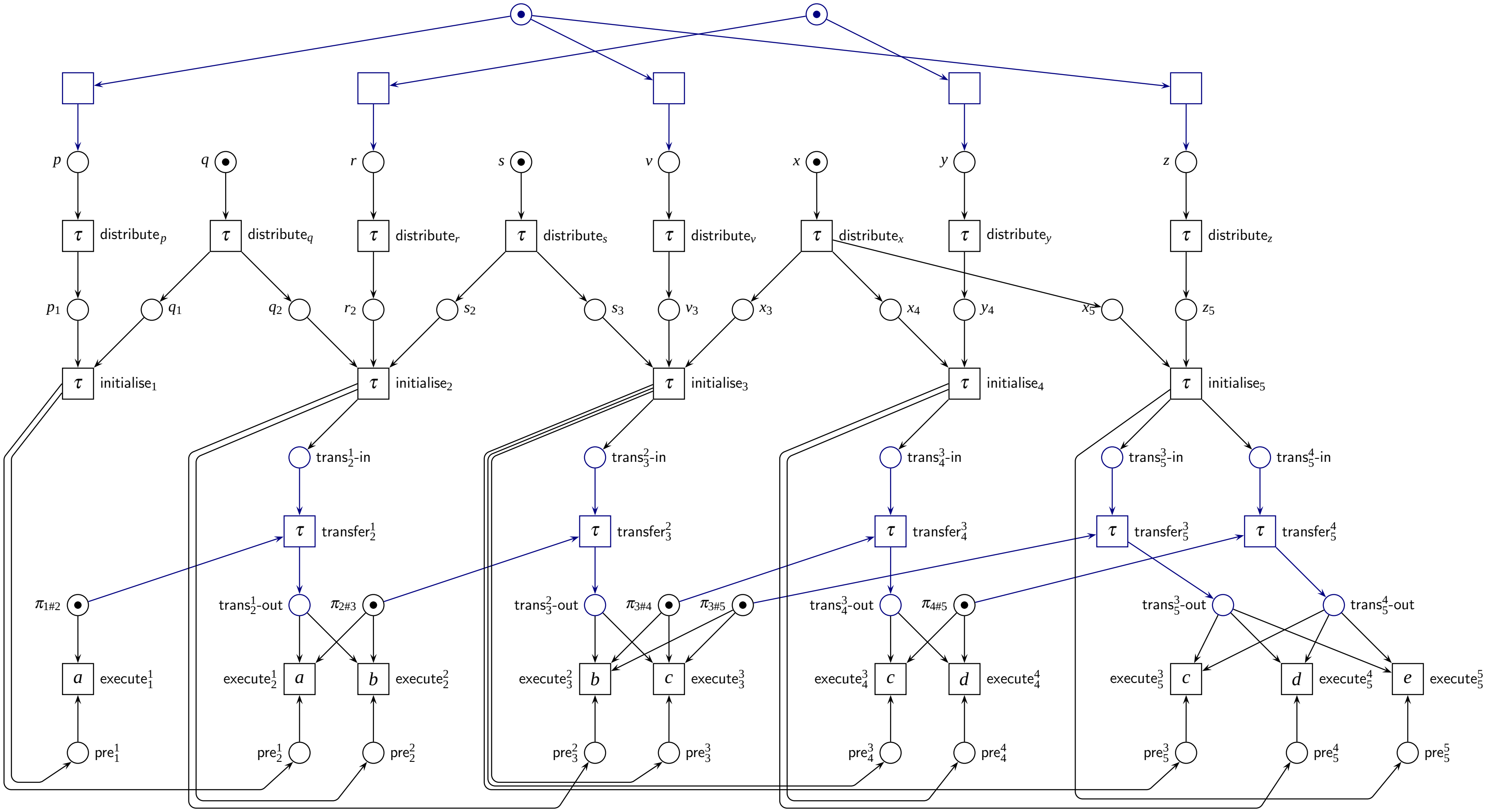

Figure 6: The (relevant parts of the) conflict replicating implementation of the net in Figure 5.

The conflict replicating implementation is illustrated by means of the finitary plain structural conflict net N of Figure 5. The places and transitions *a*-*q*-*b*-*s*-*c*-*x*-*d* in this net constitute a *Long* M: for each pair *a*-*b*, *b*-*c* and *c*-*d* of neighbouring transitions, as well as for the pair *a*-*d* of extremal transitions, there exists a reachable marking enabling them both. Moreover, neighbouring transitions in the long M are in conflict: $a\#b$, $b\#c$ and $c\#d$, whereas the extremal transitions are concurrent: $a \smile d$. However, N has no fully reachable pure M: no M-shaped triple of transitions *a*-*b*-*c*, *b*-*c*-*d* or *b*-*c*-*e* is ever simultaneously enabled.

In [6] we gave a simpler implementation, the *transition-controlled choice implementation*, that works for all finitary plain 1-safe Petri nets without such a long M. Hence N constitutes an example where that implementation does not apply, yet the conflict replicating implementation does. In fact, when leaving out the *z*-*e*-branch it may be the simplest example with these properties. We have added this branch to illustrate the situation where three transitions are pairwise in conflict.

Figure 6 presents relevant parts of the conflict replicating implementation $\mathscr{I}(N)$ of N. The ten places of N return in $\mathscr{I}(N)$, but the transitions of N are replaced by more complicated net fragments. In Figure 6 we have simplified the rendering of $\mathscr{I}(N)$ by simply just copying the five topmost transitions of N, instead of displaying the net fragments replacing them. This simplification is possible since the top half of N is already distributed. To remind the reader of this, we left those transitions unlabelled.

In order to fix a well-ordering $<$ on the remaining transitions, we named them after the first five positive natural numbers. The ordered conflicts between those transitions now are $1{\leq^{\#}}2$, $2{\leq^{\#}}3$, $3{\leq^{\#}}4$, $3{\leq^{\#}}5$ and $4{\leq^{\#}}5$. In Figure 6 we have skipped all places, transitions and arcs involved in the cleanup of tokens after firing of a transition. In this example the cleanup is not necessary, as no place of N is visited twice. Thus, we displayed only the non-reversible part of the transitions $\mathsf{initialise}_j$ and $\mathsf{transfer}^h_j$—i.e. $\mathsf{initialise}_j \cdot \mathsf{fire}$ and $\mathsf{transfer}^h_j \cdot \mathsf{fire}$—as well as the transitions $\mathsf{distribute}_p$ and $\mathsf{execute}^i_j$. Likewise, we omitted the outgoing arcs of $\mathsf{execute}^i_j$, the places π_j, and those places that have arcs only to omitted transitions. We leave it to the reader to check this net against the definition in Figure 4, and to play the token game on this net, to see that it correctly implements N.

In Section 7 we will show, for any finitary plain structural conflict net without a fully reachable pure M, that $\mathscr{I}(N) \approx^{\Delta}_{bSTb} N$, and that $\mathscr{I}(N)$ is essentially distributed. Hence $\mathscr{I}(N)$ is an essentially distributed implementation of N. By Proposition 3 this implies that N is distributable up to $\approx^{\Delta}_{bSTb}$. Together with Theorem 2 it follows that, for any equivalence between $\approx_{\mathscr{R}}$ and $\approx^{\Delta}_{bSTb}$, a finitary plain structural conflict net is distributable iff it has no fully reachable pure M.

Given the complexity of our construction, no techniques known to us were adequate for performing the equivalence proof. We therefore had to develop an entirely new method for rigorously proving the equivalence of two Petri nets up to $\approx^{\Delta}_{bSTb}$, one of which known to be plain. This method is presented in Section 6.

6 Proving Implementations Correct

This section presents a method for establishing the equivalence of two Petri nets, one of which known to be plain, up to branching ST-bisimilarity with explicit divergence. It appears as Theorem 3. First approximations of this method are presented in Lemmas 5 and 6. The progression from Lemma 5 to Lemma 6 and to Theorem 3 makes the method more specific (so less general) and more powerful. By means of a simplification a similar method can be obtained, also in three steps, for establishing the equivalence of two Petri nets up to interleaving branching bisimilarity with explicit divergence. This is elaborated at the end of this section.

Definition 20 A labelled transition system $(\mathfrak{S},\mathfrak{T},\mathfrak{M}_{\mathrm{o}})$ is called *deterministic* if for all reachable states $\mathfrak{M} \in [\mathfrak{M}_{\mathrm{o}}\rangle$ we have $\mathfrak{M} \overset{\tau}{\not\longrightarrow}$ and if $\mathfrak{M} \xrightarrow{a} \mathfrak{M}'$ and $\mathfrak{M} \xrightarrow{a} \mathfrak{M}''$ for some $a \in \mathfrak{Act}$ then $\mathfrak{M}' = \mathfrak{M}''$.

Deterministic systems may not have reachable τ-transitions at all; this way, if $\mathfrak{M} \overset{\sigma}{\Longrightarrow} \mathfrak{M}'$ and $\mathfrak{M} \overset{\sigma}{\Longrightarrow} \mathfrak{M}''$ for some $\sigma \in \mathfrak{Act}^*$ then $\mathfrak{M}' = \mathfrak{M}''$. Note that the labelled transition system associated to a plain Petri net is deterministic; the same applies to the ST-LTS, the split LTS or the step LTS associated to such a net.

Lemma 4 Let $(\mathfrak{S}_1,\mathfrak{T}_1,\mathfrak{M}_{\mathrm{o}1})$ and $(\mathfrak{S}_2,\mathfrak{T}_2,\mathfrak{M}_{\mathrm{o}2})$ be two labelled transition systems, the latter being deterministic. Suppose there is a relation $\mathscr{B} \subseteq \mathfrak{S}_1 \times \mathfrak{S}_2$ such that

(a) $\mathfrak{M}_{\mathrm{o}1} \mathscr{B} \mathfrak{M}_{\mathrm{o}2}$,

(b) if $\mathfrak{M}_1 \mathscr{B} \mathfrak{M}_2$ and $\mathfrak{M}_1 \xrightarrow{\tau} \mathfrak{M}_1'$ then $\mathfrak{M}_1' \mathscr{B} \mathfrak{M}_2$,

(c) if $\mathfrak{M}_1 \mathscr{B} \mathfrak{M}_2$ and $\mathfrak{M}_1 \xrightarrow{a} \mathfrak{M}_1'$ for some $a \in \mathfrak{Act}$ then $\exists \mathfrak{M}_2'.\ \mathfrak{M}_2 \xrightarrow{a} \mathfrak{M}_2' \wedge \mathfrak{M}_1' \mathscr{B} \mathfrak{M}_2'$,

(d) if $\mathfrak{M}_1 \mathscr{B} \mathfrak{M}_2$ and $\mathfrak{M}_2 \xrightarrow{a}$ for some $a \in \mathfrak{Act}$ then either $\mathfrak{M}_1 \xrightarrow{a}$ or $\mathfrak{M}_1 \xrightarrow{\tau}$

(e) and there is no infinite sequence $\mathfrak{M}_1 \xrightarrow{\tau} \mathfrak{M}_1' \xrightarrow{\tau} \mathfrak{M}_1'' \xrightarrow{\tau} \cdots$ with $\mathfrak{M}_1 \mathscr{B} \mathfrak{M}_2$ for some $\mathfrak{M}_2$.

Then $\mathscr{B}$ is a branching bisimulation, and the two LTSs are branching bisimilar with explicit divergence.

Proof: It suffices to show that $\mathscr{B}$ satisfies Conditions 1–3 of Definition 7; the condition on explicit divergence follows immediately from (e), using that a deterministic LTS admits no divergence at all.

1. By (a).
2. In case $\alpha = \tau$ this follows directly from (b), and otherwise from (c). In both cases $\mathfrak{M}_2^\dagger := \mathfrak{M}_2$ and when $\alpha = \tau$ also $\mathfrak{M}_2' := \mathfrak{M}_2$.
3. Suppose $\mathfrak{M}_1 \mathscr{B} \mathfrak{M}_2$ and $\mathfrak{M}_2 \xrightarrow{\alpha} \mathfrak{M}_2'$. Since $(\mathfrak{S}_2,\mathfrak{T}_2,\mathfrak{M}_{\mathrm{o}2})$ is deterministic, $\alpha = a \in \mathrm{Act}$. By (d) we have either $\mathfrak{M}_1 \xrightarrow{a} \mathfrak{M}_1^1$ or $\mathfrak{M}_1 \xrightarrow{\tau} \mathfrak{M}_1^1$ for some $\mathfrak{M}_1^1 \in \mathfrak{S}_1$. In the latter case (b) yields $\mathfrak{M}_1^1 \mathscr{B} \mathfrak{M}_2$, and using (d) again, either $\mathfrak{M}_1^1 \xrightarrow{a} \mathfrak{M}_1^2$ or $\mathfrak{M}_1^1 \xrightarrow{\tau} \mathfrak{M}_1^2$ for some $\mathfrak{M}_1^2 \in \mathfrak{S}_1$. Repeating this argument, if the choice between a and τ is made k times in favour of τ (with $k \geq 0$), we obtain $\mathfrak{M}_1^k \mathscr{B} \mathfrak{M}_2$ (where $\mathfrak{M}_1^0 := \mathfrak{M}_1$) and either $\mathfrak{M}_1^k \xrightarrow{a} \mathfrak{M}_1^{k+1}$ or $\mathfrak{M}_1^k \xrightarrow{\tau} \mathfrak{M}_1^{k+1}$. By (e), at some point the choice must be made in favour of a, say at $\mathfrak{M}_1^k$. Thus $\mathfrak{M}_1 \Longrightarrow \mathfrak{M}_1^k \xrightarrow{a} \mathfrak{M}_1^{k+1}$, with $\mathfrak{M}_1^k \mathscr{B} \mathfrak{M}_2$. We take $\mathfrak{M}_1^\dagger$ and $\mathfrak{M}_1'$ from Definition 7 to be $\mathfrak{M}_1^k$ and $\mathfrak{M}_1^{k+1}$. It remains to show that $\mathfrak{M}_1^{k+1} \mathscr{B} \mathfrak{M}_2'$. By (c) there is an $\mathfrak{M}_2'' \in \mathfrak{S}_2$ with $\mathfrak{M}_2 \xrightarrow{a} \mathfrak{M}_2''$ and $\mathfrak{M}_1^{k+1} \mathscr{B} \mathfrak{M}_2''$. Since $(\mathfrak{S}_2,\mathfrak{T}_2,\mathfrak{M}_{\mathrm{o}2})$ is deterministic, $\mathfrak{M}_2' = \mathfrak{M}_2''$. □

Lemma 5 Let $N = (S,T,F,M_0,\ell)$ and $N' = (S',T',F',M_0',\ell')$ be two nets, N' being plain. Suppose there is a relation $\mathscr{B} \subseteq (\mathbb{N}^S \times \mathbb{N}^T) \times (\mathbb{N}^{S'} \times \mathbb{N}^{T'})$ such that

(a) $(M_0,\emptyset) \mathscr{B} (M_0',\emptyset)$,

(b) if $(M_1,U_1) \mathscr{B} (M_1',U_1')$ and $(M_1,U_1) \xrightarrow{\tau} (M_2,U_2)$ then $(M_2,U_2) \mathscr{B} (M_1',U_1')$,

(c) if $(M_1,U_1) \mathscr{B} (M_1',U_1')$ and $(M_1,U_1) \xrightarrow{\eta} (M_2,U_2)$ for some $\eta \in \mathrm{Act}^\pm$
then $\exists (M_2',U_2').\ (M_1',U_1') \xrightarrow{\eta} (M_2',U_2') \wedge (M_2,U_2) \mathscr{B} (M_2',U_2')$,

(d) if $(M_1,U_1) \mathscr{B} (M_1',U_1')$ and $(M_1',U_1') \xrightarrow{\eta}$ with $\eta \in \mathrm{Act}^\pm$ then either $(M_1,U_1) \xrightarrow{\eta}$ or $(M_1,U_1) \xrightarrow{\tau}$

(e) and there is no infinite sequence $(M,U) \xrightarrow{\tau} (M_1,U_1) \xrightarrow{\tau} (M_2,U_2) \xrightarrow{\tau} \cdots$ with $(M,U) \mathscr{B} (M',U')$ for some (M',U').

Then $\mathscr{B}$ is a branching split bisimulation, and $N \approx^{\Delta}_{bSTb} N'$.

Proof: That N and N' are branching split bisimilar with explicit divergence follows directly from Lemma 4 by taking $(\mathfrak{S}_1,\mathfrak{T}_1,\mathfrak{M}_{\circ 1})$ and $(\mathfrak{S}_2,\mathfrak{T}_2,\mathfrak{M}_{\circ 2})$ to be the split LTSs associated to N and N' respectively. Here we use that the split LTS associated to a plain net is deterministic. The final conclusion follows by Proposition 2. □

Lemma 5 provides a method for proving $N \approx^{\Delta}_{bSTb} N'$ that can be more efficient than directly checking the definition. In particular, the intermediate states $\mathfrak{M}^{\dagger}$ and the sequence of τ-transitions $\Longrightarrow$ from Definition 7 do not occur in Lemma 4, and hence not in Lemma 5. Moreover, in Condition (d) one no longer has the match the targets of corresponding transitions. Lemma 6 below, when applicable, provides an even more efficient method: it is no longer needed to specify the branching split bisimulation $\mathscr{B}$, and the targets have disappeared from the transitions in Condition 2c as well. Instead, we have acquired Condition 1, but this is structural property, which is relatively easy to check.

Lemma 6 Let $N=(S,T,F,M_0,\ell)$ be a net and $N'=(S',T',F',M'_0,\ell')$ be a plain net with $S'\subseteq S$ and $M'_0=M_0\upharpoonright S'$. Suppose:

1. $\forall t\in T,\ \ell(t)\neq\tau.\ \exists t'\in T',\ \ell(t')=\ell(t).\ \exists G\in_f \mathbb{N}^T,\ \ell(G)\equiv\emptyset.\ \llbracket t'\rrbracket=\llbracket t+G\rrbracket$.
2. For any $G\in_f\mathbb{Z}^T$ with $\ell(G)\equiv\emptyset$, $M'\in\mathbb{N}^{S'}$, $U'\in\mathbb{N}^{T'}$ and $U\in\mathbb{N}^T$ with $\ell'(U')=\ell(U)$, $M'+{}^\bullet U'\in[M'_0\rangle_{N'}$ and $M:=M'+{}^\bullet U'+(M_0-M'_0)+\llbracket G\rrbracket-{}^\bullet U\in\mathbb{N}^S$ with $M+{}^\bullet U\in[M_0\rangle_N$, it holds that:
   (a) there is no infinite sequence $M\xrightarrow{\tau}M_1\xrightarrow{\tau}M_2\xrightarrow{\tau}\cdots$
   (b) if $M'\xrightarrow{a}$ with $a\in\mathrm{Act}$ then $M\xrightarrow{a}$ or $M\xrightarrow{\tau}$
   (c) and if $M\xrightarrow{a}$ with $a\in\mathrm{Act}$ then $M'\xrightarrow{a}$.

Then $N\approx^{\Delta}_{bSTb}N'$.

Proof: Define $\mathscr{B}\subseteq(\mathbb{N}^S\times\mathbb{N}^T)\times(\mathbb{N}^{S'}\times\mathbb{N}^{T'})$ by $(M,U)\mathscr{B}(M',U') :\Leftrightarrow \ell'(U')=\ell(U)\wedge M'+{}^\bullet U'\in[M'_0\rangle_{N'}$ $\wedge\,\exists G\in_f\mathbb{Z}^T.\ \ell(G)\equiv\emptyset\wedge M+{}^\bullet U=M'+{}^\bullet U'+(M_0-M'_0)+\llbracket G\rrbracket\in[M_0\rangle_N$. It suffices to show that $\mathscr{B}$ satisfies Conditions (a)–(e) of Lemma 5.

(a) Take $G=\emptyset$.

(b) Suppose $(M_1,U_1)\mathscr{B}(M'_1,U'_1)$ and $(M_1,U_1)\xrightarrow{\tau}(M_2,U_2)$. Then $\ell'(U'_1)=\ell(U_1)\wedge M'_1+{}^\bullet U'_1\in[M'_0\rangle_{N'}$ $\wedge\,\exists G\in_f\mathbb{Z}^T.\ \ell(G)\equiv\emptyset\wedge M_1=M'_1+{}^\bullet U'_1+(M_0-M'_0)+\llbracket G\rrbracket-{}^\bullet U_1\wedge M_1+{}^\bullet U\in[M_0\rangle_N$ and moreover $M_1\xrightarrow{\tau}M_2\wedge U_2=U_1$. So $M_1[t\rangle M_2$ for some $t\in T$ with $\ell(t)=\tau$. Hence $M_2=M_1+\llbracket t\rrbracket=M'_1+{}^\bullet U'_1+(M_0-M'_0)+\llbracket G+t\rrbracket-{}^\bullet U_1$. Since $(M_1+{}^\bullet U_1)[t\rangle(M_2+{}^\bullet U_1)$, we have $M_2+{}^\bullet U_1\in[M_0\rangle_N$. Since also $\ell(G+t)\equiv\emptyset$ it follows that $(M_2,U_1)\mathscr{B}(M'_1,U'_1)$.

(c) Suppose $(M_1,U_1)\mathscr{B}(M'_1,U'_1)$ and $(M_1,U_1)\xrightarrow{\eta}(M_2,U_2)$, with $\eta\in\mathrm{Act}^{\pm}$. Then $\ell'(U'_1)=\ell(U_1)$, $M'_1+{}^\bullet U'_1\in[M'_0\rangle_{N'}$ and

$$\exists G\in_f\mathbb{Z}^T.\ \ell(G)\equiv\emptyset\wedge M_1+{}^\bullet U_1=M'_1+{}^\bullet U'_1+(M_0-M'_0)+\llbracket G\rrbracket\in[M_0\rangle_N. \qquad (1)$$

First suppose $\eta=a^+$. Then $\exists t\in T.\ \ell(t)=a\wedge M_1[t\rangle\wedge M_2=M_1-{}^\bullet t\wedge U_2=U_1+\{t\}$. Using that $M_1\xrightarrow{a}$ with $a\in\mathrm{Act}$, by Condition 2c we have $M'_1\xrightarrow{a}$, i.e. $M'_1[t'\rangle$ for some $t'\in T$ with $\ell'(t')=a$. Let $M'_2:=M'_1-{}^\bullet t$ and $U'_2:=U'_1+\{t'\}$. Then $(M'_1,U'_1)\xrightarrow{a^+}(M'_2,U'_2)$. Moreover, $\ell(U_2)=\ell(U'_2)$, $M'_2+{}^\bullet U'_2=M'_1+{}^\bullet U'_1\in[M'_0\rangle_{N'}$ and $M_2+{}^\bullet U_2=M_1+{}^\bullet U_1$. In combination with (1) this yields

$$M_2+{}^\bullet U_2=M_1+{}^\bullet U_1=M'_1+{}^\bullet U'_1+(M_0-M'_0)+\llbracket G\rrbracket=M'_2+{}^\bullet U'_2+(M_0-M'_0)+\llbracket G\rrbracket,$$

so $(M_2,U_2)\mathscr{B}(M'_2,U'_2)$.

Now suppose $\eta = a^-$. Then $\exists t \in U_1.\ \ell(t) = a \wedge U_2 = U_1 - \{t\} \wedge M_2 = M_1 + t^\bullet$. Since $\ell'(U_1') = \ell(U_1)$ there is a $t' \in U_1'$ with $\ell(t') = a$. Let $M_2' := M_1' + t'^\bullet$ and $U_2' := U_1' - \{t'\}$. Then $(M_1', U_1') \xrightarrow{a^-} (M_2', U_2')$. By construction, $\ell(U_2) = \ell(U_2')$. Moreover, $M_2 + {}^\bullet U_2 = M_1 + t^\bullet + {}^\bullet U_1 - {}^\bullet t = (M_1 + {}^\bullet U_1) + [\![t]\!]$, and likewise

$$M_2' + {}^\bullet U_2' = (M_1' + {}^\bullet U_1') + [\![t']\!] \tag{2}$$

so $(M_1' + {}^\bullet U_1')[t'\rangle(M_2' + {}^\bullet U_2')$. Since $M_1' + {}^\bullet U_1' \in [M_0'\rangle_{N'}$, this yields $M_2' + {}^\bullet U_2' \in [M_0'\rangle_{N'}$. Moreover, $M_2 + {}^\bullet U_2 = M_1 + t^\bullet + {}^\bullet U_1 - {}^\bullet t = M_1 + {}^\bullet U_1 + [\![t]\!] \in [M_0\rangle_N$. Furthermore, combining (1) and (2) gives

$$\exists G \in_f \mathbb{Z}^T.\ \ell(G) \equiv \emptyset \wedge M_2 + {}^\bullet U_2 - [\![t]\!] = M_2' + {}^\bullet U_2' - [\![t']\!] + (M_0 - M_0') + [\![G]\!]. \tag{3}$$

By Condition 1 of Lemma 6, $\exists t'' \in T',\ \ell(t'') = \ell(t).\ \exists G_t \in_f \mathbb{N}^T,\ \ell(G_t) \equiv \emptyset.\ [\![t]\!] = [\![t'' - G_t]\!]$. Since N' is a plain net, it has only one transition $t^\dagger$ with $\ell(t^\dagger) = a$, so $t'' = t'$. Substitution of $[\![t' - G_t]\!]$ for t in (3) yields

$$\exists G \in_f \mathbb{Z}^T.\ \ell(G) \equiv \emptyset \wedge M_2 + {}^\bullet U_2 = M_2' + {}^\bullet U_2' + (M_0 - M_0') + [\![G - G_t]\!].$$

Since $\ell(G - G_t) \equiv \emptyset$ we obtain $(M_2, U_2) \mathscr{B} (M_2', U_2')$.

(d) Follows directly from Condition 2b and Definition 11.

(e) Follows directly from Condition 2a and Definition 11. □

In Lemma 6 a relation is explored between markings M and $M + [\![H]\!]$ (where M is $M' + {}^\bullet U' + (M_0 - M_0')$ of Lemma 6, $H := G$, and $M + [\![H]\!]$ is $M + {}^\bullet U$ of Lemma 6). In such a case, we can think of M as an "original marking", and of $M + [\![H]\!]$ as a modification of this marking by the token replacement $[\![H]\!]$. The next lemma provides a method to trace certain places s marked by $M + [\![H]\!]$ (or transitions t that are enabled under $M + [\![H]\!]$) back to places that must have been marked by M before taking into account the token replacement $[\![H]\!]$. Such places are called *faithful origins* of s (or t). In tracking the faithful origins of places and transitions, we assume that the places marked by M are taken from a set S^+ and the transitions in H from a set T^+. In Lemma 7 we furthermore assume that the flow relation restricted to $S \cup T^+$ is acyclic. We will need this lemma in proving the correctness of our final method of proving $N \approx^{\Delta}_{bSTb} N'$.

Definition 21 Let $N = (S, T, F, M_0, \ell)$ be a Petri net, $T^+ \subseteq T$ a set of transitions and $S^+ \subseteq S$ a set of places.

- A *path* in N is an alternating sequence $\pi = x_0 x_1 x_2 \cdots x_n \in (S \cup T)^*$ of places and transitions, such that $F(x_i, x_{i+1}) > 0$ for $0 \leq i < n$. The *arc weight* $F(\pi)$ of such a path is the product $\Pi_0^{n-1} F(x_i, x_{i+1})$.
- A place $s \in S$ is called *faithful* w.r.t. T^+ and S^+ iff $|\{s\} \cap S^+| + \sum_{t \in T^+} F(t, s) = 1$.
- A path $x_0 x_1 x_2 \cdots x_n \in (S \cup T)^*$ from x_0 to x_n is *faithful* w.r.t. T^+ and S^+ iff all intermediate nodes x_i for $0 \leq i < n$ are either transitions in T^+ or faithful places w.r.t. T^+ and S^+.
- For $x \in S \cup T$, the *infinitary multiset* ${}^*x \in (\mathbb{N} \cup \{\infty\})^{S^+}$ of *faithful origins* of x is given by ${}^*x(s) = \sup\{F(\pi) \mid \pi \text{ is a faithful path from } s \in S^+ \text{ to } x\}$. (So ${}^*x(s) = 0$ if no such path exists.)

Suppose a marking M_2 is reachable from a marking $M_1 \in \mathbb{N}^{S^+}$ by firing transitions from T^+ only. Then, if a faithful place s bears a token under M_2—i.e. $M_2(s) > 0$—this token has a unique source: if $s \in S^+$ it must stem from M_1 and otherwise it must be produced by the unique transition $t \in T^+$ with $F(t, s) = 1$.

In a net without arc weights, ${}^*x$ is always a set, namely the set of places s in S^+ from which the flow relation of the net admits a path to x that passes only through faithful places and transitions from T^+ (with the possible exception of x itself). For nets with arc weights, the underlying set of ${}^*x$ is the same, and the multiplicity of $s \in {}^*x$ is obtained by multiplying all arc weights on the qualifying path from s to x; in case of multiple such paths, we take the upper bound over all such paths (which could yield the value ∞).

Observation 9 Let (S,T,F,M_0,ℓ) be a Petri net, $T^+ \subseteq T$ a set of transitions and $S^+ \subseteq S$ a set of places. For faithful places s and transitions $t \in T$ we have

$$^*s = \begin{cases} \{s\} & \text{if } s \in S^+ \\ {}^*t & \text{if } t \in T^+ \wedge F(t,s) = 1 \end{cases} \qquad\qquad {}^*t = \bigcup\{F(s,t)\cdot{}^*s \mid s \in {}^\bullet t \wedge s \text{ faithful}\}.$$

Lemma 7 Let (S,T,F,M_0,ℓ) be a Petri net, $T^+ \subseteq T$ a set of transitions such that $F \upharpoonright (S \cup T^+)$ is acyclic, and $S^+ \subseteq S$ a set of places. Let $M \in \mathbb{N}^{S^+}$ and $H \in_f \mathbb{N}^{T^+}$, such that $M + [\![H]\!] \in \mathbb{N}^S$. Then

(a) for any faithful place s w.r.t. T^+ and S^+ we have $(M + [\![H]\!])(s) \cdot {}^*s \leq M$;

(b) for any $k \in \mathbb{N}$, and any transition t with $(M + [\![H]\!])[k \cdot \{t\}\rangle$, we have $k \cdot {}^*t \leq M$.

Proof: We apply induction on $|H|$.

(a). When $(M + [\![H]\!])(s) = 0$ it trivially follows that $(M + [\![H]\!])(s) \cdot {}^*s \leq M$. So suppose $(M + [\![H]\!])(s) > 0$. Then either $s \in S^+$ or there is a unique $t \in T^+$ with $H(t) > 0$ and $F(t,s) = 1$. In the first case, using that $s \in u^\bullet$ for no $u \in T^+$, we have $(M + [\![H]\!])(s) \leq M(s)$, so $(M + [\![H]\!])(s) \cdot {}^*s \leq M(s) \cdot \{s\} \leq M$.

In the latter case, $(M + [\![H]\!])(s) \leq M(s) + \sum_{u \in T^+} H(u) \cdot F(u,s) = H(t)$ and ${}^*s = {}^*t$.

Let $U := \{u \in T^+ \mid H(u) > 0 \wedge uF^+t\}$ be the set of transitions occurring in H from which the flow relation of the net offers a non-empty path to t. As $F \upharpoonright (S \cup T^+)$ is acyclic, $t \notin U$, so $H \upharpoonright U < H$. Let s' be any place with $s' \in {}^\bullet u$ for some transition $u \in U$. Then, by construction of U, it cannot happen that $s' \in v^\bullet$ for some transition $v \notin U$ with $H(v) > 0$. Hence $(M + [\![H \upharpoonright U]\!])(s') \geq (M + [\![H]\!])(s') \geq 0$. Moreover, for any other place s'' we have ${}^\bullet(H \upharpoonright U)(s'') = 0$ and thus $(M + [\![H \upharpoonright U]\!])(s'') \geq M(s'') \geq 0$. It follows that $M + [\![H \upharpoonright U]\!] \in \mathbb{N}^S$.

For each $s''' \in {}^\bullet t$ we have $(H - H \upharpoonright U)^\bullet(s''') = 0$ and ${}^\bullet(H - H \upharpoonright U)(s''') \geq H(t) \cdot {}^\bullet t(s''')$ and therefore $0 \leq (M + [\![H]\!])(s''') \leq (M + [\![H \upharpoonright U]\!])(s''') - H(t) \cdot {}^\bullet t(s''')$, and hence $H(t) \cdot {}^\bullet t \leq M + [\![H \upharpoonright U]\!]$. It follows that $(M + [\![H \upharpoonright U]\!])[H(t) \cdot \{t\}\rangle$. Thus, by induction, $(M + [\![H]\!])(s) \cdot {}^*s \leq H(t) \cdot {}^*t \leq M$.

(b). Let $(M + [\![H]\!])[k \cdot \{t\}\rangle$. For any faithful $s \in {}^\bullet t$ we have $(M + [\![H]\!])(s) \geq k \cdot F(s,t)$, and thus, using (a),

$$k \cdot F(s,t) \cdot {}^*s \leq (M + [\![H]\!])(s) \cdot {}^*s \leq M \;.$$

Therefore, by Observation 9, $k \cdot {}^*t = \bigcup\{k \cdot F(s,t) \cdot {}^*s \mid s \in {}^\bullet t \wedge s \text{ faithful}\} \leq M$. □

The following theorem is the main result of this section. It presents a method for proving $N \approx^{\Delta}_{bSTb} N'$ for N a net and N' a plain net. Its main advantage w.r.t. directly using the definition, or w.r.t. application of Lemma 5 or 6, is the replacement of requirements on the dynamic behaviour of nets by structural requirements. Such requirements are typically easier to check. Replacing the requirement "$M + {}^\bullet U \in [M_0\rangle_N$" in Condition 5 by "$M + {}^\bullet U \in \mathbb{N}^S$" would have yielded an even more structural version of this theorem; however, that version turned out not to be strong enough for the verification task performed in Section 7.

Theorem 3 Let $N = (S,T,F,M_0,\ell)$ be a net and $N' = (S',T',F',M_0',\ell')$ be a plain net with $S' \subseteq S$ and $M_0' = M_0 \upharpoonright S'$. Suppose there exist sets $T^+ \subseteq T$ and $T^- \subseteq T$ and a class $NF \subseteq \mathbb{Z}^T$, such that

1. $F \upharpoonright (S \cup T^+)$ is acyclic.
2. $F \upharpoonright (S \cup T^-)$ is acyclic.

3. $\forall t \in T,\ \ell(t) \neq \tau.\ \exists t' \in T',\ \ell(t') = \ell(t).\ \big({}^\bullet t' \leq {}^*t \wedge \exists G \in_f \mathbb{N}^T,\ \ell(G) \equiv \emptyset.\ [\![t']\!] = [\![t+G]\!]\big)$.
   Here ${}^*t$ is the multiset of faithful origins of t w.r.t. T^+ and $S' \cup \{s \in S \mid M_0(s) > 0\}$.

4. There exists a function $f : T \to \mathbb{N}$ with $f(t) > 0$ for all $t \in T$, extended to $\mathbb{Z}^T$ as in Definition 1, such that for each $G \in_f \mathbb{Z}^T$ with $\ell(G) \equiv \emptyset$ there is an $H \in_f NF$ with $\ell(H) \equiv \emptyset$, $[\![H]\!] = [\![G]\!]$ and $f(H) = f(G)$.

5. For every $M' \in \mathbb{N}^{S'}$, $U' \in \mathbb{N}^{T'}$ and $U \in \mathbb{N}^T$ with $\ell(U) = \ell'(U')$ and $M' + {}^\bullet U' \in [M'_0\rangle_{N'}$, there is an $H_{M',U} \in_f \mathbb{N}^{T^+}$ with $\ell(H_{M',U}) \equiv \emptyset$, such that for each $H \in_f NF$ with $M := M' + {}^\bullet U' + (M_0 - M'_0) + [\![H]\!] - {}^\bullet U \in \mathbb{N}^S$ and $M + {}^\bullet U \in [M_0\rangle_N$:
   (a) $M_{M',U} := M' + {}^\bullet U' + (M_0 - M'_0) + [\![H_{M',U}]\!] - {}^\bullet U \in \mathbb{N}^S$,
   (b) if $M' \xrightarrow{a}$ with $a \in \text{Act}$ then $M_{M',U} \xrightarrow{a}$,
   (c) $H \leq H_{M',U}$.
   (d) if $H(u) < 0$ then $u \in T^-$,
   (e) if $H(u) < 0$ and $H(t) > 0$ then ${}^\bullet u \cap {}^\bullet t = \emptyset$,
   (f) if $H(u) < 0$ and $(M + {}^\bullet U)[t\rangle$ with $\ell(t) \neq \tau$ then ${}^\bullet u \cap {}^\bullet t = \emptyset$,
   (g) if $(M + {}^\bullet U)[\{t\} + \{u\}\rangle$ and and $t', u' \in T'$ with $\ell'(t') = \ell(t)$ and $\ell'(u') = \ell(u)$, then ${}^\bullet t' \cap {}^\bullet u' = \emptyset$.

Then $N \approx^{\Delta}_{bSTb} N'$.

Proof: It suffices to show that Condition 2 of Lemma 6 holds (for Condition 1 of Lemma 6 is part of Condition 3 above). So let $G \in_f \mathbb{Z}^T$ with $\ell(G) \equiv \emptyset$, $M' \in \mathbb{N}^{S'}$, $U' \in \mathbb{N}^{T'}$ and $U \in \mathbb{N}^T$ with $\ell'(U') = \ell(U)$, $M' + {}^\bullet U' \in [M'_0\rangle_{N'}$, $M := M' + {}^\bullet U' + (M_0 - M'_0) + [\![G]\!] - {}^\bullet U \in \mathbb{N}^S$ and $M + {}^\bullet U \in [M_0\rangle_N$.

(a) Suppose $M \xrightarrow{\tau} M_1 \xrightarrow{\tau} M_2 \xrightarrow{\tau} \cdots$. Then there are transitions $t_i \in T$ with $\ell(t_i) = \tau$, for all $i \geq 1$, such that $M[t_1\rangle M_1[t_2\rangle M_2[t_3\rangle \cdots$. As also $(M + {}^\bullet U)[t_1\rangle (M_1 + {}^\bullet U)[t_2\rangle (M_2 + {}^\bullet U)[t_3\rangle \cdots$, it follows that $(M_i + {}^\bullet U) \in [M_0\rangle_N$ for all $i \geq 1$. Let $G_0 := G$ and for all $i \geq 1$ let $G_{i+1} := G_i + \{t_i\}$. Then $\ell(G_i) \equiv \emptyset$ and $M_i = M' + {}^\bullet U' + (M_0 - M'_0) + [\![G_i]\!] - {}^\bullet U$. Moreover, $f(G_{i+1}) = f(G_i) + f(t_i) > f(G_i)$. For all $i \geq 1$, using Condition 4, let $H_i \in_f NF$ be so that $[\![H_i]\!] = [\![G_i]\!]$ and $f(H_i) = f(G_i)$. Then $M_i = M' + {}^\bullet U' + (M_0 - M'_0) + [\![H_i]\!] - {}^\bullet U$ and $f(H_0) < f(H_1) < f(H_2) < \cdots$. However, from Condition 5c we get $f(H_i) \leq f(H_{M'})$ for all $i \geq 1$. The sequence $M \xrightarrow{\tau} M_1 \xrightarrow{\tau} M_2 \xrightarrow{\tau} \cdots$ therefore must be finite.

(b) Now suppose $M' \xrightarrow{a}$ with $a \in \text{Act}$. By Condition 4 above there exists an $H \in_f NF$ such that $\ell(H) \equiv \emptyset$ and $[\![H]\!] = [\![G]\!]$, and hence $M = M' + {}^\bullet U' + (M_0 - M'_0) + [\![H]\!] - {}^\bullet U$. Let $H^- := \{u \in T \mid H(u) < 0\}$.

- First suppose $H^- \neq \emptyset$. By Condition 5d, $H^- \subseteq T^-$. By Condition 2, $<^- := (F \upharpoonright (S \cup T^-))^+$ is a partial order on $S \cup T^-$, and hence on H^-. Let u be a minimal transition in H^- w.r.t. $<^-$. By definition, for all $s \in S$,

$$M(s) = M'(s) + {}^\bullet U'(s) + (M_0 - M'_0)(s) + \sum_{t \in T} H(t) \cdot F(t,s) + \sum_{t \in T} -H(t) \cdot F(s,t) + \sum_{t \in U} -U(t) \cdot F(t,s). \quad (4)$$

  As $M'_0 = M_0 \upharpoonright S'$, we have $M'_0 \leq M_0$. Hence the first three summands in this equation are always positive (or 0). Now assume $s \in {}^\bullet u$. Since u is minimal w.r.t. $<^-$, there is no $t \in T$ with $H(t) < 0$ and $F(t,s) \neq 0$. Hence also all summands $H(t) \cdot F(t,s)$ are positive. By Condition 5e, there is no $t \in T$ with $H(t) > 0$ and $F(s,t) \neq 0$, so all summands $-H(t) \cdot F(s,t)$ are positive as well. By Condition 5f, there is no $t \in T$ with $U(t) > 0$ and $F(s,t) \neq 0$, for this would imply that $\ell(t) \neq \tau$ and $(M + {}^\bullet U)[t\rangle$, so no summands in (4) are negative. Thus $0 \leq -H(u) \cdot F(s,u) \leq M(s)$. Since $H(u) \leq -1$, this implies $M(s) \geq F(s,u)$. Hence u is enabled in M. As $\ell(u) = \tau$, we have $M \xrightarrow{\tau}$.

- Next suppose $H^- = \emptyset$ but $H \neq H_{M',U}$. Let $H^\smile := \{u \in T \mid H_{M',U}(u) - H(u) > 0\}$. Then $H^\smile \neq \emptyset$ by Condition 5c. Since $H_{M',U} \in_f \mathbb{N}^{T^+}$, $H^\smile \subseteq T^+$. By Condition 1, $<^+ := (F \upharpoonright (S \cup T^+))^+$ is a partial order on $S \cup T^+$, and hence on $H^\smile$. Let u be a minimal transition in $H^\smile$ w.r.t. $<^+$. We have $M = M' + {}^\bullet U' + (M_0 - M'_0) + [\![H_{M',U} + (H - H_{M',U})]\!] - {}^\bullet U = M_{M',U} + [\![H - H_{M',U}]\!]$. Hence, for all $s \in S$,

$$M(s) = M_{M',U}(s) + \sum_{t \in T} (H - H_{M',U})(t) \cdot F(t,s) + \sum_{t \in T} -(H - H_{M',U})(t) \cdot F(s,t)\ . \qquad (5)$$

  By Condition 5a, $M_{M',U} \in \mathbb{N}^S$. By Condition 5c, $H - H_{M',U} \leq 0$. For $s \in {}^\bullet u$ there is moreover no $t \in H^\smile$ with $s \in t^\bullet$, so no $t \in T$ with $(H - H_{M',U})(t) < 0$ and $F(t,s) \neq 0$. Hence no summands in (5) are negative. It follows that $0 \leq -(H - M_{M',U})(u) \cdot F(s,t) \leq M(s)$. Since $(H - H_{M',U})(u) \leq -1$, this implies $M(s) \geq F(s,u)$. Hence u is enabled in M. As $\ell(u) = \tau$, we have $M \xrightarrow{\tau}$.

- Finally suppose $H = H_{M',U}$. Then $M = M_{M',U}$ and $M \xrightarrow{a}$ follows by Condition 5b.

(c) Next suppose $M \xrightarrow{a}$ with $a \in \text{Act}$. Then there is a $t \in T$ with $\ell(t) = a \neq \tau$ and $M[t\rangle$. So $(M + {}^\bullet U)[t\rangle$. We will first show that $(M' + {}^\bullet U') \xrightarrow{a}$. By Condition 4 there exists an $H_0 \in_f NF \subseteq \mathbb{N}^T$ such that $\ell(H_0) \equiv \emptyset$ and $[\![H_0]\!] = [\![G]\!]$, and hence $M + {}^\bullet U = M' + {}^\bullet U' + (M_0 - M'_0) + [\![H_0]\!] \in [M_0\rangle_N$. For our first step, it suffices to show that whenever $H \in_f NF$ with $M_H := M' + {}^\bullet U' + (M_0 - M'_0) + [\![H]\!] \in [M_0\rangle$ and $M_H[t\rangle$, then $(M' + {}^\bullet U') \xrightarrow{a}$. We show this by induction on $f(H_{M',U} - H)$, observing that $f(H_{M',U} - H) \in \mathbb{N}$ by Conditions 5c (with empty U) and 4.

We consider two cases, depending on the emptiness of $H^- := \{u \in T \mid H(u) < 0\}$.

First assume $H^- = \emptyset$. Then $H \in_f \mathbb{N}^T$. By Condition 5c (with empty U) we even have $H \in_f \mathbb{N}^{T^+}$. Let ${}^*t$ denote the multiset of faithful origins of t w.r.t. T^+ and $S^+ := S' \cup \{s \in S \mid M_0(s) > 0\}$. By Lemma 7(b), taking $k = 1$, substituting $M' + {}^\bullet U' + (M_0 - M'_0)$ for the "M" of that lemma, and using Condition 1 of Theorem 3, ${}^*t \leq M' + {}^\bullet U' + (M_0 - M'_0)$. So by Condition 3 of Theorem 3 there is a $t' \in T'$ with $\ell(t') = \ell(t)$ and ${}^\bullet t' \leq M' + {}^\bullet U' + (M_0 - M'_0)$. Since ${}^\bullet t' \in \mathbb{N}^{S'}$ and $M'_0 = M_0 \upharpoonright S'$, this implies ${}^\bullet t' \leq M' + {}^\bullet U'$. It follows that $(M' + {}^\bullet U')[t'\rangle_{N'}$ and hence $(M' + {}^\bullet U') \xrightarrow{a}$.

Now assume $H^- \neq \emptyset$. By the same proof as for (b) above, case $H^- \neq \emptyset$, there is a transition $u \in H^-$ that is enabled in M_H. So $M_H[u\rangle M_1$ for some $M_1 \in [M_0\rangle_N$, and $M_1 = M' + {}^\bullet U' + (M_0 - M'_0) + [\![H + u]\!]$. By Condition 5f of Theorem 3 (still with empty U), ${}^\bullet u \cap {}^\bullet t = \emptyset$, and thus $M_1[t\rangle$. By Condition 4 of Theorem 3 there exists an $H_1 \in_f NF$ such that $\ell(H_1) \equiv \emptyset$, $[\![H_1]\!] = [\![H + u]\!]$, and $f(H_1) = f(H + u) > f(H)$. Thus $M_1 = M_{H_1}$ and $f(H_{M',U} - H_1) < f(H_{M',U} - H)$. By induction we obtain $(M' + {}^\bullet U') \xrightarrow{a}$.

By the above reasoning, there is a $t' \in T'$ such that $\ell'(t') = \ell(t)$ and $(M' + {}^\bullet U')[t'\rangle$. Now take any $u' \in U'$. Then there must be an $u \in U$ with $\ell'(u') = \ell(u)$. Since $M[t\rangle$, we have $(M + {}^\bullet U)[\{t\} + \{u\}\rangle$ and by Condition 5g we obtain ${}^\bullet t' \cap {}^\bullet u' = \emptyset$. It follows that $M'[t'\rangle$, and hence $M' \xrightarrow{a}$. □

Digression: Interleaving semantics

Above, a method is presented for establishing the equivalence of two Petri nets, one of which known to be plain, up to branching ST-bisimilarity with explicit divergence. Here, we simplify this result into a method for establishing the equivalence of the two nets up interleaving branching bisimilarity with explicit divergence. This result is not applied in the current paper.

Lemma 8 Let $N = (S, T, F, M_0, \ell)$ and $N' = (S', T', F', M'_0, \ell')$ be two nets, N' being plain. Suppose there is a relation $\mathscr{B} \subseteq \mathbb{N}^S \times \mathbb{N}^{S'}$ such that

(a) $M_0 \mathscr{B} M'_0$,

(b) if $M_1 \mathscr{B} M_1'$ and $M_1 \xrightarrow{\tau} M_2$ then $M_2 \mathscr{B} M_1'$,

(c) if $M_1 \mathscr{B} M_1'$ and $M_1 \xrightarrow{a} M_2$ for some $a \in \text{Act}$ then $\exists M_2'.\ M_1' \xrightarrow{a} M_2' \wedge M_2 \mathscr{B} M_2'$,

(d) if $M_1 \mathscr{B} M_1'$ and $M_1' \xrightarrow{a}$ for some $a \in \text{Act}$ then either $M_1 \xrightarrow{a}$ or $M_1 \xrightarrow{\tau}$

(e) and there is no infinite sequence $M \xrightarrow{\tau} M_1 \xrightarrow{\tau} M_2 \xrightarrow{\tau} \cdots$ with $M \mathscr{B} M'$ for some M'.

Then N and N' are interleaving branching bisimilar with explicit divergence.

Proof: This follows directly from Lemma 4 by taking $(\mathfrak{S}_1, \mathfrak{T}_1, \mathfrak{M}_{\circ 1})$ and $(\mathfrak{S}_2, \mathfrak{T}_2, \mathfrak{M}_{\circ 2})$ to be the interleaving LTSs associated to N and N' respectively. Here we use that the LTS associated to a plain net is deterministic. □

Lemma 9 Let $N = (S, T, F, M_0, \ell)$ be a net and $N' = (S', T', F', M_0', \ell')$ be a plain net with $S' \subseteq S$ and $M_0' = M_0 \upharpoonright S'$. Suppose:

1. $\forall t \in T,\ \ell(t) \neq \tau.\ \exists t' \in T',\ \ell(t') = \ell(t).\ \exists G \in_f \mathbb{N}^T,\ \ell(G) \equiv \emptyset.\ [\![t']\!] = [\![t + G]\!]$.
2. For any $G \in_f \mathbb{Z}^T$ with $\ell(G) \equiv \emptyset$, $M' \in [M_0'\rangle_{N'}$ and $M := M' + (M_0 - M_0') + [\![G]\!] \in [M_0\rangle_N$, it holds that:
   (a) there is no infinite sequence $M \xrightarrow{\tau} M_1 \xrightarrow{\tau} M_2 \xrightarrow{\tau} \cdots$,
   (b) if $M' \xrightarrow{a}$ with $a \in \text{Act}$ then $M \xrightarrow{a}$ or $M \xrightarrow{\tau}$
   (c) and if $M \xrightarrow{a}$ with $a \in \text{Act}$ then $M' \xrightarrow{a}$.

Then N and N' are interleaving branching bisimilar with explicit divergence.

Proof: Define $\mathscr{B} \subseteq \mathbb{N}^S \times \mathbb{N}^{S'}$ by $M \mathscr{B} M' :\Leftrightarrow M' \in [M_0'\rangle_{N'} \wedge \exists G \in_f \mathbb{Z}^T.\ M = M' + (M_0 - M_0') + [\![G]\!] \in [M_0\rangle_N \wedge \ell(G) \equiv \emptyset$. It suffices to show that $\mathscr{B}$ satisfies Conditions (a)–(e) of Lemma 8.

(a) Take $G = \emptyset$.

(b) Suppose $M_1 \mathscr{B} M_1'$ and $M_1 \xrightarrow{\tau} M_2$. Then $\exists G \in_f \mathbb{Z}^T.\ M_1 = M_1' + (M_0 - M_0') + [\![G]\!] \wedge \ell(G) \equiv \emptyset$ and $\exists t \in T.\ \ell(t) = \tau \wedge M_2 = M_1 + [\![t]\!] = M_1' + (M_0 - M_0') + [\![G + t]\!]$. Moreover, $M_1 \in [M_0\rangle_N$ and hence $M_2 \in [M_0\rangle_N$. Furthermore, $M_1' \in [M_0'\rangle_{N'}$ and $\ell(G + t) \equiv \emptyset$, so $M_2 \mathscr{B} M_1'$.

(c) Suppose $M_1 \mathscr{B} M_1'$ and $M_1 \xrightarrow{a} M_2$. Then $\exists G \in_f \mathbb{Z}^T.\ M_1 = M_1' + (M_0 - M_0') + [\![G]\!] \wedge \ell(G) \equiv \emptyset$ and $\exists t \in T.\ \ell(t) = a \neq \tau \wedge M_2 = M_1 + [\![t]\!] = M_1' + (M_0 - M_0') + [\![G + t]\!]$. Moreover, $M_1 \in [M_0\rangle_N$ and hence $M_2 \in [M_0\rangle_N$. Furthermore, $M_1' \in [M_0'\rangle_{N'}$. By Condition 1 of Lemma 9, $\exists t' \in T',\ \ell(t') = \ell(t)$. $\exists G_t \in_f \mathbb{N}^T,\ \ell(G_t) \equiv \emptyset.\ [\![t]\!] = [\![t' - G_t]\!]$. Substitution of $[\![t' - G_t]\!]$ for t yields $M_2 = M_1' + [\![t']\!] + (M_0 - M_0') + [\![G - G_t]\!]$. By Condition 2c, $M_1' \xrightarrow{a}$, so $M_1' \xrightarrow{a} M_2'$ for some $M_2' \in [M_0'\rangle_{N'}$. As t' is the only transition in T' with $\ell'(t') = a$, we must have $M_1'[t'\rangle M_2'$. So $M_1' + [\![t']\!] = M_2'$. Since $\ell(G - G_t) \equiv \emptyset$ it follows that $M_2 \mathscr{B} M_2'$.

(d) Follows directly from Condition 2b.

(e) Follows directly from Condition 2a. □

The above is a variant of this Lemma 6 that requires Condition 2 only for $U = U' = \emptyset$, and allows to conclude that N and N' are interleaving branching bisimilar (instead of branching ST-bisimilar) with explicit divergence. Likewise, the below is a variant of Theorem 3 that requires Condition 5 only for $U = U' = \emptyset$, and misses Condition 5g.

Theorem 4 Let $N = (S, T, F, M_0, \ell)$ be a net and $N' = (S', T', F', M_0', \ell')$ be a plain net with $S' \subseteq S$ and $M_0' = M_0 \upharpoonright S'$. Suppose there exist sets $T^+ \subseteq T$ and $T^- \subseteq T$ and a class $NF \subseteq \mathbb{Z}^T$, such that

1–4. Conditions 1–4 from Theorem 3 hold, and

5. For every reachable marking $M' \in [M'_0\rangle_{N'}$ there is an $H_{M'} \in_f \mathbb{N}^{T^+}$ with $\ell(H_{M'}) \equiv \emptyset$, such that for each $H \in_f NF$ with $M := M' + (M_0 - M'_0) + [\![H]\!] \in [M_0\rangle_N$ one has:
   (a) $M_{M'} := M' + (M_0 - M'_0) + [\![H_{M'}]\!] \in \mathbb{N}^S$,
   (b) if $M' \xrightarrow{a}$ with $a \in \mathrm{Act}$ then $M_{M'} \xrightarrow{a}$,
   (c) $H \leq H_{M'}$,
   (d) if $H(u) < 0$ then $u \in T^-$,
   (e) if $H(u) < 0$ and $H(t) > 0$ then ${}^\bullet u \cap {}^\bullet t = \emptyset$,
   (f) if $H(u) < 0$ and $M[t\rangle$ with $\ell(t) \neq \tau$ then ${}^\bullet u \cap {}^\bullet t = \emptyset$.

Then N and N' are interleaving branching bisimilar with explicit divergence.

Proof: A straightforward simplification of the proof of Theorem 3. □

7 The Correctness Proof

We now apply the preceding theory to prove the correctness of the conflict replicating implementation.

Theorem 5 Let N be a finitary plain structural conflict net without a fully reachable pure M.
Then $\mathscr{I}(N) \approx^{\Delta}_{bSTb} N$.

Proof: In this proof the given finitary plain structural conflict net without a fully reachable pure M will be $N' = (S', T', F', M'_0, \ell')$, and its conflict replicated implementation $\mathscr{I}(N')$ is called $N = (S, T, F, M_0, \ell)$. This convention matches the one of Section 6, but is the reverse of the one used in Section 5; it pays off in terms of a significant reduction in the number of primes in this paper.

For future reference, Table 2 provides a place-oriented representation of the conflict replicating implementation of a given net $N' = (S', T', F', M'_0, \ell')$, with the macros for reversible transitions expanded. Here $T^{\leftarrow} = \{\mathsf{initialise}_j \mid j \in T'\} \cup \{\mathsf{transfer}^h_j \mid h <^\# j \in T'\}$, whereas $(\mathsf{transfer}^h_j)^{far} = \{\mathsf{trans}^h_j\text{-}\mathsf{out}\}$ and $(\mathsf{initialise}_j)^{far} = \{\mathsf{pre}^j_k \mid k \geq^\# j\} \cup \{\mathsf{trans}^h_j\text{-}\mathsf{in} \mid h <^\# j\}$.

We will obtain Theorem 5 as an application of Theorem 3. Following the construction of N described in Section 5.2, we indeed have $S' \subseteq S$ and $M'_0 = M_0 \upharpoonright S'$. Let $T^+ \subseteq T$ be the set of transitions

$$\mathsf{distribute}_p \qquad \mathsf{initialise}_j \cdot \mathsf{fire} \qquad \mathsf{transfer}^h_j \cdot \mathsf{fire} \tag{6}$$

for any applicable values of $p \in S'$ and $h, j \in T'$. Furthermore, $T^- := (T \setminus (T^+ \cup \{\mathsf{execute}^i_j \mid i \leq^\# j \in T'\}))$. We start with checking Conditions 1, 2 and 3 of Theorem 3.

1. Let $<^+$ be the partial order on T^+ given by the order of listing in (6)—so $\mathsf{initialise}_i \cdot \mathsf{fire} <^+ \mathsf{transfer}^h_j \cdot \mathsf{fire}$, for any $i \in T'$ and $h <^\# j \in T'$, but the transitions $\mathsf{transfer}^h_j \cdot \mathsf{fire}$ and $\mathsf{transfer}^k_l \cdot \mathsf{fire}$ for $(i, j) \neq (k, l)$ are unordered. By examining Table 2 we see that for any place with a pretransition t in T^+, all its posttransitions u in T^+ appear higher in the $<^+$-ordering: $t <^+ u$. From this it follows that $F \upharpoonright (S \cup T^+)$ is acyclic.

2. Let $<^-$ be the partial order on T^- given by the row-wise order of the following enumeration of T^-:

$$\begin{array}{lllll} t \cdot \mathsf{undo}_i & \mathsf{transfer}^h_j \cdot \mathsf{undo}(f) & \mathsf{transfer}^h_j \cdot \mathsf{undone} & \mathsf{initialise}_j \cdot \mathsf{undo}(f) & \mathsf{initialise}_j \cdot \mathsf{undone} \\ \mathsf{fetch}^{p,c}_{i,j} & \mathsf{fetched}^i_j & t \cdot \mathsf{reset}_i & t \cdot \mathsf{elide}_i & \mathsf{finalise}^i \end{array}$$

   for any $t \in \{\mathsf{initialise}_j,\ \mathsf{transfer}^h_j\}$ and any applicable values of $f \in S$, $p \in S'$, and $h, i, j, c \in T'$. By examining Table 2 we see that for any place with a pretransition t in T^-, all its posttransitions u in T^- appear higher in the $<^-$-ordering: $t <^- u$. From this it follows that $F \upharpoonright (S \cup T^-)$ is acyclic.

Place	Pretransitions	arc weights	Posttransitions	arc weights	for all
p	$\mathsf{finalise}^i$	$F'(i,p)$	$\mathsf{distribute}_p$ (if $p^\bullet \neq \emptyset$)		$p \in S',\ i \in {}^\bullet p$
p_c	$\mathsf{distribute}_p$ $\mathsf{initialise}_c \cdot \mathsf{undone}$	 $F'(p,c)$	$\mathsf{initialise}_c \cdot \mathsf{fire}$ $\mathsf{fetch}^{p,c}_{i,j}$	$F'(p,c)$ $F'(p,i)$	$p \in S',\ c \in p^\bullet$ $j \geq^\# i \in p^\bullet$
π_c (marked)	$\mathsf{initialise}_c \cdot \mathsf{reset}_i$		$\mathsf{initialise}_c \cdot \mathsf{fire}$		$i \overset{\#}{=} c \in T'$
pre^i_j	$\mathsf{initialise}_i \cdot \mathsf{fire}$ $\mathsf{execute}^i_j$		$\mathsf{execute}^i_j$ $\mathsf{initialise}_i \cdot \mathsf{undo}(\mathsf{pre}^i_j)$		$j \geq^\# i \in T'$
$\mathsf{trans}^h_j\text{-}\mathsf{in}$	$\mathsf{initialise}_j \cdot \mathsf{fire}$ $\mathsf{transfer}^h_j \cdot \mathsf{undone}$		$\mathsf{transfer}^h_j \cdot \mathsf{fire}$ $\mathsf{initialise}_j \cdot \mathsf{undo}(\mathsf{trans}^h_j\text{-}\mathsf{in})$		$h <^\# j \in T'$
$\mathsf{trans}^h_j\text{-}\mathsf{out}$	$\mathsf{transfer}^h_j \cdot \mathsf{fire}$ $\mathsf{execute}^i_j$		$\mathsf{execute}^i_j$ $\mathsf{transfer}^h_j \cdot \mathsf{undo}(\mathsf{trans}^h_j\text{-}\mathsf{out})$		$h <^\# j \in T',\ i \leq^\# j$
$\pi_{j\#l}$ (marked)	$\mathsf{fetched}^i_j$ $\mathsf{transfer}^j_l \cdot \mathsf{reset}_c$		$\mathsf{execute}^i_j$ $\mathsf{transfer}^j_l \cdot \mathsf{fire}$		$i \leq^\# j <^\# l \in T',\ c \overset{\#}{=} l$
$\mathsf{fetch}^{p,c}_{i,j}\text{-}\mathsf{in}$	$\mathsf{execute}^i_j$		$\mathsf{fetch}^{p,c}_{i,j}$		$j \geq^\# i \in T',\ p \in {}^\bullet i,\ c \in p^\bullet$
$\mathsf{fetch}^{p,c}_{i,j}\text{-}\mathsf{out}$	$\mathsf{fetch}^{p,c}_{i,j}$		$\mathsf{fetched}^i_j$		$j \geq^\# i \in T',\ p \in {}^\bullet i,\ c \in p^\bullet$
$\mathsf{undo}_i(t)$	$\mathsf{execute}^i_j \cdot \mathsf{fire}$		$t \cdot \mathsf{undo}_i,\quad t \cdot \mathsf{elide}_i$		$j \geq^\# i \in T',\ t \in \Omega_i$
$\mathsf{reset}_i(t)$	$\mathsf{fetched}^i_j$		$t \cdot \mathsf{reset}_i,\quad t \cdot \mathsf{elide}_i$		$j \geq^\# i \in T',\ t \in \Omega_i$
$\mathsf{ack}_i(t)$	$t \cdot \mathsf{reset}_i,\quad t \cdot \mathsf{elide}_i$		$\mathsf{finalise}^i$		$i \in T',\ t \in \Omega_i$
$\mathsf{fired}(t)$	$t \cdot \mathsf{fire}$		$t \cdot \mathsf{undo}_i$		$t \in T^\leftarrow,\ \Omega_i \ni t$
$\rho_i(t)$	$t \cdot \mathsf{undo}_i$		$t \cdot \mathsf{reset}_i$		$t \in T^\leftarrow,\ \Omega_i \ni t$
$\mathsf{take}(f,t)$	$t \cdot \mathsf{undo}_i$		$t \cdot \mathsf{undo}(f)$		$t \in T^\leftarrow,\ \Omega_i \ni t,\ f \in t^{far}$
$\mathsf{took}(f,t)$	$t \cdot \mathsf{undo}(f)$		$t \cdot \mathsf{undone}$		$t \in T^\leftarrow,\ f \in t^{far}$
$\rho(t)$	$t \cdot \mathsf{undone}$		$t \cdot \mathsf{reset}_i$		$t \in T^\leftarrow,\ \Omega_i \ni t$

Table 2: The conflict replicating implementation.

3. The only transitions $t \in T$ with $\ell(t) \neq \tau$ are $\mathsf{execute}^i_j$, with $i \leq^\# j \in T'$. So take $i \leq^\# j \in T'$. Then the only transition $t' \in T'$ with $\ell'(t') = \ell(\mathsf{execute}^i_j)$ is i. Now two statements regarding i and $\mathsf{execute}^i_j$ need to be proven. For the first, note that, for any $p \in {}^\bullet i$, the places p, p_i and pre^i_j are faithful w.r.t. T^+ and $S' \cup \{s \in S \mid M_0(s) > 0\}$. Hence p $\mathsf{distribute}_p$ p_i $\mathsf{initialise}_i \cdot \mathsf{fire}$ pre^i_j $\mathsf{execute}^i_j$ is a faithful path from p to $\mathsf{execute}^i_j$. The arc weight of this path is $F'(p,i)$. Thus ${}^\bullet i \leq {}^*\mathsf{execute}^i_j$.

   The second statement holds because, for all $i \leq^\# j \in T'$,

   $$[\![i]\!] = [\![\mathsf{execute}^i_j + \sum_{p \in {}^\bullet i} \big(F'(p,i) \cdot \mathsf{distribute}_p + \sum_{c \in p^\bullet} \mathsf{fetch}^{p,c}_{i,j}\big) + \mathsf{fetched}^i_j + \mathsf{finalise}^i + \sum_{t \in \Omega_i} t \cdot \mathsf{elide}_i]\!]. \tag{7}$$

   To check that these equations hold, note that

   $$\begin{aligned}
   [\![\mathsf{distribute}_p]\!] &= -\{p\} + \{p_c \mid c \in p^\bullet\},\\
   [\![\mathsf{execute}^i_j]\!] &= -\{\pi_{j\#l} \mid l \geq^\# j\} + \{\mathsf{fetch}^{p,c}_{i,j}\text{-}\mathsf{in} \mid p \in {}^\bullet i,\ c \in p^\bullet\} + \{\mathsf{undo}_i(t) \mid t \in \Omega_i\},\\
   [\![\mathsf{fetch}^{p,c}_{i,j}]\!] &= -\{\mathsf{fetch}^{p,c}_{i,j}\text{-}\mathsf{in}\} - F'(p,i) \cdot \{p_c\} + \{\mathsf{fetch}^{p,c}_{i,j}\text{-}\mathsf{out}\},\\
   [\![\mathsf{fetched}^i_j]\!] &= -\{\mathsf{fetch}^{p,c}_{i,j}\text{-}\mathsf{out} \mid p \in {}^\bullet i,\ c \in p^\bullet\} + \{\pi_{j\#l} \mid l \geq^\# j\} + \{\mathsf{reset}_i(t) \mid t \in \Omega_i\},\\
   [\![t \cdot \mathsf{elide}_i]\!] &= -\{\mathsf{undo}_i(t),\ \mathsf{reset}_i(t) \mid t \in \Omega_i\} + \{\mathsf{ack}_i(t) \mid t \in \Omega_i\},\\
   [\![\mathsf{finalise}^i]\!] &= -\{\mathsf{ack}_i(t) \mid t \in \Omega_i\} + \sum_{r \in i^\bullet} F'(i,r) \cdot \{r\}.
   \end{aligned}$$

Before we define the class $NF \subseteq \mathbb{Z}^T$ of signed multisets of transitions in normal form, and verify conditions 4 and 5, we derive some properties of the conflict replicating implementation $N = \mathscr{I}(N')$.

Claim 1 For any $M' \in \mathbb{Z}^{S'}$ and $G \in_f \mathbb{Z}^T$ such that $M := M' + (M_0 - M'_0) + [\![G]\!] \in \mathbb{N}^S$ we have

$$G(t\cdot\mathsf{elide}_i) + G(t\cdot\mathsf{undo}_i) \;\leq\; \sum_{j\geq^\# i} G(\mathsf{execute}^i_j) \tag{8}$$

$$G(\mathsf{finalise}^i) \leq G(t\cdot\mathsf{elide}_i) + G(t\cdot\mathsf{reset}_i) \;\leq\; \sum_{j\geq^\# i} G(\mathsf{fetched}^i_j) \tag{9}$$

$$G(t\cdot\mathsf{reset}_i) \;\leq\; G(t\cdot\mathsf{undo}_i) \tag{10}$$

for each $i \in T'$ and $t \in \Omega_i$. Moreover, for each $t \in T^{\leftarrow}$ and $f \in t^{far}$,

$$\sum_{\{\omega|t\in\Omega_\omega\}} G(t\cdot\mathsf{reset}_\omega) \leq G(t\cdot\mathsf{undone}) \leq G(t\cdot\mathsf{undo}(f)) \leq \sum_{\{\omega|t\in\Omega_\omega\}} G(t\cdot\mathsf{undo}_\omega) \leq G(t\cdot\mathsf{fire}) \tag{11}$$

and for each appropriate $c,h,i,j,l \in T'$ and $p \in S'$:

$$G(\mathsf{fetched}^i_j) \leq G(\mathsf{fetch}^{p,c}_{i,j}) \;\leq\; G(\mathsf{execute}^i_j) \tag{12}$$

$$G(\mathsf{initialise}_j\cdot\mathsf{fire}) \;\leq\; 1 + \sum_{\omega} G(\mathsf{initialise}_j\cdot\mathsf{reset}_\omega) \tag{13}$$

$$G(\mathsf{transfer}^h_j\cdot\mathsf{fire}) - G(\mathsf{transfer}^h_j\cdot\mathsf{undone}) \;\leq\; G(\mathsf{initialise}_j\cdot\mathsf{fire}) - G(\mathsf{initialise}_j\cdot\mathsf{undo}(\mathsf{trans}^h_j\text{-}\mathsf{in})) \tag{14}$$

$$G(\mathsf{transfer}^j_l\cdot\mathsf{fire}) + \sum_{i\leq^\# j} G(\mathsf{execute}^i_j) \;\leq\; 1 + \sum_{\omega} G(\mathsf{transfer}^j_l\cdot\mathsf{reset}_\omega) + \sum_{i\leq^\# j} G(\mathsf{fetched}^i_j) \tag{15}$$

$$\text{if } \; M[\mathsf{execute}^i_j\rangle \;\text{ then }\; 1 \;\leq\; G(\mathsf{initialise}_i\cdot\mathsf{fire}) - G(\mathsf{initialise}_i\cdot\mathsf{undo}(\mathsf{pre}^i_j)) \tag{16}$$

$$\text{if } \; \exists i.\, M[\mathsf{execute}^i_j\rangle \;\text{ then }\; 1 \;\leq\; G(\mathsf{transfer}^h_j\cdot\mathsf{fire}) - G(\mathsf{transfer}^h_j\cdot\mathsf{undo}(\mathsf{trans}^h_j\text{-}\mathsf{out})) \tag{17}$$

$$F'(p,c)\cdot\big(G(\mathsf{initialise}_c\cdot\mathsf{fire}) - G(\mathsf{initialise}_c\cdot\mathsf{undone})\big) + \sum_{j\geq^\# i\in p^\bullet} F'(p,i)\cdot G(\mathsf{fetch}^{p,c}_{i,j}) \leq G(\mathsf{distribute}_p) \tag{18}$$

$$G(\mathsf{distribute}_p) \;\leq\; M'(p) + \sum_{\{i\in T'|p\in i^\bullet\}} G(\mathsf{finalise}^i). \tag{19}$$

Proof: For any $i \in T'$ and $t \in \Omega_i$, we have

$$M(\mathsf{undo}_i(t)) = \Big(\sum_{j\geq^\# i} G(\mathsf{execute}^i_j)\Big) - G(t\cdot\mathsf{elide}_i) - G(t\cdot\mathsf{undo}_i) \geq 0,$$

given that $M'(\mathsf{undo}_i(t)) = (M_0 - M'_0)(\mathsf{undo}_i(t)) = \emptyset$. In this way, the place $\mathsf{undo}_i(t)$ gives rise to the inequation (8) about G. Likewise, the places $\mathsf{ack}_i(t)$, $\mathsf{reset}_i(t)$ and $\rho_i(t)$, respectively, contribute (9) and (10), whereas $\rho(t)$, $\mathsf{took}(t)$, $\mathsf{take}(t)$ and $\mathsf{fired}(t)$ yield (11). The remaining inequations arise from $\mathsf{fetch}^{p,c}_{i,j}\text{-}\mathsf{out}$, $\mathsf{fetch}^{p,c}_{i,j}\text{-}\mathsf{in}$, π_j, $\mathsf{trans}^h_j\text{-}\mathsf{in}$, $\pi_{j\#l}$, pre^i_j, $\mathsf{trans}^h_j\text{-}\mathsf{out}$, p_c and p, respectively. ■

(15) can be rewritten as $T^j_l + \sum_{i\leq^\# j} E^i_j \leq 1$, where $T^j_l := G(\mathsf{transfer}^j_l\cdot\mathsf{fire}) - \sum_\omega G(\mathsf{transfer}^j_l\cdot\mathsf{reset}_\omega)$ and $E^i_j := G(\mathsf{execute}^i_j) - G(\mathsf{fetched}^i_j)$. By (11) $\sum_\omega G(\mathsf{transfer}^j_l\cdot\mathsf{reset}_i) \leq G(\mathsf{transfer}^j_l\cdot\mathsf{fire})$, so $T^j_l \geq 0$, and likewise, by (12), $E^i_j \geq 0$ for all $i \leq^\# j$. Hence, for all $i \leq^\# j <^\# l \in T'$,

$$0 \leq T^j_l \leq 1 \qquad 0 \leq E^i_j \leq 1 \qquad T^j_l + \sum_{i\leq^\# j} E^i_j \leq 1. \tag{20}$$

In our next claim we study triples (M, M', G) with

(A) $M \in [M_0\rangle_N$, $M' \in [M'_0\rangle_{N'}$ and $G \in_f \mathbb{Z}^T$,

(B) $M = M' + (M_0 - M'_0) + [\![G]\!]$,

(C) $G(\mathsf{finalise}^i) = 0$ for all $i \in T'$,

(D) $G(\mathsf{distribute}_p) \leq M'(p)$ for all $p \in S'$,

(E) $G(\mathsf{fetched}^k_l) \geq 0$ for all $k \leq^{\#} l \in T'$,

(F) $G(\mathsf{distribute}_p) \geq F'(p,i) \cdot G(\mathsf{execute}^i_j)$ for all $i \leq^{\#} j \in T'$ and $p \in {}^\bullet i$,

(G) $0 \leq G(\mathsf{execute}^i_j) \leq 1$ for all $i \leq^{\#} j \in T'$,

(H) $G(\mathsf{distribute}_p) \geq F'(p,j) \cdot G(\mathsf{execute}^i_j)$ for all $i \leq^{\#} j \in T'$ and $p \in {}^\bullet j$,

(I) (in the notation of (20)) if $E^i_j = 1$ with $i \leq^{\#} j \in T'$ then $T^h_j = 1$ for all $h <^{\#} j$,

(J) there are no $j \geq^{\#} i \overset{\#}{=} k \leq^{\#} l \in T'$ with $(i,j) \neq (k,\ell)$, $G(\mathsf{execute}^i_j) > 0$ and $G(\mathsf{execute}^k_l) > 0$,

(K) there are no $i \leq^{\#} j \overset{\#}{=} k \leq^{\#} l \in T'$ with $(i,j) \neq (k,\ell)$, $G(\mathsf{execute}^i_j) > 0$ and $G(\mathsf{execute}^k_l) > 0$.

Given such a triple (M_1, M'_1, G_1) and a transition $t \in T$, we define $\mathit{next}(M_1, M'_1, G_1, t) =: (M, M', G)$ as follows: Let $G_2 := G_1 + \{t\}$. Take $M := M_1 + [\![t]\!] = M'_1 + (M_0 - M'_0) + [\![G_2]\!]$. In case t is not of the form $\mathsf{finalise}^i$ we take $M' := M'_1 \in [M'_0\rangle_{N'}$ and $G := G_2 \in_f \mathbb{Z}^T$. In case $t = \mathsf{finalise}^i$ for some $i \in T'$ we have $1 = G_2(\mathsf{finalise}^i) \leq \sum_{j \geq^{\#} i} G_2(\mathsf{execute}^i_j) = \sum_{j \geq^{\#} i} G_1(\mathsf{execute}^i_j)$ by (C), (9) and (12), so by (G) and (J) there is a unique $j \geq^{\#} i$ with $G_1(\mathsf{execute}^i_j) = 1$. We take $M' := M'_1 + [\![i]\!]$ and $G := G_2 - G^i_j$, where G^i_j is the right-hand side of (7).

Claim 2 (1) If $M_1[t\rangle$ and (M_1, M'_1, G_1) satisfies (A)-(K), then so does $\mathit{next}(M_1, M'_1, G_1, t)$.

(2) For any $M \in [M_0\rangle_N$ there exist M' and G such that (A)-(K) hold.

Proof: (2) follows from (1) via induction on the reachability of M. In case $M = M_0$ we take $M' := M'_0$ and $G := \emptyset$. Clearly, (A)–(K) are satisfied.

Hence we now show (1). Let $(M, M', G) := \mathit{next}(M_1, M'_1, G_1, t)$. We check that (M, M', G) satisfies the requirements (A)–(K).

(A) By construction, $M \in [M_0\rangle_N$ and $G \in_f \mathbb{Z}^T$. If t is not of the form $\mathsf{finalise}^i$ we have $M' = M_1 \in [M'_0\rangle_{N'}$. Otherwise, by (D) and (F) we have $M'_1(p) \geq G_1(\mathsf{distribute}_p) \geq F'(p,i)$ for all $p \in {}^\bullet i$, and hence $M'_1[i\rangle$. This in turn implies that $M' = M'_1 + [\![i]\!] \in [M'_0\rangle_{N'}$.

(B) In case t is not of the form $\mathsf{finalise}^i$ we have

$$M = M_1 + [\![t]\!] = M'_1 + (M_0 - M'_0) + [\![G_1 + t]\!] = M' + (M_0 - M'_0) + [\![G]\!].$$

In case $t = \mathsf{finalise}^i$ we have $M = M'_1 + (M_0 - M'_0) + [\![G_2]\!] = M' + (M_0 - M'_0) + [\![G]\!]$, using that $[\![i]\!] = [\![G^i_j]\!]$.

(C) In case $t = \mathsf{finalise}^i$ we have $G(\mathsf{finalise}^i) = G_1(\mathsf{finalise}^i) + 1 - G^i_j(\mathsf{finalise}^i) = 0 + 1 - 1 = 0$. Otherwise $G(\mathsf{finalise}^i) = G_1(\mathsf{finalise}^i) + 0 = 0 + 0 = 0$.

(D) This follows immediately from (C) and (19).

(E) The only time that this invariant is in danger is when $t = \mathsf{finalise}^i$. Then $G = G_1 + \{\mathsf{finalise}^i\} - G^i_j$ for a certain $j \geq^{\#} i$ with $G_1(\mathsf{execute}^i_j) = 1$. By (J)[3] $G_1(\mathsf{execute}^i_l) \leq 0$ for all $l \geq^{\#} i$ with $l \neq j$.

[3] We use (J) and (E) for G_1 only, making use of the induction hypothesis.

Hence by (12) $G_1(\mathsf{fetched}^i_l) \leq 0$ for all such l. By (C) $G_2(\mathsf{finalise}^i) = G_1(\mathsf{finalise}^i) + 1 = 1$, so by (9) $\sum_{l \geq^\# i} G_1(\mathsf{fetched}^i_l) = \sum_{l \geq^\# i} G_2(\mathsf{fetched}^i_l) > 0$; hence it must be that $G_1(\mathsf{fetched}^i_j) > 0$. By (E)[3] $G_1(\mathsf{fetched}^k_l) \geq 0$ for all $k \leq^\# l \in T'$. Given that $G^i_j(\mathsf{fetched}^i_j) = 1$ and $G^i_j(\mathsf{fetched}^k_l) = 0$ for all $(k,l) \neq (i,j)$, we obtain $G(\mathsf{fetched}^k_l) \geq 0$ for all $k \leq^\# l \in T'$.

(F) Take $i \leq^\# j \in T'$ and $p \in {}^\bullet i$. There are two occasions where the invariant is in danger: when $t = \mathsf{execute}^i_j$ and when $t = \mathsf{finalise}^k$ with $k \in T'$. First let $t = \mathsf{execute}^i_j$. Then $M_1[\mathsf{execute}^i_j\rangle$. Thus,

$$\begin{aligned}
&G(\mathsf{distribute}_p)\\
&\geq\ F'(p,i) \cdot \big(G(\mathsf{initialise}_i \cdot \mathsf{fire}) - G(\mathsf{initialise}_i \cdot \mathsf{undone})\big) + \sum_{h \geq^\# g \in p^\bullet} F'(p,g) \cdot G(\mathsf{fetch}^{p,i}_{g,h}) && \text{(by (18))}\\
&\geq\ F'(p,i) \cdot \big(G(\mathsf{initialise}_i \cdot \mathsf{fire}) - G(\mathsf{initialise}_i \cdot \mathsf{undone})\big) + \sum_{h \geq^\# g \in p^\bullet} F'(p,g) \cdot G(\mathsf{fetched}^g_h) && \text{(by (12))}\\
&\geq\ F'(p,i) \cdot \big(G(\mathsf{initialise}_i \cdot \mathsf{fire}) - G(\mathsf{initialise}_i \cdot \mathsf{undone})\big) + F'(p,i) \cdot G(\mathsf{fetched}^i_j) && \text{(by (E))}\\
&\geq\ F'(p,i) \cdot \Big(\big(G(\mathsf{initialise}_i \cdot \mathsf{fire}) - G(\mathsf{initialise}_i \cdot \mathsf{undo}(\mathsf{pre}^i_j))\big) + G(\mathsf{fetched}^i_j)\Big) && \text{(by (11))}\\
&\geq\ F'(p,i) \cdot \big(1 + G(\mathsf{fetched}^i_j)\big) && \text{(by (16))}\\
&\geq\ F'(p,i) \cdot G(\mathsf{execute}^i_j) && \text{(by (20)).}
\end{aligned}$$

Now let $t = \mathsf{finalise}^k$ with $k \in T'$. By (11) $G(\mathsf{initialise}_i \cdot \mathsf{fire}) - G(\mathsf{initialise}_i \cdot \mathsf{undone}) \geq 0$. So by (18), (E), and (12) $G(\mathsf{distribute}_p) \geq 0$. For this reason we may assume, w.l.o.g., that $G(\mathsf{execute}^i_j) \geq 1$.

We have $G = G_1 + \{\mathsf{finalise}^k\} - G^k_l$ for certain $l \geq^\# k$ with $G_1(\mathsf{execute}^k_l) = 1$. Since $G^i_j(\mathsf{execute}^i_j) \geq 0$, we also have $G_1(\mathsf{execute}^i_j) \geq 1$. By (J) this implies that $\neg(i \overset{\#}{=} k)$ or $(i,j) = (k,l)$. In the latter case we have $G(\mathsf{execute}^i_j) = G_1(\mathsf{execute}^i_j) - G^i_j(\mathsf{execute}^i_j) = 1 - 1 = 0$, contradicting our assumption. In the former case $p \notin {}^\bullet k$, so $G^k_l(\mathsf{distribute}_p) = 0$ and hence $G(\mathsf{distribute}_p) = G_1(\mathsf{distribute}_p) \geq F'(p,i) \cdot G_1(\mathsf{execute}^i_j) = F'(p,i) \cdot G(\mathsf{execute}^i_j)$.

(G) That $G(\mathsf{execute}^i_j) \geq 0$ follows from (E) and (12). If $G(\mathsf{execute}^i_j) \geq 2$ for some $i \leq^\# j \in T'$ then $M'(p) \geq G(\mathsf{distribute}_p) \geq 2 \cdot F'(p,i)$ for all $p \in {}^\bullet i$, using (D) and (F), so $M'[2 \cdot \{i\}\rangle_{N'}$. Since N' is a finitary structural conflict net, it has no self-concurrency, so this is impossible.

(H) Take $i \leq^\# j \in T'$ and $p \in {}^\bullet j$. The case $i = j$ follows from (F), so assume $i <^\# j$. By (11) we have $G(\mathsf{initialise}_i \cdot \mathsf{fire}) - G(\mathsf{initialise}_i \cdot \mathsf{undone}) \geq 0$. So by (18), (E), and (12) $G(\mathsf{distribute}_p) \geq 0$. Hence, using (G), we may assume, w.l.o.g., that $G(\mathsf{execute}^i_j) = 1$. We need to investigate the same two cases as in the proof of (F) above. First let $t = \mathsf{execute}^i_j$. Then $M_1[\mathsf{execute}^i_j\rangle$. Thus,

$$\begin{aligned}
&G(\mathsf{distribute}_p)\\
&\geq\ F'(p,j) \cdot \big(G(\mathsf{initialise}_j \cdot \mathsf{fire}) - G(\mathsf{initialise}_j \cdot \mathsf{undone})\big) + \sum_{h \geq^\# g \in p^\bullet} F'(p,g) \cdot G(\mathsf{fetch}^{p,j}_{g,h}) && \text{(by (18))}\\
&\geq\ F'(p,j) \cdot \big(G(\mathsf{initialise}_j \cdot \mathsf{fire}) - G(\mathsf{initialise}_j \cdot \mathsf{undone})\big) && \text{(by (E) and (12))}\\
&\geq\ F'(p,j) \cdot \big(G(\mathsf{initialise}_j \cdot \mathsf{fire}) - G(\mathsf{initialise}_j \cdot \mathsf{undo}(\mathsf{trans}^i_j\text{-}\mathsf{in}))\big) && \text{(by (11))}\\
&\geq\ F'(p,j) \cdot \big(G(\mathsf{transfer}^i_j \cdot \mathsf{fire}) - G(\mathsf{transfer}^i_j \cdot \mathsf{undone}) && \text{(by (14))}\\
&\geq\ F'(p,j) \cdot \big(G(\mathsf{transfer}^i_j \cdot \mathsf{fire}) - G(\mathsf{transfer}^i_j \cdot \mathsf{undo}(\mathsf{trans}^i_j\text{-}\mathsf{out}))\big) && \text{(by (11))}\\
&\geq\ F'(p,j) && \text{(by (17)).}
\end{aligned}$$

Now let $t = \mathsf{finalise}^k$ with $k \in T'$. We have $G = G_1 + \{\mathsf{finalise}^k\} - G^k_l$ for certain $l \geq^\# k$ with $G_1(\mathsf{execute}^k_l) = 1$. Since $G^i_j(\mathsf{execute}^i_j) \geq 0$, we also have $G_1(\mathsf{execute}^i_j) \geq 1$. By (K) this implies that $\neg(j \overset{\#}{=} k)$ or $(i,j) = (k,l)$. In the latter case $G(\mathsf{execute}^i_j) = G_1(\mathsf{execute}^i_j) - G^i_j(\mathsf{execute}^i_j) = 1 - 1 = 0$, contradicting our assumption. In the former case $p \notin {}^\bullet k$, so $G^k_l(\mathsf{distribute}_p) = 0$ and hence $G(\mathsf{distribute}_p) = G_1(\mathsf{distribute}_p) \geq F'(p,j) \cdot G_1(\mathsf{execute}^i_j) = F'(p,j) \cdot G(\mathsf{execute}^i_j)$.

(I) Let $i \leq^{\#} j \in T'$ and $h <^{\#} j$. Since, for all $k \leq^{\#} l \in T'$, $G^k_l(\mathsf{transfer}^h_j \cdot \mathsf{fire}) = \sum_\omega G^k_l(\mathsf{transfer}^h_j \cdot \mathsf{reset}_\omega) = 0$ and $G^k_l(\mathsf{execute}^i_j) = G^k_l(\mathsf{fetched}^i_j)$, the invariant is preserved when t has the form $\mathsf{finalise}^b$. Using (20), it is in danger only when $t = \mathsf{execute}^i_j$ or $t = \mathsf{transfer}^h_j \cdot \mathsf{reset}_\omega$ for some ω with $\mathsf{transfer}^h_j \in \Omega_\omega$.

First assume $M_1[\mathsf{execute}^i_j\rangle$ and $T^h_j = G_1(\mathsf{transfer}^h_j \cdot \mathsf{fire}) - \sum_\omega G_1(\mathsf{transfer}^h_j \cdot \mathsf{reset}_\omega) = 0$. Then

$$\begin{aligned} 1 &\leq G_1(\mathsf{transfer}^h_j \cdot \mathsf{fire}) - G_1(\mathsf{transfer}^h_j \cdot \mathsf{undo}(\mathsf{trans}^h_j\text{-}\mathsf{out})) && \text{(by (17))} \\ &\leq G_1(\mathsf{transfer}^h_j \cdot \mathsf{fire}) - \textstyle\sum_\omega G_1(\mathsf{transfer}^h_j \cdot \mathsf{reset}_\omega) = 0 && \text{(by (11)),} \end{aligned}$$

which is a contradiction.

Next assume $t = \mathsf{transfer}^h_j \cdot \mathsf{reset}_k$ with $k \overset{\#}{=} j$, and $E^i_j = 1$. By (E) and (G) the latter implies that $G_1(\mathsf{execute}^i_j) = 1$ and $G_1(\mathsf{fetched}^i_j) = 0$. Then

$$\begin{aligned} 0 &= G_1(\mathsf{finalise}^k) && \text{(by (C))} \\ &\leq G_1(\mathsf{transfer}^h_j \cdot \mathsf{elide}_k) + G_1(\mathsf{transfer}^h_j \cdot \mathsf{reset}_k) && \text{(by (9))} \\ &< G(\mathsf{transfer}^h_j \cdot \mathsf{elide}_k) + G(\mathsf{transfer}^h_j \cdot \mathsf{reset}_k) \\ &\leq \textstyle\sum_{l \geq^{\#} k} G(\mathsf{fetched}^k_l) && \text{(by (9)).} \end{aligned}$$

Hence $G_1(\mathsf{fetched}^k_l) = G(\mathsf{fetched}^k_l) > 0$ for some $l \geq^{\#} k$, and by (12) also $G_1(\mathsf{execute}^k_l) > 0$. Using (K) we obtain $(i,j) = (k,l)$, thereby obtaining a contradiction ($0 = G_1(\mathsf{fetched}^i_j) = G_1(\mathsf{fetched}^k_l) > 0$).

(J) Let $j \geq^{\#} i \overset{\#}{=} k \leq^{\#} l \in T'$ with $(i,j) \neq (k,\ell)$. The invariant is in danger only when $t = \mathsf{execute}^i_j$ or $t = \mathsf{execute}^k_l$. W.l.o.g. let $t = \mathsf{execute}^k_l$, with $G_1(\mathsf{execute}^k_l) = 0$ and $G_1(\mathsf{execute}^i_j) \geq 1$.

Making a case distinction, first assume $G(\mathsf{fetched}^i_j) \geq 1$. Using (D), (F) and that $G(\mathsf{execute}^k_l) = 1$, $M'(p) \geq G(\mathsf{distribute}_p) \geq F'(p,k)$ for all $p \in {}^\bullet k$. Likewise, $M'(p) \geq G(\mathsf{distribute}_p) \geq F'(p,i)$ for all $p \in {}^\bullet i$. Moreover, just as in the proof of (F), we derive, for all $p \in {}^\bullet i \cap {}^\bullet k$,

$$\begin{aligned} &M'(p) \geq G(\mathsf{distribute}_p) && \text{(by (D))} \\ &\quad \geq F'(p,k) \cdot \big(G(\mathsf{initialise}_k \cdot \mathsf{fire}) - G(\mathsf{initialise}_k \cdot \mathsf{undone})\big) + \sum_{h \geq^{\#} g \in p^\bullet} F'(p,g) \cdot G(\mathsf{fetch}^{p,k}_{g,h}) && \text{(by (18))} \\ &\quad \geq F'(p,k) \cdot \big(G(\mathsf{initialise}_k \cdot \mathsf{fire}) - G(\mathsf{initialise}_k \cdot \mathsf{undone})\big) + \sum_{h \geq^{\#} g \in p^\bullet} F'(p,g) \cdot G(\mathsf{fetched}^g_h) && \text{(by (12))} \\ &\quad \geq F'(p,k) \cdot \big(G(\mathsf{initialise}_k \cdot \mathsf{fire}) - G(\mathsf{initialise}_k \cdot \mathsf{undone})\big) + F'(p,i) \cdot G(\mathsf{fetched}^i_j) && \text{(by (E))} \\ &\quad \geq F'(p,k) \cdot \big(G(\mathsf{initialise}_k \cdot \mathsf{fire}) - G(\mathsf{initialise}_k \cdot \mathsf{undo}(\mathsf{pre}^k_l))\big) + F'(p,i) \cdot G(\mathsf{fetched}^i_j) && \text{(by (11))} \\ &\quad \geq F'(p,k) + F'(p,i) && \text{(by (16)).} \end{aligned}$$

It follows that $M'[\{k\}+\{i\}\rangle$. As $i \overset{\#}{=} k$ and N' is a finitary structural conflict net, this is impossible. (Note that this argument holds regardless whether $i = k$.)

Now assume $G(\mathsf{fetched}^i_j) \leq 0$. Then, in the notation of (20), $E^i_j = 1$. Since $G_1(\mathsf{execute}^k_l) = 0$, (E) and (12) yield $G_1(\mathsf{fetched}^k_l) = 0$. Hence $G(\mathsf{execute}^k_l) = 1$ and $G(\mathsf{fetched}^k_l) = 0$, so $E^k_l = 1$. We will conclude the proof by deriving a contradiction from $E^i_j = E^k_l = 1$. In case $j = l$ this contradiction emerges immediately from (20). By symmetry it hence suffices to consider the case $j < l$.

By (D) and (H) we have $M'(p) \geq G(\mathsf{distribute}_p) \geq F'(p,j)$ for all $p \in {}^\bullet j$, so $M'[j\rangle$. Likewise $M'[l\rangle$ and, using (F), $M'[i\rangle$ and $M'[k\rangle$. Since $j \overset{\#}{=} i \overset{\#}{=} k$ and N' has no fully reachable pure M, $j \overset{\#}{=} k$. Since $j \overset{\#}{=} k \overset{\#}{=} l$ and N' has no fully reachable pure M, $j \overset{\#}{=} l$. So $j <^{\#} l$. By (20), using that $E^i_j = 1$, $T^j_l = 0$. This is in contradiction with $E^k_l = 1$ and (I).

(K) Suppose that $G(\mathsf{execute}^i_j) > 0$ and $G(\mathsf{execute}^k_l) > 0$, with $i \leq^{\#} j \overset{\#}{=} k \leq^{\#} l \in T'$. By (D) and (H) we have $M'(p) \geq G(\mathsf{distribute}_p) \geq F'(p,j)$ for all $p \in {}^\bullet j$, so $M'[j\rangle$. Likewise, using (F), $M'[i\rangle$ and $M'[k\rangle$. Since $i \overset{\#}{=} j \overset{\#}{=} k$ and N' has no fully reachable pure M, $i \overset{\#}{=} k$. Using this, the result follows from (J). ■

Claim 3 For any $M \in [M_0\rangle_N$ there exist $M' \in [M'_0\rangle_{N'}$ and $G \in_f \mathbb{Z}^T$ satisfying (A)–(K) from Claim 2, and

(L) there are no $j \geq^\# i \overset{\#}{=} k \leq^\# l \in T'$ with $M[\mathsf{execute}^i_j\rangle$ and $G(\mathsf{execute}^k_l) > 0$,

(M) there are no $i \leq^\# j \overset{\#}{=} k \leq^\# l \in T'$ with $M[\mathsf{execute}^i_j\rangle$ and $G(\mathsf{execute}^k_l) > 0$,

(N) if $M[\mathsf{execute}^i_j\rangle$ for $i \leq^\# j \in T'$ then $M'[j\rangle$.

Proof: Given M, by Claim 2(2) there are M' and G so that the triple (M,M',G) satisfies (A)–(K). Assume $M[\mathsf{execute}^i_j\rangle$ for some $i \leq^\# j \in T'$. Let $M_1 := M + [\![\mathsf{execute}^i_j]\!]$ and $G_1 := G + \{\mathsf{execute}^i_j\}$. By (G) $G(\mathsf{execute}^i_j) \geq 0$, so $G_1(\mathsf{execute}^i_j) > 0$. By Claim 2(1) the triple (M_1,M',G_1) satisfies (A)–(K).

(L) Suppose $G(\mathsf{execute}^k_l) > 0$ for certain $l \geq^\# k \overset{\#}{=} i$. In case $(i,j) = (k,\ell)$ we have $G_1(\mathsf{execute}^i_j) \geq 2$, contradicting (G). In case $(i,j) \neq (k,\ell)$, G_1 fails (J), also a contradiction.

(M) Suppose $G(\mathsf{execute}^k_l) > 0$ for certain $l \geq^\# k \overset{\#}{=} j$. Then G_1 fails (G) or (K), a contradiction.

(N) By (D) and (H) $M'(p) \geq G_1(\mathsf{distribute}_p) \geq F(p,j)$ for all $p \in {}^\bullet j$, so $M'[j\rangle$. ■

Claim 4 If $M[\{\mathsf{execute}^i_j\}+\{\mathsf{execute}^k_l\}\rangle$ for some $M \in [M_0\rangle_N$ then $\neg(i \overset{\#}{=} k)$.

Proof: Suppose $M[\{\mathsf{execute}^i_j\}+\{\mathsf{execute}^k_l\}\rangle$ for some $M \in [M_0\rangle_N$. By Claim 2(2) there exist $M' \in [M'_0\rangle_{N'}$ and $G \in_f \mathbb{Z}^T$ satisfying (A)–(K). Let $M_1 := M + [\![\mathsf{execute}^k_l]\!]$ and $G_1 := G + \{\mathsf{execute}^k_l\}$. By Claim 2(1) the triple (M_1,M',G_1) satisfies (A)–(K). Let $M_2 := M_1 + [\![\mathsf{execute}^i_j]\!]$ and $G_2 := G_1 + \{\mathsf{execute}^i_j\}$. Again by Claim 2(1), also the triple (M_2,M',G_2) satisfies (A)–(K). By (G) $G(\mathsf{execute}^i_j) \geq 0$, so in case $(i,j) = (k,l)$ we obtain $G_2(\mathsf{execute}^i_j) \geq 2$, contradicting (G). Hence $(i,j) \neq (k,l)$. Moreover, $G_2(\mathsf{execute}^k_l) > 0$ and $G_2(\mathsf{execute}^i_j) > 0$. Now (J) implies $\neg(i \overset{\#}{=} k)$. ■

For any $t \in \{\mathsf{initialise}_j,\ \mathsf{transfer}^h_j\}$ with $h,j \in T'$, and any $\omega \in \Omega$ with $t \in \Omega_\omega$, we write

$$t(\omega) := t\cdot\mathsf{fire} + t\cdot\mathsf{undo}_\omega + \Big(\sum_{f \in t^{far}} t\cdot\mathsf{undo}(f)\Big) + t\cdot\mathsf{undone} + t\cdot\mathsf{reset}_\omega\ .$$

The transition t has no preplaces of type *in*, nor postplaces of type *out*. By checking in Table 1 or Figure 3 that each other place occurs as often in ${}^\bullet u(\omega) + (u\cdot\mathsf{elide}_\omega)^\bullet$ as in $u(\omega)^\bullet + {}^\bullet(u\cdot\mathsf{elide}_\omega)$, one verifies, for any $\omega \in \Omega$ with $t \in \Omega_\omega$, that

$$[\![t(\omega)]\!] = [\![t\cdot\mathsf{elide}_\omega]\!]. \tag{21}$$

Let $\equiv$ be the congruence relation on finite signed multisets of transitions generated by

$$t(\omega) \quad\equiv\quad t\cdot\mathsf{elide}_\omega \tag{22}$$

for all $t \in \{\mathsf{initialise}_j,\ \mathsf{transfer}^h_j \mid h,j \in T'\}$ and $\omega \in \Omega$ with $\Omega_\omega \ni t$. Here *congruence* means that $G_1 \equiv G_2$ implies $k\cdot G_1 \equiv k\cdot G_2$ and $G_1 + H \equiv G_2 + H$ for all $k \in \mathbb{Z}$ and $H \in_f \mathbb{Z}^T$. Using (21) $G_1 \equiv G_2$ implies $[\![G_1]\!] = [\![G_2]\!]$.

Claim 5 If $M' = [\![G]\!]$ for $M' \in \mathbb{Z}^{S'}$ and $G \in_f \mathbb{Z}^T$ such that for all $i \in T'$ we have $G(\mathsf{finalise}^i) = 0$ and either $\forall j \geq^\# i.\ G(\mathsf{execute}^i_j) \geq 0$ or $\forall j \geq^\# i.\ G(\mathsf{execute}^i_j) \leq 0$, then $G \equiv \emptyset$.

Proof: Let M' and G be as above. W.l.o.g. we assume $G(t\cdot\mathsf{elide}_\omega) = 0$ for all $t \in \{\mathsf{initialise}_j,\ \mathsf{transfer}^h_j\}$ and all $\omega \in \Omega$ with $t \in \Omega_\omega$, for any G can be brought into that form by applying (22). For each $s \in S \setminus S'$ we have $M'(s) = 0$, and using this the inequations (8)–(12) and (18) of Claim 1 turn into equations. For each $i \in T'$ we have $G(\sum_{j \geq^\# i}\mathsf{execute}^i_j) = 0$, using (the equational form of) (8)–(10), and that $G(\mathsf{finalise}^i) = 0$. Since $G(\mathsf{execute}^i_j) \geq 0$ (or ≤ 0) for all $j \geq^\# i$, this implies that $G(\mathsf{execute}^i_j) = 0$ for each $i \leq^\# j \in T'$. With (12) we obtain $G(\mathsf{fetched}^i_j) = G(\mathsf{fetch}^{p,c}_{i,j}) = 0$ for each applicable p,c,i,j. Using that $G(t\cdot\mathsf{elide}_\omega) = 0$ for each applicable t and ω, with (9)–(11) and (18) we find $G(t) = 0$ for all $t \in T$. ■

Claim 6 Let $M := M' + (M_0{-}M'_0) + [\![H]\!] \in [M_0\rangle_N$ for $M' \in [M'_0\rangle_{N'}$ and $H \in_f \mathbb{Z}^T$ with $H(\mathsf{execute}^i_j) = 0$ for all $i \leq^\# j \in T'$.

(a) If $H(\mathsf{finalise}^i) < 0$ and $H(\mathsf{finalise}^k) < 0$ for certain $i,k \in T'$ then $\neg(i \,\#\, k)$.

(b) If $M[\mathsf{execute}^i_j\rangle$ and $H(\mathsf{finalise}^k) < 0$ for certain $i,k \in T'$ then $\neg(i \stackrel{\#}{=} k)$ and $\neg(j \stackrel{\#}{=} k)$.

(c) $H(\mathsf{distribute}_p) \geq 0$ for all $p \in S'$ (with $p^\bullet \neq \emptyset$).

(d) Let $c \stackrel{\#}{=} i \in T'$. If $H(\mathsf{distribute}_p) \geq F'(p,c)$ for all $p \in {}^\bullet c$, then $H(\mathsf{finalise}^i) = 0$.

(e) If $M[\mathsf{execute}^i_j\rangle$ with $i \leq^\# j \in T'$ then $M'[j\rangle$.

Proof: By Claim 3 there exist $M'_1 \in [M'_0\rangle_{N'}$ and $G_1 \in_f \mathbb{Z}^T$ satisfying (B)–(N) (with M, M'_1 and G_1 playing the rôles of M, M' and G). In particular, $M = M'_1 + (M_0 - M'_0) + [\![G_1]\!]$, $G_1(\mathsf{finalise}^i) = 0$ for all $i \in T'$, and $G_1(\mathsf{execute}^i_j) \geq 0$ for all $i \leq^\# j \in T'$. Using (J), for each $i \in T'$ there is at most one $j \geq^\# i$ with $G_1(\mathsf{execute}^i_j) > 0$; we denote this j by $f(i)$, and let $f(i) := i$ when there is no such j. This makes $f : T' \to T'$ a function, satisfying $G_1(\mathsf{execute}^i_j) = 0$ for all $j \geq^\# i$ with $j \neq f(i)$.

Given that $H(\mathsf{execute}^i_j) = 0$ for all $i \leq^\# j \in T'$, (8)–(10) (or (9) and (12)) imply $H(\mathsf{finalise}^i) \leq 0$ for all $i \in T'$. Let $M'_2 := M' + \sum_{i \in T'} H(\mathsf{finalise}^i) \cdot [\![i]\!]$ and $G_2 := H - \sum_{i \in T'} H(\mathsf{finalise}^i) \cdot G^i_{f(i)}$, where G^i_j is the right-hand side of (7). Then $M = M' + (M_0 - M'_0) + [\![H]\!] = M'_2 + (M_0 - M'_0) + [\![G_2]\!]$, using that $[\![i]\!] = [\![G^i_{f(i)}]\!]$. Moreover, $G_2(\mathsf{finalise}^i) = 0$ for all $i \in T'$, using that $G^i_{f(i)}(\mathsf{finalise}^i) = 1$.

It follows that $M'_1 - M'_2 = [\![G_2 - G_1]\!]$. Moreover, we have $(G_2 - G_1)(\mathsf{finalise}^i) = 0$ for all $i \in T'$. We proceed to show that $G_2 - G_1$ satisfies the remaining precondition of Claim 5. So let $i \in T'$. In case $H(\mathsf{finalise}^i) = 0$, for all $j \geq^\# i$ we have $G_2(\mathsf{execute}^i_j) = 0$, and $G_1(\mathsf{execute}^i_j) \geq 0$ by (G). Hence $(G_2 - G_1)(\mathsf{execute}^i_j) \leq 0$. In case $H(\mathsf{finalise}^i) < 0$, we have $G_2(\mathsf{execute}^i_{f(i)}) \geq 1$, and hence, using (G), $(G_2 - G_1)(\mathsf{execute}^i_{f(i)}) \geq 0$. Furthermore, for all $j \neq f(i)$, $G_2(\mathsf{execute}^i_j) \geq 0$ and $G_1(\mathsf{execute}^i_j) = 0$, so again $(G_2 - G_1)(\mathsf{execute}^i_j) \geq 0$.

Thus we may apply Claim 5, which yields $G_2 \equiv G_1$. It follows that $M'_2 = M'_1 \in [M'_0\rangle_{N'}$.

(a) Suppose that $H(\mathsf{finalise}^i) < 0$ and $H(\mathsf{finalise}^k) < 0$ for certain $i \,\#\, k \in T'$. Then $G_2(\mathsf{execute}^i_{f(i)}) > 0$ and $G_2(\mathsf{execute}^k_{f(k)}) > 0$, so $G_1(\mathsf{execute}^i_{f(i)}) > 0$ and $G_1(\mathsf{execute}^k_{f(k)}) > 0$, contradicting (J).

(b) Suppose that $M[\mathsf{execute}^i_j\rangle$ and $H(\mathsf{finalise}^k) < 0$ for certain $k \stackrel{\#}{=} i$ or $k \stackrel{\#}{=} j$. Then $G_1(\mathsf{execute}^k_{f(k)}) = G_2(\mathsf{execute}^k_{f(k)}) > 0$, contradicting (L) or (M).

(c) By (a), for any given $p \in S'$ there is at most one $i \in p^\bullet$ with $H(\mathsf{finalise}^i) < 0$. For all $i \in T'$ with $i \notin p^\bullet$ we have $G^i_{f(i)}(\mathsf{distribute}_p) = 0$. First suppose $k \in p^\bullet$ satisfies $H(\mathsf{finalise}^k) < 0$. Then

$$\begin{aligned} G_1(\mathsf{execute}^k_{f(k)}) &= G_2(\mathsf{execute}^k_{f(k)}) \\ &= H(\mathsf{execute}^k_{f(k)}) - \textstyle\sum_{i \in T'} H(\mathsf{finalise}^i) \cdot G^i_{f(i)}(\mathsf{execute}^k_{f(k)}) \\ &= 0 - H(\mathsf{finalise}^k), \end{aligned}$$

so by (F) $G_1(\mathsf{distribute}_p) \geq -F'(p,k) \cdot H(\mathsf{finalise}^k)$. Hence

$$\begin{aligned} H(\mathsf{distribute}_p) &= G_2(\mathsf{distribute}_p) + \textstyle\sum_{i \in T'} H(\mathsf{finalise}^i) \cdot G^i_{f(i)}(\mathsf{distribute}_p) \\ &= G_1(\mathsf{distribute}_p) + H(\mathsf{finalise}^k) \cdot G^k_{f(k)}(\mathsf{distribute}_p) \\ &\geq -F'(p,k) \cdot H(\mathsf{finalise}^k) + H(\mathsf{finalise}^k) \cdot F'(p,k) = 0. \end{aligned}$$

In case there is no $i \in p^\bullet$ with $H(\mathsf{finalise}^i) < 0$ we have

$$H(\mathsf{distribute}_p) = G_2(\mathsf{distribute}_p) + \sum_{i \in T'} H(\mathsf{finalise}^i) \cdot G^i_{f(i)}(\mathsf{distribute}_p) = G_1(\mathsf{distribute}_p) \geq 0$$

by (F) and (G).

(d) Since $H(\mathsf{finalise}^i) \leq 0$ and $G^i_{f(i)}(\mathsf{distribute}_p) \geq 0$ for all $i \in T'$, also using (c), all summands in $H(\mathsf{distribute}_p) + \sum_{i \in T'} -H(\mathsf{finalise}^i) \cdot G^i_{f(i)}(\mathsf{distribute}_p)$ are positive. Now suppose $H(\mathsf{finalise}^i) < 0$ for certain $i \in T'$. Then, using (D), for all $p \in {}^\bullet i$,

$$M'_1(p) \geq G_1(\mathsf{distribute}_p) = G_2(\mathsf{distribute}_p) \geq G^i_{f(i)}(\mathsf{distribute}_p) = F'(p,i).$$

Furthermore, let $c \overset{\#}{=} i$ and suppose $H(\mathsf{distribute}_p) \geq F'(p,c)$ for all $p \in {}^\bullet c$. Then, using (D),

$$M'_1(p) \geq G_1(\mathsf{distribute}_p) = G_2(\mathsf{distribute}_p) \geq H(\mathsf{distribute}_p) \geq F'(p,c)$$

for all $p \in {}^\bullet c$. Moreover, if $p \in {}^\bullet c \cap {}^\bullet i$ then

$$M'_1(p) \geq G_2(\mathsf{distribute}_p) \geq H(\mathsf{distribute}_p) + G^i_{f(i)}(\mathsf{distribute}_p) \geq F'(p,c) + F'(p,i).$$

Hence $M'_2[\{c\}+\{i\}\rangle$. However, since $c \overset{\#}{=} i$ and N' is a structural conflict net, this is impossible.

(e) Suppose $M[\mathsf{execute}^i_j\rangle$ with $i \leq^\# j \in T'$. Then $M'_1[j\rangle$ by (N). Now $M' = M'_1 + \sum_{k \in T'} -H(\mathsf{finalise}^k) \cdot [\![k]\!]$, with $-H(\mathsf{finalise}^k) \geq 0$ for all $k \in T'$. Whenever $-H(\mathsf{finalise}^k) > 0$ then $\neg(j \overset{\#}{=} k)$ by (b). Hence $M'[j\rangle$. ■

We now define the class $NF \subseteq \mathbb{Z}^T$ of signed multisets of transitions in *normal form* by $H \in NF$ iff $\ell(H) \equiv \emptyset$ and, for all $t \in \{\mathsf{initialise}_j,\ \mathsf{transfer}^h_j \mid h, j \in T'\}$:

(NF-1) $H(t \cdot \mathsf{elide}_\omega) \leq 0$ for each $\omega \in \Omega$,

(NF-2) $H(t \cdot \mathsf{undo}_\omega) \geq 0$ for each $\omega \in \Omega$, or $H(t \cdot \mathsf{fire}) \geq 0$,

(NF-3) and if $H(t \cdot \mathsf{elide}_\omega) < 0$ for any $\omega \in \Omega$, then $H(t \cdot \mathsf{undo}_\omega) \leq 0$ and $H(t \cdot \mathsf{fire}) \leq 0$.

We proceed verifying the remaining conditions of Theorem 3.

4. By applying (22), each signed multiset $G \in_f \mathbb{Z}^T$ with $\ell(G) \equiv \emptyset$ can be converted into a signed multiset $H \in_f NF$ with $\ell(H) \equiv \emptyset$, such that $[\![H]\!] = [\![G]\!]$. Namely, for any $t \in \{\mathsf{initialise}_j,\ \mathsf{transfer}^h_j \mid h, j \in T'\}$, first of all perform the following three transformations, until none is applicable:

   (i) correct a positive count of a transition $t \cdot \mathsf{elide}_\omega$ in G by adding $t(\omega) - t \cdot \mathsf{elide}_\omega$ to G;

   (ii) if both $H(t \cdot \mathsf{undo}_\omega) < 0$ for some ω and $H(t \cdot \mathsf{fire}) < 0$, correct this in the same way;

   (iii) and if, for some ω, $t{\cdot}\mathsf{elide}_\omega$ has a negative and $t{\cdot}\mathsf{undo}_\omega$ a positive count, add $t \cdot \mathsf{elide}_\omega - t(\omega)$.

   Note that transformation (iii) will never be applied to the same ω as (i) or (ii), so termination is ensured. Properties (NF-1) and (NF-2) then hold for t. After termination of (i)–(iii), perform

   (iv) if, for some ω, $H(t \cdot \mathsf{elide}_\omega) < 0$ and $H(t \cdot \mathsf{fire}) > 0$, add $t \cdot \mathsf{elide}_\omega - t(\omega)$.

   This will ensure that also (NF-3) is satisfied, while preserving (NF-1) and (NF-2).

   Define the function $f : T \rightarrow \mathbb{N}$ by $f(u) := 1$ for all $u \in T$ not of the form $u = t \cdot \mathsf{elide}_\omega$, and $f(t \cdot \mathsf{elide}_\omega) := f(t(\omega))$ (applying the last item of Definition 1). Then surely $f(G) = f(H)$.

5. Let $M' \in \mathbb{N}^{S'}$, $U' \in \mathbb{N}^{T'}$ and $U \in \mathbb{N}^T$ with $\ell(U) = \ell'(U')$ and $M' + {}^\bullet U' \in [M'_0\rangle_{N'}$. Since N' is a finitary structural conflict net, it admits no self-concurrency, so, as ${}^\bullet U' \leq M' + {}^\bullet U' \in [M'_0\rangle_{N'}$, the multiset U' must be a set. As N' is plain, this implies that the multiset $\ell'(U')$ is a set. Since $\ell(U) = \ell'(U')$, also $\ell(U)$, and hence U, must be a set. All its elements have the form $\mathsf{execute}^i_j$ for $i \leq^\# j \in T'$, since these are the only transitions in T with visible labels. Note that U' is completely determined by U, namely by $U' = \{i \mid \exists j.\ \mathsf{execute}^i_j \in U\}$. We take

$$H_{M',U} := \sum_{p\in S'} (M'+{}^\bullet U')(p)\cdot\{\mathsf{distribute}_p\} + \sum_{(M'+{}^\bullet U')[j\rangle} \left(\{\mathsf{initialise}_j\cdot\mathsf{fire}\} + \sum_{h<^\# j,\ \nexists\mathsf{execute}^g_h\in U} \{\mathsf{transfer}^h_j\cdot\mathsf{fire}\}\right)$$

Since N' is finitary, $H_{M',U}\in_f \mathbb{N}^{T^+}$. Moreover, $\ell(H_{M',U})\equiv\emptyset$.

Let $H\in_f NF$ with $M := M'+{}^\bullet U'+(M_0-M'_0)+[\![H]\!]-{}^\bullet U\in\mathbb{N}^S$ and $M+{}^\bullet U\in[M_0\rangle_N$. Since $H\in NF$, and thus $\ell(H)\equiv\emptyset$, $H(\mathsf{execute}^i_j)=0$. From here on we apply Claim 1 and Claim 6 with $M+{}^\bullet U$ and $M'+{}^\bullet U'$ playing the rôles of M and M'. Note that the preconditions of these claims are met.

That $H(\mathsf{execute}^i_j)=0$ for all $i\leq^\# j\in T'$, together with (8) and the requirements (NF-1) and (NF-3) for normal forms, yields $H(t\cdot\mathsf{elide}_i)\leq 0$ as well as $H(t\cdot\mathsf{undo}_i)\leq 0$. Using this, (9)–(12) imply that

$$H(u)\leq 0 \quad\text{for each}\quad u\in T^-. \tag{23}$$

Claim 7 Let $c\in T'$ and $p\in{}^\bullet c$. Then

- if $H(\mathsf{initialise}_c\cdot\mathsf{fire})>0$ then $H(\mathsf{fetch}^{p,c}_{i,j})=0$ for all $i\in p^\bullet$ and $j\geq^\# i$, and
- if $H(\mathsf{transfer}^b_c\cdot\mathsf{fire})>0$ for some $b<^\# c$ then $H(\mathsf{fetch}^{p,c}_{i,j})=0$ for all $i\in p^\bullet$ and $j\geq^\# i$.

Proof: Suppose that $H(t\cdot\mathsf{fire})>0$, for $t=\mathsf{initialise}_c$ or $t=\mathsf{transfer}^b_c$. Then (13) resp. (20) together with (23) implies that $H(t\cdot\mathsf{reset}_\omega)=0$ for each ω with $t\in\Omega_\omega$. In order words, $H(t\cdot\mathsf{reset}_i)=0$ for each $i\overset{\#}{=}c$, so in particular for each $i\in p^\bullet$. Furthermore, $H(t\cdot\mathsf{elide}_i)\geq 0$, by requirement (NF-3) of normal forms. With (9), this yields $\sum_{j\geq^\# i}H(\mathsf{fetched}^i_j)\geq 0$, and (23) implies $H(\mathsf{fetched}^i_j)=0$ for each $j\geq^\# i$. Now (12, 23) gives $H(\mathsf{fetch}^{p,c}_{i,j})=0$ for each $j\geq^\# i\in p^\bullet$. ■

We proceed to verify the requirements (5a)–(5g) of Theorem 3.

(5a) To show that $M_{M',U}\in\mathbb{N}^S$, it suffices to apply it to the preplaces of transitions in $H_{M',U}+U$:

$$\begin{array}{lcll}
M_{M',U}(p) & = & 0 & \text{for all } p\in S'\,;\\
M_{M',U}(p_j) & = & \begin{cases}(M'+{}^\bullet U')(p)-F'(p,j) & \text{if } (M'+{}^\bullet U')[j\rangle\\ (M'+{}^\bullet U')(p) & \text{otherwise}\end{cases} & \text{for } p\in S',\ j\in p^\bullet;\\
M_{M',U}(\pi_j) & = & \begin{cases}0 & \text{if } (M'+{}^\bullet U')[j\rangle\\ 1 & \text{otherwise}\end{cases} & \text{for } j\in T';\\
M_{M',U}(\mathsf{pre}^j_k) & = & \begin{cases}1 & \text{if } (M'+{}^\bullet U')[j\rangle\wedge\mathsf{execute}^j_k\notin U\\ -1 & \text{if } \neg(M'+{}^\bullet U')[j\rangle\wedge\mathsf{execute}^j_k\in U\\ 0 & \text{otherwise}\end{cases} & \text{for } j\leq^\# k\in T';\\
M_{M',U}(\pi_{h\#j}) & = & \begin{cases}0 & \text{if } \exists\mathsf{execute}^g_h\in U\vee(M'+{}^\bullet U')[j\rangle\\ 1 & \text{otherwise}\end{cases} & \text{for } h<^\# j\in T'\\
M_{M',U}(\mathsf{trans}^h_j\text{-in}) & = & \begin{cases}1 & \text{if } (M'+{}^\bullet U')[j\rangle\wedge\exists\mathsf{execute}^g_h\in U\\ 0 & \text{otherwise}\end{cases} & \text{for } h<^\# j\in T';\\
M_{M',U}(\mathsf{trans}^h_j\text{-out}) & = & \begin{cases}1 & \text{if } (M'+{}^\bullet U')[j\rangle\wedge\nexists\mathsf{execute}^g_h\in U\wedge\nexists\mathsf{execute}^i_j\in U\\ -1 & \text{if } \big(\neg(M'+{}^\bullet U')[j\rangle\vee\exists\mathsf{execute}^g_h\in U\big)\wedge\exists\mathsf{execute}^i_j\in U\\ 0 & \text{otherwise}\end{cases} & \text{for } h<^\# j\in T'.
\end{array}$$

For all these places s we indeed have that $M_{M',U}(s)\geq 0$, for the circumstances yielding the two exceptions above cannot occur:

- Suppose $\mathsf{execute}^j_k\in U$ with $j\leq^\# k\in T'$. Then $j\in U'$, so ${}^\bullet j\subseteq M'+{}^\bullet U'$ and $(M'+{}^\bullet U')[j\rangle$. Consequently, $M_{M',U}(\mathsf{pre}^j_k)\neq -1$ for all $j\leq^\# k\in T'$.

- Suppose $\mathsf{execute}^i_j \in U$ with $i \leq^\# j \in T'$. Then ${}^\bullet\mathsf{execute}^i_j \leq {}^\bullet U$, so $(M + {}^\bullet U)[\mathsf{execute}^i_j\rangle$. Claim 6(e) with $M + {}^\bullet U$ and $M' + {}^\bullet U'$ in the rôles of M and M' yields $(M' + {}^\bullet U')[j\rangle$.
  If moreover $\mathsf{execute}^g_h \in U$ with $g \leq^\# h <^\# j$, then $\{g\}+\{i\} \subseteq U'$, so ${}^\bullet\{g\}+{}^\bullet\{i\} \subseteq M'+{}^\bullet U'$ and $(M' + {}^\bullet U')[\{g\}+\{i\}\rangle$. In particular, $g \smile i$, and since N' is a structural conflict net, ${}^\bullet g \cap {}^\bullet i = \emptyset$. By Claim 6(e)—as above—$(M'+{}^\bullet U')[h\rangle$, so ${}^\bullet g \cup {}^\bullet h \cup {}^\bullet j \cup {}^\bullet i \subseteq M'+{}^\bullet U' \in [M'_0\rangle_{N'}$. Moreover, since $g \leq^\# h <^\# j \geq^\# i$, we have ${}^\bullet g \cap {}^\bullet h \neq \emptyset$, ${}^\bullet h \cap {}^\bullet i \neq \emptyset$ and ${}^\bullet i \cap {}^\bullet j \neq \emptyset$. Now in case also ${}^\bullet h \cap {}^\bullet i \neq \emptyset$, the transitions g, h and i constitute a fully reachable pure M; otherwise $h \smile i$ and h, j and i constitute a fully reachable pure M. Either way, we obtain a contradiction. Consequently, $M_{M',U}(\mathsf{trans}^h_j\text{-}\mathsf{out}) \neq -1$ for all $h <^\# j \in T'$.

(5b) Suppose $M' \xrightarrow{a}$; say $M'[i\rangle$ with $\ell'(i) = a$. Let j be the largest transition in T' w.r.t. the well-ordering $<$ on T such that $i \leq^\# j$ and $(M' + {}^\bullet U')[j\rangle$. It suffices to show that $M_{M',U}[\mathsf{execute}^i_j\rangle$, i.e. that $M_{M',U}(\mathsf{pre}^i_j){=}1$, $M_{M',U}(\mathsf{trans}^h_j\text{-}\mathsf{out}){=}1$ for all $h <^\# j$, and $M_{M',U}(\pi_{j\#l}){=}1$ for all $l >^\# j$. If $\mathsf{execute}^i_j \in U$ we would have $i \in U'$ and hence $(M' + {}^\bullet U')[2 \cdot \{i\}\rangle$. Since N' is a finitary structural conflict net, this is impossible. Therefore $\mathsf{execute}^i_j \notin U$ and, using the calculations from (a) above, $M_{M',U}(\mathsf{pre}^i_j) = 1$.

Let $h <^\# j$. To establish that $M_{M',U}(\mathsf{trans}^h_j\text{-}\mathsf{out}) = 1$ we need to show that there is no $k \leq^\# j$ with $\mathsf{execute}^k_j \in U$ and no $g \leq^\# h$ with $\mathsf{execute}^g_h \in U$. First suppose $\mathsf{execute}^k_j \in U$ for some $k \leq^\# j$. Then $k \in U'$ and hence $(M' + {}^\bullet U')[\{i\}+\{k\}\rangle$. This implies $i \smile k$, and, as N' is a structural conflict net, ${}^\bullet i \cap {}^\bullet k = \emptyset$. Hence the transitions i, j and k are all different, with ${}^\bullet i \cap {}^\bullet j \neq \emptyset$ and ${}^\bullet j \cap {}^\bullet k \neq \emptyset$ but ${}^\bullet i \cap {}^\bullet k = \emptyset$. Moreover, the reachable marking $M' + {}^\bullet U'$ enables all three of them. Hence N' contains a fully reachable pure M, which contradicts the assumptions of Theorem 5. Next suppose $\mathsf{execute}^g_h \in U$ for some $g \leq^\# h$. Then $(M + {}^\bullet U)[\mathsf{execute}^g_h\rangle$, so $(M' + {}^\bullet U')[h\rangle$ by Claim 6(e). Moreover, $g \in U'$, so $(M' + {}^\bullet U')[\{i\}+\{g\}\rangle$. This implies $g \smile i$, and ${}^\bullet g \cap {}^\bullet i = \emptyset$. Moreover, ${}^\bullet g \cap {}^\bullet h \neq \emptyset$, ${}^\bullet h \cap {}^\bullet j \neq \emptyset$ and ${}^\bullet j \cap {}^\bullet i \neq \emptyset$, while the reachable marking $M' + {}^\bullet U'$ enables all these transitions. Depending on whether ${}^\bullet h \cap {}^\bullet i = \emptyset$, either h, j and i, or g, h and i constitute a fully reachable pure M, contradicting the assumptions of Theorem 5.

Let $l >^\# j$. To establish that $M_{M',U}(\pi_{j\#l}) = 1$ we need to show that there is no $k \leq^\# j$ with $\mathsf{execute}^k_j \in U$—already done above—and that $\neg(M' + {}^\bullet U')[l\rangle$. Suppose $(M' + {}^\bullet U')[l\rangle$. Considering that j was the largest transition with $i \leq^\# j$ and $(M' + {}^\bullet U')[j\rangle$, we cannot have $i <^\# l$. Hence the transitions i, j and l are all different, with ${}^\bullet i \cap {}^\bullet j \neq \emptyset$ and ${}^\bullet j \cap {}^\bullet l \neq \emptyset$ but ${}^\bullet i \cap {}^\bullet l = \emptyset$. Moreover, the reachable marking $M' + {}^\bullet U'$ enables all three of them. Hence N' contains a fully reachable pure M, which contradicts the assumptions of Theorem 5.

(5c) We have to show that $H(t) \leq H_{M',U}(t)$ for each $t \in T$.

- In case $t \in T^-$ this follows from (23) and $H_{M',U} \in \mathbb{N}^{T^+}$.
- In case $t = \mathsf{execute}^i_j$ it follows since $\ell(H) \equiv \emptyset$.
- In case $t = \mathsf{distribute}_p$ it follows from (19) and (23).
- Next let $t = \mathsf{initialise}_c \cdot \mathsf{fire}$ for some $c \in T'$. In case $H(\mathsf{initialise}_c \cdot \mathsf{fire}) \leq 0$ surely we have $H(\mathsf{initialise}_c \cdot \mathsf{fire}) \leq H_{M',U}(\mathsf{initialise}_c \cdot \mathsf{fire})$. So without limitation of generality we may assume that $H(\mathsf{initialise}_c \cdot \mathsf{fire}) > 0$. By (13,23) we have $H(\mathsf{initialise}_c \cdot \mathsf{fire}) = 1$. Using (18), Claim 7, (23) and (19) we obtain, for all $p \in {}^\bullet c$,

  $$F'(p,c) \cdot H(\mathsf{initialise}_c \cdot \mathsf{fire}) \leq H(\mathsf{distribute}_p) \leq (M' + {}^\bullet U')(p).$$

  Hence c is enabled under $M' + {}^\bullet U'$, which implies $H_{M',U}(\mathsf{initialise}_c \cdot \mathsf{fire}) = 1$.
- Let $t = \mathsf{transfer}^b_c \cdot \mathsf{fire}$ for some $b <^\# c \in T'$. As above, we may assume $H(\mathsf{transfer}^b_c \cdot \mathsf{fire}) > 0$. By (20,23) we have $H(\mathsf{transfer}^b_c \cdot \mathsf{fire}) = 1$. Using (23) and that $H(\mathsf{execute}^g_b) = 0$ for all

$g \leq^{\#} b$, it follows that $(M+{}^\bullet U)(\pi_{b\#c}) = 0$. Hence $\neg(M+{}^\bullet U)[\mathsf{execute}^g_b\rangle$ for all $g \leq^{\#} b$, and thus $\nexists \mathsf{execute}^g_b \in U$. For all $p \in {}^\bullet c$ we derive

$$\begin{array}{lll}
\multicolumn{2}{l}{F'(p,c)\cdot H(\mathsf{transfer}^b_c\cdot\mathsf{fire})} & \\
\leq & F'(p,c)\cdot\big(H(\mathsf{transfer}^b_c\cdot\mathsf{fire}) - H(\mathsf{transfer}^b_c\cdot\mathsf{undone})\big) & (23)\\
\leq & F'(p,c)\cdot\big(H(\mathsf{initialise}_c\cdot\mathsf{fire}) - H(\mathsf{initialise}_c\cdot\mathsf{undo}(\mathsf{trans}^b_c\text{-}\mathsf{in}))\big) & (14)\\
\leq & F'(p,c)\cdot\big(H(\mathsf{initialise}_c\cdot\mathsf{fire}) - H(\mathsf{initialise}_c\cdot\mathsf{undone})\big) & (11)\\
= & [\text{the same as above}] + \sum_{j\geq^{\#} i\in p^\bullet} F'(p,i)\cdot H(\mathsf{fetch}^{p,c}_{i,j}) & (\text{Claim } 7)\\
\leq & H(\mathsf{distribute}_p) & (18)\\
\leq & (M'+{}^\bullet U')(p) + \sum_{\{i\in T'\mid p\in i^\bullet\}} H(\mathsf{finalise}^i) & (19)\\
\leq & (M'+{}^\bullet U')(p) & (23).
\end{array}$$

Hence $(M'+{}^\bullet U')[c\rangle$, and thus $H_{M',U}(\mathsf{transfer}^b_c) = 1$.

(5d) If $u \notin T^-$, yet $H(u) \neq 0$, then u is either $\mathsf{distribute}_p$, $\mathsf{initialise}_j\cdot\mathsf{fire}$ or $\mathsf{transfer}^h_j\cdot\mathsf{fire}$ for suitable $p \in S'$ or $h,j \in T'$. For $u = \mathsf{distribute}_p$ the requirement follows from Claim 6(c); otherwise Property (NF-2), together with (11), guarantees that $H(u) \geq 0$.

(5e) If $H(t) > 0$ and $H(u) < 0$, then $t \in T^+$ and $u \in T^-$. The only candidates for ${}^\bullet t \cap {}^\bullet u \neq \emptyset$ are

- $p_c \in {}^\bullet(\mathsf{initialise}_c\cdot\mathsf{fire}) \cap {}^\bullet(\mathsf{fetch}^{p,c}_{i,j})$ for $p \in S'$, $c,i \in p^\bullet$ and $j \geq^{\#} i$,
- $\mathsf{trans}^b_c\text{-}\mathsf{in} \in {}^\bullet(\mathsf{transfer}^b_c\cdot\mathsf{fire}) \cap {}^\bullet(\mathsf{initialise}_c\cdot\mathsf{undo}(\mathsf{trans}^b_c\text{-}\mathsf{in}))$ for $b \leq^{\#} c \in T'$.

We investigate these possibilities one by one.

- $H(\mathsf{initialise}_c\cdot\mathsf{fire}) > 0 \wedge H(\mathsf{fetch}^{p,c}_{i,j}) < 0$ cannot occur by Claim 7.
- Suppose $H(\mathsf{transfer}^b_c\cdot\mathsf{fire}) > 0$. By (20, 23) we have $H(\mathsf{transfer}^b_c\cdot\mathsf{fire}) = 1$. Through the derivation above, in the proof of requirement (c), using (23, 14, 11), Claim 7 and (18), we obtain $H(\mathsf{distribute}_p) \geq F'(p,c)$ for all $p \in {}^\bullet c$. Now Claim 6(d) yields $H(\mathsf{finalise}^i) = 0$ for all $i \overset{\#}{=} c$. By (9) and (23) we obtain $H(\mathsf{initialise}_c\cdot\mathsf{reset}_i) = 0$ for each such i. Hence $\sum_{i\overset{\#}{=}c} H(\mathsf{initialise}_c\cdot\mathsf{reset}_i) = 0$, and thus $H(\mathsf{initialise}_c\cdot\mathsf{undo}(\mathsf{trans}^b_c\text{-}\mathsf{in})) = 0$ by (11, 23).

(5f) If $H(u) < 0$ and $(M+{}^\bullet U)[t\rangle$ with $\ell(t) \neq \tau$, then $t = \mathsf{execute}^i_j$ for some $i \leq^{\#} j \in T'$ and $u \in T^-$. The only candidates for ${}^\bullet t \cap {}^\bullet u \neq \emptyset$ are

- $\mathsf{pre}^i_j \in {}^\bullet(\mathsf{execute}^i_j) \cap {}^\bullet(\mathsf{initialise}_j\cdot\mathsf{undo}(\mathsf{pre}^i_j))$ and
- $\mathsf{trans}^h_j\text{-}\mathsf{out} \in {}^\bullet(\mathsf{execute}^i_j) \cap {}^\bullet(\mathsf{transfer}^h_j\cdot\mathsf{undo}(\mathsf{trans}^h_j\text{-}\mathsf{out}))$ for $h <^{\#} j$.

We investigate these possibilities one by one.

- Suppose $(M+{}^\bullet U)[\mathsf{execute}^i_j\rangle$. By Claim 6(b), $H(\mathsf{finalise}^k) \geq 0$ for each $k \overset{\#}{=} i$. By (9) and (23) we obtain $H(\mathsf{initialise}_i\cdot\mathsf{reset}_k) = 0$ for each such k. Hence $\sum_{k\overset{\#}{=}i} H(\mathsf{initialise}_i\cdot\mathsf{reset}_k) = 0$, and thus $H(\mathsf{initialise}_i\cdot\mathsf{undo}(\mathsf{pre}^i_j)) = 0$ by (11, 23).
- Suppose $(M+{}^\bullet U)[\mathsf{execute}^i_j\rangle$ and $h <^{\#} j$. By Claim 6(b), $H(\mathsf{finalise}^k) \geq 0$ for each $k \overset{\#}{=} j$. By (9) and (23) $H(\mathsf{transfer}^h_j\cdot\mathsf{reset}_k) = 0$ for each such k. So $\sum_{k\overset{\#}{=}j} H(\mathsf{transfer}^h_j\cdot\mathsf{reset}_k) = 0$, and $H(\mathsf{transfer}^h_j\cdot\mathsf{undo}(\mathsf{trans}^h_j\text{-}\mathsf{out})) = 0$ by (11, 23).

(5g) Suppose $(M+{}^\bullet U)[\{t\}+\{u\}\rangle_N$, and $i,k \in T'$ with $\ell'(i) = \ell(t)$ and $\ell'(k) = \ell(u)$. Since the net N' is plain, t and u must have the form $\mathsf{execute}^i_j$ and $\mathsf{execute}^k_j$ for some $j >^{\#} i$ and $l >^{\#} k$. Claim 4 yields $\neg(i \overset{\#}{=} k)$ and hence ${}^\bullet i \cap {}^\bullet k = \emptyset$. □

Thus, we have established that the conflict replicating implementation $\mathscr{I}(N')$ of a finitary plain structural conflict net N' without a fully reachable pure M is branching ST-bisimilar with explicit divergence to N'. It remains to be shown that $\mathscr{I}(N')$ is essentially distributed.

Lemma 10 Let N be the conflict replicating implementation of a finitary net $N' = (S',T',F',M_0',\ell')$; let $j,l \in T'$, with $l >^{\#} j$. Then no two transitions from the set $\{\mathsf{execute}_j^i \mid i \leq^{\#} j\} \cup \{\mathsf{transfer}_l^j \cdot \mathsf{fire}\} \cup \{\mathsf{transfer}_l^j \cdot \mathsf{undo}(\mathsf{trans}_l^j\text{-}\mathsf{out})\} \cup \{\mathsf{execute}_l^k \mid k \leq^{\#} l\}$ can fire concurrently.

Proof: For each $i \leq^{\#} j$ pick an arbitrary preplace q_i of i. The set $\{\mathsf{fetch}_{i,j}^{q_i,i}\text{-}\mathsf{in},\ \mathsf{fetch}_{i,j}^{q_i,i}\text{-}\mathsf{out} \mid i \leq^{\#} j\} \cup \{\pi_{j\#l},\ \mathsf{trans}_l^j\text{-}\mathsf{out},\ \mathsf{took}(\mathsf{trans}_l^j\text{-}\mathsf{out},\mathsf{transfer}_l^j),\ \rho(\mathsf{transfer}_l^j\}$ is an *S-invariant*: there is always exactly one token in this set. This is the case because each transition from N has as many preplaces as postplaces in this set. The transitions from $\{\mathsf{execute}_j^i \mid i \leq^{\#} j\} \cup \{\mathsf{transfer}_l^j \cdot \mathsf{fire}\} \cup \{\mathsf{transfer}_l^j \cdot \mathsf{undo}(\mathsf{trans}_l^j\text{-}\mathsf{out})\} \cup \{\mathsf{execute}_l^k \mid k \leq^{\#} l\}$ each have a preplace in this set. Hence no two of them can fire concurrently. □

Lemma 11 Let N be the conflict replicating implementation $\mathscr{I}(N')$ of a finitary plain structural conflict net $N' = (S',T',F',M_0',\ell')$ without a fully reachable pure M. Then for any $i \leq^{\#} j \overset{\#}{=} c \in T'$ and $f \in (\mathsf{initialise}_c)^{far}$, the transitions $\mathsf{execute}_j^i$ and $\mathsf{initialise}_c \cdot \mathsf{undo}(f)$ cannot fire concurrently.

Proof: Suppose these transitions can fire concurrently, say from the marking $M \in [M_0\rangle_N$. By Claim 3, there are $M' \in [M_0'\rangle_{N'}$ and $G \in_f \mathbb{Z}^T$ such that (B)–(N) hold. Let $t := \mathsf{initialise}_c$, $G_1 := G + \{t \cdot \mathsf{undo}(f)\}$ and $M_1 := M + [\![t\cdot\mathsf{undo}(f)]\!]$. Then (11), applied to the triples (M,M',G) and (M_1,M',G_1), yields

$$\sum_{\{\omega \mid t\in\Omega_\omega\}} G(t\cdot\mathsf{reset}_\omega) \leq G(t\cdot\mathsf{undo}(f)) < G_1(t\cdot\mathsf{undo}(f)) \leq \sum_{\{\omega \mid t\in\Omega_\omega\}} G_1(t\cdot\mathsf{undo}_\omega) = \sum_{\{\omega \mid t\in\Omega_\omega\}} G(t\cdot\mathsf{undo}_\omega).$$

Hence, there is an ω with $t \in \Omega_\omega$ and $G(t\cdot\mathsf{reset}_\omega) < G(t\cdot\mathsf{undo}_\omega)$. This ω must have the form $k \in T'$ with $k \overset{\#}{=} c$. We now obtain

$$\begin{array}{rll} 0 = & G(\mathsf{finalise}^k) & \text{(by (C))} \\ \leq & G(t\cdot\mathsf{elide}_k) + G(t\cdot\mathsf{reset}_k) & \text{(by (9))} \\ < & G(t\cdot\mathsf{elide}_k) + G(t\cdot\mathsf{undo}_k) & \\ \leq & \sum_{l\geq^{\#}k} G(\mathsf{execute}_l^k) & \text{(by (8)).} \end{array}$$

Hence, there is an $l \geq^{\#} k \overset{\#}{=} c$ with $G(\mathsf{execute}_l^k) > 0$. By (M) we obtain $\neg(j \overset{\#}{=} k)$, so ${}^\bullet j \cap {}^\bullet k = \emptyset$. Additionally, we have ${}^\bullet j \cap {}^\bullet c \neq \emptyset$ and ${}^\bullet c \cap {}^\bullet k \neq \emptyset$. By (N) we obtain $M'[j\rangle$, and by (D) and (F) $M'[k\rangle$. Furthermore, by (11), $G(t\cdot\mathsf{undo}(f)) < G_1(t\cdot\mathsf{undo}(f)) \leq G_1(t\cdot\mathsf{fire}) = G(t\cdot\mathsf{fire})$, so, for all $p \in {}^\bullet c$,

$$\begin{array}{rlll} F'(p,c) & \leq & F'(p,c)\cdot\big(G(t\cdot\mathsf{fire}) - G(t\cdot\mathsf{undo}(f))\big) & \\ & \leq & F'(p,c)\cdot\big(G(t\cdot\mathsf{fire}) - G(t\cdot\mathsf{undone})\big) & \text{(by (11))} \\ & \leq & G(\mathsf{distribute}_p) - \sum_{j\geq^{\#}i\in p^\bullet} F'(p,i)\cdot G(\mathsf{fetch}_{i,j}^{p,c}) & \text{(by (18))} \\ & \leq & G(\mathsf{distribute}_p) & \text{(by (E) and (12))} \\ & \leq & M'(p) & \text{(by (D).} \end{array}$$

It follows that $M'[c\rangle$. Thus N' contains a fully reachable pure M, which contradicts the assumptions of Lemma 11. □

Theorem 6 Let N be the conflict replicating implementation $\mathscr{I}(N')$ of a finitary plain structural conflict net N' without a fully reachable pure M. Then N is essentially distributed.

Proof: We take the canonical distribution D of N, in which $\equiv_D$ is the equivalence relation on places and transitions generated by Condition (1) of Definition 15. We need to show that this distribution satisfies Condition (2′) of Definition 16. A given transition t with $\ell(t) \neq \tau$ must have the form $\mathsf{execute}_j^i$ for some

$i \leq^\# j \in T'$. By following the flow relation of N one finds the places and transitions that, under the canonical distribution, are co-located with $\textsf{execute}^i_j$:

$$\begin{tikzcd}
\pi_{j\#l} \arrow[r] \arrow[d] & \textsf{transfer}^j_l \cdot \textsf{fire} & \textsf{trans}^j_l\textsf{-in} \arrow[l] \arrow[r] & \textsf{initialise}_l \cdot \textsf{undo}(\textsf{trans}^j_l\textsf{-in}) & \textsf{take}(\textsf{trans}^j_l\textsf{-in}, \textsf{initialise}_l) \arrow[l] \\
\textsf{execute}^i_j & & & & \\
\textsf{trans}^h_j\textsf{-out} \arrow[u] \arrow[r] \arrow[d] & \textsf{transfer}^h_j \cdot \textsf{undo}(\textsf{trans}^h_j\textsf{-out}) & \textsf{take}(\textsf{trans}^h_j\textsf{-out}, \textsf{transfer}^h_j) \arrow[l] & & \\
\textsf{execute}^g_j & & & & \\
\textsf{pre}^g_j \arrow[u] \arrow[r] & \textsf{initialise}_g \cdot \textsf{undo}(\textsf{pre}^g_j) & \textsf{take}(\textsf{pre}^g_j, \textsf{initialise}_g) \arrow[l] & &
\end{tikzcd}$$

for all $l >^\# j$, $h <^\# j$ and $g \leq^\# j$. We need to show that none of these transitions can happen concurrently with $\textsf{execute}^i_j$. For transitions $\textsf{transfer}^j_l \cdot \textsf{fire}$ and $\textsf{execute}^g_j$ this follows directly from Lemma 10. For $\textsf{transfer}^h_j \cdot \textsf{undo}(\textsf{trans}^h_j\textsf{-out})$ this also follows from Lemma 10, in which j, k and l play the rôle of the current h, i and j. For the transitions $\textsf{initialise}_l \cdot \textsf{undo}(\textsf{trans}^j_l\textsf{-in})$ and $\textsf{initialise}_g \cdot \textsf{undo}(\textsf{pre}^g_j)$ this has been established in Lemma 11. □

Our main result follows by combining Theorems 5 and 6 and Proposition 3:

Theorem 7 Let N be a finitary plain structural conflict net without a fully reachable pure M. Then N is distributable up to $\approx^\Delta_{bSTb}$.

Corollary 3 Let N be a finitary plain structural conflict net. Then N is distributable iff it has no fully reachable pure M.

8 Conclusion

In this paper, we have given a precise characterisation of distributable Petri nets in terms of a semi-structural property. Moreover, we have shown that our notion of distributability corresponds to an intuitive notion of a distributed system by establishing that any distributable net may be implemented as a network of asynchronously communicating components.

In order to formalise what qualifies as a valid implementation, we needed a suitable equivalence relation. We have chosen step readiness equivalence for showing the impossibility part of our characterisation, since it is one of the simplest and least discriminating semantic equivalences imaginable that abstracts from internal actions but preserves branching time, concurrency and divergence to some small degree. For the positive part, stating that all other nets are implementable, we have introduced a combination of several well known rather discriminating equivalences, namely a divergence sensitive version of branching bisimulation adapted to ST-semantics. Hence our characterisation is rather robust against the chosen equivalence; it holds in fact for all equivalences between these two notions. However, ST-equivalence (and our version of it) preserves the causal structure between action occurrences only as far as it can be expressed in terms of the possibility of durational actions to overlap in time. Hence a natural question is whether we could have chosen an even stronger causality sensitive equivalence for our implementability result, respecting e.g. pomset equivalence or history preserving bisimulation. Our conflict replicating implementation does not fully preserve the causal behaviour of nets; we are convinced that we have chosen the strongest possible equivalence for which our implementation works. It is an open problem to find a class of nets that can be implemented distributedly while preserving divergence, branching time and causality in full. Another line of research is to investigate which Petri nets can be implemented as distributed nets when relaxing the requirement of preserving the branching structure. If we allow linear time correct implementations (using a step trace equivalence), we conjecture that all Petri nets become distributable. However, also in this case it is problematic, in fact even impossible in our setting, to preserve the causal structure, as has been shown in [16]. A similar impossibility result has been obtained in the world of the π-calculus in [14].

The interplay between choice and synchronous communication has already been investigated in quite a number of approaches in different frameworks. We refer to [6] for a rather comprehensive overview and concentrate here on recent and closely related work.

The idea of modelling asynchronously communicating sequential components by sequential Petri nets interacting though buffer places has already been considered in [15]. There Wolfgang Reisig introduces a class of systems, represented as Petri nets, where the relative speeds of different components are guaranteed to be irrelevant. His class is a strict subset of our LSGA nets, requiring additionally, amongst others, that all choices in sequential components are free, i.e. do not depend upon the existence of buffer tokens, and that places are output buffers of only one component. Another quite similar approach was taken in [3], where transition labels are classified as being either input or output. There, asynchrony is introduced by adding new buffer places during net composition. This framework does not allow multiple senders for a single receiver.

Other notions of distributed and distributable Petri nets are proposed in [11, 1, 2]. In these works, given a distribution of the transitions of a net, the net is distributable iff it can be implemented by a net that is distributed w.r.t. that distribution. The requirement that concurrent transitions may not be co-located is absent; given the fixed distribution, there is no need for such a requirement. These papers differ from each other, and from ours, in what counts as a valid implementation. A comparison of our criterion with that of Hopkins [11] is provided in [6].

In [6] we have obtained a characterisation similar to Corollary 3, but for a much more restricted notion of distributed implementation (*plain distributability*), disallowing nontrivial transition labellings in distributed implementations. We also proved that fully reachable pure Ms are not implementable in a distributed way, even when using transition labels (Theorem 2). However, we were not able to show that this upper bound on the class of distributable systems was tight. Our current work implies the validity of Conjecture 1 of [6]. While in [6] we considered only one-safe place/transition systems, the present paper employs a more general class of place/transition systems, namely structural conflict nets. This enables us to give a concrete characterisation of distributed nets as systems of sequential components interacting via non-safe buffer places.

References

[1] E. Badouel, B. Caillaud & P. Darondeau (2002): *Distributing Finite Automata Through Petri Net Synthesis*. *Formal Aspects of Computing* 13(6), pp. 447–470, doi:`10.1007/s001650200022`.

[2] E. Best & Ph. Darondeau (2011): *Petri Net Distributability*. In: Proceedings *Ershov Informatics Conference* (PSI'11), Novosibirsk, Russia, LNCS 7162, Springer, pp. 1–18.

[3] D. El Hog-Benzina, S. Haddad & R. Hennicker (2010): *Process Refinement and Asynchronous Composition with Modalities*. In N. Sidorova & A. Serebrenik, editors: Proceedings of the 2nd International Workshop on *Abstractions for Petri Nets and Other Models of Concurrency* (APNOC'10), Braga, Portugal. Available at `http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/EHH-apnoc10.pdf`.

[4] R.J. van Glabbeek (1993): *The Linear Time - Branching Time Spectrum II*. In: Proceedings of the 4th International Conference on *Concurrency Theory* (CONCUR'93), Springer, London, UK, pp. 66–81, doi:10.1007/3-540-57208-2_6.

[5] R.J. van Glabbeek & U. Goltz (2001): *Refinement of actions and equivalence notions for concurrent systems*. *Acta Informatica* 37(4/5), pp. 229–327, doi:10.1007/s002360000041.

[6] R.J. van Glabbeek, U. Goltz & J.-W. Schicke (2008): *On Synchronous and Asynchronous Interaction in Distributed Systems*. In E. Ochmański & J. Tyszkiewicz, editors: *Mathematical Foundations of Computer Science 2008*, LNCS 5162, Springer, pp. 16–35, doi:10.1007/978-3-540-85238-4_2. Full version available as Technical Report 2008-03, TU-Braunschweig; http://arxiv.org/abs/0901.0048.

[7] R.J. van Glabbeek, U. Goltz & J.-W. Schicke (2011): *Abstract Processes of Place/Transition Systems*. *Information Processing Letters* 111(13), pp. 626 – 633, doi:10.1016/j.ipl.2011.03.013.

[8] R.J. van Glabbeek, B. Luttik & N. Trčka (2009): *Branching Bisimilarity with Explicit Divergence*. *Fundamenta Informaticae* 93(4), pp. 371–392. Archived at http://arxiv.org/abs/0812.3068.

[9] R.J. van Glabbeek & F.W. Vaandrager (1987): *Petri net models for algebraic theories of concurrency (extended abstract)*. In: Proceedings *PARLE '87*, LNCS 259, Springer, pp. 224–242, doi:10.1007/3-540-17945-3_13. Available at http://kilby.stanford.edu/~rvg/pub/petri.pdf.

[10] R.J. van Glabbeek & W.P. Weijland (1996): *Branching Time and Abstraction in Bisimulation Semantics*. *Journal of the ACM* 43(3), pp. 555–600, doi:10.1145/233551.233556.

[11] R.P. Hopkins (1991): *Distributable nets*. In: *Advances in Petri Nets 1991*, LNCS 524, Springer, pp. 161–187, doi:10.1007/BFb0019974.

[12] R. Milner (1989): *Communication and Concurrency*. Prentice Hall, Englewood Cliffs.

[13] E.-R. Olderog & C.A.R. Hoare (1986): *Specification-oriented semantics for communicating processes*. *Acta Informatica* 23, pp. 9–66, doi:10.1007/BF00268075.

[14] K. Peters, J.-W. Schicke & U. Nestmann (2011): *Synchrony vs Causality in the Asynchronous Pi-Calculus*. In B. Luttik & F. Valencia, editors: Proceedings 18th International Workshop on *Expressiveness in Concurrency,* Aachen, Germany, 5th September 2011, *Electronic Proceedings in Theoretical Computer Science* 64, pp. 89–103, doi:10.4204/EPTCS.64.7.

[15] W. Reisig (1982): *Deterministic Buffer Synchronization of Sequential Processes*. *Acta Informatica* 18, pp. 115–134, doi:10.1007/BF00264434.

[16] J.-W. Schicke, K. Peters & U. Goltz (2011): *Synchrony vs. Causality in Asynchronous Petri Nets*. In B. Luttik & F. Valencia, editors: Proceedings 18th International Workshop on *Expressiveness in Concurrency,* Aachen, Germany, 5th September 2011, *Electronic Proceedings in Theoretical Computer Science* 64, pp. 119–131, doi:10.4204/EPTCS.64.9.

[17] W. Vogler (1993): *Bisimulation and Action Refinement*. *Theoretical Computer Science* 114(1), pp. 173–200, doi:10.1016/0304-3975(93)90157-O.

Technische Universität Braunschweig
Informatik-Berichte ab Nr. 2008-08

2008-08	B. Rosic	A Review of the Computational Stochastic Elastoplasticity
2008-09	B. N. Khoromskij, A. Litvinenko, H. G. Matthies	Application of Hierarchical Matrices for Computing the Karhunen-Loeve Expansion
2008-10	M. V. Cengarle, H. Grönniger B. Rumpe	System Model Semantics of Statecharts
2009-01	H. Giese, M. Huhn, U. Nickel, B. Schätz (Herausgeber)	Tagungsband des Dagstuhl-Workshops MBEES: Modellbasierte Entwicklung eingebetteter Systeme V
2009-02	D. Jürgens	Survey on Software Engineering for Scientific Applications: Reuseable Software, Grid Computing and Application
2009-03	O. Pajonk	Overview of System Identification with Focus on Inverse Modeling
2009-04	B. Sun, M. Lochau, P. Huhn, U. Goltz	Parameter Optimization of an Engine Control Unit using Genetic Algorithms
2009-05	A. Rausch, U. Goltz, G. Engels, M. Goedicke, R. Reussner	LaZuSo 2009: 1. Workshop für langlebige und zukunftsfähige Softwaresysteme 2009
2009-06	T. Müller, M. Lochau, S. Detering, F. Saust, H. Garbers, L. Märtin, T. Form, U. Goltz	Umsetzung eines modellbasierten durchgängigen Enwicklungsprozesses für AUTOSAR-Systeme mit integrierter Qualitätssicherung
2009-07	M. Huhn, C. Knieke	Semantic Foundation and Validation of Live Activity Diagrams
2010-01	A. Litvinenko and H. G. Matthies	Sparse data formats and efficient numerical methods for uncertainties quantification in numerical aerodynamics
2010-02	D. Grunwald, M. Lochau, E. Börger, U. Goltz	An Abstract State Machine Model for the Generic Java Type System
2010-03	M. Krosche, R. Niekamp	Low-Rank Approximation in Spectral Stochastic Finite Element Method with Solution Space Adaption
2011-01	L. Märtin, M. Schatalov, C. Knieke	Entwicklung und Erweiterung einer Werkzeugkette im Kontext von IT-Ökosystemen
2011-02	B. V. Rosić, A. Litvinenko, O. Pajonk, H. G. Matthies	Direct Bayesian update of polynomial chaos representations
2011-03	H. G. Matthies	White Noise Analysis for Stochastic Partial Differential Equations
2011-04	O. Pajonk, B. Rosić, A. Litvinenko, and H. G. Matthies	A Deterministic Filter for non-Gaussian Bayesian Estimation
2011-05	H. G. Matthies	A Hitchhiker's Guide to Mathematical Notation and Definitions
2011-06	R.J. van Glabbeek, U. Goltz, J.-W. Schicke	On Causal Semantics of Petri Nets
2011-07	H. Cichos, S. Oster, M. Lochau, A. Schrr	Extended Version of Model-based Coverage-Driven Test Suite Generation for Software Product Lines
2011-08	W.-B. Pttner, J. Morgenroth, S. Schildt, L. Wolf	An Empirical Performance Comparison of DTN Bundle Protocol Implementations
2011-09	N. Khakpou, S. Jalili, M. Sirjanir	Assuring the Correctness of Large-Scale Adaptive Systems
2011-10	R.J. van Glabbeek, U. Goltz, J.-W. Schicke-Uffmann	On Distributability of Petri Nets