Fundamenta Informaticae XX (2012) 1–5
IOS Press

Building Occurrence Nets from Reveals Relations*

Sandie Balaguer C

Thomas Chatain

Stefan Haar
INRIA & LSV (CNRS & ENS Cachan)
61, avenue du Président Wilson
94235 CACHAN Cedex, France
{*balaguer, chatain, haar*}*@lsv.ens-cachan.fr*

Abstract. Occurrence nets are a well known partial order model for the concurrent behavior of Petri nets. The causality and conflict relations between events, which are explicitly represented in occurrence nets, induce logical dependencies between event occurrences: the occurrence of an event e in a run implies that all its causal predecessors also occur, and that no event in conflict with e occurs. But these structural relations do not express all the logical dependencies between event occurrences in maximal runs: in particular, the occurrence of e in any maximal run may imply the occurrence of another event that is not a causal predecessor of e, in that run. The *reveals* relation has been introduced to express this dependency between two events. Here we generalize the reveals relation to express more general dependencies, involving more than two events, and we introduce ERL logic to express them as boolean formulas. Finally we answer the synthesis problem that arises: given an ERL formula φ, is there an occurrence net $\mathcal{N}$ such that φ describes exactly the dependencies between the events of $\mathcal{N}$?

Keywords: synthesis of concurrent systems, occurrence nets, event logics, Petri nets, maximal runs

1. Introduction

Partial order representations of runs of Petri nets provide an alternative to sequential semantics, exhibiting the concurrency that naturally arises from the Petri net dynamics. *Occurrence nets* are the data structure

*This work was partially supported by the FP7 European project UniverSelf and the French ANR project ImpRo.
CCorresponding author

for the partial order semantics referred to as *unfoldings*; they are nets in which all transitions, called *events*, are executable and the flow relation induced by the arcs is acyclic. Paths between events represent *causality*.

The representation of all runs of a Petri net as an *unfolding* [15, 23] allows one to avoid the state-space explosion due to interleavings when exploring the runs of a Petri net. Unfoldings are infinite in general, but can be represented efficiently by a finite complete prefix [16, 21], for instance to check LTL formulas [19].

The structure of an occurrence net induces three relations over its events, *causality*, *concurrency* and *conflict*, thus generating a *prime event structure* [23]. Causality represents the partial ordering of events due to the progress of the run. When two events may occur in the same run, but are not related by causality, they are concurrent. The last possibility is that two events never occur in the same run; then they are in conflict. The causality and conflict relations induce logical dependencies between event occurrences: the occurrence of an event e in a run implies that all its causal predecessors also occur, and that no event in conflict with e ever occurs.

Here, we focus on a particular setting where weak fairness [25] is assumed, i.e. any enabled event has to occur or to be disabled, and when we consider these *maximal* runs, the structural relations do not express all the logical dependencies between event occurrences. Indeed, in this context, concurrency does not necessarily mean logical independency: it is possible that the occurrence of an event implies the eventual occurrence of another one, which is structurally concurrent. This happens with events a and c in Fig. 2(a): we have to observe that a is in conflict with b and that any maximal run contains either b or c. Therefore, if a occurs in a maximal run, then b does not occur and eventually c necessarily occurs. Yet c and a are not causally related.

Another case is illustrated by events a and d in the same figure: since a is a causal predecessor of d, the occurrence of d implies the occurrence of a; but in any *maximal* run, the occurrence of a also implies the occurrence of d because d is the only possible continuation to a and nothing can prevent it. Thus a and d are actually made *logically equivalent* by the maximal progress assumption.

The *reveals* relation between events was introduced in [18] to express these implicit dependencies between two events. Knowledge of *reveals* facilitates in particular the analysis of partially observable systems, in the context of diagnosis, testing, or verification: an event b revealed by a needs not be observable if a is, the occurrence of b can be *inferred*. The equivalence classes of events that mutually reveal each other are called *facets*; contracting facets into single events creates a *reduced* occurrence net whose set of maximal executions is in bijection with that of the initial occurrence net.

While the focus in [18] was on the binary *reveals* relation, we embed in this paper the relation in a more general logical framework. Starting from the observation that the *reveals* relation corresponds to logical implication between the occurrence of events, we consider general boolean formulas where the atoms express the occurrence of events. The resulting logic, which we call ERL, captures dependencies in occurrence nets. We then show first how to build a logical formula that describes all logical dependencies between the occurrence of events. Then we ask what are the formulas that are satisfied by all the runs of an occurrence net. An important result is that the logical dependencies between events, with the maximal progress assumption, are not only binary: there are logical dependencies that cannot be deduced from binary dependencies. This leads us to define an extended reveals relation.

Lastly, we solve the synthesis problem that arises: given an ERL formula over events (or facets), does this formula describe the set of possible runs of an occurrence net? We propose a method for synthesizing an occurrence net from an ERL formula. As a corollary, this allows us to identify a canonical occurrence

net to represent the equivalence class of all occurrence nets that have the same logical dependencies between events.

The paper is divided in two parts: first, Sections 2 to 4 give definitions about the structure and semantics of Petri nets and occurrence nets, then, Sections 5 and 6 introduce a logic to describe the set of runs of an occurrence net and develop a synthesis procedure. More precisely, Section 2 recalls definitions about Petri nets, processes and occurrence nets. Section 3 presents the binary reveals relation and the facets abstraction from [18]. Section 4 establishes a new result about the converse well-foundedness of the reveals relation over facets and defines tight nets. Section 5 introduces the ERL logic, capable of capturing general logical dependencies between events. ERL formulas can be interpreted with respect to a set of acceptable runs of an occurrence net; an important case is that of *maximal* runs, which gives rich dependencies, and which the last sections of the paper will focus on. Section 6 explains how to build an ERL formula that describes the dependencies between the events of a given occurrence net, and then solves the problem of synthesis of tight occurrence nets from ERL formulas. Section 7 presents a few extensions. In particular it shows that, while synthesizing an occurrence net from an ERL formula, the causality in the net can be freely chosen provided it is compatible with the reveals relation induced by the formula; it also discusses synthesis under non-maximal semantics. These extensions were not published in the conference version of this work [3].

2. Occurrence Nets and Petri Net Semantics

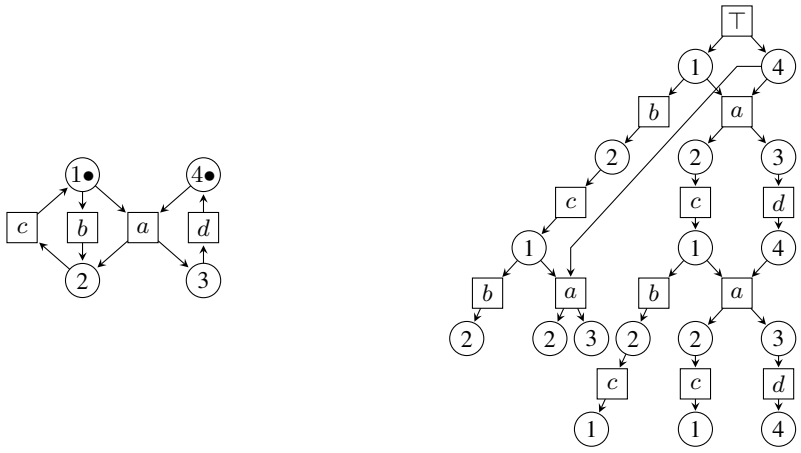
In this paper, only safe Petri nets are considered.

Definition 2.1. (Net)
A *net* is a triple (P, T, F) where P and T are disjoint sets of *places* and *transitions*, respectively, and $F \subseteq (P \times T) \cup (T \times P)$ is the *flow relation*.

For any node $x \in P \cup T$, we call *pre-set* of x the set ${}^\bullet x = \{y \in P \cup T \mid (y, x) \in F\}$ and *post-set* of x the set $x^\bullet = \{y \in P \cup T \mid (x, y) \in F\}$.

A *marking* of a net is a subset of P. A *Petri net* (PN) is a tuple (P, T, F, M_0), where (P, T, F) is a finite net and $M_0 \subseteq P$ is the *initial marking*. As usual, in figures, transitions are represented as rectangles and places as circles. If $p \in M$, a black token is drawn in p (see Fig. 1(a)). Transition t is *enabled* at M iff ${}^\bullet t \subseteq M$, i.e. t can *fire*, leading to $M' = (M \setminus {}^\bullet t) \cup t^\bullet$, in that case, we write $M \xrightarrow{t} M'$. A marking M is *reachable* if $M_0 \longrightarrow^* M$. A PN is *safe* iff for each reachable marking M, for each transition t enabled at M, $(t^\bullet \cap M) \subseteq {}^\bullet t$.

We now recall a few definitions required to introduce occurrence nets. We denote by $\lessdot$ the *direct causality* relation defined as: for any transitions s and t, $s \lessdot t \overset{def}{\iff} s^\bullet \cap {}^\bullet t \neq \emptyset$. We write $<$ for its transitive closure and $\leq$ for its reflexive transitive closure, called *causality*. For any transition t, the set $\lceil t \rceil \overset{def}{=} \{s \mid s \leq t\}$ is the *causal past* or *prime configuration* of t, and for $T' \subseteq T$, the causal past of T' is defined as $\lceil T' \rceil \overset{def}{=} \bigcup_{t \in T'} \lceil t \rceil$. Two distinct transitions s and t are in *direct conflict*, denoted by $s \#_d t$, iff ${}^\bullet s \cap {}^\bullet t \neq \emptyset$. Two transitions s and t are in *conflict*, denoted by $s \# t$, iff $\exists s' \in \lceil s \rceil, t' \in \lceil t \rceil : s' \#_d t'$, and the *conflict set* of t is defined as $\#[t] \overset{def}{=} \{s \mid s \# t\}$. Lastly, two transitions s and t are *concurrent*, denoted by $s \; co \; t$, iff $\neg(s \# t) \wedge \neg(s \leq t) \wedge \neg(t \leq s)$.



(a) Petri net (b) Occurrence net

Figure 1. A Petri net and a prefix of its unfolding

Definition 2.2. (Occurrence net)
An *occurrence net* (ON) is a net (B, E, F) where elements of B and E are called *conditions* and *events*, respectively, and such that:

1. $\forall e \in E, \neg(e \# e)$ (no self-conflict),
2. $\forall e \in E, \neg(e < e)$ ($\leq$ is a partial order),
3. $\forall e \in E, |\lceil e \rceil| < \infty$,
4. $\forall b \in B, |{}^\bullet b| = 1$ (no backward branching),
5. $\top \in E$ is the only $\leq$-minimal node (event $\top$ creates the initial conditions).

Fig. 1(b) gives an example of ON. An ON can also be given as a tuple $(B, E \setminus \{\top\}, F, \mathbf{c}_0)$, where $\mathbf{c}_0 = \top^\bullet$ is the set of minimal conditions.

The initial event is usually denoted by the symbol $\bot$, but in this paper, we exceptionally denote it by $\top$. The reason is that, in the ERL logic that we introduce later, this event corresponds exactly to the true logical formula (usually denoted $\top$), in the sense that any event reveals the initial event like any logical formula implies $\top$.

Occurrence nets are closely related to the notion of event structures [23].

Definition 2.3. ((Prime) event structure [23])
A *(prime) event structure* is a triple $(E, \leq, \#)$ where

1. E is a set, whose elements are called *events*,
2. $\leq$ is a partial order on E such that for all $x \in E$, $\{y \in E \mid y \leq x\}$ is finite,
3. $\#$ is a symmetric and irreflexive relation, and for all $x, y, z \in E$, $x \# y$ and $y \leq z$ together imply $x \# z$.

For any *finite* reduced ON (B, E, F), the triple $(E, \leq, \#)$ is an *event structure* [23].

2.1. Branching Processes and Unfoldings

A *net homomorphism* from N to N' is a map $\pi : P \cup T \to P' \cup T'$ such that $\pi(P) \subseteq P'$, $\pi(T) \subseteq T'$, and for all $t \in T$, $\pi_{|^\bullet t}$, the restriction of π to $^\bullet t$, is a bijection between $^\bullet t$ and $^\bullet \pi(t)$, and $\pi_{|t^\bullet}$ is a bijection between $t^\bullet$ and $\pi(t)^\bullet$.

Let $N = (P, T, F, M_0)$ be a PN. A *branching process* of N is a pair (N', π), where $N' = (P', T', F', \mathbf{c}_0)$ is an ON and π is a homomorphism from (P', T', F') to (P, T, F), such that:

1. $\pi_{|\mathbf{c}_0}$ is a bijection between $\mathbf{c}_0$ and M_0,
2. $\forall t, t' \in T', \left(^\bullet t = {}^\bullet t' \wedge \pi(t) = \pi(t')\right) \Rightarrow t = t'$

For Π_1, Π_2 two branching processes, Π_1 is a *prefix* of Π_2, written $\Pi_1 \sqsubseteq \Pi_2$, if there exists an injective homomorphism h from ON_1 into a prefix of ON_2, such that h induces a bijection between $\mathbf{c}_0^1$ and $\mathbf{c}_0^2$ and the composition $\pi_2 \circ h$ coincides with π_1.

By Theorem 23 of [23], there exists a unique (up to an isomorphism) $\sqsubseteq$-maximal branching process, called the *unfolding* of $\mathcal{N}$; by abuse of language, we will also call unfolding of $\mathcal{N}$ the ON obtained by the unfolding.

2.2. Maximal and General Runs

Definition 2.4. (Run, Maximal run)
A *run* of an ON is a conflict-free and causally closed set of events, i.e. $\omega \subseteq E$ is a run iff $\forall e \in \omega$, $(\#[e] \cap \omega = \emptyset) \wedge (\lceil e \rceil \subseteq \omega)$.
A run is *maximal* iff it is maximal w.r.t. $\subseteq$.

We write Ω_{gen} for the set of all runs and Ω_{max} for the set of maximal runs.

The following lemma highlights the importance of the conflict relation in the definition of maximal runs.

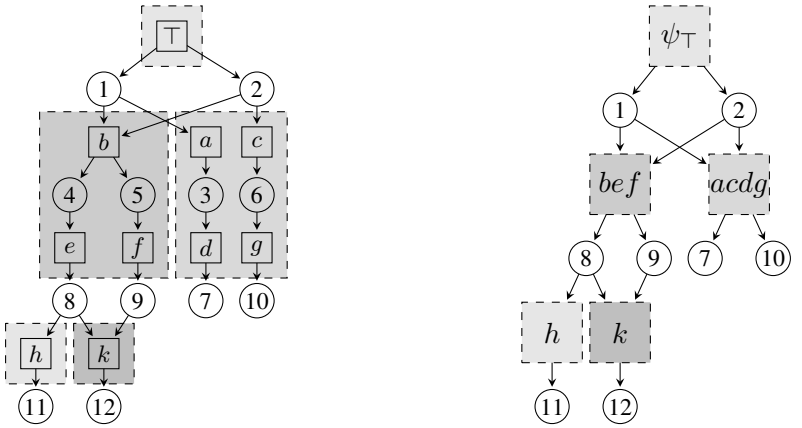
Lemma 2.1. A set of events ω is a maximal run iff $\forall a \in E, a \in \omega \iff \#[a] \cap \omega = \emptyset$.

Proof:
If ω is a run and there exists $a \in E \setminus \omega$ that is not in conflict with any event of ω, then $\omega \cup \lceil a \rceil$ is also a run and ω is not maximal. Conversely, a set of events ω which satisfies the equivalence for any event a is conflict-free and $\subseteq$-maximal, and since the conflict is inherited under the causality, ω must also be causally closed. □

3. Reveals Relation and Facets Abstraction

The structure of an occurrence net defines three relations over its events: *causality*, *concurrency* and *conflict*.

But these structural relations do not express all the logical dependencies between the occurrence of events in maximal runs. A central fact is that concurrency is not always a logical independency: it is possible that the occurrence of an event implies the occurrence of another one, which is structurally concurrent. This happens with events a and c in Fig. 2(a): we have to observe that a is in conflict with b



(a) An occurrence net. Squared events are in the same facet.

(b) The corresponding reduced ON.

Figure 2. An ON and its reduction through the facet abstraction.

and that any maximal run contains either b or c. Therefore, if a occurs in a maximal run, then b does not occur and eventually c necessarily occurs. Yet c and a are concurrent.

Another case is illustrated by events a and d in the same figure: because a is a causal predecessor of d, the occurrence of d implies the occurrence of a; but in any maximal run, the occurrence of a also implies the occurrence of d because d is the only possible continuation to a and nothing can prevent it. Then a and d are actually made logically equivalent by the maximal progress assumption.

3.1. Reveals Relation

The reveals relation expresses dependencies between events such as "if e occurs, then f has already occurred or will occur eventually" in the sense that any run that contains e also contains f.

Definition 3.1. (Reveals relation [18])
Given a set Ω of sets of *events* (these sets of events intend to be interpreted as *runs*), we say that event e *reveals* event f (in Ω), and write $e \triangleright f$, iff $\forall \omega \in \Omega$, $(e \in \omega \Rightarrow f \in \omega)$.

Notice that $\triangleright$ is transitive.

Property 1. For any events e and f, $f \leq e \Rightarrow e \triangleright f$, and if $\Omega = \Omega_{gen}$, $f \leq e \iff e \triangleright f$.

Proof:
The implication comes directly from the fact that runs are causally closed.

For $\Omega = \Omega_{gen}$, there is no progress assumption, then for any event e, $\lceil e \rceil$ is a valid run, and consequently e does not reveal any event outside $\lceil e \rceil$. □

Property 2. ($\#$-inheritance under $\triangleright$)
The conflict relation is inherited under the reveals relation: for any events a, b, c, $a \# b$ and $c \triangleright b$ together imply $a \# c$.

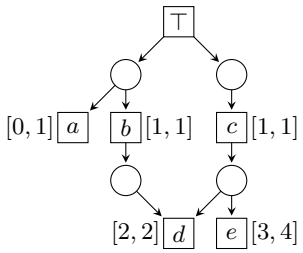


Figure 3. An occurrence net constrained by time delay intervals.

Proof:
Assume a run contains a and c. Then, because $c \triangleright b$, it also contains b, which contradicts $a \# b$. □

3.1.1. Several choices of Ω

As we have seen, the reveals relation depends on the set of runs Ω that we consider. Two natural choices are the set of maximal runs Ω_{max} and the set of all runs Ω_{gen}. But other sets of runs could also be considered, like runs of time Petri nets. We give a quick outlook below.

Maximal semantics. The maximal semantics is the one which inspired the definition of the reveals relation in [18]. Indeed this setting generates rich dependencies between events. In the following, we focus on the maximal semantics, unless explicitly mentioned.

The first interesting point with the maximal semantics is a nice characterization of the reveals relation based on the conflict relation. This characterization was actually used as the definition of the reveals relation in [18]. The equivalence with our definition was proved in [18].

Lemma 3.1. (Reveals relation: alternative definition for maximal runs)
Event e *reveals* event f in Ω_{max} iff $\#[f] \subseteq \#[e]$.

Notice that, with the general semantics, the two definitions are not equivalent. For example, in Fig. 2(a), $d \triangleright a$ holds for general runs and therefore also for maximal runs, but $a \triangleright d$ and $d \triangleright c$ hold for maximal runs only.

General semantics. When we do not assume maximal progress, the revels relation between events coincides precisely with the structural causality as stated in Property 1.

Timed semantics. Beyond the two natural setups presented above, we see many relevant situations where more specific sets of executions have to be considered. One example comes from the modeling of real-time systems. Consider the occurrence net depicted in Fig. 3 and assume that its behavior is constrained by the time constraints given by the intervals, which are interpreted like in time Petri nets [22] with dense time. We observe that, because of urgency, the occurrence of b forces the occurrence of d two time units later, i.e. $b \triangleright d$ in the time semantics. As a consequence e reveals a. This also makes b and e incompatible, although they are not in conflict in the sense of untimed occurrence nets.

Studying the logical dependencies between events in real-time systems is actually one of our perspectives after this work.

3.2. Facets Abstraction

Definition 3.2. (Facet [18])
Let $\sim$ be an equivalence relation defined as: $\forall e, f \in E, e \sim f \overset{def}{\iff} (e \triangleright f) \wedge (f \triangleright e)$, then a *facet* of an ON is an equivalence class of $\sim$.

For example, in Fig. 2(a), and with the maximal semantics, the ON has five facets: $\{\top\}$, $\{a, c, d, g\}$, $\{b, e, f\}$,$\{h\}$ and $\{k\}$. If ψ is a facet, then for any run ω and for any event e such that $e \in \psi$, $e \in \omega$ iff $\psi \subseteq \omega$. In this sense, facets can be seen as atomic sets of events.

The causality relation, $\leq$, and the conflict relation, $\#$, naturally extend to the set of facets as follows: $\forall \psi_1, \psi_2 \in \Psi$,

$$\psi_1 \leq \psi_2 \quad \overset{def}{\iff} \quad \exists e_1 \in \psi_1, e_2 \in \psi_2 : e_1 \leq e_2$$
$$\psi_1 \# \psi_2 \quad \overset{def}{\iff} \quad \exists e_1 \in \psi_1, e_2 \in \psi_2 : e_1 \# e_2$$

The set of facets equipped with $\leq$ and $\#$ is an event structure [18].

Reduced Occurrence Nets: For any facet and for any run, either all events in the facet are in the run or no event in the facet is in the run. Therefore, facets can be seen as events. In the sequel, we consider reduced ONs [18], i.e. ONs reduced by contracting the facets into events.

For example, in Fig. 2(a), the reduced ON is obtained by contracting, for each facet, the squared events into an event. With the maximal semantics, this gives the reduced ON of Fig. 2(b). From now on, runs are thus considered as conflict-free and causally closed sets of *facets*.

Definition 3.3. (Reduced occurrence net)
A *reduced ON* is an ON (B, Ψ, F) such that $\forall \psi_1, \psi_2 \in \Psi, \psi_1 \sim \psi_2 \iff \psi_1 = \psi_2$ (i.e. such that $\triangleright$ is antisymmetric).

Since this reduction yields an occurrence net, the concurrency relation, co, and the reveals relation, $\triangleright$, also naturally extend to the set of facets: $\forall \psi_1, \psi_2 \in \Psi$,

$$\begin{aligned} \psi_1 \ co \ \psi_2 \quad &\overset{def}{\iff} \quad \neg(\psi_1 \# \psi_2) \wedge \neg(\psi_1 \leq \psi_2) \wedge \neg(\psi_2 \leq \psi_1) \\ &\iff \quad \psi_1 \neq \psi_2 \wedge \forall e_1 \in \psi_1, e_2 \in \psi_2 : e_1 \ co \ e_2 \\ \psi_1 \triangleright \psi_2 \quad &\overset{def}{\iff} \quad \exists e_1 \in \psi_1, e_2 \in \psi_2 : e_1 \triangleright e_2 \end{aligned}$$

Remark 3.1. If we consider the set of general runs, then, because of Property 1, any event is a facet, and therefore, the ON is already reduced. Therefore, in the sequel, we consider the set of maximal runs, and Ω denotes the set of maximal runs.

4. Tight Occurrence Nets and Event Structures

4.1. Concurrency vs Logical Independency

Two facets may be causally ordered ($\leq$), in conflict ($\#$) or concurrent (co). The conflict relation exactly coincides with the fact that two facets never occur in the same execution. Moreover the causal ordering

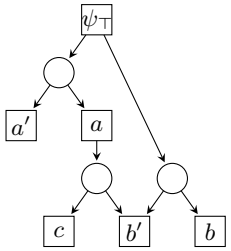


Figure 4. $a \; ind \; b$, $\neg(b \; ind \; c)$ and $\neg(b \; ind \; a')$

induces a reveals relation as stated in Property 1. But two concurrent facets are not necessarily logically independent in maximal runs. Hence causality and reveals together give a finer partition of the possible dependencies between two facets that are not in conflict. They can be either:

- causally related (and therefore also related by $\triangleright$),
- concurrent but related by $\triangleright$, or
- logically independent (and hence concurrent).

Formally, we define the *independency relation* among facets, denoted by ind, as the complement of the conflict and reveals relations:

$$\begin{aligned} \psi_1 \; ind \; \psi_2 \quad &\overset{def}{\iff} \quad \neg(\psi_1 \# \psi_2) \wedge \neg(\psi_2 \triangleright \psi_1) \wedge \neg(\psi_1 \triangleright \psi_2) \\ &\iff \quad \psi_1 \; co \; \psi_2 \wedge \neg(\psi_2 \triangleright \psi_1) \wedge \neg(\psi_1 \triangleright \psi_2) \end{aligned}$$

That is, two facets are independent if they are neither in conflict nor related by the reveals relation. For example, in Fig. 4, facets b and c are concurrent but not independent because c reveals b, and facets a and b are independent. Therefore, if a is in a run, this gives no information on the presence (or absence) of b in the run.

4.2. Well-foundedness of the Inverse Reveals Relation

Lemma 4.1. In any reduced ON $\mathcal{N} = (B, \Psi, F)$ where there is no infinite set of pairwise concurrent events (in particular in the reduced unfolding of any safe Petri net), the reveals relation, $\triangleright$, is *converse well-founded* on Ψ, i.e. there is no infinite chain of distinct facets $\psi_1 \triangleright \psi_2 \triangleright \ldots$

Proof:
In the proof, we use the alternative characterization of well-foundedness: $\triangleright$ is converse well-founded on Ψ iff every nonempty subset S of Ψ has a $\triangleright$-maximal facet, i.e. a facet ψ such that for any facet $\psi' \in S$, $\psi' \neq \psi \Rightarrow \neg(\psi \triangleright \psi')$.

Assume first that the set $S \subseteq \Psi$ is conflict-free, and consider the set S' of the facets of S that have no strict causal predecessor in S. Because causality is well-founded, S' is not empty. Moreover, by definition, the facets of S' are pairwise concurrent. Thus, by hypothesis, S' is finite. Therefore there must be a facet ψ that is $\triangleright$-maximal in S'. It remains to show that ψ is also $\triangleright$-maximal in S. Let ψ' be a facet of S such that $\psi \triangleright \psi'$. By construction of S' there exists a facet ψ'' in S' such that $\psi'' \leq \psi'$. By

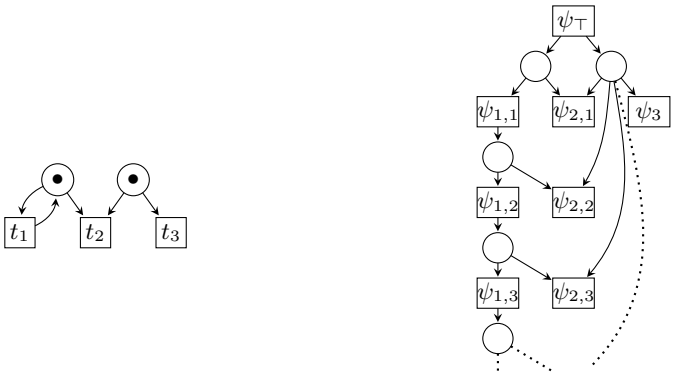


Figure 5. A Petri net and its unfolding (which is already a reduced ON)

Property 1, this implies that $\psi' \triangleright \psi''$, and by transitivity of $\triangleright$, we get $\psi \triangleright \psi''$. Since ψ is $\triangleright$-maximal in S', ψ'' must equal ψ. Then we have $\psi \triangleright \psi' \triangleright \psi$, which implies that ψ equals ψ' by construction of the facets.

If $S \subseteq \Psi$ is not conflict-free, then for any facet $\chi \in S$, the subset of S, $S_\chi = \{\chi' \in S \mid \chi \triangleright \chi'\}$ is conflict-free and hence has a $\triangleright$-maximal facet ψ. Moreover, by construction of S_χ, ψ does not reveal any facet in S, therefore, ψ is also $\triangleright$-maximal in S. □

We do not know if this lemma still holds without the hypothesis that there is no infinite set of pairwise concurrent events.

Anyway, Lemma 4.1 does *not* imply that any facet reveals only finitely many other facets. As a counterexample, consider the reduced ON of Fig. 5: facet ψ_3, associated with transition t_3, reveals all the facets $\psi_{1,i}$, $i \in \mathbb{N}^*$, associated with transition t_1.

Remark 4.1. For any *finite* reduced ON (B, Ψ, F), the triple $(\Psi, \triangleright^{-1}, \#)$ is an *event structure* because:

1. $\triangleright^{-1}$ is a partial order on Ψ,
2. For all $x \in \Psi$, $\{y \in \Psi \mid x \triangleright y\}$ is finite,
3. $\# \subseteq \Psi \times \Psi$ is an irreflexive and symmetric relation, and for all $x, y, z \in \Psi$, $x \# y$ and $z \triangleright y$ together imply $x \# z$ (Property 2).

4.3. Tight (Occurrence) Nets

A tight (occurrence) net is a reduced ON in which all binary logical dependencies among facets (given by the reveals relation) are represented as causalities.

Definition 4.1. (Tight net)
A *tight net* is an ON (B, E, F) such that $\forall e, f \in E, e \triangleright f \iff f \leq e$.

Tight nets constitute a natural and canonical class of occurrence nets, of interest in their own right as representations of logical dependencies (as opposed to temporal ones). Moreover, all nets obtained as the output of the synthesis procedure defined in Section 6 are tight.

Proposition 4.1. Every tight net is a reduced ON.

Proof:
If two events e and f of a tight net are in the same facet, then we have $e \triangleright f \wedge f \triangleright e$, which is equivalent to $f \leq e \wedge e \leq f$ because the net is tight. This implies $e = f$ by antisymmetry of $\leq$. □

Remark 4.2. In a tight net, ind is equivalent to co, and therefore the observation of the independency relation is easier than in a general reduced ON.

Remark 4.3. If we consider the set of general runs, then, since any ON is reduced (see Remark 3.1), and for any events e and f, $e \triangleright f \iff f \leq e$, any ON is tight.

We will show in Section 7.1 that it is possible to transform any finite reduced ON in a canonical tight net which accepts the same set of maximal runs Ω_{max}. This canonical tight net gives an efficient representation of the reveals relation. The example of Fig. 5, shows that the assumption of finiteness is necessary.

5. ERL: A Logic for Occurrence Nets

We introduce a logic, called *ERL* for *Event Reveal Logic*, that describes the properties of the runs of an ON by giving relations between event occurrences. Events are used as boolean variables: e stands for the presence of event e in a run.

We have seen that the causality relation does not explain all the dependencies between events of the type "if a occurs in a maximal run, then eventually b also occurs". The reveal relation was introduced to capture all these binary dependencies. But they are still not sufficient to describe more complex logical dependencies between events. Consider the ON of Fig. 4: causality gives only the dependencies $a < c$ and $a < b'$, plus the trivial ones involving $\psi_\top$. With the reveals relation we get $c \triangleright b$ and $a' \triangleright b$. They express that in any maximal run the occurrence of c implies the occurrence of b and the occurrence of a' implies the occurrence of b. But is it true that any set of events (containing $\psi_\top$) that satisfies these constraints, is a maximal run? The answer is no: for instance $\{\psi_\top, a, b\}$ satisfies these constraints, but is not a valid maximal run, since c is enabled and does not occur. Actually, all the maximal runs of this ON satisfy the following constraint: if a and b occur, then c also occurs.

Our logic is designed so that it allows us to express this kind of complex dependencies between event occurrences, and to define an appropriate *extended reveals relation*.

5.1. Syntax and Semantics

5.1.1. Syntax

The *alphabet* consists of:

variables: E is the set of variables (including $\top$)

constants: $\{\boldsymbol{tt}, \boldsymbol{ff}\}$

logical connectives: $\wedge$ and $\neg$.

Well-formed formulas are called *ERL formulas* and defined inductively with the following BNF grammar:

$$\varphi ::= \boldsymbol{tt} \mid \boldsymbol{ff} \mid e \mid \neg\varphi \mid \varphi \wedge \varphi, \text{ where } e \in E$$

5.1.2. Semantics

The semantics is given for a set of events $\gamma \subseteq E$ and an ERL formula φ. We write $\gamma \models \varphi$ when γ satisfies φ, defined as follows:

- for any event $e \in E$, $\gamma \models e$ iff $e \in \gamma$,
- the logical connectives $\neg$ and $\wedge$ have the usual semantics.

Since we are interested in properties of sets of runs, we look at the satisfaction of ERL formulas by sets of sets of events: for any ERL formula φ and for any set of sets of events Γ,

$$\Gamma \models \varphi \text{ iff } \forall \gamma \in \Gamma, \gamma \models \varphi$$

i.e. the formula is satisfied by all sets of events. Notice that, $\Gamma \not\models \varphi$ iff $\exists \gamma \in \Gamma : \gamma \not\models \varphi$ (which is different from $\Gamma \models \neg\varphi$).

We define the set $[\![\varphi]\!]$ as $[\![\varphi]\!] \stackrel{def}{=} \{\gamma \subseteq E \mid \gamma \models \varphi\}$. We write $\varphi \equiv \varphi'$ when $[\![\varphi]\!] = [\![\varphi']\!]$.

5.1.3. Extended Reveals Relation

Any well-formed formula can be brought into a *conjunctive normal form*:

$$\begin{aligned}
& \bigwedge_{i\in I}(b_{i,1} \vee b_{i,2} \vee \cdots \vee b_{i,n_i} \vee \neg a_{i,1} \vee \neg a_{i,2} \vee \cdots \vee \neg a_{i,m_i}) \\
\text{iff} \quad & \bigwedge_{i\in I}\big((a_{i,1} \wedge a_{i,2} \wedge \cdots \wedge a_{i,m_i}) \to (b_{i,1} \vee b_{i,2} \vee \cdots \vee b_{i,n_i})\big) \\
\text{iff} \quad & \bigwedge_{i\in I}(\bigwedge_{a\in A_i} a \to \bigvee_{b\in B_i} b),
\end{aligned}$$

where $A_i = \{a_{i,1}, \ldots, a_{i,m_i}\}$ and $B_i = \{b_{i,1}, \ldots, b_{i,n_i}\}$. And since for any set of runs Ω,

$$\begin{aligned}
& \Omega \models \bigwedge_{i\in I}(\bigwedge_{a\in A_i} a \to \bigvee_{b\in B_i} b) \\
\text{iff} \quad & \forall i \in I, \Omega \models \bigwedge_{a\in A_i} a \to \bigvee_{b\in B_i} b \\
\text{iff} \quad & \forall i \in I, \forall \omega \in \Omega, A_i \subseteq \omega \Rightarrow B_i \cap \omega \neq \emptyset,
\end{aligned}$$

we can focus on formulas of the form $\bigwedge_{a\in A} a \to \bigvee_{b\in B} b$, where A and B are two sets of events and that are satisfied by a set of runs Ω iff whenever all events in A occur in a run $\omega \in \Omega$, then at least one event in B occurs in ω. This leads us to define the *extended reveals relation*.

Definition 5.1. (Extended reveals relation)
Let $\Omega \subseteq 2^E$ be a set of runs, and A, B two sets of events, A reveals B written $A \rightarrowtriangle B$, iff $\forall \omega \in \Omega$, $A \subseteq \omega \Rightarrow B \cap \omega \neq \emptyset$

In this notation, Ω becomes implicit. Notice that $\neg(A \rightarrowtriangle B)$ means $\Omega \not\models \bigwedge_{a\in A} a \rightarrow \bigvee_{b\in B} b$ i.e. $\exists \omega \in \Omega : A \subseteq \omega \wedge B \cap \omega = \emptyset$.

Notice that the binary reveals relations $a \triangleright b$ correspond to the extended reveals relations between singletons $\{a\} \rightarrowtriangle \{b\}$.

Proposition 5.1. In the maximal semantics and the general semantics, conflicts can be expressed using this extended reveals relation: $\{a, b\} \rightarrowtriangle \emptyset \iff a \# b$.

This equivalence comes directly from the definition of runs. We should however consider it as a strong property of these two semantics and notice that only one direction would hold, for instance, in the timed semantics evoked at the end of Subsection 3.1.1: in the example of Fig. 3, events b and e are incompatible ($\{b, e\} \rightarrowtriangle \emptyset$), although they are not in conflict in the sense of untimed occurrence nets ($\neg(b \# e)$).

Remark 5.1. The extended reveals relation is not transitive: in general $A \rightarrowtriangle B \wedge B \rightarrowtriangle C$ does not imply $A \rightarrowtriangle C$. Indeed, the extended reveals relation is interpreted as a conjunction of events in the left part and as a disjunction of events in the right part.

5.2. Minimal and Immediate Constraints

Expressions of the form $A \rightarrowtriangle B$ are called *constraints*. We notice that some constraints can be deduced from others by monotonicity and by inheritance, which leads us to define *minimal constraints*.

5.2.1. Monotonicity Properties

First, the extended reveals relation has the following monotonicity properties:

Left Monotonicity Property . $\forall A, B, C \in 2^E, A \rightarrowtriangle C \wedge A \subseteq B \Rightarrow B \rightarrowtriangle C$.
Indeed, $A \subseteq B \Leftrightarrow \Omega \models \bigwedge_{b\in B} b \rightarrow \bigwedge_{a\in A} a$, and $\rightarrow$ is transitive.

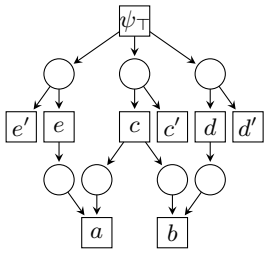
Right Monotonicity Property . $\forall A, B, C \in 2^E, A \rightarrowtriangle C \wedge C \subseteq B \Rightarrow A \rightarrowtriangle B$.
Indeed, $C \subseteq B \Leftrightarrow \Omega \models \bigvee_{c\in C} c \rightarrow \bigvee_{b\in B} b$, and $\rightarrow$ is transitive.

Therefore, we begin by considering the constraints $A \rightarrowtriangle B$ where the sets A and B are minimal.

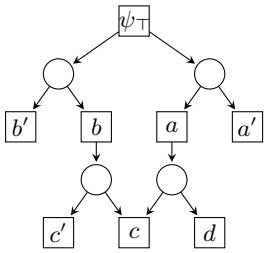
Definition 5.2. (Minimal reveals relation)
We define the *minimal reveals relation*, $\rightarrowtriangle_m$, as: $\forall A, B \in 2^E$,

$$A \rightarrowtriangle_m B \overset{def}{\iff} (A \neq B) \wedge (A \rightarrowtriangle B) \wedge (\nexists B' \subsetneq B : A \rightarrowtriangle B') \wedge (\nexists A' \subsetneq A : A' \rightarrowtriangle B)$$

i.e. if one event is removed from the left part or the right part, the reveals relation is lost.



(a) $\{c, d\} \rightarrowtriangle \{b\}$ is an immediate constraint and $\{a, d\} \rightarrowtriangle \{b\}$ is not.



(b) $\{a\} \rightarrowtriangle \{c, d\}$ is an immediate constraint and $\{a\} \rightarrowtriangle \{b, d\}$ is not.

Figure 6. Immediate constraints

For example, in Fig. 4, $\{a, b\} \rightarrowtriangle_m \{c\}$ because none of the following constraints holds: $\{a\} \rightarrowtriangle \{c\}$, $\{b\} \rightarrowtriangle \{c\}$, $\emptyset \rightarrowtriangle \{c\}$ and $\{a, b\} \rightarrowtriangle \emptyset$.

Intuitively the minimal reveals provides a more precise description than the extended reveals. Indeed, if $A \rightarrowtriangle_m B$, we know that for each $b \in B$, there is a run that contains A and b and no other event in B (otherwise $A \rightarrowtriangle B \setminus \{b\}$). Similarly, for each $a \in A$, there is a run that contains $A \setminus \{a\}$ and no event of B (otherwise $A \setminus \{a\} \rightarrowtriangle B$).

5.2.2. Deduction Through a Singleton

Moreover, the following properties also hold:

Left Inheritance Property . $\forall A, B \in 2^E, (A \cup \{d\} \rightarrowtriangle B) \wedge (d' \triangleright d) \Rightarrow A \cup \{d'\} \rightarrowtriangle B$

Right Inheritance Property . $\forall A, B \in 2^E, (A \rightarrowtriangle B \cup \{d\}) \wedge (d \triangleright d') \Rightarrow A \rightarrowtriangle B \cup \{d'\}$

We can now identify the extended reveals relations that are minimal w.r.t. deduction through a singleton.

Definition 5.3. (Immediate reveals relation)
We define the *immediate reveals relation*, $\rightarrowtriangle_i$, as: $\forall A, B \in 2^E$,

$$A \rightarrowtriangle_i B \overset{def}{\iff} \begin{cases} A \rightarrowtriangle_m B \\ \wedge\ \forall a \in A, \nexists a' \in E \setminus \{A \cup B\} : (a \triangleright a' \wedge A_{a'/a} \rightarrowtriangle B) \\ \wedge\ \forall b \in B, \nexists b' \in E \setminus \{A \cup B\} : (b' \triangleright b \wedge A \rightarrowtriangle B_{b'/b}) \end{cases}$$

where $A_{a'/a}$ denotes $A \cup \{a'\} \setminus \{a\}$.

For example, in Fig. 6(a), $\{a, d\} \rightarrowtriangle_m \{b\}$ is not an immediate constraint because $a \triangleright c$ and $\{c, d\} \rightarrowtriangle \{b\}$. And in Fig. 6(b) $\{a\} \rightarrowtriangle_m \{b, d\}$ is not an immediate constraint because $c \triangleright b$ and $\{a\} \rightarrowtriangle \{c, d\}$.

When $\triangleright$ is antisymmetric, the conjunction of all immediate constraints implied by some formula φ, is equivalent to φ (by definition of the immediate constraints).

5.3. Properties of the extended reveals relation

When we consider the maximal or the general semantics, a set of events that never occur together necessarily contains two events in conflict.

Lemma 5.1. For any set of events A, $A \rightarrowtriangle_m \emptyset \Rightarrow |A| = 2$.

Proof:
The reveals relation $A \rightarrowtriangle \emptyset$ implies that there exists no general run $\omega \in \Omega_{gen}$ such that $A \subseteq \omega$: in the general semantics, this holds simply by definition of the reveals relation; in the maximal semantics, the definition says that there exists no *maximal* run $\omega \in \Omega_{max}$ such that $A \subseteq \omega$, which implies that there exists no general run $\omega \in \Omega_{gen}$ such that $A \subseteq \omega$.

Then in particular $\lceil A \rceil$ is not a general run. Since it is causally closed, the reason why it is not a general run, is that it contains two events a and b that are in conflict. Since a and b are in $\lceil A \rceil$, there exist events a' and b' in A such that $a \in \lceil a' \rceil$ and $b \in \lceil b' \rceil$. By inheritance of the conflict along the causality, a' is in conflict with b', which implies $\{a', b'\} \rightarrowtriangle \emptyset$. And since $\{a', b'\} \subseteq A$ and $A \rightarrowtriangle_m \emptyset$, we must have $A = \{a', b'\}$. Finally, the absence of self-conflicts in occurrence nets guarantees that a' and b' are distinct. □

Remark 5.2. As well as Prop. 5.1, the previous lemma should be considered as an important property of the maximal and general semantics, and would not hold, for instance, in the timed semantics evoked at the end of Subsection 3.1.1 nor for contextual occurrence nets [4, 7, 26, 27], used for unfoldings of nets with read arcs, where weak causality may cause non binary conflicts. Non binary conflicts have also arisen from symbolic unfoldings of colored Petri nets [9, 10, 14].

When we consider the set of general runs, Ω_{gen}, we have already noticed that the binary reveals relation is given by the causality: $\forall a, b \in E, \{a\} \rightarrowtriangle \{b\} \iff b \leq a$. Furthermore, we have:

Proposition 5.2. (Decomposition of reveals relation in the general semantics)
With the general semantics, for any sets of events A and B,

$$A \rightarrowtriangle B \iff (\exists a \in A,\ b \in B : b \leq a) \vee (\exists a, a' \in A : a \# a')\,.$$

Proof:
($\Leftarrow$) If there exist $a, a' \in A$ such that $a \# a'$, then, no run contains A and for any set of events C, $A \rightarrowtriangle C$. And if there exist $a \in A$ and $b \in B$ such that $b \leq a$, then $a \triangleright b$ and by the monotonicity properties of $\rightarrowtriangle$, $A \rightarrowtriangle B$.
($\Rightarrow$) Assume $A \rightarrowtriangle B$ and A is conflict-free. Denote by $\lceil A \rceil$ the causal past of A i.e. the set $\lceil A \rceil = \cup_{a \in A} \lceil a \rceil$. Since we make no progress assumption, $\lceil A \rceil$ is a valid run. By definition of the extended reveals relation, $\forall \omega \in \Omega_{gen}$, $A \subseteq \omega \Rightarrow \omega \cap B \neq \emptyset$, and in particular, for $\omega = \lceil A \rceil$, this implies that $\lceil A \rceil \cap B \neq \emptyset$ i.e. that there exist $b \in B$ and $a \in A$ such that $b \leq a$. □

Therefore, with general runs, non binary constraints can be decomposed as disjunctions of binary ones, in contrast to the case for Ω_{max}.

5.3.1. Binary Immediate Constraints

Two kinds of binary immediate constraints will be particularly useful in the sequel.

First we define the *immediate conflict* relation, $\#_i$, as a special case of the immediate reveals relation: for all events a and b, $a \#_i b \overset{def}{\iff} \{a, b\} \rightarrowtriangle_i \emptyset$. For example, in Fig. 6(b), a' and c are in conflict but not in immediate conflict because $a' \# a$ and $c \triangleright a$. For any formula φ describing the runs of an ON, we have $\#_i \subseteq \#_d$.

Secondly, we define the *immediate reveals* relation, $\triangleright_i$, as: $a \triangleright_i b \overset{def}{\iff} \{a\} \rightarrowtriangle_i \{b\}$. For example, in Fig. 6(b), $b \triangleright_i \psi_\top$ and $\neg(c \triangleright_i \psi_\top)$.

Remark 5.3. When $\triangleright$ is antisymmetric, the reveals relation is the transitive and reflexive closure of the immediate reveals relation and the conflict relation can be deduced by $\triangleright$-inheritance from the immediate conflict relation. Therefore, the conflict relation can be deduced from the immediate reveals relation and the immediate conflict relation: $\# = (\triangleright_i^{-1})^* \circ \#_i \circ \triangleright_i^*$.

6. A Synthesis Problem

In Section 5 we have introduced ERL logic to describe logical dependencies between events of an occurrence net. Now two synthesis problems arise naturally.

First, we show how to build the ERL formula $\Phi^{\mathcal{N}}$ which describes the set of maximal runs of a finite ON $\mathcal{N}$, i.e. such that $\Omega^{\mathcal{N}}_{max} = [\![\Phi^{\mathcal{N}}]\!]$. Then we present a procedure to answer whether there exists a tight net $\mathcal{N}$ such that its set of maximal runs is described by a given ERL formula φ.

This synthesis procedure allows us to understand the power of the logical properties expressed via *reveals*-relations or, equivalently, ERL formulas. They also allow - see below - to identify the canonical shape of occurrence nets with respect to these properties. Note that we restrict our attention in this section to *finite* occurrence nets, i.e. over a fixed finite set of individuals interpreted as events. Naturally, one would hope to obtain synthesis procedures for occurrence nets of arbitrary size, imposing only regularity properties; the set of events would then be structured by an adequate equivalence relation of finite index. However, the technical difficulties posed by this general endeavor have not been resolved; note in particular the fact, highlighted by Fig. 5, that a facet (here ψ_3) may reveal infinitely many others, which means that the procedure below would fail to produce event ψ_3.

Even so, the capability of synthesizing occurrence nets with a given finite set of facets from ERL formulas has potential even in practical terms. In fact, suppose you take any finite occurrence net $\mathcal{ON}$ obtained by synthesis from φ, and convert it into a safe Petri net by adding,

- for every maximal run ω of $\mathcal{ON}$, a transition t_ω whose pre-set is formed by the maximal conditions of ω,
- an extra place p whose post-set is $\{\top\}$ and whose pre-transitions are the t_ω,
- and a token on p and no tokens elsewhere.

Then the resulting net $\mathcal{N}$ is a workflow net whose behaviors are concatenations of ωs, i.e. such that the properties satisfied at each workflow round are given by φ.

6.1. From Occurrence Nets to ERL Formulas

For a given finite ON $\mathcal{N}$, we start by building $\Phi^{\mathcal{N}}_{gen}$, a formula such that $[\![\Phi^{\mathcal{N}}_{gen}]\!] = \Omega^{\mathcal{N}}_{gen}$, from the characterization of general runs. Then we build $\Phi^{\mathcal{N}}$, a formula such that $[\![\Phi^{\mathcal{N}}]\!] = \Omega^{\mathcal{N}}_{max}$, by adding terms corresponding to the progress assumption to $\Phi^{\mathcal{N}}_{gen}$. The construction of $\Phi^{\mathcal{N}}_{gen}$ is similar to [20], where the authors build what they call "configuration constraints" also by considering the causal closure and the conflict-freeness of the configurations (or general runs).

By definition, a set of events is a general run iff it is closed under causality and conflict-free. That is, for a given finite ON $\mathcal{N} = (B, E, F)$, we can build the formula $\Phi^{\mathcal{N}}_{gen}$ as follows:

$$\Phi^{\mathcal{N}}_{gen} = \underbrace{\bigwedge_{a,b\in E, a<b} (b \to a)}_{\text{causal closure}} \wedge \underbrace{\bigwedge_{a,b\in E, a\#b} (\neg a \vee \neg b)}_{\text{conflict-freeness}}$$

Therefore, for a given finite ON $\mathcal{N}$, $\Phi^{\mathcal{N}}$ can be built as follows:

$$\begin{aligned}
\Phi^{\mathcal{N}} \;=\; & \bigwedge_{a,b\in E, a<b} (b \to a) && \text{(causal closure)}\\
\wedge\; & \bigwedge_{a,b\in E, a\#b} (\neg a \vee \neg b) && \text{(conflict-freeness)}\\
\wedge\; & \bigwedge_{a\in E} \Big(\big(\underbrace{\bigwedge_{b\in E, b\lessdot a} b}_{a \text{ enabled}} \big) \to \big(a \vee \bigvee_{c\in E, c\#_d a} c \big) \Big) && \text{(progress assumption)}
\end{aligned}$$

The new part is implied by the maximality and stands for "for any event a, if a is enabled, then a or an event in direct conflict with a has to fire".

Since $<$ is the transitive closure of the direct causality $\lessdot$, the first part can be rewritten using only $\lessdot$, and since $\#$ is inherited through $<$, in the second part, we can consider only the direct conflict $\#_d$, and eventually:

$$\Phi^{\mathcal{N}} \equiv \bigwedge_{a,b\in E, a<b} (b \to a) \wedge \bigwedge_{a,b\in E, a\#_d b} (\neg a \vee \neg b) \wedge \bigwedge_{a\in E} \Big(\big(\bigwedge_{b\in E, b\lessdot a} b \big) \to \big(a \vee \bigvee_{c\in E, c\#_d a} c \big) \Big)$$

Notice that, since $\top$ has no conflict and no causal predecessor, the third part with $a = \top$ gives $\boldsymbol{tt} \to \top$ which can be reduced in $\top$, i.e. $\top$ is always true (and so is $\psi_\top$ when we consider reduced ONs).

For example, in Fig. 6(b):

$$\begin{aligned}
\Phi^{\mathcal{N}} \;\equiv\; & (c' \to b) \wedge (c \to b) \wedge (c \to a) \wedge (d \to a)\\
& \wedge (\bar{a}' \vee \bar{a}) \wedge (\bar{b}' \vee \bar{b}) \wedge (\bar{c}' \vee \bar{c}) \wedge (\bar{c} \vee \bar{d})\\
& \wedge \psi_\top \wedge ((a \wedge b) \to (c \vee c' \vee d))\\
& \wedge (a \to (c \vee d)) \wedge (b \to (c' \vee c))\\
& \wedge (\psi_\top \to (b' \vee b)) \wedge (\psi_\top \to (a' \vee a)),
\end{aligned}$$

where $\bar{a}$ stands for $\neg a$.

We have deliberately omitted terms of the form $a \to \psi_\top$ that are redundant since $\psi_\top$ must be true.

6.1.1. Complexity

The formula is built as a conjunction of terms. First, identifying the causalities and the conflicts requires looking at each pair of events $\{a, b\} \subseteq E$. Therefore, this gives $O(n^2)$ terms with two events, where $n = |E|$. Second, there are n terms that describe the progress assumption (one for each event), and these terms are of size $O(n)$. Therefore, the size of the formula is $O(n^2)$.

6.2. From ERL formulas to Tight Nets: a Synthesis Procedure

The synthesis problem for PNs has been widely studied. It consists in answering whether, given a behavior, there exists a PN with this behavior. The behavior can be specified as a transition system [1, 6, 8, 12] or a language, be it (i) a sequential language: in [11], the behavior is bounded by two regular languages; or (ii) a finite partial language (finite set of labeled partial orders): [5]. Most of the time, the synthesis procedure is based on the notion of region [2, 13].

In this paper, we propose another approach and we solve the following synthesis problem: given an ERL formula φ, is there a tight net $\mathcal{N}$ whose behavior is the one specified by φ, i.e. such that the set of maximal runs of $\mathcal{N}$, $\Omega^{\mathcal{N}}_{max}$, is equivalent to $[\![\varphi]\!]$?

In the sequel, we give a procedure to build a net, $\mathrm{CN}(\varphi)$, from an ERL formula φ. First, a set of binary immediate constraints is extracted from φ, then, $\mathrm{CN}(\varphi)$, is built from these constraints. If $\mathrm{CN}(\varphi)$ is a reduced ON, then $\Phi^{\mathrm{CN}(\varphi)}$ is computed and compared with φ. As in the other synthesis procedures, places are used to restrict the behavior of the net and denote dependencies between occurrences of transitions.

6.2.1. Extracting the Immediate Constraints

The set of maximal runs is given by the conflict relation which can be deduced from the immediate reveals relation and the immediate conflict relation (Lemma 2.1 and Remark 5.3). Therefore, if there exists a reduced ON $\mathcal{N}$ such that $\Omega^{max}_{\mathcal{N}} = [\![\varphi]\!]$, then the binary immediate constraints, i.e. expressions of the form $a \triangleright_i b$ and $a \#_i b$, are enough to describe $\Omega^{max}_{\mathcal{N}}$ (and thus also to describe φ). That is why we focus on binary immediate constraints.

Our problem is to decide whether binary constraints of the form $a \triangleright b$ (respectively $\{a, b\} \twoheadrightarrow \emptyset$) are satisfied by φ. This amounts to deciding whether $\varphi \to (a \to b)$ (respectively $\varphi \to (\neg a \vee \neg b)$) is a tautology. This problem is co-NP-complete and can be solved quite efficiently in practice by SAT-solvers.

6.2.2. Building a Canonical Tight Net

We denote by $\Psi(\varphi)$ the set of variables that appear in φ which is supposed to be "reduced", i.e. such that for any distinct variables $a, b \in \Psi(\varphi)$, $[\![\varphi]\!] \not\models a \leftrightarrow b$. Each binary immediate constraint extracted from φ is represented by a condition connected to the facets that appear in the constraint. The net $\mathrm{CN}(\varphi)$ is defined as follows.

Definition 6.1. ($\mathrm{CN}(\varphi)$)
Let φ be an ERL formula. $\mathrm{CN}(\varphi) = (B, \Psi, F)$ is the finite net such that $\Psi = \Psi(\varphi)$, $B = B_1 \cup B_2$ and $F = F_1 \cup F_2$, where:

- $B_1 = \big\{\{\psi, \psi'\} \mid \psi \#_i \psi'\big\}$,

- $F_1 = \big\{(\{\psi, \psi'\}, \psi) \in B_1 \times \Psi\big\} \cup \big\{(\psi_\top, \{\psi, \psi'\}) \in \Psi \times B_1\big\}$.

That is, for each constraint of the form $\psi \#_i \psi'$, one condition b is created and connected to $\psi_\top$, ψ and ψ' such that ${}^\bullet b = \{\psi_\top\}$ and $b^\bullet = \{\psi, \psi'\}$.

- $B_2 = \big\{(\psi, \psi') \in (\Psi \setminus \{\psi_\top\})^2 \mid \psi' \triangleright_i \psi\big\}$,
- $F_2 = \big\{\big((\psi, \psi'), \psi'\big) \in B_2 \times \Psi\big\} \cup \big\{\big(\psi, (\psi, \psi')\big) \in \Psi \times B_2\big\}$.

That is, for each constraint of the form $\psi' \triangleright_i \psi$, one condition is created and connected to ψ and ψ' such that ${}^\bullet b = \{\psi\}$ and $b^\bullet = \{\psi'\}$. Notice that constraints of the form $\psi \triangleright_i \psi_\top$ are not considered because, if φ describes the maximal runs of a reduced ON, they are already represented by B_1 and F_1.

Remark 6.1. Actually, it is more the set of runs described by φ, i.e. $[\![\varphi]\!]$, than φ itself which is interesting. Indeed for two formulas, φ_1 and φ_2, $\varphi_1 \equiv \varphi_2 \iff \mathrm{CN}(\varphi_1) = \mathrm{CN}(\varphi_2)$. Therefore, we could also define $\mathrm{CN}(\Omega)$ for a given $\Omega \subseteq 2^\Psi$.

Lemma 6.1. Let $\mathcal{N}$ be a finite reduced ON, then $\mathrm{CN}(\Phi^\mathcal{N})$ is a tight net and $\Phi^{\mathrm{CN}(\Phi^\mathcal{N})} \equiv \Phi^\mathcal{N}$.

Proof:
First, we show that $\mathrm{CN}(\Phi^\mathcal{N})$ is a tight net. We call $\mathcal{CN}$ the net $\mathrm{CN}(\Phi^\mathcal{N})$. We first show that $\mathcal{CN}$ is an ON, then that it is reduced, and lastly that it is a tight net. $\mathcal{N}$ and $\mathcal{CN}$ have the same conflict relation, because they have the same reveals relation and the same immediate conflict relation (Remark 5.3). Moreover $\mathcal{CN}$ is built so that $\forall a, b \in \Psi, a \leq_\mathcal{CN} b \iff b \triangleright a$. Therefore, $\mathcal{CN}$ is an ON because:

- There is no self-conflict in $\mathcal{CN}$, because there is no self-conflict in $\mathcal{N}$.
- $\leq_\mathcal{CN}$ is equivalent to $\triangleright^{-1}$ therefore it is a partial order.
- $\forall \psi \in \Psi, \{\psi' \mid \psi' \leq_\mathcal{CN} \psi\}$ is finite because Ψ is finite.
- There is no backward branching by construction.
- $\psi_\top \in \Psi$ is the only minimal node by construction.

Since $\Phi^\mathcal{N}$ is associated with the reduced ON $\mathcal{N}$, it is such that, for any distinct variables $v_1, v_2 \in \Psi$, $[\![\Phi^\mathcal{N}]\!] \not\models v_1 \leftrightarrow v_2$. Therefore, $\mathcal{CN}$ is also reduced. Lastly, by construction, $\mathcal{CN}$ is a tight net.

Second, we show that $\Phi^{\mathrm{CN}(\Phi^\mathcal{N})} \equiv \Phi^\mathcal{N}$. By Lemma 2.1, the set of maximal runs can be defined from the conflict relation only. $\mathcal{N}$ and $\mathrm{CN}(\Phi^\mathcal{N})$ have the same conflict relation. Therefore, $\mathcal{N}$ and $\mathrm{CN}(\Phi^\mathcal{N})$ have the same set of runs and equivalent associated ERL formulas. □

Notice that $\mathcal{N}$ and $\mathrm{CN}(\Phi^\mathcal{N})$ may not accept the same general runs because the facets that are concurrent but related by the reveals relation in $\mathcal{N}$, become causally ordered in $\mathrm{CN}(\Phi^\mathcal{N})$.

From Lemma 6.1, we can derive the following theorem.

Theorem 6.1. Let φ be an ERL formula such that for any distinct variables $a, b \in \Psi(\varphi)$, $[\![\varphi]\!] \not\models a \leftrightarrow b$. There exists a reduced ON $\mathcal{N}$ such that $\Phi^\mathcal{N} \equiv \varphi$ iff $\mathrm{CN}(\varphi)$ is a reduced ON and $\Phi^{\mathrm{CN}(\varphi)} \equiv \varphi$.

Proof:
($\Rightarrow$) If there exists a reduced ON $\mathcal{N}$ such that $\Phi^{\mathcal{N}} \equiv \varphi$, then, by Lemma 6.1 $\mathrm{CN}(\varphi)$ is a candidate.
($\Leftarrow$) $\mathrm{CN}(\varphi)$ is an example of suitable reduced ON. □

Example 6.4 illustrates that the net $\mathrm{CN}(\varphi)$, obtained by the synthesis from an arbitrary formula φ, may not be a reduced ON. When $\mathrm{CN}(\varphi)$ is a reduced ON, it is called the *canonical tight net* associated with φ (or with $\mathcal{N}$ when ϕ is defined as the formula $\Phi^{\mathcal{N}}$ associated with some reduced occurrence net $\mathcal{N}$).

6.2.3. Examples

We extract a set of binary immediate constraints from φ and build the net $\mathrm{CN}(\varphi)$.

Example 6.1. Consider the following formula:

$$\begin{aligned}\varphi = \quad & \psi_\top \wedge (a \to b) \wedge (b' \to a') \\ & \wedge (\bar{a} \vee \bar{a'}) \wedge (\bar{b} \vee \bar{b'}) \\ & \wedge (a \vee a') \wedge (b \vee b')\end{aligned}$$

The set of runs described by φ is $[\![\varphi]\!] = \big\{\{\psi_\top, a, b\}, \{\psi_\top, a', b\}, \{\psi_\top, a', b'\}\big\}$. The binary immediate constraints are: $a \triangleright_i b$, $b' \triangleright_i a'$, $b \triangleright_i \psi_\top$, $a' \triangleright_i \psi_\top$, $a \#_i a'$ and $b \#_i b'$, and the net synthesized from these constraints is given in Fig. 7(a). This net is a reduced ON and its set of maximal runs is indeed $[\![\varphi]\!]$.

Example 6.2. Consider the following formula:

$$\varphi = \psi_\top \wedge (\bar{a} \vee \bar{b})$$

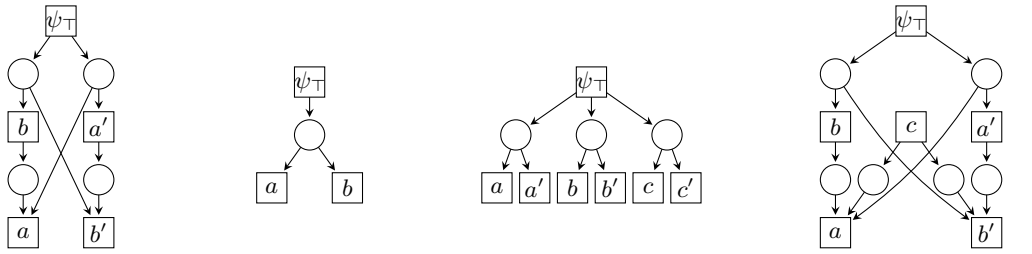
The set of runs described by φ is $[\![\varphi]\!] = \big\{\{\psi_\top\}, \{\psi_\top, a\}, \{\psi_\top, b\}\big\}$. The binary immediate constraints are: $a \triangleright_i \psi_\top$, $b \triangleright_i \psi_\top$ and $a \#_i b$, and the ON $\mathcal{N}$ synthesized from these constraints is given in Fig. 7(b). $\mathcal{N}$ is a reduced ON but $\Omega^{\mathcal{N}} = \big\{\{\psi_\top, a\}, \{\psi_\top, b\}\big\} \neq [\![\varphi]\!]$. Therefore, there is no reduced ON $\mathcal{N}$ such that $\varphi \equiv \Phi^{\mathcal{N}}$. We can see that the maximality constraint $a \vee b$ is not respected by φ.

Example 6.3. Consider the following formula:

$$\begin{aligned}\varphi = \quad & (\psi_\top \wedge a \wedge b \wedge \bar{c} \wedge \bar{a'} \wedge \bar{b'} \wedge c') \\ & \vee (\psi_\top \wedge a \wedge \bar{b} \wedge c \wedge \bar{a'} \wedge b' \wedge \bar{c'}) \\ & \vee (\psi_\top \wedge \bar{a} \wedge b \wedge c \wedge a' \wedge \bar{b'} \wedge \bar{c'}) \\ & \vee (\psi_\top \wedge \bar{a} \wedge \bar{b} \wedge \bar{c} \wedge a' \wedge b' \wedge c')\end{aligned}$$

The set of runs described by φ is $[\![\varphi]\!] = \big\{\{\psi_\top, a, b, c'\}, \{\psi_\top, a, b', c\}, \{\psi_\top, a', b, c\}\big\}$. The binary immediate constraints are: $a \#_i a'$, $b \#_i b'$, $c \#_i c'$ and for each $\psi \in \Psi \setminus \{\psi_\top\}$, $\psi \triangleright_i \psi_\top$. The ON $\mathcal{N}$ synthesized from these constraints is given in Fig. 7(c). $\mathcal{N}$ is a reduced ON but $\Omega^{\mathcal{N}} = \big\{\{\psi_\top, a, b, c\}, \{\psi_\top, a', b, c\}, \{\psi_\top, a, b', c\}, \{\psi_\top, a, b, c'\}, \{\psi_\top, a', b', c'\}, \{\psi_\top, a, b', c'\}, \{\psi_\top, a', b, c'\}, \{\psi_\top, a', b', c\}\big\} \neq [\![\varphi]\!]$. Therefore, there is no reduced ON $\mathcal{N}$ such that $\varphi \equiv \Phi^{\mathcal{N}}$.

Notice that this example illustrates an immediate conflict between a, b and c: $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$ can occur in a run, but $\{a, b, c\}$ cannot, which is not possible in general ONs (see Lemma 5.1).



(a) $\Phi^{\mathrm{CN}(\varphi)} \equiv \varphi$ (b) $\Phi^{\mathrm{CN}(\varphi)} \not\equiv \varphi$ (c) $\Phi^{\mathrm{CN}(\varphi)} \not\equiv \varphi$ (d) $\mathrm{CN}(\varphi)$ is not an ON

Figure 7. (a): There is a reduced ON $\mathcal{N}$ such that $\varphi \equiv \Phi^{\mathcal{N}}$. (b) to (d): There is no reduced ON $\mathcal{N}$ such that $\varphi \equiv \Phi^{\mathcal{N}}$.

Example 6.4. Consider the following formula:

$$\begin{aligned}\varphi = \quad & \psi_\top \wedge (a \to c) \wedge (b' \to c) \wedge (b' \to a') \\ & \wedge (\bar{a} \vee \bar{a'}) \wedge (\bar{b} \vee \bar{b'}) \\ & \wedge (a \vee a') \wedge (b \vee b') \wedge (c \to (a \vee b'))\end{aligned}$$

The set of runs described by φ is $[\![\varphi]\!] = \big\{\{\psi_\top, a, b, c\}, \{\psi_\top, a', b', c\}, \{\psi_\top, a', b\}\big\}$. The binary immediate constraints are: $a \triangleright_i b$, $a \triangleright_i c$, $b' \triangleright_i a'$, $b' \triangleright_i c$, $b \triangleright_i \psi_\top$, $a' \triangleright_i \psi_\top$, $c \triangleright_i \psi_\top$, $a \#_i a'$ and $b \#_i b'$, and the net synthesized from these constraints is given in Fig. 7(d). We can see that this net is not an ON because there are two minimal events, c and $\psi_\top$. Therefore, there is no reduced ON $\mathcal{N}$ such that $\varphi \equiv \Phi^{\mathcal{N}}$.

6.2.4. Complexity

Identifying the immediate constraints requires looking at each pair of facets $\{a, b\} \subseteq \Psi(\varphi)$, and for each pair, deciding whether the formula $\varphi \to (a \to b)$ (respectively $\varphi \to (\neg a \vee \neg b)$) is a tautology is co-NP-complete.

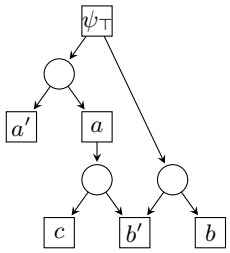
Once the immediate constraints are computed, the number of places and arcs in $\mathrm{CN}(\varphi)$ is linear in the number of constraints, and therefore at most quadratic in the number of events. The events are simply the variables that appear in the formula. The quadratic bound is reached for a formula of the type $(\psi_1 \vee \cdots \vee \psi_n) \to (\psi'_1 \wedge \cdots \wedge \psi'_n)$ which implies $\psi_i \to \psi'_j$ for all i, j.

7. Going Further

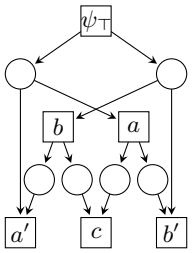
7.1. Tightening a reduced ON

A simple corollary of our synthesis procedures is the following.

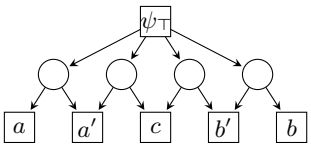
Corollary 7.1. Given any finite reduced ON $\mathcal{N}$, it is always possible to build a tight net $\mathcal{N}'$ such that $\Omega^{\mathcal{N}} = \Omega_{\mathcal{N}'}$.



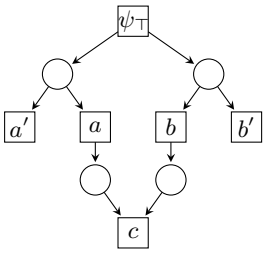
(a) Reduced ON $\mathcal{N}_1$



(b) Canonical tight net associated with $\mathcal{N}_1$



(c) Reduced ON $\mathcal{N}_2$



(d) Canonical tight net associated with $\mathcal{N}_2$

Figure 8. Examples of reduced ONs with their associated canonical tight net.

Proof:
We can compute $\Phi^{\mathcal{N}}$ as in Subsection 6.1, and build the tight net $\mathcal{N}' = \mathrm{CN}(\Phi^{\mathcal{N}})$ as in Subsection 6.2. □

The example of Fig. 5, shows that the corollary does not hold in general if we drop the assumption of finiteness.

Example 7.1. The initial reduced ON, $\mathcal{N}_1$, is depicted in Fig. 8(a). The set of maximal runs is $\Omega_{\mathcal{N}_1} = \{\{\psi_\top, a, b, c\}, \{\psi_\top, a, b'\}, \{\psi_\top, a', b\}\}$ and the binary immediate constraints are $a \triangleright_i \psi_\top$, $b \triangleright_i \psi_\top$, $c \triangleright_i a$, $c \triangleright_i b$, $a' \triangleright_i b$, $b' \triangleright_i a$, $a \#_i a'$ and $b \#_i b'$. The canonical tight net obtained by the synthesis from these constraints is represented in Fig. 8(b).

Example 7.2. Fig. 8(c) and 8(d) give another example of a reduced ON and its associated canonical tight net. The set of maximal runs is $\Omega_{\mathcal{N}_2} = \{\{\psi_\top, a, b, c\}, \{\psi_\top, a, b'\}, \{\psi_\top, a', b\}, \{\psi_\top, a', b'\}\}$ and the binary immediate constraints are $a \triangleright_i \psi_\top$, $b \triangleright_i \psi_\top$, $c \triangleright_i a$, $c \triangleright_i b$, $a \#_i a'$ and $b \#_i b'$.

It is a fact that the modifications brought about by (reduction and) tightening are often counter-intuitive and are unconventional net surgeries. At the same time, we believe that the "right" interpretation of these structural modifications should not be sought in the usual form of *temporal* properties. Rather, the reveals relations show *logical* dependencies that can be used for inference properties of the type "if a is known, then b must be the case". Thus the resulting net is in fact drastically changed, to better reflect which deductions are possible e.g. from a partial observation of behaviors.

7.2. Characterization of adequate $[\![\varphi]\!]$

There are two reasons why an ERL formula φ does not describe the set of maximal runs of any ON: either the formula allows non-maximal runs, or it expresses non-binary minimal conflicts, while all minimal conflicts are binary in occurrence nets under the maximal semantics (see Lemma 5.1).

It is possible to characterize directly the formulas φ (or equivalently the sets Γ of sets of events) such that $[\![\varphi]\!]$ (respectively Γ) is the set of maximal runs of an ON.

Theorem 7.1. (Direct characterization of adequate Γ)
Let E be a finite set whose elements are called events, and $\Gamma \subseteq 2^E$ such that any event occurs at least once in Γ, and one event denoted $\top$ occurs in all the sets of Γ. Then, there exists an ON $\mathcal{N}$ such that $\Omega_{\mathcal{N}} = \Gamma$, iff

$$\Gamma = \{\gamma \subseteq E \mid \forall a \in E,\ a \in \gamma \iff \#[a] \cap \gamma = \emptyset\}$$

where the $\#$ relation over E is defined as:

$$a \# b \overset{def}{\iff} \nexists \gamma \in \Gamma : \{a, b\} \subseteq \gamma\,.$$

Proof:
By Prop. 5.1, any ON $\mathcal{N}$ satisfying $\Omega_{\mathcal{N}} = \Gamma$, has $\#$ as its conflict relation. Then by Lemma 2.1 Γ is its set of maximal runs.

Now, when $\Gamma = \{\gamma \subseteq E \mid \forall a \in E,\ a \in \gamma \iff \#[a] \cap \gamma = \emptyset\}$, we can define an occurrence net $\mathcal{N} = (B, E, F)$ whose set of events is E, whose set of conditions is $B \overset{def}{=} \{\{e, e'\} \mid e \# e'\}$ and whose flow relation F is defined such that $\top^\bullet = B$ and for every $e \in E \setminus \{\top\}$, ${}^\bullet e = \{\{e, e'\} \mid e \# e'\}$ and $e^\bullet = \emptyset$. $\mathcal{N}$ trivially satisfies the conditions for being an occurrence net. Moreover, its set of maximal runs coincides with Γ, by immediate application of Lemma 2.1. □

Remark 7.1. Let Γ be a set of sets of events satisfying the condition of Theorem 7.1. The occurrence nets $\mathcal{N}$ such that $\Omega_{\mathcal{N}} = \Gamma$ are reduced iff for all distinct events $a, b \in E$, $\Gamma \not\models a \leftrightarrow b$, or equivalently $\#[a] \neq \#[b]$. Indeed, combining the definition of facets and Lemma 3.1, we get that two events a and b are in the same facet iff $\#[a] = \#[b]$.

7.3. Untightened synthesis

As well as runs are given as *unordered* sets of events, the syntax of ERL logic does not consider the *structural causality* between events. Therefore, the synthesis problem that we solve in Section 6 mentions only the logical dependencies between events and not the structural ones. This means that the causalities between events in the synthesized net, which represent the logical dependencies given by the formula, may come from causalities in the original net or from more complex dependencies involving the maximal progress assumption.

Indeed, we decided to represent the logical dependencies as causalities, and that is the reason why we get a tight net. However, we observed in Lemma 2.1 that the conflict relation gives enough information to define the maximal runs. That is, preserving the conflict relation is preserving the set of maximal runs. Hence, given a set of maximal runs, it is always possible to solve the synthesis problem by building a net with no causality (but the ones required by $\top$) and only conflicts, like the ones used in the proof of Theorem 7.1. Fig. 8(c) shows an example of such ON. However, with this construction, the reveals

relations in the resulting net are all hidden in the conflict relation, whereas our net $\mathrm{CN}(\varphi)$ makes explicit all the binary reveals relations as causalities, which lets us represent as little direct conflicts as possible, i.e. only the immediate conflict.

Between these two choices of representation there is a range of other possible choices which differ by the chosen causality relation (and therefore also by the conflict relation). The point is now to characterize the acceptable choices for the direct causality relation to impose in the net. To answer this question, we introduce a synthesis where a relation $\preceq$ is given, together with a formula φ. The synthesis problem is now: given an ERL formula φ on a set E of events (containing $\top$) and a partial order relation $\preceq$ on E, is there an ON $\mathcal{N}$ whose behavior is the one specified by φ, and such that the causality in $\mathcal{N}$ matches $\preceq$?

In order to solve this synthesis problem, we adapt the construction $\mathrm{CN}(\varphi)$ of Def. 6.1 in order to represent only the causalities described by $\preceq$: for each pair of events (e, e') in the transitive reduction $\prec_i$ of $\preceq$, a condition b is created and connected to e and e' (${}^\bullet b = \{e\}$ and $b^\bullet = \{e'\}$). Then, we want to represent as few direct conflicts as possible w.r.t. this imposed causality, and in order to adapt our construction, we define the direct conflict of our synthesized net, similarly to the immediate conflict, but with $\preceq$ instead of $\triangleright$.

$$a \#_d b \overset{def}{\iff} a \# b \wedge \nexists c : (c \prec a \wedge c \# b) \vee (c \prec b \wedge c \# a)$$

where $\prec$ denotes the reflexive reduction of $\preceq$.

Notice also that the general conflict relation can be defined with this direct conflict and the relation $\preceq$, as: $\# = \preceq^{-1} \circ \#_d \circ \preceq$. Therefore, the construction of Subsection 6.2 can be adapted by replacing $\#_i$ by $\#_d$ and $\triangleright_i$ by $\prec_i^{-1}$.

Definition 7.1. ($\mathrm{CN}(\varphi, \preceq)$)
Let φ be an ERL formula over a set E of events (containing $\top$) and $\preceq$ a partial order relation over E. $\mathrm{CN}(\varphi, \preceq) = (B, E, F)$ is the finite net where E is the set of events, $B = B_1 \cup B_2$ and $F = F_1 \cup F_2$, with:

- $B_1 = \big\{\{e, e'\} \mid e \#_d e'\big\}$,
- $F_1 = \big\{(\{e, e'\}, e) \in B_1 \times E\big\} \cup \big\{(\top, \{e, e'\}) \in E \times B_1\big\}$.
- $B_2 = \prec_i$,
- $F_2 = \big\{\big((e, e'), e'\big) \in B_2 \times E\big\} \cup \big\{\big(e, (e, e')\big) \in E \times B_2\big\}$.

Then, Lemma 6.1 and Theorem 6.1 can be strengthened to:

Lemma 7.1. Let $\mathcal{N}$ be a finite ON, and $\preceq$ a partial order relation on E such that $\top$ is the only minimal event w.r.t. $\preceq$ and $\preceq$ is a subrelation of the reverse of the reveals relation of $\mathcal{N}$. Then $\mathrm{CN}(\Phi^{\mathcal{N}}, \preceq)$ is an ON and $\Phi^{\mathrm{CN}(\Phi^{\mathcal{N}}, \preceq)} \equiv \Phi^{\mathcal{N}}$ and the causality in $\mathcal{N}$ matches $\preceq$.

Proof:
The proof follows the steps of the proof of Lemma 6.1. □

Now comes the main result of this section, which states that, while synthesizing an ON $\mathcal{N}$ from an ERL formula φ, the causality in $\mathcal{N}$ (denoted $\leq_{\mathcal{N}}$) can be freely chosen provided it is compatible with the reveals relation induced by φ.

Theorem 7.2. Given an adequate formula φ (i.e. a formula that describes the set of maximal runs of some ON), an ON $\mathcal{N}$ such that $\Phi^{\mathcal{N}} \equiv \varphi$ and $\leq_{\mathcal{N}} = \preceq$ exists for any partial order relation $\preceq$ on E, provided $\top$ is the only minimal event w.r.t. $\preceq$ and $\preceq$ is a subrelation of the reverse of the reveals relation induced by φ.

Proof:
The existence of $\mathcal{N}$ trivially implies the required conditions on $\preceq$. The other direction is ensured by Lemma 7.1. □

As previously mentioned, there are two special cases of such synthesis:

- $\preceq = \triangleright^{-1}$, then $\#_d = \#_i$ and the resulting net is a tight net.
- $\preceq$ relates simply $\top$ to any event; then $\#_d = \#$ and the resulting net has no causality but the one linking any event to $\top$.

Remark 7.2. For a given set of runs (or ERL formula), less causality implies more direct conflict in the synthesized net: $\preceq_1 \subseteq \preceq_2 \Rightarrow \#_{d2} \subseteq \#_{d1}$.

Example 7.3. Consider again the reduced ON $\mathcal{N}_1$, depicted in Fig. 8(a). Its associated canonical tight net was built in Example 7.1. Define now $\preceq$ such that $\prec$ relates a to c and $\psi_\top$ to every facet (except $\psi_\top$). Our goal is to build $\mathrm{CN}(\Phi^{\mathcal{N}_1}, \preceq)$. The direct conflicts w.r.t. $\preceq$ are: $a \#_d a'$, $b \#_d b'$, $c \#_d b'$ and $a' \#_d b'$. The reduced ON $\mathcal{N}_1'$ obtained by the synthesis from these constraints is represented in Fig. 9(a).

If we define now another $\preceq$ that relates simply $\psi_\top$ to the other facets, then the direct conflicts are the same as above plus $c \#_d b'$ (actually every conflict becomes direct). And the ON $\mathcal{N}_1''$ obtained by the synthesis from these constraints is represented in Fig. 9(b).

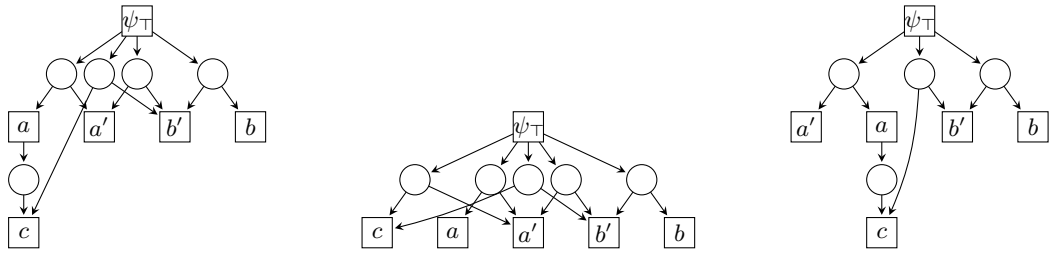
Example 7.4. Consider now the reduced ON $\mathcal{N}_2$, depicted in Fig. 8(c). $\mathcal{N}_2$ is already the result of the synthesis with no causality (except causality from $\psi_\top$ to every other facet).

Define now $\preceq$ such that $\prec$ also relates a to c. Then the direct conflicts w.r.t. $\preceq$ are $a \#_d a'$, $b \#_d b'$ and $c \#_d b'$. The reduced ON obtained by the synthesis from these constraints is represented in Fig. 9(c).

7.3.1. Synthesis in the General Semantics

We have seen in Subsection 6.1 that the set of general runs of an occurrence net can be expressed as the following ERL.

$$\Phi^{\mathcal{N}}_{gen} = \underbrace{\bigwedge_{a,b \in E, a<b} (b \to a)}_{\text{causal closure}} \wedge \underbrace{\bigwedge_{a,b \in E, a \# b} (\neg a \vee \neg b)}_{\text{conflict-freeness}}$$



(a) Reduced ON $\mathcal{N}_1'$ ($a \prec_i c$) (b) Reduced ON $\mathcal{N}_1''$ (c) Reduced ON $\mathcal{N}_2'$ ($a \prec_i c$)

Figure 9. Examples of synthesis parameterized by a causality relation $\preceq$. According to Def. 7.1, additional conditions and arcs should connect $\psi_\top$ to other facets in order to code causality. They are omitted here since this causality is already induced by the conditions used to code the conflicts.

Now we show that the problem of synthesizing an occurrence net from an ERL formula can also be solved for the general semantics. More surprisingly, the procedure for solving it is exactly the same as in Subsection 6.2 and Theorem 6.1 can be adapted.

Theorem 7.3. Let φ be an ERL formula such that for any distinct variables $a, b \in \Psi(\varphi)$, $[\![\varphi]\!] \not\models a \leftrightarrow b$. There exists a finite reduced ON $\mathcal{N}$ such that $\Phi^{\mathcal{N}}_{gen} \equiv \varphi$ iff $\mathrm{CN}(\varphi)$ is a reduced ON and $\Phi^{\mathrm{CN}(\varphi)}_{gen} \equiv \varphi$.

Proof:
The steps described in 6.2.1 and 6.2.2, can be repeated. Then we prove that if $\mathcal{N}$ is a finite reduced ON, then $\mathrm{CN}(\Phi^{\mathcal{N}}_{gen})$ is a tight net and $\Phi^{\mathrm{CN}(\Phi^{\mathcal{N}}_{gen})}_{gen} \equiv \Phi^{\mathcal{N}}_{gen}$, as in the proof of Lemma 6.1, except that, in order to prove that $\mathcal{N}$ and $\mathrm{CN}(\Phi^{\mathcal{N}}_{gen})$ have equivalent formulas (i.e. the same set of general runs), we use that they have the same conflict an causality relations. □

With the general semantics, the set of runs cannot be described with the conflict relation only. But since a net $\mathrm{CN}(\Phi^{\mathcal{N}})$, built from the formula associated with ON $\mathcal{N}$ has the same causality and conflict relations as $\mathcal{N}$, they accept the same set of general runs. Notice also that we have no longer the choice on the causality relation.

Remark 7.3. In the construction, the immediate conflicts are represented by a condition connected to $\psi_\top$. This results in a large set of initial conditions. It is possible to improve the construction by representing each immediate conflict $\psi \#_i \psi'$ by a condition connected to any facet ψ_1 such that $\psi \triangleright \psi_1$ and $\psi' \triangleright \psi_1$. One possible choice would be to consider the $\triangleright$-successors of ψ and ψ', defined as $\triangleright[\psi, \psi'] = \{\psi_1 \in \Psi \mid \psi \triangleright \psi_1 \wedge \psi' \triangleright \psi_1\}$, create one condition b_1 for each $\triangleright$-minimal facet, ψ_1, in $\triangleright[\psi, \psi']$, and connect b_1 to ψ_1, ψ and ψ'. This would define B_1 and F_1. Then, any constraint of the form $\psi' \triangleright_i \psi$ would be represented as previously by B_2 and F_2, except that, in B_2, we need to consider only non-redundant conditions. Indeed, if there exists $b \in B_1$ such that $(\psi, b) \in F_1 \wedge (b, \psi') \in F_1$, then $\psi' \triangleright_i \psi$ is already represented and can be ignored in B_2.

8. Conclusion

We have shown how the structural and binary *reveals*-relation from [18] generalizes into a relational framework for the description of *logical* dependencies - as opposed to *temporal* ones - between occurrences of sets of events in occurrence nets. For expressing these properties, a new logic, ERL, has been introduced and studied. In particular, we have solved the problem of synthesis for finite occurrence nets from ERL formulas. The extension to general occurrence nets is a future task, which is not trivial; see Fig. 5 and the discussion at the beginning of Section 6.

Even if ERL is a logic adapted for partial order semantics, it differs in its aim and structure from the other logics that have been proposed in the literature (for temporal logics for traces and event structures, see e.g. [17, 24]). First, ERL is not, strictly speaking, a *temporal* logic, since the notions of *before*, *after*, *future*, *until* etc. are of no particular relevance here; in fact, the progression of time is encapsulated in the underlying structure over which one chooses to interpret ERL formulas, and in the choice of admissible runs in that structure: maximal runs, any runs, runs satisfying additional context or timing constraints, etc. In the light of Subsection 7.3, causal ordering can be viewed as a refinement of the logical dependencies captured by the ERL formulas.

Thus far, we have intended and used the ERL logic as a means for coding and manipulating *structure* (of occurrence nets) and *knowledge* (observing A reveals B, i.e. gives knowledge about B's occurrence). The results here open some new roads towards efficient verification of system properties, as well as towards *enforcing* such properties through behavior control, or directly through synthesis of systems from logical specifications.

References

[1] Badouel, E., Caillaud, B., Darondeau, P.: Distributing Finite Automata through Petri Net Synthesis, *Journal on Formal Aspects of Computing*, **13**, 2002, 447–470.

[2] Badouel, E., Darondeau, P.: Theory of regions, in: *Lectures on Petri Nets I: Basic Models*, vol. 1491 of *LNCS*, Springer Berlin / Heidelberg, 1998, 529–586.

[3] Balaguer, S., Chatain, T., Haar, S.: Building Tight Occurrence Nets from Reveals Relations, *Proceedings of the 11th International Conference on Application of Concurrency to System Design (ACSD'11)* (B. Caillaud, J. Carmona, Eds.), IEEE Computer Society Press, Newcastle upon Tyne, UK, June 2011.

[4] Baldan, P., Corradini, A., Montanari, U.: Contextual Petri Nets, Asymmetric Event Structures, and Processes, *Information and Computation*, **171**(1), 2001, 1–49.

[5] Bergenthum, R., Desel, J., Lorenz, R., Mauser, S.: Synthesis of Petri Nets from Finite Partial Languages, *Fundam. Inform.*, **88**(4), 2008, 437–468.

[6] Bernardinello, L.: Synthesis of Net Systems, *ICATPN*, 691, Springer, 1993, ISBN 3-540-56863-8.

[7] Busi, N., Pinna, G. M.: Non Sequential Semantics for Contextual P/T Nets, *Application and Theory of Petri Nets*, 1091, Springer, 1996.

[8] Carmona, J., Cortadella, J., Kishinevsky, M., Kondratyev, A., Lavagno, L., Yakovlev, A.: A Symbolic Algorithm for the Synthesis of Bounded Petri Nets, in: *ICATPN*, vol. 5062 of *LNCS*, Springer-Verlag, 2008, 92–111.

[9] Chatain, T., Fabre, É.: Factorization Properties of Symbolic Unfoldings of Colored Petri Nets, *Petri Nets*, 6128, Springer, 2010, ISBN 978-3-642-13674-0.

[10] Chatain, T., Jard, C.: Symbolic Diagnosis of Partially Observable Concurrent Systems, *FORTE*, 3235, 2004.

[11] Darondeau, P.: Deriving Unbounded Petri Nets from Formal Languages, *CONCUR*, 1466, Springer, 1998, ISBN 3-540-64896-8.

[12] Desel, J., Reisig, W.: The synthesis problem of Petri nets, *Acta Inf.*, **33**, 1996, 297–315, ISSN 0001-5903.

[13] Ehrenfeucht, A., Rozenberg, G.: Partial (Set) 2-Structures. Parts I and II, *Acta Inf.*, **27**(4), 1989, 315–368.

[14] Ehrig, H., Hoffmann, K., Padberg, J., Baldan, P., Heckel, R.: High-Level Net Processes, *Formal and Natural Computing*, 2300, Springer, 2002.

[15] Engelfriet, J.: Branching Processes of Petri Nets, *Acta Inf.*, **28**(6), 1991, 575–591.

[16] Esparza, J., Römer, S., Vogler, W.: An Improvement of McMillan's Unfolding Algorithm, *Formal Methods in System Design*, **20**(3), 2002, 285–310.

[17] Gastin, P., Kuske, D.: Uniform satisfiability problem for local temporal logics over Mazurkiewicz traces, *Information and Computation*, **208**(7), 2010, 797–816.

[18] Haar, S.: Types of Asynchronous Diagnosability and the *Reveals*-Relation in Occurrence Nets, *IEEE Transactions on Automatic Control*, **55**(10), 2010, 2310–2320.

[19] Khomenko, V.: *Model Checking Based on Prefixes of Petri Net Unfoldings*, Ph.D. Thesis, School of Computing Science, University of Newcastle upon Tyne, 2003.

[20] Khomenko, V., Koutny, M., Yakovlev, A.: Detecting State Encoding Conflicts in STG Unfoldings Using SAT, *Fundam. Inf.*, **62**(2), 2004, 221–241, ISSN 0169-2968.

[21] McMillan, K. L.: Using Unfoldings to Avoid the State Explosion Problem in the Verification of Asynchronous Circuits, *CAV*, 663, Springer, 1992, ISBN 3-540-56496-9.

[22] Merlin, P. M.: *A study of the recoverability of computing systems*, Ph.D. Thesis, University of California, Irvine, 1974.

[23] Nielsen, M., Plotkin, G. D., Winskel, G.: Petri Nets, Event Structures and Domains, Part I, *Theor. Comput. Sci.*, **13**, 1981, 85–108.

[24] Penczek, W.: Branching Time and Partial Order in Temporal Logics, *Time and Logic: A Computational Approach*, UCL Press, 1995.

[25] Vogler, W.: Fairness and Partial Order Semantics, *Inf. Process. Lett.*, **55**(1), 1995, 33–39.

[26] Vogler, W.: Partial order semantics and read arcs, *Theoretical Computer Science*, **286**(1), 2002, 33–63.

[27] Winkowski, J.: Processes of Contextual Nets and their Characteristics, *Fundamenta Informaticae*, **36**(1), 1998.