Taking Complete Finite Prefixes To High Level, Symbolically (Full Version)

Nick Würdemann, Thomas Chatain, Stefan Haar

▶ **To cite this version:**

Nick Würdemann, Thomas Chatain, Stefan Haar. Taking Complete Finite Prefixes To High Level, Symbolically (Full Version). Petri Nets 2023 - 44TH International Conference on Applications and Theory of Petri Nets and Concurrency, R&D Group on Reconfigurable and Embedded Systems at NOVA School of Science and Technology, Mar 2023, Caparica (Lisbonne), Portugal. hal-04029490

HAL Id: hal-04029490
https://inria.hal.science/hal-04029490

Submitted on 15 Mar 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Taking Complete Finite Prefixes To High Level, Symbolically (Full Version)

Nick Würdemann[1], Thomas Chatain[2], and Stefan Haar[2]

[1] Department of Computing Science, University of Oldenburg, Oldenburg, Germany
wuerdemann@informatik.uni-oldenburg.de
[2] Université Paris-Saclay, INRIA and LMF, CNRS and ENS Paris-Saclay, Gif-sur-Yvette, France
{thomas.chatain,stefan.haar}@inria.fr

Abstract. Unfoldings are a well known partial-order semantics of P/T Petri nets that can be applied to various model checking or verification problems. For *high-level* Petri nets, the so-called *symbolic* unfolding generalizes this notion. A complete finite prefix of the unfolding of a P/T Petri net contains all information to verify, e.g., reachability of markings. We unite these two concepts and define complete finite prefixes of the symbolic unfolding of high-level Petri nets. For a class of safe high-level Petri nets, we generalize the well-known algorithm by Esparza et al. for constructing small such prefixes. Additionally, we identify a more general class of nets with infinitely many reachable markings, for which an approach with an adapted cut-off criterion extends the complete prefix methodology, in the sense that the original algorithm cannot be applied to the P/T net represented by a high-level net.

1 Introduction

Petri nets [17], also called P/T (for Place/Transition) Petri nets or low-level Petri nets, are a well-established formalism for describing distributed systems. *High-level Petri nets* [12] (also called *colored Petri nets*) are a concise representation of P/T Petri nets, allowing the places to carry tokens of different colors. Every high-level Petri net represents a P/T Petri net, here called its *expansion*[3], where the process of constructing this P/T net is called *expanding* the high-level net.

Unfoldings of P/T Petri nets are introduced by Nielsen et al. in [15]. Engelfriet generalizes this concept in [9] by introducing the notion of *branching processes*, and shows that the unfolding of a net is its maximal branching process. In [14], McMillan gives an algorithm to compute a complete finite prefix of the unfolding of a given Petri net. In a well-known paper [10], Esparza, Römer, and Vogler improve this algorithm by defining and exploiting a total order on the set of configurations in the unfolding. We call the improved algorithm the "ERV-algorithm". It leads to a comparably small complete finite prefix of the unfolding. In [13], Khomenko and

[3] In the literature, the represented Petri net is often called the *unfolding* of the high-level Petri net. To avoid a clash of notions, we use the term expansion as, e.g., in [4].

Koutny describe how to construct the unfolding of the expansion of a high-level Petri net without first expanding it.

High-level representations on the one hand and processes (resp. unfoldings) of P/T Petri nets on the other, at first glance seem to be conflicting concepts; one being a more concise, the other a more detailed description of the net('s behavior). However, in [8], Ehrig et al. define processes of high-level Petri nets, and in [5], Chatain and Jard define *symbolic branching processes* and *unfoldings* of high-level Petri nets. The work on the latter is built upon in [4] by Chatain and Fabre, where they consider so-called "puzzle nets". Based on the construction of a symbolic unfolding, in [6], complete finite prefixes of safe time Petri nets are constructed, using time constraints associated with timed processes. In [3], using a simple example, Chatain argues that in general there exists no complete finite prefix of the symbolic unfolding of a high-level Petri net. However, this is only true for high-level Petri nets with infinitely many reachable markings such that the number of steps needed to reach them is unbounded, in which case the same arguments work for P/T Petri nets.

In this paper, we lift the concepts of complete prefixes and adequate orders to the level of symbolic unfoldings of high-level Petri nets. We consider the class of *safe* high-level Petri nets (i.e., in all reachable markings, every place carries at most one token) that have decidable guards and finitely many reachable markings. This class generalizes safe P/T Petri nets, and we obtain a generalized version of the ERV-algorithm creating a complete finite prefix of the symbolic unfolding of such a given high-level Petri net. Our results are a generalization of [10] in the sense that if a P/T Petri net is viewed as a high-level Petri net, the new definitions of adequate orders and completeness of prefixes on the symbolic level, as well as the algorithm producing them, all coincide with their P/T counterparts.

We proceed to identify an even more general class of so-called *symbolically compact* high-level Petri nets; we drop the assumption of finitely many reachable markings, and instead assume the existence of a bound on the number of steps needed to reach all reachable markings. In such a case, the expansion is possibly not finite, and the original ERV-algorithm from [10] therefore not applicable. We adapt the generalized ERV-algorithm by weakening the cut-off criterion to ensure finiteness of the resulting prefix. Still, in this cut-off criterion we have to compare infinite sets of markings. We overcome this obstacle by symbolically representing these sets, using the decidability of the guards to decide cut-offs.

2 High-level Petri Nets & Symbolic Unfoldings

In [5], symbolic unfoldings for high-level Petri nets are introduced. We recall definitions and formalism for high-level Petri nets and symbolic unfoldings.

Multi-sets. For a set X, we call a functions $A : X \to \mathbb{N}$ a *multi-set over* X. We denote $x \in A$ if $A(x) \geq 1$. For two multi-sets A, A' over the same set X, we write $A \leq A'$ iff $\forall x \in X : A(x) \leq A'(x)$, and denote by $A+A'$ and $A-A'$ the multi-sets over X given by $(A+A')(x) = A(x)+A'(x)$ and $(A-A')(x) = \min(A(x)-A'(x), 0)$. We use the notation $\{\!\{ \dots \}\!\}$ as introduced in [13]: elements in a multi-set can be listed explicitly as in $\{\!\{ x_1, x_1, x_2 \}\!\}$, which describes the multi-set A with

$A(x_1) = 2$, $A(x_2) = 1$, and $A(x) = 0$ for all $x \in X \setminus \{x_1, x_2\}$. A multi-set A is finite if there are finitely many $x \in X$ such that $A(x) \geq 0$. In such a case, $\{\!\!\{ f(x) \mid x \in A \}\!\!\}$, with $f(x)$ being an object constructed from $x \in X$, denotes the multi-set A' such that $A' = \sum_{x \in X} A(x) \cdot f(x)$, where the $A(x) \cdot y$ is the multi-set containing exactly $A(x)$ copies of y.

2.1 High-level Petri Nets

We assume two given sets *Col* (colors) and *Var* (variables). A *high-level net structure* is a tuple $\mathcal{N} = \langle P, T, F, \iota \rangle$, with disjoint sets of places P and transitions T, a flow function $F : (P \times \mathit{Var} \times T) \cup (T \times \mathit{Var} \times P) \to \mathbb{N}$, and a function ι mapping each $t \in T$ to a predicate $\iota(t)$ on $\mathit{Var}(t) := \{v \in \mathit{Var} \mid \langle p, v, t \rangle \in F \vee \langle t, v, p \rangle \in F\}$, called the *guard* of t. A *marking* in $\mathcal{N}$ is a multi-set M over $P \times \mathit{Col}$, describing how often each color $c \in \mathit{Col}$ currently lies on each place $p \in P$. A *high-level Petri net* $N = \langle \mathcal{N}, \mathcal{M}_0 \rangle$ is a net structure $\mathcal{N}$ together with a set $\mathcal{M}_0$ of *initial markings*, where we assume $\forall M_0, M_0' \in \mathcal{M}_0 : \{\!\!\{ p \mid \langle p, c \rangle \in M_0 \}\!\!\} = \{\!\!\{ p \mid \langle p, c \rangle \in M_0' \}\!\!\}$, i.e., in all initial markings, the same places are marked with *the same number of colors*.

For two nodes $x, y \in P \cup T$, we write $x \to y$, if there exists a variable v such that $\langle x, v, y \rangle \in F$. The reflexive and irreflexive transitive closures of $\to$ are denoted respectively by $\leq$ and $<$. For a transition $t \in T$, we denote by $\mathit{pre}(t) := \{\!\!\{ \langle p, v \rangle \mid \langle p, v, t \rangle \in F \}\!\!\}$ and $\mathit{post}(t) := \{\!\!\{ \langle p, v \rangle \mid \langle t, v, p \rangle \in F \}\!\!\}$ the *preset* and *postset* of t. A *firing mode* of t is a mapping $\sigma : \mathit{Var}(t) \to \mathit{Col}$ such that $\iota(t)$ evaluates to *true* under the substitution given by σ, denoted by $\iota(t)[\sigma] \equiv \mathit{true}$. We then denote $\mathit{pre}(t, \sigma) := \{\!\!\{ \langle p, \sigma(v) \rangle \mid \langle p, v \rangle \in \mathit{pre}(t) \}\!\!\}$ and $\mathit{post}(t, \sigma) := \{\!\!\{ \langle p, \sigma(v) \rangle \mid \langle p, v \rangle \in \mathit{post}(t) \}\!\!\}$. The set of modes of t is denoted by $\Sigma(t)$. t can *fire* in such a mode σ from a marking M if $M \geq \mathit{pre}(t, \sigma)$, denoted by $M[t, \sigma\rangle$. This firing leads to a new marking $M' = (M - \mathit{pre}(t, \sigma)) + \mathit{post}(t, \sigma)$, which is denoted by $M[t, \sigma\rangle M'$. We collect in the set $\mathcal{R}(\mathcal{N}, \mathcal{M})$ the markings reachable by firing a sequence of transitions in $\mathcal{N}$ from any marking in a set of markings $\mathcal{M}$. $\mathcal{N}$ resp. N is called *finite* if P, T and F are finite.

Let $\mathcal{N} = \langle P, T, F, \iota \rangle$ and $\mathcal{N}' = \langle P', T', F', \iota' \rangle$ be two net structures. A function $h : P \cup T \to P' \cup T'$ is called a *high-level net homomorphism*, if:

i) it maps places and transitions in $\mathcal{N}$ into the corresponding sets in $\mathcal{N}'$, i.e., $h(P) \subseteq P' \wedge h(T) \subseteq T'$;
ii) it is "compatible" with the preset, postset, and guard of transitions, i.e., for all $t \in T$ we have $\mathit{pre}(h(t)) = \{\!\!\{ \langle h(p), v \rangle \mid \langle p, v \rangle \in \mathit{pre}(t) \}\!\!\}$, $\mathit{post}(h(t)) = \{\!\!\{ \langle h(p), v \rangle \mid \langle p, v \rangle \in \mathit{post}(t) \}\!\!\}$, and $\iota(t) = \iota'(h(t))$.

For $N = \langle \mathcal{N}, \mathcal{M}_0 \rangle$ and $N' = \langle \mathcal{N}', \mathcal{M}_0' \rangle$, the homomorphisms between N and N' are the homomorphisms between $\mathcal{N}$ and $\mathcal{N}'$. Such a homomorphism h is called *initial* if additionally $\{\{\!\!\{ \langle h(p), c \rangle \mid \langle p, c \rangle \in M_0 \}\!\!\} \mid M_0 \in \mathcal{M}_0\} = \mathcal{M}_0'$ holds.

We define *P/T Petri nets* as high-level Petri nets with singletons $\mathit{Col} = \{\bullet\}$ and $\mathit{Var} = \{v_\bullet\}$ for colors and variables, i.e., in a marking, every place holds a number of tokens $\bullet$, which is the only value ever assigned to the variable $v_\bullet$ on every arc. The guard of every transition in a P/T Petri net is *true*.

2.2 Symbolic Branching Processes and Unfoldings

We recall the definition of symbolic branching processes and unfoldings from [5]. It is a generalization of branching processes and unfoldings for P/T Petri nets.

A net structure $\mathcal{N} = \langle P, T, F, \iota \rangle$ is called *ordinary* if there is at most one arc connecting any two nodes in $\mathcal{N}$, i.e., $\forall x, y \in P \cup T : \sum_{v \in Var} F(x, v, y) \leq 1$. For such an ordinary net structure, analogously to the low-level case described, e.g., in [10], two nodes $x, y \in P \cup T$ are in *structural conflict*, denoted by $x \sharp y$, if $\exists p \in P \, \exists t, t' \in T : t \neq t' \wedge p \to t \wedge p \to t' \wedge t \leq x \wedge t' \leq y$.

A *high-level occurrence net* is a high-level Petri net $O = \langle B, E, G, \iota, \mathcal{K}_0 \rangle$ with an ordinary net structure $\langle B, E, G, \iota \rangle$, where B is a set of *conditions* (places), E is a set of *events* (transitions), G is a flow relation, and $\mathcal{K}_0$ is the set of initial *cuts* (markings), having the following properties:

i) No event is in structural self-conflict, i.e., $\forall e \in E : \neg(e \sharp e)$.

ii) No node is its own causal predecessor, i.e., $\forall x \in B \cup E : \neg(x < x)$;

iii) The flow relation is well-founded, i.e., $\forall x \in B \cup E : |\{y \mid y \leq x\}| < \infty$;

iv) For every $b \in B$, exactly one of the following holds:

- *a)* $\forall K_0 \in \mathcal{K}_0 : \sum_{c \in Col} K_0(b, c) = 0$ and there exists a unique pair $\langle e, v \rangle$ called $pre(b)$ s.t. $\langle e, v, b \rangle \in G$, and for this pair we have $G(e, v, b) = 1$.
- *b)* $\forall K_0 \in \mathcal{K}_0 : \sum_{c \in Col} K_0(b, c) = 1$ and $\{e \mid e \to b\} = \emptyset$. In this case we denote $pre(b) := \langle \bot, v^b \rangle$.

The properties *i) – iii)* are exactly as in the low-level case and concern solely the net structure. Property *iv)* generalizes the requirement of low-level occurrence nets that every condition has at most one event in its preset, and that the conditions with empty preset constitute the initial cut.

In a crucial notation for what follows in later sections, we identify in case *iv.a)* the event e by $\mathbf{e}(b)$ and the variable v by $\mathbf{v}(b)$, and in case *iv.b)* we define $\mathbf{e}(b) := \bot$, and $\mathbf{v}(b) := v^b$. We abbreviate $\mathbf{v_e}(b) := \mathbf{v}(b)_{\mathbf{e}(b)}$. We denote by $B_0 := \{b \in B \mid \exists K_0 \in \mathcal{K}_0, c \in Col : \langle b, c \rangle \in K_0\}$ the conditions from *iv.b)* occupied in all initial cuts. $\bot$ can be seen as a "special event" that fires only once to initialize the net, and produces the initial cuts $K_0 \in \mathcal{K}_0$ by assigning values to the variables v^b on "special arcs" $\langle \bot, v^b, b \rangle$ towards the conditions $b \in B_0$.

For a high-level occurrence net, we define the mappings *loc-pred* and *pred* equipping events with predicates. For any $e \in E$, $pred(e)$ is satisfiable iff e is not dead, i.e., there are cuts $K_0, \ldots, K_n$ with $K_0 \in \mathcal{K}_0$ and events $e_1, \ldots, e_n$, s.t. $K_0[e_1\rangle \ldots [e_n\rangle K_n[e\rangle$. This predicate is obtained by building a conjunction over all *local predicates* of events e' with $e' \leq e$ (including the special event $\bot$). The local predicate of e is, in its turn, a conjunction of two predicates expressing that (i) the guard of the event e is satisfied, and (ii) that for any $\langle b, v \rangle \in pre(e)$, the value of the variable v coincides with the color that the event $\mathbf{e}(b)$ placed b. To realize this, the variables $v \in Var(e)$ are instantiated by the index e, so that v_e

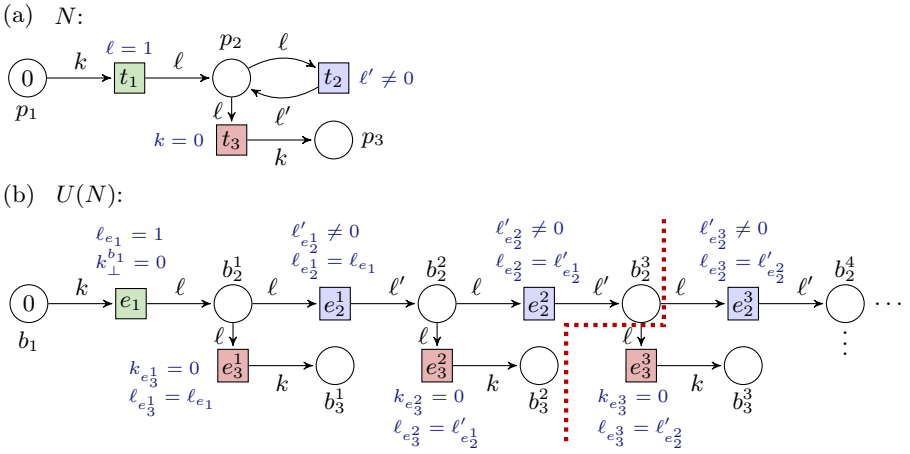


Fig. 1: A safe high-level Petri net N in (a), and (a prefix of) the infinite symbolic unfolding $U(N)$ in (b). We have $Col = \{0, \ldots, m\}$ and $Var = \{k, \ell, \ell'\}$.

describes the value assigned to v by a mode of e. Formally, we have

$$\begin{aligned} \mathit{loc\text{-}pred}(e) &:= \iota(e)[v \leftarrow v_e]_{v \in Var(e)} \quad \wedge \bigwedge_{\langle b, v\rangle \in pre(e)} v_e = \mathbf{v_e}(b) \\ \mathit{pred}(e) &:= \mathit{pred}(\bot) \wedge \bigwedge_{e' \leq e} \mathit{loc\text{-}pred}(e'), \end{aligned}$$

where $\mathit{pred}(\bot) := \bigvee_{K_0 \in \mathcal{K}_0} \bigwedge_{\langle b,c\rangle \in K_0} (v_\bot^b = c)$ describes the set of initial cuts.

A *symbolic branching process* of a high-level Petri net N is a pair $\beta = \langle O, h\rangle$ with an occurrence net $O = \langle B, E, G, \iota, \mathcal{K}_0\rangle$ in which $\mathit{pred}(e)$ is satisfiable for all $e \in E$, and an initial homomorphism $h : O \to N$ that is injective on events with the same preset, i.e., $\forall e, e' \in E : (pre(e) = pre(e') \wedge h(e) = h(e')) \Rightarrow e = e'$.

For two symbolic branching processes $\beta = \langle O, h\rangle$ and $\beta' = \langle O', h'\rangle$ of a high-level Petri net, β is a *prefix* of β' if there exists an injective initial homomorphism ϕ from O into O', such that $h' \circ \phi = h$. In [5] it is argued that for any given high-level Petri net N there exists a unique maximal branching process (maximal w.r.t. the prefix relation and unique up to isomorphism). This branching process is called the *symbolic unfolding*, and denoted by $\Upsilon(N) = \langle U(N), \pi\rangle$.

Example 1. Let $Col = \{0, \ldots, m\}$ for a fixed m, and $Var = \{k, \ell, \ell'\}$ be the given sets of colors and variables. In Fig. 1a, the running example N of a high-level Petri net[4] is depicted. Places are drawn as circles, and transitions as squares. The flow is described by labeled arrows, and the guards are written next to the respective transition. N has just one initial marking $M_0 = \{\!\{ \langle p_1, 0\rangle \}\!\}$, which is depicted in the net. From M_0 only t_1 can fire, and only in the mode $[k \leftarrow 0, \ell \leftarrow 1]$, taking 0 from p_1 and placing a token of color 1 on p_2. From there, t_2 can fire

[4] The structure of this example is taken from Figure D.4.5 in [2].

arbitrarily often, always replacing the color ℓ currently residing on p_2 by any color $0 < \ell' \leq m$, until t_3 fires, placing 0 on p_3 and ending the execution.

The infinite occurrence net $U(N)$ of the symbolic unfolding $\Upsilon(N)$ in Fig. 1b describes this behavior: we depict the prefix of the unfolding representing the executions of the net in which t_2 fires up to three times. The values of the homomorphism π (also called labels) are given by the subscript of a node's name, e.g., $\pi(e_1) = t_1$ or $\pi(b_3^2) = p_3$. The guards of events are omitted, since they have the same guards as their label. Instead, the local predicate of each event is written next to it. The local predicate of e_2^2, e.g., expresses that (i) the assignment of colors to variables by a mode of e_2^2 must satisfy the constraint given by the guard of its label t_2 ($\ell'_{e_2^2} \neq 0$), and that (ii) the color consumed when firing e_2^2 must be the one placed on b_2^2 by e_2^1 ($\ell_{e_2^2} = \ell'_{e_2^1}$). The red dotted line marks the complete finite prefix obtained by Alg. 1, as described later.

As we see in the definition of high-level occurrence nets, the notion of causality and structural conflict are the same as in the low-level case. However, a set of events in an occurrence net can also be in what we call *color conflict*, meaning that the conjunction of their predicates is not satisfiable. In a symbolic branching process, this means that the constraints on the values of the firing modes, coming from the guards of the transitions, prevent joint occurrence of all events from such a set in any *one* run of the net:

The nodes in a set $X \subseteq E \cup B$ and are in *color conflict* if $\bigwedge_{e \in X \cap E} \mathit{pred}(e) \wedge \bigwedge_{b \in X \cap B} \mathit{pred}(\mathbf{e}(b))$ is not satisfiable. The nodes of X are *concurrent* if they are *not* in color conflict, and for each $x, x' \in X'$, neither $x < x'$, nor $x' < x$, nor $x \sharp x'$ holds. A set of concurrent conditions is called a *co-set*.

Note that while a set of nodes is defined to be in structural conflict if and only if two nodes in it are in structural conflict, the same does not hold for color conflict: it is possible to have a set $\{x_1, x_2, x_3\}$ of nodes that are in color conflict, but for which every subset of cardinality 2 is *not* in color conflict.

Definition 1 (Configuration [5]). *A* (symbolic) configuration *is a set of high-level events that is free of structural conflict and color conflict, and causally closed. The configurations in a symbolic branching process β are collected in the set $\mathcal{C}(\beta)$.*

For a configuration C, we define by $\mathrm{cut}(C) := (B_0 \cup (C \rightarrow)) \setminus (\rightarrow C)$ the high-level conditions that are occupied after any concurrent execution of C. Note that $\mathrm{cut}(C)$ is a co-set, and that $\emptyset$ is a configuration with $\mathrm{cut}(\emptyset) = B_0$.

Let $e \in E$ be a high-level event. We define the so-called *cone configuration* $[e] := \{e' \in E \mid e' \leq e\}$. Additionally, we define the sets $\mathit{Var}_e := \{v_e \mid v \in \mathit{Var}(e)\}$ and $\mathit{Var}_\perp := \{v_\perp^b \mid b \in B_0\}$ of indexed variables, and for a set $E' \subseteq E \cup \{\perp\}$ we denote $\mathit{Var}_{E'} := \bigcup_{e \in E'} \mathit{Var}_e$. Note that, for every event e, $\mathit{pred}(e)$ is a predicate over the variables $\mathit{Var}_{[e] \cup \{\perp\}}$.

2.3 Properties of the Symbolic Unfolding.

Having recalled the definitions and formal language from [5], we now delve into the novel aspects of this paper. We state three analogues of well-known properties

of the Unfolding of P/T Petri nets for the symbolic unfolding of high-level nets. These properties are: (i) the cuts in the unfolding represent precisely the reachable markings in the net, (ii) for every transition that can occur in the net, there is an event in the unfolding with corresponding label (and vice versa), and (iii) the unfolding is complete in the sense that for any configuration, the part of the unfolding that "lies after" that configuration is the unfolding of the original net with the initial markings being the ones represented by the configurations cut. The properties are stated in Prop. 1, Prop. 2, and Prop.3, respectively. Their proofs are moved to App. A.1.

To express these properties, we introduce the notion of *instantiations* of configurations C, choosing a mode for every event in C without creating color conflicts. This is realized by assigning to each variable $v_e \in Var_{C\cup\{\bot\}}$ a value in Col, such that the above defined predicates evaluate to *true*. For each $e \in C$, the assignment of values to the indexed variables in Var_e corresponds to a mode of e.

Definition 2 (Instantiation). *For a given configuration C, an* instantiation of C *is a function $\theta : Var_{C\cup\{\bot\}} \to Col$, such that $\forall e \in C \cup \{\bot\} : pred(e)[\theta] \equiv$ true, i.e., it satisfies all predicates in the configuration. The set of instantiations of a given configurations C is denoted by $\Theta(C)$.*

Note that, by definition, every configuration C has an instantiation θ. We denote by $\mathrm{cut}(C,\theta) := \{\langle b, c\rangle \mid b \in \mathrm{cut}(C) \wedge \theta(\mathbf{v_e}(b)) = c\} \subseteq B \times Col$ the *cut* of an "instantiated configuration", and by $\mathrm{mark}(C,\theta) := \{\!|\, \langle h(b), c\rangle \mid \langle b, c\rangle \in \mathrm{cut}(C.\theta) \,|\!\}$ its *marking*. We collect both of these in $\mathcal{K}(C) := \{\mathrm{cut}(C,\theta) \mid \theta \in \Theta(C)\}$ and $\mathcal{M}(C) := \{\mathrm{mark}(C,\theta) \mid \theta \in \Theta(C)\}$. Note that in this notation, for the empty configuration we have $\mathcal{K}(\emptyset) = \mathcal{K}_0$ and $\mathcal{M}(\emptyset) = \mathcal{M}_0$.

Proposition 1. *Let N be a high-level Petri net and Υ its symbolic unfolding. Then $\mathcal{R}(N) = \{\mathrm{mark}(C.\theta) \mid C \in \mathcal{C}(\Upsilon), \theta \in \Theta(C)\}$.*

Proposition 2. *The symbolic unfolding $\Upsilon = \langle U, \pi\rangle$ with events E of a high-level Petri net $N = \langle P, T, F, \iota, \mathcal{M}_0\rangle$ satisfies $\forall C \in \mathcal{C}(\Upsilon)\ \forall \theta \in \Theta(C)\ \forall t \in T\ \forall \sigma \in \Sigma(t)$:*

$$\mathrm{mark}(C,\theta)[t,\sigma\rangle \ \Leftrightarrow\ \exists e \in E : \pi(e) = t \wedge \mathrm{cut}(C,\theta)[e,\sigma\rangle.$$

Given a configuration C of a symbolic branching process $\beta = \langle O, h\rangle$, we define $\Uparrow C$ as the pair $\langle O', h'\rangle$, where O' is the unique subnet of O whose set of nodes is $\{x \in B \cup E \mid x \notin (C \cup \to C) \wedge \forall y \in C : \neg(y \sharp x) \wedge (C \cup \{x\} \text{ is not in color conflict})\}$ with the set $\mathcal{K}(C)$ of initial cuts, and h' is the restriction of h to the nodes of O'. The branching process $\Uparrow C$ is referred to as the *future* of C.

Proposition 3. *If β is a symbolic branching process of $\langle \mathcal{N}, \mathcal{M}_0\rangle$ and C is a configuration of β, then $\Uparrow C$ is a branching process of $\langle \mathcal{N}, \mathcal{M}(C)\rangle$. Moreover, if β is the unfolding of $\langle \mathcal{N}, \mathcal{M}_0\rangle$, then $\Uparrow C$ is the unfolding of $\langle \mathcal{N}, \mathcal{M}(C)\rangle$.*

3 Finite & Complete Prefixes of Symbolic Unfoldings

We combine ideas from [10] (computing small finite and complete prefixes of unfoldings) with results from [5] (symbolic unfoldings of high-level Petri nets) to

define and construct complete finite prefixes of symbolic unfoldings of high-level Petri nets. We generalize the concepts and the ERV-algorithm from [10] for safe P/T Petri nets to a class of safe high-level Petri nets, and compare this generalization to the original. We will see that for P/T nets interpreted as high-level nets, all generalized concepts (i.e., complete prefixes, adequate orders, cut-off events), and, as a consequence, the result of the generalized ERV-algorithm all coincide with their P/T counterparts.

We start by lifting the definition of completeness to the level of symbolic unfoldings. Together with Prop. 1 and Prop. 2, this can be seen as a direct translation from the low-level case described, e.g., in [10].

Definition 3 (Complete prefix). *Let $\beta = \langle O, h\rangle$ be a prefix of the symbolic unfolding of a high-level Petri net N, with events E'. Then β is called* complete *if for every reachable marking M in N there exists $C \in \mathcal{C}(\beta)$ and $\theta \in \Theta(C)$ s.t.*

i) $M = \mathrm{mark}(C, \theta)$, *and*
ii) $\forall t \in T\, \forall \sigma \in \Sigma(t) :\ M[t, \sigma\rangle \ \Rightarrow\ \exists e \in E' h(e) = t \ \wedge\ \mathrm{cut}(C.\theta)[e, \sigma\rangle$.

We now define the class $\mathbf{N_f}$ of high-level Petri nets for which we generalize the construction of finite and complete prefixes of the unfolding of *safe* P/T Petri nets from [10]. We discuss the properties defining this class, and describe how it generalizes safe P/T nets.

Definition 4 (Class $\mathbf{N_f}$). *The class $\mathbf{N_f}$ contains all finite high-level Petri nets $N = \langle P, T, F, \iota, \mathcal{M}_0\rangle$ satisfying the following three properties:*

(1) *The net is* safe*, i.e., in every reachable marking there lies at most* 1 *color on every place (formally; $\forall M \in \mathcal{R}(N)\, \forall p \in P : \sum_{c \in Col} M(p, c) \leq 1$).*
(2) *Guards are written in a decidable first-order theory with the set Col as its domain of discourse.*
(3) *The net has finitely many reachable markings (formally; $|\mathcal{R}(N)| < \infty$).*

We require the safety property ***(1)*** for two reasons; on the one hand, to avoid adding to the already heavy notation. On the other hand, while we think that a generalization to bounded high-level Petri nets is possible, it comes with all the troubles known from going from safe to k-bounded in the P/T case in [10], plus the problems arising from the expressive power of the high-level formalism. We therefore postpone this generalization to future work. Note that, under the safety condition, we can w.l.o.g. assume $\mathcal{N}$ to be ordinary (i.e., $\forall x, y \in P \cup T : \sum_{v \in Var} F(x, v, y) \leq 1$), since transitions violating this property could never fire. The finiteness of $\mathcal{N}$ implies that we can assume *Var* to be finite.

While property ***(2)*** seems very strong, the goal is an algorithm that generates a complete finite prefix of the symbolic unfolding of a given high-level Petri net. The definition of symbolic branching processes requires the predicate of every event added to the prefix to be satisfiable, and the predicates are build from the guards in the given net. Thus, satisfiability checks in the generation of the prefix seem for now inevitable. An example for such a theory is Presburger arithmetic [16], which is a first order theory of the natural numbers with addition. The guards in the example from Fig. 1a are written in Presburger arithmetic.

We need Property ***(3)*** to ensure that the generalized version of the cut-off criterion from [10] yields a finite prefix constructed in the generalized ERV-Algorithm. $|\mathcal{R}(N)| < \infty$ can be ensured by having a finite set *Col* of colors. In Sec. 4, we identify a class of high-level Petri nets with infinitely many reachable markings for which the algorithm works with an adapted cut-off criterion.

Under these three assumptions we generalize the finite safe P/T Petri nets considered in [10]: every such P/T net can be seen as a high-level Petri net with $Col = \{\bullet\}$ and all guards being *true*, and thus satisfying the three properties above. Replacing the safety property ***(1)*** by a respective "k-bounded property" would result in a generalization of k-bounded P/T nets. In Sec. 3.3, we compare the result of the generalized ERV-algorithm Alg. 1 applied to a high-level net to the result of the original ERV-algorithm from [10] applied to the nets expansion.

For the rest of the section let $N = \langle P, T, F, \iota, \mathcal{M}_0\rangle \in \mathbf{N_f}$ with symbolic unfolding $\Upsilon = \langle U, \pi\rangle = \langle B, E, G, \iota, \mathcal{K}_0, \pi\rangle$.

3.1 Generalizing Adequate Orders and Cut-Off Events

We lift the concept of adequate orders on the configurations of an occurrence net to the level of symbolic unfoldings. A main property of adequate orders is the preservation by finite *extensions*, which are defined as for P/T-nets (cp. [10]):

Given a configuration C, we denote by $C \oplus D$ the fact that $C \cup D$ is a configuration such that $C \cap D = \emptyset$. We say that $C \oplus D$ is an *extension* of C, and that D is a *suffix* of C. Obviously, for a configuration C', if $C \subsetneq C'$ then there is a nonempty suffix D of C such that $C \oplus D = C'$. For a configuration $C \oplus D$, denote by $O(C|D) = \langle \mathrm{cut}(C) \cup {\to}D \cup D{\to}, D, G', \mathcal{K}(C)\rangle$ the occurrence net around D from $\mathrm{cut}(C)$, where G' is the restriction of G to the nodes of $O(C|D)$. Note that for every finite configuration C with an extension $C \oplus D$, we have that D is a configuration of $\Uparrow C$.

For better readability, we abbreviate for a marking M the fact $C[\![M]\!]D :\Leftrightarrow \exists \theta \in \Theta(C \oplus D) : \mathrm{mark}(C, \theta|_{Var_{C \cup \{\perp\}}}) = M$. Thus, $C[\![M]\!]D$ means that the transitions corresponding to the events in D can fire from $M \in \mathcal{M}(C)$.

The now stated Proposition 4 is a weak version of the arguments in [10], where the Esparza et al. follow from the low-level version of Prop. 3 that if the cuts of two low-level configurations represent the same marking in the low-level net, then their futures are isomorphic, and the respective (unique) isomorphism maps the suffixes of one configuration to the suffixes of the other.

Proposition 4. *Let C_1 and C_2 be two finite configurations in Υ, and let D be a suffix of C_1. If there is a marking $M \in \mathcal{M}(C_1) \cap \mathcal{M}(C_2)$ s.t. $C_1[\![M]\!]D$, then there is a unique monomorphism $\varphi^2_{1,D} : O(C_1|D) \to \Uparrow C_2$ that satisfies $\varphi^2_{1,D}(\mathrm{cut}(C_1)) = \mathrm{cut}(C_2)$ and preserves the labeling π.*
For this monomorphism we have that $\varphi^2_{1,D}(D)$ is a suffix of C_2.

The proof is an induction over the size of D (cp. App. A.1).

Equipped with Prop. 4, we can now lift the concept of adequate order to the level of symbolic branching processes. Compared to [14,10], the monomorphism $\varphi^2_{1,D}$ defined above replaces the isomorphism I^2_1 between $\Uparrow C_1$ and $\Uparrow C_2$ for two low-level configurations C_1, C_2 representing the same marking.

Definition 5 (Adequate order). *A partial order $\prec$ on the finite configurations of the symbolic unfolding of a high-level Petri net is an* adequate order *if:*

i) $\prec$ *is well-founded,*
ii) $C_1 \subset C_2$ *implies* $C_1 \prec C_2$*, and*
iii) $\prec$ *is preserved by finite extensions in the following way: if* C_1, C_2 *are two finite configurations, and* $C_1 \oplus D$ *is a finite extension of* C_1 *such that there is a marking* $M \in \mathcal{M}(C_1) \cap \mathcal{M}(C_2)$ *satisfying* $C_1[\![M]\!]D$*, then the monomorphism* $\varphi^2_{1,D}$ *from above satisfies* $C_1 \prec C_2 \Rightarrow C_1 \oplus D \prec C_2 \oplus \varphi^2_{1,D}(D)$*.*

In the case of a P/T net interpreted as a high-level net, we have $|\mathcal{M}(C)| = 1$ for every configuration C, and therefore, Def. 5 coincides with its P/T version [10]. We could alternatively generalize the P/T case by replacing '$\exists M \in \mathcal{M}(C_1) \cap \mathcal{M}(C_2)$ s.t. $C_1[\![M]\!]D$' by '$\mathcal{M}(C_1) = \mathcal{M}(C_2)$', and use the isomorphism I^2_1 between $\Uparrow C_1$ and $\Uparrow C_2$ to define preservation by finite extension. However, in the upcoming generalization of the ERV-algorithm from [10], the generalized cut-off criterion exploits property iii) of adequate orders. Using '$\mathcal{M}(C_1) = \mathcal{M}(C_2)$' would produce an exponential blowup of the generated prefix's size. This is circumvented by using '$\exists M \in \mathcal{M}(C_1) \cap \mathcal{M}(C_2)$ s.t. $C_1[\![M]\!]D$', which however leads to obtaining merely a monomorphism that depends on the considered suffix, instead of an isomorphism between the futures. We now show that this monomorphism sufficient:

The upcoming proof that the generalized ERV-algorithm is complete is structurally analogous to the respective proof in [10]. It uses that, under the conditions of Def. 5 *iii)*, we also have $C_2 \prec C_1 \Rightarrow C_2 \oplus \varphi^2_{1,D}(D) \prec C_1 \oplus D$. This result would directly be obtained if $\varphi^2_{1,D}$ was an isomorphism, as I^2_1 is in the low-level case. However, a monomorphism is an isomorphism when its codomain is restricted to its range. This idea is used in the proof (cp. App A.1) of the following proposition, which states that $\varphi^2_{1,D}$ indeed satisfies the above property.

Proposition 5. *Let* $\prec$ *be an adequate order. Under the conditions of Def. 5 iii) the monomorphism* $\varphi^2_{1,D}$ *also satisfies* $C_2 \prec C_1 \Rightarrow C_2 \oplus \varphi^2_{1,D}(D) \prec C_1 \oplus D$*.*

In [10], Esparza et al. discuss three adequate orders on the configurations of the low-level unfolding. In particular, they present a *total* adequate order that uses the *Foata normal form* of configurations. Using such a total order in the algorithm limits the size of the resulting finite and complete prefix; It contains at most $|\mathcal{R}(N)|$ non cut-off events. All three adequate orders presented in [10] can be directly lifted to the configurations of the symbolic unfolding by exchanging every low-level term by its high-level counterpart. The lifted order using the Foata normal form is still a total order. We include these discussions in App. A.2.

We now define cut-off events in a symbolic unfolding. In the low-level case [10], e is a cut-off event if there is another event e' satisfying $[\mathsf{e}'] \prec [\mathsf{e}]$ and $\mathrm{mark}([\mathsf{e}]) = \mathrm{mark}([\mathsf{e}'])$, which ensures that the future of e needs not be considered further. In the high-level case, we generalize these conditions to high-level events e. However, we do not require the existence of *one* other high-level event e' with $[e'] \prec [e]$ and $\mathcal{M}([e]) = \mathcal{M}([e'])$. While this would still be a valid cut-off criterion and would lead to finite and complete prefixes, the upper bound on the size of such a prefix would be exponential in the number of markings in the original net. Instead, we

check whether $\mathcal{M}([e])$ is contained in the union of *all* $\mathcal{M}([e'])$ with $[e'] \prec [e]$. This criterion expresses that we have already seen every marking in $\mathcal{M}([e])$ in the prefix β under construction, and therefore need not consider the future of e any further. By this, we obtain the same upper bounds as in [10], as discussed later.

Definition 6 (Cut-off event). *Let $\prec$ be an adequate order on the configurations of the symbolic unfolding of a high-level Petri net. Let β be a prefix of the symbolic unfolding containing a high-level event e. The high-level event e is a* cut-off *event in β (w.r.t. $\prec$) if $\mathcal{M}([e]) \subseteq \bigcup_{[e'] \prec [e]} \mathcal{M}([e'])$.*

When interpreting P/T nets as high-level nets, this definition corresponds to the cut-off events defined in [10], since then $|\mathcal{M}([e])| = 1$ for all events e.

3.2 The Generalized ERV-Algorithm

We present the algorithm for constructing a finite and complete prefix of the symbolic unfolding of a given high-level Petri net. It is a generalization of the ERV-algorithm from [10], and is structurally equal (and therefore looks very similar). However, the algorithm is contingent upon the previous section's work of generalizing adequate orders and cut-off events, which ultimately enables us to adopt this structure.

A crucial concept of the ERV-algorithm is the notion of "possible extensions", i.e., the set of individual events that extend a given prefix of the unfolding. In Def. 7, we lift this concept to the level of symbolic unfoldings. We do so by isolating the procedure of adding high-level events in the algorithm from [5] which generates the complete symbolic unfolding of a given high-level Petri net (but does not terminate if the symbolic unfolding is infinite).

We define the data structures similarly to [10]. There, an event is given by a tuple $\mathsf{e} = \langle \mathsf{t}, \mathsf{B}' \rangle$ with $\mathsf{h}(\mathsf{e}) = \mathsf{t} \in \mathsf{T}$ and $pre(\mathsf{e}) = \mathsf{B}' \subseteq \mathsf{B}$, and a condition given by a tuple $\mathsf{b} = \langle \mathsf{p}, \mathsf{e} \rangle$ with $\mathsf{h}(\mathsf{b}) = \mathsf{p} \in \mathsf{P}$ and $pre(\mathsf{b}) = \{\mathsf{e}\} \subseteq \mathsf{E}$. The finite and complete prefix is a set of such events and transitions.

In the high-level case, we need more information inside the tuples. A high-level event is given by a tuple $e = \langle t, X, pred \rangle$ described by $h(e) = t$, $pre(e) = X \subseteq B \times Var$, and $pred(e) = pred$. Analogously, a high-level condition is given by a tuple $b = \langle p, \langle e, v \rangle, pred \rangle$, where $h(b) = p$, $pre(b) = \langle e, v \rangle \in (E \times Var) \cup (\{\bot\} \times \{v^b \mid b \in B_0\})$, and $pred(\mathbf{e}(b)) = pred$.

Definition 7 (Possible extensions). *Let $\beta = \langle O, h \rangle$ be a branching process of a high-level Petri net N. The* possible extensions *$PE(\beta)$ are the set of tuples $e = \langle t, X, pred \rangle$ where t is a transition of N, and $X \subseteq B \times Var$ satisfying*

- *$\{b \mid \langle b, v \rangle \in X\}$ is a co-set, and $pre(t) = \{\langle h(b), v \rangle \mid \langle b, v \rangle \in X\}$,*
- *$pred = loc\text{-}pred \wedge \big(\bigwedge_{\langle b,v \rangle \in X} pred(\mathbf{e}(b)) \big)$ is satisfiable,*
  where $loc\text{-}pred = \iota(t)[v \leftarrow v_e]_{v \in Var(e)} \wedge \big(\bigwedge_{\langle b,v \rangle \in X} v_e = \mathbf{v}_{\mathbf{e}}(b) \big)$,
- *Fin does not contain $\langle t, X, pred \rangle$.*

Since the notion of co-set in high-level occurrence nets is achieved by the direct translation from low-level occurrence nets plus the "color conflict freedom",

possible extensions in a prefix β can be found by searching first for sets of conditions that are not in structural conflict as in the low-level case, and then checking whether these sets are in color conflict.

Algorithm 1 is a generalization of the ERV-Algorithm in [10] for complete finite prefixes of the low-level unfolding. The structure is taken from there, with the only difference being the special initial transition $\bot$. It takes as input a high-level Petri net $N \in \mathbf{N_f}$ and assumes a given adequate order $\prec$.

Algorithm 1: Generalization of the ERV-Algorithm from [10] for complete finite prefixes.

Data: High-level Petri net $N = \langle P, T, F, \iota, \mathcal{M}_0 \rangle \in \mathbf{N_f}$.
Result: A complete finite prefix *Fin* of the symbolic unfolding of N.
$Fin \leftarrow \{\bot\}$;
$pred(\bot) \leftarrow \bigvee_{M_0 \in \mathcal{M}_0} \bigwedge_{\langle p,c \rangle \in M_0} v_\bot^{b_p} = c$;
foreach $p \in P_0$ **do**
  Create a fresh condition $b_p = \langle p, \langle \bot, v^{b_p} \rangle, pred(\bot) \rangle$;
  $Fin \leftarrow Fin \cup \{b\}$;
$pe \leftarrow PE(Fin)$;
$cut\text{-}off \leftarrow \emptyset$;
while $pe \neq \emptyset$ **do**
  Pick $e = \langle t, X, pred \rangle$ from pe such that $[e]$ is minimal w.r.t. $\prec$;
  if $[e] \cap cut\text{-}off = \emptyset$ **then**
    $Fin \leftarrow Fin \cup \{e\}$;
    foreach $\langle p, v \rangle \in post(t)$ **do**
      Create a fresh condition $b = \langle p, \langle e, v \rangle, pred \rangle$;
      $Fin \leftarrow Fin \cup \{b\}$;
    $pe \leftarrow PE(Fin)$;
    if *e is a cut-off event of Fin* **then**
      $cut\text{-}off \leftarrow cut\text{-}off \cup \{e\}$;
  else
    $pe \leftarrow pe \setminus \{e\}$

We now prove correctness of Algorithm 1 analogously to [10], by stating two propositions – one each to show that the prefix is finite and complete, respectively. The proof structure is also as in [10], but adapted to the setting of high-level Petri nets and symbolic unfoldings.

Proposition 6. *Fin is finite.*

Proof (Sketch). As in [10], we prove the following results (1) – (3):

(1) For every event e of *Fin*, $d(e) \leq |\mathcal{R}(N)| + 1$, where d is the *depth* of e.
(2) For every event e of *Fin*, the sets $pre(e)$ and $post(e)$ are finite, and
(3) For every $k \geq 0$, *Fin* contains only finitely many events e such that $d(e) \leq k$

This works exactly as in [10], as shown in App. A.1, with minor adaptations to the generalization of cut-offs in the symbolic unfolding in (1). □

Proposition 7. *Fin is complete.*

The proof also has the same general structure as the respective proof in [10]. However, since here we use the generalizations of adequate order, possible extensions, and the cut-off criterion to symbolic branching processes, we include the complete proof in the body of the paper.

Notation. For functions $f : X \to Y$ and $f' : X' \to Y$ with $X \cap X' = \emptyset$ we define $f \uplus f' : X \cup X' \to Y$ by mapping x to $f(x)$ if $x \in X$ and to $f'(x)$ if $x \in X'$.

Proof of Prop. 7. We first show that for every reachable marking in N there exists a configuration in Υ satisfying a) from the definition of complete prefixes, and then show that one of these configurations (a minimal one) also satisfies b).

(1) Let M be an arbitrary reachable marking in N. Then by Prop. 1, we have that there is a $C_1 \in \mathcal{C}(\Upsilon)$ s.t. $M \in \mathcal{M}(C_1)$. Let $\theta_1 \in \Theta(C_1)$ s.t. $M = \mathrm{mark}(C_1.\theta_1)$. If C is not a configuration in *Fin*, then it contains a cut-off event e_1, and so $C_1 = [e_1] \oplus D$ for some set D of events. Let $M_1 = \mathrm{mark}([e_1].\theta_1|_{Var_{[e_1]\cup\{\perp\}}}) \in \mathcal{M}([e_1])$. By the definition of cut-off event, there exists an event e_2 with $[e_2] \prec [e_1]$ and $M_1 \in \mathcal{M}([e_2])$. Since we have $C_1 [\![M_1]\!] D$, we get by Prop. 4 that the monomorphism $\varphi_1 := \varphi^{[e_2]}_{[e_1],D} : O([e_1]|D) \to \Uparrow[e_2]$ exists and that $\varphi_1(D)$ is a suffix of $[e_2]$. By Prop. 5 we know

$$C_2 := [e_2] \oplus \varphi_1(D) \prec [e_1] \oplus D = C_1.$$

Let $\theta'_2 \in \Theta([e_2])$ s.t. $M_1 = \mathrm{mark}([e_2], \theta'_2)$. Define now $\theta_2 \in \Theta(C_2)$ by $\theta_2 = \theta'_2 \uplus \theta''_2$, where $\theta''_2 : Var_{\varphi_1(D)} \to Col$ is given by $\theta''_2(v_{\varphi_1(e)}) = \theta_1(v_e)$. By this construction we get $M = \mathrm{mark}(C_2, \theta_2) \in \mathcal{M}(C_2)$.
If C_2 is not a configuration of *Fin*, then we can iterate the procedure and find a configuration C_3 such that $C_3 \prec C_2$ and $M \in \mathcal{M}(C_3)$. The procedure cannot be iterated infinitely often because $\prec$ is well-founded. Therefore, it terminates in a configuration of *Fin*.

(2) Let now C be a minimal configuration w.r.t. $\prec$ s.t. $M \in \mathcal{M}(C)$, and let $t \in T$, $\sigma \in \Sigma(t)$ s.t. $M[t, \sigma\rangle$. If C contains some cut-off event, then we can apply the arguments of a) to conclude that *Fin* contains a configuration $C' \prec C$ such that $M \in \mathcal{M}(C')$. This contradicts the minimality of C. So C contains no cut-off events. Let $\theta \in \Theta(C)$ s.t. $M = \mathrm{mark}(C, \theta)$. Since $pre(t.\sigma) \subseteq M$, we have that there is a co-set $B_{t,\sigma} \subseteq \mathrm{cut}(C)$ s.t. $pre(t, \sigma) = \{\langle h(b), \theta(\mathbf{v_e}(b))\rangle \mid b \in B_{t,\sigma}\}$. Let now $X := \{\langle b, v\rangle \mid b \in B_{t,\sigma}, \langle h(b), v\rangle \in pre(t)\}$. We then have $\forall \langle b, v\rangle \in X : \sigma(v) = \theta(\mathbf{v_e}(b))$.
We now show that $pred := \iota(t)[v \leftarrow v_e]_{v \in Var(e)} \wedge \big(\bigwedge_{\langle b,v\rangle \in X} v_e = \mathbf{v_e}(b)\big) \wedge \bigwedge_{(b,v)\in X} pred(\mathbf{e}(b))$ is satisfiable. Let $\theta' := \theta \uplus (\sigma \circ [v_e \mapsto v]_{v \in Var(e)})$. Then
- $\iota(t)[v \leftarrow v_e]_{v \in Var(e)}[\theta'] \equiv \iota(t)[\sigma] \equiv true$, and
- $\big(\bigwedge_{\langle b,v\rangle \in X} v_e = \mathbf{v_e}(b)\big)[\theta'] \equiv \big(\bigwedge_{\langle b,v\rangle \in X} \sigma(v) = \theta(\mathbf{v_e}(b))\big) \equiv true$, and
- $\bigwedge_{\langle b,v\rangle \in X} pred(\mathbf{e}(b))[\theta'] \equiv \bigwedge_{\langle b,v\rangle \in X} pred(\mathbf{e}(b))[\theta] \equiv true$, since $\theta \in \Theta(C)$.

Thus, $pred[\theta'] \equiv true$. Therefore, $e = \langle t, X, pred \rangle$ is a possible extension and added in the execution of the algorithm. Then we directly have $e \notin C$, $h(e) = t$, and with the same arguments as in a), we get $C \cup \{e\} \in \mathcal{C}(Fin)$ and $\theta \uplus (\sigma \circ [v_e \mapsto v]_{v \in Var(e)}) \in \Theta(C \cup \{e\})$, which means $\mathrm{cut}(C, \theta)[e, \sigma\rangle$. Since we chose θ independently of t and σ, this concludes the proof. □

Notice that by this construction, as described in [10], we get that if $\prec$ is a total order, then *Fin* contains at most $|\mathcal{R}(N)|$ non cut-off events. As already discussed in Sec. 3.1, the total adequate order defined in [10] can be lifted to the configurations in the symbolic unfolding, where it again is total (cp. App A.2). Thus, we generalized the possibility to construct such a small complete finite prefix by application of Alg. 1 with $\prec$ being a total adequate order.

Running Example. For the example N from Fig 1a, the algorithm produces the complete finite prefix marked by the red, dotted line in Fig 1b: starting with the initial condition b_1, the event e_1 is the only possible extension and added to *Fin*. Since e_1 is obviously not a cut-off event, e_2^1 and e_3^1 are possible extensions and also added. Now we have $\mathcal{M}([e_2^1]) = \{\{\!|\, \langle p_2, i\rangle \,|\!\} \mid 0 < i \leq m\}$, and $\mathcal{M}([e_1]) = \{\{\langle p_2, 1\rangle\}\}$, so e_2^1 is also not a cut-off event, and the possible extensions e_3^2 and e_2^2 are added. Now, however, we have that $\mathcal{M}([e_2^2]) = \{\{\!|\, \langle p_2, i\rangle \,|\!\} \mid 0 < i \leq m\} = \mathcal{M}([e_2^1])$, and therefore, e_2^2 is a cut-off event.

3.3 High-level versus P/T Expansion

Every high-level Petri net represents a P/T Petri net with the same behavior, in which the places can only carry a number tokens with color $\bullet$. Markings in a P/T Petri net describe only how many tokens lie on each place. Each transitions only has one possible firing mode that takes and/or lays a fixed number of tokens from resp. onto each connected place.

In this section we state in Lem. 2 that the expansion of a finite complete prefix of the unfolding of a high-level Petri net is a finite and complete prefix of the unfolding of the expanded high-level Petri net. This means the generalization of complete prefixes is "canonical", and compatible with the established low-level concepts. We then shortly compare the results of

- applying the generalized ERV-algorithm Alg. 1 to obtain a complete finite prefix of the symbolic unfolding of a given high-level Petri net, and
- first expanding a given high-level Petri net and then applying the ERV-algorithm from [10] for a complete finite prefix of the (P/T) unfolding.

The procedure of constructing the represented P/T Petri net $\mathrm{Exp}(N)$ (called the *expansion*) of a high-level Petri net N is well established (cp., e.g., Chapter 2.4 in [12]), and we describe it here only briefly; the places of $\mathrm{Exp}(N)$ are given by $\mathsf{P} = \{p.c \mid p \in P, c \in Col\}$, and its transitions by $\mathsf{T} = \{t.\sigma \mid t \in T, \sigma \in \Sigma(t)\}$. There is an arc from $p.c$ to $t.\sigma$ iff $\langle p, c\rangle \in pre(t, \sigma)$, and analogously for arcs from transitions to places. Markings in $\mathrm{Exp}(N)$ are functions $\mathsf{M} : \mathsf{P} \to \mathbb{N}$, describing how often the only color $\bullet$ lies on each place $p.c$. Every such marking corresponds to a marking M in the high-level net N, with $M(p, c) = \mathsf{M}(p.c)$, and a transition t can fire in mode σ from M iff $t.\sigma$ can fire from M. Thus, we say that N and

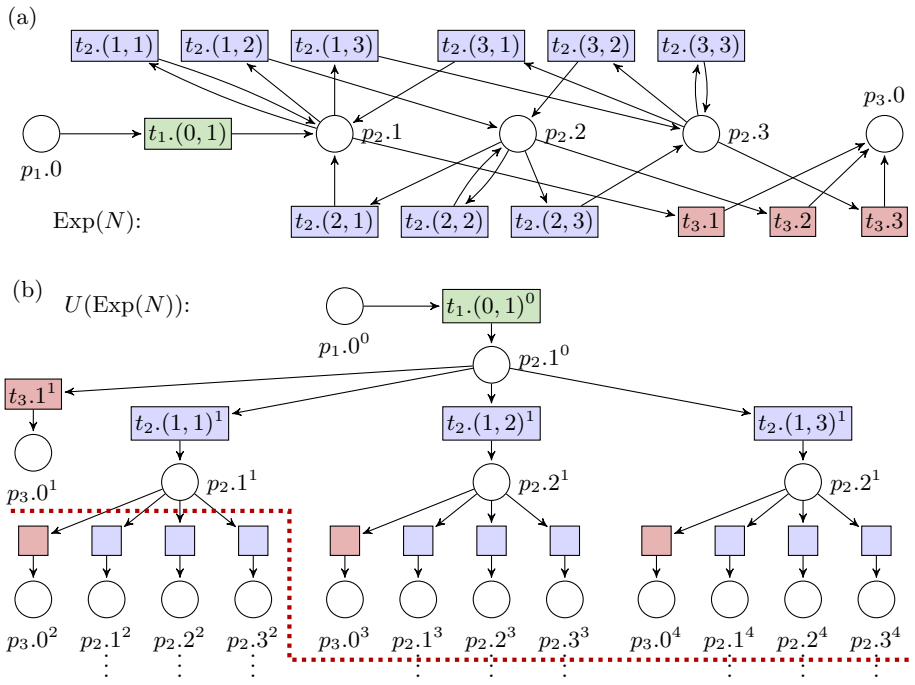


Fig. 2: The expansion $\mathrm{Exp}(N)$ of the running example N from Fig. 1a for $Col = \{0,1,2,3\}$ in (a), and (a prefix of) the respective unfolding $\Upsilon(\mathrm{Exp}(N))$ in (b).

$\mathrm{Exp}(N)$ have the same behavior. For a finite high-level Petri net N, the expansion $\mathrm{Exp}(N)$ is finite iff Col is finite.

For a high-level occurrence net O, we define the P/T net $\mathrm{Exp}_\mathrm{O}(O) := U(\mathrm{Exp}(O))$. The operator Exp_O maps high-level occurrence nets to occurrence nets, which is shown in [4]. We denote $\Upsilon(\mathrm{Exp}(O)) = \langle \mathrm{Exp}_\mathrm{O}(O), \pi_\mathrm{O} \rangle$. Let now $\beta = \langle O, h \rangle$ be a symbolic branching process of N. Then we can define the *expanded symbolic branching process* $\mathrm{Exp}_\mathrm{O}(\beta) = \langle \mathrm{Exp}_\mathrm{O}(O), h_\mathrm{O} \rangle$ of $\mathrm{Exp}(N)$ with the homomorphism $h_\mathrm{O} : \mathrm{Exp}_\mathrm{O}(O) \to \mathrm{Exp}(N)$, defined by $h_\mathrm{O}(\mathsf{e}) = t.\sigma \Leftrightarrow \pi_\mathrm{O}(\mathsf{e}) = e.\sigma \wedge h(e) = t$ and $h_\mathrm{O}(\mathsf{b}) = p.c \Leftrightarrow \pi_\mathrm{O}(\mathsf{b}) = e.c \wedge h(b) = p$ for events e resp. conditions b in $\mathrm{Exp}_\mathrm{O}(O)$. The following result is shown in [4].

Lemma 1 ([4], Sec. 4.1). $\Upsilon(\mathrm{Exp}(N)) \simeq \mathrm{Exp}_\mathrm{O}(\Upsilon(N))$

With this result, we state the following:

Lemma 2. *Let N be a high-level Petri net and β be a prefix of $\Upsilon(N)$. Then β is finite and complete iff $\mathrm{Exp}_\mathrm{O}(\beta)$ is a finite and complete prefix of $\Upsilon(\mathrm{Exp}(N))$.*

The detailed proof is moved to App. A.1. It mainly uses the results from Prop. 1 and Prop. 2, since the definition of completeness on the symbolic level is a direct translation from its P/T analogue.

We can now compare the two complete finite prefixes resulting from the original ERV-algorithm from [10] applied to $\mathrm{Exp}(N)$ and the generalized ERV-algorithm Alg. 1 applied to N. From the definition of the generalized cut-off criterion we get that both these prefixes have the same depth. However, due to the high-level representation, the breadth of the symbolic prefix can be substantially smaller.

Running Example. Consider again $N \in \mathbf{N_f}$ from Fig. 1a and assume $Col = \{0, 1, 2, 3\}$ (i.e., $m = 3$). The expansion $\mathrm{Exp}(N)$ is depicted in Fig. 2a. The (infinite) unfolding of $\mathrm{Exp}(N)$ is shown in Fig. 2b. The prefix resulting from applying the original ERV-algorithm from [10] is marked by the red dotted line. We see that for this example and $Col = \{0, \ldots, m\}$, the low-level prefix obtained by the original ERV-algorithm has $O(m^2)$ nodes. In contrast, the complete finite prefix (cp. Fig. 1b) obtained by Alg. 1 has 11 nodes for every m.

The structure of this running example can easily be generalized, resulting in the following proposition.

Proposition 8. *For every $a \in \mathbb{N}$ there is a high-level net $N \in \mathbf{N_f}$ such that for $Col = \{0, \ldots, m\}$ the complete finite prefix obtained by Alg. 1 has a constant number of nodes, while the number of nodes in the low-level prefix obtained by the original ERV-algorithm is in $O(m^a)$.*

4 Handling Infinitely Many Reachable Markings

Unfoldings of unbounded P/T Petri nets (i.e., with infinitely many markings) have been investigated in [1,7], and in [11] concurrent well-structured transition systems with infinite state space are unfolded. When applying the generalized ERV-algorithm, Alg. 1, to high-level Petri nets with infinitely many reachable markings (therefore violating ***(3)*** from the definition of $\mathbf{N_f}$), the proof for finiteness of the resulting prefix does not hold anymore: the proof of Prop. 6, step (1), is a generalization of the proof of the respective claim in [10] (which uses the pigeonhole principle). It is argued that we cannot have $|\mathcal{R}(N)|+1$ consecutive events s.t. their cone configurations each generate a marking in the net not seen before, and we thus have a cut-off event. When we deal with infinitely many markings, this argument cannot be made.

In this section, we introduce a class $\mathbf{N_{sc}}$ of safe high-level nets, called symbolically compact, that have possibly infinitely many reachable markings (and therefore an infinite expansion), generalizing the class $\mathbf{N_f}$. We then proceed to make adaptions to Alg. 1 (i.e., to the used cut-off criterion), so that it generates a finite and complete prefix of the symbolic unfolding for any $N \in \mathbf{N_{sc}}$.

The following Lemma precisely describes the finite high-level Petri nets for which a finite and complete prefix of the symbolic unfolding exists.

Lemma 3. *For a finite high-level Petri net $N = \langle \mathcal{N}, \mathcal{M}_0 \rangle$ there exists a finite and complete prefix of $\Upsilon(N)$ if and only if there exists a bound $n \in \mathbb{N}$ such that every marking in $\mathcal{R}(N)$ is reachable from a marking in $\mathcal{M}_0$ by firing at most n transitions.*

For the proof (cp. App A.1), we argue that in the case of such a bound, the symbolic unfolding up to depth $n+1$ is a finite and complete prefix, and that in the absence of such a bound no depth of a prefix is enough for it to be complete.

4.1 Symbolically Compact High-level Petri Nets

We use the result of Lemma 3 to define the class $\mathbf{N_{sc}}$ of high-level nets for which we adapt the algorithm for constructing finite and complete prefixes of the symbolic unfolding.

Definition 8 (Class $\mathbf{N_{sc}}$). *A finite high-level Petri net N is called* symbolically compact *if it satisfies **(1)** and **(2)** from Def. 4, and*

(3*) *There is a bound $n \in \mathbb{N}$ on the number of transition firings needed to reach all markings in $\mathcal{R}(N)$.*

The class $\mathbf{N_{sc}}$ contains all symbolically compact high-level Petri nets.

Note that in the case of a (finite, safe) P/T net, property ***(3*)*** is equivalent to ***(3)*** (i.e., $|\mathcal{R}(N)| < \infty$). However, this is *not* true for all high-level nets N: while $|\mathcal{R}(N)| < \infty$ still implies ***(3*)*** (meaning $\mathbf{N_f} \subseteq \mathbf{N_{sc}}$), the reverse implication does not hold, as our running example from Fig. 1a demonstrates when we change the set of colors to $Col = \mathbb{N}$: it still satisfies ***(1)*** and ***(2)***, with $\mathcal{R}(N) = \{\{\!|\langle p_1, 0\rangle|\!\}, \{\!|\langle p_3, 0\rangle|\!\}\} \cup \{\{\!|\langle p_2, \ell\rangle|\!\} \mid \ell \in \mathbb{N}\}$. So we have infinitely many markings that can all be reached by firing at most two transitions, meaning the net satisfies ***(3*)*** and is therefore symbolically compact.

Lemma 3 implies that the class $\mathbf{N_{sc}}$ of symbolically compact nets contains exactly all high-level Petri nets satisfying ***(1)*** and ***(2)*** for which a finite and complete prefix of the symbolic unfolding exists (independently of the number of reachable markings). Since the reachable markings of a high-level Petri net and its expansion correspond to each other, this observation leads to an interesting subclass $\mathbf{N_{sc}} \setminus \mathbf{N_f}$ of symbolically compact high-level Petri nets that have infinitely many reachable markings (such as our running example from Fig. 1a with $Col = \mathbb{N}$). For every net N in this subclass

- there exists a finite and complete prefix of $\Upsilon(N)$, but
- there does *not* exist a finite and complete prefix of $\Upsilon(\mathrm{Exp}(N))$.

In particular, the original ERV-algorithm cannot be applied to $\mathrm{Exp}(N)$, since the expansion is an infinite net.

For the rest of the paper, let $N = \langle P, T, F, \iota, \mathcal{M}_0\rangle \in \mathbf{N_{sc}}$ with symbolic unfolding $\Upsilon = \langle U, \pi\rangle = \langle B, E, G, \iota, \mathcal{K}_0, \pi\rangle$.

4.2 The Finite Prefix Algorithm for Symbolically Compact Nets

As previously discussed, the argument that states the existence of one event in a chain of $|\mathcal{R}(N)| + 1$ consecutive events, such that every marking represented by its cone configuration is contained in the union of all markings represented by previous cone configurations, cannot be applied in the case of an infinite number of reachable markings. Consequently, Alg. 1 may not terminate when applied to a

net in $\mathbf{N_{sc}} \setminus \mathbf{N_f}$. However, condition ***(3*)*** guarantees that every marking reached by a cone configuration $[e]$ with depth $> n$ can be reached by a configuration C containing no more than n events.

For the algorithm to terminate, we need to adjust the cut-off criterion since we do not know whether C is also a cone configuration, as demanded in Def. 6. Therefore, we define *cut-off* events*, that generalize cut-off events. They only require that every marking in $\mathcal{M}([e])$ has been observed in a set $\mathcal{M}(C)$ for *any* configuration $C \prec [e]$, rather than just considering cone configurations:

Definition 9 (Cut-off* event). *Under the assumptions of Def. 6, the high-level event e is a* cut-off* *event (w.r.t. $\prec$) if $\mathcal{M}([e]) \subseteq \bigcup_{C \prec [e]} \mathcal{M}(C)$.*

We additionally assume that the used adequate order satisfies $|C_1| < |C_2| \Rightarrow C_1 \prec C_2$, so that every event with depth $> n$ will be a cut-off event. Since all adequate orders discussed in [10] satisfy this this property (cp. App A.2), this is a reasonable requirement. This adaption and assumption now lead to:

Theorem 1. *Assume a given adequate order $\prec$ to satisfy $|C_1| < |C_2| \Rightarrow C_1 \prec C_2$. When replacing in Alg. 1 the term "cut-off event" by "cut-off* event", it terminates for any input net $N \in \mathbf{N_{sc}}$, and generates a complete finite prefix of $\Upsilon(N)$.*

Proof. The properties of symbolic unfoldings that we stated in Sec. 2.3 are independent on the class of high-level nets. Def. 10 only uses that the considered net is safe, and so do Prop. 4 and Prop. 5. We therefore only have to check that the correctness proof for the algorithm still holds. In the proof of Prop. 6 (*Fin* is finite), the steps (2) and (3) are independent of the used cut-off criterion. In step (1), however, it is shown that the depth of events never exceeds $|\mathcal{R}(N)| + 1$. This is not applicable when $|\mathcal{R}(N)| = \infty$, as argued above. Instead we show:

(1*) For every event e of *Fin*, $d(e) \leq n + 1$, where n is the bound on the number of transitions needed to reach all markings in $\mathcal{R}(N)$.

This is done in detail in App. A.1 and proves that *Fin* is finite. In the proof of Prop. 7, the cut-off criterion is used to show (by an infinite descent approach), for any marking $M \in \mathcal{R}(N)$ the existence of a minimal configuration $C \in Fin$ with $M \in \mathcal{M}(C)$. Due to the similarity of cut-off and cut-off*, this proof can easily be adapted to work as before.

The only thing remaining to show is termination. In the case of nets in $\mathbf{N_f}$, every object is finite, which, together with Prop. 6, leads to termination of the algorithm. For nets in $\mathbf{N_{sc}} \setminus \mathbf{N_f}$, however, there is at least one event e in *Fin* s.t. $|\mathcal{M}([e])| = \infty$. Thus, we have to show that we can check the cut-off* criterion in finite time. This follows from Cor. 2 in the next section, which is dedicated to symbolically representing markings generated by configurations. □

4.3 Checking Cut-offs Symbolically

We show how to check whether a high-level event e is a cut-off* event in finite time. By definition, this means checking whether $\mathcal{M}([e]) \subseteq \bigcup_{C \prec [e]} \mathcal{M}(C)$. However, since the cut of a configuration can represent infinitely many markings, we cannot simply store the set $\mathcal{M}(C)$ for every $C \in \mathcal{C}(Fin)$. Instead, we now

define constraints that symbolically describe the markings represented by a configuration's cut. Checking the inclusion above then reduces to checking an implication of these constraints. Since we consider high-level Petri nets with guards written in a decidable first order theory, such implications can be checked in finite time.

We first define for every condition b a new predicate $pred^{\odot}(b)$ by

$$pred^{\odot}(b) := pred(\mathbf{e}(b)) \wedge (b = \mathbf{v_e}(b)).$$

This predicate now has (in an abuse of notation) an extra variable, called b. The remaining variables in $pred(\mathbf{e}(b))$ are $Var_{[\mathbf{e}(b)]\cup\{\perp\}}$, and $pred(\mathbf{e}(b))$ evaluates to *true* under an assignment $\theta : Var_{[\mathbf{e}(b)]\cup\{\perp\}} \to Col$ if and only if a concurrent execution of $[\mathbf{e}(b)]$ with the assigned modes is possible (i.e., under every instantiation of $[\mathbf{e}(b)]$). In such an execution, $\theta(\mathbf{v_e}(b)) \in Col$ is placed on b.

For a co-set $B' \subseteq B$ of high-level conditions, the constraint on B' is an expression over B' describing which color combinations can lie on the high-level conditions. We build the conjunction over all predicates $pred^{\odot}(b)$ for $b \in B'$ and quantify over all appearing variables v_e: the *constraint on* B' is defined by

$$\kappa(B') := \exists_{\bigcup_{b\in B'} Var_{[\mathbf{e}(b)]\cup\{\perp\}}} : \bigwedge_{b\in B'} pred^{\odot}(b),$$

where B' serves as the set of free variables in $\kappa(B')$.

We denote by $\Xi(B')$ the set of variable assignments $\vartheta : B' \to Col$ that satisfy $\kappa(B')[\vartheta] \equiv true$. Note that for a configuration C, we have $\bigcup_{b\in \mathrm{cut}(C)} Var_{[\mathbf{e}(b)]} = Var_C$, i.e., the bounded variables in $\kappa(\mathrm{cut}(C))$ are exactly the variables appearing in predicates in C. For every instantiation θ of C we define a variable assignment $\vartheta_\theta : \mathrm{cut}(C) \to Col$ by setting $\forall b \in \mathrm{cut}(C) : \vartheta_\theta(b) = \theta(\mathbf{v_e}(b))$. Instantiations of a configuration and the constraint on its cut are now related as follows.

Lemma 4. *Let $C \in \mathcal{C}(\Upsilon)$. Then $\Xi(\mathrm{cut}(C)) = \{\vartheta_\theta \mid \theta \in \Theta(C)\}$.*

The proof is moved to App. A.1, and follows by construction of $pred^{\odot}$ and ϑ_θ. From the definition of $\mathcal{K}(C)$ and $\mathcal{M}(C)$ we get:

Corollary 1. *Let $C \in \mathcal{C}(\Upsilon)$. Then $\mathcal{K}(C) = \{\{\langle b, \vartheta(b)\rangle \mid b \in \mathrm{cut}(C)\} \mid \vartheta \in \Xi(\mathrm{cut}(C))\}$ and $\mathcal{M}(C) = \{\{\!|\, \langle \pi(b), \vartheta(b)\rangle \mid b \in \mathrm{cut}(C) \,|\!\}\} \mid \vartheta \in \Xi(\mathrm{cut}(C))\}$.*

We now show how to check whether an event is a cut-off* event via the constraints defined above. For that, we first look at general configurations in Thm. 2, and then explicitly apply this result to cone configurations $[e]$ in Cor. 2.

Since we consider safe high-level Petri nets, we can relate two cuts representing the same marking in the following way:

Definition 10. *Let $C_1, C_2 \in \mathcal{C}(\Upsilon)$ with $\pi(\mathrm{cut}(C_1)) = \pi(\mathrm{cut}(C_2))$. Then there is a unique bijection $\phi : \mathrm{cut}(C_1) \to \mathrm{cut}(C_2)$ preserving π. We call this mapping $\phi_{C_1}^{C_2}$.*

Theorem 2. *Let $C, C_1, \ldots, C_n$ be finite configurations in the symbolic unfolding of a safe high-level Petri net s.t. $\forall 1 \le i \le n : \pi(\mathrm{cut}(C)) = \pi(\mathrm{cut}(C_i))$. Then*

$$\mathcal{M}(C) \subseteq \bigcup_{i=1}^{n} \mathcal{M}(C_i) \quad \textit{if and only if} \quad \kappa(\mathrm{cut}(C)) \Rightarrow \bigvee_{i=1}^{n} \kappa(\mathrm{cut}(C_i))[\phi_{C_i}^{C}].$$

Proof. Denote $\phi_i := \phi^C_{C_i}$. Assume $\mathcal{M}(C) \subseteq \bigcup_{i=1}^n \mathcal{M}(C_i)$ and let $\vartheta \in \Xi(\mathrm{cut}(C))$. By Cor. 1 we have that $M_\vartheta := \{\langle \pi(b), \vartheta(b)\rangle \mid b \in \mathrm{cut}(C)\} \in \mathcal{M}(C)$. Thus, $\exists 1 \leq i \leq n : M_\vartheta \in \mathcal{M}(C_i)$. This, again by Cor. 1, means $\exists \vartheta_i \in \Xi(\mathrm{cut}(C_i)) :$

$$\begin{aligned} M_\vartheta &= \{\langle \pi(b'), \vartheta_i(b')\rangle \mid b' \in \mathrm{cut}(C_i)\} = \{\langle \pi(\phi_i^{-1}(b)), \vartheta_i(\phi_i^{-1}(b))\rangle \mid b \in \mathrm{cut}(C)\} \\ &= \{\langle \pi(b), (\vartheta_i \circ \phi_i^{-1})(b)\rangle \mid b \in \mathrm{cut}(C)\}. \end{aligned}$$

This shows that $\vartheta|_{\mathrm{cut}(C)} = \vartheta_i \circ \phi_i^{-1}$. Thus, $\kappa(\mathrm{cut}(C_i))[\phi_i][\vartheta] \equiv \kappa(\mathrm{cut}(C_i))[\vartheta \circ \phi_i] \equiv \kappa(\mathrm{cut}(C_i))[\vartheta_i \circ \phi_i^{-1} \circ \phi_i] \equiv \kappa(\mathrm{cut}(C_i))[\vartheta_i] \equiv \mathit{true}$, which proves the implication.

Assume on the other hand $\kappa(\mathrm{cut}(C)) \Rightarrow \bigvee_{i=1}^n \kappa(\mathrm{cut}(C_i))[\phi_i]$. Let $M \in \mathcal{M}(C)$. Then $\exists \vartheta \in \Xi(\mathrm{cut}(C)) : M = \{\langle \pi(b), \vartheta(b)\rangle \mid b \in \mathrm{cut}(C)\}$. Thus, $\exists 1 \leq i \leq n : \kappa(\mathrm{cut}(C_i))[\phi_i][\vartheta] \equiv \mathit{true}$. Let $\vartheta_i = \vartheta \circ \phi_i$. Then $\vartheta_i \in \Xi(\mathrm{cut}(C_i))$, and $M_{\vartheta_i} := \{\langle \pi(b'), \vartheta_i(b')\rangle \mid b' \in \mathrm{cut}(C_i)\} \in \mathcal{M}(C_i)$. Since

$$M_{\vartheta_i} = \{\langle \pi(\phi_i^{-1}(b)), \vartheta \circ \phi_i(\phi_i^{-1}(b))\rangle \mid b \in \mathrm{cut}(C)\} = \{\langle \pi(b), \vartheta(b)\rangle \mid b \in \mathrm{cut}(C)\},$$

we have $M = M_{\vartheta_i} \in \mathcal{M}(C_i)$, which completes the proof. □

The following Corollary now gives us a characterization of cut-off* events in a symbolic branching process. It follows from Thm. 2 together with the facts that $\mathcal{M}(C_1) \cap \mathcal{M}(C_2) \neq \emptyset \Rightarrow \pi(\mathrm{cut}(C_1)) = \pi(\mathrm{cut}(C_2))$, and that $\prec[e]$ is finite.

Corollary 2. *Let β be a symbolic branching process and e an event in β. Then e is a cut-off* event in β if and only if*

$$\kappa(\mathrm{cut}([e])) \Rightarrow \bigvee_{\substack{C \prec [e] \\ h(\mathrm{cut}(C)) = h(\mathrm{cut}([e]))}} \kappa(\mathrm{cut}(C))[\phi^{[e]}_C].$$

Thus, we showed how to decide for any event e added to a prefix of the unfolding whether it is a cut-off* event, namely, by checking the above implication in Cor. 2. Note that we can also check whether e is a *cut-off* event (w.r.t. Def. 6) by the implication in Cor. 2 when we replace all occurrences of "C" by "$[e']$" .

5 Conclusions and Outlook

We introduced the notion of complete finite prefixes of symbolic unfoldings of high-level Petri nets. We identified a class of 1-safe high-level nets generalizing 1-safe P/T nets, for which we generalized the well-known algorithm by Esparza et al. to compute such a finite and complete prefix. This constitutes a consolidation and generalization of the concepts of [10,3,4,5]. While the resulting symbolic prefix has the same depth as a finite and complete prefix of the unfolding of the represented P/T net, it can be significantly smaller due to less branching. In the case of infinitely many reachable markings (where the original algorithm is not applicable) we identified the class of so-called *symbolically compact* nets for which an adapted version of the generalized algorithm works. For that, we showed how to check an adapted cut-off criterion by symbolically describing sets of markings.

The next step is an implementation of the generalized algorithm. Future works also include the generalization for k-bounded high-level Petri nets.

References

1. Abdulla, P.A., Iyer, S.P., Nylén, A.: Unfoldings of unbounded petri nets. In: Proc. CAV 2000. pp. 495–507. LNCS 1855, Springer (2000). https://doi.org/10.1007/10722167_37
2. Best, E., Grahlmann, B.: Programming Environment based on Petri nets – Documentation and User Guide Version 1.4 (1995), https://uol.de/f/2/dept/informatik/ag/parsys/PEP1.4_man.ps.gz?v=1346500853
3. Chatain, T.: Symbolic Unfoldings of High-Level Petri Nets and Application to Supervision of Distributed Systems. Ph.D. thesis, Universit é de Rennes (2006), https://www.sudoc.fr/246936924
4. Chatain, T., Fabre, E.: Factorization properties of symbolic unfoldings of colored Petri nets. In: Lilius, J., Penczek, W. (eds.) Proc. PETRI NETS 2010. pp. 165–184. LNCS 6128, Springer (2010). https://doi.org/10.1007/978-3-642-13675-7_11
5. Chatain, T., Jard, C.: Symbolic diagnosis of partially observable concurrent systems. In: Proc. FORTE 2004. pp. 326–342. LNCS 3235, Springer (2004). https://doi.org/10.1007/978-3-540-30232-2_21
6. Chatain, T., Jard, C.: Complete finite prefixes of symbolic unfoldings of safe time Petri nets. In: Proc. ICATPN 2006. pp. 125–145. LNCS 4024, Springer (2006). https://doi.org/10.1007/11767589_8
7. Desel, J., Juhás, G., Neumair, C.: Finite unfoldings of unbounded petri nets. In: ICATPN 2004. pp. 157–176. LNCS 3099, Springer (2004). https://doi.org/10.1007/978-3-540-27793-4_10
8. Ehrig, H., Hoffmann, K., Padberg, J., Baldan, P., Heckel, R.: High-level net processes. In: Formal and Natural Computing. pp. 191–219. LNCS 2300, Springer (2002). https://doi.org/10.1007/3-540-45711-9_12
9. Engelfriet, J.: Branching processes of Petri nets. Acta Informatica **28**(6), 575–591 (1991). https://doi.org/10.1007/BF01463946
10. Esparza, J., Römer, S., Vogler, W.: An improvement of McMillan's unfolding algorithm. Formal Methods Syst. Des. **20**(3), 285–310 (2002). https://doi.org/10.1023/A:1014746130920
11. Herbreteau, F., Sutre, G., Tran, T.Q.: Unfolding concurrent well-structured transition systems. In: Proc. TACAS 2007. pp. 706–720. LNCS 4424, Springer (2007). https://doi.org/10.1007/978-3-540-71209-1_55
12. Jensen, K.: Coloured Petri Nets - Basic Concepts, Analysis Methods and Practical Use - Volume 1, Second Edition. Monographs in Theoretical Computer Science. An EATCS Series, Springer (1996). https://doi.org/10.1007/978-3-662-03241-1
13. Khomenko, V., Koutny, M.: Branching processes of high-level Petri nets. In: Proc. TACAS 2003. pp. 458–472. LNCS 2619, Springer (2003). https://doi.org/10.1007/3-540-36577-X_34
14. McMillan, K.L.: A technique of state space search based on unfolding. Formal Methods Syst. Des. **6**(1), 45–65 (1995). https://doi.org/10.1007/BF01384314
15. Nielsen, M., Plotkin, G.D., Winskel, G.: Petri nets, event structures and domains, part I. Theor. Comput. Sci. **13**, 85–108 (1981). https://doi.org/10.1016/0304-3975(81)90112-2
16. Presburger, M.: über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. In: Proc. Comptes-rendus du I Congrés des Mathématiciens des Pays Slaves, Varsovie 1929. pp. 92–101 (1930)
17. Reisig, W.: Understanding Petri Nets - Modeling Techniques, Analysis Methods, Case Studies. Springer (2013). https://doi.org/10.1007/978-3-642-33278-4

A Appendix

A.1 Additional Proofs

In this section we present the proofs which are omitted in the body of the paper.

We start by proving the propositions Prop. 1, Prop 2, and Prop 3, which each state a property of the symbolic unfolding that is a high-level analogue to a property of (low-level) unfoldings.

Proof of Prop. 1. The proof is an easy induction over the number n of transitions/events needed to reach a respective marking/cut. The induction anchor $n = 0$ is proved by using that π is an initial homomorphism which gives $\mathcal{M}_0 = \{\{\!\!\{ \langle \pi(b), c\rangle \mid \langle b, c\rangle \in K_0 \}\!\!\} \mid K_0 \in \mathcal{K}_0\} = \{\{\!\!\{ \langle \pi(b), c\rangle \mid \langle b, c\rangle \in K \}\!\!\} \mid K \in \mathcal{K}(\emptyset)\} = \{\mathrm{mark}(\emptyset.\theta) \mid \theta \in \Theta(\emptyset)\}$. The induction step is realized by Prop 2. □

Proof of Prop 2. Let $U = \langle B, E, G, \iota, \mathcal{K}_0\rangle, C \in \mathcal{C}(\Upsilon), \theta \in \Theta(C), t \in T, \sigma \in \Sigma(t)$.

Let $\mathrm{mark}(C.\theta)[t, \sigma\rangle$, which means $pre(t, \sigma) \leq \mathrm{mark}(C.\theta) = \{\!\!\{ \langle \pi(b), \theta(\mathbf{v_e}(b))\rangle \mid \langle b, \theta(\mathbf{v_e}(b))\rangle \in \mathrm{cut}(C.\theta) \}\!\!\}$, leading to

$$\{\!\!\{ \langle \pi(b), v\rangle \mid \langle p, v\rangle \in pre(t), \pi(b) = p, \langle b, \theta(\mathbf{v_e}(b))\rangle \in \mathrm{cut}(C.\theta) \}\!\!\} = pre(t).$$

Aiming a contradiction, assume $\nexists e \in E : \pi(e) = t \wedge \mathrm{cut}(C.\theta)[e, \sigma\rangle$. We now extend Υ by such an event. We add to E an event $\widetilde{e}$ with $\pi(\widetilde{e}) = t$ and $\iota(\widetilde{e}) = \iota(t)$. We define $pre(\widetilde{e}) = \{\!\!\{ \langle b, v\rangle \mid \langle p, v\rangle \in pre(t), \pi(b) = p, \langle b, \theta(\mathbf{v_e}(b))\rangle \in \mathrm{cut}(C.\theta) \}\!\!\}$. Then we have $pre(\pi(\widetilde{e})) = \{\!\!\{ \langle \pi(b), v\rangle \mid \langle b, v\rangle \in pre(\widetilde{e}) \}\!\!\}$. For every $\langle p, v\rangle \in post(t)$, we then add $post(t)(p, v)$ conditions b with $\pi(b) = p$ to B and add $\langle \widetilde{e}, v, b\rangle$ to G. We thus get $post(\pi(\widetilde{e})) = \{\!\!\{ \langle \pi(b), v\rangle \mid \langle b, v\rangle \in post(\widetilde{e}) \}\!\!\}$. We now created a symbolic branching process bigger than Υ, contradicting that Υ is the symbolic unfolding.

Assume on the other hand $\exists e \in E : \pi(e) = t \wedge \mathrm{cut}(C.\theta)[e, \sigma\rangle$. Then $pre(e, \sigma) \leq \mathrm{cut}(C.\theta)$, and therefore, $pre(t) = \{\!\!\{ \langle \pi(b), v\rangle \mid \langle b, v\rangle \in pre(e) \}\!\!\} \leq \{\!\!\{ \langle \pi(b), v\rangle \mid \langle b, v\rangle \in \mathrm{cut}(C.\theta) \}\!\!\} = \mathrm{mark}(C.\theta)$, meaning $\mathrm{mark}(C.\theta)[t, \sigma\rangle$. □

Proof of Prop 3. Let $\Uparrow C = \langle O', h'\rangle$ with $O' = \langle B', E', F', \iota', \mathcal{K}(C)\rangle$. To show that O' is an occurrence net, we have to show *i* – *iv* from the definition on page 4. *i* – *iii* are purely structural properties and follow from the fact that O is an occurrence net. *iv* is satisfied since $\forall b \in \mathrm{cut}(C)\ \forall K \in \mathcal{K}(C) : \sum_{c \in Col} K(b, c) = 1$ and $\forall b \in B' \setminus \mathrm{cut}(C)\ \forall K \in \mathcal{K}(C) : \sum_{c \in Col} K(b, c) = 0$. h' is a homomorphism that is injective on events with the same preset since h is, and that h' is initial follows by Prop. 1 and Prop. 2.

When β is the symbolic unfolding of $\langle N, \mathcal{M}_0\rangle$, then the maximality of $\Uparrow C$ follows from the maximality of β, making $\Uparrow C$ the symbolic unfolding of $\langle N, \mathcal{M}(C)\rangle$. □

Prop. 4 states the existence of a unique monomorphism $\varphi^2_{1,D}$ from $O(C_1|D)$ into $\Uparrow C_2$, given the existence of a marking $M \in \mathcal{M}(C_1) \cap \mathcal{M}(C_2)$ satisfying $C_1[\![M]\!]D$.

Proof of Prop. 4. By induction over the size $k = |D|$ of the suffix D.
Base case $k = 0$. This means $D = \emptyset$. Then $O(C_1|D) = \langle \mathrm{cut}(C_1), \emptyset, \emptyset, \mathcal{K}(C_1)\rangle$. Since $M \in \mathcal{M}(C_1) \cap \mathcal{M}(C_2)$, we know that $\pi(\mathrm{cut}(C_1)) = \pi(\mathrm{cut}(C_2))$. Since we only consider safe nets, $\varphi^2_{1,D}$ is uniquely realized by $\phi^{C_2}_{C_1} : \mathrm{cut}(C_1) \to \mathrm{cut}(C_2)$ from Def. 10.

Induction step. Let $k > 0$. Let $\theta \in \Theta(C_1 \oplus D)$ s.t. $\mathrm{mark}(C_1, \theta|_{Var_{C_1 \cup \{\perp\}}}) = M$. Let $e \in Min(D)$. Then for $\sigma = [v \leftarrow \theta(v_e)]_{v \in Var(e)}$ we have $M[\pi(e), \sigma\rangle$. Thus, by Prop 2, $\exists e' \in E : \pi(e') = \pi(e) \wedge C_2 \oplus \{e'\} \in \mathcal{C}(\Upsilon)$. This means $\rightarrow e' \subseteq (B_0 \cup (C_2 \rightarrow)) \setminus (\rightarrow C_2)$; else, $C_2 \oplus \{e'\}$ would not be a configuration. Thus, e' is an event in $\Uparrow C_2$. Since $\pi(e) = \pi(e')$, we get by definition of homomorphisms that $\{\langle \pi(b), v\rangle \mid \langle b, v\rangle \in post(e)\} = \{\langle \pi(b), v\rangle \mid \langle b, v\rangle \in post(e')\}$. The net N is safe, therefore we can define the bijection $\phi_1 : (e \rightarrow) \to (e' \rightarrow)$ by $\phi_1(b) = b' \Leftrightarrow \pi(b) = \pi(b')$. We now define $\varphi_1 : O(C_1|\{e\}) \to \Uparrow C_2$ by $\varphi_1 = \phi^{C_2}_{C_1} \uplus [e \mapsto e'] \uplus \phi_1$, which is a homomorphism satisfying the claimed conditions.

Let now $C_1' = C_1 \cup \{e\}$, $C_2' = C_2 \cup \{\varphi_1(e)\}$ and $D' = D \setminus \{e\}$. We then have for M' given by $M[\pi(e), \sigma\rangle M'$ that $C_1'[\![M']\!]D'$, $M' \in \mathcal{M}(C_1') \cap \mathcal{M}(C_2')$, and $|D'| < k$. Thus, by the induction hypothesis, we get that there is a unique monomorphism $\varphi_2 : O(C_1'|D') \to \Uparrow C_2'$ satisfying the conditions above. Since φ_1 and φ_2 coincide on $\mathrm{cut}(C_1')$, we can now define $\varphi^2_{1,D}$ by "gluing together" φ_1 and φ_2 at $\mathrm{cut}(C_1')$.

This proves the claim for finite extensions. For an infinite extension, every node also contained in a finite extension. Due to uniqueness of the homomorphisms, we can define the $\varphi^2_{1,D}$ in the case of an infinite D as the union of all homomorphisms of smaller finite extensions. □

We continue with the proof of Prop. 5 which states that adequate orders are compatible with extensions also in the other direction.

Proof of Prop. 5. Let $D' = \varphi^2_{1,D}(D)$. We first show that $\varphi^1_{2,D'}(D') = D$.

Let $\varphi_1 : O(C_1|D) \to \varphi^2_{1,D}(O(C_1|D))$ be the isomorphism that acts on $O(C_1|D)$ as $\varphi^2_{1,D}$ does, and let $\varphi_2 : O(C_2|D') \to \varphi^1_{2,D'}(O(C_2|D'))$ be the isomorphism that acts on $O(C_2|D')$ as $\varphi^1_{2,D'}$ does. Since $\varphi_1^{-1} : \varphi^2_{1,D}(O(C_1|D)) \to O(C_1|D)$ and $O(C_1|D) \subset \Uparrow C_1$, and $\varphi_1^{-1}(\varphi^2_{1,D}(D)) = D$ is a suffix of C_1, we get by Prop. 4 that $\varphi_1^{-1} = \varphi_2$, which means $\varphi^1_{2,D'}(D') = D$.

Assume now $C_2 \prec C_1$. From the proof of Prop. 4 we see that $C_2[\![M]\!]\varphi^2_{1,D}(D)$. Thus, we get by the definition of adequate order and the result above that $C_2 \oplus \varphi^2_{1,D}(D) \prec C_1 \oplus \varphi^1_{2,\varphi^2_{1,D}(D)}(\varphi^2_{1,D}(D)) = C_1 \oplus D$ □

We explicate the proof of Prop. 6 stating that the constructed prefix *Fin* is finite. For that, we show the results (1),(2) and (3) claimed in the main body of the paper (Sec. 3.2). Additionally, we prove (1*) from Sec. 4.2 in the case $N \in \mathbf{N_{sc}}$. For (1), (2), and (3), this works exactly as in the low-level case in [10] and is taken from there. The proof of (1*) combines the ideas of proving (1) and Prop. 7.

Given an event e, define the *depth* of e as the length of the longest chain of events $e_1 < e_2 < \cdots < e$; the depth of e is denoted by $d(e)$.

Proof of Prop. 6. (i) For every event e of *Fin*, $d(e) \leq n+1$, where n is the number of reachable markings of N:
Every chain of events $e_1 < e_2 < \cdots < e_n < e_{n+1}$ in the unfolding contains an event e_i, $i > 1$, s.t. $\mathcal{M}([e_i]) \subseteq \bigcup_{j=1}^{i-1} \mathcal{M}([e_j])$, since, if every $\mathcal{M}([e_j])$, $j = 1, \ldots, n$, contains a marking not contained in $\bigcup_{k=1}^{j-1} \mathcal{M}([e_k])$, then finally $\bigcup_{j=1}^{n} \mathcal{M}([e_j])$ contains all n markings. This makes e_{n+1} a cut-off event.

(1*) For every event e of *Fin*, $d(e) \leq n+1$, where n bound on the number of transitions needed to reach all markings in $\mathcal{R}(N)$:
Assume that at some point during the algorithm, we reach a state $Fin = (B', E', G', \iota', \mathcal{K}'_0)$, such that there occurs a chain of events $e_1 < e_2 < \cdots < e_{n+1}$. We prove that e_{n+1} must be a cut-off* event. Let $M \in \mathcal{M}([e_{n+1}])$. Then, by definition of $\mathbf{N_{sc}}$, M can be reached by firing at most n transitions. Accordingly, from Prop. 2, we get that there is a configuration $C \in \Upsilon$ such that $M \in \mathcal{M}(C)$. As in the proof of Prop. 7, we can now follow that there is a configuration $\widetilde{C} \in \mathcal{C}(\Upsilon)$ such that $M \in \mathcal{M}(\widetilde{C})$ and $\widetilde{C} \prec C$, that contains no cut-off event and is therefore in *Fin*. Since $|C| \leq n < n+1 \leq |[e_{n+1}]|$, we follow $\widetilde{C} \prec [e_{n+1}]$. So we have that $\forall M \in \mathcal{M}([e_{n+1}])\, \exists \widetilde{C} \prec [e_{n+1}]$, which means that e_{n+1} is a cut-off* event.

(ii) For every event e of *Fin*, the sets $pre(e)$ and $post(e)$ are finite:

By the construction in the algorithm we see that there is a bijection between $post(e)$ and $post(h(e))$, and similarly for $pre(e)$ and $pre(h(e))$. The result then follows from the finiteness of N.

(iii) For every $k \geq 0$, *Fin* contains only finitely many events e such that $d(e) \leq k$:

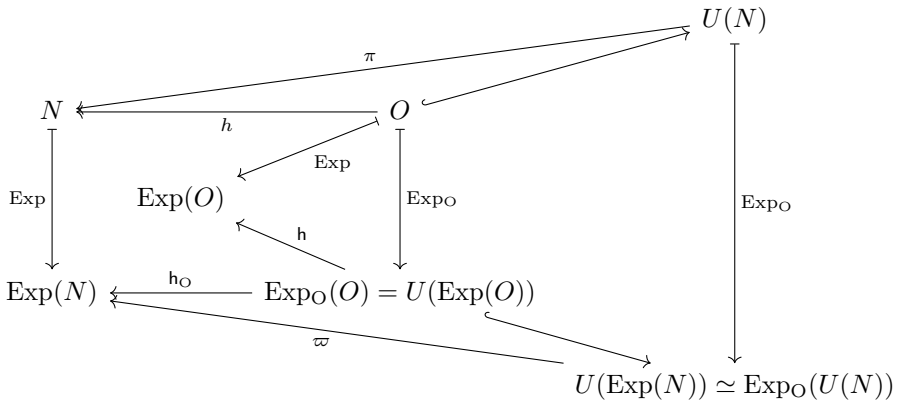
By complete induction on k. The base case, $k = 0$, is trivial. Let E_k be the set of events of depth at most k. We prove that if E_k is finite then E_{k+1} is finite. By (2) and the induction hypothesis, $post(E_k)$ is finite. Since $\{b \mid \exists v \in Var : \langle b, v\rangle \in pre(E_{k+1})\} \subseteq \{b \mid \exists v \in Var : \langle b, v\rangle \in post(E_k)\}$, we get by property *iv* in the definition of occurrence nets that E_{k+1} is finite.

□

We now prove that the expansion of a finite and complete prefix of the symbolic unfolding is a finite and complete prefix of the expansion of the net. We start by introducing some notation.

Lemma 1 gives that, by defining $\varpi : \mathrm{Exp_O}(U(N)) \to \mathrm{Exp}(N)$ s.t. for all $b \in B, c \in Col, t \in T, \sigma \in \Sigma(t)$ we have $\varpi(b.c) = \pi(b).c$ and $\varpi(t.\sigma) = \pi(t).\sigma$, we get that $\langle \mathrm{Exp_O}(U(N)), \varpi\rangle$ is the unfolding of $\mathrm{Exp}(N)$.

For any symbolic branching process $\beta = \langle O, h\rangle$ of N we have $\langle O, h\rangle \leq \langle U(N), \pi\rangle$. Thus, by defining $\mathsf{h_O} : \mathrm{Exp_O}(O) \to \mathrm{Exp}(N)$ by $\mathsf{h_O} = \varpi|_{\mathrm{Exp_O}(O)}$, we get that $\mathrm{Exp_O}(\beta) := \langle \mathrm{Exp_O}(O), \mathsf{h_O}\rangle$ is a branching process of $\mathrm{Exp}(N)$. We define this branching process by $\mathrm{Exp_O}(\beta)$. This is illustrated in the following diagram:



For more details, cp. [4].

Proof of Lemma 2. Let $\beta = \langle O, h\rangle$ be finite and complete. From Lemma 1 we already know that $\mathrm{Exp_O}(O) \subseteq U(\mathrm{Exp}(N))$. Since $\mathrm{Exp_O}(\beta)$ is a branching process of $\mathrm{Exp}(N)$, we see that is a prefix of the unfolding of $\mathrm{Exp}(N)$. Also, $\mathrm{Exp_O}(\beta)$ is obviously finite since O is a finite high-level occurrence net.

We now prove that $\mathrm{Exp_O}(\beta)$ is complete. Let M be a reachable marking in $\mathrm{Exp}(N)$. Then the high-level marking M defined by $M(p, c) = \mathsf{M}(p.c, c)$ is reachable in N. Thus, since β is complete, there is a configuration $C \in \mathcal{C}(\beta)$ and an instantiation $\theta \in \Theta(C)$ satisfying a) and b) from Definition 3. This means there is a firing sequence $K_0[e_1, \sigma_1\rangle K_1 \ldots [e_n, \sigma_n\rangle K_n$ with $\{e_1, \ldots, e_n\} = C$, $\sigma_i = \theta \circ [v \mapsto v_{e_i}]_{v \in Var(e_i)}$, and $K_n = \mathrm{cut}(C.\theta)$ (meaning $M = \mathrm{mark}(C, \theta) = \{\!\!\{ \langle h(b), c\rangle \mid \langle b, c\rangle \in K_n \}\!\!\}$). Then, in $\mathrm{Exp}(\beta)$, the marking $\{\!\!\{ \langle b.c, c\rangle \mid \langle b, c\rangle \in K_n \}\!\!\}$ is reachable from the initial marking $\{\!\!\{ \langle b.c, c\rangle \mid \langle b, c\rangle \in K_0 \}\!\!\}$ by the firing sequence $(e_1.\sigma_1, \sigma_1, \ldots, e_n.\sigma_n, \sigma_n)$. Thus, there is a configuration $\mathsf{C} = \{\mathsf{e}_1, \ldots, \mathsf{e}_n\}$ in $U(\mathrm{Exp}(O)) = \mathrm{Exp_O}(O)$ with $\forall i : \pi_{\mathrm{O}}(\mathsf{e}_i) = e_i.\sigma_i$, such that $\mathrm{mark}(\mathsf{C}.\theta') = \{\!\!\{ \langle \pi_{\mathrm{O}}(\mathsf{b}), \theta'(\mathbf{v}_{\mathbf{e}}(\mathsf{b}))\rangle \mid \mathsf{b} \in \mathrm{cut}(\mathsf{C}) \}\!\!\} = \{\!\!\{ \langle b.c, c\rangle \mid \langle b, c\rangle \in K_n \}\!\!\}$, where $\theta' \in \Theta(\mathsf{C})$ is the only possible instantiation of C (since every event has only one possible mode). Then, by the definition of h_{O}, we get $\mathrm{mark_O}(\mathsf{C}.\theta') := \{\!\!\{ \langle h_{\mathrm{O}}(\mathsf{b}), \theta'(\mathbf{v}_{\mathbf{e}}(\mathsf{b}))\rangle \mid \mathsf{b} \in \mathrm{cut}(\mathsf{C}) \}\!\!\} = \{\!\!\{ \langle h(b).c, c\rangle \mid \langle b, c\rangle \in K_n \}\!\!\} = \mathsf{M}$.

Let now $t.\sigma \in \mathsf{T}$ s.t. $\mathsf{M}[t.\sigma\rangle$. Then $M[t, \sigma\rangle$. Since C, θ satisfy property b) from Definition 3, we know that $\exists e \in E$ s.t. $e \notin C$, $h(e) = t$, and $C.\theta[e, \sigma\rangle$. This means, in $\mathrm{Exp}(\beta)$, we have $\{\!\!\{ \langle b.c, c\rangle \mid \langle b, c\rangle \in K_n \}\!\!\}[e.\sigma, \sigma\rangle$. Thus, there exists an e in $U(\mathrm{Exp}(\beta))$ such that $\mathsf{C}.\theta'[\mathsf{e}.\sigma\rangle$ and $\pi_{\mathrm{O}}(\mathsf{e}) = e.\sigma$, which again means that $h_{\mathrm{O}}(\mathsf{e}) = h(e).\sigma = t.\sigma$. This proves that C and θ satisfy a) and b) from Definition 3, and therefore that $\mathrm{Exp_O}(\beta)$ is complete.

The other direction works analogously. □

Lemma 3 gives a characterization of high-level Petri nets for which a complete finite prefix of the symbolic unfolding exists.

Proof of Lemma 3. From Prop. 1 and Prop. 2 we see that for a finite high-level Petri net with such a bound n, the prefix of the symbolic unfolding containing

exactly the events e with $d(e) \leq n+1$ is complete. Finiteness of this prefix follows from the finiteness of the original net and the definition of homomorphism.

Assume now that no such bound exists, and, for the purpose of contradiction, assume that there is a finite and complete prefix β of $\Upsilon(N)$. Denote $\widetilde{n} = \max\{|C| \mid C \in \mathcal{C}(\beta)\} < \infty$. Then there exists a marking $M \in \mathcal{R}(N)$ for which we have to fire at least $\widetilde{n}+1$ transitions to reach it. Again from Prop. 1 and Prop. 2 it follows that a configuration C with $M \in \mathcal{M}(C)$ must contain at least $\widetilde{n}+1$ events, contradicting that β is complete. □

Lemma 4 concerns the relation between instantiations of a configuration and the constraint on its cut.

Proof of Lemma 4. Let $\vartheta \in \Xi(\mathrm{cut}(C))$. Then $\mathit{true} \equiv \kappa(\mathrm{cut}(C))[\vartheta]$. Thus, there exists $\theta : \mathit{Var}_{C\cup\{\bot\}} \to \mathit{Col}$ s.t. $\big(\bigwedge_{b\in\mathrm{cut}(C)} \mathit{pred}^{\odot}(b)\big)[\vartheta][\theta] \equiv \mathit{true}$ and therefore

$$\Big(\bigwedge_{b\in\mathrm{cut}(C)} \mathit{pred}(\mathbf{e}(b))[\theta]\Big) \wedge \Big(\bigwedge_{b\in\mathrm{cut}(C)} \vartheta(b) = \theta(\mathbf{v_e}(b))\Big) \quad \equiv \quad \mathit{true}. \qquad (1)$$

From the inductive definition of *pred* then follows that $\forall e \in C\cup\{\bot\} : \mathit{pred}(e)[\theta] \equiv \mathit{true}$. Thus, θ is an instantiation of C, and $\vartheta_\theta = \vartheta$, as shown by the posterior conjunction in (1).

Let on the other hand $\theta \in \Theta(\mathrm{cut}(C))$. Then directly, by the definition of $\mathit{pred}^{\odot}(b)$ and ϑ_θ, we get $\big(\bigwedge_{b\in\mathrm{cut}(C)} \mathit{pred}^{\odot}(b)\big)[\vartheta_\theta][\theta] \equiv \mathit{true}$ and by the definition of $\kappa(\mathrm{cut}(C))$ that $\kappa(\mathrm{cut}(C))[\vartheta_\theta] \equiv \mathit{true}$, i.e., $\vartheta_\theta \in \Xi(\mathrm{cut}(C))$. □

A.2 Examples of adequate orders

We show that the adequate order used in [14], as well as the orders $\prec_E$ and $\prec_F$ treated in [10], when lifted to the symbolic unfolding, are still adequate orders. In particular we show that $\prec_F$ is a total adequate order on the symbolic unfolding, limiting the size of the later constructed finite prefix. The definition of these orders does not change, so we take most of the following notation directly from [10].

The orders $\prec_M$ and $\prec_E$. The order $\prec_M$ used in [14] is defined by $C_1 \prec_M C_2 :\Leftrightarrow |C_1| < |C_2|$. It is trivial to see that $\prec_M$ satisfies i) and ii) from Def. 5. Since $\varphi^2_{1,D}$ is a injective, we have $|\varphi^2_{1,D}(D)| = |D|$, which yields iii).

For a high-level Petri net N, let $\ll$ be an arbitrary total order on the transitions of N. Given a set E' of events in the unfolding of N, let $\mathbf{p}(E')$ be that sequence of transitions which is ordered according to $\ll$, and contains each transition t as often as there are events in E' with label t. We say $\mathbf{p}(E_1) \ll \mathbf{p}(E_2)$ if $\mathbf{p}(E_1)$ is lexicographically smaller than $\mathbf{p}(E_2)$ with respect to the order $\ll$.

The order $\prec_E$ is then defined as follows: let C_1, C_2 be two configurations of the symbolic unfoldings of a high-level Petri net. $C_1 \prec_E C_2$ holds if either $|C_1| < |C_2|$, or $|C_1| = |C_2|$ and $\mathbf{p}(C_1) \ll \mathbf{p}(C_2)$. The proof that $\prec_E$ is an adequate order works exactly as in [10]:

It is easy to show that $\prec_E$ is a well-founded partial order implied by inclusion. We now show that $\prec_E$ is preserved by finite extensions. As already mentioned above, $|D| = |\varphi^2_{1,D}(D)|$. Additionally, we have $\mathbf{p}(D) = \mathbf{p}(\varphi^2_{1,D}(D))$, since $\varphi^2_{1,D}$ preserves the labeling of events.

Assume $C_1 \prec_E C_2$. If $|C_1| < |C_2|$, then $|C_1 \oplus D| < |C_2 \oplus \varphi^2_{1,D}(D)|$. If $|C_1| = |C_2|$ and $\mathbf{p}(C_1) \ll \mathbf{p}(C_2)$, then $|C_1 \oplus D| = |C_2 \oplus \varphi^2_{1,D}(D)|$ and, by the properties of the lexicographic order, $\mathbf{p}(C_1 \oplus D) \ll \mathbf{p}(C_2 \oplus \varphi^2_{1,D}(D))$.

The Total Adequate Order $\prec_F$. The *Foata normal form* FC of a configuration C is obtained by starting with FC empty, and iteratively deleting the set $Min(C)$ from C and appending it to FC, until C is empty.

Given two configurations C_1, C_2, we can compare their Foata normal forms $FC_1 = C_{11} \dots C_{1n_1}$ and $FC_2 = C_{21} \dots C_{2n_2}$ with respect to the order $\ll$ by saying $FC_1 \ll FC_2$ if there exists $i \leq i \leq n_1$ such that $\mathbf{p}(C_{1j}) = \mathbf{p}(C_{2j})$ for every $1 \leq j < i$, and $\mathbf{p}(C_{1i}) \ll \mathbf{p}(C_{2i})$.

Definition 11 (Order $\prec_F$). *let C_1 and C_2 be two configurations of the symbolic unfolding of a high-level Petri net. $C_1 \prec_F C_2$ holds if*

- $|C_1| < |C_2|$, *or*
- $|C_1| = |C_2|$ *and* $\mathbf{p}(C_1) \ll \mathbf{p}(C_2)$, *or*
- $\mathbf{p}(C_1) = \mathbf{p}(C_2)$ *and* $FC_1 \ll FC_2$.

We prove that $\prec_F$ is a total adequate order. In the proof, (a) – (c) are taken directly from [10], with very small adaptations due to the high-level formalism. While the ideas from (d) also come directly from [10], we have work with the monomorphism $\varphi^2_{1,D}$ instead of the isomorphism I^2_1, and the new definition of adequate order. This is where the only deviation from [10] happens.

Let $\beta = \langle O, h \rangle$ be the symbolic unfolding of $N = \langle \mathcal{N}, \mathcal{M}_0 \rangle$.

(a) $\prec_F$ is a well-founded partial order.
This follows immediately from the fact that $\prec_E$ is a well-founded partial order as is the lexicographic order on transition sequences of some fixed length.

(b) $C_1 \subset C_2$ implies $C_1 \prec_F C_2$.
This is obvious, since $C_1 \subset C_2$ implies $|C_1| < |C_2|$.

(c) $\prec_F$ is total.
Assume that C_1 and C_2 are two incomparable configurations under $\prec_F$, i.e., $|C_1| = |C_2|$, $\mathbf{p}(C_1) = \mathbf{p}(C_2)$, and $\mathbf{p}(FC_1) = \mathbf{p}(FC_2)$. We prove $C_1 = C_2$ by induction on the common size $k = |C_1| = |C_2|$.
The base case $k = 0$ gives $C_1 = C_2 = \emptyset$, so assume $k > 0$.
We first prove $Min(C_1) = Min(C_2)$. Aiming a contradiction, assume w.l.o.g. that $e_1 \in Min(C_1) \setminus Min(C_2)$. Since $\mathbf{p}(Min(C_1)) = \mathbf{p}(Min(C_2))$, $Min(C_2)$ contains an event e_2 s.t. $h(e_1) = h(e_2)$. Since $\rightarrow Min(C_1)$ and $\rightarrow Min(C_2)$ are subsets of B_0, and all conditions of B_0 carry different labels, we have $\rightarrow e_1 = \rightarrow e_2$, and thus, $pre(e_1) = pre(e_2)$. This contradicts the definition of symbolic branching processes.

Since $Min(C_1) = Min(C_2)$, both $C_1 \setminus Min(C_1)$ and $C_2 \setminus Min(C_1)$ are configurations of the branching process $\Uparrow Min(C_1)$ of $\langle \mathcal{N}, \mathcal{M}(Min(C_1))\rangle$, and they are incomparable under $\prec_F$ by construction. Since the common size of $C_1 \setminus Min(C_1)$ and $C_2 \setminus Min(C_1)$ is strictly smaller than k, we can apply the induction hypothesis and conclude $C_1 = C_2$.

(d) $\prec_F$ is preserved by finite extensions.
Take two finite configurations C_1 and C_2, let D be a finite suffix of C_1, and let $M \in \mathcal{M}(C_1) \cap \mathcal{M}(C_2)$ such that $C_1[\![M]\!\rangle D$. We have to show that $C_1 \prec C_2$ implies $C_1 \oplus D \prec C_2 \oplus \varphi^2_{1,D}(D)$.
First, notice that we can assume $D = \{e\}$: For $e \in Min(D)$ we have from $C_1[\![M]\!\rangle D$ that $\exists \theta \in \Theta(C_1 \oplus D) : \mathrm{mark}(C_1.\theta|_{Var_{C_1 \cup \{\bot\}}}) = M$. Thus, for M' s.t. $M[h(e).\sigma\rangle M'$ with $\sigma = \theta \circ [v \mapsto v_e]_{v \in Var(e)}$, we have that $M' \in \mathcal{M}(C_1 \oplus \{e\}) \cap \mathcal{M}(C_2 \oplus \{\varphi^2_{1,D}(e)\})$ and $(C_1 \oplus \{e\})[\![M']\!\rangle (D \setminus \{e\})$.
Second, the cases $|C_1| < |C_2|$ and $C_1 \prec_E C_2$ in (i), (and the respective cases $|C_2| < |C_1|$ and $C_2 \prec_E C_1$ in (ii)) are easy (shown above). Hence, assume $|C_1| = |C_2|$ and $\mathbf{p}(C_1) = \mathbf{p}(C_2)$.
Third, we show that under these two assumptions e is a minimal event of $C_1' := C_1 \cup \{e\}$ if and only if $\varphi^2_{1,D}(e)$ is a minimal event of $C_2' := C_2 \cup \{\varphi^2_{1,D}(e)\}$. Let e be minimal in C_1', i.e., the transition $h(e)$ can be fired in a mode in one initial marking. Let $p \in {\to}h(e)$; then no condition in $\to C \cup C\to$ is labeled p, since these conditions would be concurrent to the p-labeled condition in $\to e$, contradicting that $\langle \mathcal{N}, \mathcal{M}_0\rangle$ is safe. Thus, C_1 contains no event e' with $p \in {\to}h(e')$, and the same holds for C_2, since $\mathbf{p}(C_1) = \mathbf{p}(C_2)$. Therefore, the conditions in $\mathrm{cut}(C_2)$ with label in ${\to}h(e)$ are minimal conditions of β, and $\varphi^2_{1,D}(e) = e$ is minimal in C_2'. The reverse implication holds analogously, since about C_1 and C_2 we have only used the hypothesis $\mathbf{p}(C_1) = \mathbf{p}(C_2)$.
With this knowledge, we now show the implication. Assume $C_1 \prec_F C_2$. We show $C_1' \prec_F C_2'$.
If $Min(C_1) \prec_E Min(C_2)$, then we now see $Min(C_1') \prec_E Min(C_2')$, hence $\mathbf{p}(FC_1') \ll \mathbf{p}(FC_2')$ and so we are done. If $\mathbf{p}(Min(C_1)) = \mathbf{p}(Min(C_2))$ and $e \in Min(C_1')$, then

$$C_1' \setminus Min(C_1') = C_1 \setminus Min(C_1) \prec_F C_2 \setminus Min(C_2) = C_2' \setminus Min(C_2'),$$

hence $C_1' \prec_F C_2'$. Finally, if $\mathbf{p}(Min(C_1)) = \mathbf{p}(Min(C_2))$ and $e \notin Min(C_1')$, we again argue that $Min(C_1) = Min(C_2)$ and that, hence, $C \setminus Min(C_1)$ and $C_2 \setminus Min(C_1)$ are configurations of the branching process $\Uparrow Min(C_1)$ of $\langle \mathcal{N}, \mathcal{M}(Min(C_1))\rangle$. With an inductive argument we get $C_1' \setminus Min(C_1') \prec_F C_2' \setminus Min(C_2')$ and are also done in this case.