Separators in Continuous Petri Nets[⋆]

Michael Blondin[1] and Javier Esparza[2]

[1] Université de Sherbrooke, Sherbrooke, Canada
michael.blondin@usherbrooke.ca
[2] Technical University of Munich, Munich, Germany
esparza@in.tum.de

Abstract. Leroux has proved that unreachability in Petri nets can be witnessed by a Presburger separator, i.e. if a marking $\boldsymbol{m}_{\text{src}}$ cannot reach a marking $\boldsymbol{m}_{\text{tgt}}$, then there is a formula φ of Presburger arithmetic such that: $\varphi(\boldsymbol{m}_{\text{src}})$ holds; φ is forward invariant, i.e., $\varphi(\boldsymbol{m})$ and $\boldsymbol{m} \to \boldsymbol{m}'$ imply $\varphi(\boldsymbol{m}')$; and $\neg\varphi(\boldsymbol{m}_{\text{tgt}})$ holds. While these separators could be used as explanations and as formal certificates of unreachability, this has not yet been the case due to their (super-)Ackermannian worst-case size and the (super-)exponential complexity of checking that a formula is a separator. We show that, in continuous Petri nets, these two problems can be overcome. We introduce locally closed separators, and prove that: (a) unreachability can be witnessed by a locally closed separator computable in polynomial time; (b) checking whether a formula is a locally closed separator is in NC (so, simpler than unreachablity, which is P-complete).

Keywords: Petri net · continuous reachability · separators · certificates.

1 Introduction

Petri nets form a widespread formalism of concurrency with several applications ranging from the verification of concurrent programs to the analysis of chemical systems. The reachability problem — which asks whether a a marking $\boldsymbol{m}_{\text{src}}$ can reach another marking $\boldsymbol{m}_{\text{tgt}}$ — is fundamental as a plethora of problems, such as verifying safety properties, reduce to it (e.g. [13,11,2]).

Leroux has shown that unreachability in Petri nets can be witnessed by a Presburger *separator*, i.e., if a marking $\boldsymbol{m}_{\text{src}}$ cannot reach a marking $\boldsymbol{m}_{\text{tgt}}$, then there exists a formula φ of Presburger arithmetic such that: $\varphi(\boldsymbol{m}_{\text{src}})$ holds; φ is forward invariant, i.e., $\varphi(\boldsymbol{m})$ and $\boldsymbol{m} \to \boldsymbol{m}'$ imply $\varphi(\boldsymbol{m}')$; and $\varphi(\boldsymbol{m}_{\text{tgt}})$ does not hold [14]. Intuitively, φ "separates" $\boldsymbol{m}_{\text{tgt}}$ from the set of markings reachable from $\boldsymbol{m}_{\text{src}}$. Leroux's result leads to a very simple algorithm to decide the Petri net reachability problem, consisting of two semi-algorithms; the first one explores the markings reachable from $\boldsymbol{m}_{\text{src}}$, and halts if and when it hits $\boldsymbol{m}_{\text{tgt}}$, while the

[⋆] M. Blondin was supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (NSERC), and by the Fonds de recherche du Québec – Nature et technologies (FRQNT). J. Esparza was supported by an ERC Advanced Grant (787367: PaVeS).

© The Author(s) 2022
P. Bouyer and L. Schröder (Eds.): FoSSaCS 2022, LNCS 13242, pp. 81–100, 2022.
https://doi.org/10.1007/978-3-030-99253-8_5

second enumerates formulas from Presburger arithmetic, and halts if and when it hits a separator.

Separators can be used as *explanations* and as formal *certificates*. Verifying a safety property can be reduced to proving that a target marking (or set of markings) is not reachable from a source marking, and a separator is an invariant of the system that *explains* why the property holds. Further, if a reachability tool produces separators, then the user can check that the properties of a separator indeed hold, and so trust the result even if they do not trust the tool (e.g., because it has not been verified, or is executed on a remote faster machine). Yet, in order to be useful as explanations and certificates, separators have to satisfy two requirements: (1) they should not be too large, and (2) checking that a formula is a separator should have low complexity, and in particular lower complexity than deciding reachability. This does not hold, at least in the worst-case, for the separators of [14]: In the worst case, the separator has super-Ackermannian size in the Petri net size (a consequence of the fact that the reachability problem is Ackermann-complete [16,15,7]) and the complexity of the check is super-exponential.

In this paper, we show that, unlike the above, *continuous* Petri nets do have separators satisfying properties (1) and (2). Continuous Petri nets are a relaxation of the standard Petri net model, called *discrete* in the following, in which transitions are allowed to fire "fluidly": instead of firing once, consuming i_p tokens from each input place p and adding o_q tokens to each output place q, a transition can fire α times for any nonnegative real number α, consuming and adding $\alpha \cdot i_p$ and $\alpha \cdot o_q$ tokens, respectively. Continuous Petri nets are interesting in their own right [8], and moreover as an overapproximation of the discrete model. In particular, if $\boldsymbol{m}_{\text{tgt}}$ is not reachable from $\boldsymbol{m}_{\text{src}}$ under the continuous semantics, then it is also not under the discrete one. As reachability in continuous Petri nets is P-complete [12], and so drastically more tractable than discrete reachability, this approximation is used in many tools for the verification of discrete Petri nets, VAS, or multiset rewriting systems (e.g. [5,4,10]).

It is easy to see that unreachability in continuous Petri nets can be witnessed by separators expressible in linear arithmetic (the first-order theory of the reals with addition and order). Indeed, Blondin et al. show in [5] that the continuous reachability relation is expressible by an existential formula $\mathit{reach}(\boldsymbol{m}, \boldsymbol{m}')$ of linear arithmetic, from which we can obtain a separator for any pair of unreachable markings. To wit, for all markings $\boldsymbol{m}_{\text{src}}$ and $\boldsymbol{m}_{\text{tgt}}$, if $\boldsymbol{m}_{\text{tgt}}$ is not reachable from $\boldsymbol{m}_{\text{src}}$, then the formula $\mathit{sep}_{\boldsymbol{m}_{\text{src}}}(\boldsymbol{m}) := \neg \mathit{reach}(\boldsymbol{m}_{\text{src}}, \boldsymbol{m})$ is a separator. Further, $\mathit{reach}(\boldsymbol{m}, \boldsymbol{m}')$ has only linear size. However, these separators do not satisfy property (2) unless P = NP. Indeed, while the reachability problem for continuous Petri nets is P-complete [12], checking if a formula of linear arithmetic is a separator is coNP-hard, even for quantifier-free formulas in disjunctive normal form, a very small fragment. So, the separators arising from [5] cannot be directly used as certificates.

In this paper, we overcome this problem. We identify a class of *locally closed separators*, satisfying the following properties: unreachability can always be witnessed by locally closed separators; locally closed separators can be constructed in polynomial time; and checking whether a formula is a locally closed separator is computationally easier than deciding unreachability. Let us examine the last claim in more detail. While the reachability problem for continuous Petri nets is decidable in polynomial time, it is still time consuming for larger models, which can have tens of thousands of nodes. Indeed, for a Petri net with n places and m transitions, the algorithm of [12] requires to solve $\mathcal{O}(m^2)$ linear programming problems in n variables, each of them with up to m constraints. Moreover, since the problem is P-complete, it is unlikely that a parallel computer can significantly improve performance. We prove that, on the contrary, checking if a formula is a locally closed separator is in NC rather than P-complete, and so efficiently parallelizable. Further, the checking algorithm only requires to solve linear programming problems in *a single* variable.

The paper is organized as follows. Section 2 introduces terminology, and defines separators (actually, a slightly different notion called bi-separators). Section 3 recalls the characterization of the reachability relation given by Fraca and Haddad in [12], and derives a characterization of *un*reachability suitable for finding bi-separators. Section 4 shows that checking the separators derivable from [5] is coNP-hard, and introduces locally closed bi-separators. Sections 5 and 6 show that locally closed bi-separators satisfy the aforementioned properties (1) and (2). Finally, Section 7 shows that all our results can be extended to separators that separate two sets of markings instead of singletons.

2 Preliminaries

Numbers, vectors and relations. We write $\mathbb{N}$, $\mathbb{R}$ and $\mathbb{R}_+$ to denote the naturals (including 0), reals, and non-negative reals (including 0). Let S be a finite set. We write $\boldsymbol{e}_s$ to denote the unit vector $\boldsymbol{e}_s \in \mathbb{R}^S$ such that $\boldsymbol{e}_s(s) = 1$ and $\boldsymbol{e}_s(t) = 0$ for all $s, t \in S$ such that $t \neq s$. Given $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^S$, we write $\boldsymbol{x} \sim_S \boldsymbol{y}$ to indicate that $\boldsymbol{x}(s) \sim \boldsymbol{y}(s)$ for all $s \in S$, where $\sim$ is a total order such as $\leq$. We define the *support* of a vector $\boldsymbol{x} \in \mathbb{R}^S$ as $\operatorname{supp}(\boldsymbol{x}) \coloneqq \{s \in S : \boldsymbol{x}(s) > 0\}$. We write $\boldsymbol{x}(S) \coloneqq \sum_{s \in S} \boldsymbol{x}(s)$. The *transpose* of a binary relation $\mathcal{R}$ is $\mathcal{R}^\intercal \coloneqq \{(y, x) : (x, y) \in \mathcal{R}\}$.

Petri nets. A *Petri net*[3] is a tuple $\mathcal{N} = (P, T, F)$ where P and T are disjoint finite sets, whose elements are respectively called *places* and *transitions*, and where $F = (\mathbf{F}_-, \mathbf{F}_+)$ with $\mathbf{F}_-, \mathbf{F}_+ \colon P \times T \to \mathbb{N}$. For every $t \in T$, vectors $\Delta_t^-, \Delta_t^+ \in \mathbb{N}^P$ are respectively defined as the column of $\mathbf{F}_-$ and $\mathbf{F}_+$ associated to t, i.e. $\Delta_t^- \coloneqq \mathbf{F}_- \cdot \boldsymbol{e}_t$ and $\Delta_t^+ \coloneqq \mathbf{F}_+ \cdot \boldsymbol{e}_t$. A *marking* is a vector $\boldsymbol{m} \in \mathbb{R}_+^P$. We say that transition t is *α-enabled* if $\boldsymbol{m} \geq \alpha\Delta_t^-$ holds. If this is the case, then t can be *α-fired* from $\boldsymbol{m}$, which leads to marking $\boldsymbol{m}' \coloneqq \boldsymbol{m} - \alpha\Delta_t^- + \alpha\Delta_t^+$, which we denote $\boldsymbol{m} \xrightarrow{\alpha t} \boldsymbol{m}'$. A transition is *enabled* if it is α-enabled for some real number

[3] In this work, "Petri nets" stands for "continuous Petri nets". In other words, we will consider standard Petri nets, but equipped with a *continuous* reachability relation. We will work over the reals, but note that it is known that working over the rationals is equivalent. For decidability issues, we will assume input numbers to be rationals.

$\alpha > 0$. We define $\mathbf{F} \coloneqq \mathbf{F}_+ - \mathbf{F}_-$ and $\mathit{\Delta}_t \coloneqq \mathbf{F} \cdot \boldsymbol{e}_t$. In particular, $\boldsymbol{m} \xrightarrow{\alpha t} \boldsymbol{m}'$ implies $\boldsymbol{m}' = \boldsymbol{m} + \alpha\mathit{\Delta}_t$. For example, for the Petri net of Figure 1:

$$\{p_1 \mapsto 2, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 0\} \xrightarrow{(1/2)t_1} \{p_1 \mapsto 3/2, p_2 \mapsto 1/2, p_3 \mapsto 0, p_4 \mapsto 0\}.$$

Moreover, w.r.t. to orderings $p_1 < \cdots < p_4$ (rows) and $t_1 < \cdots < t_4$ (columns):

$$\mathbf{F}_- = \begin{bmatrix} 1&2&2&0 \\ 0&0&1&0 \\ 0&0&0&1 \\ 0&1&0&0 \end{bmatrix}, \ \mathbf{F}_+ = \begin{bmatrix} 0&0&1&0 \\ 1&0&0&0 \\ 0&1&1&0 \\ 0&1&0&1 \end{bmatrix} \ \text{and} \ \mathbf{F} = \begin{bmatrix} -1&-2&-1&0 \\ 1&0&-1&0 \\ 0&1&1&-1 \\ 0&0&0&1 \end{bmatrix}.$$

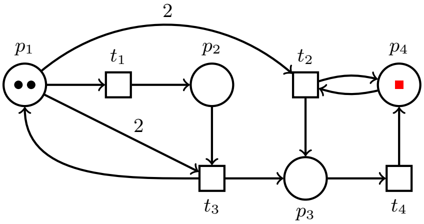

Fig. 1. A Petri net and two markings $\boldsymbol{m}_{\text{src}} = \{p_1 \mapsto 2, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 0\}$ (black circles) and $\boldsymbol{m}_{\text{tgt}} = \{p_1 \mapsto 0, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 1\}$ (colored squares).

A sequence $\sigma = \alpha_1 t_1 \cdots \alpha_n t_n$ is a *firing sequence* from $\boldsymbol{m}_{\text{src}}$ to $\boldsymbol{m}_{\text{tgt}}$ if there are markings $\boldsymbol{m}_0, \ldots, \boldsymbol{m}_n$ satisfying $\boldsymbol{m}_{\text{src}} = \boldsymbol{m}_0 \xrightarrow{\alpha_1 t_1} \boldsymbol{m}_1 \cdots \xrightarrow{\alpha_n t_n} \boldsymbol{m}_n = \boldsymbol{m}_{\text{tgt}}$. We write $\boldsymbol{m}_0 \xrightarrow{\sigma} \boldsymbol{m}_n$. We say that $\boldsymbol{m}_{\text{src}}$ *enables* σ, and that $\boldsymbol{m}_{\text{tgt}}$ enables σ backwards, or *backward-enables* σ. The *support* of σ is the set $\{t_1, \ldots, t_n\}$. For example, for the Petri net of Figure 1, we have $\boldsymbol{m}_{\text{src}} \xrightarrow{\sigma} \boldsymbol{m}_{\text{tgt}}$ where

$$\begin{aligned} \boldsymbol{m}_{\text{src}} &= \{p_1 \mapsto 2, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 0\}, \\ \boldsymbol{m}_{\text{tgt}} &= \{p_1 \mapsto 0, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 1\}, \\ \sigma &= (1/2)t_1\ (1/2)t_3\ (1/2)t_4\ (1/2)t_2\ (1/2)t_4. \end{aligned}$$

Let $U \subseteq T$. We write $\boldsymbol{m} \rightarrow^U \boldsymbol{m}'$ to denote that $\boldsymbol{m} \xrightarrow{\alpha t} \boldsymbol{m}'$ for some $\alpha > 0$ and $t \in U$, and $\rightarrow^{U^*}$ for the transitive and reflexive closure of $\rightarrow^U$. We simply write $\rightarrow$ and $\rightarrow^*$ when $U = T$. The Petri net $\mathcal{N}_U$ is obtained by removing transitions $T \setminus U$ from $\mathcal{N}$. In particular, $\boldsymbol{m} \rightarrow^{U^*} \boldsymbol{m}'$ holds in $\mathcal{N}$ iff $\boldsymbol{m} \rightarrow^* \boldsymbol{m}'$ holds in $\mathcal{N}_U$.

The *transpose* of $\mathcal{N} = (P, T, (\mathbf{F}_-, \mathbf{F}_+))$ is $\mathcal{N}^\intercal \coloneqq (P, T, (\mathbf{F}_+, \mathbf{F}_-))$. We have $\boldsymbol{m}_{\text{src}} \xrightarrow{\sigma} \boldsymbol{m}_{\text{tgt}}$ in $\mathcal{N}$ iff $\boldsymbol{m}_{\text{tgt}} \xrightarrow{\tau} \boldsymbol{m}_{\text{src}}$ in $\mathcal{N}^\intercal$, where τ is the reverse of σ. For $U \subseteq T$, we write $U^\intercal$ to denote U in the context of $\mathcal{N}^\intercal$. This way, when we write, e.g. $\rightarrow^U$ and $\rightarrow^{U^\intercal}$, it is clear that we respectively refer to $\mathcal{N}$ and $\mathcal{N}^\intercal$.

Linear arithmetic and Farkas' lemma. An *atomic proposition* is a linear inequality of the form $\boldsymbol{ax} \leq b$ or $\boldsymbol{ax} < b$, where b and the components of $\boldsymbol{a}$ are over

$\mathbb{R}$. Such a proposition is *homogeneous* if $b = 0$. A *linear formula* is a first-order formula over atomic propositions with variables ranging over $\mathbb{R}_+$ (the classical definition uses $\mathbb{R}$, but in our context variables will encode markings.) The *solutions* of a linear formula φ, denoted $[\![\varphi]\!]$, are the assignments to the free variables of φ that satisfy φ. A linear formula is *homogeneous* if all of its atomic propositions are homogeneous. For every formula $\varphi(\boldsymbol{x}, \boldsymbol{y})$ where $\boldsymbol{x}$ and $\boldsymbol{y}$ have the same arity, we write φ^T to denote the formula that syntactically swaps $\boldsymbol{x}$ and $\boldsymbol{y}$, so that $[\![\varphi^\mathsf{T}]\!] = [\![\varphi]\!]^\mathsf{T}$. Throughout the paper, we will use Farkas' lemma, a fundamental result of linear arithmetic that rephrases the absence of solution to a system into the existence of one for another system:

Lemma 1 (Farkas' lemma). *Let* $\mathbf{A} \in \mathbb{R}^{m \times n}$ *and* $\boldsymbol{b} \in \mathbb{R}^m$. *The formula* $\mathbf{A}\boldsymbol{x} \leq \boldsymbol{b}$ *has no solution iff* $\mathbf{A}^\mathsf{T}\boldsymbol{y} = \mathbf{0} \wedge \boldsymbol{b}^\mathsf{T}\boldsymbol{y} < 0 \wedge \boldsymbol{y} \geq \mathbf{0}$ *has a solution.*

2.1 Separators and bi-separators

Let us fix a Petri net $\mathcal{N} = (P, T, F)$ and two markings $\boldsymbol{m}_\text{src}, \boldsymbol{m}_\text{tgt} \in \mathbb{R}_+^P$.

Definition 1. *A* separator *for* $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$ *is a linear formula* φ *over* $\mathbb{R}_+^P$ *such that: (1)* $\boldsymbol{m}_{src} \in [\![\varphi]\!]$*; (2)* φ *is* forward invariant*, i.e.,* $\boldsymbol{m} \in [\![\varphi]\!]$ *and* $\boldsymbol{m} \to \boldsymbol{m}'$ *implies* $\boldsymbol{m}' \in [\![\varphi]\!]$*; and (3)* $\boldsymbol{m}_{tgt} \notin [\![\varphi]\!]$.

It follows immediately from the definition that if there exists a separator φ for $(\boldsymbol{m}_\text{src}, \boldsymbol{m}_\text{tgt})$, then $\boldsymbol{m}_\text{src} \not\to^* \boldsymbol{m}_\text{tgt}$. Thus, in order to show that $\boldsymbol{m}_\text{src} \not\to^* \boldsymbol{m}_\text{tgt}$ in $\mathcal{N}$, we can either give a separator for $(\boldsymbol{m}_\text{src}, \boldsymbol{m}_\text{tgt})$ w.r.t. $\mathcal{N}$, or a separator for $(\boldsymbol{m}_\text{tgt}, \boldsymbol{m}_\text{src})$ w.r.t. $\mathcal{N}^\mathsf{T}$. Let us call them *forward* and *backward* separators. Loosely speaking, a forward separator shows that $\boldsymbol{m}_\text{tgt}$ is not among the markings reachable from $\boldsymbol{m}_\text{src}$, and a backward separator shows that $\boldsymbol{m}_\text{src}$ is not among the markings backward-reachable from $\boldsymbol{m}_\text{tgt}$. Bi-separators are formulas from which we can easily obtain forward and backward separators. The symmetry w.r.t. forward and backward reachability make them easier to handle.

Definition 2. *A linear formula* φ *over* $(\mathbb{R}_+^P)^2$ *is* forward invariant *if* $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi]\!]$ *and* $\boldsymbol{m}' \to \boldsymbol{m}''$ *imply* $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\varphi]\!]$*;* backward invariant *if* $(\boldsymbol{m}', \boldsymbol{m}'') \in [\![\varphi]\!]$ *and* $\boldsymbol{m} \to \boldsymbol{m}'$ *imply* $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\varphi]\!]$*; and* bi-invariant *if it is forward and backward invariant. A* bi-separator *for* $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$ *is a bi-invariant linear formula* φ *s.t.* $(\boldsymbol{m}_{src}, \boldsymbol{m}_{src}) \in [\![\varphi]\!]$, $(\boldsymbol{m}_{tgt}, \boldsymbol{m}_{tgt}) \in [\![\varphi]\!]$ *and* $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt}) \notin [\![\varphi]\!]$.

The following proposition shows how to obtain separators from bi-separators.

Proposition 1. *Let* φ *be a bi-separator for* $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$. *The following holds:*

- $\psi(\boldsymbol{m}) := \varphi(\boldsymbol{m}_{src}, \boldsymbol{m})$ *is a separator for* $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$ *in* $\mathcal{N}$*;*
- $\psi'(\boldsymbol{m}) := \varphi(\boldsymbol{m}, \boldsymbol{m}_{tgt})$ *is a separator for* $(\boldsymbol{m}_{tgt}, \boldsymbol{m}_{src})$ *in* $\mathcal{N}^\mathsf{T}$.

Proof. It suffices to prove the first statement, the second is symmetric.

It is the case that $\boldsymbol{m}_\text{src} \in [\![\psi]\!]$ and $\boldsymbol{m}_\text{tgt} \notin [\![\psi]\!]$ as $(\boldsymbol{m}_\text{src}, \boldsymbol{m}_\text{src}) \in [\![\varphi]\!]$ and $(\boldsymbol{m}_\text{src}, \boldsymbol{m}_\text{tgt}) \notin [\![\varphi]\!]$. It remains to show that ψ is forward invariant. Let $\boldsymbol{m} \in [\![\psi]\!]$ and $\boldsymbol{m} \xrightarrow{\alpha t} \boldsymbol{m}'$. Since $(\boldsymbol{m}_\text{src}, \boldsymbol{m}) \in [\![\varphi]\!]$ and φ is forward invariant, it is the case that $(\boldsymbol{m}_\text{src}, \boldsymbol{m}') \in [\![\varphi]\!]$. Hence, $\boldsymbol{m}' \in [\![\psi]\!]$ as desired. □

3 A characterization of unreachability

In [12], Fraca and Haddad gave the following characterization of the reachability relation in continuous Petri nets:

Theorem 1 ([12]). *Let $\mathcal{N} = (P, T, F)$ be a Petri net, let $U \subseteq T$, and let $\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt} \in \mathbb{R}_+^P$. It is the case that $\boldsymbol{m}_{src} \rightarrow^{U^*} \boldsymbol{m}_{tgt}$ iff there exists $S \subseteq U$ such that the following conditions hold:*

1. *some vector $\boldsymbol{x} \in \mathbb{R}_+^T$ with support S satisfies $\boldsymbol{m}_{src} + \mathbf{F}\boldsymbol{x} = \boldsymbol{m}_{tgt}$,*
2. *some firing sequence σ with support S is enabled at $\boldsymbol{m}_{src}$, and*
3. *some firing sequence τ with support S is backward-enabled at $\boldsymbol{m}_{tgt}$.*

Furthermore, these conditions can be checked in polynomial time.

Theorem 1 has the following form, where P_1, P_2 and P_3 stand for the conditions of 1., 2., and 3.:

$$\boldsymbol{m}_{\text{src}} \rightarrow^{U^*} \boldsymbol{m}_{\text{tgt}} \iff \exists S \subseteq U : (\exists \boldsymbol{x} \colon P_1(S, \boldsymbol{x})) \wedge (\exists \sigma \colon P_2(S, \sigma) \wedge (\exists \tau \colon P_3(S, \tau)).$$

Therefore, $\boldsymbol{m}_{\text{src}} \not\rightarrow^{U^*} \boldsymbol{m}_{\text{tgt}}$ holds iff

$$\forall S \subseteq U : (\forall \boldsymbol{x} \colon \neg P_1(S, \boldsymbol{x})) \vee (\forall \sigma \colon \neg P_2(S, \sigma)) \vee (\forall \tau \colon \neg P_3(S, \tau)).$$

To obtain a witness of unreachability for a given $S \subseteq U$, we replace each universally quantified disjunct by an existentially quantified equivalent one. For conditions 2. and 3., the solution (implicitly given in [12]) is formulated in Proposition 2. Given a set of places X, let ${}^\bullet X$ (resp. $X^\bullet$) be the set of transitions t such that $\mathbf{F}_+(p, t) > 0$ (resp. $\mathbf{F}_-(p, t) > 0$) for some $p \in X$. A *siphon* of $\mathcal{N}$ is a subset Q of places such that ${}^\bullet Q \subseteq Q^\bullet$. A *trap* is a subset R of places such that $R^\bullet \subseteq {}^\bullet R$. Informally, empty siphons remain empty, and marked traps remain marked. Formally, if $\boldsymbol{m} \rightarrow \boldsymbol{m}'$, then $\boldsymbol{m}(Q) = 0$ implies $\boldsymbol{m}'(Q) = 0$, and $\boldsymbol{m}(R) > 0$ implies $\boldsymbol{m}'(R) > 0$. We have:

Proposition 2 ([12]). *Let $\mathcal{N} = (P, T, F)$ be a Petri net, let $S \subseteq T$, and let $\boldsymbol{m} \in \mathbb{R}_+^P$. The following statements hold:*

- *No firing sequence with support S is enabled at $\boldsymbol{m}$ iff there exists a siphon Q of $\mathcal{N}_S$ such that $Q^\bullet \neq \emptyset$ satisfies $\boldsymbol{m}(Q) = 0$;*
- *No firing sequence with support S is backward-enabled at $\boldsymbol{m}$ iff there exists a trap R of $\mathcal{N}_S$ such that ${}^\bullet R \neq \emptyset$ satisfies $\boldsymbol{m}(R) = 0$.*

So the universal statements "no firing sequence ... is enabled/backward-enabled ..." are replaced by existential statements "there exists a siphon/trap ...". The if-direction of the proposition is easy to prove. A siphon Q of $\mathcal{N}_S$ satisfies $Q^\bullet \subseteq S$. Since Q is empty at $\boldsymbol{m}$, if we only fire transitions from S then Q remains empty, and so no transition of $Q^\bullet$ ever becomes enabled. So transitions of $Q^\bullet$ can only fire after transitions that do not belong to S have fired first. But no such firing sequence has support S, and we are done. The case of traps is analogous. For the only-if direction we refer the reader to [12].

For condition 1. of Theorem 1, we obtain a solution in terms of *exclusion functions*.

Definition 3. *Let $\mathcal{N} = (P, T, F)$ be a Petri net, let $\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt} \in \mathbb{R}_+^P$ and let $S \subseteq S' \subseteq T$. An* exclusion function for (S, S') *is a function $f \colon \mathbb{R}_+^P \to \mathbb{R}$ s.t.*

1. *$\boldsymbol{m} \xrightarrow{s} \boldsymbol{m}'$ implies $f(\boldsymbol{m}) \leq f(\boldsymbol{m}')$ for all $s \in S'$; and*
2. *either $f(\boldsymbol{m}_{src}) > f(\boldsymbol{m}_{tgt})$, or $f(\boldsymbol{m}_{src}) = f(\boldsymbol{m}_{tgt})$ and there exists $s \in S$ such that $\boldsymbol{m} \xrightarrow{s} \boldsymbol{m}'$ implies $f(\boldsymbol{m}) < f(\boldsymbol{m}')$.*

An exclusion function for S *is an exclusion function for (S, S).*

An exclusion function for S excludes the existence of a firing sequence from $\boldsymbol{m}_{\text{src}}$ to $\boldsymbol{m}_{\text{tgt}}$ with support S, i.e., witnesses that condition 1 of Theorem 1 fails. To see why, call $f(\boldsymbol{m})$ the *value* of m. By definition of f, either $\boldsymbol{m}_{\text{tgt}}$ has lower value than $\boldsymbol{m}_{\text{src}}$ but no transition of S decreases it, or $\boldsymbol{m}_{\text{src}}$ and $\boldsymbol{m}_{\text{tgt}}$ have the same value but no transition of S decreases it, and at least one increases it. So it is impossible to reach $\boldsymbol{m}_{\text{tgt}}$ from $\boldsymbol{m}_{\text{src}}$ by firing *all* and *only* the transitions of S. Let us apply exclusion functions and Proposition 2 to an example.

Example 1. Consider the Petri net of Figure 1, but with $\boldsymbol{m}_{\text{tgt}} := \{p_1 \mapsto 0, p_2 \mapsto 0, p_3 \mapsto 1, p_4 \mapsto 0\}$ as target. We prove $\boldsymbol{m}_{\text{src}} \not\rightarrow^* \boldsymbol{m}_{\text{tgt}}$. For the sake of contradiction, assume $\boldsymbol{m}_{\text{src}} \rightarrow^{U^*} \boldsymbol{m}_{\text{tgt}}$ for some $U \subseteq T$. We proceed in several steps:

- *Claim:* $t_4 \notin U$. The function $f(\boldsymbol{m}) := \boldsymbol{m}(p_4)$ is an exclusion function for T. Indeed, since no transition decreases the number of tokens of p_4, $\boldsymbol{m} \xrightarrow{t} \boldsymbol{m}'$ implies $f(\boldsymbol{m}) \leq f(\boldsymbol{m}')$ for every transition $t \in T$. Furthermore, $f(\boldsymbol{m}_{\text{src}}) = 0 = f(\boldsymbol{m}_{\text{tgt}})$, and, since t_4 adds tokens to p_4, $\boldsymbol{m} \xrightarrow{t_4} \boldsymbol{m}'$ implies $f(\boldsymbol{m}) < f(\boldsymbol{m}')$. It follows that no firing sequence from $\boldsymbol{m}_{\text{src}}$ to $\boldsymbol{m}_{\text{tgt}}$ can fire t_4.
- *Claim:* $t_2 \notin U$. The set $Q := \{p_4\}$ is a siphon of $\mathcal{N}_{T\setminus\{t_4\}}$ (but not of $\mathcal{N}$). Since $\boldsymbol{m}_{\text{src}}(Q) = 0$, it is impossible to use transitions of $\mathcal{N}_{T\setminus\{t_4\}}$ that consume from Q, i.e. transitions of $Q^\bullet = \{t_2\}$.
- *Claim:* $t_1, t_3 \notin U$. The set $R := \{p_1, p_2\}$ is a trap of $\mathcal{N}_{T\setminus\{t_2,t_4\}}$ (but not of $\mathcal{N}_{T\setminus\{t_4\}}$). Since $\boldsymbol{m}_{\text{tgt}}(R) = 0$, it is impossible to reach $\boldsymbol{m}_{\text{tgt}}$ using transitions of $\mathcal{N}_{T\setminus\{t_2,t_4\}}$ that produce in R, i.e. transitions of ${}^\bullet R = \{t_1, t_3\}$.

By the claims, $U = \emptyset$, hence we reach the contradiction $\boldsymbol{m}_{\text{src}} = \boldsymbol{m}_{\text{tgt}}$. □

Proposition 4 below shows that condition 1. of Theorem 1 fails if and only if there is an exclusion function for S (actually, a slightly more general result). We need the following consequence of Farkas' lemma:

Proposition 3. *The system $\exists \boldsymbol{x} \geq \boldsymbol{0} : \mathbf{A}\boldsymbol{x} = \boldsymbol{b} \wedge S \subseteq \text{supp}(\boldsymbol{x}) \subseteq S'$ has no solution iff this system has some: $\exists \boldsymbol{y} : \mathbf{A}^\intercal \boldsymbol{y} \geq_{S'} \boldsymbol{0} \wedge \boldsymbol{b}^\intercal \boldsymbol{y} \leq 0 \wedge \boldsymbol{b}^\intercal \boldsymbol{y} < \sum_{s \in S} (\mathbf{A}^\intercal \boldsymbol{y})_s$.*

Proposition 4. *Let $\mathcal{N} = (P, T, F)$ be a Petri net, let $\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt} \in \mathbb{R}_+^P$, and let $S \subseteq S' \subseteq T$. No vector $\boldsymbol{x} \in \mathbb{R}_+^T$ satisfies $S \subseteq \text{supp}(\boldsymbol{x}) \subseteq S'$ and $\boldsymbol{m}_{src} + \mathbf{F}\boldsymbol{x} = \boldsymbol{m}_{tgt}$ iff there exists a linear exclusion function for (S, S').*

Proof. Assume no such $\boldsymbol{x} \in \mathbb{R}_+^T$ exists. Let $\boldsymbol{b} := \boldsymbol{m}_{\text{tgt}} - \boldsymbol{m}_{\text{src}}$. By Proposition 3, there exists $\boldsymbol{y} \in \mathbb{R}^P$ such that: $\mathbf{F}^\intercal \boldsymbol{y} \geq_{S'} \mathbf{0} \wedge \boldsymbol{b}^\intercal \boldsymbol{y} \leq 0 \wedge \boldsymbol{b}^\intercal \boldsymbol{y} < \sum_{s \in S} (\mathbf{F}^\intercal \boldsymbol{y})_s$. We show that $f(\boldsymbol{k}) := \boldsymbol{y}^\intercal \boldsymbol{k}$ is a linear exclusion function for (S, S').

1. We have $f(\boldsymbol{m}_{\text{tgt}}) - f(\boldsymbol{m}_{\text{src}}) = \boldsymbol{y}^\intercal \boldsymbol{m}_{\text{tgt}} - \boldsymbol{y}^\intercal \boldsymbol{m}_{\text{src}} = \boldsymbol{y}^\intercal (\boldsymbol{m}_{\text{tgt}} - \boldsymbol{m}_{\text{src}}) = \boldsymbol{y}^\intercal \boldsymbol{b} = \boldsymbol{b}^\intercal \boldsymbol{y} \leq 0$, and hence $f(\boldsymbol{m}_{\text{tgt}}) \leq f(\boldsymbol{m}_{\text{src}})$.
2. Let $\boldsymbol{m} \xrightarrow{\lambda s} \boldsymbol{m}'$ with $s \in S'$ and $\lambda \in \mathbb{R}_+$. We have $\boldsymbol{m}' = \boldsymbol{m} + \lambda \mathbf{F} \boldsymbol{e}_s$. Thus: $f(\boldsymbol{m}') = \boldsymbol{y}^\intercal \boldsymbol{m}' = \boldsymbol{y}^\intercal \boldsymbol{m} + \lambda (\boldsymbol{y}^\intercal \mathbf{F}) \boldsymbol{e}_s = \boldsymbol{y}^\intercal \boldsymbol{m} + \lambda (\mathbf{F}^\intercal \boldsymbol{y})^\intercal \boldsymbol{e}_s \geq \boldsymbol{y}^\intercal \boldsymbol{m} = f(\boldsymbol{m})$, where the inequality follows from $\lambda > 0$, $\mathbf{F}^\intercal \boldsymbol{y}$, $\geq_{S'} \mathbf{0}$ and $s \in S'$.
3. Recall that $\boldsymbol{b}^\intercal \boldsymbol{y} \leq 0$ and $\sum_{s \in S} (\mathbf{F}^\intercal \boldsymbol{y})_s > \boldsymbol{b}^\intercal \boldsymbol{y}$. If the latter sum equals zero, then $\boldsymbol{b}^\intercal \boldsymbol{y} < 0$, and hence we are done since $f(\boldsymbol{m}_{\text{tgt}}) - f(\boldsymbol{m}_{\text{src}}) = \boldsymbol{b}^\intercal \boldsymbol{y} < 0$. Otherwise, we have $\sum_{s \in S} (\mathbf{F}^\intercal \boldsymbol{y})_s > 0$ since $S \subseteq S'$ and $\mathbf{F}^\intercal \boldsymbol{y} \geq_{S'} \mathbf{0}$. Therefore, there exists a transition $s \in S$ such that $(\mathbf{F}^\intercal \boldsymbol{y})_s > 0$. Let $\boldsymbol{m} \xrightarrow{s} \boldsymbol{m}'$. We have $\boldsymbol{m}' = \boldsymbol{m} + \lambda \mathbf{F} \boldsymbol{e}_s$ for some $\lambda > 0$. Thus, $f(\boldsymbol{m}') = \boldsymbol{y}^\intercal \boldsymbol{m} + \lambda (\mathbf{F}^\intercal \boldsymbol{y})^\intercal \boldsymbol{e}_s > \boldsymbol{y}^\intercal \boldsymbol{m} = f(\boldsymbol{m})$, where the inequality holds by $\lambda > 0$ and $(\mathbf{F}^\intercal \boldsymbol{y})_s > 0$. □

Putting together Proposition 4 with Theorem 1 and Proposition 2, we obtain the following characterization of unreachability.

Proposition 5. *Let $\mathcal{N} = (P, T, F)$ be a Petri net, let $U \subseteq T$, and $\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt} \in \mathbb{R}_+^P$. It is the case that $\boldsymbol{m}_{src} \not\rightarrow^{U^*} \boldsymbol{m}_{tgt}$ iff for every $S \subseteq U$:*

1. *there exists an exclusion function for S, or*
2. *there exists a siphon Q of $\mathcal{N}_S$ such that $Q^\bullet \neq \emptyset$ and $\boldsymbol{m}_{src}(Q) = 0$, or*
3. *there exists a trap R of $\mathcal{N}_S$ such that ${}^\bullet R \neq \emptyset$ and $\boldsymbol{m}_{tgt}(R) = 0$.*

This proposition shows that, for all supports S, we can produce a witness of unreachability as an exclusion function, a siphon, or a trap. In the next section, we transform these witnesses into separators useful as certificates.

4 Separators as certificates

Let $\mathcal{N} = (P, T, F)$ be a Petri net and let $\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}} \in \mathbb{R}_+^P$ be two markings of $\mathcal{N}$. From [5], one can easily show that if $\boldsymbol{m}_{\text{src}} \not\rightarrow^* \boldsymbol{m}_{\text{tgt}}$, then there is a separator for $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$. Indeed, [5, Prop. 3.2] shows that there exists an existential formula ψ of linear arithmetic such that $\boldsymbol{m} \rightarrow^* \boldsymbol{m}'$ iff $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!]$. Thus, the formula $\varphi(\boldsymbol{m}) := \psi(\boldsymbol{m}_{\text{src}}, \boldsymbol{m})$ is a separator.

However, φ is not adequate as a *certificate* of unreachability. Indeed, checking a certificate for $\boldsymbol{m}_{\text{src}} \not\rightarrow^* \boldsymbol{m}_{\text{tgt}}$ should have smaller complexity than deciding whether $\boldsymbol{m}_{\text{src}} \rightarrow^* \boldsymbol{m}_{\text{tgt}}$. This is not the case for existential linear formulas, because $\boldsymbol{m}_{\text{src}} \rightarrow^* \boldsymbol{m}_{\text{tgt}}$ can be decided in polynomial time, but checking that an existential linear formula is a separator is coNP-hard.

Proposition 6. *The problem of determining whether an existential linear formula φ is a separator for $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$ is coNP-hard, even if φ is a quantifier-free formula in DNF and homogeneous.*

In the rest of the section, we introduce locally closed bi-separators, and then, in Sections 5 and 6, we respectively prove that they satisfy the following:

- If $\boldsymbol{m}_{\text{src}} \not\to^* \boldsymbol{m}_{\text{tgt}}$, then some locally closed bi-separator for $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$ can be computed in polynomial time;
- Deciding whether a formula is a locally closed bi-separator is in NC.

4.1 Locally closed bi-separators

The most difficult part of checking that a formula φ is a bi-separator consists of checking that it is forward and backward invariant. Let us focus on forward invariance, backward invariance being symmetric.

Recall the definition: for all markings $\boldsymbol{m}, \boldsymbol{m'}, \boldsymbol{m''}$ and every transition t: if $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi]\!]$ and $\boldsymbol{m}' \xrightarrow{\alpha t} \boldsymbol{m}''$ then $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\varphi]\!]$. Assume now that φ is in DNF, i.e., a disjunction of clauses $\varphi = \varphi_1 \vee \cdots \vee \varphi_n$. The forward invariance check can be decomposed into n smaller checks, one for each $i \in [1..n]$, of the form: if $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi_i]\!]$, then $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\varphi]\!]$. However, in general the check *cannot* be decomposed into *local* checks of the form: there exists $j \in [1..m]$ such that $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi_i]\!]$ implies $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\varphi_j]\!]$. Indeed, while this property is sufficient for forward invariance, it is not necessary. Intuitively, locally closed bi-separators are separators where invariance can be established by local checks.

For the formal definition, we need to introduce some notations. Given a transition t and atomic propositions ψ, ψ', we say that ψ *t-implies* ψ', written $\psi \rightsquigarrow_t \psi'$, if $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!]$ and $\boldsymbol{m}' \xrightarrow{\alpha t} \boldsymbol{m}''$ implies $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\psi']\!]$. We further say that a clause $\psi = \psi_1 \wedge \cdots \wedge \psi_m$ *t-implies* a clause $\psi' = \psi'_1 \wedge \cdots \wedge \psi'_n$, written $\psi \rightsquigarrow_t \psi'$, if for every $j \in [1..n]$, there exists $i \in [1..m]$ such that $\psi_i \rightsquigarrow_t \psi'_j$.

Definition 4. *A linear formula φ is* locally closed *w.r.t. $\mathcal{N} = (P, T, F)$ if:*

- *$\varphi = \varphi_1 \vee \cdots \vee \varphi_n$ is quantifier-free, in DNF and homogeneous,*
- *for every $t \in T$ and every $i \in [1..n]$, there exists $j \in [1..n]$ s.t. $\varphi_i \rightsquigarrow_t \varphi_j$,*
- *for every $t \in T^\intercal$ and every $i \in [1..n]$, there exists $j \in [1..n]$ s.t. $\varphi_i^\intercal \rightsquigarrow_t \varphi_j^\intercal$.*

Note that the definition is semantic. We make the straightforward but crucial observation that:

Proposition 7. *Locally closed formulas are bi-invariant.*

Proof. Let $\varphi = \varphi_1 \vee \cdots \vee \varphi_n$ be a locally closed formula. We only consider the forward case; the other case is symmetric. Let $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi]\!]$ and $\boldsymbol{m}' \xrightarrow{\alpha t} \boldsymbol{m}''$. Let $i \in [1..n]$ be such that $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi_i]\!]$. Since φ is locally closed, there exists $j \in [1..n]$ such that $\varphi_i \rightsquigarrow_t \varphi_j$. For every atomic proposition ψ' of φ_j, there exists an atomic proposition ψ of φ_i such that $\psi \rightsquigarrow_t \psi'$. Since each atomic proposition of φ_i is satisfied by $(\boldsymbol{m}, \boldsymbol{m}')$, we obtain $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\varphi_j]\!]$. □

Proposition 7 justifies the following definition:

Definition 5. *A* locally closed bi-separator *for $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$ is a locally closed formula φ s.t. $(\boldsymbol{m}_{src}, \boldsymbol{m}_{src}) \in [\![\varphi]\!]$, $(\boldsymbol{m}_{tgt}, \boldsymbol{m}_{tgt}) \in [\![\varphi]\!]$ and $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt}) \notin [\![\varphi]\!]$.*

Indeed, by Proposition 7, a locally closed bi-separator is a bi-separator, as the bi-invariance condition of Definition 2 follows from local closedness.

5 Constructing locally closed bi-separators

In this section, we prove that unreachability can always be witnessed by locally closed bi-separators of polynomial size and computable in polynomial time. The proof uses the results of Section 3.

Theorem 2. *If $\boldsymbol{m}_{src} \not\rightarrow^{U^*} \boldsymbol{m}_{tgt}$, then there is a locally closed bi-separator φ for $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$ w.r.t. $\mathcal{N}_U$. Further, $\varphi = \bigvee_{1 \leq i \leq n} \varphi_i$, where $n \leq 2|U| + 1$ and each φ_i contains at most $2|U| + 1$ atomic propositions. Moreover, φ is computable in polynomial time.*

Proof. We proceed by induction on $|U|$. First consider $U = \emptyset$. Let $p \in P$ be such that $\boldsymbol{m}_{\text{src}}(p) \neq \boldsymbol{m}_{\text{tgt}}(p)$. Take $\varphi(\boldsymbol{m}, \boldsymbol{m}') := \boldsymbol{e}_p\boldsymbol{m} \leq \boldsymbol{e}_p\boldsymbol{m}'$ or $-\boldsymbol{e}_p\boldsymbol{m} \leq -\boldsymbol{e}_p\boldsymbol{m}'$.

Now, assume that $U \neq \emptyset$. Consider the system $\exists \boldsymbol{x} \in \mathbb{R}_+^T : \boldsymbol{m}_{\text{src}} + \mathbf{F}\boldsymbol{x} = \boldsymbol{m}_{\text{tgt}} \wedge \text{supp}(\boldsymbol{x}) \subseteq U$. Suppose first that the system has no solution. By Proposition 4, taking $S = \emptyset$ and $S' = U$, there is a linear exclusion function for $(\emptyset, U)$, i.e. a linear function f satisfying:

1. $f(\boldsymbol{m}_{\text{src}}) > f(\boldsymbol{m}_{\text{tgt}})$,
2. $\boldsymbol{m} \xrightarrow{u} \boldsymbol{m}'$ implies $f(\boldsymbol{m}) \leq f(\boldsymbol{m}')$ for all $u \in U$.

(The first item holds due to Item 2 of Definition 3 and $S = \emptyset$.) So we can take $\varphi(\boldsymbol{m}, \boldsymbol{m}') \coloneqq (f(\boldsymbol{m}) \leq f(\boldsymbol{m}'))$.

Suppose now that the system has a solution $\boldsymbol{x} \in \mathbb{R}_+^U$. By convexity, we can suppose that $\text{supp}(\boldsymbol{x}) \subseteq U$ is maximal. Indeed, if $\boldsymbol{x}'$ and $\boldsymbol{x}''$ are solutions, then $(1/2)\boldsymbol{x}' + (1/2)\boldsymbol{x}''$ is a solution with support $\text{supp}(\boldsymbol{x}') \cup \text{supp}(\boldsymbol{x}'')$. Let $U' \coloneqq \text{supp}(\boldsymbol{x})$. For every $t \in U \setminus U'$, consider the system of Proposition 4 with $S = \{t\}$ and $S' = U$. By maximality of $U' \subseteq U$, none of these systems has a solution. Consequently, for each $t \in U \setminus U'$, Proposition 4 yields a linear exclusion function for $(\{t\}, U)$, i.e. a linear function f_t that satisfies:

3. $f_t(\boldsymbol{m}_{\text{src}}) \geq f_t(\boldsymbol{m}_{\text{tgt}})$,
4. $\boldsymbol{m} \xrightarrow{u} \boldsymbol{m}'$ implies $f_t(\boldsymbol{m}) \leq f_t(\boldsymbol{m}')$ for all $u \in U$,
5. either $f_t(\boldsymbol{m}_{\text{src}}) > f_t(\boldsymbol{m}_{\text{tgt}})$, or $\boldsymbol{m} \xrightarrow{t} \boldsymbol{m}'$ implies $f_t(\boldsymbol{m}) < f_t(\boldsymbol{m}')$.

If $f_t(\boldsymbol{m}_{\text{src}}) > f_t(\boldsymbol{m}_{\text{tgt}})$ holds for some $t \in U \setminus U'$, then we are done by taking $\varphi(\boldsymbol{m}, \boldsymbol{m}') \coloneqq (f_t(\boldsymbol{m}) \leq f_t(\boldsymbol{m}'))$ as Item 4 ensures that $\varphi \rightsquigarrow_u \varphi$ for every $u \in U$. So assume it does not hold for any $t \in U \setminus U'$, i.e. assume that $f_t(\boldsymbol{m}_{\text{src}}) = f_t(\boldsymbol{m}_{\text{tgt}})$ holds, and the second disjunct of Item 5 holds for all $t \in U \setminus U'$. This is the most involved case. Let

$$\varphi_{\text{inv}}(\boldsymbol{m}, \boldsymbol{m}') \coloneqq \bigwedge_{t \in U \setminus U'} (f_t(\boldsymbol{m}) \leq f_t(\boldsymbol{m}')) \quad \text{and} \quad \varphi_t(\boldsymbol{m}, \boldsymbol{m}') \coloneqq (f_t(\boldsymbol{m}) < f_t(\boldsymbol{m}')).$$

Let $Q, R \subseteq P$ be respectively the maximal siphon and trap of $\mathcal{N}_{U'}$ such that $\boldsymbol{m}_{\text{src}}(Q) = 0$ and $\boldsymbol{m}_{\text{tgt}}(R) = 0$ (well-defined by closure under union). Let $U'' \coloneqq U' \setminus (Q^\bullet \cup {}^\bullet R)$. By Theorem 1 and Proposition 2, $Q^\bullet \cup {}^\bullet R \neq \emptyset$. Thus, U'' is a strict subset of U', and, by induction hypothesis, there is a locally closed bi-separator w.r.t. $\mathcal{N}_{U''}$ of the form $\psi = \bigvee_{1 \leq i \leq m} \psi_i$ that satisfies the claim for set U''. Let

$$\begin{aligned}\varphi(\boldsymbol{m}, \boldsymbol{m}') \coloneqq \bigvee_{t \in U \setminus U'} \varphi_t(\boldsymbol{m}, \boldsymbol{m}') \vee [\varphi_{\text{inv}}(\boldsymbol{m}, \boldsymbol{m}') \wedge \boldsymbol{m}(Q) + \boldsymbol{m}'(R) > 0] \vee \\ \bigvee_{1 \leq i \leq m} [\varphi_{\text{inv}}(\boldsymbol{m}, \boldsymbol{m}') \wedge \boldsymbol{m}(R) + \boldsymbol{m}'(Q) \leq 0 \wedge \psi_i(\boldsymbol{m}, \boldsymbol{m}')].\end{aligned}$$

As $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}) \in [\![\varphi_{\text{inv}}]\!]$ and $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}) \in [\![\psi]\!]$, we have $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}) \in [\![\varphi]\!]$. Similarly, $(\boldsymbol{m}_{\text{tgt}}, \boldsymbol{m}_{\text{tgt}}) \in [\![\varphi]\!]$. By Item 3, $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}}) \notin [\![\bigvee_{t \in U \setminus U'} \varphi_t(\boldsymbol{m}, \boldsymbol{m}')]\!]$. Further, $\boldsymbol{m}_{\text{src}}(Q) + \boldsymbol{m}_{\text{tgt}}(R) = 0$ and $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}}) \notin [\![\psi]\!]$. So, $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}}) \notin [\![\varphi]\!]$.

The number of disjuncts of φ is $|U \setminus U'| + 1 + m$ and hence at most

$$\begin{aligned}|U \setminus U'| + 1 + 2|U''| + 1 \leq |U| - |U''| + 1 + 2|U''| + 1 = \\ |U| + |U''| + 2 \leq |U| + (|U| - 1) + 2 = 2|U| + 1.\end{aligned}$$

The same bounds holds for the number of atomic propositions per disjunct.

It remains to show that $\varphi(\boldsymbol{m}, \boldsymbol{m}')$ is locally closed w.r.t. $\mathcal{N}_U$. We only consider the forward case, as the backward case is symmetric. Let $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi]\!]$ and $\boldsymbol{m}' \xrightarrow{u} \boldsymbol{m}''$ for some $u \in U$. By Item 4, $\varphi_t \rightsquigarrow_u \varphi_t$ holds for each φ_t. Indeed, $f_t(\boldsymbol{m}) < f_t(\boldsymbol{m}')$ and $\boldsymbol{m}' \xrightarrow{u} \boldsymbol{m}''$ imply $f_t(\boldsymbol{m}) < f_t(\boldsymbol{m}') \leq f_t(\boldsymbol{m}'')$, and hence $f_t(\boldsymbol{m}) < f_t(\boldsymbol{m}'')$. To handle the other clauses, we make a case distinction on u.

- *Case $u \in U \setminus U'$.* Atomic proposition $\theta = (f_u(\boldsymbol{m}) \leq f_u(\boldsymbol{m}'))$ of φ_{inv} satisfies $\theta \rightsquigarrow_u \varphi_u$. Indeed, if $f_u(\boldsymbol{m}) \leq f_u(\boldsymbol{m}')$ and $\boldsymbol{m}' \xrightarrow{u} \boldsymbol{m}''$, then we have $f_u(\boldsymbol{m}) < f_u(\boldsymbol{m}')$ by Item 5.
- *Case $u \in U'$.* By Item 4, each atomic proposition θ of φ_{inv} satisfies $\theta \rightsquigarrow_u \theta$.
  - *Case $u \in {}^\bullet R$.* We have $\theta' \rightsquigarrow_u (\boldsymbol{m}(Q) + \boldsymbol{m}'(R) > 0)$ for any atomic proposition θ', since $\boldsymbol{m}' \xrightarrow{u} \boldsymbol{m}''$ implies $\boldsymbol{m}''(R) > 0$ (regardless of θ').
  - *Case $u \in Q^\bullet$.* If $\boldsymbol{m}'(Q) \leq 0$, then u is disabled in $\boldsymbol{m}'$. Thus, it only remains to handle $\theta_{>0} \coloneqq (\boldsymbol{m}(Q) + \boldsymbol{m}'(R) > 0)$. Since R is a trap of $\mathcal{N}_{U'}$, firing u from $\boldsymbol{m}'$ does not empty R, and hence $\theta_{>0} \rightsquigarrow_u \theta_{>0}$.
  - *Case $u \in U''$.* Let $\theta_{\leq 0} \coloneqq (\boldsymbol{m}(R) + \boldsymbol{m}'(Q) \leq 0)$ and $\theta_{>0} \coloneqq (\boldsymbol{m}(Q) + \boldsymbol{m}'(R) > 0)$. Since Q and R are respectively a siphon and trap of $\mathcal{N}_{U'}$, we have $\theta_{\leq 0} \rightsquigarrow_u \theta_{\leq 0}$ and $\theta_{>0} \rightsquigarrow_u \theta_{>0}$. Moreover, by induction hypothesis, for every $i \in [1..m]$, there exists $j \in [1..m]$ such that $\psi_i \rightsquigarrow_u \psi_j$.

We conclude the proof by observing that it is constructive and can be turned into Algorithm 1. The procedure works in polynomial time. Indeed, there are at most $|U|$ recursive calls. Moreover, each set can be obtained in polynomial time via either linear programming or maximal siphons/traps computations [9]. □

Example 2. Let us apply the construction of Theorem 2 to the Petri net and the markings of Example 1: $\boldsymbol{m}_{\text{src}} = \{p_1 \mapsto 2, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 0\}$ and $\boldsymbol{m}_{\text{tgt}} \coloneqq \{p_1 \mapsto 0, p_2 \mapsto 0, p_3 \mapsto 1, p_4 \mapsto 0\}$. The locally closed bi-separator is the formula φ below, where the colored arrows represent the relations $\rightsquigarrow_{t_1}, \ldots, \rightsquigarrow_{t_4}$:

$$\begin{tikzcd}[row sep=small]
{[\boldsymbol{m}(p_4) < \boldsymbol{m}'(p_4)] \vee} \arrow[loop left, squiggly, "{t_1, t_2, t_3, t_4}"] \\
{[\boldsymbol{m}(p_4) \leq \boldsymbol{m}'(p_4) \wedge \boldsymbol{m}(p_4) + \boldsymbol{m}'(p_4) > 0] \vee} \arrow[u, squiggly, bend left, "t_4"] \arrow[loop right, squiggly, "{t_1, t_2, t_3}"] \\
{[\boldsymbol{m}(p_4) \leq \boldsymbol{m}'(p_4) \wedge \boldsymbol{m}'(p_1) + \boldsymbol{m}'(p_2) > 0] \vee} \arrow[uu, squiggly, bend left, "t_4"] \arrow[u, squiggly, "t_2"'] \arrow[loop right, squiggly, "{t_1, t_3}"] \\
{[\boldsymbol{m}(p_4) \leq \boldsymbol{m}'(p_4) \wedge \boldsymbol{m}(p_1) + \boldsymbol{m}(p_2) \leq 0 \wedge -\boldsymbol{m}(p_3) \leq -\boldsymbol{m}'(p_3)]} \arrow[uuu, squiggly, bend left, "t_4"] \arrow[uu, squiggly, bend right, "t_2"'] \arrow[loop right, squiggly, "{t_1, t_3}"]
\end{tikzcd}$$

The forward separator $\psi(\boldsymbol{m}) := \varphi(\boldsymbol{m}_{\text{src}}, \boldsymbol{m})$ is, after simplifications, given by

$$\psi(\boldsymbol{m}) \equiv \boldsymbol{m}(p_1) + \boldsymbol{m}(p_2) > 0 \vee \boldsymbol{m}(p_4) > 0.$$

Similarly, we obtain this backward separator $\psi'(\boldsymbol{m}) := \varphi(\boldsymbol{m}, \boldsymbol{m}_{\text{tgt}})$:

$$\psi'(\boldsymbol{m}) \equiv \boldsymbol{m}(p_1) + \boldsymbol{m}(p_2) = 0 \wedge \boldsymbol{m}(p_3) \geq 1 \wedge \boldsymbol{m}(p_4) = 0.$$

The backward separator ψ' provides a much simpler proof of $\boldsymbol{m}_{\text{src}} \overset{*}{\nrightarrow} \boldsymbol{m}_{\text{tgt}}$ than the one of Example 1. The proof goes as follows: ψ' is trivially backward invariant, because markings that only mark p_3 do not backward-enable any transition. In particular, since $\boldsymbol{m}_{\text{tgt}}$ only marks p_3, it can only be reached from $\boldsymbol{m}_{\text{tgt}}$. □

Algorithm 1: Construction of a locally closed bi-sep. for $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$.

```
Input: $\mathcal{N} = (P, T, F)$, $U \subseteq T$ and $\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}} \in \mathbb{Q}_+^P$ s.t. $\boldsymbol{m}_{\text{src}} \nrightarrow^{U^*} \boldsymbol{m}_{\text{tgt}}$
Output: A locally closed bi-separator w.r.t. $\mathcal{N}_U$
bi-separator($U$)
    if $U = \emptyset$ then
        pick $p \in P$ such that $\boldsymbol{m}_{\text{src}}(p) \neq \boldsymbol{m}_{\text{tgt}}(p)$
        return $(\boldsymbol{a}\boldsymbol{m} \leq \boldsymbol{a}\boldsymbol{m}')$ where $\boldsymbol{a} := \text{sign}(\boldsymbol{m}_{src}(p) - \boldsymbol{m}_{tgt}(p)) \cdot \boldsymbol{e}_p$
    else
        $\boldsymbol{b} := \boldsymbol{m}_{\text{tgt}} - \boldsymbol{m}_{\text{src}}$
        $X := \{\boldsymbol{x} \in \mathbb{R}_+^T : \mathbf{F}\boldsymbol{x} = \boldsymbol{b}, \text{supp}(\boldsymbol{x}) \subseteq U\}$
        $Y_S := \{\boldsymbol{y} \in \mathbb{R}^P : \mathbf{F}^\intercal \boldsymbol{y} \geq_U \mathbf{0}, \boldsymbol{b}^\intercal \boldsymbol{y} \leq 0, \boldsymbol{b}^\intercal \boldsymbol{y} < \sum_{s \in S} (\mathbf{F}^\intercal \boldsymbol{y})_s\}$
        if $X = \emptyset$ then
            pick $\boldsymbol{y} \in Y_\emptyset$ and return $(\boldsymbol{y}^\intercal \boldsymbol{m} \leq \boldsymbol{y}^\intercal \boldsymbol{m}')$
        else
            $U' := \{u \in U : \boldsymbol{x}(u) > 0$ for some $\boldsymbol{x} \in X\}$
            for $t \in U \setminus U'$ do
                pick $\boldsymbol{y}_t \in Y_{\{t\}}$; $f_t(\boldsymbol{m}) := \boldsymbol{y}_t^\intercal \boldsymbol{m}$
                if $f_t(\boldsymbol{m}_{src}) > f_t(\boldsymbol{m}_{tgt})$ then return $(f_t(\boldsymbol{m}) < f_t(\boldsymbol{m}'))$
            $Q :=$ largest siphon of $\mathcal{N}_{U'}$ such that $\boldsymbol{m}_{\text{src}}(Q) = 0$
            $R :=$ largest trap of $\mathcal{N}_{U'}$ such that $\boldsymbol{m}_{\text{tgt}}(R) = 0$
            $\varphi_{\text{inv}} := \bigwedge_{t \in U \setminus U'} (f_t(\boldsymbol{m}) \leq f_t(\boldsymbol{m}'))$
            $\psi_1 \vee \cdots \vee \psi_m :=$ bi-separator($U' \setminus (Q^\bullet \cup {}^\bullet R)$)
            return $\bigvee_{t \in U \setminus U'} \varphi_t(\boldsymbol{m}, \boldsymbol{m}') \vee [\varphi_{\text{inv}}(\boldsymbol{m}, \boldsymbol{m}') \wedge \boldsymbol{m}(Q) + \boldsymbol{m}'(R) > 0] \vee$
                   $\bigvee_{1 \leq i \leq m} [\varphi_{\text{inv}}(\boldsymbol{m}, \boldsymbol{m}') \wedge \boldsymbol{m}(R) + \boldsymbol{m}'(Q) \leq 0 \wedge \psi_i(\boldsymbol{m}, \boldsymbol{m}')]$
```

6 Checking locally closed bi-separators is in NC

We show that the problem of deciding whether a given linear formula is a locally closed bi-separator is in NC. To do so, we provide a characterization of $\psi \rightsquigarrow_t \psi$ for homogeneous atomic propositions ψ and ψ'. We only focus on forward firability, as backward firability can be expressed as forward firability in the transpose Petri net. Recall that $\psi \rightsquigarrow_t \psi'$ holds iff the following holds:

$$(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!] \text{ and } \boldsymbol{m}' \xrightarrow{\alpha t} \boldsymbol{m}'' \text{ imply } (\boldsymbol{m}, \boldsymbol{m}'') \in [\![\psi']\!]. \qquad (*)$$

Property (*) can be rephrased as:

$$(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!] \text{ and } \boldsymbol{m}' \geq \alpha \cdot \Delta_t^- \text{ imply } (\boldsymbol{m}, \boldsymbol{m}' + \alpha \cdot \Delta_t) \in [\![\psi']\!].$$

As we will see towards the end of the section, due to homogeneity, it actually suffices to consider the case where $\alpha = 1$, which yields this reformulation:

$$\underbrace{\{(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!] : \boldsymbol{m}' \geq \Delta_t^-\}}_{X} \subseteq \underbrace{\{(\boldsymbol{m}, \boldsymbol{m}') : (\boldsymbol{m}, \boldsymbol{m}' + \Delta_t) \in [\![\psi']\!]\}}_{Y}.$$

Therefore, testing $\psi \rightsquigarrow_t \psi'$ amounts to the inclusion check $X \subseteq Y$. Of course, if $X = \emptyset$, then this is trivial. Hence, we will suppose that $X \neq \emptyset$, assuming for now that it can somehow be tested efficiently. In the forthcoming Propositions 8 and 9, we will provide necessary and sufficient conditions for $X \subseteq Y$ to hold. In Proposition 10, we will show that these conditions are testable in NC. Then, in Proposition 11, we will explain how to check whether $X \neq \emptyset$ actually holds.

For $X \subseteq Y$, we can characterize the case of atomic propositions ψ that use "$\leq$" (rather than "$<$") with a generalization of Farkas' lemma:

Proposition 8. *Let $\boldsymbol{a}, \boldsymbol{a}', \boldsymbol{l} \in \mathbb{R}^n$ and $b' \in \mathbb{R}$. Let $X := \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}\boldsymbol{x} \leq 0 \wedge \boldsymbol{x} \geq \boldsymbol{l}\}$ and $Y := \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}'\boldsymbol{x} \leq b'\}$ be such that $X \neq \emptyset$. It is the case that $X \subseteq Y$ iff there exists $\lambda \geq 0$ such that $\lambda\boldsymbol{a} \geq \boldsymbol{a}'$ and $-b' \leq (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l}$.*

We now give the conditions for all four combinations of "$\leq$" and "$<$":

Proposition 9. *Let $\boldsymbol{a}, \boldsymbol{a}' \in \mathbb{R}^n$, $b' \in \mathbb{R}$, $\boldsymbol{l} \geq \boldsymbol{0}$ and $\sim, \sim' \in \{\leq, <\}$. Let $X_\sim := \{\boldsymbol{x} \geq \boldsymbol{l} : \boldsymbol{a}\boldsymbol{x} \sim \boldsymbol{0}\}$ and $Y_{\sim'} := \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}'\boldsymbol{x} \sim' b'\}$ be such that $X_\sim \neq \emptyset$. It holds that $X_\sim \subseteq Y_{\sim'}$ iff there exists $\lambda \geq 0$ s.t. $\lambda\boldsymbol{a} \geq \boldsymbol{a}'$ and one of the following holds:*

1. *$\sim' = \leq$ and $-b' \leq (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l}$;*
2. *$\sim = \leq$, $\sim' = <$, and $-b' < (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l}$;*
3. *$\sim = <$, $\sim' = <$, and either $-b' < (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l}$ or $-b' = (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l} \wedge \lambda > 0$.*

Proof.

1. If $\sim = \leq$, then it follows immediately from Proposition 8. Thus, assume $\sim = <$. We claim that $X_< \subseteq Y_\leq$ iff $X_\leq \subseteq Y_\leq$. The validity of this claim concludes the proof of this case as we have handled $\sim = \leq$ and as $X_\leq \supseteq X_< \neq \emptyset$.

Let us show the claim. It is clear that $X_< \subseteq Y_\leq$ is implied by $X_\leq \subseteq Y_\leq$. So, we only have to show direction from left to right. For the sake of contradiction, suppose that $X_< \subseteq Y_\leq$ and $X_\leq \not\subseteq Y_\leq$. Let $X_= := X_\leq \setminus X_<$. Note that $X_= \neq \emptyset$. Let $\boldsymbol{x} \in X_<$ and $\boldsymbol{x}' \in X_= \setminus Y_\leq$. We have $\boldsymbol{x}, \boldsymbol{x}' \geq \boldsymbol{l}$, $\boldsymbol{ax} < 0$, $\boldsymbol{ax}' = 0$, $\boldsymbol{a}'\boldsymbol{x} = c \leq b'$ and $\boldsymbol{a}'\boldsymbol{x}' = c' > b'$ for some $c, c' \in \mathbb{R}$. In particular, $b' \in [c, c')$. Let $\epsilon \in (0, 1]$ be such that $b' < \epsilon c + (1 - \epsilon)c'$. Let $\boldsymbol{x}'' := \epsilon\boldsymbol{x} + (1 - \epsilon)\boldsymbol{x}'$. Observe that $\boldsymbol{x}'' \geq \boldsymbol{l}$. Moreover, we have:

$$\begin{aligned} \boldsymbol{ax}'' &= \epsilon\boldsymbol{ax} + (1-\epsilon)\boldsymbol{ax}' &&= \epsilon\boldsymbol{ax} &&< 0, \\ \boldsymbol{a}'\boldsymbol{x}'' &= \epsilon\boldsymbol{a}'\boldsymbol{x} + (1-\epsilon)\boldsymbol{a}'\boldsymbol{x}' &&= \epsilon c + (1-\epsilon)c' &&> b'. \end{aligned}$$

Therefore, we have $\boldsymbol{x}'' \in X_<$ and $\boldsymbol{x}'' \notin Y_\leq$, which is a contradiction.

2. $\Rightarrow$) Since $X_\leq \subseteq Y_<$, the system $\exists \boldsymbol{x} : \boldsymbol{x} \geq \boldsymbol{l} \land \boldsymbol{ax} \leq 0 \land \boldsymbol{a}'\boldsymbol{x} \geq b'$ has no solution. In matrix notation, the system corresponds to $\exists \boldsymbol{x} : \mathbf{A}\boldsymbol{x} \leq \boldsymbol{c}$ where

$$\mathbf{A} := \begin{bmatrix} -\mathbf{I} \\ \boldsymbol{a} \\ -\boldsymbol{a}' \end{bmatrix} \text{ and } \boldsymbol{c} := \begin{pmatrix} -\boldsymbol{l} \\ 0 \\ -b' \end{pmatrix}.$$

By Farkas' lemma (Lemma 1), $\mathbf{A}^\mathsf{T}\boldsymbol{y} = \mathbf{0}$ and $\boldsymbol{c}^\mathsf{T}\boldsymbol{y} < 0$ for some $\boldsymbol{y} \geq \mathbf{0}$. In other words,

$$\exists \boldsymbol{z} \geq \mathbf{0}, \lambda, \lambda' \geq 0 : \lambda\boldsymbol{a} - \lambda'\boldsymbol{a}' = \boldsymbol{z} \land -\lambda' b' < \boldsymbol{zl}.$$

Since $\boldsymbol{z} \geq \mathbf{0}$, we have $\lambda\boldsymbol{a} \geq \lambda'\boldsymbol{a}' \land -\lambda' b' < (\lambda\boldsymbol{a} - \lambda'\boldsymbol{a}')\boldsymbol{l}$. If $\lambda' > 0$, then we are done by dividing all terms by λ'. For the sake of contradiction, suppose that $\lambda' = 0$. This means that $\lambda\boldsymbol{a} \geq \mathbf{0}$ and $0 < \lambda\boldsymbol{al}$. We necessarily have $\lambda > 0$ and $\boldsymbol{al} > 0$. Let $\boldsymbol{x} \in X_\leq$. We have $0 \geq \boldsymbol{ax} \geq \boldsymbol{al} > 0$, which is a contradiction.

$\Leftarrow$) Let $\boldsymbol{x} \in X_\leq$. We have $\boldsymbol{a}'\boldsymbol{x} < b'$ and hence $\boldsymbol{x} \in Y_<$ as desired, since:

$$\begin{aligned} -b' &< (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l} \\ &\leq (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{x} && \text{(by } (\lambda\boldsymbol{a} - \boldsymbol{a}') \geq \mathbf{0} \text{ and } \boldsymbol{x} \geq \boldsymbol{l} \geq \mathbf{0}) \\ &= \lambda\boldsymbol{ax} - \boldsymbol{a}'\boldsymbol{x} \\ &\leq -\boldsymbol{a}'\boldsymbol{x} && \text{(by } \lambda \geq 0 \text{ and } \boldsymbol{ax} \leq 0). \end{aligned}$$

3. The proof is similar albeit slightly more complicated. □

The conditions arising from Proposition 9 involve solving linear programs with *one* variable λ. It is easy to see that this problem is in NC:

Proposition 10. *Given $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Q}^n$ and $\sim\, \in \{\leq, <\}^n$, testing $\exists \lambda \geq 0 : \boldsymbol{a}\lambda \sim \boldsymbol{b}$ is in NC.*

Recall that at the beginning of the section we made the assumption that some pair $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!]$ is such that $\boldsymbol{m}'$ enables a transition t. Checking whether this is actually true has a cost. Fortunately, we provide a simple characterization of enabledness which can checked in NC. Formally, we say that φ *enables* t if there exists $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi]\!]$ such that $\boldsymbol{m}'$ α-enables t for some $\alpha > 0$. We have:

Proposition 11. *Let $\varphi_\sim(\boldsymbol{m}, \boldsymbol{m}') := \boldsymbol{a}\boldsymbol{m} \sim \boldsymbol{b}\boldsymbol{m}'$ where $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^P$. This holds:*

1. *$\varphi_<$ enables u iff $\boldsymbol{a} \not\geq \boldsymbol{0}$ or $\boldsymbol{b} \not\leq \boldsymbol{0}$, and*
2. *$\varphi_\leq$ enables u iff $\boldsymbol{b}\Delta_u^- \geq 0$ or $(\boldsymbol{b}\Delta_u^- < 0 \wedge (\boldsymbol{a}, -\boldsymbol{b}) \not\geq (\boldsymbol{0}, \boldsymbol{0}))$.*

Proof.

1. $\Rightarrow$) Since $\varphi_<$ enables u, we have $[\![\varphi_<]\!] \neq \emptyset$. Let $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi_<]\!]$. We have $\boldsymbol{a}\boldsymbol{m} < \boldsymbol{b}\boldsymbol{m}'$. It cannot be that $\boldsymbol{a} \geq \boldsymbol{0}$ and $\boldsymbol{b} \leq \boldsymbol{0}$, as otherwise $\boldsymbol{a}\boldsymbol{m} \geq 0 \geq \boldsymbol{b}\boldsymbol{m}'$.

   $\Leftarrow$) It suffices to give a pair $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi_<]\!]$ such that $\boldsymbol{m}' \geq \Delta_u^-$. Informally, if $\boldsymbol{a}$ has a negative value (resp. $\boldsymbol{b}$ has a positive value), then we can consider the pair $(\boldsymbol{0}, \Delta_u^-)$ and "fix" the value on the left-hand-side (resp. right-hand side) so that $\varphi_<$ is satisfied. More formally, if $\boldsymbol{a}(p) < 0$, then $(k\boldsymbol{e}_p, \Delta_u^-) \in [\![\varphi_<]\!]$ with $k := (|\boldsymbol{b}\Delta_u^-| + 1)/|\boldsymbol{a}(p)|$; if $\boldsymbol{b}(p) > 0$, then $(\boldsymbol{0}, \Delta_u^- + k\boldsymbol{e}_p) \in [\![\varphi_<]\!]$ with $k := (|\boldsymbol{b}\Delta_u^-| + 1)/\boldsymbol{b}(p)$.
2. The proof is similar albeit slightly more complicated. □

We can finally show that testing $\psi \rightsquigarrow_t \psi'$ can be done in NC, for atomic propositions ψ and ψ'. In turn, this allows us to show that we can test in NC whether a linear formula is a locally closed bi-separator.

Proposition 12. *Given a Petri net $\mathcal{N}$, a transition t and homogeneous atomic propositions ψ and ψ', testing whether $\psi \rightsquigarrow_t \psi'$ can be done in NC.*

Proof. Recall that addition, subtraction, multiplication, division and comparison can be done in NC. Note that, by Proposition 11, we can check whether ψ enables t in NC. If it does, then we must test whether $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!]$ and $\boldsymbol{m}' \xrightarrow{\alpha t} \boldsymbol{m}''$ implies $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\psi']\!]$. We claim that this amounts to testing $X \subseteq Y$, where:

$$\begin{aligned} X &:= \{(\boldsymbol{m}, \boldsymbol{m}') \in \mathbb{R}_+^P \times \mathbb{R}_+^P : (\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!] \text{ and } (\boldsymbol{m}, \boldsymbol{m}') \geq (\boldsymbol{0}, \Delta_t^-)\}, \\ Y &:= \{(\boldsymbol{m}, \boldsymbol{m}') \in \mathbb{R}_+^P \times \mathbb{R}_+^P : (\boldsymbol{m}, \boldsymbol{m}' + \Delta_t) \in [\![\psi']\!]\}. \end{aligned}$$

Let us prove this claim.

$\Rightarrow$) Let $(\boldsymbol{m}, \boldsymbol{m}') \in X$. We have $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!]$ and $(\boldsymbol{m}, \boldsymbol{m}') \geq (\boldsymbol{0}, \Delta_t^-)$. Thus $\boldsymbol{m}' \xrightarrow{t} \boldsymbol{m}' + \Delta_t$. By assumption, $(\boldsymbol{m}, \boldsymbol{m}' + \Delta_t) \in [\![\psi']\!]$, and hence $(\boldsymbol{m}, \boldsymbol{m}') \in Y$.

$\Leftarrow$) Let $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\psi]\!]$ and $\boldsymbol{m}' \xrightarrow{\alpha t} \boldsymbol{m}''$. We have $\boldsymbol{m}' \geq \alpha\Delta_t^-$ and $\boldsymbol{m}'' = \boldsymbol{m}' + \alpha\Delta_t$. Let $\boldsymbol{k} := \boldsymbol{m}/\alpha$, $\boldsymbol{k}' := \boldsymbol{m}'/\alpha$ and $\boldsymbol{k}'' := \boldsymbol{m}''/\alpha$. As $\alpha > 0$ and ψ is homogeneous, we have $(\boldsymbol{k}, \boldsymbol{k}') \in [\![\psi]\!]$, $(\boldsymbol{k}, \boldsymbol{k}') \geq (\boldsymbol{0}, \Delta_t^-)$ and $\boldsymbol{k}'' = \boldsymbol{k}' + \Delta_t$. Thus, $(\boldsymbol{k}, \boldsymbol{k}') \in X \subseteq Y$. By definition of Y, this means that $(\boldsymbol{k}, \boldsymbol{k}'') \in [\![\psi']\!]$. By homogeneity, we conclude that $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\psi']\!]$.

Now that we have shown the claim, let us explain how to check whether $X \subseteq Y$ in NC. Note that $X \neq \emptyset$ since ψ enables t. Thus, by Proposition 9, testing $X \subseteq Y$ amounts to solving a linear program in one variable. For example, if $\psi = (\boldsymbol{a} \cdot (\boldsymbol{m}, \boldsymbol{m}') \leq 0)$ and $\psi' = (\boldsymbol{a}' \cdot (\boldsymbol{m}, \boldsymbol{m}') < 0)$, then we must check whether this system has a solution:

$$\exists \lambda \geq 0 : \lambda\boldsymbol{a} \geq \boldsymbol{a}' \wedge \boldsymbol{a} \cdot (\boldsymbol{0}, \Delta_t) < (\lambda\boldsymbol{a} - \boldsymbol{a}') \cdot (\boldsymbol{0}, \Delta_t^-).$$

Thus, by Proposition 10, testing $X \subseteq Y$ can be done in NC. □

Theorem 3. *Given $\mathcal{N} = (P, T, F)$, $\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt} \in \mathbb{Q}_+^P$ and a formula φ, testing whether φ is a locally closed bi-separator for $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$ can be done in NC.*

Proof. Recall that $\varphi = \varphi_1 \vee \cdots \vee \varphi_n$ must be in DNF with homogeneous atomic propositions. As arithmetic belongs in NC and φ is in DNF, we can test whether $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}) \in [\![\varphi]\!]$, $(\boldsymbol{m}_{\text{tgt}}, \boldsymbol{m}_{\text{tgt}}) \in [\![\varphi]\!]$ and $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}}) \notin [\![\varphi]\!]$ in NC by evaluating φ in parallel. We can further test whether φ is locally closed by checking the following (which is simply the definition of "locally closed"):

$$\left[\bigwedge_{\substack{t \in T \\ i \in [1..n]}} \bigvee_{j \in [1..n]} \bigwedge_{\psi \in \varphi_i} \bigvee_{\psi' \in \varphi_j} \psi \rightsquigarrow_t \psi' \right] \wedge \left[\bigwedge_{\substack{t \in T^\intercal \\ i \in [1..n]}} \bigvee_{j \in [1..n]} \bigwedge_{\psi \in \varphi_i} \bigvee_{\psi' \in \varphi_j} \psi^\intercal \rightsquigarrow_t \psi'^\intercal \right].$$

By Proposition 12, each test $\psi \rightsquigarrow_t \psi'$ can be carried in NC. Therefore, we can perform all of them in parallel. Note that we do not have to explicitly compute the transpose of transitions and formulas; we can simply swap arguments. □

Remark 1. Testing whether φ is locally closed is even simpler if the tester is also given annotations indicating for every clause φ_i and transition t which clause φ_j is supposed to satisfy $\varphi_i \rightsquigarrow_t \varphi_j$. This mapping is a byproduct of the procedure to compute a locally closed bi-separator, and so comes at no cost. □

7 Bi-separators for set-to-set unreachability

In most applications, one does not have to prove unreachability of one marking, but rather of a *set* of markings, usually defined by means of some simple linear constraints. We show that our approach can be extended to "set-to-set reachability", i.e. queries of the form $\exists \boldsymbol{m}_{\text{src}} \in A, \boldsymbol{m}_{\text{tgt}} \in B : \boldsymbol{m}_{\text{src}} \rightarrow^* \boldsymbol{m}_{\text{tgt}}$, which we denote by $A \rightarrow^* B$. We focus on the case where sets A and B are described by conjunctions of atomic propositions; in other words, A and B are convex polytopes defined as intersections of half-spaces. In particular, this includes "coverability" queries which are important in practice, i.e. where A is a singleton and B is of the form $\{\boldsymbol{m} : \boldsymbol{m} \geq \boldsymbol{b}\}$. More generally, our approach can directly be adapted to convex linear Horn constraints, which is a fragment of linear arithmetic that extends linear programs and that captures the expressiveness of continuous Petri nets [6].

As shown in [6, Lem. 3.7], given an atomic proposition $\psi = (\boldsymbol{ax} \sim b)$, one can construct (in logarithmic space) a Petri net $\mathcal{N}_\psi$ and some $\boldsymbol{y} \in \{0, 1\}^5$ such that $\psi(\boldsymbol{x})$ holds iff $(\boldsymbol{x}, \boldsymbol{y}) \rightarrow^* (\boldsymbol{0}, \boldsymbol{0})$ in $\mathcal{N}_\psi$. The idea—depicted in Figure 2, which is adapted from [6, Fig. 1])—is simply to cancel out positive and negative coefficients of ψ. It is straightforward to adapt this construction to a conjunction $\bigwedge_{1 \leq i \leq k} \psi_k(\boldsymbol{x})$ of atomic propositions. Indeed, it suffices to make k copies of the gadget, but where places $\{p_1, \ldots, p_n\}$ and transitions $\{t_1, \ldots, t_n\}$ are shared. In this more general setting, t_i consumes from p_i and simultaneously spawns the respective coefficient to each copy. In summary, the following holds:

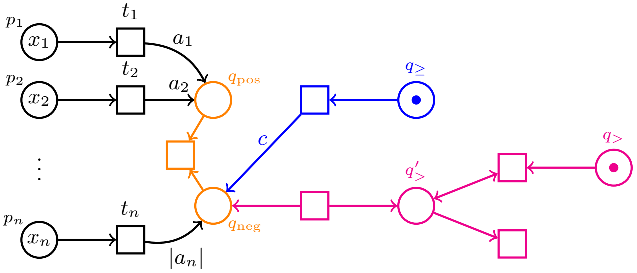

Fig. 2. Petri net for $\psi(\boldsymbol{x}) = (a_1 \cdot x_1 + \cdots + a_n \cdot x_n > c)$ where $a_1, a_2, c > 0$ and $a_n < 0$.

Proposition 13. *Given a conjunction of atomic propositions φ, it is possible to construct, in logarithmic space, a Petri net $\mathcal{N}_\varphi$ and $\boldsymbol{y} \in \{0,1\}^{5k}$ such that $\varphi(\boldsymbol{x})$ holds iff $(\boldsymbol{x}, \boldsymbol{y}) \rightarrow^* (\boldsymbol{0}, \boldsymbol{0})$ in $\mathcal{N}_\varphi$.*

With the previous construction in mind, we can reformulate any set-to-set reachability query into a standard ("marking-to-marking") reachability query.

Proposition 14. *Given a Petri net $\mathcal{N}$ and convex polytopes A and B described as conjunctions of atomic propositions, one can construct, in log. space, a Petri net $\mathcal{N}'$ and markings $\boldsymbol{m}_{src}$ and $\boldsymbol{m}_{tgt}$ s.t. $A \rightarrow^* B$ in $\mathcal{N}$ iff $\boldsymbol{m}_{src} \rightarrow^* \boldsymbol{m}_{tgt}$ in $\mathcal{N}'$.*

Proof. Let $\mathcal{N} = (P, T, \mathbf{F}_-, \mathbf{F}_+)$ where $P = \{p_1, \ldots, p_n\}$. Let us describe $\mathcal{N}' = (P', T', \mathbf{F}'_-, \mathbf{F}'_+)$ with the help of Figure 3. The Petri net $\mathcal{N}'$ extends $\mathcal{N}$ as follows:

- we add transitions $\{t_1, \ldots, t_n\}$ whose purpose is to nondeterministically guess an initial marking of $\mathcal{N}$ in P, and make a copy in $P' := \{p'_1, \ldots, p'_n\}$;
- we add a gadget, obtained from Proposition 13, to test whether the marking in P' belongs to A; and we add a gadget, obtained from Proposition 13, to test whether the marking in P belongs to B.

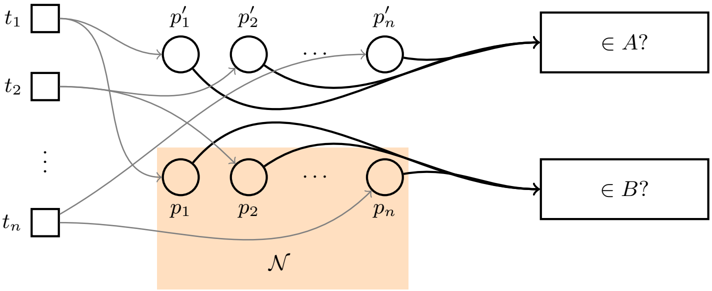

Fig. 3. Reduction from set-to-set reachability to (marking-to-marking) reachability.

The Petri net $\mathcal{N}'$ is *intended* to work sequentially as follows: (1) guess the initial marking $\boldsymbol{m}$ of $\mathcal{N}$; (2) execute $\mathcal{N}$ on $\boldsymbol{m}$ and reach a marking $\boldsymbol{m}'$; and (3) test whether $\boldsymbol{m} \in A$ and $\boldsymbol{m}' \in B$. If $\mathcal{N}'$ follows this order, then it is straightforward to see that $A \rightarrow^* B$ in $\mathcal{N}$ iff $(\mathbf{0}, \mathbf{0}, \boldsymbol{y}, \boldsymbol{y}') \rightarrow^* (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0})$ in $\mathcal{N}'$, where $\boldsymbol{y}$ and $\boldsymbol{y}'$ are obtained from Proposition 13. However, $\mathcal{N}'$ may interleave the different phases.[4] Nonetheless, this is not problematic, as any run of $\mathcal{N}'$ can be reordered in such a way that all three phases are consecutive. Indeed, phase (1) only produces tokens in $P \cup P'$, and phase (3) only consumes tokens from $P \cup P'$. □

As a consequence of Proposition 14, combined with Theorems 2 and 3, we obtain the following corollary:

Corollary 1. *A negative answer to a convex polytope query $A \rightarrow^* B$ is witnessed by a locally closed bi-separator computable in polynomial time and checkable in NC.*

8 Conclusion

We have shown that continuous Petri nets admit locally closed bi-separators that can be efficiently computed. These separators are succinct and very efficiently checkable certificates of unreachability. In particular, checking that a linear formula is a locally closed bi-separator is in NC, and only requires to solve linear inequations in one variable over the nonnegative reals.

Verification tools that have not been formally verified, or rely (as is usually the case) on external packages for linear arithmetic, can apply our results to provide certificates for their output. Further, our separators can be used as explanations of why a certain marking is unreachable. Obtaining minimal explanations is an interesting research avenue.

From a logical point of view, separators are very closely related to interpolants for linear arithmetic, which are widely used in formal verification to refine abstractions in the CEGAR approach [3,17,18,1]. We intend to explore whether they can constitute the basis of a CEGAR approach for the verification of continuous Petri nets.

Acknowledgments. We thank the anonymous referees for their comments, and in particular for suggesting a more intuitive definition of bi-separator.

References

1. Althaus, E., Beber, B., Kupilas, J., Scholl, C.: Improving interpolants for linear arithmetic. In: Proc. 13th International on Automated Technology for Verification and Analysis (ATVA). pp. 48–63 (2015). https://doi.org/10.1007/978-3-319-24953-7_5

[4] It is tempting to implement a lock, but this only works under discrete semantics.

2. Baumann, P., Majumdar, R., Thinniyam, R.S., Zetzsche, G.: Context-bounded verification of liveness properties for multithreaded shared-memory programs. Proceedings of the ACM on Programming Languages (PACMPL) **5**, 1–31 (2021). https://doi.org/10.1145/3434325
3. Beyer, D., Zufferey, D., Majumdar, R.: Csisat: Interpolation for LA+EUF. In: Proc. 20th International Conference on Computer Aided Verification (CAV). pp. 304–308 (2008). https://doi.org/10.1007/978-3-540-70545-1_29
4. Blondin, M., Esparza, J., Helfrich, M., Kucera, A., Meyer, P.J.: Checking qualitative liveness properties of replicated systems with stochastic scheduling. In: Proc. 32nd International Conference on Computer Aided Verification (CAV). vol. 12225, pp. 372–397 (2020). https://doi.org/10.1007/978-3-030-53291-8_20
5. Blondin, M., Finkel, A., Haase, C., Haddad, S.: The logical view on continuous Petri nets. ACM Transactions on Computational Logic (TOCL) **18**(3), 24:1–24:28 (2017). https://doi.org/10.1145/3105908
6. Blondin, M., Haase, C.: Logics for continuous reachability in Petri nets and vector addition systems with states. In: Proc. 32^{nd} Annual ACM/IEEE Symposium on Logic in Computer Science (LICS). pp. 1–12 (2017). https://doi.org/10.1109/LICS.2017.8005068
7. Czerwinski, W., Orlikowski, L.: Reachability in vector addition systems is Ackermann-complete. In: Proc. 62^{nd} Annual IEEE Symposium on Foundations of Computer Science (FOCS) (2021), to appear
8. David, R., Alla, H.: Discrete, Continuous, and Hybrid Petri nets. Springer, 2 edn. (2010)
9. Desel, J., Esparza, J.: Free choice Petri nets. No. 40, Cambridge University Press (1995)
10. Esparza, J., Helfrich, M., Jaax, S., Meyer, P.J.: Peregrine 2.0: Explaining correctness of population protocols through stage graphs. In: Proc. 18th International Symposium on Automated Technology for Verification and Analysis (ATVA). vol. 12302, pp. 550–556 (2020). https://doi.org/10.1007/978-3-030-59152-6_32
11. Feng, Y., Martins, R., Wang, Y., Dillig, I., Reps, T.W.: Component-based synthesis for complex APIs. In: Proc. 44th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL). pp. 599–612. ACM (2017). https://doi.org/10.1145/3009837.3009851
12. Fraca, E., Haddad, S.: Complexity analysis of continuous Petri nets. Fundamenta Informaticae **137**(1), 1–28 (2015). https://doi.org/10.3233/FI-2015-1168
13. German, S.M., Sistla, A.P.: Reasoning about systems with many processes. Journal of the ACM **39**(3), 675–735 (1992). https://doi.org/10.1145/146637.146681
14. Leroux, J.: Vector addition systems reachability problem (A simpler solution). In: Turing-100 – The Alan Turing Centenary. vol. 10, pp. 214–228 (2012). https://doi.org/10.29007/bnx2
15. Leroux, J.: The reachability problem for Petri nets is not primitive recursive. In: Proc. 62^{nd} Annual IEEE Symposium on Foundations of Computer Science (FOCS) (2021), to appear
16. Leroux, J., Schmitz, S.: Reachability in vector addition systems is primitive-recursive in fixed dimension. In: Proc. 34th Symposium on Logic in Computer Science (LICS). pp. 1–13 (2019). https://doi.org/10.1109/LICS.2019.8785796
17. Rybalchenko, A., Sofronie-Stokkermans, V.: Constraint solving for interpolation. Journal of Symbolic Computation **45**(11), 1212–1233 (2010). https://doi.org/10.1016/j.jsc.2010.06.005

18. Scholl, C., Pigorsch, F., Disch, S., Althaus, E.: Simple interpolants for linear arithmetic. In: Proc. Conference & Exhibition on Design, Automation & Test in Europe (DATE). pp. 1–6 (2014). https://doi.org/10.7873/DATE.2014.128

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.