Logical Methods in Computer Science
Volume 20, Issue 1, 2024, pp. 15:1–15:24
https://lmcs.episciences.org/

Submitted Sep. 08, 2022
Published Feb. 21, 2024

SEPARATORS IN CONTINUOUS PETRI NETS

MICHAEL BLONDIN [a] AND JAVIER ESPARZA [b]

[a] Université de Sherbroke, Sherbrooke, Canada
e-mail address: michael.blondin@usherbrooke.ca

[b] Technical University of Munich, Munich, Germany
e-mail address: 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 worst-case size, which is at least Ackermannian, and the complexity of checking that a formula is a separator, which is at least exponential (in the formula size).

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 unreachability, which is P-complete).

We further consider the more general problem of (existential) set-to-set reachability, where two sets of markings are given as convex polytopes. We show that, while our approach does not extend directly, we can efficiently certify unreachability via an altered Petri net.

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 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. [GS92, FMW$^+$17, BMTZ21]).

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 [Ler12]. 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;

Key words and phrases: Petri net and continuous reachability and separators and certificates.

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).

LOGICAL METHODS IN COMPUTER SCIENCE
DOI:10.46298/LMCS-20(1:15)2024

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 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, strictly lower complexity than deciding reachability. This does not hold, at least in the worst-case, for the separators of [Ler12]: In the worst case, the separator has a size at least Ackermannian in the Petri net size (a consequence of the fact that the reachability problem is Ackermann-complete [LS19, Ler21, CO21]) and the complexity of the check is at least 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 [DA10], 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 [FH15], 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. [BFHH17, BEH$^+$20, EHJM20]).

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 [BFHH17] 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. Namely, 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 $\mathit{sep}_{\boldsymbol{m}_{\text{src}}}(\boldsymbol{m}) \coloneqq \neg \mathit{reach}(\boldsymbol{m}_{\text{src}}, \boldsymbol{m})$ is a separator. Further, $\mathit{reach}(\boldsymbol{m}, \boldsymbol{m}')$ has only linear size. However, these separators do not satisfy property (2). Indeed, while the reachability problem for continuous Petri nets is P-complete [FH15], 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 [BFHH17] 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 strictly[1] 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

[1]Assuming P $\neq$ NC.

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 [FH15] 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.

We further consider "set-to-set reachability" where one must determine whether there exists a marking $\boldsymbol{m}_{\text{src}} \in A$ that can reach some marking $\boldsymbol{m}_{\text{tgt}} \in B$. This naturally generalizes the case where $A = \{\boldsymbol{m}_{\text{src}}\}$ and $B = \{\boldsymbol{m}_{\text{tgt}}\}$. We focus on the case where sets A and B are convex polytopes, as it can be solved in polynomial time for continuous Petri nets [BH17]. We prove that, unfortunately, we cannot validate locally closed separators in NC for set-to-set reachability. Nonetheless, we show that we can efficiently construct and validate locally closed separators (respectively in P and NC), at the cost of working with an altered Petri net that encodes A and B.

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 [FH15], and derives a characterization of *un*reachability suitable for finding bi-separators. Section 4 shows that checking the separators derivable from [BFHH17] 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 the limitation and extension of our approach to set-to-set reachability.

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). Given $a, b \in \mathbb{N}$, we write $[a..b]$ to denote $\{a, a+1, \ldots, b\}$. 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 $\text{supp}(\boldsymbol{x}) \coloneqq \{s \in S : \boldsymbol{x}(s) > 0\}$. We write $\boldsymbol{x}(S) \coloneqq \sum_{s \in S} \boldsymbol{x}(s)$. The *transpose* of a binary relation $\mathcal{R}$ is $\mathcal{R}^\mathsf{T} \coloneqq \{(y, x) : (x, y) \in \mathcal{R}\}$.

Petri nets. A *Petri net*[2] 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 $\boldsymbol{m} \in \mathbb{R}_+^P$. For every $Q \subseteq P$, let $\boldsymbol{m}(Q) \coloneqq \sum_{p \in Q} \boldsymbol{m}(p)$. 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

[2] 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.

it is α-enabled for some real number $\alpha > 0$. We define $\mathbf{F} \coloneqq \mathbf{F}_+ - \mathbf{F}_-$ and $\Delta_t \coloneqq \mathbf{F} \cdot \boldsymbol{e}_t$. In particular, $\boldsymbol{m} \xrightarrow{\alpha t} \boldsymbol{m}'$ implies $\boldsymbol{m}' = \boldsymbol{m} + \alpha\Delta_t$. 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):

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

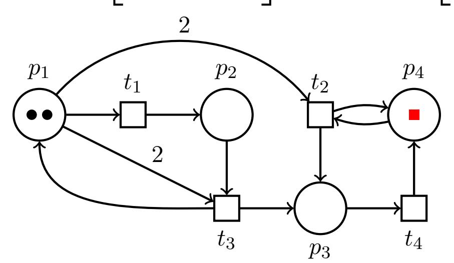


Figure 1: A Petri net and two markings $\boldsymbol{m}_{\text{src}} = \{p_1 \mapsto 2, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 0\}$ (black circles) and $\boldsymbol{m}_{\text{tgt}} = \{p_1 \mapsto 0, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 1\}$ (colored squares).

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

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

We write $\boldsymbol{m} \to \boldsymbol{m}'$ to denote that $\boldsymbol{m} \xrightarrow{\alpha t} \boldsymbol{m}'$ for some transition t and some $\alpha > 0$, and $\boldsymbol{m} \to^* \boldsymbol{m}'$ to denote that $\boldsymbol{m} \xrightarrow{\sigma} \boldsymbol{m}'$ for some firinng sequence σ.

The Petri net $\mathcal{N}_U$ is obtained by removing transitions $T \setminus U$ from $\mathcal{N}$. In particular, $\boldsymbol{m} \to^{U^*} \boldsymbol{m}'$ holds in $\mathcal{N}$ iff $\boldsymbol{m} \to^* \boldsymbol{m}'$ holds in $\mathcal{N}_U$.

The *transpose* of $\mathcal{N} = (P, T, (\mathbf{F}_-, \mathbf{F}_+))$ is $\mathcal{N}^\mathsf{T} \coloneqq (P, T, (\mathbf{F}_+, \mathbf{F}_-))$. 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 $\mathcal{N}^\mathsf{T}$, where τ is the reverse of σ. For $U \subseteq T$, we write U^T to denote U in the context of $\mathcal{N}^\mathsf{T}$.

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. The lemma has many variants, of which we give just one (e.g. see [GM07, Proposition 6.4.3(iii)]):

Lemma 2.1 (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.*

We give some geometric intuition for this lemma. We consider only the case $n = m$. Let $\boldsymbol{y}$ be a vector satisfying $\boldsymbol{y} \geq \mathbf{0}$ (that is, $\boldsymbol{y}$ belongs to the positive orthant) and $\boldsymbol{b}^\mathsf{T}\boldsymbol{y} < 0$. The hyperplane H perpendicular to $\boldsymbol{y}$ divides the space into two half-spaces. Since $\boldsymbol{b}^\mathsf{T}\boldsymbol{y} < 0$, the vectors $\boldsymbol{y}$ and $\boldsymbol{b}$ lie in opposite half-spaces; we say that H *separates* $\boldsymbol{b}$ from $\boldsymbol{y}$. Further, since $\boldsymbol{y}$ belongs to the positive orthant, the complete positive orthant lies in the same half-space as $\boldsymbol{y}$. In other words, H separates $\boldsymbol{b}$ not only from $\boldsymbol{y}$, but from the positive orthant.

We argue that $\mathbf{A}^\mathsf{T}\boldsymbol{y} = \mathbf{0}$ holds for some $\boldsymbol{y}$ satisfying $\boldsymbol{y} \geq \mathbf{0}$ and $\boldsymbol{b}^\mathsf{T}\boldsymbol{y} < 0$ iff $\mathbf{A}\boldsymbol{x} \leq \boldsymbol{b}$ has no solution. It is the case that $\mathbf{A}^\mathsf{T}\boldsymbol{y} = \mathbf{0}$ holds for a vector $\boldsymbol{y}$ iff every column vector of $\mathbf{A}$ is perpendicular to $\boldsymbol{y}$, and so iff every column vector of $\mathbf{A}$ lies in H. Since H separates $\boldsymbol{y}$ and $\boldsymbol{b}$, and $\mathbf{A}\boldsymbol{x}$ is a linear combination of the columns of $\mathbf{A}$ for every vector $\boldsymbol{x}$, every column vector of $\mathbf{A}$ lies in H iff $\boldsymbol{b} - \mathbf{A}\boldsymbol{x}$ lies on the same half-space as $\boldsymbol{b}$ for every $\boldsymbol{x}$. Since H separates $\boldsymbol{b}$ from the positive orthant, this is the case iff $\boldsymbol{b} - \mathbf{A}\boldsymbol{x}$ is not in the positive orthant for any $\boldsymbol{x}$, and so iff $\mathbf{A}\boldsymbol{x} \leq \boldsymbol{b}$ has no 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 2.2. A *separator* for $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$ is a linear formula φ over $\mathbb{R}_+^P$ such that:

(1) $\boldsymbol{m}_{\text{src}} \in [\![\varphi]\!]$;
(2) φ is *forward invariant*, i.e., $\boldsymbol{m} \in [\![\varphi]\!]$ and $\boldsymbol{m} \to \boldsymbol{m'}$ implies $\boldsymbol{m'} \in [\![\varphi]\!]$; and
(3) $\boldsymbol{m}_{\text{tgt}} \notin [\![\varphi]\!]$.

It follows immediately from the definition that if there is 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 2.3. A linear formula φ over $\mathbb{R}_+^P \times \mathbb{R}_+^P$ 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 $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$ is a bi-invariant linear formula φ such that $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}) \in [\![\varphi]\!]$, $(\boldsymbol{m}_{\text{tgt}}, \boldsymbol{m}_{\text{tgt}}) \in [\![\varphi]\!]$ and $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}}) \notin [\![\varphi]\!]$.

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

Proposition 2.4. *Let* φ *be a bi-separator for* $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$*. The following holds:*

- $\psi(\boldsymbol{m}) \coloneqq \varphi(\boldsymbol{m}_{src}, \boldsymbol{m})$ *is a separator for* $(\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt})$ *in* $\mathcal{N}$*;*

- *$\psi'(\boldsymbol{m}) \coloneqq \varphi(\boldsymbol{m}, \boldsymbol{m}_{tgt})$ is a separator for $(\boldsymbol{m}_{tgt}, \boldsymbol{m}_{src})$ in $\mathcal{N}^\intercal$.*

Proof. It suffices to prove the first statement, the second is symmetric. We have $\boldsymbol{m}_{\text{src}} \in [\![\psi]\!]$ 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

Given a Petri net $\mathcal{N} = (P, T, F)$, a set of transitions $U \subseteq T$, and two markings $\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}} \in \mathbb{R}_+^P$, we write $\boldsymbol{m}_{\text{src}} \hookrightarrow^U \boldsymbol{m}_{\text{tgt}}$ to denote that $\boldsymbol{m}_{\text{src}} \xrightarrow{\sigma} \boldsymbol{m}_{\text{tgt}}$ for some sequence σ with support U. In words, $\boldsymbol{m}_{\text{src}} \xrightarrow{\sigma} \boldsymbol{m}_{\text{tgt}}$ denotes that $\boldsymbol{m}_{\text{tgt}}$ can be reached from $\boldsymbol{m}_{\text{src}}$ by firing *all* transitions of U and *only* transitions of U. We say that $\boldsymbol{m}_{\text{tgt}}$ is *U-reachable* from $\boldsymbol{m}_{\text{src}}$

In [FH15], Fraca and Haddad gave the following characterization of U-reachability in continuous Petri nets:

Theorem 3.1 [FH15]**.** *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 $\boldsymbol{m}_{src} \hookrightarrow^U \boldsymbol{m}_{tgt}$ iff the following conditions hold:*
1. *some vector $\boldsymbol{x} \in \mathbb{R}_+^T$ with support U satisfies $\boldsymbol{m}_{src} + \mathbf{F}\boldsymbol{x} = \boldsymbol{m}_{tgt}$,*
2. *some firing sequence σ with support U is enabled at $\boldsymbol{m}_{src}$, and*
3. *some firing sequence τ with support U is backward-enabled at $\boldsymbol{m}_{tgt}$.*

Furthermore, these conditions can be checked in polynomial time.

Theorem 3.1 provides a witness of U-reachability in the shape of a vector $\boldsymbol{x}$ and two firing sequences σ and τ. In this section, we find a witness of U-unreachability, i.e., a witness showing that $\boldsymbol{m}_{\text{src}} \not\hookrightarrow^U \boldsymbol{m}_{\text{tgt}}$.

Consider the logical form of Theorem 3.1:

$$\begin{gathered} \boldsymbol{m}_{\text{src}} \hookrightarrow^U \boldsymbol{m}_{\text{tgt}} \\ \iff (\exists \boldsymbol{x} \in \mathbb{R}_+^T \colon A_1(\boldsymbol{x})) \land (\exists \sigma \in T^* \colon A_2(\sigma)) \land (\exists \tau \in T^* \colon A_3(\tau)), \end{gathered} \tag{3.1}$$

where $A_1(\boldsymbol{x}), A_2(\sigma), A_3(\tau)$ denote that $\boldsymbol{x}$ has support U and satisfies $\boldsymbol{m}_{\text{src}} + \mathbf{F}\boldsymbol{x} = \boldsymbol{m}_{\text{tgt}}$, that σ has support U and is enabled at $\boldsymbol{m}_{\text{src}}$, and that τ has support U and is backward-enabled at $\boldsymbol{m}_{\text{tgt}}$, respectively. The theorem is logically equivalent to

$$\begin{gathered} \boldsymbol{m}_{\text{src}} \not\hookrightarrow^U \boldsymbol{m}_{\text{tgt}} \\ \iff (\forall \boldsymbol{x} \in \mathbb{R}_+^T \colon \neg A_1(\boldsymbol{x})) \lor (\forall \sigma \in T^* \colon \neg A_2(\sigma)) \lor (\forall \tau \in T^* \colon \neg A_3(\tau)). \end{gathered} \tag{3.2}$$

To obtain a witness of U-unreachability, we proceed in two steps:
- In Section 3.1, we define predicates $B_2(Q)$ and $B_3(R)$, where $Q, R \subseteq P$, satisfying

$$\begin{gathered} (\forall \sigma \in T^* \colon \neg A_2(\sigma)) \iff (\exists Q \subseteq P \colon B_2(Q)), \\ (\forall \tau \in T^* \colon \neg A_3(\tau)) \iff (\exists R \subseteq P \colon B_3(R)). \end{gathered} \tag{3.3}$$

- In Section 3.2, we define a predicate $B_1(\boldsymbol{y})$, where $\boldsymbol{y} \in \mathbb{R}_+^P$, satisfying

$$(\forall \boldsymbol{x} \in \mathbb{R}_+^T \colon \neg A_1(\boldsymbol{x})) \implies (\exists \boldsymbol{y} \in \mathbb{R}_+^P \colon B_1(\boldsymbol{y})) \implies \boldsymbol{m}_{\text{src}} \not\hookrightarrow^U \boldsymbol{m}_{\text{tgt}}. \tag{3.4}$$

Here, a remark is in order. Observe that we do not claim that "$\forall \boldsymbol{x} \in \mathbb{R}_+^T \colon \neg A_1(\boldsymbol{x})$" is equivalent to "$\exists \boldsymbol{y} \in \mathbb{R}_+^P \colon B_1(\boldsymbol{y})$." Rather, we claim that the former implies the latter, and the latter implies U-unreachability.

Altogether, applying propositional logic to (3.2), (3.3), and (3.4) we obtain:

$$\begin{aligned} &\boldsymbol{m}_{\text{src}} \not\to^U \boldsymbol{m}_{\text{tgt}} \\ \iff &(\exists \boldsymbol{y} \in \mathbb{R}_+^P \colon B_1(\boldsymbol{y})) \lor (\exists Q \subseteq P \colon B_2(Q)) \lor (\exists R \subseteq P \colon B_3(R)). \end{aligned} \tag{3.5}$$

This shows that U-unreachability is witnessed either by a vector $\boldsymbol{y}$, a set Q, or a set R.

3.1. **The predicates $B_2(Q)$ and $B_3(R)$.** The predicates $B_2(Q)$ and $B_3(R)$ were already implicitly defined in [FH15] in terms of sets of places called *siphons* and *traps*. 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 $\boldsymbol{m} \to \boldsymbol{m}'$, then $\boldsymbol{m}(Q) = 0$ implies $\boldsymbol{m}'(Q) = 0$, and $\boldsymbol{m}(R) > 0$ implies $\boldsymbol{m}'(R) > 0$. Fraca and Haddad proved in [FH15]:

Proposition 3.2 [FH15]**.** *Let $\mathcal{N} = (P, T, F)$ be a Petri net, let $U \subseteq T$, and let $\boldsymbol{m} \in \mathbb{R}_+^P$. The following statements hold:*

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

The if-direction of the proposition is easy to prove. A siphon Q of $\mathcal{N}_U$ satisfies $Q^\bullet \subseteq U$. Since Q is empty at $\boldsymbol{m}$, if we only fire transitions from U 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 U have fired first. But no such firing sequence has support U, and we are done. The case of traps is analogous. For the only-if direction, we refer the reader to [FH15].

By Proposition 3.2, the predicates

$$\begin{aligned} B_2(Q) &\coloneqq Q \text{ is a siphon of } \mathcal{N}_U \text{ such that } Q^\bullet \neq \emptyset \text{ and } \boldsymbol{m}_{\text{src}}(Q) = 0, \\ B_3(R) &\coloneqq R \text{ is a trap of } \mathcal{N}_U \text{ such that } {}^\bullet R \neq \emptyset \text{ and } \boldsymbol{m}_{\text{tgt}}(R) = 0, \end{aligned}$$

satisfy (3.3).

3.2. **The predicate $B_1(\mathbf{y})$.** In order to define the predicate $B_1(\boldsymbol{y})$, we need to introduce *exclusion functions.*

Definition 3.3. Let $\mathcal{N} = (P, T, F)$ be a Petri net, let $\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}} \in \mathbb{R}_+^P$ and let $S \subseteq S' \subseteq T$. An *exclusion function for* (S, S') is a function $f \colon \mathbb{R}_+^P \to \mathbb{R}$ such that

(1) for all $t \in S'$, if $\boldsymbol{m} \xrightarrow{t} \boldsymbol{m}'$ then $f(\boldsymbol{m}) \leq f(\boldsymbol{m}')$; and
(2) either $f(\boldsymbol{m}_{\text{src}}) > f(\boldsymbol{m}_{\text{tgt}})$, or $f(\boldsymbol{m}_{\text{src}}) = f(\boldsymbol{m}_{\text{tgt}})$ and there exists $t \in S$ such that if $\boldsymbol{m} \xrightarrow{t} \boldsymbol{m}'$ then $f(\boldsymbol{m}) < f(\boldsymbol{m}')$.

An *exclusion function for* S is an exclusion function for (S, S). An exclusion function $f\colon \mathbb{R}_+^P \to \mathbb{R}$ is *linear* if there exists a vector $\boldsymbol{y} \in \mathbb{R}^P$ such that $f(\boldsymbol{m}) = \sum_{p \in P} \boldsymbol{y}(p) \cdot \boldsymbol{m}(p)$ for every $\boldsymbol{m} \in \mathbb{R}_+^P$. Abusing language, we speak of the linear exclusion function $\boldsymbol{y}$.

We define:

$$B_1(\boldsymbol{y}) \coloneqq \boldsymbol{y} \text{ is a linear exclusion function for } U.$$

We can easily show the second implication of (3.4), namely that an exclusion function for U is a witness of U-unreachabilty:

Lemma 3.4. *If there exists a (linear) exclusion function for* $U \subseteq T$*, then* $\boldsymbol{m}_{src} \not\to^U \boldsymbol{m}_{tgt}$.

Proof. Let f be an exclusion function for U. Call $f(\boldsymbol{m})$ the *value* of $\boldsymbol{m}$. By the definition of an exclusion function, either $\boldsymbol{m}_{\text{tgt}}$ has lower value than $\boldsymbol{m}_{\text{src}}$ and no transition of U decreases the value, or $\boldsymbol{m}_{\text{src}}$ and $\boldsymbol{m}_{\text{tgt}}$ have the same value, no transition of U decreases the value, and at least one transition of U 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 U. □

The first implication of (3.4) is shown in the forthcoming Proposition 3.6. We first need a technical lemma, one of the many consequences of Farkas' lemma. Recall that, given $\sim \in \{\leq, =, \geq\}$, the notation $\boldsymbol{x} \sim_U \boldsymbol{y}$ stands for "$\boldsymbol{x}(t) \sim \boldsymbol{y}(t)$ for all $t \in U$".

Lemma 3.5. *The system* $\exists \boldsymbol{x} \geq \mathbf{0} : \mathbf{A}\boldsymbol{x} = \boldsymbol{b} \wedge U \subseteq \text{supp}(\boldsymbol{x}) \subseteq V$ *has no solution iff this system has a solution:* $\exists \boldsymbol{y} : \mathbf{A}^\intercal \boldsymbol{y} \geq_V \mathbf{0} \wedge \boldsymbol{b}^\intercal \boldsymbol{y} \leq 0 \wedge \boldsymbol{b}^\intercal \boldsymbol{y} < \sum_{t \in U} (\mathbf{A}^\intercal \boldsymbol{y})(t)$.

Rather than giving a proof (which appears in the appendix), let us give some geometric intuition. Consider the case in which $\emptyset = U \subseteq V = T$. In this case, $U \subseteq \text{supp}(\boldsymbol{x}) \subseteq V$ holds vacuously, and we can replace "$\geq_V$" by "$\geq$" and "$\boldsymbol{b}^\intercal \boldsymbol{y} < \sum_{t \in U} (\mathbf{A}^\intercal \boldsymbol{y})(t)$" by "$\boldsymbol{b}^\intercal \boldsymbol{y} < 0$". The conditions can now be geometrically interpreted as follows:

(1) $\exists \boldsymbol{x} \geq \mathbf{0} : \mathbf{A}\boldsymbol{x} = \boldsymbol{b}$. The vector $\boldsymbol{b}$ lies in the cone spanned by the columns of $\mathbf{A}$.
(2) $\exists \boldsymbol{y} : \mathbf{A}^\intercal \boldsymbol{y} \geq \mathbf{0} \wedge \boldsymbol{b}^\intercal \boldsymbol{y} < 0$. There exists a hyperplane H (the hyperplane perpendicular to $\boldsymbol{y}$) such that all columns of $\mathbf{A}$ lie on the same side of the hyperplane as $\boldsymbol{y}$ (because $\mathbf{A}^\intercal \boldsymbol{y} \geq \mathbf{0}$), while $\boldsymbol{b}$ lies on the opposite side (because $\boldsymbol{b}^\intercal \boldsymbol{y} < 0$).

Clearly, the two conditions are incompatible. The conditions of the general case $U \subseteq V$ are similar, but restricted to the columns of $\mathbf{A}$ for which $\boldsymbol{x}$ is positive: (1) now states that $\boldsymbol{b}$ lies in the cone spanned by these columns, and (2) that some hyperplane separates these columns from $\boldsymbol{b}$.

We are now ready to prove the first implication of (3.4), namely

$$(\forall \boldsymbol{x} \in \mathbb{R}_+^T \colon \neg A_1(\boldsymbol{x})) \implies (\exists \boldsymbol{y} \in \mathbb{R}_+^P \colon \neg B_1(\boldsymbol{y})).$$

Recall that $A_1(\boldsymbol{x})$ means that $\boldsymbol{x}$ has support U and satisfies $\boldsymbol{m}_{\text{src}} + \mathbf{F}\boldsymbol{x} = \boldsymbol{m}_{\text{tgt}}$, and $B_1(\boldsymbol{y})$ means that $\boldsymbol{y}$ is a linear exclusion function for U. We prove a slightly more general result; the first implication of (3.4) is the special case $S = U = S'$:

Proposition 3.6. *Let* $\mathcal{N} = (P, T, F)$ *be a Petri net, let* $\boldsymbol{m}_{src}, \boldsymbol{m}_{tgt} \in \mathbb{R}_+^P$*, and let* $S \subseteq S' \subseteq T$*. If no vector* $\boldsymbol{x} \in \mathbb{R}_+^T$ *satisfies* $S \subseteq \text{supp}(\boldsymbol{x}) \subseteq S'$ *and* $\boldsymbol{m}_{src} + \mathbf{F}\boldsymbol{x} = \boldsymbol{m}_{tgt}$*, then there exists a linear exclusion function for* (S, S').

Proof. Assume no such $\boldsymbol{x} \in \mathbb{R}_+^T$ exists. Let $\boldsymbol{b} \coloneqq \boldsymbol{m}_{\text{tgt}} - \boldsymbol{m}_{\text{src}}$. By Lemma 3.5, 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 $f(\boldsymbol{k}) \coloneqq \boldsymbol{y}^\intercal \boldsymbol{k}$ is a linear exclusion function for (S, S').

(1) We have $f(\boldsymbol{m}_{\text{tgt}}) - f(\boldsymbol{m}_{\text{src}}) = \boldsymbol{y}^\mathsf{T}\boldsymbol{m}_{\text{tgt}} - \boldsymbol{y}^\mathsf{T}\boldsymbol{m}_{\text{src}} = \boldsymbol{y}^\mathsf{T}(\boldsymbol{m}_{\text{tgt}} - \boldsymbol{m}_{\text{src}}) = \boldsymbol{y}^\mathsf{T}\boldsymbol{b} = \boldsymbol{b}^\mathsf{T}\boldsymbol{y} \leq 0$, 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: $f(\boldsymbol{m}') = \boldsymbol{y}^\mathsf{T}\boldsymbol{m}' = \boldsymbol{y}^\mathsf{T}\boldsymbol{m} + \lambda(\boldsymbol{y}^\mathsf{T}\mathbf{F})\boldsymbol{e}_s = \boldsymbol{y}^\mathsf{T}\boldsymbol{m} + \lambda(\mathbf{F}^\mathsf{T}\boldsymbol{y})^\mathsf{T}\boldsymbol{e}_s \geq \boldsymbol{y}^\mathsf{T}\boldsymbol{m} = f(\boldsymbol{m})$, where the inequality follows from $\lambda > 0$, $\mathbf{F}^\mathsf{T}\boldsymbol{y} \geq_{S'} \mathbf{0}$ and $s \in S'$.

(3) Recall that $\boldsymbol{b}^\mathsf{T}\boldsymbol{y} \leq 0$ and $\sum_{s \in S}(\mathbf{F}^\mathsf{T}\boldsymbol{y})_s > \boldsymbol{b}^\mathsf{T}\boldsymbol{y}$. If the latter sum equals zero, then $\boldsymbol{b}^\mathsf{T}\boldsymbol{y} < 0$, and hence we are done since $f(\boldsymbol{m}_{\text{tgt}}) - f(\boldsymbol{m}_{\text{src}}) = \boldsymbol{b}^\mathsf{T}\boldsymbol{y} < 0$.

Otherwise, we have $\sum_{s \in S}(\mathbf{F}^\mathsf{T}\boldsymbol{y})_s > 0$ since $S \subseteq S'$ and $\mathbf{F}^\mathsf{T}\boldsymbol{y} \geq_{S'} \mathbf{0}$. Therefore, there exists a transition $s \in S$ such that $(\mathbf{F}^\mathsf{T}\boldsymbol{y})_s > 0$. Let $\boldsymbol{m} \xrightarrow{s} \boldsymbol{m}'$. We have $\boldsymbol{m}' = \boldsymbol{m} + \lambda\mathbf{F}\boldsymbol{e}_s$ for some $\lambda > 0$. Thus, $f(\boldsymbol{m}') = \boldsymbol{y}^\mathsf{T}\boldsymbol{m} + \lambda(\mathbf{F}^\mathsf{T}\boldsymbol{y})^\mathsf{T}\boldsymbol{e}_s > \boldsymbol{y}^\mathsf{T}\boldsymbol{m} = f(\boldsymbol{m})$, where the inequality holds by $\lambda > 0$ and $(\mathbf{F}^\mathsf{T}\boldsymbol{y})_s > 0$. □

Putting together Theorem 3.1 with Proposition 3.2, and Proposition 3.6, we obtain the following characterization of unreachability:

Proposition 3.7. *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 $\boldsymbol{m}_{src} \not\hookrightarrow^U \boldsymbol{m}_{tgt}$ iff*

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

This proposition shows that we can produce a witness of unreachability for a given support either as an exclusion function, a siphon, or a trap. The following example shows how to use this to show that a marking cannot be reached from another one.

Example 3.8. Consider the Petri net of Figure 1, but with $\boldsymbol{m}_{\text{tgt}} \coloneqq \{p_1 \mapsto 0, p_2 \mapsto 0, p_3 \mapsto 1, p_4 \mapsto 0\}$ as target. We prove $\boldsymbol{m}_{\text{src}} \not\to^* \boldsymbol{m}_{\text{tgt}}$. For the sake of contradiction, assume $\boldsymbol{m}_{\text{src}} \hookrightarrow^U \boldsymbol{m}_{\text{tgt}}$ for some $U \subseteq T$. We proceed in several steps:

- *Claim:* $t_4 \notin U$. The function $f(\boldsymbol{m}) \coloneqq \boldsymbol{m}(p_4)$ 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. Therefore, $\boldsymbol{m}_{\text{tgt}}$ is reachable from $\boldsymbol{m}_{\text{src}}$ in $\mathcal{N}$ iff it is reachable from $\boldsymbol{m}_{\text{src}}$ in $\mathcal{N}_{T \setminus \{t_4\}}$.
- *Claim:* $t_2 \notin U$. The set $Q \coloneqq \{p_4\}$ 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 $Q^\bullet = \{t_2\}$. So $\boldsymbol{m}_{\text{tgt}}$ is reachable from $\boldsymbol{m}_{\text{src}}$ in $\mathcal{N}$ iff it is reachable from $\boldsymbol{m}_{\text{src}}$ in $\mathcal{N}_{T\setminus\{t_2,t_4\}}$
- *Claim:* $t_1, t_3 \notin U$. The set $R \coloneqq \{p_1, p_2\}$ 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, $\boldsymbol{m}_{\text{tgt}}$ is reachable from $\boldsymbol{m}_{\text{src}}$ in $\mathcal{N}$ iff it is reachable from $\boldsymbol{m}_{\text{src}}$ in $\mathcal{N}_\emptyset$. But this can only happen if $\boldsymbol{m}_{\text{src}} = \boldsymbol{m}_{\text{tgt}}$, which is not the case.

In the next section, we transform this collection of witnesses of unreachability into one single separator that can be used as certificate.

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 markings of $\mathcal{N}$. From [BFHH17], 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, [BFHH17, 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 $\varphi(\boldsymbol{m}) \coloneqq \psi(\boldsymbol{m}_{\text{src}}, \boldsymbol{m})$ 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 4.1. *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 (i.e., each atomic proposition $\boldsymbol{ax} \sim b$ is such that $b = 0$.)*

Proof. We give a reduction from the problem of determining whether a DNF boolean formula $\psi(x_1, \ldots, x_m)$ is a tautology. Since ψ is in DNF, we can test whether it is satisfiable in polynomial time. Obviously, if it is not, then it is not a tautology. Thus, we consider the case where ψ is satisfiable. We define ψ' as ψ but where literals are modified as follows: x_i becomes $\boldsymbol{m}(x_i) > 0$, and $\neg x_i$ becomes $\boldsymbol{m}(x_i) \leq 0$. We construct a Petri net $\mathcal{N} = (P, T, F)$, where $P = \{x_1, \ldots, x_m, p, q\}$, $T = \{t\}$, and t produces a token in p. Note that all places but p are disconnected. Let $\boldsymbol{m}_{\text{tgt}} \coloneqq \boldsymbol{0}$ and $\boldsymbol{m}_{\text{src}}$ be such that $\boldsymbol{m}_{\text{src}}(p) = \boldsymbol{m}_{\text{src}}(q) = 1$ and $(\boldsymbol{m}_{\text{src}}(x_1), \ldots, \boldsymbol{m}_{\text{src}}(x_n))$ encodes an (arbitrary) assignment that satisfies ψ. We claim that the following formula φ is a separator for $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$ iff ψ is a tautology:

$$\varphi(\boldsymbol{m}) \coloneqq (\boldsymbol{m}(p) \leq 0 \wedge \boldsymbol{m}(q) > 0) \vee (\boldsymbol{m}(p) > 0 \wedge \boldsymbol{m}(q) > 0 \wedge \psi'(\boldsymbol{m})).$$

As $\boldsymbol{m}_{\text{src}} \in [\![\varphi]\!]$ and $\boldsymbol{m}_{\text{tgt}} \notin [\![\varphi]\!]$, it suffices to show that φ is forward invariant iff ψ is a tautology

$\Rightarrow$) Let $(y_1, \ldots, y_m) \in \{0, 1\}^n$. We show that $\psi(y_1, \ldots, y_m)$ holds. Let $\boldsymbol{m}$ be such that $\boldsymbol{m}(p) = 0$, $\boldsymbol{m}(q) = 1$ and $\boldsymbol{m}(x_i) = y_i$ for every $i \in [1..m]$. We have $\boldsymbol{m} \in [\![\varphi]\!]$ since the first disjunct is satisfied. We can fire t in $\boldsymbol{m}$ which leads to a marking $\boldsymbol{m}'$ where $\boldsymbol{m}'(p) > 0$, $\boldsymbol{m}'(q) = 1$ and $\boldsymbol{m}'(x_i) = y_i$ for every $i \in [1..m]$. Since φ is forward invariant by assumption, we have $\boldsymbol{m}' \in [\![\varphi]\!]$. Since $\boldsymbol{m}'(p) > 0$ and $\boldsymbol{m}'(q) > 0$, this means that the second disjunct is satisfied. In particular, this means that $\psi'(\boldsymbol{m}')$ holds, and hence that $\psi(y_1, \ldots, y_m)$ holds.

$\Leftarrow$) Let $\boldsymbol{m} \in [\![\varphi]\!]$ and $\boldsymbol{m} \xrightarrow{\alpha t} \boldsymbol{m}'$. We have $\boldsymbol{m}(q) > 0$. By definition of t, we have $\boldsymbol{m}'(p) > 0$, and $\boldsymbol{m}'$ equal to $\boldsymbol{m}$ on all other places. Since ψ is a tautology, $\psi'(\boldsymbol{m})$ holds. Thus, $\boldsymbol{m}' \in [\![\varphi]\!]$ holds as the second disjunct is satisfied. □

Remark 4.2. The problem of determining whether a quantifier-free linear formula φ is a separator for $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$ is in coNP. Indeed, we can specify that a formula φ separates $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$ as follows:

$$\varphi(\boldsymbol{m}_{\text{src}}) \wedge \neg\varphi(\boldsymbol{m}_{\text{tgt}}) \wedge \forall \boldsymbol{m} \geq \boldsymbol{0}\ \forall \alpha > 0 \bigwedge_{t \in T} [\varphi(\boldsymbol{m}) \wedge \boldsymbol{m} \geq \alpha \Delta_t^-) \rightarrow \varphi(\boldsymbol{m} + \alpha \Delta_t)].$$

Membership follows since the universal fragment of linear arithmetic is in coNP [Son85].

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 $\boldsymbol{m}_{\text{src}} \not\rightarrow^* \boldsymbol{m}_{\text{tgt}}$, then some locally closed bi-separator for $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$ can be computed in polynomial time by solving at most $\mathcal{O}(|T|)$ linear programs;

- 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 4.3. 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 $t \in T^\mathsf{T}$ and every $i \in [1..n]$, there exists $j \in [1..n]$ s.t. $\varphi_i^\mathsf{T} \rightsquigarrow_t \varphi_j^\mathsf{T}$.

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

Proposition 4.4. *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 4.4 justifies the following definition:

Definition 4.5. A *locally closed bi-separator* for $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}})$ is a locally closed formula φ s.t. $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}) \in [\![\varphi]\!]$, $(\boldsymbol{m}_{\text{tgt}}, \boldsymbol{m}_{\text{tgt}}) \in [\![\varphi]\!]$ and $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}}) \notin [\![\varphi]\!]$.

Indeed, by Proposition 4.4, a locally closed bi-separator is a bi-separator, as the bi-invariance condition of Definition 2.3 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 5.1. *If $\boldsymbol{m}_{src} \not\to^{U^*} \boldsymbol{m}_{tgt}$, 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 $U = \emptyset$. There must exist $p \in P$ such that $\boldsymbol{m}_{\text{src}}(p) \neq \boldsymbol{m}_{\text{tgt}}(p)$. Take $\varphi(\boldsymbol{m}, \boldsymbol{m}') \coloneqq \boldsymbol{e}_p \boldsymbol{m} \leq \boldsymbol{e}_p \boldsymbol{m}'$ or $-\boldsymbol{e}_p \boldsymbol{m} \leq -\boldsymbol{e}_p \boldsymbol{m}'$, depending on whether $\boldsymbol{m}_{\text{src}}(p) > \boldsymbol{m}_{\text{tgt}}(p)$ or $\boldsymbol{m}_{\text{src}}(p) < \boldsymbol{m}_{\text{tgt}}(p)$.

Now, assume that $U \neq \emptyset$. We make a case distinction on whether the system

$$\exists \boldsymbol{x} \in \mathbb{R}_+^T : \boldsymbol{m}_{\text{src}} + \mathbf{F}\boldsymbol{x} = \boldsymbol{m}_{\text{tgt}} \wedge \operatorname{supp}(\boldsymbol{x}) \subseteq U \ .$$

has a solution. Suppose first that it has no solution. By Proposition 3.6, taking $S = \emptyset$ and $S' = U$, there is a linear exclusion function for $(\emptyset, U)$, i.e. a linear function f satisfying (1) $f(\boldsymbol{m}_{\text{src}}) > f(\boldsymbol{m}_{\text{tgt}})$, and (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 3.3 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 $\operatorname{supp}(\boldsymbol{x}) \subseteq U$ 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 $\operatorname{supp}(\boldsymbol{x}') \cup \operatorname{supp}(\boldsymbol{x}'')$. Let $U' \coloneqq \operatorname{supp}(\boldsymbol{x})$. For every $t \in U \setminus U'$, consider the system of Proposition 3.6 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 3.6 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 3.1 and Proposition 3.2, $Q^\bullet \cup {}^\bullet R \neq \emptyset$. 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

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

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

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

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

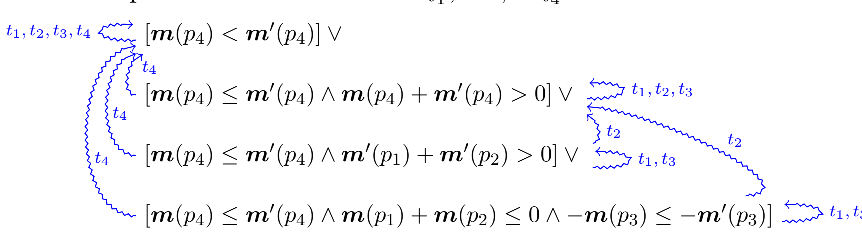
The same bounds holds for the number of atomic propositions per disjunct.

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 [DE95]. □

Example 5.2. Let us apply the construction of Theorem 5.1 to the Petri net and the markings of Example 3.8: $\boldsymbol{m}_{\text{src}} = \{p_1 \mapsto 2, p_2 \mapsto 0, p_3 \mapsto 0, p_4 \mapsto 0\}$ 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 $\rightsquigarrow_{t_1}, \ldots, \rightsquigarrow_{t_4}$:



As an example, consider transition t_4 and these atomic propositions occurring within φ:

$$\theta(\boldsymbol{m}, \boldsymbol{m}') \coloneqq \boldsymbol{m}(p_4) \leq \boldsymbol{m}'(p_4),$$
$$\theta'(\boldsymbol{m}, \boldsymbol{m}') \coloneqq \boldsymbol{m}(p_4) < \boldsymbol{m}'(p_4).$$

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. $\boldsymbol{m}_{\text{src}} \not\rightarrow^{U^*} \boldsymbol{m}_{\text{tgt}}$
Output: A locally closed bi-separator w.r.t. $\mathcal{N}_U$

```
bi-separator(U)
  if U = ∅ then
    pick p ∈ P such that m_src(p) ≠ m_tgt(p)
    return (am ≤ am') where a := sign(m_src(p) − m_tgt(p)) · e_p
  else
    b   := m_tgt − m_src
    X   := {x ∈ ℝ_+^T : Fx = b, supp(x) ⊆ U}
    Y_S := {y ∈ ℝ^P : Fᵀy ≥_U 0, bᵀy ≤ 0, bᵀy < Σ_{s∈S} (Fᵀy)_s}
    if X = ∅ then
      pick y ∈ Y_∅ and return (yᵀm ≤ yᵀm')
    else
      U' := {u ∈ U : x(u) > 0 for some x ∈ X}
      for t ∈ U \ U' do
        pick y_t ∈ Y_{t}; f_t(m) := y_tᵀm
        if f_t(m_src) > f_t(m_tgt) then  return (f_t(m) < f_t(m'))
      Q := largest siphon of N_U' such that m_src(Q) = 0
      R := largest trap    of N_U' such that m_tgt(R) = 0
      φ_inv := ⋀_{t∈U\U'} (f_t(m) ≤ f_t(m'))
      ψ_1 ∨ ··· ∨ ψ_m := bi-separator(U' \ (Q• ∪ •R))
      return ⋁_{t∈U\U'} φ_t(m, m') ∨ [φ_inv(m, m') ∧ m(Q) + m'(R) > 0] ∨
               ⋁_{1≤i≤m} [φ_inv(m, m') ∧ m(R) + m'(Q) ≤ 0 ∧ ψ_i(m, m')]
```

Given $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\theta]\!]$ and $\boldsymbol{m}' \xrightarrow{\alpha t_4} \boldsymbol{m}''$, we must have $\boldsymbol{m}'(p_4) < \boldsymbol{m}''(p_4)$ since t_4 produces in place p_4, and hence $(\boldsymbol{m}, \boldsymbol{m}'') \in [\![\theta']\!]$. Thus, by definition of t_4-implication, we have $\theta \rightsquigarrow_{t_4} \theta'$. This explains why the first clause of φ is t_4-implied by each clause of φ. Similar reasoning yields the other t_i-implications, which shows that φ is bi-invariant.

Recall that since φ is a locally closed bi-separator, taking $\psi(\boldsymbol{m}) := \varphi(\boldsymbol{m}_{\text{src}}, \boldsymbol{m})$ yields a forward separator. Since $\boldsymbol{m}_{\text{src}}(p_2) = \boldsymbol{m}_{\text{src}}(p_3) = \boldsymbol{m}_{\text{src}}(p_4) = 0$, several atomic propositions trivially hold. After making these simplifications, we obtain

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

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

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

The backward separator ψ' provides a much simpler proof of $\boldsymbol{m}_{\text{src}} \not\xrightarrow{*} \boldsymbol{m}_{\text{tgt}}$ than the one of Example 3.8. 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 $\boldsymbol{m}_{\text{tgt}}$.

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:

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

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 of ψ and ψ', 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 6.1 and 6.2, we will provide necessary and sufficient conditions for $X \subseteq Y$ to hold. In Proposition 6.3, we will show that these conditions are testable in NC. Then, in Proposition 6.4, 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 "$<$"):

Proposition 6.1. *Let $\boldsymbol{a}, \boldsymbol{a}', \boldsymbol{l} \in \mathbb{R}^n$ and $b' \in \mathbb{R}$. Let $X \coloneqq \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}\boldsymbol{x} \leq 0 \wedge \boldsymbol{x} \geq \boldsymbol{l}\}$ and $Y \coloneqq \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}'\boldsymbol{x} \leq b'\}$ 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 $-b' \leq (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l}$.*

Proof. The *conical hull* of a finite set V is defined as

$$\text{conic}(V) \coloneqq \left\{\sum_{\boldsymbol{v} \in V} \lambda_{\boldsymbol{v}} \boldsymbol{v} : \lambda_{\boldsymbol{v}} \in \mathbb{R}_+\right\}.$$

We first state a generalization of Farkas' lemma sometimes known as Haar's lemma (e.g. see [Sch86, p. 216]):

> Let $\mathbf{A} \in \mathbb{R}^{m \times n}$, $\boldsymbol{b} \in \mathbb{R}^m$, $\boldsymbol{a}' \in \mathbb{R}^n$ and $b' \in \mathbb{R}$ be such that $[\![\mathbf{A}\boldsymbol{x} \leq \boldsymbol{b}]\!] \neq \emptyset$. It is the case that $[\![\mathbf{A}\boldsymbol{x} \leq \boldsymbol{b}]\!] \subseteq [\![\boldsymbol{a}'\boldsymbol{x} \leq b]\!]$ iff $(\boldsymbol{a}', b') \in \text{conic}(\{(\boldsymbol{0}, 1)\} \cup \{(\mathbf{A}_i, \boldsymbol{b}_i) : i \in [1..m]\})$.

We now prove the proposition. Let

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

Note that $X = [\![\mathbf{A}\boldsymbol{x} \leq \boldsymbol{b}]\!]$. So, by Haar's lemma, we have $X \subseteq Y$ iff $(\boldsymbol{a}', b') \in \text{conic}(\{(\boldsymbol{0}, 1)\} \cup \{(\mathbf{A}_i, \boldsymbol{b}_i) : i \in [1..m]\})$. Consequently, we have:

$$\begin{aligned} X \subseteq Y &\iff \exists \lambda, \lambda_1, \ldots, \lambda_n \geq 0 : \boldsymbol{a}' = \lambda\boldsymbol{a} - \sum_{i=1}^n \lambda_i \boldsymbol{e}_i \text{ and } b' \geq -\sum_{i=1}^n \lambda_i \boldsymbol{l}_i \\ &\iff \exists \lambda \geq 0 : \lambda\boldsymbol{a} \geq \boldsymbol{a}' \text{ and } -b' \leq (\lambda\boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l}. \end{aligned}$$

□

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

Proposition 6.2. *Let $\boldsymbol{a}, \boldsymbol{a}' \in \mathbb{R}^n$, $b' \in \mathbb{R}$, $\boldsymbol{l} \geq \boldsymbol{0}$ and $\sim, \sim' \in \{\leq, <\}$. Let $X_\sim \coloneqq \{\boldsymbol{x} \geq \boldsymbol{l} : \boldsymbol{ax} \sim \boldsymbol{0}\}$ and $Y_{\sim'} \coloneqq \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{a}'\boldsymbol{x} \sim' b'\}$ 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 6.1. 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 $X_= \coloneqq X_\leq \setminus X_<$. 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 $\boldsymbol{x}'' \coloneqq \epsilon\boldsymbol{x} + (1-\epsilon)\boldsymbol{x}'$. 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 $\exists\boldsymbol{x} : \boldsymbol{x} \geq \boldsymbol{l} \wedge \boldsymbol{ax} \leq 0 \wedge \boldsymbol{a}'\boldsymbol{x} \geq b'$ has no solution. In matrix notation, the system corresponds to $\exists\boldsymbol{x} : \mathbf{A}\boldsymbol{x} \leq \boldsymbol{c}$ where

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

By Farkas' lemma (Lemma 2.1), $\mathbf{A}^\mathsf{T}\boldsymbol{y} = \boldsymbol{0}$ and $\boldsymbol{c}^\mathsf{T}\boldsymbol{y} < 0$ for some $\boldsymbol{y} \geq \boldsymbol{0}$. In other words,

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

Since $\boldsymbol{z} \geq \boldsymbol{0}$, we have $\lambda\boldsymbol{a} \geq \lambda'\boldsymbol{a}' \wedge -\lambda' b' < (\lambda\boldsymbol{a} - \lambda'\boldsymbol{a}')\boldsymbol{l}$. 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 $\lambda\boldsymbol{a} \geq \boldsymbol{0}$ 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:

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

(3) $\Rightarrow$) Since $X_< \subseteq Y_<$, this system has no solution: $\exists\boldsymbol{x} : \boldsymbol{x} \geq \boldsymbol{l} \wedge \boldsymbol{ax} < 0 \wedge \boldsymbol{a}'\boldsymbol{x} \geq b'$. The latter can be rephrased as $\exists\boldsymbol{x}, y : y \geq 1 \wedge \boldsymbol{x} \geq y\boldsymbol{l} \wedge \boldsymbol{ax} \leq -1 \wedge \boldsymbol{a}'\boldsymbol{x} \geq yb'$. In matrix

notation, this corresponds to $\exists \boldsymbol{x} : \mathbf{A}\boldsymbol{x} \leq \boldsymbol{c}$ where

$$\mathbf{A} \coloneqq \begin{bmatrix} -\mathbf{I} & \boldsymbol{l}^\top \\ \boldsymbol{a} & 0 \\ -\boldsymbol{a}' & b' \\ \mathbf{0} & -1 \end{bmatrix} \text{ and } \boldsymbol{c} \coloneqq \begin{pmatrix} \mathbf{0} \\ -1 \\ 0 \\ -1 \end{pmatrix}.$$

By Lemma 2.1, $\mathbf{A}^\top \boldsymbol{y} = \mathbf{0}$ and $\boldsymbol{c}^\top \boldsymbol{y} < 0$ for some $\boldsymbol{y} \geq \mathbf{0}$. In other words,

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

Since $\boldsymbol{z} \geq \mathbf{0}$, $\lambda \geq 0$ and $\lambda'' \geq 0$, we have:

$$\lambda \boldsymbol{a} \geq \lambda' \boldsymbol{a}' \land [(-\lambda' b' < (\lambda \boldsymbol{a} - \lambda' \boldsymbol{a}')\boldsymbol{l}) \lor (-\lambda' b' = (\lambda \boldsymbol{a} - \lambda' \boldsymbol{a}')\boldsymbol{l} \land \lambda > 0)].$$

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 either $0 < \lambda \boldsymbol{a}\boldsymbol{l}$ or $0 = \lambda \boldsymbol{a}\boldsymbol{\ell} \land \lambda > 0$. We necessarily have $\lambda > 0$ and $\boldsymbol{a} \geq \mathbf{0}$. Let $\boldsymbol{x} \in X_<$. We have $0 > \boldsymbol{a}\boldsymbol{x} \geq \boldsymbol{a}\boldsymbol{l} \geq 0$, which is a contradiction.

$\Leftarrow$) Let $\boldsymbol{x} \in X_<$. If $-b' < (\lambda \boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l}$ holds, then we get $\boldsymbol{x} \in Y_<$ as in Item 2. Otherwise, we have $-b' = (\lambda \boldsymbol{a} - \boldsymbol{a}')\boldsymbol{l}$ and $\lambda > 0$. Hence, we have:

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

Thus, $\boldsymbol{a}'\boldsymbol{x} < b'$ and hence $\boldsymbol{x} \in Y_<$ as desired. □

The conditions arising from Proposition 6.2 involve solving linear programs with *one* variable λ. It is easy to see that this problem is in NC:

Proposition 6.3. *Given $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Q}^n$ and $\boldsymbol{\sim} \in \{\leq, <\}^n$, testing $\exists \lambda \geq 0 : \boldsymbol{a}\lambda \boldsymbol{\sim} \boldsymbol{b}$ is in NC.*

Proof. Let $X_i \coloneqq \{\lambda \geq 0 : \boldsymbol{a}_i \lambda \boldsymbol{\sim}_i \boldsymbol{b}_i\}$. Let "${}_i\langle$" and "$\rangle_i$" denote "[" and "]" if $\boldsymbol{\sim}_i = \leq$, and "(" and ")" otherwise. Each X_i is an interval:

$$X_i = \begin{cases} \emptyset & \text{if } \boldsymbol{a}_i = 0 \text{ and } 0 \not\sim_i \boldsymbol{b}_i, \\ [0, \boldsymbol{b}_i/\boldsymbol{a}_i\rangle_i & \text{if } \boldsymbol{a}_i > 0, \\ {}_i\langle \boldsymbol{b}_i/\boldsymbol{a}_i, +\infty) & \text{if } \boldsymbol{a}_i < 0 \text{ and } \boldsymbol{b}_i \leq 0, \\ [0, +\infty) & \text{otherwise.} \end{cases}$$

We want to test whether $X_1 \cap \cdots \cap X_n \neq \emptyset$. Since arithmetic belongs to NC, it suffices to: (1) compute the left endpoint ℓ_i and the right endpoint r_i of each X_i in parallel; (2) compute $\ell \coloneqq \max(\ell_1, \ldots, \ell_n)$ and $r \coloneqq \min(r_1, \ldots, r_n)$; and (3) accept iff $\ell < r$, or $\ell = r$ and each X_i is closed on the left and the right. □

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 6.4. *Let $\varphi_\sim(\boldsymbol{m}, \boldsymbol{m}') \coloneqq \boldsymbol{a}\boldsymbol{m} \sim \boldsymbol{b}\boldsymbol{m}'$ where $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{R}^P$. It is the case that*

(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 $\boldsymbol{am} < \boldsymbol{bm}'$. It cannot be that $\boldsymbol{a} \geq \boldsymbol{0}$ and $\boldsymbol{b} \leq \boldsymbol{0}$, as otherwise $\boldsymbol{am} \geq 0 \geq \boldsymbol{bm}'$.

$\Leftarrow$) 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 $k \coloneqq (|\boldsymbol{b}\Delta_u^-| + 1)/|\boldsymbol{a}(p)|$; if $\boldsymbol{b}(p) > 0$, then $(\boldsymbol{0}, \Delta_u^- + k\boldsymbol{e}_p) \in [\![\varphi_<]\!]$ with $k \coloneqq (|\boldsymbol{b}\Delta_u^-| + 1)/\boldsymbol{b}(p)$.

(2) $\Rightarrow$) Let $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi_\leq]\!]$ be such that $\boldsymbol{m}'$ enables u. We have $\boldsymbol{m}' = \boldsymbol{x} + \alpha\Delta_u^-$ for some $\boldsymbol{x} \geq \boldsymbol{0}$ and $\alpha > 0$. Therefore, $\boldsymbol{am} \leq \boldsymbol{bx} + \alpha\boldsymbol{b}\Delta_u^-$. We assume that $\boldsymbol{b}\Delta_u^- < 0$, as we are otherwise trivially done. If $\boldsymbol{a} \geq \boldsymbol{0}$ and $-\boldsymbol{b} \geq \boldsymbol{0}$, then we obtain a contradiction since $\boldsymbol{am} \geq 0 > \boldsymbol{bx} + \alpha\boldsymbol{b}\Delta_u^-$.

$\Leftarrow$) It suffices to exhibit a pair $(\boldsymbol{m}, \boldsymbol{m}') \in [\![\varphi_\leq]\!]$ such that $\boldsymbol{m}' \geq \Delta_u^-$. If $\boldsymbol{b}\Delta_u^- \geq 0$, then we are done by taking $(\boldsymbol{0}, \Delta_u^-)$. Let us consider the second case where $\boldsymbol{b}\Delta_u^- < 0$ and $\boldsymbol{a}(p) < 0 \vee \boldsymbol{b}(p) > 0$ for some $p \in P$. Informally, we consider the pair $(\boldsymbol{0}, \Delta_u^-)$ and "fix" the value on the left-hand-side or right-hand side depending on whether $\boldsymbol{a}(p) < 0$ or $\boldsymbol{b}(p) > 0$. More formally, we are done by taking either the pair $(k\boldsymbol{e}_p, \Delta_u^-)$ where $k \coloneqq |\boldsymbol{b}\Delta_u^-|/|\boldsymbol{a}(p)|$, or the pair $(\boldsymbol{0}, \Delta_u^- + \ell\boldsymbol{e}_p)$ where $\ell \coloneqq |\boldsymbol{b}\Delta_u^-|/\boldsymbol{b}(p)$. □

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 6.5. *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 6.4, 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:

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

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 $\boldsymbol{k} \coloneqq \boldsymbol{m}/\alpha$, $\boldsymbol{k}' \coloneqq \boldsymbol{m}'/\alpha$ and $\boldsymbol{k}'' \coloneqq \boldsymbol{m}''/\alpha$. 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 6.2, 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 6.3, testing $X \subseteq Y$ can be done in NC. □

Theorem 6.6. *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"):

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

By Proposition 6.5, 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 6.7. 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 some 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. Thus, we now consider the more general setting of "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 $\{\boldsymbol{m} : \boldsymbol{m} \geq \boldsymbol{b}\}$.

It follows from [BH17] that testing whether $A \not\rightarrow^* B$ can be done in polynomial time. In this work, we have shown that, whenever A and B are singleton sets, we can validate a certificate for $A \not\rightarrow^* B$ in NC (and so with lower complexity). In the general case where either A or B is not a singleton, we could proceed similarly by constructing a (locally closed) bi-separator, as defined previously, but with the natural generalization that $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}) \in [\![\varphi]\!]$, $(\boldsymbol{m}_{\text{tgt}}, \boldsymbol{m}_{\text{tgt}}) \in [\![\varphi]\!]$ and $(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{tgt}}) \notin [\![\varphi]\!]$ *for every* $\boldsymbol{m}_{\text{src}} \in A$ and $\boldsymbol{m}_{\text{tgt}} \in B$.

Unfortunately, as we will show in Section 7.1, checking that a given linear formula is a (locally closed) bi-separator is coNP-hard. Nonetheless, in Section 7.2, we will show that one can construct a locally closed bi-separator on an *altered* Petri net with a single source and target marking.

7.1. **Hardness of checking set-to-set bi-separators.**

Proposition 7.1. *The problem of determining whether a given linear formula φ is a locally closed bi-separator for convex polytopes (A, B) is coNP-hard, even if (1) A is a singleton and B is of the form $\{\boldsymbol{m} : \boldsymbol{m} \geq \boldsymbol{b}\}$, or (2) vice versa.*

Proof of (1). We give a reduction from the problem of determining whether a DNF boolean formula $\psi = \bigvee_{j \in J} \psi_j(x_1, \ldots, x_m)$ is a tautology. As in the proof of Proposition 4.1, we define ψ'_j as ψ_j but where literals are modified as follows: x_i becomes $\boldsymbol{m}(x_i) > 0$, and $\neg x_i$ becomes $\boldsymbol{m}(x_i) \leq 0$.

Let $\mathcal{N} = (P, T, F)$ be the Petri net such that $P \coloneqq \{x_1, \ldots, x_m, y\}$, $T \coloneqq \{t\}$, and t consumes and produces a token in y. Let

$$\varphi(\boldsymbol{m}, \boldsymbol{m}') \coloneqq (\boldsymbol{m}'(y) \leq 0) \vee \bigvee_{j \in J} [\psi'_j(\boldsymbol{m}) \wedge \boldsymbol{m}(y) > 0].$$

Let $A \coloneqq \{\mathbf{0}\}$ and $B \coloneqq \{\boldsymbol{m}_{\text{tgt}} \in \mathbb{R}_+^P : \boldsymbol{m}_{\text{tgt}}(y) \geq 1\}$.

Note that φ is homogeneous. Moreover, transition t leaves markings unchanged, i.e. $\boldsymbol{m}' \to \boldsymbol{m}''$ implies $\boldsymbol{m}'' = \boldsymbol{m}'$, and likewise backward. Therefore, we trivially have $\theta \rightsquigarrow_t \theta$ and $\theta^\mathsf{T} \rightsquigarrow_t \theta^\mathsf{T}$ for every atomic proposition θ of φ. Further observe that $(\mathbf{0}, \mathbf{0}) \in [\![\varphi]\!]$ and $(\mathbf{0}, \boldsymbol{m}_{\text{tgt}}) \notin [\![\varphi]\!]$ for every $\boldsymbol{m}_{\text{tgt}} \in B$.

Consequently, φ satisfies all of the properties of a locally closed bi-separator for (A, B), except possibly the requirement that $(\boldsymbol{m}_{\text{tgt}}, \boldsymbol{m}_{\text{tgt}}) \in [\![\varphi]\!]$ for every $\boldsymbol{m}_{\text{tgt}} \in B$. The latter holds iff ψ is a tautology (since $\varphi(\boldsymbol{m}_{\text{tgt}}, \boldsymbol{m}_{\text{tgt}}) \equiv \bigvee_{j \in J} \varphi'_j(\boldsymbol{m}_{\text{tgt}})$). Thus, we are done. □

Proof of (2). This follows immediately from the fact that φ is a locally closed bi-separator for (A, B) in $\mathcal{N}$ iff φ^T is a locally closed bi-separator for (B, A) in $\mathcal{N}^\mathsf{T}$. □

7.2. **Certifying set-to-set unreachability.** As shown in [BH17, Lem. 3.7], given an atomic proposition $\psi = (\boldsymbol{a}\boldsymbol{x} \sim b)$, 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 $(\boldsymbol{x}, \boldsymbol{y}) \to^* (\mathbf{0}, \mathbf{0})$ in $\mathcal{N}_\psi$. The idea—depicted in Figure 2, which is adapted from [BH17, 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.

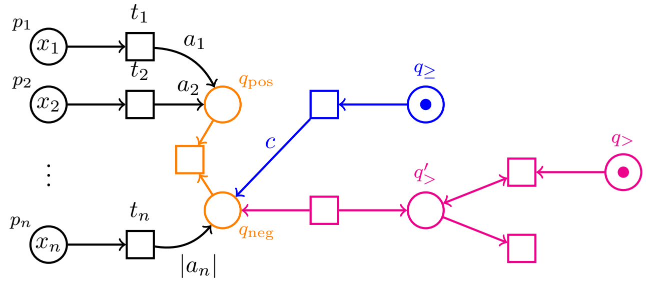


Figure 2: Petri net for $\psi(\boldsymbol{x}) = (a_1 \cdot x_1 + \cdots + a_n \cdot x_n > c)$ where $a_1, a_2, c > 0$ and $a_n < 0$.

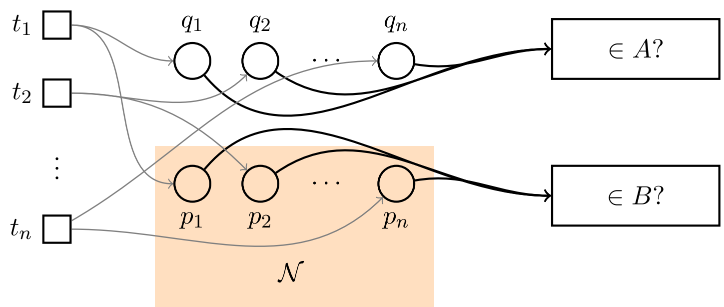


Figure 3: Reduction from set-to-set reachability to (marking-to-marking) reachability.

In summary, the following holds:

Proposition 7.2. *Given a conjunction of k 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 $(\boldsymbol{x}, \boldsymbol{y}) \to^* (\mathbf{0}, \mathbf{0})$ 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 7.3. *Given a Petri net $\mathcal{N}$ and convex polytopes A and B described as conjunctions of atomic propositions, one can construct, in logarithmic space, a Petri net $\mathcal{N}'$ and markings $\boldsymbol{m}_{src}$ and $\boldsymbol{m}_{tgt}$ such that $A \to^* B$ in $\mathcal{N}$ iff $\boldsymbol{m}_{src} \to^* \boldsymbol{m}_{tgt}$ 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 $Q \coloneqq \{q_1, \ldots, q_n\}$;
- we add a net $\mathcal{N}_A = (P_A, T_A, F_A)$, obtained from Proposition 7.2, to test whether the marking in Q belongs to A; and we add a net $\mathcal{N}_B = (P_B, T_B, F_B)$, obtained from Proposition 7.2, to test whether the marking in P belongs to B.

The Petri net $\mathcal{N}'$ is *intended* to work sequentially as follows:

(1) guess the initial marking $\boldsymbol{m}_{\text{src}}$ of $\mathcal{N}$;
(2) test whether $\boldsymbol{m}_{\text{src}} \in A$;
(3) execute $\mathcal{N}$ on $\boldsymbol{m}_{\text{src}}$ and reach a marking $\boldsymbol{m}_{\text{tgt}}$; and
(4) test whether $\boldsymbol{m}_{\text{tgt}} \in B$.

If $\mathcal{N}'$ follows this order, then it is straightforward to see that $A \to^* B$ in $\mathcal{N}$ iff $(\mathbf{0}, \mathbf{0}, \boldsymbol{y}, \boldsymbol{y}') \to^* (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0})$ in $\mathcal{N}'$, where $\boldsymbol{y}$ and $\boldsymbol{y}'$ are obtained from Proposition 7.2. However, $\mathcal{N}'$ may interleave the different phases.[3] Nonetheless, this is not problematic, as any run of $\mathcal{N}'$ can be reordered in such a way that all four phases are consecutive.

More formally, let $(\mathbf{0}, \mathbf{0}, \boldsymbol{y}, \boldsymbol{y}') \xrightarrow{\sigma} (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0})$ in $\mathcal{N}'$. Note that $\Delta_{t_i}^- = \mathbf{0}$ for every $i \in [1..n]$. Thus, we can reorder σ so that

$$(\mathbf{0}, \mathbf{0}, \boldsymbol{y}, \boldsymbol{y}') \xrightarrow{\alpha_1 t_1 \cdots \alpha_n t_n} (\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}, \boldsymbol{y}, \boldsymbol{y}') \xrightarrow{\sigma'} (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}) \text{ in } \mathcal{N}',$$

for some $\alpha_1, \ldots, \alpha_n \in \mathbb{R}_+$, marking $\boldsymbol{m}_{\text{src}}$, and firing sequence σ' whose support does not contain any of $t_1, \ldots, t_n$.

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

We have $\Delta_t^-(r) = 0$ for every $t \in T_A$ and $r \notin Q \cup P_A$. Furthermore, we have $\Delta_t^+(r) = 0$ for every $t \notin \{t_1, \ldots, t_n\}$ and $r \in Q \cup P_A$. Thus, we can reorder σ' into $\tau\tau'$ so that

$$(\boldsymbol{m}_{\text{src}}, \boldsymbol{m}_{\text{src}}, \boldsymbol{y}, \boldsymbol{y}') \xrightarrow{\tau} (\boldsymbol{0}, \boldsymbol{m}_{\text{src}}, \boldsymbol{0}, \boldsymbol{y}') \xrightarrow{\tau'} (\boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}) \text{ in } \mathcal{N}',$$

the support of τ only contains transitions from T_A, no transition from T_A occurs in the support of τ'.

We have $\Delta_t^+(r) = 0$ for every $t \in T_B$ and $r \notin P_B$. Therefore, we can reorder τ' into $\tau''\tau'''$ so that

$$(\boldsymbol{0}, \boldsymbol{m}_{\text{src}}, \boldsymbol{0}, \boldsymbol{y}') \xrightarrow{\tau''} (\boldsymbol{0}, \boldsymbol{m}_{\text{tgt}}, \boldsymbol{0}, \boldsymbol{y}') \xrightarrow{\tau'''} (\boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}, \boldsymbol{0}) \text{ in } \mathcal{N}',$$

the support of τ'' only contains transitions from T, no transition from T occurs in the support of τ''', and $\boldsymbol{m}_{\text{tgt}} \in \mathbb{R}_+^P$.

Altogether, we obtain

$$(\boldsymbol{m}_{\text{src}}, \boldsymbol{y}) \xrightarrow{\tau} (\boldsymbol{0}, \boldsymbol{0}) \text{ in } \mathcal{N}_A, \boldsymbol{m}_{\text{src}} \xrightarrow{\tau'} \boldsymbol{m}_{\text{tgt}} \text{ in } \mathcal{N}, \text{ and } (\boldsymbol{m}_{\text{tgt}}, \boldsymbol{y}') \xrightarrow{\tau''} (\boldsymbol{0}, \boldsymbol{0}) \text{ in } \mathcal{N}_B.$$

From this, we conclude that $\boldsymbol{m}_{\text{src}} \in A$, $\boldsymbol{m}_{\text{tgt}} \in B$ and $\boldsymbol{m}_{\text{src}} \to^* \boldsymbol{m}_{\text{tgt}}$ in $\mathcal{N}$. □

As a consequence of Proposition 7.3, combined with Theorems 5.1 and 6.6, we obtain the following corollary:

Corollary 7.4. *A negative answer to a convex polytope query $A \to^* B$ is witnessed by a locally closed bi-separator, for an altered Petri net, 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. While this does not directly hold for the more general of set-to-set reachability, we have shown that it can be extended to an altered Petri net (in the case of convex polytopes).

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 [BZM08, RS10, SPDA14, ABKS15]. We intend to explore whether they can constitute the basis of a CEGAR approach for the verification of continuous Petri nets.

Acknowledgment

We thank the anonymous referees of LMCS and FoSSaCS 2022 for their comments, and in particular for suggesting a more intuitive definition of bi-separators.

References

[ABKS15] Ernst Althaus, Björn Beber, Joschka Kupilas, and Christoph Scholl. Improving interpolants for linear arithmetic. In *Proc. 13th International on Automated Technology for Verification and Analysis (ATVA)*, pages 48–63, 2015. doi:10.1007/978-3-319-24953-7_5.

[BEH$^+$20] Michael Blondin, Javier Esparza, Martin Helfrich, Antonín Kucera, and Philipp J. Meyer. Checking qualitative liveness properties of replicated systems with stochastic scheduling. In *Proc. 32nd International Conference on Computer Aided Verification (CAV)*, volume 12225, pages 372–397, 2020. doi:10.1007/978-3-030-53291-8_20.

[BFHH17] Michael Blondin, Alain Finkel, Christoph Haase, and Serge Haddad. The logical view on continuous Petri nets. *ACM Transactions on Computational Logic (TOCL)*, 18(3):24:1–24:28, 2017. doi:10.1145/3105908.

[BH17] Michael Blondin and Christoph Haase. Logics for continuous reachability in Petri nets and vector addition systems with states. In *Proc. 32nd Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12, 2017. doi:10.1109/LICS.2017.8005068.

[BMTZ21] Pascal Baumann, Rupak Majumdar, Ramanathan S. Thinniyam, and Georg Zetzsche. Context-bounded verification of liveness properties for multithreaded shared-memory programs. *Proceedings of the ACM on Programming Languages (PACMPL)*, 5:1–31, 2021. doi:10.1145/3434325.

[BZM08] Dirk Beyer, Damien Zufferey, and Rupak Majumdar. Csisat: Interpolation for LA+EUF. In *Proc. 20th International Conference on Computer Aided Verification (CAV)*, pages 304–308, 2008. doi:10.1007/978-3-540-70545-1_29.

[CO21] Wojciech Czerwinski and Lukasz Orlikowski. Reachability in vector addition systems is Ackermann-complete. In *Proc. 62nd IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1229–1240. IEEE, 2021. doi:10.1109/FOCS52979.2021.00120.

[DA10] René David and Hassane Alla. *Discrete, Continuous, and Hybrid Petri nets*. Springer, second edition, 2010.

[DE95] Jorg Desel and Javier Esparza. *Free choice Petri nets*. Number 40. Cambridge University Press, 1995.

[EHJM20] Javier Esparza, Martin Helfrich, Stefan Jaax, and Philipp J. Meyer. Peregrine 2.0: Explaining correctness of population protocols through stage graphs. In *Proc. 18th International Symposium on Automated Technology for Verification and Analysis (ATVA)*, volume 12302, pages 550–556, 2020. doi:10.1007/978-3-030-59152-6_32.

[FH15] Estíbaliz Fraca and Serge Haddad. Complexity analysis of continuous Petri nets. *Fundamenta Informaticae*, 137(1):1–28, 2015. doi:10.3233/FI-2015-1168.

[FMW$^+$17] Yu Feng, Ruben Martins, Yuepeng Wang, Işil Dillig, and Thomas W. Reps. Component-based synthesis for complex APIs. In *Proc. 44th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL)*, pages 599–612. ACM, 2017. doi:10.1145/3009837.3009851.

[GM07] Bernd Gärtner and Jirí Matousek. *Understanding and using linear programming*. Universitext. Springer, 2007.

[GS92] Steven M. German and A. Prasad Sistla. Reasoning about systems with many processes. *Journal of the ACM*, 39(3):675–735, 1992. doi:10.1145/146637.146681.

[Ler12] Jérôme Leroux. Vector addition systems reachability problem (A simpler solution). In *Turing-100 – The Alan Turing Centenary*, volume 10, pages 214–228, 2012. doi:10.29007/bnx2.

[Ler21] Jérôme Leroux. The reachability problem for Petri nets is not primitive recursive. In *Proc. 62nd IEEE Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1241–1252. IEEE, 2021. doi:10.1109/FOCS52979.2021.00121.

[LS19] Jérôme Leroux and Sylvain Schmitz. Reachability in vector addition systems is primitive-recursive in fixed dimension. In *Proc.* 34th *Symposium on Logic in Computer Science (LICS)*, pages 1–13, 2019. doi:10.1109/LICS.2019.8785796.

[RS10] Andrey Rybalchenko and Viorica Sofronie-Stokkermans. Constraint solving for interpolation. *Journal of Symbolic Computation*, 45(11):1212–1233, 2010. doi:10.1016/j.jsc.2010.06.005.

[Sch86] Alexander Schrijver. *Theory of Linear and Integer Programming*. John Wiley & Sons, 1986.

[Son85] Eduardo D. Sontag. Real addition and the polynomial hierarchy. *Information Processing Letters*, 20(3):115–120, 1985.

[SPDA14] Christoph Scholl, Florian Pigorsch, Stefan Disch, and Ernst Althaus. Simple interpolants for linear arithmetic. In *Proc. Conference & Exhibition on Design, Automation & Test in Europe (DATE)*, pages 1–6, 2014. doi:10.7873/DATE.2014.128.

Appendix A. Missing proofs

Proof of Lemma 3.5. Let $\mathcal{S}$ and $\mathcal{S}'$ denote the two systems of the proposition. We must show that $\mathcal{S}$ has no solution iff $\mathcal{S}'$ has a solution. First, we prove the following claim:

Claim: The system $\exists \boldsymbol{x} \geq \mathbf{0} : \mathbf{A}\boldsymbol{x} = \boldsymbol{b} \land S \subseteq \text{supp}(\boldsymbol{x}) \subseteq S'$ has a solution iff this system has a solution: $\exists \boldsymbol{x} \geq \mathbf{0}, y \geq 1 : \mathbf{A}\boldsymbol{x} = y\boldsymbol{b} \land \boldsymbol{x} =_{\overline{V}} \mathbf{0} \land \boldsymbol{x} \geq_U \mathbf{1}$, where $\mathbf{1} \coloneqq (1, \ldots, 1)$.

Proof of the claim: $\Rightarrow$) Since $\boldsymbol{x}(t) > 0$ for all $t \in S$, we can pick $y \geq 1$ sufficiently large so that $y\boldsymbol{x}(t) \geq 1$ for every $t \in S$. Let $\boldsymbol{x}' \coloneqq y\boldsymbol{x}$. We have $\mathbf{A}\boldsymbol{x}' = y\mathbf{A}\boldsymbol{x} = y\boldsymbol{b}$ and $\boldsymbol{x}' = y\boldsymbol{x} \geq \boldsymbol{x} \geq \mathbf{0}$. Moreover, $\boldsymbol{x}'(t) = y\boldsymbol{x}(t) = 0$ for every $t \notin S'$, and $\boldsymbol{x}'(t) = y\boldsymbol{x}(t) \geq 1$ for every $t \in S$.

$\Leftarrow$) Let $\boldsymbol{x}' \coloneqq \boldsymbol{x}/y$. We have $\mathbf{A}\boldsymbol{x}' = \boldsymbol{b}$. Moreover, for every $t \notin S'$ it is the case that $\boldsymbol{x}'(t) = (1/y)\boldsymbol{x}(t)t = 0$ and for every $ts \in S$ it is the case that $\boldsymbol{x}'(t) = (1/y)\boldsymbol{x}(t) \geq 1/y > 0$. Hence, $S \subseteq \text{supp}(\boldsymbol{x}') \subseteq S'$.

Now we proceed to prove the proposition. Let $\mathbf{J} \in \mathbb{R}^{\overline{S'} \times T}$ be the matrix that contains 0 everywhere except for $\mathbf{J}_{t,t} = 1$ for all $t \notin S'$. Let $\boldsymbol{c} \in \mathbb{R}^T$ be such that $\boldsymbol{c}(t) = 1$ for every $t \in S$ and $\boldsymbol{c}(t) = 0$ for every $t \notin S$. By the claim above, the system $\mathcal{S}$ has a solution iff the system $\exists \boldsymbol{x}' : \mathbf{A}'\boldsymbol{x}' \leq \boldsymbol{b}'$ has a solution, where

$$\mathbf{A}' \coloneqq \begin{pmatrix} \mathbf{A} & -\boldsymbol{b} \\ -\mathbf{A} & \boldsymbol{b} \\ \mathbf{J} & \mathbf{0} \\ -\mathbf{I} & \mathbf{0} \\ \mathbf{0}^\mathsf{T} & -1 \end{pmatrix} \text{ and } \boldsymbol{b}' \coloneqq \begin{pmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{0} \\ -\boldsymbol{c} \\ -1 \end{pmatrix}.$$

By Lemma 2.1, the latter system has no solution iff the following has one: $\exists \boldsymbol{z} \geq \mathbf{0} : (\mathbf{A}')^\mathsf{T}\boldsymbol{z} = \mathbf{0} \land (\boldsymbol{b}')^\mathsf{T}\boldsymbol{z} < 0$. We can rewrite the latter as follows:

$$\begin{aligned}
&\exists \boldsymbol{z} \geq \mathbf{0} : (\mathbf{A}')^\mathsf{T}\boldsymbol{z} = \mathbf{0} \land (\boldsymbol{b}')^\mathsf{T}\boldsymbol{z} < 0 \\
\equiv\ &\exists (\boldsymbol{u}, \boldsymbol{u}', \boldsymbol{v}, \boldsymbol{v}', \alpha) \geq \mathbf{0} : \mathbf{A}^\mathsf{T}(\boldsymbol{u} - \boldsymbol{u}') = \boldsymbol{v}' - \mathbf{J}^\mathsf{T}\boldsymbol{v} \land \boldsymbol{b}^\mathsf{T}(\boldsymbol{u}' - \boldsymbol{u}) = \alpha \land -\boldsymbol{c}^\mathsf{T}\boldsymbol{v}' - \alpha < 0 \\
\equiv\ &\exists \boldsymbol{y}\ \exists (\boldsymbol{v}, \boldsymbol{v}', \alpha) \geq \mathbf{0} : \mathbf{A}^\mathsf{T}\boldsymbol{y} = \boldsymbol{v}' - \mathbf{J}^\mathsf{T}\boldsymbol{v} \land \boldsymbol{b}^\mathsf{T}\boldsymbol{y} = -\alpha \land -\alpha < \boldsymbol{c}^\mathsf{T}\boldsymbol{v}' \\
\equiv\ &\exists \boldsymbol{y}\ \exists (\boldsymbol{v}, \boldsymbol{v}') \geq \mathbf{0} : \mathbf{A}^\mathsf{T}\boldsymbol{y} = \boldsymbol{v}' - \mathbf{J}^\mathsf{T}\boldsymbol{v} \land \boldsymbol{b}^\mathsf{T}\boldsymbol{y} \leq 0 \land \boldsymbol{b}^\mathsf{T}\boldsymbol{y} < \boldsymbol{c}^\mathsf{T}\boldsymbol{v}' \\
\equiv\ &\exists \boldsymbol{y} : \mathbf{A}^\mathsf{T}\boldsymbol{y} \geq_{S'} \mathbf{0} \land \boldsymbol{b}^\mathsf{T}\boldsymbol{y} \leq 0 \land \boldsymbol{b}^\mathsf{T}\boldsymbol{y} < \sum_{s \in S} (\mathbf{A}^\mathsf{T}\boldsymbol{y})_s.
\end{aligned}$$

Note that the last equivalence holds since $(\mathbf{J}^\mathsf{T}\boldsymbol{v}) =_{S'} \mathbf{0}$ and since $\boldsymbol{c}^\mathsf{T}$ sums entries over S. □