Modelchecking counting properties of 1-safe nets with buffers in paraPSPACE

M. Praveen and Kamal Lodaya
The Institute of Mathematical Sciences
Chennai, India

October 2009

Abstract

We consider concurrent systems that can be modelled as 1-safe Petri nets communicating through a fixed set of buffers (modelled as unbounded places). We identify a parameter K, which we call "benefit depth", formed from the communication graph between the buffers. We show that for our system model, the coverability and boundedness problems can be solved in polynomial space assuming K to be a fixed parameter, that is, the space requirement is $f(K)p(n)$, where f is an exponential function and p is a polynomial in the size of the input. We then obtain similar complexity bounds for modelchecking a logic based on such counting properties. This means that systems that have sparse communication patterns can be analyzed more efficiently than using previously known algorithms for general Petri nets.

1 Introduction

Many theoretical models exist for concurrent, infinite-state systems. Petri nets [22], process rewrite systems [5], lossy channel systems (LCS) [6] and networks of pushdown systems [1] are some of them. The power to express properties of the original system in sufficient detail and existence of efficient algorithms for analysis are often conflicting goals in these models. Reachability in LCS is non-primitive recursive [25] and reachability for Petri nets is decidable but with no known upper bound [20, 17].

More structure is sometimes imposed on the models to handle these conflicting goals. Communicating automata with buffers [4] is one such model. In this paper we consider a small generalization where 1-safe Petri nets (which we call components) communicate via buffers. Thus we have a system model which allows both asynchronous and synchronous communication, since 1-safe Petri nets can model the latter.

The diagram shown in Fig. 1 illustrates the kind of systems we are interested in. The boxes labelled as line 1, line 2 etc. can be thought of as assembly lines

represented by 1-safe Petri nets, drawing raw materials from buffers ib_1, ib_2 etc. Output of these assembly lines are deposited into buffers ob_1, ob_2 etc. Boxes labelled master line 1 and master line 2 can be thought of as master assembly lines that use output of earlier assembly lines as their input. They deposit their output in buffers pr_1 and pr_2 respectively. We are concerned with verifying

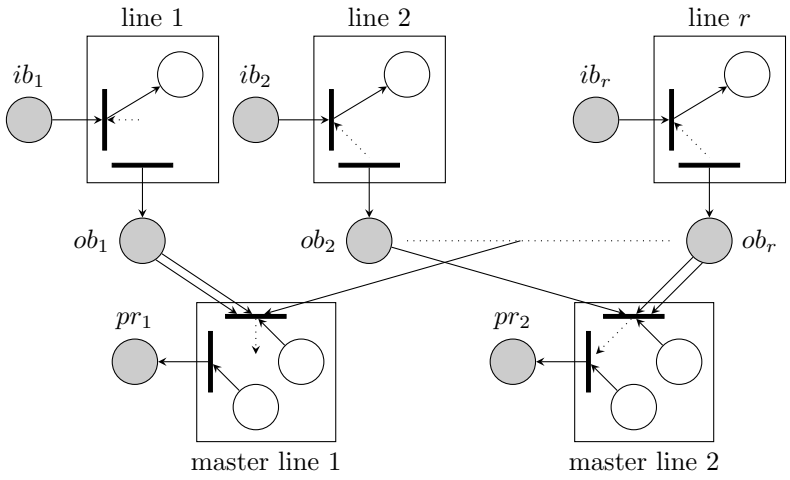

Figure 1: Illustration of communicating automata with buffers

properties like $\exists c : pr_1 \leq c$ *in all reachable configurations* (boundedness) or $ob_1 + ob_2 \geq 100$ *in some reachable configuration* (coverability). For instance, the latter property might show that the two buffers are dealing with enough throughput. Karp and Miller examined these properties in the context of Petri nets [16] and Lipton and Rackoff showed them to be ExpSpace-complete [19, 23].

As Esparza notes in his survey article [12], verification of a "logic" based on such properties, for instance LTL or CTL extended with counting properties, quickly becomes undecidable. Modalities of the form $\mathbf{EF}(M \geq M_c)$ (where M, M_c are markings) can be handled without getting into undecidability [27]. However, a "usual" definition of a logic based on these modalities can express reachability, as in Howell, Rosier and Yen's logic [15] and in Yen's logic [27] (as was recently shown by Atig and Habermehl [2]). So we are left with positive Boolean combinations of formulae of the form $\mathbf{EF}(M \geq M_c)$ [27] for which modelchecking is ExpSpace-hard. Rosier and Yen analyzed boundedness [24] using what we today call parameterized complexity [10] to show that the space requirement is exponential in the number of unbounded places and polynomial in the number of bounded places. If we give up counting properties, Habermehl shows that the full linear time μ-calculus can be reduced to the problem of repeated control state reachability [14] and is Pspace-complete in the size of the formula and ExpSpace-complete in the size of the model.

An ExpSpace lower bound in the size of the model is not very encouraging

for potential verifiers. Our first contribution is the identification of a parameter K, which we call benefit depth. A buffer p_1 can benefit by another buffer p_2 if there is a sequence of transitions that decrease tokens in p_2 and increase tokens in p_1. Benefit depth is the maximum number of buffers benefited by any one buffer. It seems reasonable that, in a sparsely communicating system, benefit depth can be low.

We show that boundedness and coverability in our models, when parameterized by benefit depth, are solvable in paraPSPACE [13]. That is, the space requirement is of the form $\mathcal{O}(f(K)p(n))$, where f is an exponential function of benefit depth and p is some polynomial of the size of the model and the marking to be covered. For constant benefit depth, boundedness and coverability can be solved in PSPACE. Thus, our results are refinements of Rosier and Yen's [24], improving them if benefit depth is less than the number of buffers (as happens in sparsely communicating systems).

As our final contribution, we define a logic which can express counting properties such as coverability *and* show that it can be modelchecked on Petri nets in paraPSPACE.

Related work. We did look at other parameters such as cycle rank [11] and DAG-width [3, 21] which have been explored as a measure of "cycle complexity". These do not seem to work in the case of coverability problems since the structure of cycles used in Lipton's hardness proof has low cycle rank and DAG-width.

2 Problem definitions

Let $\mathbb{Z}$ be the set of integers and $\mathbb{N}$ the set of natural numbers. A Petri net is a 4-tuple $N = (P, T, Pre, Post)$ where P is a set of places, T is a set of transitions and Pre and $Post$ are the incidence functions: $Pre : P \times T \to [0 \dots W]$ (arcs going from places to transitions), $Post : P \times T \to [0 \dots W]$ (arcs going from transitions to places), where $W \geq 1$.

Definition 1. *Given a place p, the set of places $Ben(p) \subseteq P$ and the set of transitions $T_{ben}(p) \subseteq T$ benefited by p are those connected to p by a sequence of arcs with weight ≥ 1. Formally they are the smallest sets satisfying:*

1. *$p \in Ben(p)$.*
2. *If some $p' \in Ben(p)$ and there is a transition t with $Pre(p', t) \geq 1$, then $t \in T_{ben}(p)$.*
3. *If some transition $t \in T_{ben}(p)$ and there is a place p'' such that $Post(p'', t) \geq 1$, then $p'' \in Ben(p)$.*

$Ind(p) = P \setminus Ben(p)$ and $T_{ind}(p) = T \setminus T_{ben}(p)$ are the places and transitions not benefiting from p.

We call a function $M : P \to \mathbb{Z}$ a vector. For two vectors M_1 and M_2, we say M_1 covers M_2 (written $M_1 \geq M_2$) if for every place p, $M_1(p) \geq M_2(p)$. $M_1 > M_2$ means that M_1 covers M_2 but they are not the same.

If the range of the vector is $\mathbb{N}$, it is called a marking. At a marking M, a place p is said to have $M(p)$ tokens. A pair (N, M_0) consisting of a Petri net N and an initial marking M_0 is called a **system**. We assume a net is presented as two matrices for Pre and $Post$. In the rest of this paper, we will assume that a Petri net N has m places, n transitions and that W is the maximum of the range of Pre and $Post$. We define the size of the net to be $2mn \log W$ bits. The system has size $2mn \log W + \log |M_0|$ bits.

A transition t may be taken as a step at the vector M yielding a new vector M' given by the equation $M'(p) = M(p) - Pre(p,t) + Post(p,t)$ for all $p \in P$. The transition t is said to be fired at M if, in addition, t is enabled at M, that is, for all $p \in P$, $M(p) \geq Pre(p,t)$. Thus firing a transition leads from a marking to another marking, while stepping is a more general notion leading from a vector to a vector.

A finite transition sequence $\sigma = t_1 t_2 \dots t_r$ is a walk from an initial vector M_0 to a vector M_r if there exist intermediate vectors $M_1, M_2, \dots, M_r$ such that for all i with $1 \leq i \leq r$, we have a step from M_{i-1} to M_i using the transition t_i. We write $M_0 \xrightarrow{\sigma} M_r$. σ is a firing sequence enabled at some initial marking M_0 if the transitions are enabled at the intermediate vectors, so that $M_1, M_2, \dots, M_r$ are all markings. We write $M_0 \stackrel{\sigma}{\Longrightarrow} M_r$ and say that the marking M_r is reachable from M_0. $\mathcal{R}(N, M_0)$ is the set of markings reachable from M_0. A place is said to be c-bounded, $c \in \mathbb{N}$, in the system (N, M_0), if for all its reachable markings M, $M(p)$ is in $\{0, \dots, c\}$. The system is c-bounded if all its places are. A 1-bounded system is commonly called a 1-Safe net.

Definition 2 (Reachability, coverability, boundedness)**.** *Given a system (N, M_0) and a marking M as input data, the reachability problem is to decide if the marking M is in $\mathcal{R}(N, M_0)$; the coverability problem is to decide if there is an M' in $\mathcal{R}(N, M_0)$ such that M' covers M. Given a system (N, M_0), the boundedness problem is to decide if there is some $c \in \mathbb{N}$ such that the system is c-bounded.*

Given a c-bounded system, the reachability and coverability problems are known to be PSPACE-complete [7]. For systems in general, which can be unbounded, Lipton showed that all three problems are EXPSPACE-hard [19]. Rackoff showed that boundedness and coverability are in EXPSPACE[23]. Reachability has been shown to be decidable [20, 17], obtaining an upper bound is a famous open problem.

2.1 A logic of properties

Inspired by Yen [27], we now formulate a logic of properties such that its model checking can be reduced to coverability (κ) and boundedness (β) problems, but is designed to avoid expressing reachability. In particular, a κ formula of the form $\tau \leq c$, $c \in \mathbb{N}$, is *not* provided and the κ and ϕ formulas are *not* closed

under negation.

$$\tau ::= p,\ p \in P \mid \tau_1 + \tau_2 \mid c\tau,\ c \in \mathbb{N}$$
$$\kappa ::= \tau \geq c,\ c \in \mathbb{N} \mid \kappa_1 \wedge \kappa_2 \mid \kappa_1 \vee \kappa_2 \mid \mathbf{EF}\kappa$$
$$\beta ::= \{\tau_1, \ldots, \tau_r\} < \omega \mid \neg\beta \mid \beta_1 \vee \beta_2$$
$$\phi ::= \beta \mid \kappa \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$$

The satisfaction of a formula ϕ by a system (N, M_0) (denoted as $N, M_0 \models \phi$) is defined below. The boolean operators work as usual. Note that every term (of type τ) gives a function $L_\tau : P \to \mathbb{N}$ such that τ is syntactically equivalent to $\sum_{p \in P} L_\tau(p)p$.

- $N, M_0 \models \tau \geq c$ if $\sum_{p \in P} L_\tau(p)M_0(p) \geq c$.
- $N, M_0 \models \mathbf{EF}\kappa$ if $\exists M \in \mathcal{R}(N, M_0)$ such that $N, M \models \kappa$.
- $N, M_0 \models \{\tau_1, \ldots \tau_r\} < \omega$ if $\exists c \in \mathbb{N} : \forall M \in \mathcal{R}(N, M_0)\ \exists j \in \{1, \ldots, r\}$ such that $\sum_{p \in P} L_{\tau_j}(p)M(p) \leq c$.

We use $\{\tau_1, \ldots, \tau_r\} = \omega$ as an abbreviation for $\neg(\{\tau_1, \ldots, \tau_r\} < \omega)$.

The formula $\{p_1, \ldots, p_r\} < \omega$ says that the given set of places is bounded according to Valk and Vidal-Naquet [26, Section 4.1]. On the other hand, $\{p_1 + \cdots + p_r\} < \omega$ says that the same set of places is uniformly bounded according to the same authors [26].[1]

2.2 System model

Though our results work for any Petri net, we work with the model defined below to emphasize the fact that our problem formulation strictly generalizes reachability for 1-bounded systems. The model of concurrent systems we consider in this paper consists of some 1-safe nets, called components, which can add or remove tokens to/from a set of unbounded places that we refer to as buffers.

Definition 3. *A **net communicating with buffers** (we just use the word "net" below) is a Petri net $N = (C, B, T, Pre, Post)$ where the set of places $P = C \cup B$ is partitioned into a set of buffers B and component places $C = P \setminus B$, such that all places in C remain 1-bounded (regardless of the number of tokens in the buffers in an initial marking).*

In the rest of the paper, we will assume that $|C| = a$, $|B| = b$ and that $a+b = m$, where m is the total number of places. In our model, the components do not contribute to exponential space complexity. Our results can be generalized to the case where the components are declared to be c-bounded (for a constant c) rather than 1-bounded.

[1] We thank an anonymous FSTTCS referee for pointing out this subtlety. Following their suggestion, we have slightly extended our logic beyond the submitted version to cover both kinds of boundedness.

Definition 4. *The* ***benefit depth*** *of a net is defined as* $K = max\{|Ben(p) \cap B| - 1 \mid p \in B\}$.

Benefit depth depends only on the communication pattern among buffers, even though the communication link may involve some component places. It can be computed efficiently (in NLOGSPACE).

The communication graph of the system of Fig. 1 is shown in Fig. 2. Irrespective of the number of assembly lines, benefit depth is 3 since only ob_i, pr_1 and pr_2 can benefit by decreasing tokens from ib_i. If there are interdependencies

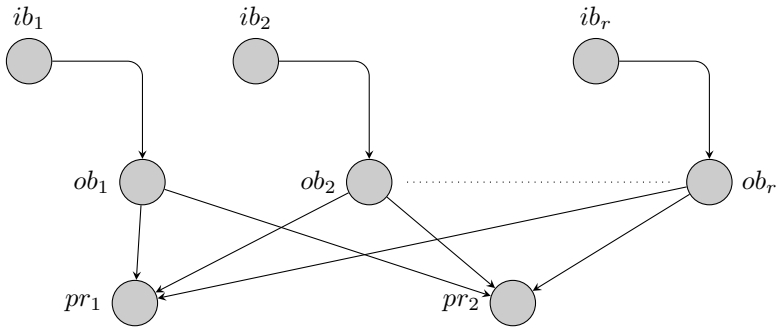

Figure 2: Communication graph of buffers of the system in Fig. 1

among the assembly lines, such as a byproduct of one being the raw material of another (not shown in the figure), then benefit depth will increase. The more such dependencies (i.e., more dense the communication graph among the buffers is), the higher will be the benefit depth. Intuitively, the number of tokens in a place in $Ben(p)$ can be increased by decreasing some tokens in p through a sequence of transitions in $T_{ben}(p)$. Only those transitions use the extra tokens from p.

Our earlier definitions are modified to be well-behaved on the components. A vector will now be given by a pair of functions $C \to \{0, 1\}$ and $B \to \mathbb{Z}$; it is a marking if the second function has range $\mathbb{N}$. Walks and firing sequences will now be defined with these kinds of intermediate vectors and markings.

3 Benefit depth and coverability

Let $Q \subseteq P$ be a subset of places. For this paper we will need the inbetween notion (due to Rackoff) of σ being a Q**-run** where for the vectors $M_i, 0 \leq i < r$, $M_i(p) \geq Pre(p, t_{i+1})$ for every place p in Q. Thus a walk is a $\emptyset$-run and a firing sequence is a P-run. For two vectors M_1 and M_2, we say $M_1 \geq_Q M_2$ if for every $p \in Q, M_1(p) \geq M_2(p)$ and $M_1(p) = M_2(p)$ for every $p \in C$. A walk σ from M_1 is said to Q**-cover** a marking M_{cov} if it is a Q-run and the final vector M_2 obtained by walking σ at M_1 satisfies $M_2 \geq_Q M_{cov}$. We say σ **covers** a marking if σ P-covers it.

We will fix for this section M_{cov} as the marking to be covered. For the purpose of complexity analysis, we will denote the maximum of the range of M_{cov} by R.

Definition 5. *A Q-**covering** run is a Q-run that Q-covers M_{cov}. Let $Q_0 \subseteq Q$. A Q-run from M_0 to M_r is said to be c-**bounded for** Q_0, $c \in \mathbb{N}$, if for all intermediate vectors $M_i, 0 \leq i < r$, $M_i(p)$ is in $\{0, \ldots, c\}$ for every place p in Q_0.*

Definition 6. *[23, Rackoff] Let $C \subseteq Q \subseteq P$. Define $lencov(Q, M, M_{cov})$ to be the length of the shortest Q-covering run from the vector M. If there is no such sequence, define $lencov(Q, M, M_{cov})$ to be 0. For $0 \leq i \leq b$, $\ell(i, M_{cov})$ is defined to be $max\{lencov(Q, M, M_{cov}) \mid M$ a vector, $C \subseteq Q \subseteq P$ and $|Q \setminus C| = i\}$. In this section we abbreviate $\ell(i, M_{cov})$ to $\ell(i)$. In section 5 we will abbreviate $\ell(b, M)$ to $\ell'(M)$.*

Definition 7. *Let $C \subseteq Q \subseteq P$ and $p \in B$ be a buffer. Define $covind^p(Q, M, M_{cov})$ to be the length of the shortest Q-covering run in $T_{ben}(p)^*$ from the vector M. If there is no such sequence, define $covind^p(Q, M, M_{cov})$ to be 0. Let $\ell_1(i) = max\{covind^p(Q, M, M_{cov}) \mid M$ a vector, p a buffer, $|Q \cap Ben(p) \cap B| = i\}$.*

Our strategy is to segregate covering sequences into two parts, the first made of transitions in $T_{ind}(p)$ and the second one made of transitions in $T_{ben}(p)$. We need the following technical lemma, which is a generalization of the exchange lemma [8, Lemma 2.14] to Petri nets with weighted arcs.

Lemma 8. *Let p be a place, transitions $t_{ben} \in T_{ben}(p)$ and $t_{ind} \in T_{ind}(p)$. Let $Q \subseteq P$ be some subset of places. If $t_{ben}t_{ind}$ is a Q-run from some vector M, then so is $t_{ind}t_{ben}$.*

Proof. We will first prove that t_{ind} is a Q-run from M. Suppose not. Now, suppose $p' \in Q$ is one of the places that do not have sufficient tokens at M to enable t_{ind}. Since $t_{ind} \in T_{ind}(p)$, we know from Definition 1 that for all $p'' \in Ben(p)$, $Pre(p'', t_{ind}) = 0$. Hence, $p' \notin Ben(p)$, i.e., $p' \in Ind(p) \cap Q$. Now, we have $M \xrightarrow{t_{ben}} M_1 \xrightarrow{t_{ind}} M_2$ for some vector M_1, t_{ind} is a Q-run from M_1 but not from M since a place $p' \in Ind(p) \cap Q$ doesn't have enough tokens at M. Since p' has enough tokens at M_1, t_{ben} adds some tokens to p', i.e., $Post(p', t_{ben}) \geq 1$. This contradicts the fact that $t_{ben} \in T_{ben}(p)$. Therefore, t_{ind} is a Q-run from M. So, $M \xrightarrow{t_{ind}} M_3$ for some vector M_3.

Now, we will prove that t_{ben} is a Q-run from M_3. Suppose not. Let $p' \in Q$ be one of the places that do not have enough tokens at M_3 to enable t_{ben}. Since t_{ben} is a Q-run from M, t_{ind} must decrease the number of tokens in p'. Since $t_{ind} \in T_{ind}(p)$, we know from Definition 1 that t_{ind} doesn't decrease tokens in any place that belongs to $Ben(p)$. Hence, $p' \notin Ben(p)$, i.e., $p' \in Ind(p) \cap Q$. Let q' be the number of tokens in p' at M and let t_{ind} decrease the number of tokens in p' by q_1. Now, if $d_2 = Pre(p', t_{ben})$ is the number of tokens needed by t_{ben}, then $d_2 > q' - q_1$. Now, if $t_{ben}t_{ind}$ is run from M, number of tokens in p' at the end will be $q' - d_2 - q_1 < 0$ ($Post(p', t_{ben}) = 0$ since $p' \in Ind(p)$), which

contradicts the fact that $t_{ben}t_{ind}$ is a Q-run from M. Therefore, p' cannot be in $Ind(p) \cap Q$ and hence there is no such p'. This means that t_{ben} is a Q-run from M_3 and hence $t_{ind}t_{ben}$ is a Q-run from M. □

Lemma 9. *If $K \leq i < b$, then $\ell(i+1) \leq (W\ell_1(K) + R)^{i+1}2^a + \ell(i) + \ell_1(K)$.*

Proof. Suppose that $Q_{i+1} = C \cup A$ where $|A| = i+1$ and that there is a Q_{i+1}-covering run from some vector M. If this run is $W\ell_1(K)+R$-bounded for Q_{i+1}, then there is a similar run where no two intermediate vectors are equal when restricted to Q_{i+1}. The length of such a sequence is at most $(W\ell_1(K)+R)^{i+1}2^a$.

Otherwise, there is a Q_{i+1}-covering run from M that is *not* $W\ell_1(K) + R$-bounded for Q_{i+1}. Then there exist runs σ_1 and σ_2 such that $\sigma_1\sigma_2$ is Q_{i+1}-covering from M, σ_1 is $W\ell_1(K) + R$-bounded for Q_{i+1} and the final vector M' obtained by walking σ_1 at M has more than $W\ell_1(K) + R$ tokens at some place $p \in A$. Let $Q_i = Q_{i+1} \setminus \{p\}$. As above, we can assume that length of σ_1 is at most $(W\ell_1(K) + R)^{i+1}2^a$.

Now, σ_2 is a Q_i-covering run from M'. By definition, there is a Q_i-covering run σ_2' from M' whose length is at most $\ell(i)$. Since σ_2' is a Q_i-run from M', we can apply Lemma 8 repeatedly to rearrange σ_2' into another sequence $\tau_1\tau_2$ such that $\tau_1 \in T_{ind}(p)^*$, $\tau_2 \in T_{ben}(p)^*$, $\tau_1\tau_2$ is a Q_i-run from M' and $|\tau_1\tau_2| = |\sigma_2'|$ (see Fig. 3). This rearrangement of σ_2' could potentially cause places in C to

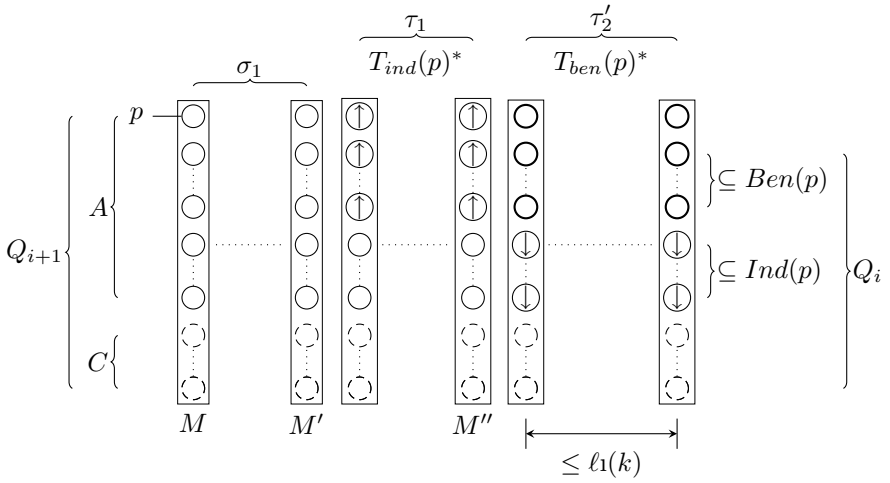

Figure 3: Sequences and bounds used in the proof of Lemma 9
↑ (resp. ↓) inside places indicates that tokens are non-decreasing (resp. non-increasing).

get more than 1 token in an arbitrary Petri net. However, our assumption that places in C remain 1-bounded regardless of the number of tokens in the buffers at the initial marking ensures that the rearrangement doesn't disturb the 1-boundedness of places in C. Let M'' be the final vector obtained by walking

τ_1 at M'. Now, $\tau_2 \in T_{ben}(p)^*$ and is a Q_i-covering run from M''. Hence, by Definition 7, there is a Q_i-covering run τ_2' from M'' with $\tau_2' \in T_{ben}(p)^*$ and $|\tau_2| \leq \ell_1(|Ben(p) \cap B| - 1)$. Since $|\tau_1| \leq \ell(i)$ and $\ell_1(|Ben(p) \cap B| - 1) \leq \ell_1(K)$, $|\tau_1\tau_2'| \leq \ell(i) + \ell_1(K)$. Since $\tau_1 \in T_{ind}(p)^*$, Definition 1 implies that no transition in τ_1 decreases tokens from p. Since $M''(p) \geq M'(p) \geq W\ell_1(K) + R$ and each transition in τ_2' removes at most W tokens from p, $\sigma_1\tau_1\tau_2'$ is a Q_{i+1}-covering run from M whose length is at most $(W\ell_1(K) + R)^{i+1}2^a + \ell(i) + \ell_1(K)$. □

The bound on $\ell(i+1)$ given by Rackoff in [23] is similar to the one in Lemma 9 but uses $\ell(i)$ in place of $\ell_1(K)$. Since $\ell_1(K)$ can be much smaller than $\ell(i)$, the bound in Lemma 9 is better. This is the fact that enables us to restrict exponential space complexity to K. The following lemma gives a recurrence relation for length of covering sequences made of transitions in $T_{ben}(p)$.

Lemma 10. *$\ell_1(0) \leq 2^a$ and $\ell_1(i+1) \leq (W\ell_1(i) + R)^{i+1}2^a + \ell_1(i)$.*

Proof. (Following [23].) We will first prove the bound on $\ell_1(0)$. Let $Q = C \cup A$ and $A \cap Ben(p) = \emptyset$ for some buffer p. Suppose $\sigma \in T_{ben}(p)^*$ is a Q-covering run from some vector M. If any two intermediate vectors reached by walking σ at M are equal when restricted to C, remove the subsequence between these two intermediate vectors. Since the removed subsequence never added any tokens to any place in A, such removals will never decrease tokens from places in A. Therefore, after all such removals, the sequence that is left is still a Q-covering run from M. The length of this run is at most 2^a.

Next, we will prove the bound on $\ell_1(i+1)$. Suppose that $Q = Q_{i+1} = C \cup A \cup A'$ where $|A'| = i+1$, with $A \cap Ben(p) = \emptyset$ for some buffer p. Suppose that there is a Q_{i+1}-covering run in $T_{ben}(p)^*$ from some vector M.

Case 1: There is a Q_{i+1}-covering run from M that is $W\ell_1(i)+R$-bounded for A'. Then, as above, there is a Q_{i+1}-covering run σ from M that is $W\ell_1(i) + R$-bounded for A' such that no two intermediate vectors obtained from walking σ at M are equal when restricted to $Q_{i+1} \setminus A$. The length of such a run is at most $(W\ell_1(i) + R)^{i+1}2^a$.

Case 2: Otherwise, there is a Q_{i+1}-covering run from M that is *not* $W\ell_1(i)+R$-bounded for A'. Then there exist sequences σ_1 and σ_2 such that $\sigma_1\sigma_2 \in T_{ben}(p)^*$ is a Q_{i+1}-covering run from M, σ_1 is $W\ell_1(i) + R$-bounded for A' and the final vector M' obtained by walking σ_1 at M has more than $W\ell_1(i) + R$ tokens at some place $p' \in A'$. Let $Q_i = Q_{i+1} \setminus \{p'\}$. As in case 1, we can assume that length of σ_1 is at most $(W\ell_1(i) + R)^{i+1}2^a$.

Now, $\sigma_2 \in T_{ben}(p)^*$ is a Q_i-covering run from M'. By definition, there is a Q_i-covering run $\sigma_2' \in T_{ben}(p)^*$ from M' whose length is at most $\ell_1(i)$. Since $M'(p) \geq W\ell_1(i) + R$ and each transition in σ_2' removes at most W tokens from p', $\sigma_1\sigma_2'$ is a Q_{i+1}-covering run from M whose length is at most $(W\ell_1(i) + R)^{i+1}2^a + \ell_1(i)$. □

It now only remains to solve the recurrence relations we have obtained and use them in a nondeterministic algorithm that guesses covering sequences to get our first main theorem.

Definition 11. *Let* $W' = \max\{W, 2\}$, $R' = \max\{R, 2\}$. *Define a growth function* $g : \mathbb{N} \to \mathbb{N}$ *as* $g(0) = W'R'2^a$ *and* $g(i+1) = (g(i))^{3(i+1)}2^a$.

Lemma 12. $\ell(K+j) \leq (K+j)(W\ell_1(K) + R)^{K+j}2^a + j\ell_1(K) + \ell(K)$.

Proof. By induction on j. The base case $j = 0$ is clear since RHS of the inequation is at least $\ell(K)$.

$$\begin{aligned}
\ell(K+j+1) &\leq (W\ell_1(K) + R)^{K+j+1}2^a + \ell(K+j) + \ell_1(K) \\
&\leq (W\ell_1(K) + R)^{K+j+1}2^a \\
&\quad + (K+j)(W\ell_1(K) + R)^{K+j}2^a + j\ell_1(K) \\
&\quad + \ell(K) + \ell_1(K) \\
&\leq (K+j+1)(W\ell_1(K) + R)^{K+j+1}2^a + (j+1)\ell_1(K) \\
&\quad + \ell(K)
\end{aligned}$$

□

Lemma 13. $\ell_1(i), \ell(i) \leq g(i) \leq (W'R')^{3^i i!}2^{6^i i! a}$ *and* $\ell(K+j) \leq (K+j)(g(K))^{3(K+j)}2^a$.

Proof. Bounds on $\ell_1(i)$ and $\ell(i)$ are by induction on i. For the base case $i = 0$, we have $\ell_1(0) \leq 2^a \leq g(0)$ and $\ell(0) \leq 2^a \leq g(0)$ (this bound on $\ell(0)$ can be obtained by arguments similar to those used for the bound on $\ell_1(0)$ in Lemma 10).

$$\begin{aligned}
\ell_1(i+1) &\leq (W\ell_1(i) + R)^{i+1}2^a + \ell_1(i) \\
&\leq (Wg(i) + R)^{i+1}2^a + g(i) \\
&\leq (W'R')^{i+1}(g(i))^{i+1}2^a + g(i) \\
&\leq (g(i))^{2(i+1)}2^a + g(i) \\
&\leq (g(i))^{3(i+1)}2^a \\
&= g(i+1)
\end{aligned}$$

For the bound on $\ell(i)$, we will use Rackoff's result from [23], which states that $\ell(i+1) \leq (W\ell(i) + R)^{i+1}2^a + \ell(i)$.

$$\begin{aligned}
\ell(i+1) &\leq (W\ell(i) + R)^{i+1}2^a + \ell(i) \\
&\leq (Wg(i) + R)^{i+1}2^a + g(i) \\
&\leq (g(i))^{3(i+1)}2^a \\
&= g(i+1)
\end{aligned}$$

Next, we will prove the bound on $\ell(K+j)$.

$$\begin{aligned}
\ell(K+j) &\leq (K+j)(Wg(K) + R)^{K+j}2^a + jg(K) + g(K) \\
&\leq (K+j)(W'R')^{K+j}(g(K))^{K+j}2^a + (j+1)g(K) \\
&\leq (K+j)(g(K))^{3(K+j)}2^a
\end{aligned}$$

Finally, the bound on $g(i)$ is by induction i. For the base case $i = 0$, we have $g(0) = (W'R')2^a = (W'R')^{3^0 0!} 2^{6^0 0! a}$.

$$\begin{aligned} g(i+1) &= (g(i))^{3(i+1)} 2^a \\ &\leq \left((W'R')^{3^i i!} 2^{6^i i! a}\right)^{3(i+1)} 2^a \\ &\leq (W'R')^{3^{i+1}(i+1)!} 2^{(6^i i! 3(i+1)+1)a} \\ &\leq (W'R')^{3^{i+1}(i+1)!} 2^{(6^i i! 3(i+1)2)a} \\ &= (W'R')^{3^{i+1}(i+1)!} 2^{6^{i+1}(i+1)! a} \end{aligned}$$

□

Theorem 14. *Suppose a net under consideration has benefit depth K. There is a non-deterministic algorithm that decides if there is a firing sequence covering M_{cov} from M_0 in space $\mathcal{O}(\log |M_0| + \log n + (\log W' + \log R')6^{K+2} K! m^3 \log m)$.*

Proof. Since there are b buffers in the net, $\ell(b)$ gives an upper bound on the length of the shortest P-covering run. Therefore, there exists a P-covering run iff there is one of length at most $\ell(b)$. From Lemma 13 we get

$$\ell(b) \leq b(g(K))^{3b} 2^a \leq m(g(K))^{3m} 2^a \leq m \left((W'R')^{3^K K! 2^{6^K K! a}}\right)^{3m} 2^a \leq m \left((W'R')^{6^{K+1} K! a}\right)^{3m} 2^a$$

Hence $\ell(b) \leq m(W'R')^{6^{K+2} K! m^2}$. A nondeterministic algorithm can guess a sequence of transitions of this length and verify that it is P-covering from M_0. The memory needed is dominated by a counter to count up to maximum $\ell(b)$ and the memory needed to store intermediate markings. The memory needed for the counter is $\mathcal{O}((\log W' + \log R')6^{K+2} K! m^2 \log m)$ and to store markings we need $\mathcal{O}(\log |M_0| + \log n + (\log W' + \log R')6^{K+2} K! m^3 \log m)$. □ □

Given a net, its benefit depth K can be computed in polynomial time. Hence, the upper bound on the memory requirement in the above theorem is space constructible and the well known Savitch's theorem can be applied to determinize the above algorithm (see any standard text on complexity theory). The memory required will still be polynomial in the size of the input net and this gives us the paraPSPACE algorithm.

For later use in section 5, we name the exponent $6^{K+2} K! m^2$ used in the above proof $expcov(1)$, and let $expcov(i) = expcov(1)^i$.

4 Benefit depth and boundedness

In this section, we will tighten Rosier and Yen's analysis [24] and prove that the complexity of boundedness problem is paraPSPACE when parameterized by benefit depth. As in coverability, we segregate transitions that reduce tokens from a place and those that do not.

Definition 15. *Let $U \subseteq B$ be a subset of buffers, $Q \subseteq P$ a subset of places and M a vector. A Q-run σ from M is said to be U-**self-covering** if it can be decomposed as $\sigma_1\sigma_2$ with $M \xrightarrow{\sigma_1} M_1 \xrightarrow{\sigma_2} M_2$, $M_2 \geq M_1$ and for all $p \in U$, $M_2(p) > M_1(p)$. We call σ_2 as the **pumping portion** of the self-covering sequence.*

It is well known that a place p is unbounded iff there is a firing sequence that is U-self-covering from the initial marking[2] for some $U \subseteq P$ with $p \in U$. In the rest of this section, we will fix a non-empty subset U of places and refer to U-self-covering sequences as self-covering sequences. Let $T_{dep}(p) = \{t \in T_{ben}(p) \mid \forall p' \in Ind(p) : Pre(p', t) = 0\}$.

Definition 16. *Let $C \subseteq Q \subseteq P$ and $p \in B$ be a buffer. Let $scov^p(Q, M)$ be the length of the shortest Q-run in $T_{ben}(p)^*$ that is self-covering from the vector M with the pumping portion of the sequence in $T_{dep}(p)^*$. If there is no such sequence, define $scov^p(Q, M)$ to be 0. Let $s_1(i) = \max\{scov^p(Q, M) \mid M$ a vector, $|Q \cap Ben(p) \cap B| = i\}$. Also, let $scov(Q, M)$ be the length of the shortest self-covering Q-run from the vector M and 0 if there is no such sequence. Let $s(i) = \max\{scov(Q, M) \mid M$ a vector, $|Q \cap B| = i\}$.*

Lemma 17. *For $0 \leq i < b$, $s(i+1) \leq (W^2 s_1(K))^{poly(m)} + s_1(K) + (W s_1(K) + 2)s(i)$ for $poly(m)$ a polynomial in m with degree independent of W, m, K.*

Proof. Suppose that $Q = Q_{i+1} = C \cup A$ with $|A| = i + 1$ and that there is a self-covering Q_{i+1}-run from some vector M. If this run is $W s_1(K)$-bounded for Q_{i+1}, the required result is a consequence of [24, Lemma 2.2].

Otherwise, let $\sigma_1\sigma_2$ be a self-covering Q_{i+1}-run from M such that $M \xrightarrow{\sigma_1} M'$ and M' is the first vector to contain more than $W s_1(K)$ tokens in some place $p \in A$. Let σ_3 be the pumping portion of $\sigma_1\sigma_2$. Without loss of generality, we can assume that length of σ_1 is at most $(W s_1(K))^{i+1} 2^a$. Let $Q_i = Q_{i+1} \setminus \{p\}$. Now, $\sigma_2\sigma_3$ is a self-covering Q_i-run from M'. By definition, there is a self-covering Q_i-run σ_2' of length at most $s(i)$. Let $\sigma_2' = \sigma_3'\sigma_4'$ where σ_4' is the pumping portion of σ_2'. By applying Lemma 8 repeatedly, rearrange σ_3' into $\tau_1\tau_2$ and σ_4' into $\tau_1'\tau_2'$ such that $\tau_1, \tau_1' \in T_{ind}(p)^*$ and $\tau_2, \tau_2' \in T_{ben}(p)^*$. Let $M' \xrightarrow{\tau_1} M_1 \xrightarrow{\tau_2} M_2 \xrightarrow{\tau_1'} M_3 \xrightarrow{\tau_2'} M_4$ (see Fig. 4). Since $\tau_1'\tau_2'$ is the pumping portion, $M_4 > M_2$.

We claim that $M_3 \geq M_2$. Suppose not. Let p' be a place such that $M_3(p') < M_2(p')$. Since $\tau_1' \in T_{ind}(p)^*$ and transitions in $T_{ind}(p)$ don't decrease tokens from $Ben(p)$, $p' \in Ind(p)$. Since $\tau_2' \in T_{ben}(p)^*$ and transitions in $T_{ben}(p)$ don't increase tokens in $Ind(p)$, $M_4(p') \leq M_3(p') < M_2(p')$, which contradicts $M_4 > M_2$. Hence, $M_3 \geq M_2$.

Case 1: $M_3 = M_2$. In this case $\tau_1\tau_2\tau_2'$ is a self-covering Q_i-run from M' with τ_2' as the pumping portion. In other words, $\tau_2\tau_2'$ is a self-covering Q_i-run from M_1. Also, for any $p' \in Ind(p)$ and any transition t occurring in τ_2', $Pre(p', t) = 0$ (otherwise, some other transition t' in τ_2' would have to satisfy $Post(p', t') \geq 1$

[2] We thank an anonymous FSTTCS referee for pointing out a mistake here.

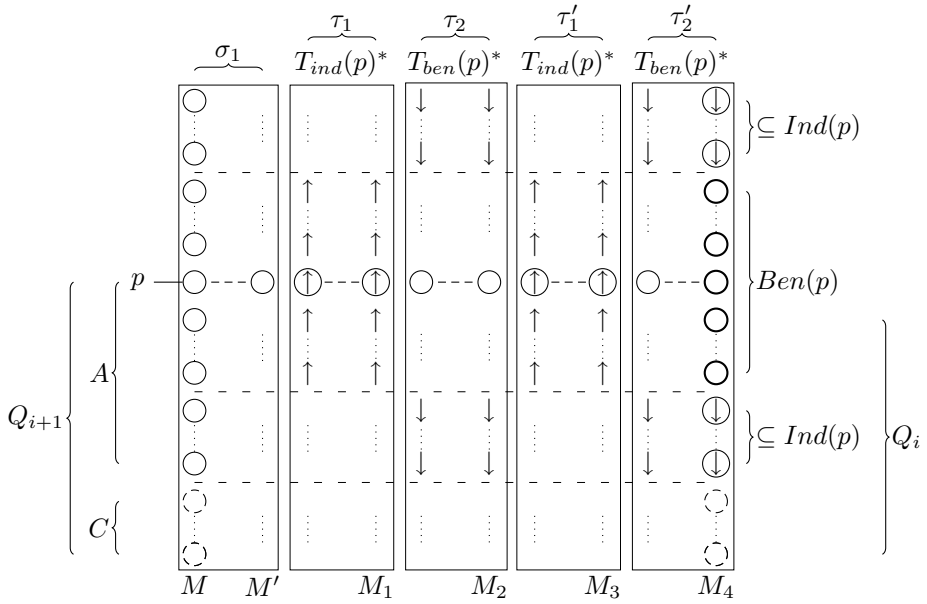

Figure 4: Sequences and bounds used in the proof of Lemma 17

in order to maintain $M_4 > M_3$, which is not possible since $\tau_2' \in T_{ben}(p)^*$). Since $\tau_2\tau_2'$ is a self-covering Q_i-run in $T_{ben}(p)^*$ from M_1 with pumping portion in $T_{dep}(p)^*$, by Definition 16, we conclude that there is a self-covering Q_i-run in $T_{ben}(p)^*$ from M_1 whose length is at most $s_1(|Q_i \cap Ben(p) \cap B|) \leq s_1(K)$.

Case 2: $M_3 > M_2$. In this case, although τ_1' strictly increases the number of tokens in some unbounded buffers, it may not do so for all buffers in U. We need to do some more work to achieve that. We partition the buffers into four subsets $B^u_{ben}, B^c_{ben}, B^u_{ind}$ and B^c_{ind}. $B^u_{ben} = (Ben(p) \cap U) \cup \{p' \in Ben(p) \setminus U \mid M_4(p') > M_2(p')\}$ are the buffers in $Ben(p)$ that are pumped up by $\tau_1'\tau_2'$ while $B^c_{ben} = Ben(p) \setminus B^u_{ben}$ are the buffers in $Ben(p)$ that are not pumped up by $\tau_1'\tau_2'$. $B^u_{ind} = (Ind(p) \cap U) \cup \{p' \in Ind(p) \setminus U \mid M_3(p') > M_2(p')\}$ are the buffers in $Ind(p)$ that are pumped up by $\tau_1'\tau_2'$ while $B^c_{ind} = Ind(p) \setminus B^u_{ind}$ are the buffers in $Ind(p)$ that are not pumped up by $\tau_1'\tau_2'$. Since $\tau_2' \in T_{ben}(p)^*$ cannot increase tokens in $Ind(p)$, it follows that for all $p' \in B^u_{ind}$, $M_3(p') > M_2(p')$. For the same reason, for all $p' \in B^c_{ind}$ and $t \in T_{ben}(p)$, $Pre(p', t) = 0$.

For all $p' \in B^c_{ben}$, p' is not pumped up by $\tau_1'\tau_2'$ due to two possible reasons:

- Neither τ_1' nor τ_2' increase pumps up tokens in p' or
- τ_1' pumps up tokens in p' but τ_2' decreases the tokens so that after walking $\tau_1'\tau_2'$, number of tokens in p' doesn't change.

Accordingly, we will further partition B^c_{ben} into $B^c_{ben}(in) = \{p' \in B^c_{ben} \mid M_3(p') > M_2(p')\}$ and $B^p_{ben}(nin) = B^p_{ben} \setminus B^p_{ben}(in)$. For all $p' \in B^c_{ben}(nin)$,

$M_4(p') = M_3(p')$. The increase in number of tokens in places in B^u_{ben} can be either due to τ'_1 or τ'_2 or both. So, we further partition B^u_{ben} into $B^u_{ben}(ind)$ and $B^u_{ben}(ben) = B^u_{ben} \setminus B^u_{ben}(ind)$ such that for all $p' \in B^u_{ben}(ind)$, $M_3(p') > M_2(p')$. The job of τ'_2 is to "pump up" number of tokens in $B^u_{ben}(ben)$ without decreasing "too many" tokens in places in $B^u_{ind} \cup B^u_{ben}(ind) \cup B^p_{ben}(in)$. However, τ'_2 might decrease a few tokens from places in $B^u_{ind} \cup B^u_{ben}(ind) \cup B^p_{ben}(in)$. If we disregard this action of τ'_2 on $B^u_{ind} \cup B^u_{ben}(ind) \cup B^p_{ben}(in)$, the only other effect of τ'_2 is to ensure that for all $p' \in B^u_{ben}(ben)$, $M_4(p') > M_3(p')$ and for all $p' \in B^c_{ben}(nin)$, $M_4(p') = M_3(p')$. This effect can be achieved by another run τ''_2 of length at most $s_1(k)$ (in fact $|\tau_2| + |\tau''_2| \leq s_1(k)$). Since τ''_2 may decrease tokens from places in $B^u_{ind} \cup B^u_{ben}(ind) \cup B^p_{ben}(in)$, we will compensate for it by firing τ'_1 $Ws_1(K)$ times before τ''_2.

Now, let $M_2 \xrightarrow{\tau_1'^{Ws_1(K)+1}} M'_3 \xrightarrow{\tau''_2} M'_4$. We claim that $\tau_1\tau_2\tau_1'^{Ws_1(K)+1}\tau''_2$ is a self-covering Q_i-run from M', with $\tau_1'^{Ws_1(k)+1}\tau''_2$ as the pumping portion. We have to prove that it is a Q_i-run from M', $M'_4 \geq M_2$ and that for all $p' \in U$, $M'_4(p') > M_2(p')$. Since $M' \xrightarrow{\tau_1} M_1 \xrightarrow{\tau_2} M_2 \xrightarrow{\tau'_1} M_3$, $M_3 \geq M_2$ and $\tau_1\tau_2\tau'_1$ is a Q_i-run from M', $\tau_1\tau_2\tau_1'^{Ws_1(K)+1}$ is also a Q_i-run from M'. We prove the remaining properties for every place p' by looking at which partition p' is in.

1. $p' \in B^u_{ben}(ind) \cup B^u_{ind} \cup B^c_{ben}(in)$. Then, $M'_3(p') > M_2(p') + Ws_1(K)$. Since $|\tau''_2| \leq s_1(k)$, $M'_4(p') > M_2(p')$.
2. $p' \in B^u_{ben}(ben)$. Then, $M'_3(p') = M_2(p')$ and $M'_4(p') > M'_3(p')$ (since τ''_2 pumps up tokens in places from $B^u_{ben}(ben)$). Hence, $M'_4(p') > M_2(p')$.
3. $p' \in B^c_{ben}(nin) \cup B^c_{ind}$. Then, $M'_4(p') = M'_3(p') = M_2(p')$.

In both cases 1 and 2, σ'_2 can be replaced by another self-covering Q_i-run σ''_2 from M' whose length is at most $s(i) + s_1(K) + (Ws_1(K)+1)s(i)$ and that contains at most $s_1(K)$ transition occurrences from $T_{ben}(p)$. Since $M'(p) \geq Ws_1(K)$ and only transitions in $T_{ben}(p)$ decrease tokens from p, $\sigma_1\sigma''_2$ is a self-covering Q_{i+1}-run from M. □

The following lemmas give recurrence relations for length of self-covering sequences in $T_{ben}(p)^*$. The proofs are similar to those of corresponding lemmas in [24] with the additional fact that transitions in $T_{ben}(p)$ don't increase tokens in $Ind(p)$. As before, $W' = \max\{W, 2\}$.

Lemma 18. *Let $C \subseteq Q \subseteq P$ and $p \in B$ a buffer. For $c \in \mathbb{N}$, suppose there is a self-covering Q-run in $T_{ben}(p)^*$ from some vector M which is c-bounded for $Q \cap Ben(p) \cap B$. If its pumping portion is in $T_{dep}(p)^*$, then a similar sequence exists whose length is at most $(W'c2^a)^{poly(K)}$ for $poly(K)$ some polynomial in K whose degree is independent of W, c, a, K.*

Proof. The proof of this lemma is very similar to the corresponding ones in [23, 24]. Suppose $\sigma = \sigma_1\sigma_2$ is a run satisfying the properties given in the lemma with σ_2 being the pumping portion. Since σ_1 is in $T_{ben}(p)^*$, there are at

most k buffers that are in Q that increase their tokens while walking σ_1 from M. Hence, following an argument similar to the one in Lemma 10, we can assume that length of σ_1 is at most $c^K 2^a$. Next, consider the pumping portion σ_2. Note that transitions in σ_2 affect at most K buffers and a component places. Hence, σ_2 can be decomposed into a sequence σ_s and some Q-loops (runs that start and end in vectors that are equal when restricted to Q), such that length of σ_s is at most $(c^K 2^a + 1)^2$. Now, the fact that σ_s and the Q-loops together form a pumping portion can be represented by a system of equations $\mathbf{Bx} \geq \mathbf{b}$, where the matrix $\mathbf{B}$ contains one row for every place and one column for every Q-loop. Now, observe that component places are not affected by Q-loops. Hence, rows corresponding to component places can be removed from $\mathbf{B}$. Of the remaining buffers, transitions in σ_2 affect at most K. Hence, all rows except the K corresponding to the above buffers can also be removed from $\mathbf{B}$. Thus, our system of equations has at most K rows. In addition, each entry in the remaining $\mathbf{B}$ is of absolute value at most $Wc^K 2^a$. Hence, there are at most $(2(Wc^K 2^a) + 1)^K$ columns in B. To find a shorter pumping portion, it suffices to find a smaller solution to $\mathbf{Bx} \geq \mathbf{b}$. We can use [24, Lemma 2.1] by letting $d_1 = K$ and $d = (W'c2^a)^{K^2}$ to conclude that there is a solution where each Q-loop occurs at most $(W'c2^a)^{K^k}$ times. By replacing these Q-loops back into σ_s and combining with σ_1, we get a self-covering Q-run from M whose length is at most $(W'c2^a)^{K^k}$ for some constant k. □

Lemma 19. *$s_1(0) \leq (W'2^a)^{poly(K)}$ and $s_1(i+1) \leq (W'^2 s_1(i) 2^a)^{poly(K)}$.*

Proof. For $s_1(0)$, all buffers can go into negative values while walking a self-covering sequence. Since component places are 1-bounded, we can put $r = 1$ in Lemma 18 to get the result.

For $s_1(i+1)$, suppose $Q_{i+1} = Q \subseteq P$ such that $Q_{i+1} \cap Ben(p) \cap B = A'$ and $|A'| = i + 1$ for some buffer p. Suppose there is a self-covering Q_{i+1}-run in $T_{ben}(p)^*$ from some vector M with its pumping portion in $T_{dep}(p)^*$.

Case 1: If the above sequence is $Ws_1(i)$-bounded for A', the required result is a consequence of Lemma 18.

Case 2: Otherwise, let the above sequence be $\sigma_1\sigma_2$ with $M \xrightarrow{\sigma_1} M'$ and σ_3 being the pumping portion of $\sigma_1\sigma_2$, where M' is the first intermediate marking with some place (say p') in A' having more than $Ws_1(i)$ tokens. We can assume length of σ_1 to be at most $(Ws_1(i))^{i+1}2^a$. Let $Q_i = Q_{i+1} \setminus \{p'\}$. Now, $\sigma_2\sigma_3$ is a self-covering Q_i-run in $T_{ben}(p)^*$ from M'. σ_3 is the pumping portion of this sequence and is in $T_{dep}(p)^*$. Hence, by definition, there is a self-covering Q_i-run $\sigma_2' \in T_{ben}(p)^*$ from M' with length at most $s_1(i)$ whose pumping portion is in $T_{dep}(p)^*$. Since $M'(p') \geq Ws_1(i)$, $\sigma_1\sigma_2'$ is a self-covering Q_{i+1}-run in $T^*_{ben(p)}$ from M, whose length is at most $(Ws_1(i))^{i+1}2^a + s_1(i) \leq (W'^2 s_1(i) 2^a)^{poly(K)}$. □

Now we give upper bounds for these recurrence relations and use them in a nondeterministic algorithm. A technical point is that the recurrence relation in Lemma 17 for $s(i)$ starts from $i = 1$ (unlike that in Lemma 9). This avoids the

calculation of an upper bound for $s(u)$ using Lemma 20 below from containing terms m^K in the exponent, which is not acceptable in paraPSPACE algorithms.

Lemma 20. *For $0 < i < b$, we have $s_1(i) \leq W'^{2(i+1)poly(K^{i+1})}2^{a(i+1)poly(K^{i+1})}$, as also $s(i) \leq 2^{i-1}(4Ws_1(K))^{i-1}(W^2s_1(K))^{poly(m)} + (4Ws_1(K))^i s(0)$.*

Proof. Bound on $s_1(i)$ is by induction on i. For the base case $i = 0$, $s_1(0) \leq (W'2^a)^{poly(K)}$.

$$\begin{aligned}
s_1(i+1) &\leq (W'^2 s_1(i)2^a)^{poly(K)} \\
&\leq W'^{2poly(K)}2^{apoly(K)}\left(W'^{2(i+1)poly(K^{i+1})}2^{a(i+1)poly(K^{i+1})}\right)^{poly(K)} \\
&\leq W'^{2(i+2)poly(K^{i+2})}2^{a(i+2)poly(K^{i+2})}
\end{aligned}$$

Bound on $s(i)$ is by induction on i. For the base case $i = 1$, Lemma 17 implies $s(1) \leq (W^2s_1(K))^{poly(m)} + s_1(K) + (Ws_1(K) + 2)s(0) \leq (W^2s_1(K))^{poly(m)} + 4Ws_1(K)s(0)$.

$$\begin{aligned}
s(i+1) &\leq (W^2s_1(K))^{poly(m)} + s_1(K) + (Ws_1(K) + 2)s(i) \\
&\leq (W^2s_1(K))^{poly(m)} + s_1(K)(1 + Ws(i) + 2s(i)) \\
&\leq (W^2s_1(K))^{poly(m)} + 4Ws_1(K)s(i) \\
&\leq (W^2s_1(K))^{poly(m)} + \\
&\quad 4Ws_1(K)\left(2^{i-1}(4Ws_1(k))^{i-1}(W^2s_1(K))^{poly(m)} + (4Ws_1(K))^i s(0)\right) \\
&\leq 2^i(4Ws_1(K))^i(W^2s_1(K))^{poly(m)} + (4Ws_1(K))^{i+1}s(0)
\end{aligned}$$

□

Theorem 21. *There is a nondeterministic algorithm that decides if a net is bounded in space $\mathcal{O}(\log|M_0| + \log W'K^{cK}m^c a + m\log n)$ where c is some constant.*

Proof. Since there are b buffers in the net, $s(b)$ gives an upper bound on the length of the shortest self-covering sequence from the initial marking M_0. By Lemma 2.3 in [24], $(Wn)^{cm}$ is an upper bound for $s(0)$. Using Lemma 20, it can be seen that $W'^{daK^{cK}m^c}n^{cm}$ is an upper bound for $s(b)$ for some constants c and d.

A non-deterministic algorithm can guess a sequence of transitions of length at most $s(b)$ and verify that it is a self-covering P-run from M_0. The memory needed is dominated by a counter to count upto maximum of $s(b)$ and store the intermediate markings. The memory needed for the counter is $\mathcal{O}(\log W'K^{cK}m^c a + m\log n)$ and memory needed for intermediate markings is $\mathcal{O}(\log|M_0| + \log W'K^{cK}m^c a + m\log n)$. □

5 The model checking algorithm

We now show that checking whether a given system (N, M_0) satisfies a given formula ϕ of the logic defined in sub-section 2.1 can be done in paraPSPACE with benefit depth as the parameter. This requires a lot of technical work. First of all, we simplify the kind of formulas that our algorithm has to handle by nondeterministically choosing a disjunct from a disjunctive subformula. We then end up with ϕ a sequence of conjuncts $\beta_1, \ldots, \beta_c, \kappa$, where each β_i is of the form $\{\tau_1, \cdots \tau_r\} < \omega$ or $\{\tau_1, \cdots \tau_r\} = \omega$ and κ consists of conjunctions of nested **EF** modalities over $\tau \geq c$ formulas. If we can check such formulas in paraPSPACE, Savitch's theorem ensures that satisfiability of ϕ can be checked in paraPSPACE.

For checking β_i, we need the following lemma. Recall that every term τ gives a function $L_\tau : P \to \mathbb{N}$ such that τ is syntactically equivalent to $\sum_{p \in P} L_\tau(p)p$.

Lemma 22. *$N, M_0 \models \{\tau_1, \ldots, \tau_r\} = \omega$ iff there exists a U-self-covering sequence for some $U \subseteq P$ such that for every $j \in \{1 \ldots, r\}$, there is a $p_j \in U$ with $L_{\tau_j}(p_j) \geq 1$.*

Proof. ($\Leftarrow$) If there is a U-self-covering sequence as stated, the pumping portion of the sequence can be fired arbitrarily many times so that we have $\forall c \in \mathbb{N}$ $\exists M \in \mathcal{R}(N, M_0)$ such that for all $j \in \{1, \ldots, r\}$ $\sum_{p \in P} L_{\tau_j}(p)M(p) > c$.

($\Rightarrow$) Suppose $N, M_0 \models \{\tau_1, \ldots, \tau_r\} = \omega$. By semantics, we get $\forall c \in \mathbb{N}$, $\exists M \in \mathcal{R}(N, M_0)$ such that for all $j \in \{1, \ldots, r\}$ $\sum_{p \in P} L_{\tau_j}(p)M(p) > c$. Hence, we can conclude that for all $c \in \mathbb{N}$, there are buffers $p_1^c, p_2^c, \ldots, p_r^c$ and $M^c \in \mathcal{R}(N, M_0)$ such that $M^c(p_j^c) > c \wedge L_{\tau_j}(p_j^c) \geq 1$ for all $j \in \{1, \ldots, r\}$. For each $c \in \mathbb{N}$, let $U^c = \{p_1^c, \ldots, p_r^c\}$. Since the sequence $U^1, U^2, \ldots$ is infinite and there are only finitely many subsets of B, at least one subset of B occurs infinitely often in this sequence. Let U be this subset. We will now prove that there is a U-self-covering sequence using some results about coverability trees [9, Section 4.6].

Recall that in Karp-Miller tree, markings $M : P \to \mathbb{N}$ are extended to ω-markings $\overline{M} : P \to \mathbb{N} \cup \{\omega\}$, by mapping unbounded places to ω. We first claim that there is some reachable ω-marking $\overline{M}$ in the coverability tree of (N, M_0) such that for all $p \in U$, $\overline{M}(p) = \omega$. Suppose not. Then, for every reachable ω-marking $\overline{M}$, there is some place $p \in U$ such that $\overline{M}(p) < \omega$. Let c be the maximum of such bounds. Then, by [9, Theorem 22], for every marking $M \in \mathcal{R}(N, M_0)$, there exists $p \in U$ such that $M(p) \leq c$, a contradiction. Hence, there is a reachable ω-marking $\overline{M}$ in the coverability tree of (N, M_0) such that for all $p \in U$, $\overline{M}(p) = \omega$. Now, the required U-self-covering sequence can be constructed [9, Theorem 21]. □

Hence, checking of β_i can be done in paraPSPACE by using results of section 4.

We now consider verifying the formulas κ, which are of the form $\gamma \wedge \mathbf{EF}(\kappa_1) \wedge \cdots \wedge \mathbf{EF}(\kappa_r)$, with γ having only conjunctions of $\tau \geq c$ formulas. We call γ the **content** of κ and $\kappa_1, \ldots, \kappa_r$ as the **children** of κ. Each of the children may have their own content and children, thus generating a tree with nodes Γ, with

κ at the root of this tree. We will represent nodes of this tree by sequences of natural numbers, 0 being the root.

The maximum length of sequences in Γ is one more than the nesting depth of the **EF** modality in κ and we denote it by D. Let $[D] = \{0, 1, \ldots, D-1\}$. If $\alpha \in \Gamma$ is a tree node that represents the formula $\kappa(\alpha) = \gamma \wedge \mathbf{EF}(\kappa_1) \wedge \cdots \wedge \mathbf{EF}(\kappa_r)$, $content(\alpha) = \gamma$ denotes the content of the node α. Let $ratio(\tau \geq c) = max\{\lceil c/L_\tau(p) \rceil \mid L_\tau(p) \neq 0, p \in P\}$. Defining $\max(\emptyset) = 0$, we define the maximum ratio at height i in the tree by $ratio(i) = \max\{ratio(\tau \geq c) \mid \tau \geq c$ appears as a conjunct in $content(\alpha)$ for some $\alpha \in \Gamma, |\alpha| = i+1\}$. Recall from Definition 6 that b is the number of buffers and $\ell'(M)$ the length of the shortest run covering M using all the buffers $\ell(b, M)$.

Definition 23. *Given a formula κ and a system (N, M_0), the bound function $f : [D] \times P \to \mathbb{N}$ is defined as follows. We use $f(j)$ for the marking defined by $f(j)(p) = f(j, p)$.*

- $f(D-1, p) = ratio(D-1)$,
- $f(D-i, p) = \max\{ratio(D-i), W\ell'(f(D-i+1)) + f(D-i+1, p)\}$, $1 < i < D$,
- $f(0, p) = M_0(p)$.

A guess function $h : \Gamma \times P \to \mathbb{N}$ is any function that satisfies $h(\alpha, p) \leq f(|\alpha| - 1, p)$ for all $\alpha \in \Gamma$ and $p \in P$. If h is a guess function, $h(\alpha)$ is the marking defined by $h(\alpha)(p) = h(\alpha, p)$.

If a given system satisfies the formula $\kappa = \gamma \wedge \mathbf{EF}(\kappa_1) \wedge \cdots \wedge \mathbf{EF}(\kappa_r)$, then there exist firing sequences $\sigma_{01}, \ldots, \sigma_{0r}$ that are all enabled at the initial marking M_0 such that $M_0 \xrightarrow{\sigma_{0i}} M_{0i}$ and M_{0i} satisfies κ_i. In general, if κ generates a tree with set of nodes Γ, then there is a set of sequences $\{\sigma_\alpha \mid \alpha \in \Gamma \setminus \{0\}\}$ and set of markings $\{M_\alpha \mid \alpha \in \Gamma\}$ such that $M_\alpha \xrightarrow{\sigma_{\alpha j}} M_{\alpha j}$ for all $\alpha, \alpha j \in \Gamma$ and M_α satisfies $content(\alpha)$ for all $\alpha \in \Gamma$.

Lemma 24. *There exist sequences $\{\mu_\alpha \mid \alpha \in \Gamma \setminus \{0\}\}$ and markings $\{M_\alpha \mid \alpha \in \Gamma\}$ such that $M_\alpha \xrightarrow{\mu_{\alpha j}} M_{\alpha j}$ for all $\alpha, \alpha j \in \Gamma$ with M_α satisfying $content(\alpha)$ and $|\mu_\alpha| \leq \ell'(f(|\alpha| - 1))$ iff there exist sequences $\{\sigma_\alpha \mid \alpha \in \Gamma \setminus \{0\}\}$ and markings $\{M'_\alpha \mid \alpha \in \Gamma\}$ (M'_0 should be equal to M_0) such that $M'_\alpha \xrightarrow{\sigma_{\alpha j}} M'_{\alpha j}$ for all $\alpha, \alpha j \in \Gamma$ with M'_α satisfying $content(\alpha)$.*

Proof. ($\Rightarrow$) Since M_α satisfies $content(\alpha)$, we can take $M'_\alpha = M_\alpha$ and $\sigma_\alpha = \mu_\alpha$.

($\Leftarrow$) Consider the following guess function:

$$h(\alpha, p) = \begin{cases} M_0(p) & \text{if } \alpha = 0 \\ M'_\alpha(p) & \text{if } \alpha \neq 0 \text{ and } M'_\alpha(p) \leq f(|\alpha| - 1, p) \\ f(|\alpha| - 1, p) & \text{otherwise} \end{cases}$$

By definition, $h(\alpha) \leq M'_\alpha$ and $h(\alpha) \leq f(|\alpha| - 1)$. Since $\sigma_{\alpha j}$ is a firing sequence that covers $M'_{\alpha j}$ from M'_α, there exist sequences $\mu_{\alpha j}$ that cover $h(\alpha j)$ starting

from M'_α whose length is at most $\ell'(h(\alpha j))$ (and hence at most $\ell'(f(|\alpha j|-1))$). We claim that there exist markings $\{M_\alpha \mid \alpha \in \Gamma\}$ such that $M_\alpha \xrightarrow{\mu_{\alpha j}} M_{\alpha j}$ for all $\alpha, \alpha j \in \Gamma$ and that M_α satisfies $content(\alpha)$ for all $\alpha \in \Gamma$.

First, we claim that every $\mu_{\alpha j}$ can be fired from M_α and that every place p will satisfy at least one of the following two conditions:

1. $M_{\alpha j}(p) \geq M'_{\alpha j}(p)$
2. $M_{\alpha j}(p) \geq f(|\alpha j|-1, p)$

We will prove this claim by induction on $|\alpha|$.

Base case: $|\alpha| = 1$. μ_{0j} is a firing sequence of length at most $\ell'(h(0j))$ that covers $h(0j)$ starting from M_0. The claim is clear by the definition of $h(0j)$.

Induction step: We want to prove that $\mu_{\alpha j}$ can be fired at M_α and that $M_{\alpha j}$ satisfies the stated claims. We will prove these for an arbitrary place p. By induction hypothesis, either $M_\alpha(p) \geq M'_\alpha(p)$ or $M_\alpha(p) \geq f(|\alpha|-1, p)$.

First, suppose that $M_\alpha(p) \geq M'_\alpha(p)$. Since $\mu_{\alpha j}$ covers $h(\alpha j)$ starting from M'_α, $M_{\alpha j}(p) \geq h(\alpha j)(p)$ and there are no intermediate markings between M_α and $M_{\alpha j}$ where p receives negative number of tokens. Also, since $M_{\alpha j}(p) \geq h(\alpha j)(p)$, either $M_{\alpha j}(p) \geq M'_{\alpha j}(p)$ or $M(\alpha j)(p) \geq f(|\alpha j|-1, p)$.

Second, suppose that $M_\alpha(p) \geq f(|\alpha|-1, p)$. $|\mu_{\alpha j}| \leq \ell'(h(\alpha j))$ and $h(\alpha j) \leq f(|\alpha j|-1)$ by definition. Hence $\ell'(h(\alpha j)) \leq \ell'(f(|\alpha j|-1))$ and $|\mu_{\alpha j}| \leq \ell'(f(|\alpha j|-1))$. By definition of $f(|\alpha|-1, p)$, we get $M_\alpha(p) \geq W\ell'(f(|\alpha j|-1)) + f(|\alpha j|-1, p)$. $\mu_{\alpha j}$ will remove at most $W\ell'(f(|\alpha j|-1))$ tokens from p and hence, at least $f(|\alpha j|-1, p)$ tokens will be left in place p at marking $M_{\alpha j}$. Therefore, $M_{\alpha j}(p) \geq f(|\alpha j|-1, p)$.

This completes the induction and hence the claim.

Now, we will prove that each M_α satisfies $content(\alpha)$. For each conjunct $\tau \geq c$ in $content(\alpha)$, we will prove that $\sum_{p \in P} L_\tau(p) M_\alpha(p) \geq c$, where L_τ is the positive linear combination represented by τ. If $c = 0$, then the required result can be obtained by just observing that both $L_\tau(p)$ and $M_\alpha(p)$ are positive for all $p \in P$. So suppose that $c \neq 0$. Let $Q_\tau = \{p \in P \mid L_\tau(p) \neq 0\}$. We distinguish between two cases:

1. For some $p \in Q_\tau$, $M_\alpha(p) \geq f(|\alpha|-1, p)$. In this case, $M_\alpha(p) \geq f(|\alpha|-1, p) \geq \frac{c}{L_\tau(p)}$. Hence, $L_\tau(p) M_\alpha(p) \geq c$.
2. For all $p \in Q_\tau$, $M_\alpha(p) < f(|\alpha|-1, p)$. In this case, for all $p \in Q_\tau$, $M_\alpha(p) \geq M'_\alpha(p)$. Since M'_α satisfies $content(\alpha)$, we have $\sum_{p \in Q_\tau} L_\tau(p) M'_\alpha(p) \geq c$. Therefore, $\sum_{p \in Q_\tau} L_\tau(p) M_\alpha(p) \geq c$.

□ □

To derive an upper bound for $f(i)$ to use in a nondeterministic algorithm, let $R = \max\{ratio(\tau \geq c) \mid \tau \geq c \text{ is a subformula of } \kappa\}$, $R' = \max\{R, 2\}$ and $W' = \max\{W, 2\}$. Recall that $D-1$ is the nesting depth of **EF** and note that boundedness and coverability can be expressed with $D \leq 2$.

Lemma 25. *For $i \geq 2$, $f(D-i, p) \leq (i+1) R' W \ell'(f(D-i+1))$.*

Proof. By induction on i.

Base case: $i = 2$

$$\begin{aligned} f(D-2,p) &\leq \max\{R, W\ell'(f(D-1)) + f(D-1,p)\} \\ &\leq R + W\ell'(f(D-1)) + f(D-1,p) \\ &\leq R + W\ell'(f(D-1)) + R \\ &\leq 2R + W\ell'(f(D-1)) \\ &\leq 2R'W\ell'(f(D-1)) \end{aligned}$$

Induction step:

$$\begin{aligned} f(D-i-1,p) &\leq \max\{R, W\ell'(f(D-i)) + f(D-i,p)\} \\ &\leq R + W\ell'(f(D-i)) + (i+1)R'W\ell'(f(D-i+1)) \\ &\leq R'W\ell'(f(D-i)) + (i+1)R'W\ell'(f(D-i)) \\ &= (i+2)R'W\ell'(f(D-i)) \end{aligned}$$

□

Lemma 26. *Recall from the end of section 3 that* $expcov(i) = (6^{K+2}K!m^2)^i$. *Then* $\ell'(f(D-1)) \leq m(W'R')^{expcov(1)}$ *and* $\ell'(f(D-i)) \leq m\prod_{j=D-i}^{D}\left((D-j+1)W'^2R'm\right)^{expcov(i+j+1-D)}$.

Proof. $\ell'(f(D-1)) \leq m(W'R')^{expcov(1)}$ is by Lemma 13. Next result is by induction on i.

Base case: $i = 2$. Since $f(D-2,p) \leq 2R'W\ell'(f(D-1))$ and $\ell'(f(D-2)) \leq m(W'R')^{expcov(1)}$ where $r' = \max\{f(D-2,p) \mid p \in P\}$, we get

$$\begin{aligned} \ell'(f(D-2)) &\leq m(W'2R'W\ell'(f(D-1)))^{q(1)} \\ &\leq m(2W'^2R'm(W'R')^{expcov(1)})^{expcov(1)} \\ &\leq m(2W'^2R'm)^{expcov(1)}(W'R')^{expcov(2)} \end{aligned}$$

Induction step: Since $f(D-i-1,p) \leq (i+2)R'W'\ell'(f(D-i))$, we have

$$\begin{aligned} \ell'(f(D-i-1)) &\leq m(W'(i+2)R'W'\ell'(f(D-i-1)))^{expcov(1)} \\ &\leq m\left((i+2)W'^2R'm\prod_{j=D-i}^{D}((D-j+1)W'^2R'm)^{expcov(i+j+1-D)}\right)^{expcov(1)} \\ &= m\left((i+2)W'^2R'm\right)^{expcov(1)}\prod_{j=D-i}^{D}\left((D-j+1)W'^2R'm\right)^{expcov(i+1+j+1-D)} \\ &= m\prod_{j=D-i-1}^{D}\left((D-j+1)W'^2R'm\right)^{expcov(i+1+j+1-D)} \end{aligned}$$

□

Theorem 27. *Given a net and a formula ϕ, if the benefit depth of the net is treated as a parameter and the nesting depth D of **EF** modality in the formula is treated as a constant, then there is a* para-PSPACE *algorithm that checks if the net satisfies the given formula.*

Proof. First reduce ϕ to the form $\gamma \wedge \kappa$ by nondeterministically choosing disjuncts from subformulas of ϕ, as explained in the beginning of this section. Since γ can be verified by using the boundedness algorithm, it remains to verify κ. By Lemma 24, it is enough for a nondeterministic algorithm to guess sequences $\sigma_{\alpha j}$, $\alpha j \in \Gamma$ of lengths at most $\ell'(f(|\alpha j| - 1))$ and verify that they satisfy the formula. Using bounds given by Lemma 26 and an argument similar to the one in the proof of Theorem 14, it can be shown that the space used is exponential in K and polynomial in the size of the net and numeric constants in the formula. This gives the paraPSPACE algorithm. □ □

The space requirement of the above algorithm will have terms like m^{2D} and hence it will not be paraPSPACE if D is treated as a parameter instead of a constant.

6 Conclusion

We considered nets communicating with buffers. These are infinite-state concurrent systems allowing 1-safe Petri net components communicating through synchronization, which in turn communicate asynchronously through a fixed set of buffers. We identified the parameter benefit depth that measures the maximum number of other buffers that any one buffer can influence. We showed that based on this parameter, paraPSPACE algorithms can be obtained for the coverability and boundedness problems. Note that this does *not* yield a paraPSPACE algorithm for the reachability problem. Whether benefit depth can yield such an algorithm is open; for work of this kind we refer to Kostin [18]. We then extended the above technique to show that satisfiability of formulas of the logic given in sub-section 2.1 can be checked in paraPSPACE if the nesting depth of **EF** quantifiers in such formulas is treated as a constant.

Readers familiar with the repeated control state reachability problem in [14] may infer that arguments similar to Lemma 17 can be employed for that problem too. However, we do not get a paraPSPACE result in terms of benefit depth for model checking linear time μ-calculus because Habermehl's reduction of this problem to repeated control state reachability constructs a bigger net, its benefit depth might be greater than in the original one.

References

[1] M. F. Atig, A. Bouajjani, and T. Touili. On the reachability analysis of acyclic networks of pushdown systems. In *CONCUR*, volume 5201 of *LNCS*, pages 356–371, 2008.

[2] M. F. Atig and P. Habermehl. On Yen's path logic for Petri nets. In *RP 2009*, volume 5797 of *LNCS*, pages 51–63, 2009.

[3] D. Berwanger, A. Dawar, P. Hunter, and S. Kreutzer. Dag-width and parity games. In *STACS'06*, volume 3884 of *LNCS*, pages 524–536. Springer-Verlag, 2006.

[4] D. Brand and P. Zafiropulo. On communicating finite-state machines. *JACM*, 30(2):323–342, April 1983.

[5] D. Caucal. On the regular structure of prefix rewriting. *TCS*, 106:61–86, 1992.

[6] G. Cécé, A. Finkel, and S. Purushothaman Iyer. Unreliable channels are easier to verify than perfect channels. *Inf. Comput.*, 124(1):20–31, 1996.

[7] A. Cheng, J. Esparza, and J. Palsberg. Complexity results for 1-safe nets. *Theoret. Comp. Sci.*, 147(1-2):117–136, 1995.

[8] J. Desel and J. Esparza. *Free choice Petri nets*, volume 40 of *Cambridge Tracts in Theoretical Computer Science*. Cambridge University Press, 1995.

[9] J. Desel and W. Reisig. *Place transition Petri nets*, volume 1491 of *LNCS*. 1998.

[10] R. G. Downey and M. R. Fellows. *Parameterized complexity*. Springer-Verlag, 1999.

[11] L.C. Eggan. Transition graphs and star-height of regular events. *Michigan Math. J.*, 10(4):385–397, 1963.

[12] J. Esparza. *Decidability and complexity of Petri net problems — An introduction*, volume 1491 of *LNCS*, pages 374–428. 1998.

[13] J. Flum and M. Grohe. Describing parameterized complexity classes. *Inf. Comput.*, 187(2):291–319, 2003.

[14] P. Habermehl. On the complexity of the linear-time μ-calculus for Petri-nets. In *ATPN '97*, volume 1248 of *LNCS*, pages 102–116, 1997.

[15] R. Howell, L.E. Rosier, and H.-C. Yen. A taxonomy of fairness and temporal logic problems for petri nets. *Theoret. Comp. Sci.*, 82(2):341–372, 1991.

[16] R.M. Karp and R.E. Miller. Parallel program schemata. *JCSS*, 3(2):147–195, May 1969.

[17] S.R. Kosaraju. Decidability of reachability in vector addition systems. In *Proc. 14th STOC*, pages 267–281. ACM, 1982.

[18] A.E. Kostin. Using transition invariants for reachability analysis of Petri nets. In V. Kordic, editor, *Petri net: theory and applications*, pages 435–458. I-Tech Edu. Pub., 2008.

[19] R. Lipton. The reachability problem requires exponential space. Yale university, 1975.

[20] E.W. Mayr. An algorithm for the general Petri net reachability problem. *SIAM J. Comput.*, 13(3):441–460, 1984.

[21] J. Obdržálek. DAG-width – connectivity measure for directed graphs. In *SODA'06*, pages 814–821. ACM-SIAM, 2006.

[22] C.A. Petri. *Kommunikation mit Automaten.* PhD thesis, Inst. Instrumentelle Math., 1962.

[23] C. Rackoff. The covering and boundedness problems for vector addition systems. *Theoret. Comp. Sci.*, 6:223–231, 1978.

[24] L.E. Rosier and H.-C. Yen. A multiparameter analysis of the boundedness problem for vector addition systems. *J. Comput. Syst. Sci.*, 32(1):105–135, 1986.

[25] P. Schnoebelen. Verifying lossy channel systems has nonprimitive recursive complexity. *Inf. Proc. Lett.*, 83(5):251–261, 2002.

[26] R. Valk and G. Vidal-Naquet. Petri nets and regular languages. *JCSS*, 23:299–325, 1981.

[27] H.-C. Yen. A unified approach for deciding the existence of certain petri net paths. *Inf. Comput.*, 96(1):119–137, 1992.