Verifying Generalized Soundness of Workflow Nets

Kees van Hee, Olivia Oanea*, Natalia Sidorova, and Marc Voorhoeve

Department of Mathematics and Computer Science
Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
{k.m.v.hee, o.i.oanea, n.sidorova, m.voorhoeve}@tue.nl

Abstract. We improve the decision procedure from [10] for the problem of generalized soundness of workflow nets. A workflow net is generalized sound iff every marking reachable from an initial marking with k tokens on the initial place terminates properly, i.e. it can reach a marking with k tokens on the final place, for an arbitrary natural number k. Our new decision procedure not only reports whether the net is sound or not, but also returns a counterexample in case the workflow net is not generalized sound. We report on experimental results obtained with the prototype we made and explain how the procedure can be used for the compositional verification of large workflows.

Keywords: Petri nets; workflows; verification; soundness.

1 Introduction

Petri nets are intensively used in workflow modeling [1,2]. Workflow management systems are modeled by *workflow nets* (WF-nets), i.e. Petri nets with one initial and one final place and every place or transition being on a directed path from the initial to the final place. The execution of a case is represented as a firing sequence that starts from the initial marking consisting of a single token on the initial place. The token on the final place with no garbage (tokens) left on the other places indicates the *proper termination* of the case execution. A model is called *sound* iff every reachable marking can terminate properly.

In [9] we showed that the traditional notion of soundness from [1] is not compositional, and moreover, it does not allow for handling of multiple cases in the WF-net. We introduced there a notion of *generalized soundness* that amounts to the proper termination of all markings obtained from markings with multiple tokens on the initial place, which corresponds to the processing of batches of cases in the WF-net. We proved that generalized soundness is compositional w.r.t. refinement, which allows the verification of soundness in a compositional way.

* Supported by the NWO Open Competitie project "Modeling and Verification of Business Processes" (MoveBP), project number 612.000.315.

I. Virbitskaite and A. Voronkov (Eds.): PSI 2006, LNCS 4378, pp. 235–247, 2007.

The generalized soundness problem is decidable and [10] gives a decision procedure for it. The problem of generalized soundness is reduced to two checks. First, some linear equations for the incidence matrix are checked. Secondly, the proper termination of a finite set of markings is checked. This finite set of markings is computed from an over-approximation of the set of reachable markings that has a regular algebraic structure. In practice, this set turns out to be very large, which seriously limits the applicability of the decision procedure from [10].

In this paper we show that the check of generalized soundness can be reduced to checking proper termination for a much smaller set of markings, namely minimal markings of the set from [10]. We describe a new decision procedure for soundness. Additionally, our procedure produces a counterexample in case a WF-net turns out to be unsound, showing a reachable marking that cannot terminate properly and a trace leading to it.

We implemented our decision procedure in a prototype tool and performed a series of experiments with it. The experimental results confirmed that the new procedure is considerably more effective than the old one. When applied together with standard reduction techniques in a compositional way, it allows us to check soundness of real-life examples.

Related work. For some subclasses of workflow nets (e.g. well-handled, free-choice, extended free-choice, asymmetric choice where every siphon includes at least one trap, extended non-self controlling workflow nets), 1-soundness implies generalized soundness (see [13]). A different decision procedure for generalized soundness was presented in [17], where the generalized soundness problem is reduced to the home marking problem in an extension of the workflow net, which is an *unbounded* net. The home marking problem is shown to be decidable in [7] by reducing it to the reachability problem for a finite set of markings. Checking generalized soundness in this way can however hardly be done in practice, since the complexity of the reachability problem for unbounded nets is still an open question, and the procedure for checking reachability, though known from 1981 [11], has never been implemented due to its complexity (the known algorithms require non-primitive recursive space) [15]. In our procedure we also check reachability for a finite set of markings, but reachability is checked on *bounded* nets only.

The paper is structured as follows. Section 2 introduces basic notions. Section 3 presents the new decision procedure, and Section 4 provides details about the implementation and experimental results. Section 5 covers conclusions and directions for future work.

2 Preliminaries

We denote the set of natural numbers by $\mathbb{N}$, the set of non-zero natural numbers by $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$, the set of integers by $\mathbb{Z}$, the set of rational numbers by $\mathbb{Q}$ and the set of non-negative rational numbers by $\mathbb{Q}^+$. We denote the set of all finite words over a finite set S by S^*. The empty word is denoted by ϵ.

A *Petri net* is a tuple $N = (P, T, F^+, F^-)$, where

- P and T are two disjoint non-empty finite sets of *places* and *transitions* respectively;
- F^+ and F^- are mappings $(P \times T) \to \mathbb{N}$ that are *flow functions* from transitions to places and from places to transitions respectively.

$F = F^+ - F^-$ is the *incidence matrix* of net N.

We denote the set of *output transitions* of a place p by $p^\bullet$, i.e. $p^\bullet \overset{\text{def}}{=} \{t \mid F^+(p,t) > 0, t \in T\}$, and the set of output transitions of $Q \subseteq P$ by $Q^\bullet$, i.e. $Q^\bullet \overset{\text{def}}{=} \bigcup_{p \in Q} p^\bullet$. Similarly, ${}^\bullet p \overset{\text{def}}{=} \{t \mid F^-(p,t) > 0, t \in T\}$ denotes the set of *input transitions* of a place p and ${}^\bullet Q \overset{\text{def}}{=} \bigcup_{p \in Q} {}^\bullet p$ the set of input transitions of $Q \subseteq P$. A place p with ${}^\bullet p = \emptyset$ is called a *source place* and a place q with $q^\bullet = \emptyset$ is called a *sink place.*

Markings, the states (configurations) of a net, represent the distribution of tokens in the places are interpreted as vectors $m \colon P \to \mathbb{N}$. We denote by $\bar{0}$ the zero marking (vector) of an arbitrary (defined by the context) dimension and by $\bar{p}$, for some $p \in P$, the vector such that $\bar{p}(p) = 1$ and $\bar{p}(p') = 0$ for all $p' \in P$ such that $p' \neq p$. A *marked net* is a tuple (N, m), where N is a net and m is a marking.

A transition $t \in T$ is *enabled* in a marking m if $F^-(p,t) \leq m(p)$, for all $p \in P$. If t is enabled in a marking m (denoted by $m \xrightarrow{t}$), t may *fire* yielding a new marking m', denoted by $m \xrightarrow{t} m'$, where $m'(p) = m(p) - F^-(p,t) + F^+(p,t)$, for all $p \in P$. We extend this homomorphically to the firing sequences $\sigma \in T^*$, denoted by $m \xrightarrow{\sigma} m'$. We say that m' is reachable from m and write $m \xrightarrow{*} m'$ when there exists $\sigma \in T^*$ such that $m \xrightarrow{\sigma} m'$. We denote the set of all markings reachable from m by $\mathcal{R}(m)$. Similarly, $\mathcal{S}(m)$ denotes the set of markings that can reach m. A marked net (N, m_0) is *bounded* iff there exists $n \in \mathbb{N}$ such that for all $m \in \mathcal{R}(m_0)$, $m(p) < n$ for all $p \in P$. A marked net (N, m_0) is *t-live* iff for all markings $m \in \mathcal{R}(m_0)$ there exists a marking m' such that $m \xrightarrow{*} m'$ and $m \xrightarrow{t}$.

Let σ be a sequence of transitions. The *Parikh vector* $\overrightarrow{\sigma}$ maps every transition t of σ to the number of occurrences of t in σ. Let $m \xrightarrow{\sigma} m'$. Then the *marking equation* [8] holds: $m' = m + F \cdot \overrightarrow{\sigma}$. Note that the reverse is not true: not every marking m' that can be represented as $m + F \cdot x$, for some $x \in \mathbb{N}^T$, is reachable from the marking m.

A subset of places Q is called a *trap* if $Q^\bullet \subseteq {}^\bullet Q$. A subset $Q \subseteq P$ is called a *siphon* if ${}^\bullet Q \subseteq Q^\bullet$. A trap or a siphon is called *proper* iff it is nonempty. Traps have the property that once marked they remain marked, whereas unmarked siphons remain unmarked whatever transition sequence occurs [6].

A place invariant is a row vector $I \colon P \to \mathbb{Q}$ such that $I \cdot F = 0$. We denote a matrix that consists of basis place invariants as rows by $\mathcal{I}$. We say that markings m and m' *agree on a place invariant* I if $I \cdot m = I \cdot m'$ (see [8]). The main property of place invariants is that any two markings m, m' such that $m \xrightarrow{*} m'$ agree on all place invariants, i.e. $\mathcal{I} \cdot m = \mathcal{I} \cdot m'$.

Batch Workflow Nets. Workflow nets are used to model the processing of tasks in workflow processes. The initial and final nodes indicate respectively the initial and final states of cases flowing through the process.

Definition 1. *A Petri net N is a* Workflow net (WF-net) *iff:*

1. *N has two special places: i and f. The initial place i is a source place, i.e. ${}^\bullet i = \emptyset$, and the final place f is a sink place, i.e. $f^\bullet = \emptyset$.*
2. *For any node $n \in (P \cup T)$ there exists a path from i to n and a path from n to f (*path property *of WF-nets.)*

In [10], we introduced two structural correctness criteria for WF-nets based on siphons and traps:

non-redundancy. Every place can be marked and every transition can fire, provided there are enough tokens in the initial place.
non-persistency. All places can become empty again.

As proven in [10], non-redundancy and non-persistency are behavioral properties which imply restrictions on the structure of the net: all proper siphons of the net should contain i and all proper traps should contain f.

Following [10], we define a class of nets called batch workflow nets (BWF-nets). Actually, BWF-nets are WF-nets without redundant and persistent places, i.e. workflow nets that satisfy minimal correctness requirements.

Definition 2. *A* Batch Workflow net (BWF-net) *N is a Petri net having the following properties:*

1. *N has a single source place i and a single sink place f.*
2. *Every transition of N has at least one input and one output place.*
3. *Every proper siphon of N contains i.*
4. *Every proper trap of N contains f.*

Workflow nets were originally used to model the execution of one case. In [10], we defined a generalized notion of soundness for modeling the execution of batches of cases in WF-nets.

Definition 3. *A WF-net N is called k-*sound *for some $k \in \mathbb{N}$ iff*

$$\mathcal{R}(k \cdot \bar{i}) \subseteq \mathcal{S}(k \cdot \bar{f}).$$

A WF-net N is called generalized sound *iff*

$$\forall k \in \mathbb{N}\colon \mathcal{R}(k \cdot \bar{i}) \subseteq \mathcal{S}(k \cdot \bar{f}).$$

For the sake of brevity, we omit the word "generalized" in the rest of the paper. In [10], it has been shown that a WF-net N is sound iff a certain derived BWF-net N' is sound. The derivation is straightforward and only uses structural analysis of the net.

We assume that the reader is familiar with the basics of convexity theory (see e.g. [16]). A *convex polyhedral cone* $\mathcal{H}$ over $\mathbb{Q}^m$ can be defined by its finite set of generators $E \subseteq \mathbb{Q}^m$, i.e. $\mathcal{H} = \{\Sigma_{e \in E} \lambda_e \cdot e \mid \lambda_e \in \mathbb{Q}^+\}$. A generator e is called *trivial* if $e = \bar{j}$, for some $1 \leq j \leq m$.

3 Decision Procedure of Soundness for BWF-Nets

In this section, we describe our decision procedure for checking generalized soundness of BWF-nets. Our decision procedure improves the one from [10] since we check proper termination for a much smaller set of markings. We give an algorithm for computing this set of markings and enhance the procedure with a backward reachability algorithm that checks whether these markings are backward reachable from some final marking. If not, our procedure returns a counterexample.

We start by briefly discussing the decision procedure from [10]. We first give some necessary conditions of soundness:

Lemma 4. [10] *Let N be a sound BWF-net. Then,*

1. $\mathcal{I} \cdot \bar{i} = \mathcal{I} \cdot \bar{f}$ *(i and f agree on the basis place invariants);*
2. $\mathcal{I} \cdot x = \bar{0}$ *for* $x \in (\mathbb{Q}^+)^P$ *iff* $x = \bar{0}$.

The conditions of Lemma 4 can be easily checked by standard algebraic techniques. Further on, we we consider only nets that meet these two conditions.

The set of all markings reachable from some initial marking of N is given by $\mathcal{R} = \bigcup_{k \in \mathbb{N}} \mathcal{R}(k \cdot \bar{i})$. Due to the marking equation, $\mathcal{R}(k \cdot \bar{i})$ is a subset of $\mathcal{G}_k = \{k \cdot \bar{i} + F \cdot v \mid v \in \mathbb{Z}^T\} \cap \mathbb{N}^P$. Note that the reverse is not true.

Let $m \in \mathcal{G}_k$, for some $k \in \mathbb{N}$. Then $\mathcal{I} \cdot m = \mathcal{I} \cdot (k \cdot \bar{i})$. Since condition 2 of Lemma 4 holds, $\mathcal{G}_k \cap \mathcal{G}_\ell = \emptyset$ for all $k, \ell \in \mathbb{N}$, with $k \neq l$, and we can define the *i-weight* function $w(m)$ for m as k. Now consider the set $\mathcal{G} = \bigcup_{k \in \mathbb{N}} \mathcal{G}_k$, i.e. $\mathcal{G} = \{k \cdot \bar{i} + F \cdot v \mid k \in \mathbb{N} \wedge v \in \mathbb{Z}^T\} \cap \mathbb{N}^P$. We will say that a marking $m \in \mathcal{G}$ *terminates properly* if $m \xrightarrow{*} w(m) \cdot \bar{f}$.

Lemma 5. [10] *Let $m_1, m_2 \in \mathcal{G}$ be markings that terminate properly and $m = \lambda_1 \cdot m_1 + \lambda_2 \cdot m_2$ for some $\lambda_1, \lambda_2 \in \mathbb{N}$. Then $m \in \mathcal{G}$ and it terminates properly.*

Theorem 6. [10] *Let N be a BWF-net. Then N is sound iff for any $m \in \mathcal{G}$, $m \xrightarrow{*} w(m) \cdot \bar{f}$.*

$\mathcal{G}$ is an infinite set, but unlike $\mathcal{R}$ it has a regular algebraic structure, which allows to reduce the check of proper termination to a check on a finite set of markings.

The following lemma is proved by using convexity analysis [16], notably the Farkas-Minkowski-Weyl theorem.

Lemma 7. [10] *Let $\mathcal{H} \overset{def}{=} \{a \cdot \bar{i} + F \cdot v \mid a \in \mathbb{Q}^+ \wedge v \in \mathbb{Q}^T\} \cap (\mathbb{Q}^+)^P$. Then there exist a finite set $E_\mathcal{G} \subseteq \mathcal{G}$ of generators of $\mathcal{H}$, i.e. $\mathcal{H} = \{\Sigma_{e \in E_\mathcal{G}} \lambda_e \cdot e \mid \lambda_e \in \mathbb{Q}^+\}$.*

The soundness check can now be reduced to the check of proper termination for a finite set of markings:

Theorem 8. [10] *Let N be a BWF-net such that the conditions of Lemma 4 hold and let $\Gamma \overset{def}{=} \{\sum_{e \in E_\mathcal{G}} \alpha_e \cdot e \mid 0 \leq \alpha_e \leq 1 \wedge e \in E_\mathcal{G}\} \cap \mathcal{G}$, where $E_\mathcal{G} \subseteq \mathcal{G}$ is a finite set of generators. Then N is sound iff all markings in Γ terminate properly.*

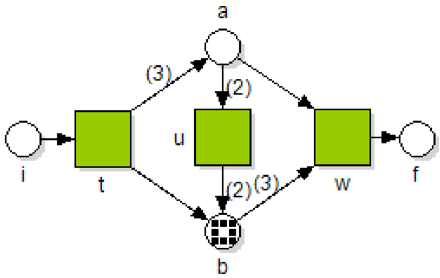

Fig. 1. Example of a BWF-net

In fact, Γ represents the set of integer points of the bounded convex polyhedral cone (also called polytope) having the set $E_{\mathcal{G}}$ as generators.

The decision procedure from [10] comprises the following steps:

1. Find an invariant matrix $\mathcal{I}$ and check whether $\mathcal{I} \cdot \overline{i} = \mathcal{I} \cdot \overline{f}$ and whether $\mathcal{I} \cdot x = \overline{0}$ has only the trivial solution on $\mathbb{N}^P$;
2. Find a set $E_{\mathcal{G}} \subset \mathcal{G}$ of generators of $\mathcal{H}$;
3. Compute the set of markings Γ;
4. Check for all markings $m \in \Gamma$ that $m \xrightarrow{*} w(m) \cdot \overline{f}$.

Example 9. We illustrate the main steps of the algorithm on the BWF-net in Figure 1. First we compute $\mathcal{I} = (4, 1, 1, 4)$. The first two conditions are satisfied: $(4, 1, 1, 4) \cdot \overline{i} = (4, 1, 1, 4) \cdot \overline{f}$ and $(4, 1, 1, 4) \cdot x = \overline{0}$ implies $x = \overline{0}$. Further we compute $\mathcal{H} = \{a \cdot \overline{i} + F \cdot v | a \in \mathbb{Q}^+, v \in \mathbb{Q}^T\} \cap (\mathbb{Q}^+)^P = (A+B) \cap C$, where A, B and C are polyhedra having the generators $\{\overline{i}\}$, $\{\pm(3 \cdot \bar{a} + \overline{b} - \overline{i}), \pm(\bar{a} + \overline{b}), \pm(\overline{i} - \bar{a} - 3 \cdot \overline{b})\}$ and $\{\overline{i}, \overline{f}, \bar{a}, \overline{b}\}$, respectively. Next we compute the generators of the polytope: $E_{\mathcal{G}} = \{\overline{i}, \overline{f}, 8 \cdot \bar{a}, 8 \cdot \overline{b}\}$. The markings of Γ have the following form:

$$\Gamma = \{m' | (m' = \sum_{m \in E_{\mathcal{G}} \cup \{3 \cdot \bar{a} + \overline{b}, \bar{a} + 3 \cdot \overline{b}\}; \alpha_m \in \mathbb{N}} \alpha_m \cdot m) \wedge (\overline{0} \leq m' \leq \sum_{e \in E_{\mathcal{G}}} e)\}$$

The size of Γ is very large compared to the size of the net: $|\Gamma| = 44$. Furthermore in order to check whether all markings of Γ terminate properly, we need to build the backward reachability sets $\mathcal{S}(k \cdot \overline{i})$ for $0 \leq k \leq \max_{m \in \Gamma} w(m) = 6$ and check whether they include all markings of Γ. We observe that $8 \cdot \overline{b} \notin \mathcal{S}(2 \cdot \overline{f})$ and therefore the net is not sound.

Steps $1 - 2$ are not computationally costly. The set of markings Γ turns out to be very large in practice, and Step 3 and 4 are thus very expensive for real-life examples. We shall reduce the check of proper terminations of markings from Γ to a check of a smaller set of markings by replacing the last two steps with the following steps:

3'. Compute the set Υ of *minimal markings* of $\mathcal{G}^+ \overset{\text{def}}{=} \bigcup_{k \in \mathbb{N}^+} \mathcal{G}(k \cdot \overline{i})$, i.e.

$$\Upsilon \overset{\text{def}}{=} \{m \mid \forall m' \in \mathcal{G}^+ : m' \leq m \Rightarrow m' = m\}.$$

4'. Check that for all markings $m \in \Upsilon$, $m \xrightarrow{*} w(m) \cdot \bar{f}$. In case this does not hold, give a counterexample, i.e. a trace σ such that $w(m') \cdot \bar{i} \xrightarrow{\sigma} m' \not\xrightarrow{*} w(m') \cdot \bar{f}$, for some m'.

To show that Υ can be used instead of Γ, we first prove an auxiliary lemma.

Lemma 10. *Let N be a BWF-net, $m_1 \in \mathcal{G}_{k_1}$, $m_2 \in \mathcal{G}_{k_2}$, for some $k_1, k_2 \in \mathbb{N}$, and $m_2 > m_1$. Then $k_2 > k_1$.*

Proof. Since $m_2 \in \mathcal{G}_{k_2}$ and $m_1 \in \mathcal{G}_{k_1}$, $m_1 = k_1 \cdot \bar{i} + F \cdot v$ and $m_2 = k_2 \cdot \bar{i} + F \cdot v_2$ for some v_1 and v_2. Hence, $\mathcal{I} \cdot m_1 = \mathcal{I} \cdot k_1 \cdot \bar{i}$ and $\mathcal{I} \cdot m_2 = \mathcal{I} \cdot k_2 \cdot \bar{i}$ and by linearity $\mathcal{I}(m_2 - m_1 + (k_1 - k_2)\bar{i}) = \bar{0}$. Since condition 2 of Lemma 4 holds for N, $m_2 - m_1 + (k_1 - k_2) \cdot \bar{i} \notin (\mathbb{Q}^+)^P \setminus \{\bar{0}\}$. Since $m_2 - m_1$ and $\bar{i}$ are in $(\mathbb{Q}^+)^P$, we deduce that $k_1 - k_2 < 0$. □

The set of markings Υ has the following properties:

- Let $E_\mathcal{G} \subseteq \mathcal{G}$ be a set of minimal generators of $\mathcal{H}$ in $\mathcal{G}$ (i.e. for any $e \in E_\mathcal{G}$ and $e' \in \mathcal{G}$, $e' \leq e$ implies $e = e'$). Then $E_\mathcal{G} \subseteq \Upsilon$. Note that in particular $\bar{i}$, $\bar{f} \in E_\mathcal{G} \subseteq \Upsilon$.
- $\mathcal{G}_1 \subseteq \Upsilon$. Suppose that there is an $m \in \mathcal{G}_1$ such that $m \notin \Upsilon$. Then there is $m' \in \Upsilon$ such that $m' < m$. By Lemma 10, $w(m') < w(m) = 1$, contradiction.

We now formulate our theorem.

Theorem 11. *Let N be a BWF-net such that $\mathcal{I} \cdot \bar{i} = \mathcal{I} \cdot \bar{f}$, $\mathcal{I} \cdot x = \bar{0}$ has only the trivial solution in $(\mathbb{Q}^+)^P$, $\mathcal{G}^+ \overset{def}{=} \{k \cdot \bar{i} + F \cdot v \mid k \in \mathbb{N}^+ \wedge v \in \mathbb{Z}^T\} \cap \mathbb{N}^P$, $\mathcal{H} = \{a \cdot \bar{i} + F \cdot v \mid a \in \mathbb{Q}^+, v \in \mathbb{Q}^T\} \cap (\mathbb{Q}^+)^P$, $E_\mathcal{G} \subseteq \mathcal{G}^+$ be a set of minimal generators of $\mathcal{H}$ in $\mathcal{G}^+$, $\Gamma = \{\sum_{e \in E_\mathcal{G}} \alpha_e \cdot e \mid 0 \leq \alpha_e \leq 1 \wedge e \in E_\mathcal{G}\} \cap \mathcal{G}$, and Υ be the set of minimal markings of $\mathcal{G}^+$. Then:*

1. *N is sound iff for any marking $m \in \Upsilon$, $m \xrightarrow{*} w(m) \cdot \bar{f}$.*
2. *Each marking $m \in \Upsilon$ satisfies $m < M$, where $M(p) = \max_{e \in E_\mathcal{G}} e(p)$, for every $p \in P$.*
3. *$\Upsilon \subset \Gamma$.*

Proof. (1) (⇒) Since N is sound, all markings of $\mathcal{G}$ terminate properly (by Theorem 6). Since $\Upsilon \subseteq \mathcal{G}$, all markings of Υ terminate properly.
(⇐) Let $m \xrightarrow{*} w(m) \cdot \bar{f}$ for every marking m from Υ. We will prove that $m \xrightarrow{*} w(m) \cdot \bar{f}$ for every marking m from Γ, which implies then that N is sound (by Theorem 8).

Let $m \in \Gamma$. We have two cases: $m \in \Upsilon$ and $m \in \Gamma \setminus \Upsilon$. If $m \in \Upsilon$, then $m \xrightarrow{*} w(m) \cdot \bar{f}$. If $m \in (\Gamma \setminus \Upsilon)$, $m > \Delta^0$ for some $\Delta^0 \in \Upsilon$ and by Lemma 10, $w(m) > w(\Delta^0)$, which also implies that $(m - \Delta^0) \in \mathcal{G}^+$.

Set $m^0 = m - \Delta^0$. In case $m^0 \in \Upsilon$, $m^0 \xrightarrow{*} w(m^0) \cdot \bar{f}$. By Lemma 5, since $\Delta^0 \xrightarrow{*} w(\Delta^0) \cdot \bar{f}$, $m \xrightarrow{*} w(m) \cdot \bar{f}$. In case $m^0 \notin \Upsilon$, m^0 can be further written as $m^0 = \Delta^1 + m^1$, where $\Delta^1 \in \Upsilon$ and $m^1 \in \mathcal{G}^+$.

We continue until we reach an $m^{l-1} = m^l + \Delta^l$ with $\Delta^l \in \Upsilon$ and $m^l \in \Upsilon$. Note that the process is finite since $0 < m^{i+1} < m^i$, for $0 \leq i \leq l$. Therefore $m = \sum_{i=0}^{l} \Delta^i + m^l$, where $m^l \in \Upsilon$ and $\Delta^i \in \Upsilon$ for all $i = 0 \ldots l$. Since the markings of Υ terminate properly, we can apply Lemma 5 to $\sum_{i=0}^{l} \Delta^l + m^0$. As a result, $m \xrightarrow{*} w(m) \cdot \bar{f}$.
(2) Suppose that there is a marking $m \in \Upsilon$ such that $m \geq M$. Since $M \geq e$ for every generator $e \in E_{\mathcal{G}}$, we have $\forall e \in E_{\mathcal{G}} \colon m \geq e$. That means that m and e are comparable, which contradicts the hypothesis.
(3) $\Upsilon \subseteq \Gamma$ follows trivially from (2) and the definition of Γ. Furthermore, $\bar{M} = \sum_{e \in E_{\mathcal{G}}} e \in \Gamma$. However $\bar{M} > M$ and from (2), we have that $\bar{M} \notin \Upsilon$, hence $\Upsilon \subset \Gamma$. □

Now we can describe the implementation the steps $2, 3', 4'$.

Computing the generators of the convex polyhedral cone $\mathcal{H}$. $\mathcal{H}$ is given as the intersection of two polyhedra: A with the set of generators $\{\bar{i}\} \cup \{\pm F(t) \mid t \in T\}$ (column vectors of the matrices F and $-F$) and B with the set of generators $\{\bar{p} \mid p \in P\}$ (trivial generators). Let E be a (minimal) set of generators of the convex polyhedral cone $\mathcal{H} = \{a \cdot \bar{i} + F \cdot v \mid a \in \mathbb{Q}^+, v \in \mathbb{Q}^T\} \cap (\mathbb{Q}^+)^P$. All generators of $\mathcal{H}$ can be represented as $a \cdot \bar{i} + F \cdot v$, where $a \in \mathbb{Q}$ and $v \in \mathbb{Q}^T$ can be found by solving linear equations. In order to find the set of generators that are in $\mathcal{G}$ ($E_{\mathcal{G}}$), the generators of $\mathcal{H}$ need to be rescaled. The rescaling factor of each generator is the lcm of the denominators of a and v_t, for all $t \in T$ divided by the gcd of the numerators of them. $\bar{i}$ and $\bar{f}$ are generators of $\mathcal{H}$ with rescaling factor 1.

Computing Υ. The next step is to find Υ — the set of minimal markings of $\mathcal{G}$. Note that the markings of Υ are smaller than the marking M whose components are the maxima of the respective components of the rescaled generators (statement 2 of Theorem 11).

We compute Υ by an optimized enumeration of all vectors m from $\mathbb{N}^P$ which are smaller than M and checking whether $m = k \cdot \bar{i} + F \cdot v$ has a solution in $\mathbb{N}^+$, i.e. whether $m \in \mathcal{G}$. The optimization is due to avoiding the consideration of markings which are greater than some markings already added to Υ.

Checking proper termination for markings of Υ. We need to check that $m \xrightarrow{*} w(m) \cdot \bar{f}$ for all $m \in \Upsilon$. Since condition 2 of Lemma 4 holds, we conclude that $\mathcal{S}(k \cdot \bar{f})$ is a finite set for any k. Therefore we employ a backward reachability algorithm to check proper termination of markings in Υ. Let J be the (finite) set of weights of markings from Υ. The backward reachability algorithm constructs for each i-weight $j \in J$, starting from weight 1, the backward reachability set B_j. We start from the marking $j \cdot \bar{f}$ and continue by adding the markings $\{m - F_t \mid m \in B_j \wedge m - F_t^+ \geq \bar{0} \wedge t \in T\}$, where F_t is column of F corresponding to transition t, until B_j contains all markings from Υ_j or we reach the fixpoint $\mathcal{S}(j \cdot \bar{f})$. In the first case all markings of Υ_j terminate properly; as a

Algorithm 1. Backward reachability check

```
Input: $N = (P, T, F)$, $\Upsilon$, $J = \{w(m) \mid m \in \Upsilon\}$
Output: “the BWF-net is sound” or “the BWF-net is not sound, $m, k$” where
        $m \in \mathcal{G}_k$ and $m \not\xrightarrow{*} k \cdot \bar{f}$.
for $j \in J$ do
    $B_j = \{j \cdot \bar{f}\}$;
    repeat
        $B_j = B_j \cup \{m - F_t \mid \forall p \in P : m(p) \geq F(p,t) \wedge m \in B_j \wedge t \in T\}$
    until a fixpoint is reached or $\Upsilon_j \subseteq B_j$ ;
    if $\Upsilon_j \not\subseteq B_j$ then
        pick $m \in \Upsilon_j \setminus B_j$;
        return (“the BWF-net is not sound”, $m, j$)
    end
end
return (“the BWF-net is sound”)
```

result the BWF-net is sound. In the latter case the markings in Υ_j do not terminate properly; therefore the net is not sound. Note that the backward reachability sets B_j are distinct (since $\mathcal{G}_k \cap \mathcal{G}_\ell = \emptyset$ for any $k \neq \ell$).

This check results either in verdict “sound” (if all markings from Υ terminate properly), or “unsound” together with some marking that does not terminate properly in the contrary case.

Finding a counterexample. Let m be a marking from Υ_j returned by the check above as non-properly terminating. Like all markings from Υ_j, m does not necessarily belong to $\mathcal{R}(j \cdot \bar{i})$. To give a counterexample, we search through $\mathcal{R}(k \cdot \bar{i})$ $(k \geq w(m))$ to find a marking m' reachable from $w(m') \cdot \bar{i}$ and not terminating properly and show a trace σ such that $w(m') \cdot \bar{i} \xrightarrow{\sigma} m'$.

Example 9 continued. We compute Υ for the example from Figure 1:

$$\Upsilon = \{\bar{i}, \bar{f}, 8 \cdot \overline{a}, 8 \cdot \overline{b}, \overline{a} + 3 \cdot \overline{b}, 3 \cdot \overline{a} + \overline{b}\}$$

Note that $|\Upsilon| = 6$, while $|\Gamma| = 44$. Moreover, the maximal i-weight of the markings of Υ is a lot smaller than that of the markings of Γ: $\max_{m \in \Upsilon} w(m) = 2 < \max_{m \in \Gamma} w(m) = 6$. Hence, we need to compute only $\mathcal{S}(\bar{f})$ and $\mathcal{S}(2 \cdot \bar{f})$ instead of $\mathcal{S}(k \cdot \bar{f})$ for $k = 1 \ldots 6$. We find a counterexample $8 \cdot \overline{b} \in \mathcal{R}(2 \cdot \bar{i})$: $2 \cdot \bar{i} \xrightarrow{tt} 6 \cdot \overline{a} + 2 \cdot \overline{b} \xrightarrow{uuu} 8 \cdot \overline{b}$ and conclude that the net is not sound. Figure 1 shows the dead marking.

Example 12. Figure 2 shows a Petri net which is 1-sound, but not 2-sound. In this case $\Upsilon = \Upsilon_1 = \{\bar{i}, \bar{f}, \overline{a}, \overline{b}, \overline{c}\} = E_{\mathcal{G}}$. Using the backward reachability algorithm, we find that the net is not sound and $\overline{b} \in \Upsilon_1$ such that $\overline{b} \not\xrightarrow{*} \bar{f}$. However, $\overline{b} \notin \mathcal{R}(\bar{i})$. We find $2 \cdot \overline{b} + \bar{f} > \overline{b}$ such that $2 \cdot \bar{i} \xrightarrow{tvy} 2 \cdot \overline{b} + \bar{f} \not\xrightarrow{*} 2 \cdot \bar{f}$.

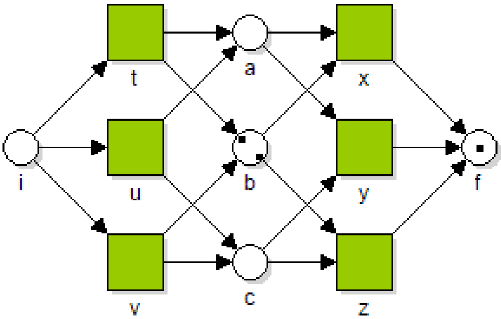

Fig. 2. A net for which $\Upsilon = \Upsilon_1 \not\subseteq \mathcal{R}(\bar{i})$

4 Practical Application of the Decision Procedure

In this section, we we give some details on the implementation of the procedure and experimental results and discuss how to check soundness for large nets compositionally and by using reduction techniques.

Implementation and experimental results. The decision procedure described in Section 3 has been implemented in a prototype tool. The tool uses the Yasper editor [14] for input of batch workflow nets and gives as output the conclusion on soundness and a counterexample in case the net is not sound. The prototype is written in C++ and uses the Parma Polyhedra Library [3,4] for the computation of the minimal set of generators of the convex polyhedral cone $\mathcal{H}$.

The complexity of the procedure is dominated by the complexity of the reachability problem (which is still not known, all known algorithms are non-primitive recursive); however, for BWF-nets modelling real-life business processes the performance turned out to be acceptable. We have run our prototype on a series of examples. The nets were first reduced with the standard reduction rules from [12], which preserve soundness. Table 1 shows the experimental results comparing the size of Γ with the size of Υ. In most of the experiments Υ turned out to be equal to the set of rescaled generators. Our experiments showed that our tool can handle models of business processes of realistic size in reasonable time; a typical case: for a (reduced) BWF-net with $|P| = 18$ and $|T| = 22$, our algorithm checks soundness within 8 seconds.

Using reduction rules to verify soundness. We can apply our procedure in combination with reduction techniques that preserve soundness in order to reduce the size of the net for which we are checking soundness.

We start with introducing the notion of *k-closure of a BWF-net*, which is the strongly connected net obtained by adding a transition whose only input place is the final place, the only output place is the initial place, and the weights of the arcs equal k.

Table 1. Experimental results

Net	Soundness	$\vert P\vert$	$\vert T\vert$	$\vert\Gamma\vert/\vert\Upsilon\vert$	$\max_{m\in\Gamma} w(m)$	$\max_{m\in\Upsilon} w(m)$	$\vert\Upsilon\vert$	Time(ms)
1	sound	23	27	19	75	1	75 $(=\vert E_{\mathcal{G}}\vert)$	19909
2	sound	18	22	11	70	1	70 $(=\vert E_{\mathcal{G}}\vert)$	8005
3	sound	12	12	46	14	1	14 $(=\vert E_{\mathcal{G}}\vert)$	131
4	sound	9	10	57	9	1	9 $(=\vert E_{\mathcal{G}}\vert)$	16
5	sound	9	9	18	10	1	10 $(=\vert E_{\mathcal{G}}\vert)$	26
6	sound	7	8	18	8	2	7 $(=\vert E_{\mathcal{G}}\vert)$	9
7	sound	9	6	8	11	1	11 $(=\vert E_{\mathcal{G}}\vert)$	48
8	sound	6	6	6	6	1	6 $(=\vert E_{\mathcal{G}}\vert)$	9
9	sound	7	5	5	6	1	6 $(=\vert E_{\mathcal{G}}\vert)$	5
10	not 2-sound	5	6	6	5	1	5 $(=\vert E_{\mathcal{G}}\vert)$	5
11	sound	5	5	8	5	1	5	7
12	not 2-sound	4	3	7	6	2	6	8

Definition 13. *The* k-closure of a BWF-net $N = (P, T, F^+, F^-)$ *is a net* $(P, T \cup \{\bar{t}\}, \bar{F}^+, \bar{F}^-)$*, where* $\bar{F}^-(i, \bar{t}) = \bar{F}^+(f, \bar{t}) = k$*,* $\bar{F}^+(i, \bar{t}) = \bar{F}^-(f, \bar{t}) = 0$*,* $\bar{F}^+(p, t) = F^+(p, t)$ *and* $\bar{F}^-(p, t) = F^-(p, t)$ *for all* $(p, t) \in P \times T$*.*

Lemma 14. *The k-closure of a BWF-net N is bounded and $\bar{t}$-live iff N is k-sound.*

Proof. $(\Rightarrow)$ Since the closure of N is $\bar{t}$-live, for all $m \in \mathcal{R}(k \cdot \bar{i})$, there exists an m' such that $m \xrightarrow{*} m' \xrightarrow{\bar{t}} m''$. Boundedness of N implies $m' = k \cdot \bar{f}$ and $m'' = k \cdot \bar{i}$. Thus, N is sound.

$(\Leftarrow)$ Suppose the closure of N is unbounded. Then there exists $m \in \mathcal{R}(k \cdot \bar{i})$ such that $m \xrightarrow{*} m'$ and $m < m'$. Since N is k-sound, $m \xrightarrow{*} k \cdot \bar{f}$ and $m' \xrightarrow{*} k \cdot \bar{f} + m - m'$, which contradicts soundness of N. Hence N is bounded. By k-soundness of N, for all $m \in \mathcal{R}(k \cdot \bar{i})$, $m \xrightarrow{*} k \cdot \bar{f}$. Hence, $m \xrightarrow{*} k \cdot \bar{f} \xrightarrow{\bar{t}} k \cdot \bar{i}$. Thus the closure of N is $\bar{t}$-live. □

Thus, natural candidates for preserving soundness are rules that preserve $\bar{t}$-liveness and boundedness of the closure of the net in both directions, i.e. the closure of the BWF-net is $\bar{t}$-live and bounded iff the reduced closure of the BWF-net is $\bar{t}$-live and bounded. Such rules have been intensively investigated; among them, we recall the place substitution rule and the identical transitions rule of Berthelot [5] and the reduction rules Murata [12] (fusion of series places/transitions, fusion of parallel places/transitions, elimination of self loop transitions).

Let $\mathfrak{R}$ be a set of transformation rules between two k-closures of a BWF-net which preserve boundedness and $\bar{t}$-liveness in both directions (we also assume that $\bar{t}$, i and f are not reduced). Note that since the only initially marked place is i, the transformations from $\mathfrak{R}$ are applied to unmarked places only.

Soundness is preserved by applying rules from $\mathfrak{R}$ to the closure a BWF-net:

Theorem 15. *A BWF-net is sound iff the BWF-net obtained by applying reductions from the set $\mathfrak{R}$ is sound.*

Proof. By Lemma 14 soundness of a BWF-net is equivalent to the boundedness and $\bar{t}$-liveness of the k-closure of the BWF-net, for all $k \in \mathbb{N}$. The latter is equivalent to the boundedness and $\bar{t}$-liveness of the k-closure of the reduced BWF-net, for all $k \in \mathbb{N}$. By applying again Lemma 14, this is equivalent to the soundness of the reduced BWF-net. □

Compositional verification of soundness. In practice it is often needed to verify soundness of large workflow nets that cannot be handled by current verification tools. Therefore, a more efficient approach is needed to handle these cases. Applying simple reduction rules that preserve soundness, like the ones from [12], facilitates the task a lot. The reduced net can then be checked using a compositional approach:

1. Identify BWF-subnets in the original workflow by using classical graph techniques (e.g. by detecting strongly connected components).
2. Check whether the found BWF-subnets are generalized sound using the procedure described.
3. Reduce every sound BWF-subnet to one place and repeat the procedure iteratively, till the soundness of the whole net is determined.

Correctness of the reduction part of Step 3 is justified by Theorem 6 from [9].

5 Conclusion and Future Work

In this paper, we have presented an improved procedure for deciding generalized soundness of BWF-nets. We showed that the problem reduces to checking proper termination for a set of *minimal markings* from the set found in [10], which significantly reduces the number of markings for which proper termination has to be checked. Further, we described a backwards reachability algorithm for checking proper termination for the found set of markings.

As discussed in Section 4, soundness of workflow nets can be checked in a compositional way. In addition to that, our soundness check can be used for compositional verification of Petri net properties. By adapting the proof of Theorem 6 from [9], it is easy to prove that if a Petri net has a subnet which is a generalized sound net whose transitions are labelled by invisible labels, the net obtained by reducing this subnet to one place is branching bisimilar to the original net. For future work, we are interested in the verification of temporal logic properties of Petri nets (not necessarily WF-nets) with using such a reduction technique.

The idea can also be applied to build sound by construction nets in a hierarchical way similarly to Vogler's refinement by modules [18,19].

References

1. W. M. P. van der Aalst. The Application of Petri Nets to Workflow Management. *The Journal of Circuits, Systems and Computers*, 8(1):21–66, 1998.
2. W. M. P. van der Aalst and K. M. van Hee. *Workflow Management: Models, Methods, and Systems.* MIT Press, 2002.

3. R. Bagnara, P. Hill, and E. Zaffanela. *The Parma Polyhedra Library users manual.* Department of Mathematics, University of Parma,Italy. `www.cs.unipr.it/ppl/Documentation`.
4. R. Bagnara, E. Ricci, E. Zaffanella, and P. M. Hill. Possibly not closed convex polyhedra and the Parma Polyhedra Library. In *SAS*, volume 2477 of *LNCS*, pages 213–229, 2002.
5. G. Berthelot. *Verification de Reseaux de Petri.* PhD thesis, Universite Pierre et Marie Curie (Paris), 1978.
6. F. Commoner. *Deadlocks in Petri Nets.* Applied Data Research, Inc., Wakefield, Massachusetts, Report CA-7206-2311, 1972.
7. D. de Frutos Escrig and C. Johnen. Decidability of home space property. Technical report, Univ. de Paris-Sud, Centre d'Orsay, Laboratoire de Recherche en Informatique Report LRI–503, July 1989.
8. J. Desel and J. Esparza. *Free Choice Petri nets.*, volume 40 of *Cambridge Tracts in Theoretical Computer Science.* Cambridge University Press, 1995.
9. K. van Hee, N. Sidorova, and M. Voorhoeve. Soundness and separability of workflow nets in the stepwise refinement approach. In *Proc. of ICATPN'2003*, volume 2679 of *LNCS*, pages 337–356, 2003.
10. K. van Hee, N. Sidorova, and M. Voorhoeve. Generalized soundness of workflow nets is decidable. In *Proc. of ICATPN'2004*, volume 3099 of *LNCS*, pages 197–216, 2004.
11. E. W. Mayr. An algorithm for the general Petri net reachability problem. In *Conference Proceedings of the 13th Annual ACM Symposium on Theory of Computation, STOC'1981*, pages 238–246. ACM, 1981.
12. T. Murata. Petri nets: Properties, analysis and applications. In *Proceedings of the IEEE*, volume 7(4), pages 541–580, 1989.
13. L. Ping, H. Hao, and L. Jian. On 1-soundness and soundness of workflow nets. In *Third Workshop on Modelling of Objects, Components, and Agents Aarhus, Denmark, October 11-13, 2004*, pages 21–36, 2004.
14. R. Post. YASPER Petri net editor. Department of Mathematics and Computer Science, Technical University Eindhoven, The Netherlands. `www.yasper.org`.
15. C. Reutenauer. *The mathematics of Petri nets.* Prentice-Hall, Inc., 1990.
16. A. Schrijver. *Theory of Linear and Integer Programming.* Wiley-Interscience series in discrete mathematics. John Wiley & Sons, 1986.
17. F. Tiplea and D. Marinescu. Structural soundness for workflow nets is decidable. *Information Processing Letters*, 96(2):54–58, 2005.
18. W. Vogler. Behaviour preserving refinement of Petri nets. In *WG*, volume 246 of *LNCS*, pages 82–93. Springer, 1986.
19. W. Vogler. *Modular Construction and Partial Order Semantics of Petri Nets*, volume 625 of *LNCS.* Springer-Verlag, 1992.