# Verifying generalized soundness for workflow nets

# Verifying Generalized Soundness for Workflow Nets

Kees van Hee Olivia Oanea* Natalia Sidorova
Marc Voorhoeve

Department of Mathematics and Computer Science
Technical University Eindhoven
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 [7] for the problem of generalized soundness for workflow nets: "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 $k$". Moreover, our new decision procedure returns a counterexample in case the workflow net is not generalized sound. We also 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 [6] 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 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 us to verify soundness in a compositional way.

The generalized soundness problem is decidable and [7] gives a decision procedure for it. The problem of generalized soundness is reduced to a check of some linear equations for the incidence matrix together with the check of proper termination for a finite set of markings

*Supported by the NWO Open Competitie project MoveBP, Project number 612.000.315

from an over-approximation of the set of reachable marking with a regular algebraic structure. This finite set of markings turns out to be very large in practice, which seriously limits the applicability of the decision procedure from [7].

In this paper we show that the check of proper termination can be reduced to a check of proper termination for a much smaller set of markings, namely minimal markings of the set from [7]. We describe a new decision procedure for soundness. In case a WF-net turns out to be unsound, our procedure produces a counterexample 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 to check soundness of real-life examples.

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

As usual, we denote the set of natural numbers by $\mathbb{N}$, the set of non-zero natural numbers by $\mathbb{N}^+ = \mathbb{N} - \{0\}$, 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 $\epsilon$.

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. $p^\bullet \stackrel{\text{def}}{=} \{t \mid F^+(p,t) > 0, t \in T\}$, and the set of output transitions of $Q \subseteq P$ by $Q^\bullet$, i.e. $Q^\bullet \stackrel{\text{def}}{=} \bigcup_{p \in Q} p^\bullet$. Similarly, ${}^\bullet p \stackrel{\text{def}}{=} \{t \mid F^-(p,t) > 0, t \in T\}$ denotes the set of *input transitions* of a place $p$ and ${}^\bullet Q \stackrel{\text{def}}{=} \bigcup_{p \in Q} {}^\bullet p$ 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 represent the states (configurations) of the net and are interpreted as vectors $m\colon P \to \mathbb{N}$. When we consider a particular ordering on the set of places, $P = \{p_1, \ldots, p_n\}$, where $n = \mid P \mid$, then $m_j \stackrel{\text{def}}{=} m(p_j)$, for $1 \leq j \leq n$. 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 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 $m$, then $t$ may *fire* or *occur* 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 exits $\sigma \in T^*$ 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 $m$.

Let $\sigma$ be a sequence of transitions. The *Parikh vector* $\overrightarrow{\sigma}$ maps every transition $t$ of $\sigma$ to the number of occurrences of $t$ in $\sigma$. Let $m \xrightarrow{\sigma} m'$. Then the *marking equation* 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 (siphon) is a proper trap (siphon) iff it is not empty. Traps have the property that once marked they remain marked, whereas unmarked siphons remain unmarked whatever transition sequence occurs.

A place invariant is a row vector $I\colon P \to \mathbb{Q}$ such that $I \cdot F = 0$. We denote by $\mathcal{I}$ the matrix that consists of basis place invariants as rows. We say that markings $m$ and $m'$ *agree on a place invariant* $I$ if $I \cdot m = I \cdot m'$ (see [5]). 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** A Petri net $N$ is a *workflow net* (WF-net) iff it has two special places — the initial source place $i$ corresponding to the initial state of the processed cases and the final sink place $f$ corresponding to the final state of the processed cases; moreover every place and transition of $N$ is on a directed path from $i$ to $f$.

Following [7], 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 1** *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 $f$.*

We define a property called *generalized soundness* for WF-nets.

**Definition 2** *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 [7], 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. [10]).

## 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 [7] since we need to 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 and if not our procedure returns a counterexample.

We start by briefly discussing the decision procedure from [7]. We first give some necessary conditions for soundness:

**Lemma 1** *[7] 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 $x = \bar{0}$, i.e. $\mathcal{I} \cdot x = \bar{0}$ has only the trivial solution on $\mathbb{N}^P$.*

These conditions can be easily checked and further on, we assume they are satisfied.

The set of all markings reachable from some initial marking of a BWF-net $N$ 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 1 holds, $\mathcal{G}_k \cap \mathcal{G}_\ell = \bar{0}$ for all $k, \ell \in \mathbb{N}$ 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. $\mathcal{G} = \{k \cdot \bar{i} + F \cdot v \mid k \in \mathbb{N} \wedge v \in \mathbb{Z}^T\} \cap \mathbb{N}^P$:

**Theorem 1** *[7] Let $N$ be a BWF-net. Then $N$ is sound iff for any $m \in \mathcal{G}$, $m \xrightarrow{*} w(m)\bar{f}$.*

We will say that a marking $m \in \mathcal{G}$ *terminates properly* if $m \xrightarrow{*} w(m) \cdot \bar{f}$.
$\mathcal{G}$ 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 for a finite set of markings.

The following lemma is proved by using convexity analysis [10], notably the Farkas-Minkowski-Weyl theorem.

**Lemma 2** *[7] Let $\mathcal{H} \stackrel{def}{=} \{a \cdot \bar{i} + F \cdot v \mid a \in \mathbb{Q}^+ \wedge v \in \mathbb{Q}^T\} \cap (\mathbb{Q}^+)^P$. Then there exist a finite set $E_\mathcal{G}$ of generators $e^1 \ldots e^n \in \mathcal{G}$ of $\mathcal{H}$, i.e. $\mathcal{H} = \{\Sigma_{i=1}^n \lambda_i \cdot e^i \mid \lambda_i \in \mathbb{Q}^+\}$.*

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

**Theorem 2** *[7] Let $N$ be a BWF-net such that the conditions of Lemma 1 hold and let $\Gamma \stackrel{def}{=} \{\sum_i \alpha_i \cdot e^i \mid 0 \leq \alpha_i \leq 1 \wedge e^i \in E_\mathcal{G}\} \cap \mathcal{G}$. Then $N$ is sound iff all markings in $\Gamma$ terminate properly.*

In fact, $\Gamma$ represents the set of markings ("integer points") of the bounded convex polyhedral cone having as generators the set of rescaled generators (also called polytope).

The decision procedure from [7] comprises the following steps:

1. Check whether $\mathcal{I} \cdot \bar{i} = \mathcal{I} \cdot \bar{f}$;
2. Check whether $\mathcal{I} \cdot x = \bar{0}$ has only the trivial solution on $\mathbb{N}^P$.
3. Check for all markings $m \in \Gamma$ that $m \xrightarrow{*} w(m) \cdot \bar{f}$.

Steps 1 and 2 are not computationally costly. The set of markings $\Gamma$ turns out to be very large in practice, and Step 3 is thus very expensive for real-life examples. We shall reduce this check to a check for a smaller set of markings. In what follows we will replace the last step with the following step:

**3'.** Check for all markings $m$ of the set $\Upsilon$ that $m \xrightarrow{*} w(m) \cdot \bar{f}$, where $\Upsilon$ is the set of *minimal markings* of $\mathcal{G}^+ \stackrel{\text{def}}{=} \bigcup_{k \in \mathbb{N}^+} \mathcal{G}(k \cdot \bar{i})$, i.e. $\Upsilon \stackrel{\text{def}}{=} \{m \mid \forall\, m' \in \mathcal{G}^+ : m' \leq m \Rightarrow m' = m\}$.

In the rest of this Section, we show that Step 3 can be replaced with Step 3', and $\Upsilon \subseteq \Gamma$, i.e. we reduce the number of markings for which the proper termination has to be checked indeed. For this purpose, we prove the following statements:

**Lemma 3** *Let $m_1 \in \mathcal{G}_{k_1}$ and $m_2 \in \mathcal{G}_{k_2}$ such that $m_2 > m_1$. Then $k_2 > k_1$.*

**Proof 1 (Sketch)** *Suppose that $k_1 \geq k_2$. Then, there is $\epsilon \geq 0$ such that $k_1 = k_2 + \epsilon$.*

*Then, by substitutions we obtain $\mathcal{I} \cdot m_1 = \mathcal{I} \cdot (m_2 + \epsilon \cdot \bar{i})$. Since the equation $\mathcal{I} \cdot (m_2 + \epsilon \cdot \bar{i} - m_1) = \bar{0}$ has only the trivial solution in $(\mathbb{Q}^+)^P$, we conclude that $m_1 = m_2 + \epsilon \cdot \bar{i}$ with $\epsilon \geq 0$. This contradicts the fact that $m_2 > m_1$.* □

**Theorem 3** *Let $N$ be a BWF-net such that $\mathcal{I} \cdot \bar{i} = \mathcal{I} \cdot \bar{f}$ and $\mathcal{I} \cdot x = \bar{0}$ has only the trivial solution in $(\mathbb{Q}^+)^P$, let $\mathcal{G}^+ \stackrel{def}{=} \{k \cdot \bar{i} + F \cdot v \mid k \in \mathbb{N}^+ \wedge v \in \mathbb{Z}^T\} \cap \mathbb{N}^P$, $\Gamma = \{\sum_i \alpha_i \cdot e^i \mid 0 \leq \alpha_i \leq 1 \wedge e^i \in E_{\mathcal{G}}\} \cap \mathcal{G}$, and $\Upsilon$ is the set of minimal markings of $\mathcal{G}^+$. Then:*

1. *$N$ is sound iff for any making $m \in \Upsilon$, $m \xrightarrow{*} w(m) \cdot \bar{i}$.*
2. *Each marking $m \in \Upsilon$ satisfies $m \leq M$, where $M = (\max_i\{e^i_1\}, \ldots, \max_i\{e^i_{|P|}\})$ and $e^i$ are the markings from a set $E_{\mathcal{G}} \subseteq \mathcal{G}^+$ of generators of the cone $\mathcal{H} = \{a \cdot \bar{i} + F \cdot v \mid a \in \mathbb{Q}^+, v \in \mathbb{Q}^T\} \cap (\mathbb{Q}^+)^P$.*
3. *$\Upsilon \subseteq \Gamma$.*

**Proof 2 (Sketch)** *(1) ($\Rightarrow$) This part trivially results from Theorem 2 since $\Upsilon \subseteq \mathcal{G}$.*
*($\Leftarrow$) Let $m \xrightarrow{*} w(m) \cdot \bar{i}$ for every marking $m$ from $\Upsilon$. We will prove that $m \xrightarrow{*} w(m) \cdot \bar{i}$ for every marking $m$ from $\Gamma = \{\sum_i \alpha_i \cdot e^i \mid 0 \leq \alpha_i \leq 1 \wedge e^i \in E_{\mathcal{G}}\} \cap \mathcal{G}$, which implies then that $N$ is sound (Theorem 2).*

*Let $m \in \Gamma$. If $m \in \Upsilon$, $m \xrightarrow{*} w(m) \cdot \bar{i}$. Otherwise $m \in (\Gamma \setminus \Upsilon)$ and it can be represented as $m = m' + \Delta_0$, where $m' \in \Upsilon$ and $\Delta_0 \in \mathcal{G}^+$, $\Delta_0 > \bar{0}$. In case $\Delta_0 \in \Upsilon$, $\Delta_0 \xrightarrow{*} w(\Delta_0) \cdot \bar{f}$. Since $m' \xrightarrow{*} w(m') \cdot \bar{i}$, $m \xrightarrow{*} w(m) \cdot \bar{i}$. In case $\Delta_0 \notin \Upsilon$, $\Delta_0$ can be further written as $\Delta_0 = \Delta_1 + \Delta_2$, where $\Delta_1 \in \Upsilon$ and $\Delta_2 \in \mathcal{G}^+$, $\Delta_2 \geq \bar{0}$. We continue until we reach a $\Delta_{l-1} = \Delta_l + \bar{0}$ with $\Delta_l \in \Upsilon$ (the process is finite since $\Delta_i$ are non-zero vectors from $\mathbb{N}^{|P|}$). Therefore $m = \sum_{i=0}^{l} \Delta_i$, where $\Delta_i \in \Upsilon$. As a result, $m \xrightarrow{*} w(m) \cdot \bar{i}$.*
*(2) Suppose that there is a marking $m \in \Upsilon$ such that $m \geq M$. Since $M \geq e^i$ for any generator*

*$e^i \in E_{\mathcal{G}}$, we have $m \geq e^i$. That means that $m$ and $e^i$ are comparable, which contradicts the hypothesis.*
*(3) follows trivially from (2) and the definition of* $\Gamma$. □

Now we can describe how we check condition $3'$ in practice.

### 3.0.1 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).

### 3.0.2 Computing the rescaled generators of $\mathcal{H}$ that are in $\mathcal{G}$

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 of $\mathcal{G}$ ($E_{\mathcal{G}}$), 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 $\mathcal{H}$ and moreover their rescaling factor is 1.

### 3.0.3 Computing $\Upsilon$

The next step is to find $\Upsilon$ — the set of minimal markings of $\mathcal{G}$. Note that the markings of $\Upsilon$ are smaller than the marking $M$ whose components are the maximums of the respective components of the rescaled generators, i.e. $M = (\max_i\{e_1^i\}, \ldots, \max_i\{e_{|P|}^i\})$ (Theorem 3).

The set of markings $\Upsilon$ has the following properties:

- $E_{\mathcal{G}} \subseteq \Upsilon$, since $\forall\, e^i \in E_{\mathcal{G}}$, $e^i < M$ and $e^i$ are incomparable; 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 3, $w(m') < w(m) = 1$, contradiction.

When computing $\Upsilon$, we make use of the following observations:

**Remark 1** *$\bar{i}, \bar{f} \in \Upsilon$. Let $\Upsilon' = \Upsilon \setminus \{\bar{i}, \bar{f}\}$. We take an ordering on the set of places of the form $P = \{p_1, \ldots, p_s, i, f\}$, where $s =\mid P \mid -2$. Therefore the markings of $\Upsilon'$ have the form $(m_1, \ldots, m_s, 0, 0)$, where $0 \leq m_j \leq M_j$ for all $j \in \{1, \ldots, s\}$.*

*The markings from $\Upsilon'$ are thus less than $M' = (\max_i\{e_1^i\}, \ldots, \max_i\{e_s^i\}, 0, 0)$ $(= M - (0, \ldots, 0, 1, 1))$.*

**Remark 2** *Let $m$ be a given marking. If the equation $m = k \cdot \bar{i} + F \cdot v$ has no solution in $\mathbb{N}^+$ then $m \notin \mathcal{G}$. Otherwise, $m \in \mathcal{G}_k$.*

We compute $\Upsilon'$ by an optimized enumeration of all vectors from $\mathbb{N}^+$ which are smaller than $M$. The optimization is due to avoiding the consideration of markings which are greater than some marking already added to $\Upsilon'$.

**Algorithm 1** Backward reachability check

1: INPUT: $N = (P, T, F)$, $\Upsilon$, $J = \{w(m) \mid m \in \Upsilon\}$
2: OUTPUT: "the BWF-net is sound" or "the BWF-net is not sound, $m, k$" where $m \in \mathcal{G}_k$, $m \not\xrightarrow{*} k \cdot \bar{f}$ and $k = \min\{\ell \mid m \in \Upsilon : \ell \cdot \bar{i} \xrightarrow{\sigma} m \not\xrightarrow{*} \ell \cdot \bar{f}\}$

3: **for** $j \in J$ **do**
4: $B_j = \{j \cdot \bar{f}\}$;
5: **repeat**
6: $B_j = B_j \cup \{m - F_t \mid m - F_t^+ \geq \bar{0} \wedge m \in B_j \wedge t \in T\}$
7: **until** a fixpoint is reached or $\Upsilon_j \subseteq B_j$;
8: **if** $\Upsilon_j \not\subseteq B_j$ **then**
9: pick $m \in \Upsilon_j \setminus B_j$; $\ell = 1$;
10: **loop**
11: **if** $(j + \ell) \cdot \bar{i} \in B_{j+\ell}$ **then**
12: **return**("the BWF-net is not sound", $m, j + \ell$)
13: **else** $\ell$++
14: **end if**
15: **end loop**
16: **end if**
17: **end for**
18: **return**("the BWF-net is sound")

### 3.0.4 Checking proper termination for markings of $\Upsilon$

We need to check that for all $m \in \Upsilon$, $m \xrightarrow{*} w(m) \cdot \bar{f}$. Due to condition 2 of Lemma 1, $\mathcal{S}(k \cdot \bar{f})$ is a finite set for any $k$. Therefore we employ a backward reachability algorithm to check proper termination of markings in $\Upsilon$. Let $J$ be the (finite) set of weights of markings from $\Upsilon$. 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 it either $B_j$ contains all markings from $\Upsilon_j$ or we reach the fixpoint ($\mathcal{S}(j \cdot \bar{f})$). In the first case all markings of $\Upsilon_j$ terminate properly; as a result the BWF-net is sound. In the latter case the markings in $\Upsilon_j$ 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 $\Upsilon$ terminate properly), or "unsound" together with some marking that does not terminate properly in the contrary case.

### 3.0.5 Finding a counterexample

Let $m$ be a marking from $\Upsilon$ returned by the check above as non-properly terminating. Like all markings from $\Gamma$, $m$ does not necessarily belong to $\mathcal{R}$. To give a counterexample, we still need to find a marking reachable from some $k \cdot \bar{i}$ that does not terminate properly. We use the following lemma to find a counterexample:

**Lemma 4** *[7] Let $N$ be a sound BWF-net and let $m \in \mathcal{G}_k$ for some $k \in \mathbb{N}$. Then there exists*

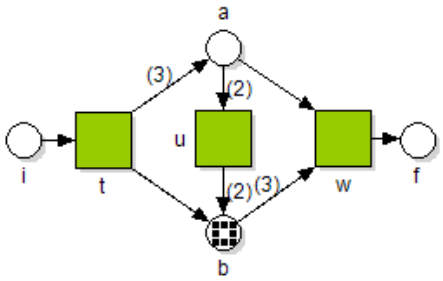


Figure 1: Example of an BWF-net

$\ell \in \mathbb{N}$ *such that* $(k+\ell)\cdot \bar{i} \xrightarrow{*} m + \ell \cdot \bar{f}$.

In order to find a counterexample, we use backward reachability analysis for markings $m+\ell\cdot\bar{f}$, where $d \in \mathbb{N}^+$, starting with $d = 1$. If this backward reachability reaches $(k+\ell)\cdot\bar{i}$, then the net is not $(k+\ell)$-sound and the counterexample is $(k+\ell)\cdot\bar{i} \xrightarrow{*} m+\ell\cdot\bar{f}$ $(\not\xrightarrow{*} (k+\ell)\cdot\bar{f})$.

# 4 Practical Application of the Decision Procedure

In this section, we illustrate the application of the procedure described in the previous section by means of a simple example, discuss how to check soundness for large nets compositionally and we give some details on the implementation of the procedure and experimental results.

### 4.0.6 Example

We illustrate the main steps of the algorithm on the BWF-net in Figure 1. The corresponding polyhedral cone has trivial generators: $E = \{\bar{i}, \bar{f}, \bar{a}, \bar{b}\}$. The set of rescaled generators is $E_{\mathcal{G}} = \{\bar{i}, \bar{f}, 8\cdot\bar{a}, 8\cdot\bar{b}\}$.

Next compute $\Upsilon^*$:

$$\Upsilon = \{(8,0,0,0),(0,8,0,0),(1,3,0,0),(3,1,0,0),(0,0,0,1),(0,0,1,0)\}$$

Note that in this example $\mid \Upsilon \mid = 6$, while $\mid \Gamma \mid = 44$. Thus we gain a lot in comparison with the algorithm from [7].

The backward reachability algorithm finds that $8\cdot\bar{b} \notin \mathcal{S}(2\cdot\bar{f})$ and therefore the net is not sound. The marking $8\cdot\bar{b} \in \mathcal{R}(2\cdot\bar{f})$: $2\cdot\bar{i} \xrightarrow{tt} 6\cdot\bar{a} + 2\cdot\bar{b} \xrightarrow{uuu} 8\cdot\bar{b}$, and the net is not 2-sound. Figure 1 shows the dead marking.

### 4.0.7 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 [8], facilitates the task a lot. The reduced net can then be checked using a compositional approach:

1. Identify sub-BWF-nets in the original workflow by using classical graph techniques (e.g. 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 [6].

#### 4.0.8 Implementation and experimental results

The decision procedure described in Section 3 has been implemented in a prototype tool. The tool uses the Yasper editor [9] 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 recuresive); 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 [8], which preserve soundness. In most of the experiments $\Upsilon$ 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 $\mid P \mid = 18$ and $\mid T \mid = 22$, our algorithm checks soundness within 8 seconds.

## 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 [7], 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 [6], it is easy to prove that if a Petri net has a subnet which is a generalized sound net whose transition 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 [11, 12].

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

[6] 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.

[7] 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.

[8] T. Murata. Petri nets: Properties, analysis and applications. In *Proceedings of the IEEE*, volume 7(4), pages 541–580, 1989.

[9] R. Post. YASPER Petri net editor. Department of Mathematics and Computer Science, Technical University Eindhoven, The Netherlands. `www.yasper.org`.

[10] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley-Interscience series in discrete mathematics. John Wiley & Sons, 1986.

[11] W. Vogler. *Modular Construction and Partial Order Semantics of Petri Nets*. Springer-Verlag.

[12] W. Vogler. Behaviour preserving refinement of Petri nets. In *WG*, volume 246 of *LNCS*, pages 82–93. Springer, 1986.