Business Processes Modelling

MPB (6 cfu, 295AA)

Roberto Bruni

http://www.di.unipi.it/~bruni

15 - Sound by construction
Object

We show a technique to build sound Workflow nets
Soundness proof by construction

Idea
1. Find a suitable set of "building blocks"
   they are (small) workflow nets
   that can be (easily) proved
   to be sound and
   to be safe (1-bounded)

2. Define composition patterns so that
   by composing safe and sound WF nets
   we get safe and sound WF nets
Sound and safe by composition

Let $N$, $N'$ be two safe and sound workflow nets
Sound and safe by composition

Let $t$ be a task of $N$ with exactly one input and one output place.
Sound and safe by composition

Let $N[N'/t]$ denote the net obtained by replacing the task $t$ in $N$ by $N'$
Sound and safe by composition

The net $N[N'/t]$ is a sound and safe workflow net (proof omitted)
Proof sketch

Intuitively
a sound workflow net behaves as a transition:
it takes one token from its input place and
it produces one token to its output place
(but not atomically)

Formally
the crux of the proof is showing a bijective correspondence
between
markings of the composed net $N[N'/t]$
and the pairs of markings in $N$ and $N'$
Some Building Blocks 1

- basic
- sequence

Implicit XOR:

Iteration:
Some Building Blocks 2

explicit XOR-split

explicit XOR-join
Some Building Blocks 3

XOR block
Some Building Blocks 4

But you can define more blocks on your own

AND (parallel)
Example: refinement
Example: refinement
Example: refinement
Example: refinement
Example: refinement
Example: refinement
Example: abstraction

Prove that the net below is a safe and sound workflow net
Example: abstraction

Prove that the net below is a safe and sound workflow net

explicit XOR block
Example: abstraction

Prove that the net below is a safe and sound workflow net

sequence
Example: abstraction

Prove that the net below is a safe and sound workflow net

iteration
Example: abstraction

Prove that the net below is a safe and sound workflow net

sequence
Example: abstraction

Prove that the net below is a safe and sound workflow net

parallel (AND) block
Example: abstraction

Prove that the net below is a safe and sound workflow net
Design Example: Car Damage
Design Example: Car Damage
Design Example: Car Damage

begin

register
c1
classify
simple
AND split
c2
phone garage
c5
AND join

complex
check insurance
c4
check history
c7
phone garage

OK
pay
c9
decide
NOK
send letter
end

sequence
Design Example: Car Damage

[Diagram of a process flowchart showing decision points and actions related to car damage, including steps like classification, insurance check, and payment decisions.]
Design Example: Car Damage

Sound and safe by construction!
Exercise

Prove that the net below is a safe and sound workflow net
Exercise

Prove that the net below is a safe and sound workflow net (hint: "desugar" it)
Generalization

We would like to progressively refine transitions with multiple incoming and outgoing arcs.
Lemma: Let $N$ be a sound WF net. If $(i,t) \in F$ then the pre-set of $t$ is $\{i\}$

(otherwise $t$ would be a dead transition)

Lemma: Let $N$ be a sound WF net. If $(t,o) \in F$ then the post-set of $t$ is $\{o\}$

(otherwise $t$ would be dead or proper completion would not hold)
Sketching the idea
General replacement

Let \( T_{i'} = \{ u \mid \bullet u = \{i'\} \} \). (initial transitions of \( N' \))

Let \( T_{o'} = \{ v \mid v\bullet = \{o'\} \} \). (final transitions of \( N' \))

If \((p, t) \in F_N, u \in T_{i'}\) then \((p, u) \in F_{N[N'/t]}\)

If \((t, q) \in F_N, v \in T_{o'}\) then \((v, q) \in F_{N[N'/t]}\)

The net \( N[N'/t] \) is a sound and safe workflow net
General replacement

Let $T_{i'} = \{ u \mid \bullet u = \{ i' \} \}$. (initial transitions of $N'$)
Let $T_{o'} = \{ v \mid v\bullet = \{ o' \} \}$. (final transitions of $N'$)

If $(p, t) \in F_N, u \in T_{i'}$ then $(p, u) \in F_{N[N'/t]}$
If $(t, q) \in F_N, v \in T_{o'}$ then $(v, q) \in F_{N[N'/t]}$

The net $N[N'/t]$ is a **sound** and **safe** workflow net
Some Building Blocks 5

But you can define more blocks on your own
Example
Example
Exercise

Prove that the net below is a safe and sound workflow net