See example specifications.

MODULE *PetriNet*

from "Formal definition and basic terminology" https://*en.wikipedia.org*/wiki/*Petri_net*

Definition 1. A net is a tuple $N = (P, T, F)$ where
1. P and T are disjoint finite sets of places and transitions, respectively.
2. $F \subseteq (P \times T) \cup (T \times P)$ is a set of (directed) arcs (or flow relations).

Definition 4. A Petri net is a net of the form $PN = (N, M, W)$, which extends the elementary net so that
1. $N = (P, T, F)$ is a net.
2. $M : P \to Z$ is a place multiset, where Z is a countable set. M extends the concept of configuration and is commonly described with reference to Petri net diagrams as a marking.
3. $W : F \to Z$ is an arc multiset, so that the count (or weight) for each arc is a measure of the arc multiplicity.

* firing a transition t in a marking M consumes $W(s, t)$ tokens from each of its input places s, and produces $W(t, s)$ tokens in each of its output places s
* a transition is enabled (it may fire) in M if there are enough tokens in its input places for the consumptions to be possible, *i.e.* if and only if $\forall\, s\colon M(s) \geq W(s, t)$.

Instantiate *PetriNet* with (*Places* , *Transitions* , *Arcs* , *InitialMarking* , *ArcWeights*) constants and (*Marking*) variable. *Marking* variable should be declared but not assigned by users of this module.

LOCAL INSTANCE *Integers*
LOCAL INSTANCE *Sequences*
LOCAL INSTANCE *FiniteSets*
LOCAL INSTANCE *TLC*
LOCAL INSTANCE *Helpers*

CONSTANTS *Places*, *Transitions*, *Arcs*, *InitialMarking*, *ArcWeights*

$$
\begin{aligned}
\mathit{ConstsInvariant} \triangleq\ & \land\ \mathit{Places} \in \text{SUBSET STRING} \\
& \land\ \mathit{Transitions} \in \text{SUBSET STRING} \\
& \land\ \forall\, k \in \text{DOMAIN } \mathit{Arcs} :\ \land\ k \in \text{STRING} \\
& \qquad\qquad\qquad\qquad\ \land\ \mathit{Arcs}[k] \in \text{SUBSET STRING} \\
& \land\ \forall\, p \in \text{DOMAIN } \mathit{InitialMarking} :\ \land\ p \in \text{STRING} \\
& \qquad\qquad\qquad\qquad\qquad\qquad\ \land\ \mathit{InitialMarking}[p] \in \mathit{Int}
\end{aligned}
$$

An arc weight is a tuple of (from node, to node, weight)

$$
\begin{aligned}
& \land\ \forall\, i \in 1 \,..\, \mathit{Len}(\mathit{ArcWeights}) :\ \land\ \mathit{Len}(\mathit{ArcWeights}[i]) = 3 \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\ \land\ \mathit{ArcWeights}[i][1] \in \text{STRING} \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\ \land\ \mathit{ArcWeights}[i][2] \in \text{STRING} \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\ \land\ \mathit{ArcWeights}[i][3] \in \mathit{Int}
\end{aligned}
$$

ASSUME *ConstsInvariant*

Marking is a Bag where the domain is *Places* and the range is $\mathit{Int} \geq 0$.

VARIABLE *Marking*

$$\mathit{vars} \triangleq \langle \mathit{Marking} \rangle$$

Invariants

$$
\begin{array}{l}
\mathit{TypeInvariant} \triangleq \\
\quad \land\ \mathit{ConstsInvariant} \\
\quad \land\ \forall\, p \in \text{DOMAIN}\ \mathit{Marking} : \\
\qquad \land\ p \in \text{STRING} \\
\qquad \land\ \mathit{Marking}[p] \in \mathit{Int}
\end{array}
$$

$$
\begin{array}{l}
\mathit{ModelInvariant} \triangleq \\
\quad \land\ \mathit{Places} \cap \mathit{Transitions} = \{\} \\
\quad \land\ \forall\, k \in \text{DOMAIN}\ \mathit{Arcs} : \\
\qquad \lor\ (k \in \mathit{Places} \land \mathit{Arcs}[k] \subseteq \mathit{Transitions}) \\
\qquad \lor\ (k \in \mathit{Transitions} \land \mathit{Arcs}[k] \subseteq \mathit{Places}) \\
\quad \land\ \forall\, k \in \text{DOMAIN}\ \mathit{InitialMarking} : \\
\qquad \land\ k \in \mathit{Places} \\
\qquad \land\ \mathit{InitialMarking}[k] \geq 0 \\
\quad \land\ \forall\, i \in 1 \mathinner{..} \mathit{Len}(\mathit{ArcWeights}) : \\
\qquad \land\ \lor\ \land\ \mathit{ArcWeights}[i][1] \in \mathit{Places} \\
\qquad\qquad \land\ \mathit{ArcWeights}[i][2] \in \mathit{Transitions} \\
\qquad\quad \lor\ \land\ \mathit{ArcWeights}[i][1] \in \mathit{Transitions} \\
\qquad\qquad \land\ \mathit{ArcWeights}[i][2] \in \mathit{Places} \\
\qquad \land\ \mathit{ArcWeights}[i][3] \geq 1 \\
\quad \land\ \forall\, k \in \text{DOMAIN}\ \mathit{Marking} : k \in \mathit{Places} \land \mathit{Marking}[k] \geq 0 \\
\quad \land\ \text{DOMAIN}\ \mathit{Marking} = \mathit{Places}
\end{array}
$$

$$\mathit{Invariants} \triangleq \mathit{TypeInvariant} \land \mathit{ModelInvariant}$$

Operators

Hydrate a marking bag with all missing *Places* mapped to 0.

$$M^* \triangleq M \mathbin{@@} [p \in \mathit{Places} \mapsto 0]$$

(Input and output) places and transitions for transitions and places respectively.

$$\mathit{Inputs}(v) \triangleq \{k \in \text{DOMAIN}\ \mathit{Arcs} : v \in \mathit{Arcs}[k]\}$$

$$\mathit{Outputs}(v) \triangleq \text{IF}\ v \in \text{DOMAIN}\ \mathit{Arcs}\ \text{THEN}\ \mathit{Arcs}[v]\ \text{ELSE}\ \{\}$$

Unspecified arc weights default to 1.

$$
\begin{array}{l}
\mathit{ArcWeight}(\mathit{from},\ \mathit{to}) \triangleq \text{LET} \\
\quad \mathit{match}(w) \triangleq w[1] = \mathit{from} \land w[2] = \mathit{to} \\
\quad \mathit{ws} \triangleq \mathit{SelectSeq}(\mathit{ArcWeights},\ \mathit{match}) \\
\text{IN} \\
\quad \text{IF}\ \mathit{Len}(\mathit{ws}) > 0\ \text{THEN}\ \mathit{ws}[1][3]\ \text{ELSE}\ 1
\end{array}
$$

$$
\begin{array}{l}
\mathit{Enabled}(t) \triangleq \\
\quad \land\ t \in \mathit{Transitions} \\
\quad \land\ \forall\, p \in \mathit{Inputs}(t) : \mathit{Marking}[p] \geq \mathit{ArcWeight}(p,\ t)
\end{array}
$$

$$
\begin{array}{l}
\mathit{Fire}(t) \triangleq \\
\quad \land\ \mathit{Enabled}(t) \\
\quad \land\ \mathit{Marking}' = \mathit{Marking} \oplus \\
\qquad\qquad [p \in \mathit{Inputs}(t) \mapsto 0 - \mathit{ArcWeight}(p,\ t)] \oplus \\
\qquad\qquad [p \in \mathit{Outputs}(t) \mapsto \mathit{ArcWeight}(t,\ p)]
\end{array}
$$

Properties

$Reachable(m) \triangleq \Diamond(Marking = m^*)$

$FinalMarking(m) \triangleq \Diamond\Box(Marking = m^*)$

$Bound(k) \triangleq \Box(\forall\, p \in \text{DOMAIN } Marking : Marking[p] \leq k)$

Optional restrictions on the structure of Petri Nets.

$$IsStateMachine \triangleq \land \forall\, t \in Transitions : \land Cardinality(Inputs(t)) = 1 \\ \land Cardinality(Outputs(t)) = 1 \\ \land \Box(BagSum(Marking) = 1)$$

$$IsMarkedGraph \triangleq \forall\, p \in Places : \land Cardinality(Inputs(p)) = 1 \\ \land Cardinality(Outputs(p)) = 1$$

$$IsFreeChoiceNet \triangleq \forall\, k \in \text{DOMAIN } Arcs \cap Places : \\ \lor Cardinality(Outputs(k)) = 1 \\ \lor \forall\, t \in Arcs[k] : Cardinality(Inputs(t)) = 1$$

TODO: implement more!

Spec

$Init \triangleq Marking = InitialMarking^*$
$Next \triangleq \exists\, t \in Transitions : Fire(t)$

$Spec \triangleq Init \land \Box[Next]_{vars} \land (\forall\, t \in Transitions : \mathrm{WF}_{vars}(Fire(t)))$
