MODULE *Reachability*

This module defines reachability in a directed graph. A directed graph is a collection of nodes and directed edges between nodes. The set of nodes reachable from a node n consists of n and all nodes that can be reached from n by following edges in the direction the edges point. The first thing we must do is decide how to represent a directed graph mathematically. There are two simple ways to do it. The most obvious way is by a set *Nodes* of nodes and a set Edges of edges, where an edge pointing from node n to node m is represented by the pair $\langle n, m \rangle$. We could do this by declaring *Nodes* and Edges to be constants and adding the assumption

ASSUME Edges $\subseteq$ *Nodes* $\times$ *Nodes*

The second way is by a set *Nodes* of nodes and a function *Succ* such that *Succ*$[n]$ is the set of nodes pointed to by edges from n. These two ways of representing directed graphs are obviously equivalent. Starting with *Nodes* and Edges, we can define *Succ* by

Succ$[n \in$ *Nodes*$] \triangleq$
  LET *EdgesFromN* $\triangleq \{e \in$ *Edges* $: e[1] = n\}$
  IN $\{e[2] : e \in$ *EdgesFromN*$\}$

Conversely, given *Nodes* and *Succ*, we can define Edges by

Edges $\triangleq$ UNION $\{$*Succ*$[n] : n \in$ *Nodes*$\}$

We represent a directed graph by *Nodes* and *Succ*.

EXTENDS *Integers*, *Sequences*, *FiniteSets*

CONSTANTS *Nodes*, *Succ*
ASSUME *SuccAssump* $\triangleq$ *Succ* $\in [$*Nodes* $\to$ SUBSET *Nodes*$]$

We define *ReachableFrom* so that for any set S of nodes, *ReachableFrom*(S) is the set of nodes reachable from nodes in S–that is, the set of nodes to which there exists a path starting from a node in S. A path is a sequence of nodes such that there is an edge from each node to the next. We define *ReachableFrom* in terms of *ExistsPath*, where *ExistsPath*(m, n) is true for nodes m and n iff there is a path from m to n.

$$\begin{aligned} &\mathit{IsPathFromTo}(p, m, n) \triangleq \\ &\qquad \land \mathit{Len}(p) > 0 \\ &\qquad \land (p[1] = m) \land (p[\mathit{Len}(p)] = n) \\ &\qquad \land \forall\, i \in 1 \,..\, (\mathit{Len}(p) - 1) : p[i+1] \in \mathit{Succ}[p[i]] \end{aligned}$$

$$\begin{aligned} &\mathit{ExistsPath}(m, n) \triangleq \\ &\quad \exists\, p \in \mathit{Seq}(\mathit{Nodes}) : \mathit{IsPathFromTo}(p, m, n) \end{aligned}$$

$$\begin{aligned} &\mathit{ReachableFrom}(S) \triangleq \\ &\quad \{n \in \mathit{Nodes} : \exists\, m \in S : \mathit{ExistsPath}(m, n)\} \end{aligned}$$

The following two statements import modules that are distributed with the *TLAPS* proof system. If you get a parsing error because those modules can't be found, then you probably don't have *TLAPS* installed and should uncomment the following module-ending line so the rest of this module will be ignored.

* Modification History
* Last modified Sat *Apr* 13 17:50:56 *PDT* 2019 by *lamport*
* Created *Tue Apr* 09 15:06:42 *PDT* 2019 by *lamport*