MODULE *ReachableProofs*

This module contains the *TLAPS* checked proofs of partial correctness of the algorithm in module *Reachable*, based on the invariants *Inv*1, *Inv*2, and *Inv*3 defined in that module. The proofs here are pretty simple because the difficult parts involve proving general results about reachability that are independent of the algorithm. Those results are stated and proved in module *ReachabilityProofs* and are used by the proofs in this module.

You might be sufficiently motivated to make sure the algorithm is correct to want a machine-checked proof that is, but not motivated enough to write machine-checked proofs of the properties of directed graphs that the proof uses. If that's the case, or you're curious about why it might be the case, read module *ReachabilityTest*.

After writing the proof, it occurred to me that it might be easier to replace invariants *Inv*2 and *Inv*3 by the single invariant

$$Inv23 \triangleq Reachable = ReachableFrom(marked \cup vroot)$$

*Inv*23 is obviously true initially and its invariance is maintained by this general result about marked graphs

$$\begin{aligned}&\forall\, S \in \text{SUBSET } Nodes : \\ &\quad \forall\, n \in S : reachableFrom(S) = reachableFrom(S \cup Succ[n])\end{aligned}$$

since $marked \cup vroot$ is changed only by adding successors of nodes in *vroot* to it. Partial correctness is true because when $vroot = \{\}$, we have

$$\begin{aligned}&Inv1 \Rightarrow \forall\, n \in marked : Succ[n] \subseteq marked \\ &Inv23 \equiv Reachable = ReachableFrom(marked)\end{aligned}$$

and the following is true for any directed graph:

$$\forall\, S \in \text{SUBSET } Nodes: (\forall\, n \in S : Succ[n] \subseteq S) \Rightarrow (S = reachableFrom(S))$$

As an exercise, you can try rewriting the proof of partial correctness of the algorithm using only the invariants *Inv*1 and *Inv*23, using the necessary results about reachability. When you've finished doing that, you can try proving those reachability results.

EXTENDS *Reachable*, *ReachabilityProofs*, *TLAPS*

Note that there is no need to write a separate proof that *TypeOK* is invariant, since its invariance is implied by the invariance of *Inv*1.

THEOREM $Thm1 \triangleq Spec \Rightarrow \Box Inv1$

The three level ⟨1⟩ steps and its QED step's proof are the same for any inductive invariance proof. Step ⟨1⟩2 is the only one that *TLAPS* couldn't prove with a BY proof.

⟨1⟩1. $Init \Rightarrow Inv1$

BY *RootAssump* DEF *Init*, *Inv*1, *TypeOK*

⟨1⟩2. $Inv1 \wedge [Next]_{vars} \Rightarrow Inv1'$

The steps of this level ⟨2⟩ proof are the standard way of proving the formula ⟨1⟩2; they were generated by the *Toolbox*'s Decompose Proof Command. The algorithm is simple enough that *TLAPS* can prove steps ⟨2⟩1 and ⟨2⟩2, which are the only nontrivial ones, with BY proofs.

⟨2⟩ SUFFICES ASSUME $Inv1$,
$[Next]_{vars}$
PROVE $Inv1'$

OBVIOUS

⟨2⟩1. CASE *a*

BY $\langle 2\rangle 1$; *SuccAssump* DEF *Inv*1; *TypeOK*; *a*

$\langle 2\rangle 2.$CASE UNCHANGED *vars*

BY $\langle 2\rangle 2$ DEF *Inv*1; *TypeOK*; *vars*

$\langle 2\rangle 3.$ QED

BY $\langle 2\rangle 1$; $\langle 2\rangle 2$ DEF *Next*

$\langle 1\rangle 3.$ QED

BY $\langle 1\rangle 1$; $\langle 1\rangle 2$; *PTL* DEF *Spec*

THEOREM $Thm2 \triangleq Spec \Rightarrow \Box(TypeOK \land Inv2)$

This theorem is a trivial consequence of a general fact about reachability in a directed graph, which is called *Reachable*1 and proved in Module *ReachabilityProofs*,

$\langle 1\rangle 1.$ $Inv1 \Rightarrow TypeOK \land Inv2$

BY *Reachable*1 DEF *Inv*1; *Inv*2; *TypeOK*

$\langle 1\rangle$ QED

BY $\langle 1\rangle 1$; *Thm*1; *PTL*

The best way to read the proof of the following theorem is hierarchically. Read all the steps of a proof at a given level, then read separately the proof of each of those steps, starting with the proof of the QED step. Start by executing the Hide Current Subtree command on the theorem, then use the little + and - icons beside the theorem and each proof step to show and hide its proof.

THEOREM $Thm3 \triangleq Spec \Rightarrow \Box Inv3$

Observe the level $\langle 1\rangle$ proof and the proof of its QED step to see how the invariance of *TypeOK* and *Inv*2 are used in the proof of invariance of *Inv*3.

$\langle 1\rangle 1.$ $Init \Rightarrow Inv3$

BY *RootAssump* DEF *Init*; *Inv*3; *TypeOK*; *Reachable*

$\langle 1\rangle 2.$ $TypeOK \land TypeOK' \land Inv2 \land Inv2' \land Inv3 \land [Next]_{vars} \Rightarrow Inv3'$

The SUFFICES step and its proof, the QED step and its proof, and the CASE steps $\langle 2\rangle 2$ and $\langle 2\rangle 3$ were generated by the *Toolbox*'s Decompose Proof command.

$\langle 2\rangle$ SUFFICES ASSUME *TypeOK*;
TypeOK';
*Inv*2;
*Inv*2';
*Inv*3;
$[Next]_{vars}$
PROVE $Inv3'$

OBVIOUS

Step $\langle 2\rangle 1$ is obviously true because *Reachable* and *ReachableFrom* are constants. It helps *TLAPS* to give it these results explicitly so it doesn't have to figure them out when it needs them.

$\langle 2\rangle 1.$ $\land\ Reachable' = Reachable$
$\land\ ReachableFrom(vroot)' = ReachableFrom(vroot')$
$\land\ ReachableFrom(marked \cup vroot)' = ReachableFrom(marked' \cup vroot')$

OBVIOUS

$\langle 2\rangle 2.$CASE *a*

a is a simple enough formula so there's no need to hide its definition when it's not needed.

$\langle 3 \rangle$ USE $\langle 2 \rangle 2$ DEF *a*

Splitting the proof into these two cases is an obvious way to write the proof–especially since *TLAPS* is not very good at figuring out by itself when it should do a proof by a case split.

$\langle 3 \rangle 1.$CASE $vroot = \{\}$
BY $\langle 2 \rangle 1$; $\langle 3 \rangle 1$ DEF $Inv3$; $TypeOK$

$\langle 3 \rangle 2.$CASE $vroot \neq \{\}$

The way to use a fact of the form $\exists\, x \in S : P(x)$ is to pick an x in S satisfying $P(x)$.

$\langle 4 \rangle 1.$ PICK $v \in vroot$:
IF $v \notin marked$
THEN $\wedge\ marked' = (marked \cup \{v\})$
$\wedge\ vroot' = vroot \cup Succ[v]$
ELSE $\wedge\ vroot' = vroot \setminus \{v\}$
$\wedge$ UNCHANGED $marked$
BY $\langle 3 \rangle 2$

Again, the obvious way to use a fact of the form

IF P THEN $\ldots$ ELSE $\ldots$

is by splitting the proof into the two cases P and $\sim P$.

$\langle 4 \rangle 2.$CASE $v \notin marked$

This case follows immediately from the general reachability result *Reachable*2 from module *ReachabilityProofs*.

$\langle 5 \rangle 1.$ $\wedge\ ReachableFrom(vroot') = ReachableFrom(vroot)$
$\wedge\ v \in ReachableFrom(vroot)$
BY $\langle 4 \rangle 1$; $\langle 4 \rangle 2$; $Reachable2$ DEF $TypeOK$

$\langle 5 \rangle 2.$ QED
BY $\langle 5 \rangle 1$; $\langle 4 \rangle 1$; $\langle 4 \rangle 2$; $\langle 5 \rangle 1$; $\langle 2 \rangle 1$ DEF $Inv3$

$\langle 4 \rangle 3.$CASE $v \in marked$

This case is obvious.

$\langle 5 \rangle 1.$ $marked' \cup vroot' = marked \cup vroot$
BY $\langle 4 \rangle 1$; $\langle 4 \rangle 3$

$\langle 5 \rangle 2.$ QED
BY $\langle 5 \rangle 1$; $\langle 2 \rangle 1$ DEF $Inv2$; $Inv3$

$\langle 4 \rangle 4.$ QED
BY $\langle 4 \rangle 2$; $\langle 4 \rangle 3$

$\langle 3 \rangle 3.$ QED
BY $\langle 3 \rangle 1$; $\langle 3 \rangle 2$

$\langle 2 \rangle 3.$CASE UNCHANGED $vars$

As is almost all invariance proofs, this case is trivial.

BY $\langle 2 \rangle 1$; $\langle 2 \rangle 3$ DEF $Inv3$; $TypeOK$; $vars$

$\langle 2 \rangle 4.$ QED
BY $\langle 2 \rangle 2$; $\langle 2 \rangle 3$ DEF $Next$

$\langle 1 \rangle 3.$ QED
BY $\langle 1 \rangle 1$; $\langle 1 \rangle 2$; $Thm2$; PTL DEF $Spec$

THEOREM $Spec \Rightarrow \Box((pc = \text{"Done"}) \Rightarrow (marked = Reachable))$

This theorem follows easily from the invariance of *Inv*1 and *Inv*3 and the trivial result *Reachable*3 of module *ReachabilityProofs* that *Reachable*({}) equals {}. That result was put in module *ReachabilityProofs* so all the reasoning about the algorithm depends only on properties of *ReachableFrom*, and doesn't depend on how *ReachableFrom* is defined.

$\langle 1 \rangle 1.\ Inv1 \Rightarrow ((pc = \text{"Done"}) \Rightarrow (vroot = \{\}))$

BY DEF $Inv1$; $TypeOK$

$\langle 1 \rangle 2.\ Inv3 \land (vroot = \{\}) \Rightarrow (marked = Reachable)$

BY $Reachable3$ DEF $Inv3$

$\langle 1 \rangle 3.$ QED

BY $\langle 1 \rangle 1$; $\langle 1 \rangle 2$; $Thm1$; $Thm3$; PTL

* Modification History

* Last modified Sun *Apr* 14 16:24:32 *PDT* 2019 by *lamport*

* Created *Thu Apr* 11 18:41:11 *PDT* 2019 by *lamport*