MODULE *RiverCrossing*

This specification describes a history of the universe where the rules of the "Fox, goose, and bag of beans" puzzle are enforced. As taken from *Wikipedia* (https://*en.wikipedia.org*/wiki/Fox,_*goose_and_bag_of_beans_puzzle*):

> Once upon a time a farmer went to a market and purchased a fox, a goose, and a bag of beans. On his way home, the farmer came to the bank of a river and rented a boat. But in crossing the river by boat, the farmer could carry only himself and a single one of his purchases: the fox, the goose, or the bag of beans.
>
> If left unattended together, the fox would eat the goose, or the goose would eat the beans.
>
> The farmer's challenge was to carry himself and his purchases to the far bank of the river, leaving each purchase intact. How did he do it?

This specification includes the following invariants:

- *TypeOK*: Type invariant that ensures the river banks are represented by the actors on them.
- *NothingEatenNow*: Invariant that ensures the fox doesn't eat the goose and the goose doesn't eat the beans.
- *SolutionInvariant*: An invariant that we know does not hold, because this puzzle has a solution. By adding it as an invariant to a model, TLC will provide an error trace that provides a solution to the puzzle. Set the number of TLC worker threads to 1 to see the shortest solution.

EXTENDS *TLC* Pull in *PrintT* for debugging

State

The riverbanks the farmer starts from and finishes at.

VARIABLES *riverbankstart*, *riverbankfinish*

All the actors in this puzzle.

$Actors \triangleq \{\text{"farmer"}, \text{"fox"}, \text{"goose"}, \text{"beans"}\}$

Riverbanks are represented by the actors on them. The boat, though critical to the human perception of how the farmer transports the items, does not play any role in the specification itself and is therefore omitted.

$$TypeOK \triangleq \begin{array}{l} \land\ riverbankstart \subseteq Actors \\ \land\ riverbankfinish \subseteq Actors \end{array}$$

Operations

This was useful for debugging purposes as I wrote the initial specification of this system. Include as the last conjunct in an expression to minimize the number of things printed.

$PrintVariables \triangleq PrintT(\langle \text{"Start was"}, riverbankstart, \text{" and is now "}, riverbankstart',$

"Finish was", $riverbankfinish$, " and is now ", $riverbankfinish'\rangle$)

Items are only safe when the fox isn't left alone with the goose and the goose isn't left alone with the beans.

$$\begin{aligned} ItemsAreSafe(riverbank) \triangleq\ & \land riverbank \neq \{\text{"fox"}, \text{"goose"}\} \\ & \land riverbank \neq \{\text{"goose"}, \text{"beans"}\} \end{aligned}$$

Ensure things don't get eaten on either bank, either in current state or next (primed). Use *NothingEatenNow* in a *TLC* model to ensure this safety property holds for this specification.

$$\begin{aligned} NothingEatenNow &\triangleq ItemsAreSafe(riverbankstart) \land ItemsAreSafe(riverbankfinish) \\ NothingEatenNext &\triangleq ItemsAreSafe(riverbankstart') \land ItemsAreSafe(riverbankfinish') \\ NothingGetsEaten &\triangleq NothingEatenNow \land NothingEatenNext \end{aligned}$$

Move an item from one bank to the other, maintaining safety.

$$\begin{aligned} &MoveItem(item, start, finish) \triangleq \\ &\quad \text{The farmer finds himself on a given } start \text{ riverbank} \\ &\quad \land \text{"farmer"} \in start \\ &\quad \text{He leaves } start \text{ with himself and one } item \\ &\quad \land start' = start \setminus \{item, \text{"farmer"}\} \\ &\quad \text{He immediately takes that } item \text{ and himself to } finish \text{ riverbank} \\ &\quad \land finish' = finish \cup \{item, \text{"farmer"}\} \\ &\quad \text{Everything survives or we don't do it} \\ &\quad \land NothingGetsEaten \end{aligned}$$

Operations for moving specific items to/from *riverbankstart* and *riverbankfinish*.

$$\begin{aligned} MoveItemAZ(item) &\triangleq MoveItem(item, riverbankstart, riverbankfinish) \\ MoveItemZA(item) &\triangleq MoveItem(item, riverbankfinish, riverbankstart) \end{aligned}$$

$$\begin{aligned} MoveFoxAZ &\triangleq MoveItemAZ(\text{"fox"}) \\ MoveFoxZA &\triangleq MoveItemZA(\text{"fox"}) \\ MoveGooseAZ &\triangleq MoveItemAZ(\text{"goose"}) \\ MoveGooseZA &\triangleq MoveItemZA(\text{"goose"}) \\ MoveBeansAZ &\triangleq MoveItemAZ(\text{"beans"}) \\ MoveBeansZA &\triangleq MoveItemZA(\text{"beans"}) \end{aligned}$$

Spec

We begin with all items on *riverbankstart* and nothing on *riverbankfinish*.

$$\begin{aligned} Init \triangleq\ & \land riverbankstart = Actors \\ & \land riverbankfinish = \{\} \end{aligned}$$

We can move items from one bank to the other, maintaining the safety invariant that nothing gets eaten.

$$Next \triangleq \lor MoveFoxAZ$$

$\lor$ *MoveFoxZA*
$\lor$ *MoveGooseAZ*
$\lor$ *MoveGooseZA*
$\lor$ *MoveBeansAZ*
$\lor$ *MoveBeansZA*

Temporal formula that is the specification of the system. If true, then both the *Init* state is valid and the *Next* state is always valid for every step in every behavior following the initial state. This includes behaviors that contain stuttering steps, or steps in the history of the universe wherein neither *riverbankstart* nor *riverbankfinish* change at all.

$Spec \triangleq Init \land \Box[Next]_{\langle riverbankstart,\, riverbankfinish \rangle}$

See a solution to this puzzle by setting this as an invariant in the model.

$SolutionInvariant \triangleq riverbankfinish \neq Actors$

\ * Modification History
\ * Last modified *Wed Nov* 15 16:57:35 *EST* 2017 by *dgregoire*
\ * Created *Tue Nov* 14 15:18:30 *EST* 2017 by *dgregoire*