MODULE *WaterBottles*

The Water Bottles problem is a fairly trivial reasoning problem. In this problem, one is provided two bottles: one with a 3 liter capacity, and one with a 5 liter capacity. A hose is available to fill either bottle, and the contents of a bottle can be poured on the ground to empty it. Bottles have no graduation marks, and cannot be marked or otherwise drawn on. The only possible actions are completely filling either bottle, emptying a bottle, or transferring as much of the contents of one bottle as can fit into the other.

Based on these constraints, the goal of the problem is to fill the 5 liter bottle with exactly 4 liters of water.

This TLA+ specification describes the states involved in this system, as the possible operations to the system. We define an invariant relating to levels in the water bottles, and then an invariant which we will disprove in order to come to the solution.

The output of *TLC* is included at the end of this document for completeness. The source document included in this repository includes the source used to produce this document, in TLA+ format, which can be passed to *TLC* in order to prove the assertions made herein.

It should also be noted that this is part of a learning project; proving the water bottle problem to be solvable is not novel in any way, but serves as a simple demonstration of TLA+ and its toolchain.

This statement pulls in basic arithmetic operations, as well as ranges.

EXTENDS *Integers*

This system has only two state variables.

VARIABLES
small, the amount of water in the small bottle
large the amount of water in the large bottle

Invariant which states that the small bottle can have between 0 and 3 liters of water, and the large bottle can have between 0 and 5 liters of water.

$$
\begin{aligned}
&TypeOK \triangleq \\
&\quad \land\ small \in 0 \,..\, 3 \\
&\quad \land\ large \in 0 \,..\, 5
\end{aligned}
$$

The invariant which we will disprove using *TLC*. By defining it this way, we can run *TLC* and find sequence which violates this invariant; this sequence is necessarily the solution to the water bottle problem.

$$
\begin{aligned}
&NoFoundSolution \triangleq \\
&\quad \land\ large \neq 4
\end{aligned}
$$

Next, we define each state transition. At any point, a 'step' in our system is defined as fulfilling one of these conditions. The implementation of that 'step' logic will be defined after the steps themselves.

Fill the small bottle to its capacity of 3 liters

$$
\begin{aligned}
&FillSmall \triangleq \\
&\quad \land\ small' = 3 \\
&\quad \land\ \text{UNCHANGED } \langle large \rangle
\end{aligned}
$$

Fill the large bottle to its capacity of 5 liters

$FillLarge \triangleq$

$\quad \land\ large' = 5$

$\quad \land\ \text{UNCHANGED}\ \langle small \rangle$

Empty the contents of the small bottle

$EmptySmall \triangleq$

$\quad \land\ small' = 0$

$\quad \land\ \text{UNCHANGED}\ \langle large \rangle$

Empty the contents of the large bottle

$EmptyLarge \triangleq$

$\quad \land\ large' = 0$

$\quad \land\ \text{UNCHANGED}\ \langle small \rangle$

Pour the contents of the large bottle into the small bottle

$LargeToSmall \triangleq$

$\quad \text{IF}\ small + large > 3$

Handle the case where the large bottle's contents would overflow the small bottle

$\quad\quad \text{THEN}\ \land\ small' = 3$

$\quad\quad\quad\quad \land\ large' = large - (3 - small)$

Otherwise, pour the entire contents of the large bottle into the small bottle

$\quad\quad \text{ELSE}\ \land\ small' = small + large$

$\quad\quad\quad\quad \land\ large' = 0$

Pour the contents of the small bottle into the large bottle

$SmallToLarge \triangleq$

$\quad \text{IF}\ small + large > 5$

Handle the case where the small bottle's contents would overflow the large bottle

$\quad\quad \text{THEN}\ \land\ small' = small - (5 - large)$

$\quad\quad\quad\quad \land\ large' = 5$

Otherwise, pour the entire contents of the small bottle into the large bottle

$\quad\quad \text{ELSE}\ \land\ small' = 0$

$\quad\quad\quad\quad \land\ large' = small + large$

Next, we define the initial state for the system as having both bottles empty, represented as having 0 liters of water.

$Init \triangleq$

$\quad \land\ small = 0$

$\quad \land\ large = 0$

This defines the function for a 'step' in the system, capturing all valid state transitions as the disjunction of the steps listed above.

$Next \triangleq$

$\vee$ *FillSmall*
$\vee$ *FillLarge*
$\vee$ *EmptySmall*
$\vee$ *EmptyLarge*
$\vee$ *LargeToSmall*
$\vee$ *SmallToLarge*

The following is the abbreviated output of running *TLC* against the above definitions. Line numbers and references have been removed for brevity.

Intuitively, the steps below are a solution to the water bottle problem. Note that this isn't exhaustive; there are other ways to arrive at a solution, but that isn't what we're solving for here. The sole purpose of this is to formally prove the solvability of the problem.

Error: Invariant *NoFoundSolution* is violated.
Error: The behavior up to this point is:

State 1: $<$ Initial predicate $>$
$\wedge\ large = 0$
$\wedge\ small = 0$

State 2: $<$ *FillLarge* $>$
$\wedge\ large = 5$
$\wedge\ small = 0$

State 3: $<$ *LargeToSmall* $>$
$\wedge\ large = 2$
$\wedge\ small = 3$

State 4: $<$ *EmptySmall* $>$
$\wedge\ large = 2$
$\wedge\ small = 0$

State 5: $<$ *LargeToSmall* $>$
$\wedge\ large = 0$
$\wedge\ small = 2$

State 6: $<$ *FillLarge* $>$
$\wedge\ large = 5$
$\wedge\ small = 2$

State 7: $<$ *LargeToSmall* $>$
$\wedge\ large = 4$
$\wedge\ small = 3$
