Rigorous Digital Engineering

High-Assurance Cyber-Physical Systems

Missionaries and Cannibals

Three missionaries and three cannibals must cross a river using a boat which can carry at most two people, under the constraint that, for both banks, if there are missionaries present on the bank, they cannot be outnumbered by cannibals (if they were, the cannibals would eat the missionaries). The boat cannot cross the river by itself with no people on board.

Some math

- $\mathcal{M}$, the set of missionaries
- $\mathcal{C}$, the set of cannibals
- $\mathcal{B} = \{E, W\}$, the banks of the river

It is helpful to realize that everyone is the union of $\mathcal{M}$ and $\mathcal{C}$.

$$\text{everyone} = \mathcal{M} \cup \mathcal{C}$$

Describing the boat and who is on each bank

- b is the bank where the boat is

$$b \in \mathcal{B} = \{E, W\}$$

- $o(b)$, the other bank

b	$o(b)$
E	W
W	E

Who is on each bank

Let's call who is on a bank w. There are wwo way to think of this:

1. w is a function from $\mathcal{B}$ to some subset of everyone $\mathcal{M} \cup \mathcal{C}$

$$w : \mathcal{B} \rightarrow S \subset \mathcal{M} \cup \mathcal{C}$$

2. w is an array indexed by E and W telling you who is on each bank.

x	$w(x)$
E	S
W	$\bar{S}$

where $S \cup \bar{S} = \mathcal{M} \cup \mathcal{C}$

Is it safe?

Let S be a subset of people on a bank of the river. There are two possibilities.

1. The people on the bank can just be cannibals: $S \subseteq \mathcal{C}$
2. Or, the number of cannibals in S must be less than or equal to the number of missionaries.

$$|S \cap C| \leq |S \cap M|$$

We can write this as a function

$$\text{IsSafe} : S \to \text{boolean}$$

$$\begin{aligned} \text{IsSafe}(S) &= (S \subseteq \mathcal{C}) \\ &\vee (|S \cap C| \leq |S \cap M|) \end{aligned}$$

We want to move the people in S from bank b to the other bank $o(b)$

Let's define two things

1. After the move, the new set of people on the bank is who is on the bank minus who went on the boat

$$N = w(b) \setminus S \qquad \text{(new on this bank)}$$

2. After the move the new set of people on the other bank is who is on the other bank plus who went on the boat

$$O = w(o(b)) \cup S \qquad \text{(new on other bank)}$$

What is a valid move?

Several things must be true:

1. Only two people can be in the boat

$$|S| \in \{1, 2\} \qquad \text{(number in boat)}$$

2. The new set of people on the bank must be safe

$$\text{IsSafe}(N) = \text{true}$$

3. The new set of people on the other bank must be safe

$$\text{IsSafe}(O) = \text{true}$$

4. The boat is now on the other bank

$$b' = o(b)$$

5. Who is on each bank is

$$w'(b) = N \quad \text{and} \quad w'(o(b)) = O$$

The prime indicates the new state for the bank of the canoe b' and the new state of who is on a particular bank w'.

In math terms

$$\begin{aligned}
\text{ValidMove(S,b)} \quad &= S \in \{1,2\} \\
&\wedge \text{IsSafe}(N) \\
&\wedge \text{IsSafe}(O) \\
&\wedge b' = o(b) \\
&\wedge w'(b) = N \\
&\wedge w'(o(b)) = O
\end{aligned}$$

Finally, we know that at any step, there must be some group of people on the bank where the canoe is that result in a valid move

$$\text{ValidNext} = \exists S \subset w(b) \ : \ \text{ValidMove}(S, b) = \text{true}$$

An initial condition

To start out, everyone and the canoe are on the east bank.

$$b = E$$

bank	who
E	$\mathcal{M} \cup \mathcal{C}$
W	$\emptyset$

We will use TLA+ to solve this problem.

The usual reason for writing a spec is to check the system you're specifying for errors. This means checking that it satisfies some property. The most commonly checked property is invariance, asserting that some condition is satisfied by every state in in every possible execution.

The purpose of this spec is to solve the cannibals and missionaries problem, which means finding some possible execution in which everyone reaches bank "W". We can find that solution by having the TLC model checker check an invariance property that, in every reachable state, there is someone left on bank "E".

When TLC finds that an invariant isn't an invariant, it outputs an execution that reaches a state in which the invariant is not true. In our case, this means an execution that solves the problem (one ending in a state with no one on bank "E").

So to find the solution, you just have to run TLC on a model of this specification in which

1. 3-element sets are substituted for the constants Missionaries and Cannibals and
2. The invariant

$$w(E) \neq \emptyset$$

The error trace TLC produces is a solution to the problem.

The error trace

Bank *E*	**Bank** *W*	*S*	**Direction**
{c1, c2, c3, m1, m2, m3}	{}	{c1, c2}	→
{c3, m1, m2, m3}	{c1, c2}	{c2}	←
{c1, c3, m1, m2, m3}	{c2}	{c1, c3}	→
{m1, m2, m3}	{c1, c2, c3}	{c1}	←
{c1, m1, m2, m3}	{c2, c3}	{m1, m2}	→
{c1, m3}	{c2, c3, m1, m2}	{c2, m1}	←
{c1, c2, m1, m3}	{c3, m2}	{m1, m3}	→
{c1, c2}	{c3, m1, m2, m3}	{c3}	←
{c1, c2, c3}	{m1, m2, m3}	{c1, c2}	→
{c3}	{c1, c2, m1, m2, m3}	{c1}	←
{c1, c3}	{c2, m1, m2, m3}	{c1, c3}	→
{}	{c1, c2, c3, m1, m2, m3}		