Homework 2: Combination Lock

Bart Massey
February 6, 2016

An entrepreneur has come to you with a request for a specification for an electronic combination lock that is under development. After some discussion, you find that the basic operation of the lock is intended to be as follows:

- The lock can be reset by spinning it to the right or by pushing the lock button.
- Once the lock is reset, it requires a combination consisting of left, right and left spins to targets in the range $0 \mathrel{..} 35$, followed by a press of the lock button, to unlock.
- Hardware and software has already been developed that will report the position and last spin direction of the lock when the user pauses for 100ms or more.
- Note that if the user then continues spinning in the same direction, this is considered a "pause" and ignored for the purposes of determining the combination.
- The higher level software being developed must assert a locked or unlocked signal after receiving every spin event.
- The combination will be preset at the factory, per lock, and cannot be changed.

Your task is to provide a Z specification (mixed with English as necessary) of the operation of the lock software.

As a starting point, you might consider defining some types and some schemas for your lock. To start with, you might consider the types you will need.

$$\begin{array}{l}
POSITION == 0 \mathrel{..} 35 \\
DIRECTION ::= left \mid right \\
LOCK\_STATE ::= unlocked \mid locked
\end{array}$$

You would then presumably define a state schema for the lock as a whole, something like:

$$\begin{array}{|l}
\multicolumn{1}{l}{\_\,Lock\,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \\
last\_event : DIRECTION \times POSITION \\
stages\_completed : 0 \mathrel{..} 3 \\
\hline
\end{array}$$

You would then proceed to define an initial schema $InitLock'$ which describes the starting state of the lock, then continue with some state change schemas for the lock that describe the response to user actions.

Please consider writing your lock description in Z or UTF-8 and using the CZT typechecker to check it for syntax and type correctness.