MODULE *gear*

EXTENDS *Integers*, *TLAPS*

Without loss of generality, see our figures, the point of view vector z is $\langle 0, 0, 1\rangle$, as the gear wheel lies in the plane (O, X, Y); where O is the center of the gear wheel.

Still without loss of generality, such wheel has constant radius 1.

VARIABLES x, y 3D vectors of the physical space.

Without loss of generality, we only pick x, y in the following *Circle*; see above assumptions.

$$abs[t \in Int] \triangleq \text{IF } t > 0 \text{ THEN } t \text{ ELSE } -t$$

Circle is a subset of $Int \times Int \times \{0\}$; which is infinite... This works (slowly!)IF you add additional constraints in *InvX*, *InvY* (See the "Unecessay if .. " comment). IF NOT, then it fails: *TLAPS* will not solve any polynomial equation for you.

Note that *TLC* will not like it either and will raise the usual "non-enumerable set" exception.

$$Circle \triangleq \{$$
$$w \in Int \times Int \times \{0\} :$$

Manhattan norm:

$$\land\ abs[w[1]] + abs[w[2]] = 1$$

Euclidian norm:

$$\land\ abs[w[1]] * abs[w[1]] + abs[w[2]] * abs[w[2]] = 1$$
$$\}$$

Better use this *Circle* if you want *TLC* be nice to your spec. You can drop the additional constaints in *InvX*, *InvY* (see above), since *CircleTLC* is now a subset of a FINITE set.

$$CircleTLC \triangleq \{$$
$$w \in \{-1, 0, 1\} \times \{-1, 0, 1\} \times \{0\} : abs[w[1]] + abs[w[2]] = 1$$
$$\}$$

Simpler is better: Straighforward definition of *Circle*:

$$CircleEnum \triangleq \{$$
$$\langle 1, 0, 0\rangle, \langle -1, 0, 0\rangle,$$
$$\langle 0, 1, 0\rangle, \langle 0, -1, 0\rangle$$
$$\}$$

You may drop "BY DEF ... *abs*" whether you use it.

InnerProd is the usual inner product $x \cdot y$. Hence

$$InnerProd \triangleq x[1] * y[1] + x[2] * y[2]$$

Our assumption $z = \langle 0, 0, 1\rangle$ implies that the matrix $[x\ y\ z]$ has determinant
$Det := x[1] * y[2] - x[2] * y[1]$.
Hence the following operator *Det*

$$Det \triangleq \text{IF } (x \in Circle \land y \in Circle) \text{ THEN } x[1] * y[2] - x[2] * y[1] \text{ ELSE } 0$$

InvX: x is picked in *Circle* $*$; now x is fixed and MUST NOT change.

$$InvX \triangleq$$

$\land x \in Circle$

Unnecessary if *Circle* is explicitely defined as a finite set:

$\land x[1] \in \{-1, 1\}$

$\land x[2] = 0$

InvY y is picked in *Circle* as well.

$InvY \triangleq$

$\land y \in Circle$

$\land y[1] = 0$

Unnecessary if *Circle* is explicitely defined as a finite set:

$\land y[2] \in \{-1, 1\}$

InvXY: x and y MUST BE nontrivially orthogonal.

$InvXY \triangleq$

$\land x \in Circle$

$\land y \in Circle$

$\land InnerProd = 0$

Our invariant $\Box Inv$ is now "controlled" by the follwing *Inv*.

$Inv \triangleq$

$\land InvX$

$\land InvY$

$\land InvXY$

The *Next* action:

$Next \triangleq$

Boundaries

$\land y \in Circle$

$\land x \in Circle$

So, x no action will ever change x:

$\land$ UNCHANGED x

$\land y' \in Circle$ You want to request that.

y is flipped in the sense that $y' := -y$:

$\land y' = [y \text{ EXCEPT } ![1] = -y[1], ![2] = -y[2]]$

Our spec *Spec*, then. Remark that *Inv* is also the initial condition.

$Spec \triangleq Inv \land \Box[Next]_{\langle x, y \rangle}$

Typing variables: Relevant type is *Circle*.

$Typing(v) \triangleq v \in Circle$

The following lemma states that *Next* preserves *Inv*.

LEMMA $LemInv \triangleq Inv \land Next \Rightarrow Inv'$

$\langle 1 \rangle$ SUFFICES ASSUME $Inv \land Next$

PROVE Inv'

OBVIOUS

$\langle 1 \rangle 1$ $Inv \land Next \Rightarrow InvX'$

BY DEF $InvX$, $InvXY$, Inv, $Next$

$\langle 1 \rangle 2$ $Inv \land Next \Rightarrow InvY'$

BY DEF $InvY$, $InvXY$, Inv, $Next$, $Circle$

$\langle 1 \rangle 3$ $Inv \land Next \Rightarrow InvXY'$

BY DEF $InvXY$, Inv, $Next$, $Circle$, $InnerProd$

$\langle 1 \rangle 4$ QED BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$ DEF Inv

Equivalently, the invariant $\Box Inv$ is true under specs *Spec*.

THEOREM $ThInv \triangleq Spec \Rightarrow \Box Inv$

$\langle 1 \rangle 1$ $Inv \land$ UNCHANGED $\langle x, y \rangle \Rightarrow Inv'$

BY DEF $Circle$, $InnerProd$, $InvX$, $InvY$, $InvXY$, Inv

$\langle 1 \rangle 2$ $Inv \land \Box [Next]_{\langle x, y \rangle} \Rightarrow \Box Inv$

BY PTL, $LemInv$, $\langle 1 \rangle 1$

$\langle 1 \rangle$ QED BY PTL, $\langle 1 \rangle 1$, $\langle 1 \rangle 2$ DEF $Spec$

ThInv straightforwardly establishes that, under specification Spec, x, y, have always type *Circle*.

ThType: *Stephan*'s version.

THEOREM $ThTypeCompactVersion \triangleq Spec \Rightarrow \Box Typing(x) \land \Box Typing(y)$

$\langle 1 \rangle.Inv \Rightarrow Typing(x) \land Typing(y)$

BY DEF Inv, $InvX$, $InvY$, $Typing$

$\langle 1 \rangle$.QED

BY $ThInv$, PTL

ThType: *Stephan*'s version, with a SUFFICES ASSUME − PROVE .

THEOREM $ThType \triangleq Spec \Rightarrow \Box Typing(x) \land \Box Typing(y)$

$\langle 1 \rangle$ SUFFICES ASSUME $Spec$

PROVE

$\land\ Spec \Rightarrow \Box Inv$

$\land\ Inv \Rightarrow Typing(x) \land Typing(y)$

BY PTL DEF Inv, $InvX$, $InvY$, $Typing$

$\langle 1 \rangle$ $Inv \Rightarrow Typing(x) \land Typing(y)$

BY DEF Inv, $InvX$, $InvY$, $Typing$

$\langle 1 \rangle$ QED BY $ThInv$, PTL

The following theorem asserts that there are only three options for the step $det(x, y, z) \rightarrow det(x', y', z')$:

1. $det(x, y, z) = det(x', y', z) \land$ UNCHANGED $\langle x, y \rangle$
2. $det(x, y, z) = 1 \land det(x', y', z) = -1 \land Next$
3. $det(x, y, z) = -1 \land det(x', y', z) = 1 \land Next$;

which establishes that our spec is correct. QED

THEOREM $ThOscillatingDet \triangleq Inv \land Next \Rightarrow$

$\land\ Det \in \{-1, 1\}$

$\quad \land Det' \in \{-1, 1\}$
$\quad \land Det' = -Det$
$\langle 1 \rangle$ SUFFICES ASSUME $Inv \land Next$
PROVE
$\quad \land Det \in \{-1, 1\}$
$\quad \land Det' \in \{-1, 1\}$
$\quad \land Det' = -Det$
OBVIOUS
$\langle 1 \rangle 1$ $Inv \land Next \Rightarrow Det \in \{-1, 1\}$
BY DEF $InvX$, $InvY$, Inv, $Next$, Det, $Circle$, abs
$\langle 1 \rangle 2$ $Inv \land Next \Rightarrow Det' = -Det$
BY DEF $InvX$, $InvY$, Inv, $Next$, Det, $Circle$
$\langle 1 \rangle 3$ $Inv \land Next \Rightarrow$
$\quad \land Det \in \{-1, 1\}$
$\quad \land Det' = -Det$
BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$
$\langle 1 \rangle 4$ $Det \in \{-1, 1\} \land Det' = -Det \Rightarrow Det' \in \{-1, 1\}$
OBVIOUS
$\langle 1 \rangle 5$ $Inv \land Next \Rightarrow Det' \in \{-1, 1\}$
BY $\langle 1 \rangle 3$, $\langle 1 \rangle 4$
$\langle 1 \rangle 6$ QED BY $\langle 1 \rangle 1$, $\langle 1 \rangle 2$, $\langle 1 \rangle 3$, $\langle 1 \rangle 5$