Specification of Brunelleschi's hoist: A device that alternatively raises and lowers payloads without inversion of motive force.

G.Cordier

August 4, 2023

1 From Brunelleschi's hoist to TLA+ specification

As an introduction, let us quote[1]:

> The problem is based on a real machine, developed by the Renaissance [goldsmith/sculptor/architect/engineer/inventor] Filippo Brunelleschi during the period 1420-1425. The machine was used to hoist large sandstone and marble blocks for completion of the cupola of the cathedral in Florence [Since] it bothered him [...] that when the block reached the top of the cupola, the oxen had to be un-harnessed and re-harnessed to change the direction of the hoist and lower the lifting tackle back to the ground. Brunelleschi's solution was a three-speed, reversible hoist. This was a novel concept and drew much admiration from other Renaissance artists and engineers [...].

So, Brunelleschi's design may be described as follow: The very hoisting system (*the gear*: A wheel around an horizontal shaft) gets motion from a main (vertical) shaft. Such motion is captured from a wheel (A) that is rigidly fixed to the main shaft. In other words, A is the driving wheel. Contact between gear and wheel A (only) occurs at point P; see [Figure 1].

Moreover, a second wheel A′, which can be seen as a (distinct) copy of A is symmetrically set. More specifically, the symmetry is performed with respect to the "mirror"plan (O, X, Z); see [Figure 1].

The key ingredient is that a vertical shift can make the gear switch contact P to its A′ counterpart P′. The gear is then equipped with (only) two degrees of freedom (off rotation) : Either contact in P or in P′
It can now be shown that the gear can either lift or pull payloads, on demand. To do so, it is enough to switch from one state/configuration to the other one. In other words, raising and lowering payloads can now be done (1) with a single device, (2) **without reversing** the driving force, *i.e.* without reversing the vertical shaft rotation. To sum it up, changing the rotation direction is no longer done at the "engine level" but, instead, by a simple, effortless shift of the wheels.
The following specification "encodes" the system (the gear) and its environment (wheels A, A′) at a geometrical level of astraction; see [Figure 1.B]. Provided celerity vector x, radius vector y and normal vector z (all being

normalized, then nonzero), the rotation direction is identified with the determinant $\det(x, y, z) \in \{-1, 1\}$ of the block matrix $[x\,y\,z]$. The spec shall then be proved once established that such determinant "oscillates" between -1 (given one contact, say P) and 1 (provided the other one, say P$'$).

The following specification is written in TLA+; see [2], [3]. TLA+ is based on TLA, an extension of the first logic order (in ZFC). Noticeably,

(a) ' denotes a variable assignement at the next following step;

(b) $\square$ asserts that a formula is always valid, *i.e.* true for every reachable step.

Such specification is actually pretty general:

(a) It does not force us to explicitely choose a rotation direction for the vertical shaft;

(b) It does not force us to explicitely choose an initial driving wheel (A or A$'$);

(c) In theory, it is easy to drop gear and wheels, so that the system keeps working as long as there exists at any time a single contact point P, P$'$. For instance, we may replace wheels by arbitray convex shapes. Another approach is to see that the fundamental properties of the whole system are stable under "conservative" diffeomorphism φ (more rigorously: $\det \varphi' > 0$). This would mean a of useless trouble in practice ...but that is not a part of the specification!
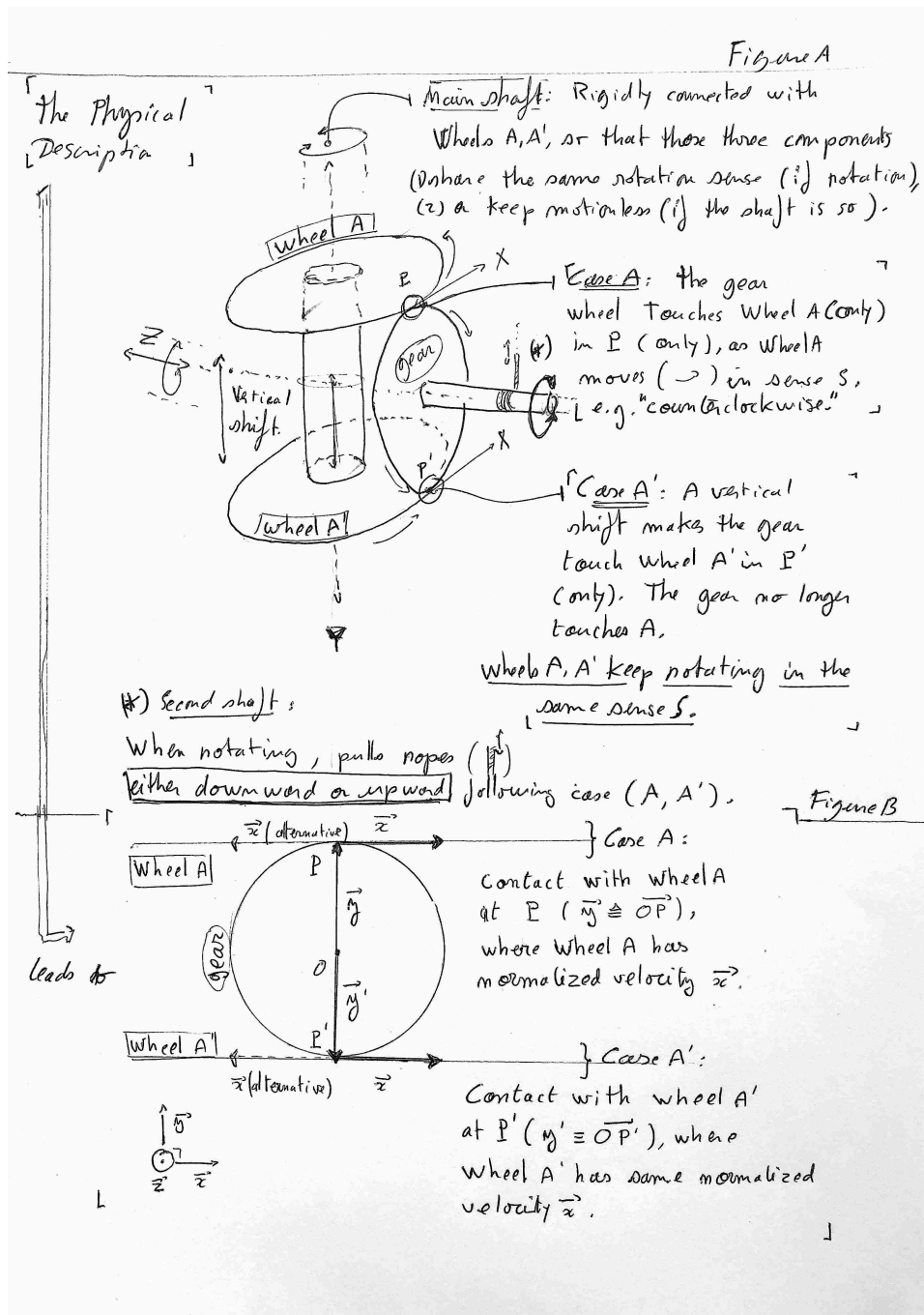
The Physical Description

Main shaft: Rigidly connected with Wheels A, A', or that those three components (1) share the same rotation sense ("i") notation), (2) a keep motionless ("i" the shaft is so).

Wheel A

P

X

Case A: the gear wheel touches Wheel A (only) in P (only), as Wheel A moves (→) in sense S, i.e. "counterclockwise."

(*)

z

Vertical shift

Gear

P'

X

Wheel A'

Case A': A vertical shift makes the gear touch Wheel A' in P' (only). The gear no longer touches A.

Wheels A, A' keep rotating in the same sense S.

Y

(#) Second shaft:

When rotating, pulls ropes (P) either downward or upward following case (A, A').

$\overrightarrow{x}$ (alternative) $\overrightarrow{x}$

Wheel A

P

$\overrightarrow{y}$

gear

O

$\overrightarrow{y'}$

P'

Wheel A'

$\overrightarrow{x}$ (alternative) $\overrightarrow{x}$

} **Case A:** Contact with Wheel A at P ($\overrightarrow{y} \triangleq \overrightarrow{OP}$), where Wheel A has normalized velocity $\overrightarrow{x}$.

} **Case A':** Contact with wheel A' at P' ($y' \equiv \overrightarrow{OP'}$), where wheel A' has same normalized velocity $\overrightarrow{x}$.

$\overrightarrow{v}$

$\overrightarrow{z}$ $\overrightarrow{x}$

leads to

Figure 1: Physical and geometrical descriptions of the system (the gear) and its environment (the vertical shaft)

3

2 The TLA+ source code

---------------------------- MODULE gear ----------------------------

EXTENDS Integers, Reals, 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.

$abs[t \in Int] \triangleq$ IF $t > -t$ THEN t 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:
        $\wedge abs[w[1]] + abs[w[2]] = 1$
        Euclidian norm:
        $\wedge abs[w[1]] * abs[w[1]] + abs[w[2]] * abs[w[2]] = 1$
$\}$

> 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

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

4

$Det \stackrel{\Delta}{=}$ IF (x ∈ Circle ∧ y ∈ Circle) THEN x[1] * y[2] − x[2] * y[1] ELSE 0

$InvX \stackrel{\Delta}{=}$
    ∧ x ∈ Circle
    ∧ x[1] ∈ { − 1, 1}
    ∧ x[2] = 0

$InvY \stackrel{\Delta}{=}$
    ∧ y ∈ Circle
    ∧ y[1] = 0
    ∧ y[2] ∈ { − 1, 1}

$InvXY \stackrel{\Delta}{=}$
    ∧ x ∈ Circle
    ∧ y ∈ Circle
    ∧ InnerProd = 0

$Inv \stackrel{\Delta}{=}$
    ∧ InvX
    ∧ InvY
    ∧ InvXY

$Next \stackrel{\Delta}{=}$
    ∧ y ∈ Circle
    ∧ x ∈ Circle
    ∧ UNCHANGED x
    ∧ y′ ∈ Circle
    ∧ y′ = [y EXCEPT ![1] = − y[1], ![2] = − y[2]]

$\text{Spec} \overset{\Delta}{=} \text{Inv} \wedge \square[\text{Next}]_{\langle x, y \rangle}$

$\text{Typing}(v) \overset{\Delta}{=} v \in \text{Circle}$

LEMMA LemInv $\overset{\Delta}{=} \text{Inv} \wedge \text{Next} \implies \text{Inv}'$
$\langle 1 \rangle$ SUFFICES ASSUME Inv, Next
PROVE Inv$'$
OBVIOUS
$\langle 1 \rangle 1$ Inv $\wedge$ Next $\implies$ InvX$'$
    BY DEF InvX, InvXY, Inv, Next
$\langle 1 \rangle 2$ Inv $\wedge$ Next $\implies$ InvY$'$
    BY DEF InvY, InvXY, Inv, Next, Circle
$\langle 1 \rangle 3$ Inv $\wedge$ Next $\implies$ 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

THEOREM ThInv $\overset{\Delta}{=}$ Spec $\implies \square$Inv
$\langle 1 \rangle 1$ Inv $\wedge$ UNCHANGED $\langle x, y \rangle \implies$ Inv$'$
    BY DEF Circle, InnerProd, InvX, InvY, InvXY, Inv
$\langle 1 \rangle 2$ Inv $\wedge \square[\text{Next}]_{\langle x, y \rangle} \implies \square$Inv
    BY PTL, LemInv, $\langle 1 \rangle 1$
$\langle 1 \rangle$ QED BY PTL, $\langle 1 \rangle 1, \langle 1 \rangle 2$ DEF Spec

THEOREM ThTypeCompactVersion $\overset{\Delta}{=}$ Spec $\implies \square$Typing(x) $\wedge \square$Typing(y)
$\langle 1 \rangle$.Inv $\implies$ Typing(x) $\wedge$ Typing(y)
  BY DEF Inv, InvX, InvY, Typing
$\langle 1 \rangle$.QED
  BY ThInv, PTL

THEOREM ThType $\overset{\Delta}{=}$ Spec $\implies \square$Typing(x) $\wedge \square$Typing(y)
$\langle 1 \rangle$ SUFFICES ASSUME Spec
    PROVE
     $\wedge$ Spec $\implies \square$Inv

$\wedge\,\mathrm{Inv} \implies \mathrm{Typing(x)} \wedge \mathrm{Typing(y)}$
  BY PTL DEF Inv, InvX, InvY, Typing
$\langle 1\rangle$ Inv $\implies$ Typing(x) $\wedge$ 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) $\to$ det(x$'$, y$'$, z):
>
> 1. det(x, y, z) = det(x$'$, y$'$, z) $\wedge$ UNCHANGED $\langle$x, y$\rangle$
> 2. det(x, y, z) = 1 $\wedge$ det(x$'$, y$'$, z) = -1 $\wedge$ Next
> 3. det(x, y, z) = -1 $\wedge$ det(x$'$, y$'$, z) = 1 $\wedge$ Next;
>
> which establishes that our spec is correct. QED

THEOREM ThOscillatingDet $\stackrel{\Delta}{=}$ Inv $\wedge$ Next $\implies$
  $\wedge$ Det $\in \{-1,\,1\}$
  $\wedge$ Det$'$ $\in \{-1,\,1\}$
  $\wedge$ Det$'$ = $-$ Det
$\langle 1\rangle$ SUFFICES ASSUME Inv, Next
PROVE
  $\wedge$ Det $\in \{-1,\,1\}$
  $\wedge$ Det$'$ = $-$ Det
  OBVIOUS
$\langle 1\rangle 1$ Inv $\wedge$ Next $\implies$ Det $\in \{-1,\,1\}$
  BY DEF InvX, InvY, Inv, Next, Det, Circle, abs
$\langle 1\rangle 2$ Inv $\wedge$ Next $\implies$ Det$'$ = $-$ Det
  BY DEF InvX, InvY, Inv, Next, Det, Circle
$\langle 1\rangle 3$ QED BY $\langle 1\rangle 1$, $\langle 1\rangle 2$

\ * Modification History
\ * Last modified Fri Aug 04 17:17:23 CEST 2023 by gcordier
\ * Created Wed Aug 01 13:07:52 CEST 2023 by gcordier

3 Acknowledgements

References

[1] Biomimetics & Dexterous Manipulation Laboratory. BrunelleschiNotes. http://bdml.stanford.edu/Main/BrunelleschiNotes. Accessed: August 4, 2023.

[2] Leslie Lamport. TLA+. http://lamport.azurewebsites.net/tla/tla.html. Accessed: August 4, 2023.

[3] Markus Kuppe *et al.* TLA+ repository. https://github.com/tlaplus. Accessed: August 4, 2023.