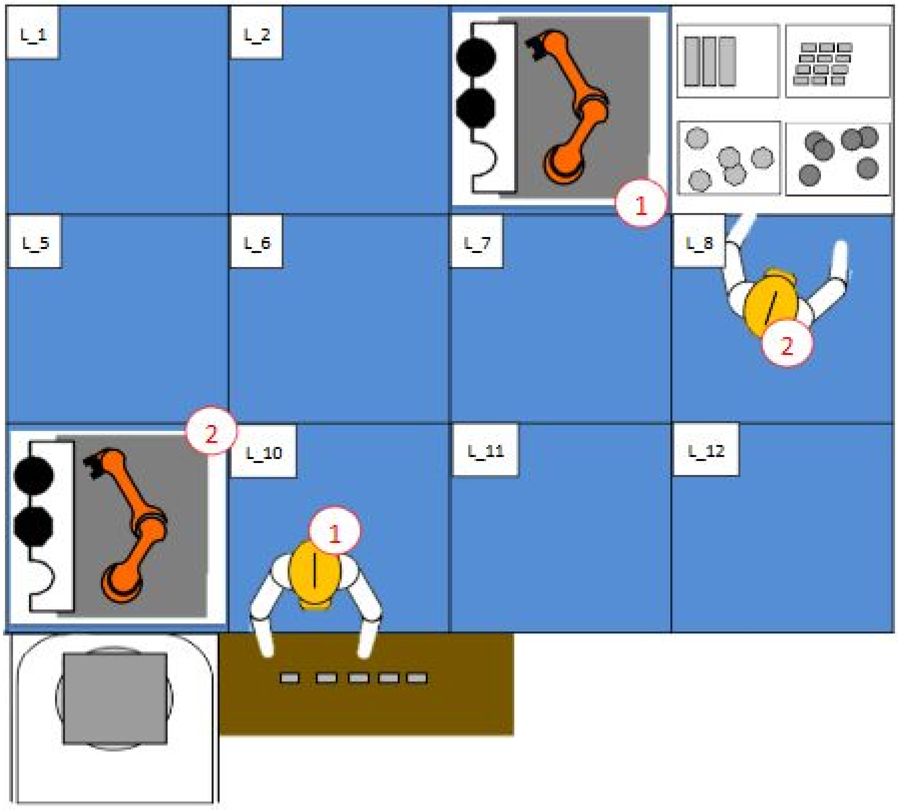
Formal Methods Project’s Report

Frigerio Matteo
Romano Leonardo

The goal of this project is to create a model and verify the satisfiability of properties.
The model is a workspace within which a robot and a human can move between two particular work positions; the workspace is represented by a matrix composed by twelve possible positions that the two actors can cover; among this twelve locations there are two cell representing the two work position of the human and others two cell representing the two work positions of the robot.



This figure is a representation of the workspace and in particular the position L_3 and L_9 represent the work positions of the robot, while the position L_8 and L_10 represent the work positions of the human; the cell L_4 represents a position that can’t be covered by the two actors.

The property to be verified inside the model is the absence of collision between the human and the robot; inside the model a collision occurs when the human and the robot are in the same cell and the robot has moved in that cell with respect to the previous step.
We speak of temporal steps because in this model the time is discrete and at each instant of discrete time the two actors can either stay in the same cell in which it is located or move in one of the adjacent cells.

Lisp program structure

The model is created by a program written in temporal logic, the program is composed by three main parts: the Init, the Transition System and the Property.

Transition System

The transition system in composed by various defvar, which one represents a specific feature of the TS and together define the workspace model and the movement of the two actors.

Init

The init provides the initial state of our transition system and it will represent the step 0 of discrete time in our model.

Property

The property represents the specification of the property that the model must satisfied.

Verification

The verification is done by Zot and in particular through the execution of the procedure:

```
(eezot: zot N
        (&&
                (yesterday init)
                (!! property)
                trans
        )
)
```

This procedure represents the execution of our transition system starting from the init condition for N steps and the transition system is intersected with the denied property with the purpose to obtain that the execution is unsatisfiable.

The demonstration that the execution of the intersection between a transition system and a denied property have an unsatisfiable result is the best way to guarantee that a transition system respects the property.

Explanation of the lisp program

To represent the transition system, we chose to use two arrays called Human and Robot both with twelve position and both with domain two value Y and N.
When one element of the array has value Y, it means that the respective actors is in the cell represented by the index of the array and all the others position have value N.
Instead the other two variables are called targetHuman and targetRobot, with respective domain 8, 10 and 3, 9, and these represent the four target cell of the two actors.

```
(defvar state-d '(N Y))
(defvar pos-d  '(1 2 3 4 5 6 7 8 9 10 11 12))
(defvar targetHuman-d '(8 10))
(defvar targetRobot-d '(3 9))

(define-array human pos-d state-d)
(define-array robot pos-d state-d)
(define-item targetHuman targetHuman-d)
(define-item targetRobot targetRobot-d)
```

state-d: is the domain of the values of the array *human* and array *robot*
pos-d: is the domain of the position of the two arrays *human* and *robot*
targetHuman-d and _targetRobot-d_: are the domain of the variables *targetHuman* and *targetRobot*

TRIO Model

In the following part there is the explanation of our TRIO model, which is composed by severals temporal logic formulas.
The whole model is the result of the AND logic operator applied to each formulas.
The predicate $Human_x$ and $Robot_x$ are true when respectively the human and the robot are in the x-th cell.
The predicate $TargetHuman_x$ and $TargetRobot_x$ mean that the next work position of the human and the robot is the x-th cell.

Init

This temporal logic formula means the starting condition of our model: the robot starts from cell 3, the human starts from cell 10 and the respective targets are cell 9 and cell 8

$Futr(Human_{10}, 0) \wedge Futr(Robot_{3}, 0) \wedge Futr(TargetHuman_{8}, 0) \wedge Futr(TargetRobot_{9}, 0)$

OnePlaceHuman

This temporal logic formula means that the human can be always in one and only one cell.

$$
\begin{array}{l}
Alw(\\
\quad \exists i \ (i \in [1,12] \ (Human_{i})) \wedge \\
\quad \forall i,j \ (((i \in [1,12]) \wedge (j \in [1,12]) \wedge (i \neq j)) \rightarrow \neg(Human_{i} \wedge Human_{j})) \\
)
\end{array}
$$

OnePlaceRobot

This temporal logic formula means that the robot can be always in one and only one cell.

$$
\begin{array}{l}
Alw(\\
\quad \exists i \ (i \in [1,12] \ (Robot_{i})) \wedge \\
\quad \forall i,j \ (((i \in [1,12]) \wedge (j \in [1,12]) \wedge (i \neq j)) \rightarrow \neg(Robot_{i} \wedge Robot_{j})) \\
)
\end{array}
$$

NeverInCellFour

This temporal logic formula means that the robot and the human never go in the cell 4 because this cell is unreachable.

$Alw(\neg(Human_{4}) \wedge \neg(Robot_{4}))$

EventuallyWorkPosition

This temporal logic formula means that both the robot and the human go infinitely often to their work position cell.

$$
\begin{array}{l}
Alw(\\
\quad SomF(Human_{8}) \wedge \\
\quad SomF(Human_{10}) \wedge \\
\quad SomF(Robot_{3}) \wedge \\
\quad SomF(Robot_{9}) \\
)
\end{array}
$$

MovementHuman

This temporal logic formula specifies the permitted movement of the human with respect to each possible position in the workspace.
Moreover this formula specifies that the human can take only one step for each temporal step.

$Alw($

$(Human_1 \rightarrow (Futr(Human_1, 1) \vee Futr(Human_2, 1) \vee Futr(Human_5, 1) \vee Futr(Human_6, 1)))$

$\wedge$

$(Human_2 \rightarrow (Futr(Human_1, 1) \vee Futr(Human_2, 1) \vee Futr(Human_3, 1) \vee Futr(Human_5, 1) \vee Futr(Human_6, 1) \vee Futr(Human_7, 1)))$

$\wedge$

$(Human_3 \rightarrow Futr(Human_2, 1) \vee Futr(Human_3, 1) \vee Futr(Human_6, 1) \vee Futr(Human_7, 1) \vee Futr(Human_8, 1)))$

$\wedge$

$(Human_5 \rightarrow (Futr(Human_1, 1) \vee Futr(Human_2, 1) \vee Futr(Human_5, 1) \vee Futr(Human_6, 1) \vee Futr(Human_9, 1) \vee Futr(Human_{10}, 1)))$

$\wedge$

$(Human_6 \rightarrow \neg(Futr(Human_8, 1) \vee Futr(Human_{12}, 1)))$

$\wedge$

$(Human_7 \rightarrow \neg(Futr(Human_1, 1) \vee Futr(Human_5, 1) \vee Futr(Human_9, 1)))$

$\wedge$

$(Human_8 \rightarrow (Futr(Human_3, 1) \vee Futr(Human_7, 1) \vee Futr(Human_8, 1) \vee Futr(Human_{11},1) \vee Futr(Human_{12}, 1)))$

$\wedge$

$(Human_9 \rightarrow (Futr(Human_5, 1) \vee Futr(Human_6, 1) \vee Futr(Human_9, 1) \vee Futr(Human_{10},1)))$

$\wedge$

$(Human_{10} \rightarrow (Futr(Human_5, 1) \vee Futr(Human_6, 1) \vee Futr(Human_7, 1) \vee Futr(Human_9, 1) \vee Futr(Human_{10}, 1) \vee Futr(Human_{11}, 1)))$

$\wedge$

$(Human_{11} \rightarrow (Futr(Human_6, 1) \vee Futr(Human_7, 1) \vee Futr(Human_8, 1) \vee Futr(Human_{10},1) \vee Futr(Human_{11}, 1) \vee Futr(Human_{12}, 1)))$

$\wedge$

$(Human_{12} \rightarrow (Futr(Human_7, 1) \vee Futr(Human_8, 1) \vee Futr(Human_{11}, 1) \vee Futr(Human_{12},1)))$

$)$

MovementRobot

This temporal logic formula specifies the permitted movement of the robot with respect to each possible position in the workspace.
Moreover this formula specifies that the robot can take only one step for each temporal step.

$$
\begin{array}{lll}
Alw(& & \\
\quad & (Robot_1 \rightarrow & (Futr(Robot_1, 1) \lor Futr(Robot_2, 1) \lor Futr(Robot_5, 1) \lor Futr(Robot_6,))) \\
\quad & \land & \\
\quad & (Robot_2 \rightarrow & (Futr(Robot_1, 1) \lor Futr(Robot_2, 1) \lor Futr(Robot_3, 1) \lor Futr(Robot_5, 1) \\
\quad & & \lor Futr(Robot_6, 1) \lor Futr(Robot_7, 1))) \\
\quad & \land & \\
\quad & (Robot_3 \rightarrow & Futr(Robot_2, 1) \lor Futr(Robot_3, 1) \lor Futr(Robot_6, 1) \lor Futr(Robot_7, 1) \\
\quad & & \lor Futr(Robot_8, 1))) \\
\quad & \land & \\
\quad & (Robot_5 \rightarrow & (Futr(Robot_1, 1) \lor Futr(Robot_2, 1) \lor Futr(Robot_5, 1) \lor Futr(Robot_6, 1) \\
\quad & & \lor Futr(Robot_9, 1) \lor Futr(Robot_{10}, 1))) \\
\quad & \land & \\
\quad & (Robot_6 \rightarrow & \neg(Futr(Robot_8, 1) \lor Futr(Robot_{12}, 1))) \\
\quad & \land & \\
\quad & (Robot_7 \rightarrow & \neg(Futr(Robot_1, 1) \lor Futr(Robot_5, 1) \lor Futr(Robot_9, 1))) \\
\quad & \land & \\
\quad & (Robot_8 \rightarrow & (Futr(Robot_3, 1) \lor Futr(Robot_7, 1) \lor Futr(Robot_8, 1) \lor Futr(Robot_{11},1) \\
\quad & & \lor Futr(Robot_{12}, 1))) \\
\quad & \land & \\
\quad & (Robot_9 \rightarrow & (Futr(Robot_5, 1) \lor Futr(Robot_6, 1) \lor Futr(Robot_9, 1) \lor Futr(Robot_{10},1))) \\
\quad & \land & \\
\quad & (Robot_{10} \rightarrow & (Futr(Robot_5, 1) \lor Futr(Robot_6, 1) \lor Futr(Robot_7, 1) \lor Futr(Robot_9, 1) \\
\quad & & \lor Futr(Robot_{10}, 1) \lor Futr(Robot_{11}, 1))) \\
\quad & \land & \\
\quad & (Robot_{11} \rightarrow & (Futr(Robot_6, 1) \lor Futr(Robot_7, 1) \lor Futr(Robot_8, 1) \lor Futr(Robot_{10},1) \\
\quad & & \lor Futr(Robot_{11}, 1) \lor Futr(Robot_{12}, 1))) \\
\quad & \land & \\
\quad & (Robot_{12} \rightarrow & (Futr(Robot_7, 1) \lor Futr(Robot_8, 1) \lor Futr(Robot_{11}, 1) \lor Futr(Robot_{12},1))) \\
\quad &) &
\end{array}
$$

NoCollision

This temporal logic formula describes the movement of the robot with respect to the movement of the human to avoid collisions with him when the robot is moving.

$Alw($

$((Futr(Human_1,1) \wedge (Robot_2 \vee Robot_5 \vee Robot_6))$

$\rightarrow$

$(Futr(Robot_2,1) \vee Futr(Robot_3,1) \vee Futr(Robot_5,1) \vee Futr(Robot_6,1) \vee Futr(Robot_7,1) \vee$
$Futr(Robot_9,1) \vee Futr(Robot_{10},1) \vee Futr(Robot_{11},1)))$

$\wedge$

$((Futr(Human_2,1) \wedge (Robot_1 \vee Robot_3 \vee Robot_5 \vee Robot_6 \vee Robot_7))$

$\rightarrow$

$(Futr(Robot_1,1) \vee Futr(Robot_3,1) \vee Futr(Robot_5,1) \vee Futr(Robot_6,1) \vee Futr(Robot_7,1) \vee$
$Futr(Robot_8,1) \vee Futr(Robot_9,1) \vee Futr(Robot_{10},1) \vee Futr(Robot_{11},1) \vee Futr(Robot_{12},1)))$

$\wedge$

$((Futr(Human_3,1) \wedge (Robot_2 \vee Robot_6 \vee Robot_7 \vee Robot_8))$

$\rightarrow$

$(Futr(Robot_1,1) \vee Futr(Robot_2,1) \vee Futr(Robot_5,1) \vee Futr(Robot_6,1) \vee Futr(Robot_7,1) \vee$
$Futr(Robot_8,1) \vee Futr(Robot_9,1) \vee Futr(Robot_{10},1) \vee Futr(Robot_{11},1) \vee Futr(Robot_{12},1)))$

$\wedge$

$((Futr(Human_5,1) \wedge (Robot_1 \vee Robot_2 \vee Robot_6 \vee Robot_9 \vee Robot_{10}))$

$\rightarrow$

$(Futr(Robot_1,1) \vee Futr(Robot_2,1) \vee Futr(Robot_3,1) \vee Futr(Robot_6,1) \vee Futr(Robot_7,1)$
$\vee Futr(Robot_9,1) \vee Futr(Robot_{10},1) \vee Futr(Robot_{11},1)))$

$\wedge$

$((Futr(Human_6,1) \wedge (Robot_1 \vee Robot_2 \vee Robot_3 \vee Robot_5 \vee Robot_7 \vee Robot_9 \vee$
$Robot_{10}$
$\vee Robot_{11}))$

$\rightarrow$

$(Futr(Robot_1,1) \vee Futr(Robot_2,1) \vee Futr(Robot_3,1) \vee Futr(Robot_5,1) \vee Futr(Robot_7,1) \vee$
$Futr(Robot_8,1) \vee Futr(Robot_9,1) \vee Futr(Robot_{10},1) \vee Futr(Robot_{11},1) \vee Futr(Robot_{12},1)))$

$\wedge$

$((Futr(Human_7,1) \wedge (Robot_2 \vee Robot_3 \vee Robot_6 \vee Robot_8 \vee Robot_{10} \vee Robot_{11} \vee$
$Robot_{12}))$

$\rightarrow$

$(Futr(Robot_1,1) \vee Futr(Robot_2,1) \vee Futr(Robot_3,1) \vee Futr(Robot_5,1) \vee Futr(Robot_6,1) \vee$
$Futr(Robot_8,1) \vee Futr(Robot_9,1) \vee Futr(Robot_{10},1) \vee Futr(Robot_{11},1) \vee Futr(Robot_{12},1)))$

$\wedge$

$((Futr(Human_8,1) \wedge (Robot_3 \vee Robot_7 \vee Robot_{11} \vee Robot_{12}))$

$\rightarrow$

$(Futr(Robot_2,1) \vee Futr(Robot_3,1) \vee Futr(Robot_6,1) \vee Futr(Robot_7,1) \vee$
$Futr(Robot_{10},1) \vee$
$Futr(Robot_{11},1) \vee Futr(Robot_{12},1)))$

$\land$

$((\mathit{Futr}(\mathit{Human}_{9},1) \land (\mathit{Robot}_{5} \lor \mathit{Robot}_{6} \lor \mathit{Robot}_{10}))$

$\rightarrow$

$(\mathit{Futr}(\mathit{Robot}_{1},1) \lor \mathit{Futr}(\mathit{Robot}_{2},1) \lor \mathit{Futr}(\mathit{Robot}_{3},1) \lor \mathit{Futr}(\mathit{Robot}_{5},1) \lor \mathit{Futr}(\mathit{Robot}_{6},1)$

$\lor \mathit{Futr}(\mathit{Robot}_{7},1) \lor \mathit{Futr}(\mathit{Robot}_{10},1) \lor \mathit{Futr}(\mathit{Robot}_{11},1)))$

$\land$

$((\mathit{Futr}(\mathit{Human}_{10},1) \land (\mathit{Robot}_{5} \lor \mathit{Robot}_{6} \lor \mathit{Robot}_{7} \lor \mathit{Robot}_{9} \lor \mathit{Robot}_{11}))$

$\rightarrow$

$(\mathit{Futr}(\mathit{Robot}_{1},1) \lor \mathit{Futr}(\mathit{Robot}_{2},1) \lor \mathit{Futr}(\mathit{Robot}_{3},1) \lor \mathit{Futr}(\mathit{Robot}_{5},1) \lor$
$\mathit{Futr}(\mathit{Robot}_{6},1) \lor \mathit{Futr}(\mathit{Robot}_{7},1) \lor \mathit{Futr}(\mathit{Robot}_{8},1) \lor \mathit{Futr}(\mathit{Robot}_{9},1) \lor \mathit{Futr}(\mathit{Robot}_{11},1) \lor$
$\mathit{Futr}(\mathit{Robot}_{12},1)))$

$\land$

$((\mathit{Futr}(\mathit{Human}_{11},1) \land (\mathit{Robot}_{6} \lor \mathit{Robot}_{7} \lor \mathit{Robot}_{8} \lor \mathit{Robot}_{10} \lor \mathit{Robot}_{12}))$

$\rightarrow$

$(\mathit{Futr}(\mathit{Robot}_{1},1) \lor \mathit{Futr}(\mathit{Robot}_{2},1) \lor \mathit{Futr}(\mathit{Robot}_{3},1) \lor \mathit{Futr}(\mathit{Robot}_{5},1) \lor \mathit{Futr}(\mathit{Robot}_{6},1) \lor$
$\mathit{Futr}(\mathit{Robot}_{7},1) \lor \mathit{Futr}(\mathit{Robot}_{8},1) \lor \mathit{Futr}(\mathit{Robot}_{9},1) \lor \mathit{Futr}(\mathit{Robot}_{10},1) \lor \mathit{Futr}(\mathit{Robot}_{12},1)))$

$\land$

$((\mathit{Futr}(\mathit{Human}_{12},1) \land (\mathit{Robot}_{7} \lor \mathit{Robot}_{8} \lor \mathit{Robot}_{11}))$

$\rightarrow$

$(\mathit{Futr}(\mathit{Robot}_{2},1) \lor \mathit{Futr}(\mathit{Robot}_{3},1) \lor \mathit{Futr}(\mathit{Robot}_{6},1) \lor \mathit{Futr}(\mathit{Robot}_{7},1) \lor$
$\mathit{Futr}(\mathit{Robot}_{8},1) \lor$
$\mathit{Futr}(\mathit{Robot}_{10},1) \lor \mathit{Futr}(\mathit{Robot}_{11},1))))$

SwitchTarget

This temporal logic formula means that both the human and the robot switch their target when they reach their workcells.
For example when the robot with $\mathit{TargetRobot}_{3}$ reaches the cell 3, the target will be switched to $\mathit{TargetRobot}_{9}$.

$\mathit{Alw}($

$(\mathit{Futr}(\mathit{Robot}_{3},1) \rightarrow \mathit{Futr}(\mathit{TargetRobot}_{9},1)) \land$
$(\mathit{Futr}(\mathit{Robot}_{9},1) \rightarrow \mathit{Futr}(\mathit{TargetRobot}_{3},1)) \land$
$((\neg \mathit{Futr}(\mathit{Robot}_{3},1) \land \neg \mathit{Futr}(\mathit{Robot}_{9},1) \land \mathit{TargetRobot}_{3}) \rightarrow \mathit{Futr}(\mathit{TargetRobot}_{3},1)) \land$
$((\neg \mathit{Futr}(\mathit{Robot}_{3},1) \land \neg \mathit{Futr}(\mathit{Robot}_{9},1) \land \mathit{TargetRobot}_{9}) \rightarrow \mathit{Futr}(\mathit{TargetRobot}_{9},1)) \land$
$(\mathit{Futr}(\mathit{Human}_{8},1) \rightarrow \mathit{Futr}(\mathit{TargetHuman}_{10},1)) \land$
$(\mathit{Futr}(\mathit{Human}_{10},1) \rightarrow \mathit{Futr}(\mathit{TargetHuman}_{8},1)) \land$
$((\neg \mathit{Futr}(\mathit{Human}_{8},1) \land \neg \mathit{Futr}(\mathit{Human}_{10},1) \land \mathit{TargetHuman}_{8}) \rightarrow \mathit{Futr}(\mathit{TargetHuman}_{8},1)) \land$
$((\neg \mathit{Futr}(\mathit{Human}_{8},1) \land \neg \mathit{Futr}(\mathit{Human}_{10},1) \land \mathit{TargetHuman}_{10}) \rightarrow \mathit{Futr}(\mathit{TargetHuman}_{10},1))$

$)$

RobotNearToTheTarget

This temporal logic formula means that when the robot is near the target and the target's cell is occupied by the human, the robot will wait until the target cell is released in order to avoid unnecessary cycles around the target.

$Alw($

$\quad (Futr(Human_9,1) \land Target_9 \land Robot_5) \rightarrow (Futr(Robot_5,1)) \land$

$\quad (Futr(Human_9,1) \land Target_9 \land Robot_6) \rightarrow (Futr(Robot_6,1)) \land$

$\quad (Futr(Human_9,1) \land Target_9 \land Robot_{10}) \rightarrow (Futr(Robot_{10},1)) \land$

$\quad (Futr(Human_3,1) \land Target_3 \land Robot_2) \rightarrow (Futr(Robot_2,1)) \land$

$\quad (Futr(Human_3,1) \land Target_3 \land Robot_6) \rightarrow (Futr(Robot_6,1)) \land$

$\quad (Futr(Human_3,1) \land Target; \land Robot_7) \rightarrow (Futr(Robot_7,1)) \land$

$\quad (Futr(Human_3,1) \land Target_3 \land Robot_8) \rightarrow (Futr(Robot_8,1))$

$)$

WorkTime

This temporal logical formula represents the working time that the robot and the human spend to their respective workstations.
Both human and robot remain 2 time steps in their work positions when they reach them.

$Alw($

$\quad ((Futr(Human_8,1) \land (TargetHuman_8)) \rightarrow (Futr(Human_8,2) \land Futr(Human_8,3))) \land$

$\quad ((Futr(Human_{10},1) \land (TargetHuman_{10})) \rightarrow (Futr(Human_{10},2) \land Futr(Human_{10},3))) \land$

$\quad ((Futr(Robot_3,1) \land (TargetRobot_3)) \rightarrow (Futr(Robot_3,2) \land Futr(Robot_3,3))) \land$

$\quad ((Futr(Robot_9,1) \land (TargetRobot_9)) \rightarrow (Futr(Robot_9,2) \land Futr(Robot_9,3))) \land$

$)$

Property

This temporal logical formula represents the property that the transition system must satisfy.
The formula means that, when the robot is moving, the robot and the human cannot end up in the same cell, in order to avoid collision.

$Alw($

$\quad \forall i\ ((i \in [1,12]) \land Past(\neg Robot_i,1)) \rightarrow (Robot_i \land \neg Human_i))$

$)$