Project of Formal Methods for Concurrent and Real-time Systems course (PoliMi/UIC 545)

Model and Report

Ludovico Crotta,
Lorenzo Semeria,
Gabriele Vanoni

1 Introduction

The aim of this report is to introduce a possible model for the Human-Robot Collaborative (HRC) application shown in class, both in terms of modeling the world and the constraints needed to ensure the safety of the human operator. We will first describe the environment that the robot and the human will work in, along with the assumptions made to simplify the model while keeping it detailed enough to give a meaningful representation of reality.

1.1 The environment

The environment is assumed to be a room, as shown in the image. We decided to position the pallet, where the operator and the robot will work together, on the right side of the room. On the left we put the bin, where the robot will go alone to refill his own “local” bin. The room is divided in squares, according to the natural X and Y axis, allowing us to simply identify the cells via their coordinates. We decided that the path between the bin and the pallet could be a straight line without introducing an oversimplification of the model. This is motivated by the fact that the room does not contain any obstacle and is big enough to for the walls not to interfere with standard robot movement. Therefore – should the path not be a straight line in the first place – a trivial change of basis would make the line straight. The new basis would only be a rotation of the starting one.

1.2 The robot

We modeled the robot as a two-square object, which represents the whole cart. The robotic arm is modeled in more detail and we track the position of the elbow, the arm and the hand of the robot. The cart can move left- and rightward only, since the bin to pallet path is straight and the are no fixed obstacles. Should the operator be in the way the robot will simply stop moving, as we shall see. The arm is modeled to be retracted (on the same square of the cart) during movement, while its position during activity is modeled accordingly.
We assumed that the robot has sensors to detect his own position in the room as well as the operator's. More specifically, the robot can detect the position of the human operator in terms of distance and direction. This is simply represented by knowing the position of the operator on the grid modeling the room. The robot has also sensors that detect proximity of the human to the robotic arm to ensure the safety conditions. Furthermore, the robot has knowledge of the layout of the room (no physical obstacle is present, the position of the bin and the pallet).

1.3 The human operator

The behaviour of the human operator is assumed not to be constrained by any “common sense” as he might try to hurt himself. This is to ensure that no harm can be done to a human operator even in the event of a human error. The position of the human is modeled as the position of his body and of the arms, all of which occupy a single square of the room. The arms can be stretched out or resting, in which case they occupy the same position of the body.

2 List of predicates

We now introduce the predicates needed to properly model the room, the robot, the human and all the events related to the work done by the robot. We split the predicates based on how the robot can know their state: from sensors or directly, since it can control them.

2.1 Whose state is known by the robot by mean of sensors

We shall first introduce the predicates whose state is known by some sensor. This includes the position of the operator as well as the state of the bins (both the “local” and the “remote” ones).
Predicates referring to the operator:

- isLeftArmAt(x, y)
- isRightArmAt(x, y)
- isOpOnTheLeft
- isOpOnTheRight
- isOperatorAt(x, y)

Predicates referring to the robot or the bins:

- isLocalBinEmpty
- isLocalBinFull
- isJointAt(x, y)
- isEndEffectorAt(x, y)
- isCartAt(x, y)
- isRobotResting

In all above predicates, as well as those that we will introduce later, we indicate with x and y the coordinate of the square describing the room as already explained.

2.2 Controlled by the robot

We now introduce the predicates modeling the robot. We modeled both the movement of the cart – which can move at two different speeds or be still – and the movement of the joint.

- isCartMoving
- isCartStill
- isCartMovingFast

- isCartMovingSlow
- isJointMoving
- isCartMovingeLeft
- isCartMovingRight

3 Specification of the system

3.1 Specification of the model

3.1.1 Description of the environment

3.1.2 Specification of the cart

1. It is impossible that the cart is moving and is still at the same time.

$$\mathsf{isCartMoving} \longleftrightarrow \neg\mathsf{isCartStill}$$

2. The cart is moving if and only if it is moving at some speed.

$$\mathsf{isCartMoving} \longleftrightarrow (\mathsf{isCartMovingFast} \vee \mathsf{isCartMovingSlow})$$

3. It is impossible that the cart is moving at different speeds at the same time.

$$\neg(\mathsf{isCartMovingFast} \wedge \mathsf{isCartMovingSlow})$$

4. The cart is moving if and only if is moving to the bin or to the pallet.

$$\mathsf{isCartMoving} \longleftrightarrow (\mathsf{isCartMovingToBin} \vee \mathsf{isCartMovingToPallet})$$

5. It is impossible that the cart is moving to the bin and to the pallet at the same time.

$$\neg(\mathsf{isCartMovingToBin} \wedge \mathsf{isCartMovingToPallet})$$

6. The cart has to be in a cell.
7. The cart can't be in more than one cell.
8. Slow speed is one cell per time step. $2 \leq x \leq 13, 1 \leq y \leq 3$

$$\begin{aligned}\mathsf{isCartMovingSlow} \wedge \mathsf{isCartAt}(x, y) \rightarrow & Dist(\mathsf{isCartAt}(x + \mathit{1}, y) \vee \mathsf{isCartAt}(x, y + \mathit{1}) \\ & \vee \mathsf{isCartAt}(x - \mathit{1}, y) \vee \mathsf{isCartAt}(x, y - \mathit{1}), 1)\end{aligned}$$

9. Fast speed is two cells per time step.

$$\begin{aligned}\mathsf{isCartMovingFast} \wedge \mathsf{isCartAt}(x,y) \rightarrow & Dist(\mathsf{isCartAt}(x+\mathit{2},y) \vee \mathsf{isCartAt}(x,y+\mathit{1}) \\ & \vee \mathsf{isCartAt}(x-\mathit{2},y) \vee \mathsf{isCartAt}(x,y-\mathit{1}),1)\end{aligned}$$

10. The robot is resting if and only if both the joint and the end effector are in the same cell of the cart.

$$\mathsf{isRobotResting} \longleftrightarrow (\mathsf{isCartAt}(x,y) \rightarrow \mathsf{isEndEffectorAt}(x,y) \wedge \mathsf{isJointAt}(x,y))$$

11. The cart is moving left if it is moving on the adjecent left cell at distance one or two.

$$\begin{aligned}\mathsf{isCartMovingeLeft} \longleftrightarrow & (\mathsf{isCartAt}(x,y) \rightarrow Dist(\mathsf{isCartAt}(x-\mathit{1},y),1)) \\ & \vee (\mathsf{isCartAt}(x,y) \rightarrow Dist(\mathsf{isCartAt}(x-\mathit{2},y),1))\end{aligned}$$

12. The cart is moving right if is moving on the adjecent right cell at distance one or two.

$$\begin{aligned}\mathsf{isCartMovingRight} \longleftrightarrow & (\mathsf{isCartAt}(x,y) \rightarrow Dist(\mathsf{isCartAt}(x+\mathit{1},y),1)) \\ & \vee (\mathsf{isCartAt}(x,y) \rightarrow Dist(\mathsf{isCartAt}(x+\mathit{2},y),1))\end{aligned}$$

3.1.3 Specification of the local bin

1. It is impossible that the local bin is empty and full at the same time.

$$\neg(\mathsf{isLocalBinEmpty} \wedge \mathsf{isLocalBinFull})$$

3.1.4 Specification of the arm

1. The joint can be in only one position at a time.

2. The joint has to be close to the cart.

$$\begin{aligned}\mathsf{isCartAt}(x,y) \rightarrow & \mathsf{isJointAt}(x,y) \vee \mathsf{isJointAt}(x+\mathit{1},y) \vee \mathsf{isJointAt}(x,y+\mathit{1}) \\ & \vee \mathsf{isJointAt}(x+\mathit{1},y+\mathit{1}) \vee \mathsf{isJointAt}(x-\mathit{1},y) \vee \mathsf{isJointAt}(x,y-\mathit{1}) \\ & \vee \mathsf{isJointAt}(x-\mathit{1},y-\mathit{1}) \vee \mathsf{isJointAt}(x+\mathit{1},y-\mathit{1}) \vee \mathsf{isJointAt}(x-\mathit{1},y+\mathit{1})\end{aligned}$$

3. The end effector can be in only one position at a time.

4. The end effector has to be close to the joint.

$$\begin{aligned}\mathsf{isJointAt}(x,y) \rightarrow & \mathsf{isEndEffectorAt}(x,y) \vee \mathsf{isEndEffectorAt}(x+1,y) \vee \mathsf{isEndEffectorAt}(x,y+1)\\ & \vee \mathsf{isEndEffectorAt}(x+1,y+1) \vee \mathsf{isEndEffectorAt}(x-1,y)\\ & \vee \mathsf{isEndEffectorAt}(x,y-1) \vee \mathsf{isEndEffectorAt}(x-1,y-1)\\ & \vee \mathsf{isEndEffectorAt}(x+1,y-1) \vee \mathsf{isEndEffectorAt}(x-1,y+1)\end{aligned}$$

5. The joint can move close to its position.

$$\begin{aligned}\mathsf{isJointMoving} \wedge \mathsf{isJointAt}(x,y) \rightarrow & Dist(\mathsf{isJointAt}(x+1,y) \vee \mathsf{isJointAt}(x,y+1)\\ & \vee \mathsf{isJointAt}(x+1,y+1) \vee \mathsf{isJointAt}(x-1,y)\\ & \vee \mathsf{isJointAt}(x,y-1) \vee \mathsf{isJointAt}(x-1,y-1)\\ & \vee \mathsf{isJointAt}(x+1,y-1) \vee \mathsf{isJointAt}(x-1,y+1), 1)\end{aligned}$$

6. The end effector can move close to its position.

$$\begin{aligned}\mathsf{isEndEffectorMoving} \wedge \mathsf{isEndEffectorAt}(x,y) \rightarrow & Dist(\mathsf{isEndEffectorAt}(x+1,y) \vee \mathsf{isEndEffectorAt}(x,y+1)\\ & \vee \mathsf{isEndEffectorAt}(x+1,y+1) \vee \mathsf{isEndEffectorAt}(x-1,y)\\ & \vee \mathsf{isEndEffectorAt}(x,y-1) \vee \mathsf{isEndEffectorAt}(x-1,y-1)\\ & \vee \mathsf{isEndEffectorAt}(x+1,y-1) \vee \mathsf{isEndEffectorAt}(x-1,y+1)\end{aligned}$$

7. The operator is on the left of the cart if its in the adjecent cell to the left.

$$\mathsf{isOpOnTheLeft} \longleftrightarrow \mathsf{isCartAt}(x,y) \wedge \bigvee_{x-3\leq h\leq x+2, y-2\leq k\leq y+2} \mathsf{isOperatorAt}(h,k)$$

8. The operator is on the right of the cart if its in the adjecent cell to the right.

$$\mathsf{isOpOnTheRight} \longleftrightarrow \mathsf{isCartAt}(x,y) \wedge \bigvee_{x-1\leq h\leq x+3, y-2\leq k\leq y+2} \mathsf{isOperatorAt}(h,k)$$

9. Definition of picking.

$$\begin{aligned}\mathsf{isRobotPicking} \longleftrightarrow & (\mathsf{isOperatorAt}(x,y) \wedge y \leq 3 \wedge \neg\mathsf{isRightArmAt}(12,4) \wedge \neg\mathsf{isLeftArmAt}(12,4)\\ & \rightarrow Dist(\mathsf{isJointAt}(13,5) \wedge \mathsf{isEndEffectorAt}(12,4), 1))\\ & \vee (\mathsf{isOperatorAt}(x,y) \wedge y \geq 5 \wedge \neg\mathsf{isRightArmAt}(12,4) \wedge \neg\mathsf{isLeftArmAt}(12,4)\\ & \rightarrow Dist(\mathsf{isJointAt}(13,3) \wedge \mathsf{isEndEffectorAt}(12,4), 1)) \vee (\mathsf{isOperatorAt}(14,4)\\ & \rightarrow Dist(\mathsf{isJointAt}(13,4) \wedge \mathsf{isEndEffectorAt}(12,4), 1))\end{aligned}$$

10. Definition of holding.

$$\begin{aligned}\mathsf{isRobotHolding} \longleftrightarrow & (\mathsf{isOperatorAt}(x,y) \wedge y \leq 3 \wedge \neg\mathsf{isRightArmAt}(\mathit{15},\mathit{4}) \wedge \neg\mathsf{isLeftArmAt}(\mathit{15},\mathit{4}) \\ & \rightarrow \mathit{Dist}(\mathsf{isJointAt}(\mathit{14},\mathit{5}) \wedge \mathsf{isEndEffectorAt}(\mathit{15},\mathit{4}),1)) \\ & \vee (\mathsf{isOperatorAt}(x,y) \wedge y \geq 5 \wedge \neg\mathsf{isRightArmAt}(\mathit{15},\mathit{4}) \wedge \neg\mathsf{isLeftArmAt}(\mathit{15},\mathit{4}) \\ & \rightarrow \mathit{Dist}(\mathsf{isJointAt}(\mathit{14},\mathit{3}) \wedge \mathsf{isEndEffectorAt}(\mathit{15},\mathit{4}),1)) \vee (\mathsf{isOperatorAt}(x,\mathit{4}) \\ & \rightarrow \mathit{Dist}(\mathsf{isJointAt}(\mathit{14},\mathit{4}) \wedge \mathsf{isEndEffectorAt}(\mathit{15},\mathit{4}),1))\end{aligned}$$

3.1.5 Specification of the operator

1. The body of the operator has to be somewhere.
2. Arms of the operator have to be close to the body.

$$\begin{aligned}\mathsf{isOperatorAt}(x,y) \rightarrow & \mathsf{isRightArmAt}(x,y) \vee \mathsf{isRightArmAt}(x+\mathit{1},y) \vee \mathsf{isRightArmAt}(x,y+\mathit{1}) \\ & \vee \mathsf{isRightArmAt}(x+\mathit{1},y+\mathit{1}) \vee \mathsf{isRightArmAt}(x-\mathit{1},y) \\ & \vee \mathsf{isRightArmAt}(x,y-\mathit{1}) \vee \mathsf{isRightArmAt}(x-\mathit{1},y-\mathit{1}) \\ & \vee \mathsf{isRightArmAt}(x+\mathit{1},y-\mathit{1}) \vee \mathsf{isRightArmAt}(x-\mathit{1},y+\mathit{1})\end{aligned}$$

$$\begin{aligned}\mathsf{isOperatorAt}(x,y) \rightarrow & \mathsf{isLeftArmAt}(x,y) \vee \mathsf{isLeftArmAt}(x+\mathit{1},y) \vee \mathsf{isLeftArmAt}(x,y+\mathit{1}) \\ & \vee \mathsf{isLeftArmAt}(x+\mathit{1},y+\mathit{1}) \vee \mathsf{isLeftArmAt}(x-\mathit{1},y) \\ & \vee \mathsf{isLeftArmAt}(x,y-\mathit{1}) \vee \mathsf{isLeftArmAt}(x-\mathit{1},y-\mathit{1}) \\ & \vee \mathsf{isLeftArmAt}(x+\mathit{1},y-\mathit{1}) \vee \mathsf{isLeftArmAt}(x-\mathit{1},\mathit{jointy}+\mathit{1})\end{aligned}$$

3. The operator can move by only one cell per time step.

$$\begin{aligned}\mathsf{isOperatorAt}(x,y) \rightarrow & \mathit{Dist}(\mathsf{isOperatorAt}(x,y) \vee \mathsf{isOperatorAt}(x+\mathit{1},y) \vee \mathsf{isOperatorAt}(x,y+\mathit{1}) \\ & \vee \mathsf{isOperatorAt}(x+\mathit{1},y+\mathit{1}) \vee \mathsf{isOperatorAt}(x-\mathit{1},y) \vee \mathsf{isOperatorAt}(x,y-\mathit{1}) \\ & \vee \mathsf{isOperatorAt}(x-\mathit{1},y-\mathit{1}) \vee \mathsf{isOperatorAt}(x+\mathit{1},y-\mathit{1}) \\ & \vee \mathsf{isOperatorAt}(x-\mathit{1},y+\mathit{1}),1)\end{aligned}$$

3.2 Specification of the behaviour

3.2.1 Cart movement

1. When the cart is moving, the robot (joint plus end effector) has to be still.

$$\neg(\mathsf{isRobotResting} \wedge \mathit{Dist}(\mathsf{isRobotResting},1)) \rightarrow \neg\mathsf{isCartMoving}$$

2. The cart has to move to the bin when the local bin is empty.

$$\mathsf{isLocalBinEmpty} \wedge \neg\mathsf{isOpOnTheLeft} \wedge \mathsf{isRobotResting} \wedge \neg\mathsf{isCartAt}(\mathit{2}, \mathit{4}) \rightarrow \mathsf{isCartMovingeLeft}$$

3. The cart has to move to the pallet when the local bin is full.

$$\mathsf{isLocalBinFull} \wedge \neg\mathsf{isOpOnTheRight} \wedge \mathsf{isRobotResting} \wedge \neg\mathsf{isCartAt}(\mathit{13}, \mathit{4}) \rightarrow \mathsf{isCartMovingRight}$$

4. The cart has to move slowly near pallet and near bin.

$$\mathsf{isCartMoving} \wedge (\mathsf{isCartAt}(\mathit{2}, \mathit{4}) \vee \mathsf{isCartAt}(\mathit{3}, \mathit{4}) \vee \mathsf{isCartAt}(\mathit{4}, \mathit{4}) \vee \mathsf{isCartAt}(\mathit{11}, \mathit{4})$$
$$\vee \mathsf{isCartAt}(\mathit{12}, \mathit{4}) \vee \mathsf{isCartAt}(\mathit{13}, \mathit{4})) \rightarrow \mathsf{isCartMovingSlow}$$

5. The cart has to move slowly when the operator is close to it.

$$\mathsf{isCartMovingeLeft} \wedge \mathsf{isCartAt}(x, y) \wedge (\mathsf{isOperatorAt}(x - \mathit{4}, y + \mathit{2}) \vee \mathsf{isOperatorAt}(x - \mathit{4}, y + \mathit{1})$$
$$\vee \mathsf{isOperatorAt}(x - \mathit{4}, y) \vee \mathsf{isOperatorAt}(x - \mathit{4}, y - \mathit{1}) \vee \mathsf{isOperatorAt}(x - \mathit{4}, y - \mathit{2})) \rightarrow \mathsf{isCartMovingSlow}$$

$$\mathsf{isCartMovingRight} \wedge \mathsf{isCartAt}(x, y) \wedge (\mathsf{isOperatorAt}(x + \mathit{4}, y + \mathit{2}) \vee \mathsf{isOperatorAt}(x + \mathit{4}, y + \mathit{1})$$
$$\vee \mathsf{isOperatorAt}(x + \mathit{4}, y) \vee \mathsf{isOperatorAt}(x + \mathit{4}, y - \mathit{1}) \vee \mathsf{isOperatorAt}(x + \mathit{4}, y - \mathit{2})) \rightarrow \mathsf{isCartMovingSlow}$$

6. The cart has to move fast if the operator is distant.

$$\mathsf{isCartMovingSlowisCartMovingRight} \wedge \mathsf{isCartAt}(x, y) \wedge x \geq 5\mathsf{isOperatorAt}(h, k) \wedge ophk \wedge (h \geq x + 5 \vee h \leq x -$$

$$\mathsf{isCartMovingSlowisCartMovingeLeft} \wedge \mathsf{isCartAt}(x, y) \wedge x \leq 10\mathsf{isOperatorAt}(h, k) \wedge ophk \wedge (h \geq x + 1 \vee h \leq x -$$

3.2.2 Robot Arm working

1. The robot has to set in the right position to grab.

$$\neg\mathsf{isLocalBinEmpty} \wedge \mathsf{isEndEffectorClosed} \wedge \mathsf{isCartAt}(\mathit{13}, \mathit{4}) \rightarrow \mathsf{isRobotPicking}$$

2. Once the robot has set it waits until it has grabbed the piece.

$$\mathsf{isEndEffectorAt}(\mathit{12},\mathit{4}) \wedge \neg\mathsf{isRightArmAt}(\mathit{12},\mathit{4}) \wedge \neg\mathsf{isLeftArmAt}(\mathit{12},\mathit{4}) \rightarrow \mathsf{isEndEffectorGrabbing}$$

3. After the end effector has grabbed, it returns in the base position.

$$\mathsf{isPieceLoaded} \rightarrow Dist(\mathsf{isEndEffectorAt}(\mathit{13},\mathit{4}) \wedge \mathsf{isJointAt}(\mathit{13},\mathit{4}), 1)$$

4. It the robot is in the base position and is holding a piece, it has to set in order to let the operator work on it.

$$\mathsf{isPieceLoaded} \wedge \mathsf{isEndEffectorAt}(\mathit{13},\mathit{4}) \wedge \mathsf{isJointAt}(\mathit{13},\mathit{4})\neg \wedge 144 \rightarrow \mathsf{isRobotHolding}$$

5. Until the piece is held, the robot mustn't move.

$$\mathsf{isPieceLoaded} \wedge \mathsf{isEndEffectorAt}(\mathit{15},\mathit{4}) \wedge \mathsf{isJointAt}(x,y) \rightarrow Dist(\mathsf{isEndEffectorAt}(\mathit{15},\mathit{4}) \wedge \mathsf{isJointAt}(x,y), 1)$$

6. If the piece is unloaded, the robot returns to the base position.

$$\neg\mathsf{isPieceLoaded} \wedge \mathsf{isEndEffectorAt}(\mathit{15},\mathit{4})\& \wedge \neg\mathsf{isOperatorAt}(\mathit{14},\mathit{4}) \rightarrow$$
$$Dist(\mathsf{isJointAt}(\mathit{13},\mathit{4}) \wedge \mathsf{isEndEffectorAt}(\mathit{13},\mathit{4})\& \wedge \mathsf{isEndEffectorClosed}, 1)$$

4 Specification of the safety properties

1. The cart and the operator cannot be in the same cell of the pallet.

$$\neg\mathsf{isCartAt}(\mathit{15},\mathit{4})$$

2. The body of the operator cannot be in the same cells of the cart.

$$\mathsf{isCartAt}(x,y) \rightarrow \neg\mathsf{isOperatorAt}(x,y) \wedge \neg\mathsf{isOperatorAt}(x-\mathit{1},y)$$

3. Operator left and right arms cannot be in the same cell of the base of the robotic arm.

$$\mathsf{isCartAt}(x,y) \wedge \neg\mathsf{isRobotResting} \rightarrow \neg\mathsf{isLeftArmAt}(x,y) \wedge \neg\mathsf{isRightArmAt}(x,y)$$

4. While the end effector is in the same cell of the operator arms, it cannot move or work.

$$\begin{aligned}&\mathsf{isEndEffectorAt}(x, y) \land (\mathsf{isEndEffectorGrabbing} \lor \mathsf{isRobotPicking} \lor \mathsf{isRobotHolding})\\ &\quad \to \neg\mathsf{isRightArmAt}(x, y) \land \neg\mathsf{isLeftArmAt}(x, y)\end{aligned}$$

5. The robotic arm cannot be in the same cell of the operator body.

$$\mathsf{isOperatorAt}(x, y) \to \neg\mathsf{isJointAt}(x, y) \land \neg\mathsf{isEndEffectorAt}(x, y)$$

6. The operator cannot be trapped at the bin.

$$\mathsf{isOperatorAt}(\mathit{1}, \mathit{4}) \to \neg\mathsf{isJointAt}(\mathit{1}, \mathit{4}) \lor \mathsf{isEndEffectorAt}(\mathit{1}, \mathit{4})$$

7. The operator cannot be trapped at the pallet.

$$\mathsf{isOperatorAt}(\mathit{14}, \mathit{4}) \to \neg\mathsf{isJointAt}(\mathit{14}, \mathit{4}) \lor \mathsf{isEndEffectorAt}(\mathit{14}, \mathit{4})$$