Formalization and Runtime Verification of Invariants for Robotic Systems*

Ricardo Cordeiro[1], Alcides Fonseca[1], and Christopher Timperley[2]

[1] Faculdade de Ciências da Universidade de Lisboa, Lisboa, Portugal
[2] Carnegie Mellon University, Pittsburgh, PA

Abstract. Robotics has a big influence in today's society, so much that a potential failure in a robot may have extraordinary costs, not only financial, but can also cost lives. Current practices in robot testing are vast and involve such methods as simulations, log checking, or field tests. The frequent common denominator between these practices is the need for human visualization to determine the correctness of a given behavior. Automating this analysis could not only relieve this burden from a high-skilled engineer, but also allow for massive parallel executions of tests, that could potentially detect behavioral faults in the robots that would otherwise not be found due to human error or lack of time. We have developed a domain-specific language to specify properties of robotic systems in ROS. Specifications written by developers in this language can be compiled to a monitor ROS module, that will detect violations of those properties. We have used this language to express the temporal and positional properties of robots, and we have automated the monitoring of some behavioral violations of robots in relation to their state or events during a simulation.

Keywords: Robotics · Domain-specific language · Runtime Monitoring · Error detection · Automation.

1 Introduction

Robotics already have a great impact on our current society. Due to their broad practicality, the quality of software used by robots should be of extreme importance to us.

The Cyber-Physical systems of robots are non-deterministic and unreliable, mainly because robots interact directly with the real world. A sensor can return imprecise values since the environment itself can be very hard to predict. As a result, verifying whether a task or movement is correct can be hard for a system to conceive.

Current practices in testing robot software involve, field testing, simulation testing, logs checking, among others. The common denominator among these is that they require a human to analyze the behavior of the robot to determine whether the behavior is correct.

* Supported by organization x.

In the case of simulators, we can use the real value of objects' attributes in a simulation to compare with what the robot system perceives, but even so problems like what components to monitor and how to express them arise. Having a domain-specific language to specify a robotic system's properties can be useful or a burden depending on its complexity and accessibility.

This work has the objective of showing how a domain-specific language can be used to specify temporal and positional properties of robotic systems and monitor the simulation components associated with these properties.

The language allows describing a robotic system's properties in a somewhat simple and intuitive way, while at the same time still being able to express relevant temporal and positional arguments between robots and objects in the simulation. The language is supported by a compiler. The compiler translates the language to a monitoring mechanism. In this way, if a robotic system doesn't follow the properties defined by the user writing in the language, during execution, the compiler detects an anomaly and makes the analysis that the behavior of the robot is not consistent.

2 Language

The domain-specific language relies on an adaptation of linear temporal logic to express temporal relations of and between simulation objects.

The domain-specific language also has shortcuts to express the absolute values of certain useful concepts of objects in a simulation.

2.1 Temporal Keywords

- always X (X has to hold on the entire subsequent path);
- never X (X never holds on the entire subsequent path);
- eventually X (X eventually has to hold, somewhere on the subsequent path);
- after X, Y (after the event X is observed, Y has to hold on the entire subsequent path);
- until X, Y (X holds at the current or future position, and Y has to hold until that position. At that position, Y does not have to hold anymore);
- after_until X, Y, Z (after the event X is observed, Z has to hold on the entire subsequent path up until Y happens, at that position Z does not have to hold anymore);

It is also possible to reference previous variable states:

$$@\{X, -y\} \tag{1}$$

This will represent the value of the variable X in the point in time -y.

2.2 Useful Predicates

- X.position (The position of the robot in the simulation);
- X.position.y (The position in the y axis of the robot in the simulation. Also works for x and z);
- X.distance.Y (The absolute distance between two objects in the simulation. For the x and y axis);
- X.distanceZ.Y (The absolute distance between two objects in the simulation. For the x, y, and z axis);
- X.velocity (The velocity of an object in the simulation. This refers to linear velocity);
- X.velocity.x (The velocity in the x axis of an object in the simulation. This refers to linear velocity);
- X.localization_error - The difference between the robot's perception of its position and the actual position in the simulation;

2.3 Examples

As an example, we specify two properties of an arbitary autonomous driving robot:

Property One :

The robot velocity will never be above 2 in the duration of the simulation;

never robot.velocity > 2.0

Property Two :

The robot always needs to stop when coming near a stop sign;

after_until robot.distance.stop_sign < 1, robot.distance.stop_sign > 1, eventually robot.velocity == 0

(Translating to a more human language we are saying that, after the robot distance to the stop_sign is below the value of 1 in the simulator, up until the distance is again above 1, the robot velocity will eventually be equal to 0)

3 Monitoring

Should i go in specifics about generated file? (subscribers, properties, etc..)?

References