UNIVERSIDADE DE LISBOA

FACULDADE DE CIÊNCIAS

DEPARTAMENTO DE INFORMÁTICA

Formalization and Runtime Verification of Invariants for Robotic Systems

Ricardo Jorge Dias Cordeiro

Mestrado em Engenharia Informática
Especialização em Interação e Conhecimento

Versão Provisória

Dissertação orientada por:
Alcides Miguel Cachulo Aguiar Fonseca

2021

Agradecimentos

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Typi non habent claritatem insitam; est usus legentis in iis qui facit eorum claritatem. Investigationes demonstraverunt lectores legere me lius quod ii legunt saepius. Claritas est etiam processus dynamicus, qui sequitur mutationem consuetudium lectorum. Mirum est notare quam littera gothica, quam nunc putamus parum claram, anteposuerit litterarum formas humanitatis per seacula quarta decima et quinta decima. Eodem modo typi, qui nunc nobis videntur parum clari, fiant sollemnes in futurum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Typi non habent claritatem insitam; est usus legentis in iis qui facit eorum claritatem. Investigationes demonstraverunt lectores legere me lius quod ii legunt saepius.

Dedicatória

Resumo

Os documentos escritos em português devem ter um resumo em português e um resumo noutra língua comunitária que contenham até 300 palavras cada. Num trabalho final escrito em língua estrangeira, este deve ser acompanhado de um resumo em português entre 1200 e 1500 palavras.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Typi non habent claritatem insitam; est usus legentis in iis qui facit eorum claritatem. Investigationes demonstraverunt lectores legere me lius quod ii legunt saepius. Claritas est etiam processus dynamicus, qui sequitur mutationem consuetudium lectorum. Mirum est notare quam littera gothica, quam nunc putamus parum claram, anteposuerit litterarum formas humanitatis per seacula quarta decima et quinta decima. Eodem modo typi, qui nunc nobis videntur parum clari, fiant sollemnes in futurum. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Typi non habent claritatem insitam; est usus legentis in iis qui facit eorum claritatem. Investigationes demonstraverunt lectores legere me lius quod ii legunt saepius.

Palavras-chave: Máximo de 5 palavras-chave separadas por vírgulas.

Abstract

Abstract in English here (max 300 words)!

Keywords: Maximum of 5 keywords separated by commas.

Contents

List of Figures

List of Tables

Listings

Chapter 1

Introduction

Robotics already have a great impact in our current society so, the quality of software used by robots should be of extreme importance for us. Robot software as well as the techniques used to test their quality are very specific to the field and differ a lot from the norm. Automatic tests are barely used in robotics due to multiple factors. The intention is then to create a tool that will promote the safe and reliable execution of automatic tests. This tool will contemplate both a descriptive high-level language that should capture certain properties of a robot and a way to create test scenarios.

1.1 Motivation

Currently, robots are vastly used industrially (medicine, agriculture, etc.) or as a form of leisure (contests, personal use, etc.). The tendency is for robot usage to keep growing at a global level. Robot tasks tend to be repetitive and/or rather specific. Robot software also tends to be quite different from conventional software. The Cyber-Physical systems of robots are non-deterministic and unreliable. One reason is the fact that robots interact directly with their environment. A sensor can return imprecise values since the environment itself can be very hard to predict. As a result, the notion that a task or movement is correct is really hard for a robot to conceive.

The current practices on testing robot software are more or less similar around developers. Field testing, simulation testing, logs checking, among others. The common denominator among these is that they require a human to analyze the behavior. The developer needs to watch the robot in action and interpret if the behavior is correct. If there were a tool that could interpret that the behavior of a robot is or isn't correct, there would be no need for human supervising at this level. No human supervision would mean automatic tests could be easily achieved for robot software. Currently, automatic tests are hardly used. Opening this door would mean an improvement in the quality of current and future robot software.

1.2 Problem Statement

There are multiple challenges in robot testing, costs, complexity, hardware integration, among others. When planning on how to test a robot there are tradeoffs between the different choices to make given into account all the challenges. While tests using simulations are a promising approach for automation there is still distrust in the precision and validity of the results. This means, although dangerous and sometimes expensive real-life robot testing is still the prime choice. Be the tests done in the real world or resorting to simulation, human supervising will most likely still be necessary. This is because identifying if a robot fulfills an expected behavior is really hard for the robot itself. For this reason, automatic tests in the robotics field are hardly reliable and hard to implement. The resulting product is a lack of quality in the software across projects [1].

1.3 Objectives

This work has the objective of showing the potencial of automatic tests in robotics and of simplifying their execution. With this in mind, the proposal is to create a mechanism that can be able to monitor certain components of the robot during or after a test execution. These components aren't arbitrary but defined by the help of a descriptive high-level language. The objective of the language is to describe a robot property in a simple and intuitive way. This language will need to be supported by a compiler. The compiler should translate the language to a monitoring mechanism. In this way, if a robot doesn't follow the properties defined by the language during a test, the compiler will infer that the robot behavior isn't correct.

The Robot Operating System (ROS) is a collection of libraries and tools that help build robot software. ROS is the most widely used tool for writing robot software. Robot simulation is an essential tool for testing. Gazebo offers the ability to simulate populations of robots in complex environments. This being said, the final scheme of the tool that will accomplish the objective should look something like the below image.

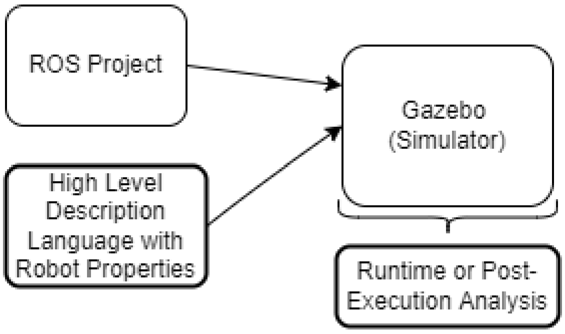
ROS Project
High Level Description Language with Robot Properties
Gazebo (Simulator)
Runtime or Post-Execution Analysis

Figure 1.1: Tool for monitoring robot properties.

1.4 Contributions

The expected contributions of this thesis are below enumerated.

1. Definition of a descriptive high-level language to specify robots properties.

2. A compiler for the language that can be used for monitoring.

3. After evaluating the capability of the solution. Model multiple relevant problems in robotics.

1.5 Structure of the document

The document is organized as follows:

- Section 1...
- Section 2...
- Section 3...

Chapter 2

Background & Related Work

Brief paragraph introducing the chapter.

Chapter 3

Proposed Approach

This is an example of a citation [2].

Appendix A

Bibliography

[1] Afsoon Afzal. A study on challenges of testing robotic systems.

[2] Alan M. Turing. Computing machinery and intelligence. In Margaret A. Boden, editor, *The Philosophy of Artificial Intelligence*, Oxford readings in philosophy, pages 40–66. Oxford University Press, 1990.