A Framework for Verifying/Testing Autonomous Robotics Systems

Huan Zhang
Supervised by Hao Wu
Principles of Programming Research Group Maynooth University (MU)

1 Abstract

*T*he development and deployment of autonomous robotic systems require rigorous verification and testing frameworks to ensure reliability, safety, and performance. This paper introduces a framework specifically designed for the verification and testing of autonomous robots,focusing primarily on enhancing the overall efficiency of the verification process.Central to this framework is the innovative specification language,Cyclone,which enables users to express graphical patterns and safety properties effectively and concisely. By integrating advanced simulation-based testing,real-world validation, and formal verification techniques, the framework establishes a multifaceted approach to ensure the reliability, safety,and performance of autonomous robotic systems.

Formal verification techniques are employed to mathematically prove the correctness of critical system components, providing a high level of assurance in their operation.The proposed framework is evaluated through a series of case studies involving different types of autonomous robots,demonstrating its effectiveness in identifying and mitigating potential failures.Scholarly discussions highlight the practical application of established methodologies such as theorem proving and hybrid systems to address the complex verification challenges inherent in autonomous robotics. Theorem proverbs like Dafny,along with interactive theorem provers such as Coq,Learn, and Isabelle,are crucial for articulating safety properties and facilitating semi-automated proof searches. Additionally,specialized tools like KeYmaera X are meticulously designed to meet the specific demands of hybrid systems verification,significantly advancing verification methodologies.

The framework's effectiveness is demonstrated through a series of case studies involving various types of autonomous robots,underscoring its capability to identify and address potential failure scenarios efficiently.By tailoring Cyclone to suit the specific needs of autonomous robotic systems,the framework leverages its inherent strengths in graph notations and safety property validation.This research aims to transform verification processes,ensuring that autonomous robotic systems adhere to rigorous safety and performance standards,ultimately paving the way for their widespread adoption across various industries.