Translating C to PlusCal for Model Checking of Safety Properties on Source Code

Abstract: Model checking is a powerful technique for verifying the correctness of systems. In practice, ensuring that an implementation adheres to its specification remains a challenging problem, especially when working with low-level languages such as C. We propose a tool that automates the translation of C code into PlusCal, enabling systematic model checking of actual programs.

Our tool is implemented as a Frama-C plug-in written in OCaml. It performs a faithful translation from C to PlusCal, preserving the semantics of the original code as much as possible. This approach allows developers to verify properties of their programs by leveraging the TLA+ model checker (TLC). The generated PlusCal code serves either:

- as a "test model" that can be used to verify properties directly on the source code; or
- as an intermediate model that can be used to establish a refinement relation between the implementation and a higher-level TLA+ specification that encodes desired correctness properties and invariants.

This tool is developed as part of a five-month internship at Asterios Technologies (Footnote), a company that develops a certified micro-kernel used in safety-critical airborne systems. Although this is not the main focus of the internship, we are experimenting with applying the transpiler to parts of that micro-kernel. The objective is to strengthen development processes and identify bugs earlier than with traditional testing campaigns. Detecting issues at this stage reduces the cost and complexity of fixing errors that would otherwise be discovered much later.

The translation process has the following methodology:

1. **Parsing and Analysis**: The Frama-C framework is used to parse and analyze the C source code, extracting its control-flow and data structures.
2. **Structural Translation**: The core translation phase converts C constructs (e.g., loops, conditionals, and function calls) into their closest PlusCal equivalents.
3. **Model Checking Integration**: The generated PlusCal code can be executed using TLC to verify safety and liveness properties.

This tool is particularly useful for safety-critical software, where formal verification can significantly enhance reliability. We will demonstrate the effectiveness of our approach with case studies showcasing the verification of concurrent C programs using PlusCal and TLA+.

We propose a presentation, including discussion, to introduce our methodology, discuss implementation details, and present experimental results. This work aims to contribute to the adoption of formal methods in software engineering by providing a

practical approach to integrating model checking into existing C-based development workflows.

(Footnote) Asterios Technologies is a subsidiary of Safran Electronics and Defense