Formal Methods

Rodolfo Lopez

USD

March 2023

Overview

Definition

- Formal methods are mathematical techniques used for the specification, verification, and validation of software and hardware systems.
- Formal methods can be used to ensure the correctness, reliability, and safety of critical systems, such as those used in aerospace, defense, transportation, and healthcare.

Model Checking

- Model checking is a formal verification technique that checks whether a model of a system satisfies a given specification.
- Let M be a model of a system and ϕ be a specification of the system. If we can check that M satisfies ϕ using model checking, then we can guarantee that the system satisfies ϕ as well.
- Model checking can be used to verify that a circuit design meets its functional requirements and does not have any logical errors that could cause it to malfunction.

Model Checking Example

- Suppose M is a model of a system and ϕ is a specification of the system.
- To check if M satisfies ϕ, we construct the negation of ϕ, denoted as $\neg\phi$.
- We then check if there exists a state in M where $\neg\phi$ holds. If such a state exists, then M does not satisfy ϕ. Otherwise, M satisfies ϕ.
- This proof is based on the soundness and completeness of propositional logic, which ensures that the negation of a true proposition is false and vice versa.

Lean Proof Assistant

- Lean is a powerful proof assistant that allows users to write and verify mathematical proofs using formal logic.
- It is based on dependent type theory, which allows for the definition of complex data structures and logical propositions.
- Lean provides a user-friendly interface for writing and checking proofs, making it an ideal tool for formal methods.

Lean Example Code

```
inductive mynat
| zero : mynat
| succ (n : mynat) : mynat

lemma zero_add (n : mynat) : zero + n = n :=
begin
induction n with d hd,
{
  rw add_zero,
},
{
  rw add_succ,
  rw hd,
}
end
```

Modern Applications

Formal methods and proof assistants like Lean are used in a variety of applications, including:

- **Software Verification**: Formal methods can be used to verify that software is correct and free of bugs. This is particularly important in safety-critical systems, such as medical devices and transportation systems.
- **Hardware Verification**: Formal methods can also be used to verify that hardware designs are correct and meet specifications.
- **Artificial Intelligence**: Formal methods are increasingly being used in the development of AI systems, to ensure that they are safe, reliable, and free of bias.
- **Blockchain Technology**: Formal methods are used to verify the correctness and security of smart contracts and other blockchain-based systems.

Challenges

- Formal methods require a high level of mathematical expertise and are often time-consuming and expensive to apply.
- Formal methods can only guarantee correctness with respect to a given specification, which may not capture all possible scenarios or requirements of a system.

Conclusion

- Formal methods and proof assistants like Lean are powerful tools for specifying, developing and verifying software and hardware systems.
- They are used in a variety of applications and are particularly important in safety-critical systems, AI, and blockchain technology.