The Lean Theorem Prover

Gabriel Ebner

2017-09-18

TU Wien

The Lean Theorem Prover

- Interactive theorem prover

- Primarily developed by Leonardo de Moura (Microsoft)
- Big group at CMU around Jeremy Avigad

- `https://leanprover.github.io/`
- Open Source

Logical foundations

- Dependent type theory
  - Variant of the Calculus of Inductive Constructions

- Small kernel
  - Only basic inductive types and structural recursion
  - Well-founded recursion, etc., defined on top

- Proofs can be independently checked
  - 3 independent type-checkers
  - $\sim$ 1500 lines of code

- Dependent pattern-matching
- Type classes
- Coercions
- Syntax for structures, do-notation
- Default arguments
- Call-by-name arguments
- Custom operators

Meta-programming features

- Fast virtual machine
- Efficient meta-programming
- Tactics implemented in Lean
- User-extensible syntax
- Profiler, debugger

Interactive features

- Editor modes for Emacs and VS Code
- Immediate feedback
- Go-to-definition, etc.

- Parallel and incremental compilation

Automation

- Type-class inference
  - General back-chaining solver

- Simplifier
  - (Conditional) term rewriting system

- Congruence closure (modulo AC)
- Unit propagation
- Heuristic instantiation (E-matching)
  - "SMT tactics"

Tutorial

https://github.com/gebner/avm2017_tutorial

Lean

Tutorial

Conclusion

- Native compilation

- Automation for arithmetic

- Macros and refactoring

- Certified bit-blasting