

[Demo]

# MoChi: Software Model Checker for a Higher-Order Functional Language

Ryosuke Sato

Tohoku University

Hiroshi Unno

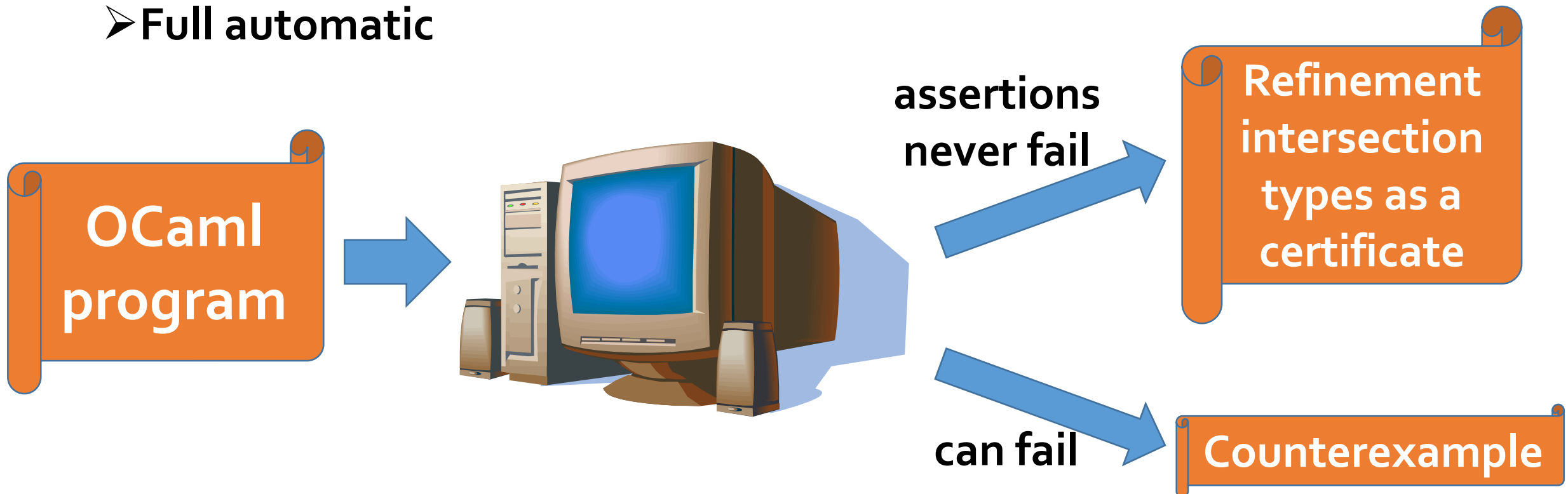
University of Tsukuba

Naoki Kobayashi

University of Tokyo

# MoChi: Software Model Checker for Higher-Order Functional Programs

- Based on *higher-order model checking* [Ong 2006, Kobayashi 2009], *predicate abstraction*, and *CEGAR* [PLDI 2011]
- Full automatic



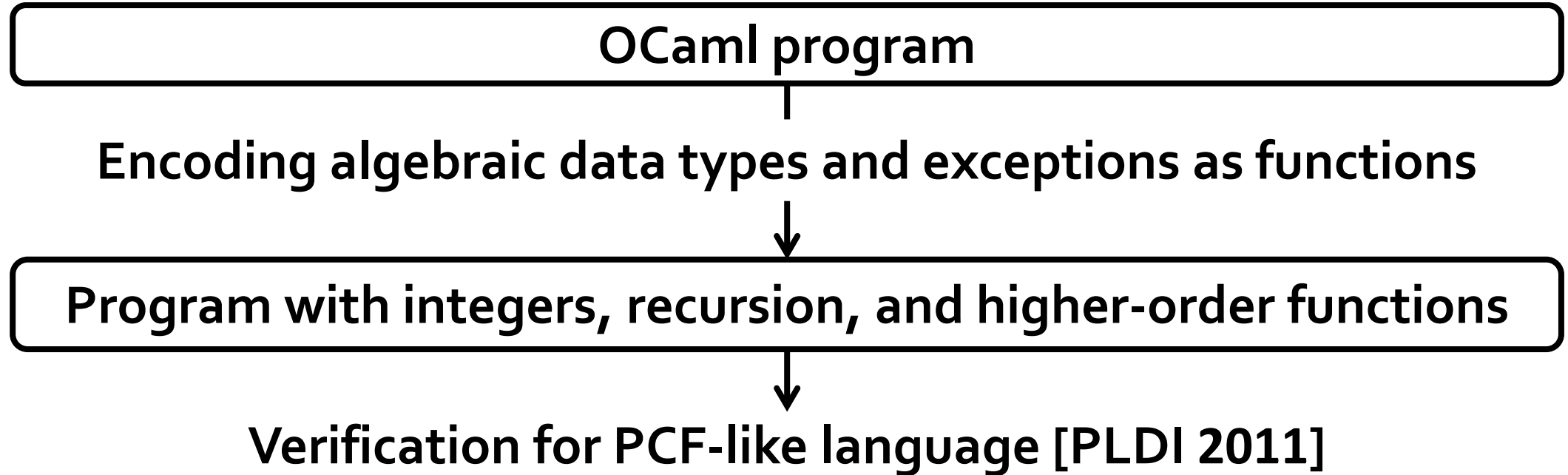
# Supported Language Features

- **Booleans, integers, tuples**
- **Recursion**
- **Higher-order functions**
- **Exceptions (modulo some restrictions)**
- **Algebraic data types (includes user-defined data types)**

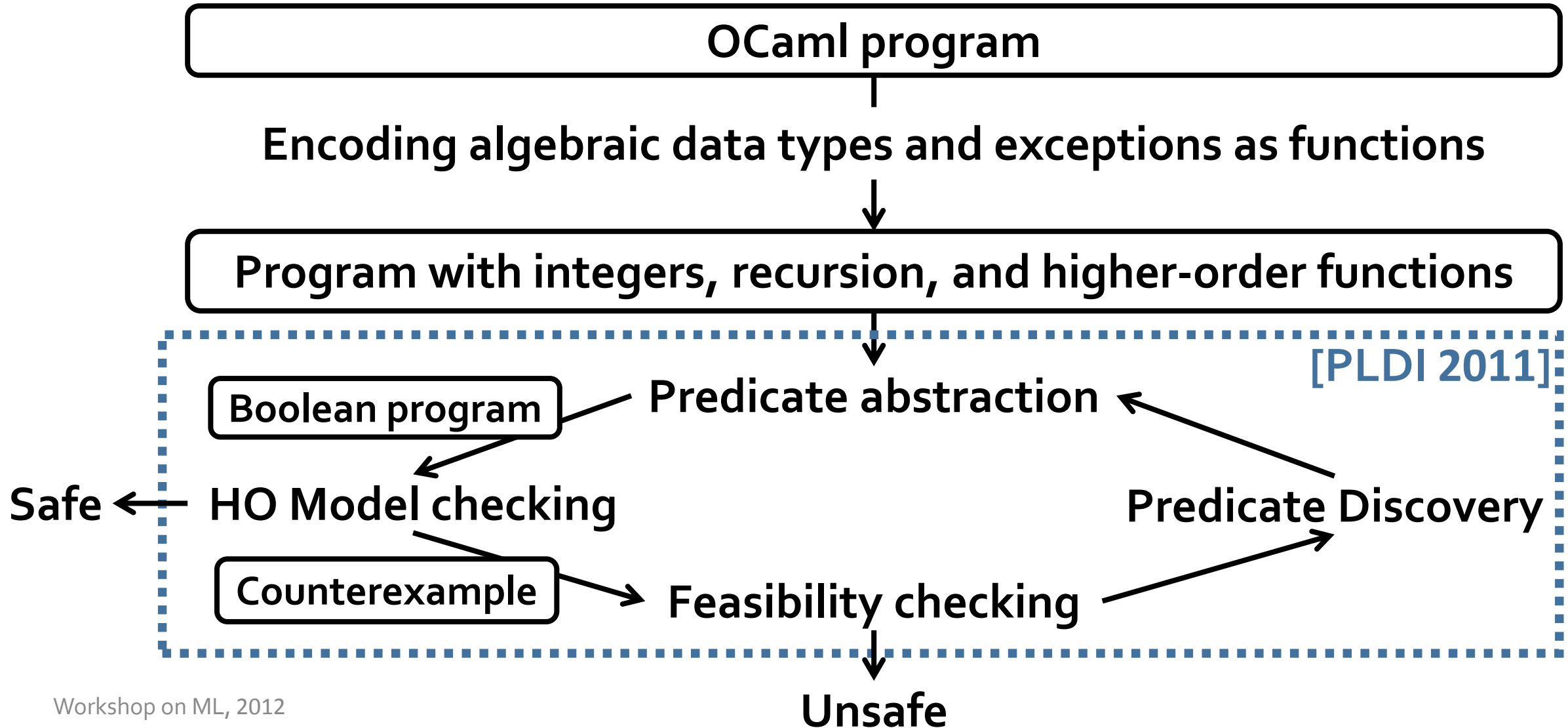
# Supported Properties

- The assertions in the program never fail
- The pattern matches in the program are exhaustive
- An uncaught exception does not occur

# Internals of MoCHi



# Internals of MoChi



# Comparison with Related work

	Annotations	Counterexample discovery	Intersection types (Context-sensitivity)
MoChi	Nothing	✓	✓
Liquid types [Rondon et al.]	Predicates used in refinements	✗	✗
DML [Xi et al.]	Refinement types of recursive functions	✗	✗
HMC [Jhala et al.]	Nothing	✓?	✗

# Conclusion & Future work

- **We have implemented MoChi, a verifier for a subset of OCaml with**
  - **base types, tuples, higher-order functions, recursions**
  - **exceptions, algebraic data types**
- **Future work includes:**
  - **Supporting a larger subset of OCaml**
  - **To be more scalable**