TLA$^+$

Denis Cousineau
Damien Doligez
Leslie Lamport
Stephan Merz
Hernán Vanzetto

Kaustuv Chaudhuri, Dan Ricketts,
Jean-Baptiste Tristan, Simon Zambrovski

Outline

TLA$^+$

TLA$^+$ is :

- A specification language based on :
  - First-order logic and Set theory
  - (Linear) temporal logic
- Especially suited for specifying concurrent and distributed systems
  - Distributed fault-tolerant consensus (Paxos)
  - Shared virtual memory hardware (WildFire, alpha EV7)
  - Garbage collection algorithm (Concurrent Caml Light)
  - Web services protocols
- A declarative tree-structured proof language
- A front-end language (PlusCal)

2009 : Peterson's algorithm

What's new since 2009

Language :

- tuples and sequences
- characters and strings
- records
- CASE expressions
- CHOOSE operator
- arithmetic

A GUI connected with :

- PlusCal translator
- TLC model-checker
- SANY analyzer
- TLAPM proof manager

More automation in the back-end provers

2011 : Byzantine Paxos

Future Work

- temporal logic (hard to integrate with FOL)
- arithmetic
- enhance the back-ends (Isabelle/TLA+, Zenon)
- new back-ends (SMT solvers, VeriT)
- more examples
- proofs of real-world systems : PharOS (CEA)
- tuning the language and the system

Thank you