Interaction and Automation

N. Shankar

Computer Science Laboratory
SRI International
Menlo Park, CA

Aug 7, 2009

\[1\text{This research was supported NSF Grants CNS-0823086 and CNS-0644783.}\]
Proof construction is an important formal activity, but there are others: *modeling, testing, refutation, abstraction, evaluation, search, exploration, synthesis, and simplification.*

There's a range of verification techniques: *model checking, test generation, simulation, abstraction, SAT, SMT, and static analysis.*

Interactive proof checkers are great for some things, but . . .

*How can we expand the range of tools that can be integrated and used interactively?*
SAT/SMT solvers (Yices 1, Yices 2, Z3) have been used for proving, constraint solving, planning, test generation, predicate abstraction, breaking/verifying crypto, synthesis, and image construction.

Yices has been integrated into PVS and Isabelle/HOL (Erkok/Matthews).
PVS: ITP as a Front-End

- Typechecker
- Model checker
- SMT Solver
- Mona
- Code Generator
Toolbus: P2P Integration

- SAT/SMT
- Model Checker
- Type Checker
- Abstractor
- PVS
- Code Generator

Tool Bus
Verification involves requirements, models, domains, assertions, programs, test cases, abstractions, and proofs.

It is going to involve multiple tools and multiple collaborators.

OVP is a framework for sustaining such a collaboration.

The foundation for OVP is provided by a hyperfile system (HyFile) that keeps file systems functionally synchronized.

When files are checked in, HyFile executes actions needed to update the files, e.g., \texttt{\LaTeX}, \texttt{make}, clones, regressions, profiling, notifications, email, provenance, workflow, distributed computing, file sharing, . . .
Verified Reference Kernel (V Kernel)

- Untrusted Frontline Verifier
- Verified Offline Verifier
- Verified Checker
- Trusted Proof Kernel

Connections:
- Hints to Verified Offline Verifier
- Certificates to Trusted Proof Kernel
- Proofs to Verified Checker
Interaction + Automation

- Interaction without automation is laborious.
- Automation without interaction is misguided.
- There’s more to formality than proof.
- The evidential tool bus is a P2P architecture for gathering evidence.
- HyFile manages the consistency of a file system and supports collaboration between multiple, distributed users and tools.
- The V Kernel efficiently certifies the claims.