Model Checking for the Practical Verificationist: A User's Perspective on SAL

Lee Pike
leepike@galois.com

Galois Inc.

May 2, 2008

SAL's language in a slide

- Typed with predicate subtypes (incomplete type-checker).
- Higher-order functions.
- Uninterpreted functions.
- Infinite types (e.g., `INTEGER` and `REAL`).
- Synchronous (lock-step) and asynchronous (interleaving) composition (`||` and `[]`, respectively).
- Algebraic data types.
- Quantification (over finite types).
- Recursion (over finite types).

Cheap Invariants

Finding inductive invariants is hard and is the basis for proving safety properties. Three strategies:

1. k-Induction to strengthen invariants *automatically*.
   - Generalizes induction over transition systems.
   - Automatic, but exponential in the size of k.
2. Disjunctive invariants.
   - Each disjunction covers some configuration of the system.
   - Developed by Pneuli & Rushby, independently.
   - A disjunctive invariant can be built iteratively to cover the reachable states from the counterexamples returned by SAL for the hypothesized invariant being verified.
3. Nondeterministic assignment vs. asynchronous composition.

k-induction

Generalize from single transitions to trajectories of fixed length.

Consider a transition system $< S, S^0, \rightarrow >$. For safety property P, show

- **Base**: If $s_0 \in S^0$, then for all trajectories $s_0 \rightarrow s_1 \rightarrow \ldots \rightarrow s_k$, $P(s_i)$ for $0 \leq i \leq k$;
- **IS**: For all trajectories $s_0 \rightarrow s_1 \rightarrow \ldots \rightarrow s_k$, If $P(s_i)$ for $0 \leq i \leq k-1$, then $P(s_k)$.

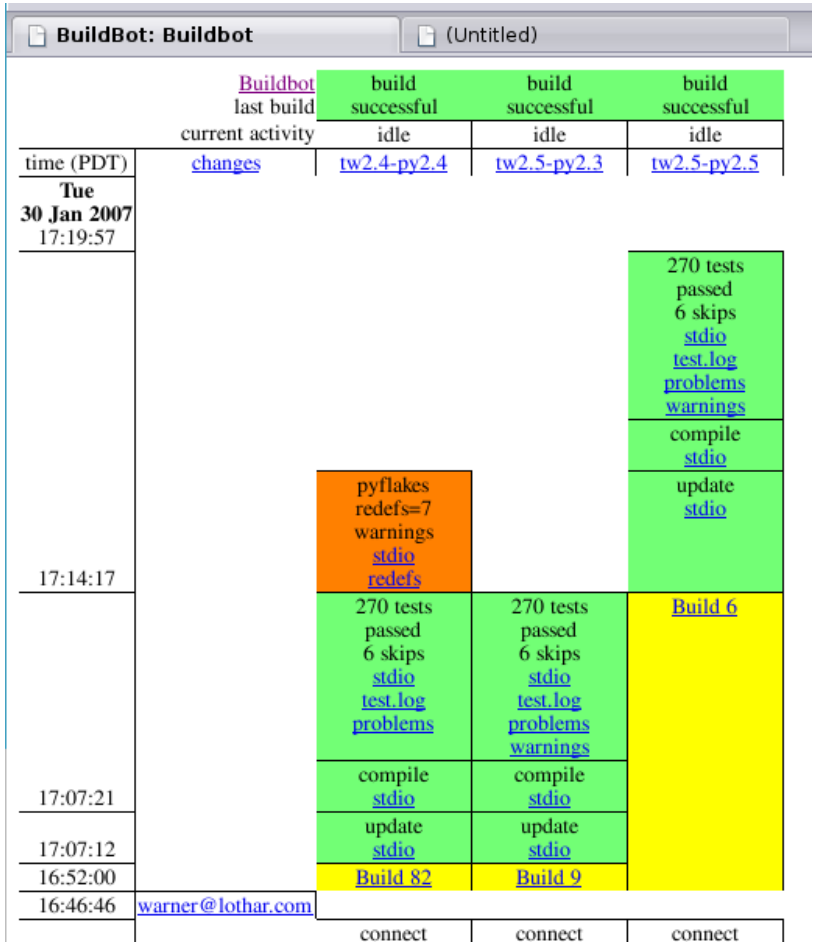
Conclude that for all reachable s, $P(s)$.

Induction is the special case when $k = 1$.

Models and Development

We build our models and code side-by-side.

- Helps ensure design + code stays in sink.
- Healthy shame if proofs fail.
- Takes FM seriously as part of development process.
- I've added some Bash scripts to the SAL wiki:
  http://sal-wiki.csl.sri.com/index.php/User-supplied_SAL-related_shell_scripts



Credit: Buildbot web page
http://buildbot.net/trac/wiki/ScreenShots

Acknowledgments and Resources

SAL coauthors: Geoffrey Brown, Paul Miner, Steve Johnson, and Wilfredo Torres-Pomales.

Paper & Specification:

`http://www.cs.indiana.edu/~lepike`

Google: lee pike