A Panel on Proof Certificates

Dale Miller (moderator),
Andrew Appel, Frank Pfenning, and Benjamin Werner

Certified Programs and Proofs, 7 December 2011

Imagine a world in which computational logic systems can communicate and trust proofs on a routine basis.

There is a lot of diversity to address

A wide range of provers:

- automated and interactive theorem provers
- model checkers, SAT solvers
- type inference, static analysis
- testers

A wide range of "evidence" of proof.

- proof scripts: steer a theorem prover to a proof
- resolution refutations, natural deduction, tableaux, etc
- winning strategies, simulations

More exotics evidence should be admitted as well.

- Partial proofs
- Counter-examples

A (familiar) revolution is needed in formal methods

Sun Microsystems (1984):
The network *is* the computer

Can we move from using many *isolated provers* to the expectation that a proof is not finished until it is *shared* and *checked*.

N.B.: The world of the "bad guys" is highly *dynamic* and *networked:* viruses, mutations of viruses, botnets, root kits, etc.

Some questions

1. Should we push the de Bruijn criterion (proofs should be checked by simple kernels) to the next step: require provers to output proofs into a format that a trusted proof checker can check?
2. Can theorem provers output proof evidence that is free from their specific implementation details?
3. How complex can proof checkers be? Can they contain a programming language? How do we trust a proof checker?

Some more questions

1. What approaches to communicating and trusting proofs are already working at some scale: eg, used in SAT competitions, resolution systems (eg, the Ivy checker), and deduction modulo (Dedukti)?
2. Is it worthwhile to build the infrastructure of proof certificates and proof checkers and to modify existing provers to use that infrastructure?
3. The structure of proofs derive not only from the underlying logic but also from theories built on top of logics. How are theories and proofs related? How are two different theories related?