Compiling HOL4 to Native Code

Joe Hurd
joe.hurd@comlab.ox.ac.uk

Oxford University

Interactive Theorem Provers?

- Most higher order logic theorem proving takes place in interactive mode.
  - Users guide the theorem prover towards the proof of a few key theorems.
- Formal reasoning might also be useful inside a software application.
  - For example, a compiler might need to justify that an optimization is safe at a particular program point.
- The application could code up the reasoning as a tactic, and link with a higher order logic theorem prover.
  - Higher order logic allows many application domains to be naturally modelled.
  - LCF kernel gives high assurance of soundness.

Client Applications for HOL4

- Synthesis of Verilog monitors from PSL assertion formulas [Gordon, Hurd and Slind]
  - Prove that the monitor flags an error iff the assertion has been violated.
- NetSem: deriving a formal semantics of the TCP protocol [Sewell et. al.]
  - Special purpose tactic to check whether a captured network trace conforms to the current specification.
  - Whenever there’s a conflict, fix the specification!

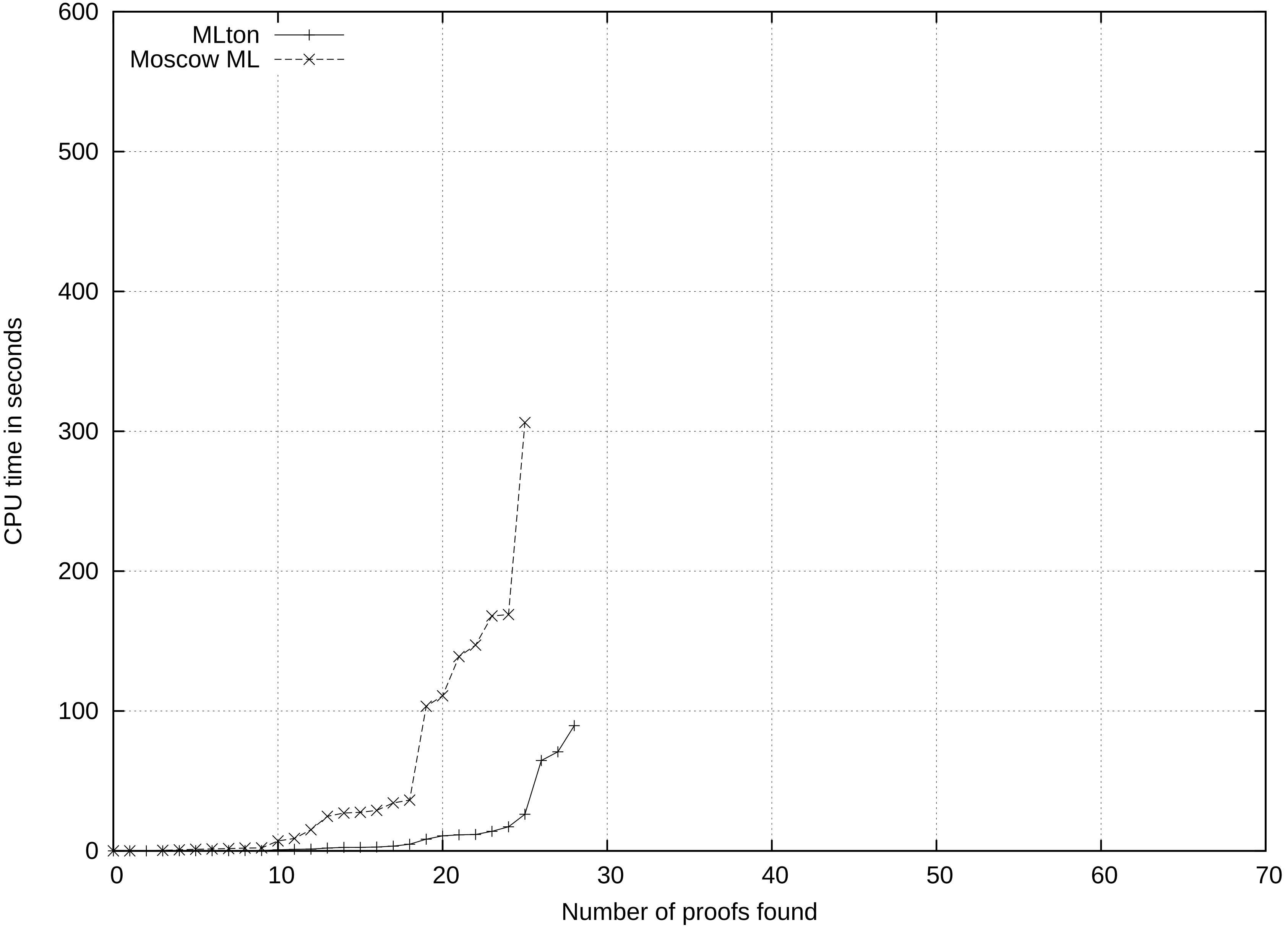
MLton

- MLton is a whole-program optimizing compiler for Standard ML.
- Executing HOL4 ’in batch mode’ instead of via a top-level interactive loop means that we can use MLton to compile our applications.
- What kind of efficiency gain is possible over the existing platform of interpreted Moscow ML bytecode?

Case Study: A First Order Prover

- Wrap up the HOL4 first order proof tactic, METIS_TAC, as a program suitable for entry in CADE Automated Systems Competition (CASC).
- Source: 60,000 lines of Standard ML
  Moscow ML: 0.5Mb executable
  MLton: 14Mb executable
- Run on the First Order Formula division of CASC 2003.
- Moscow ML solves 23 problems out of 70
  - Places between the 4th prover (DCTP) and 5th prover (Otter) out of the 6 entered.
- MLton solves 28 problems (same placing).
  - On average a factor of 10 speed-up.

Case Study: A First Order Prover


MLton
Moscow ML
CPU time in seconds
Number of proofs found