Proof Engineering: The Soft Side of Hard Proof

Submitted by Katie Dey on Thu, 04/23/2015 - 6:36pm. Contributor:
Gerwin Klein

Abstract:
We do formal machine-checked proof because it produces mathematical theorems and hard guarantees. But there is also a softer side: the process by which we arrive at the final proof. Especially in larger-scale formal proofs such as in the Odd-Order theorem or in program verification such as the correctness proof of the seL4 microkernel, issues of proof engineering become important factors in determining success or failure. This talk will give an overview of proof engineering problems in large-scale proofs, and present some of the solutions employed in the seL4 verification. A particular open problem in proof engineering is effort prediction. I will give an overview of recent preliminary statistical results on the correlation of proof size and effort and of specification size and proof size.

Biography:
Gerwin Klein is a Senior Principal Researcher at NICTA, Australia's National Centre of Excellence for ICT Research, and Conjoint Professor at UNSW in Sydney, Australia. He is leading NICTA's Formal Methods research discipline and is the leader of the seL4 verification effort that created the first machine-checked proof of functional correctness of a general-purpose microkernel in 2009. He joined NICTA in 2003 after receiving his PhD from Technische Universitat Munchen, Germany, where he formally proved type-safety of the Java Bytecode Verifier in the theorem prover Isabelle/HOL. His research interests are in interactive formal verification, programming languages, and systems code. Gerwin Klein has won a number of awards, among them together with his team the 2011 MIT TR-10 award for the top ten emerging technologies world-wide for the kernel verification work, and NICTA's Richard E. Newton impact award for the same.

Other available formats:

Proof Engineering: The Soft Side of Hard Proof

Validation and Verification prediction specification theorems National HCSS Conference 2015 Abstract HCSS'15 Proof Engineering (HCSS'15)