Prototype Verification System

Bob van der Linden

02-06-2010

Prototype Verification System

- Specificatie-taal
  - Uitgebreide typerings-mogelijkheden.
- Interactive prover
  - Veel geautomatiseerd.

Achtergrond

- Computer Science Laboratory of SRI International in Californië
- Komt voort uit LCF en Nqthm.
  - Meer automatisatie dan LCF.
  - Meer controle dan Nqthm.
- Gesponsort door NASA

Ontwikkeling

- 1993: beschikbaar
- 2006 december: Versie 4.0 en open-source
- 2008 juli: eerste teken van 4.2
- 2010 februari: versie 4.2
- 2010 april: laatste commit

Toepassingen

- Verification of the AAMP5 microprocessor - Mandayam K. Srivas, Steven P. Miller
- TAME (Timed Automata Modeling Environment) uses PVS as back end It is used for requirements and security, have a Common Criteria EAL7 certified embedded system - C.L. Heitmeyer, M.M. Archer, E.I. Leonard, J.D. McLean
- LOOP is used to verify Java code, applied to JavaCard - J. van den Berg, B. Jacobs, E. Poll
- Mifare card security broken - Bart Jacobs
- Many NASA/NIA applications - clock synchronization, fault-tolerance, floating point, collision avoidance - C. Mu ˜oz, R. Butler, B. Di Vito, P. Miner n
- InVeSt: A Tool for the Verification of Invariants - S. Bensalem, Y. Lakhnech, S. Owre
- Maple interface - Andrew Adams, Martin Dunstan, Hanne Gottliebsen, Tom Kelsey, Ursula Martin, Sam Owre, Clare So
- A Semantic Embedding of the Ag Dynamic Logic - Carlos Pombo
- Early validation of requirements - Steve Miller
- Programming language meta theory - David Naumann
- Cache coherence protocols - Paul Loewenstein
- Systematic Verification of Pipelined Microprocessors - Ravi Hosabettu
- Vamp processor - Christoph Berg, Christian Jacobi, Wolfgang Paul, Daniel Kroening, Mark Hillebrand, Sven Beyer, Dirk Leinenbach
- Flash protocol - Seungjoon Park
- Trust management kernel - Drew Dean, Ajay Chander, John Mitchell
- Self stabilization - N. Shankar, Shaz Qadeer, Sandeep Kulkarni, John Rushby
- Sequential Reactive Systems, Garbage Collection verifications - Paul Jackson
- Software reuse, Java verification, CMULisp port of PVS - Joe Kiniry
- Reactive systems, literate PVS - Pertti Kellomaki
- Garbage collection - Klaus Havelund, N. Shankar
- Nova microhypervisor, Coalgebras, Numerous PVS bug reports - Hendrik Tews
- Why: software verification platform has PVS as a back-end prover - Jean-Christophe Fillitre
- Adaptive cache coherence protocol - Joe Stoy, et al
- PBS: Support for the B-Method in PVS - CsarMuoz
- SPOTS: A System for Proving Optimizing Transformations Sound - Aditya Kanade
- Time Warp-based parallel simulation - Perry Alexander
- Linking QEPCAD with PVS - Ashish Tiwari
- Distributed Embedded Real-Time Systems, Reactive Objects - Jozef Hooman
- TLPVS: A PVS-Based LTL Verification System - Amir Pnueli, Tamarah Arons

Toepassingen

- LOOP-tool bij PVS voor JavaCard - J. van den Berg, B. Jacobs, E. Poll
- Mifare/OVchip-kaart - Bart Jacobs
- Why gebruikt PVS - Jean-Christophe Fillitre

Bronnen

- http://www.csl.sri.com/users/owre/papers/tphols08/pvstut-tphols08.pdf
- http://en.wikipedia.org/wiki/Prototype_Verification_System
- http://www.csl.sri.com/projects/pvs/