VERIFICATION OF CONCURRENT DATA STRUCTURES

VERCORS
MARIEKE HUISMAN

22ND OF APRIL, 2010
THE FUTURE OF COMPUTING IS MULTICORE

Single core processors: The end of Moore’s law

Solution: Multi-core processors

Multiple threads of execution
Coordination problem shifts from hardware to software
MULTIPLE THREADS CAUSE PROBLEMS

- Order?
- More threads?

Possible consequences: errors such as data races caused lethal bugs as in Therac-25

UNIVERSITY OF TWENTE.
PROGRAM LOGICS CHASE BUGS

Floyd - Hoare → LOOP FOREVER KEY → ESC/Java2

concurrency → Owicki - Gries

Owicki - Gries → O’Hearn

O’Hearn → 2007 separation logic

2007 separation logic with Haack & Hurlin → VerCors

VerCors - UNIVERSITY OF TWENTE.
WHAT WILL BE NEW IN VERCORS?

Automated verification of concurrent software

- Collection of verified concurrent data structures
- Generic verification theory of concurrent programming
  - Different concurrency and synchronisation techniques
  - Allows to change locking policy
  - Different programming languages
- Automation
  - Decision procedures for proof obligations
  - Generation of specifications
SUCCESS FACTORS VERCORS

Experienced researcher
Expert in area of
- program verification
- concurrency

Successful in supervision

Now is the time
- Theory is maturing
- Multicore is omnipresent
- Practical usability in reach

Guaranteed dissemination
- Collaboration with tool builders for sequential programs
- High demand for results
- Good contacts

and others...

UNIVERSITY OF TWENTE.
OBJECTIVES VERCORS

Automated verification of concurrent software