Program Verification in the Presence of Cached Address Translation

Hira Taqdees Syeda | Gerwin Klein

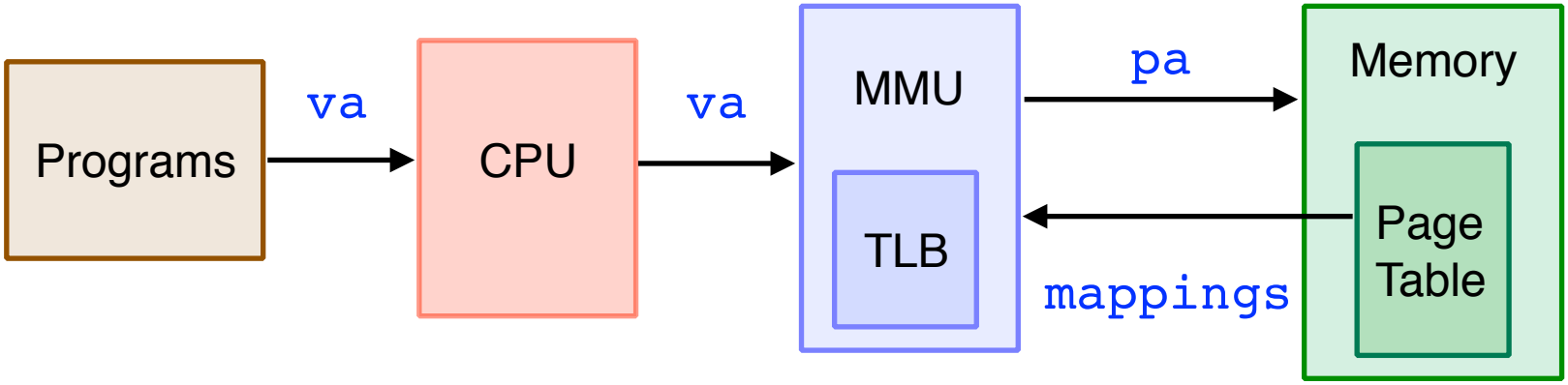
July 2018

www.ts.data61.csiro.au

UNSW SYDNEY

CSIRO

What is Cached Address Translation



- Translation Lookaside Buffer (TLB) is
  - a dedicated cache for page table walks
  - architecture specific
  - managed by hardware and operating system together

TLB Effects on Program Execution

- TLB being cache
  - has *no* functional effects
  - only makes execution faster, *if* maintained correctly
  - is an assumption in formally verified kernels such as seL4

- Poorly managed TLB leads to
  - memory operations on the wrong addresses
  - inconsistent translation ⇒ system crash

- TLB-aware logic for program reasoning
  - abstract model for ARMv7-style MMU

Contributions

- TLB-aware program logic in Isabelle/HOL
  - sound abstraction of ARMv7-style MMU
  - language with TLB management primitives
  - TLB-aware Hoare logic rules
- Reduction theorems for program verification at
  - user- and kernel-level execution
  - context switch

Sound Abstraction of ARMv7-style MMU

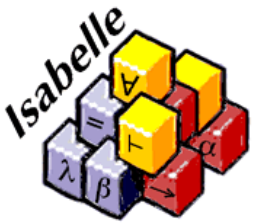
- Formalised TLB model
  - hardware details
  - instructions affecting the TLB state

- For program reasoning, TLB introduces
  - unspecified entry replacement
  - state change during memory read and memory write
  - potential inconsistencies

- Programs
  - must avoid inconsistencies
  - should not require reasoning about eviction and state change

Sound Abstraction of ARMv7-style MMU

- Formalised TLB model
  - hardware details
  - instructions affecting the TLB state



Stepwise data refinement
to achieve functional abstraction

Functionality of a TLB
is captured by the record of
inconsistent virtual addresses

abstract TLB

set of
inconsistent vaddrs

Program Verification

- Address space management
  - inspired by seL4
- User-level programs
  - cannot update page table,
    hence cannot affect TLB consistency

reasoning is reduced to
standard Hoare logic rule with address translation

- Kernel-level programs
  - that do not modify page table

Program Verification

- Address space management
  - inspired by seL4
- Kernel-level programs
  - that do modify page tables

✓TLB consistency is regained by flushing the entries

✓logic correctly identifies when the flush is due

Taken Together

- simplicity of the logic and memory model
- reduction to Hoare logic for most use-cases

more in the papers:
details of memory model and
reduction theorems

theories available on github:
`SEL4PROJ/tlb`

Questions