

# Sound and Efficient WCET Analysis in the Presence of Timing Anomalies

Jan Reineke<sup>1</sup>, Rathijit Sen<sup>2</sup>

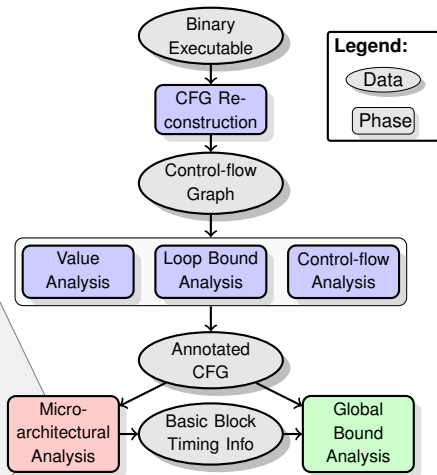
<sup>1</sup>Saarland University, Saarbrücken

<sup>2</sup>University of Wisconsin, Madison

Workshop on WCET Analysis, Dublin 2009

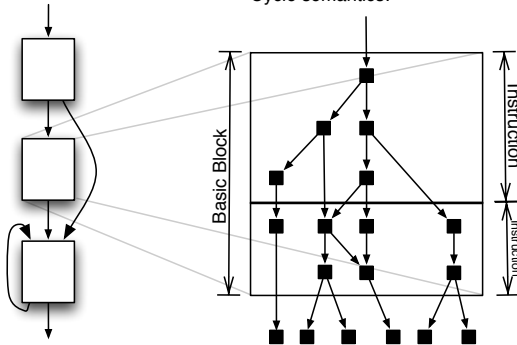


- ▷ Determines bounds on execution times of basic blocks
- ▷ Based on an abstract model of the hardware
- ▷ Either *sound* or *efficient* due to *timing anomalies*
- ▷ Usually most expensive part of WCET analysis

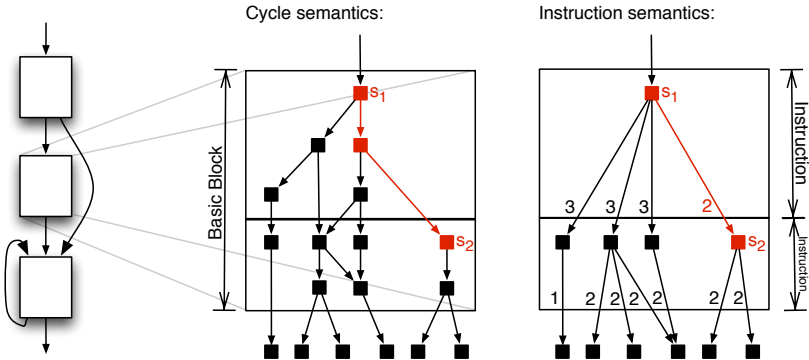


# Model of Micro-Architectural Analysis

Cycle semantics:



# Model of Micro-Architectural Analysis



*Notation:*

$$s \xrightarrow[l_0 \dots l_n]{t} s'$$

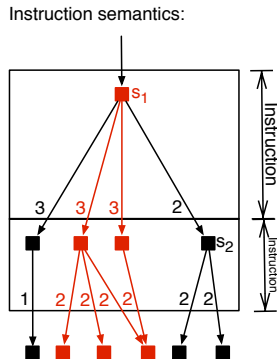
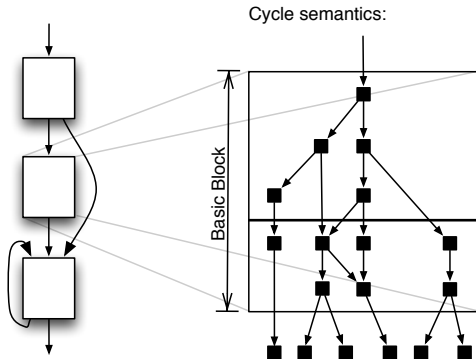
$$\max(s, l_0 \dots l_n) := \max\{t \mid s \xrightarrow[l_0 \dots l_n]{t} s'\}$$

*Example:*

$$s_1 \xrightarrow[l_1]{2} s_2$$

$$\max(s_1, l_1 l_2) = 5$$

# Model of Micro-Architectural Analysis



Notation:

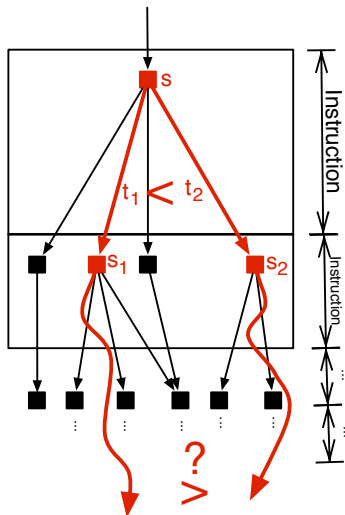
$$s \xrightarrow[t]{l_0 \dots l_n} s'$$

$$\max(s, l_0 \dots l_n) := \max\{t \mid s \xrightarrow[t]{l_0 \dots l_n} s'\}$$

Example:

$$s_1 \xrightarrow[l_1]{2} s_2$$

$$\max(s_1, l_1 l_2) = 5$$

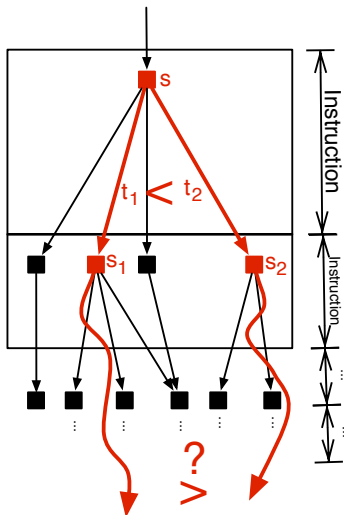


## Definition (Timing anomaly)

An instruction semantics has a *timing anomaly* if there exists a sequence of instructions  $l_0 l_1 \dots l_n$ , and an abstract state  $s$ , such that

- there are states  $s_1, s_2$ , with  $s \xrightarrow{t_1} s_1$  and  $s \xrightarrow{t_2} s_2$ , and  $t_1 < t_2$ , such that
- $t_1 + \max(s_1, l_1 \dots l_n) > t_2 + \max(s_2, l_1 \dots l_n)$ .

# Safely Discarding Analysis States



**Idea:** Precompute maximal difference in timing for pairs of states.

Discard states that cannot “overtake” others anymore.

“Locally exclude timing anomalies.”





## System of *difference constraints*:

For empty sequence of instructions:

$$\Delta(s_1, s_2) \geq 0$$

Recursive constraints:

$$\Delta(s_1, s_2) \geq t'_1 - t'_2 + \Delta(s'_1, s'_2) \quad \text{if } s_1 \xrightarrow{t'_1} s'_1 \wedge s_2 \xrightarrow{t'_2} s'_2 \text{ for some } \iota.$$

→ Can be solved by a shortest paths computation.

Least  $\Delta(s_1, s_2)$  not always finite:

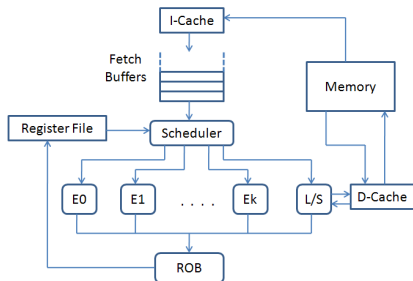
## Definition (Domino effect)

An instruction semantics has a *domino effect* if there are two states  $s_1, s_2$ , such that for each  $\Delta \in \mathbb{N}$  there is a sequence of instructions  $\iota_0 \dots \iota_n$ , such that

$$\max(s_1, \iota_0 \dots \iota_n) - \max(s_2, \iota_0 \dots \iota_n) \geq \Delta.$$

**But:** Ratio  $\frac{\max(s_1, \iota_0 \dots \iota_n)}{\max(s_2, \iota_0 \dots \iota_n)}$  always bounded.

- Computed  $\Delta$  function for simple processor with:
  - ▶ 2 instruction types
  - ▶ 2 functional units
  - ▶ execution times between 2 and 6 cycles
  - ▶ a 4 instruction fetch buffer
- Results:
  - ▶ 555 states
  - ▶ 97340 constraints
  - ▶  $\Delta$  function ranges from 0 through 7



- Sound and efficient WCET analysis in the presence of timing anomalies, by
  - ▶ locally excluding timing anomalies, using
  - ▶ precomputed  $\Delta$  functions.
- Computed  $\Delta$  functions for relatively simple architectures.
  
- Future work:
  - ▶ Compute  $\Delta$  functions for real-world architectures.
  - ▶ Perform WCET analysis based on that basis.
  - ▶ Explore further trade-offs between efficiency and precision.