Precise Worst-Case Execution Time Analysis for Processors with Timing Anomalies

Raimund KIRNER
Vienna University of Technology

ARTIST Design, Brussels, 21.01.2009

Searching for Simple HW Models

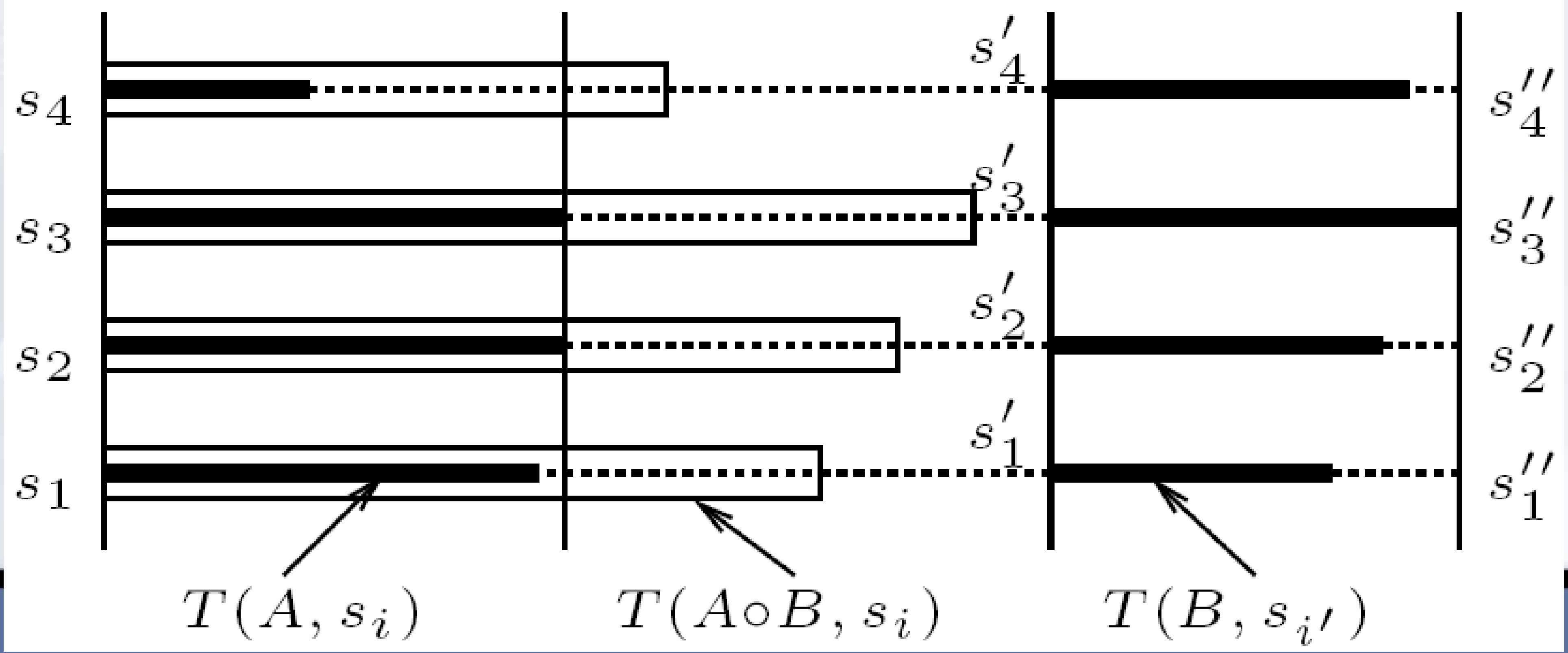
- **Challenge:** static WCET analysis for modern processors having complicated caches, pipelines, and other dynamic features results in large and complex timing models
- **Techniques to simplify HW models:**
  - safe abstraction: over-approximation by reducing granularity of model → behavior of abstract model subsumes multiple concrete behaviors, includes the real one → **safe by construction**
  - simplification: approximation by assuming the absence of certain execution scenarios (e.g., reducing transitions in state-transition system) → **needs proof!!**
    - Example: assumption that guessing cache a miss always results into global WCET

Basic Concepts

- Def: TRDCS (timing-relevant dynamic computer state) contains all memory elements in the target hardware whose content influences the timing.
- $T(I,s)$: the execution time for instruction sequence I with initial state s.
- $T_{hwA}(I,a)$: total latency of hardware component hw_A with instruction sequence I.
- $\Delta(I,s,s') = T(I,s) - T(I,s')$
- IN_I: the set of reachable states at instruction sequence I.
- $IN_{I,max}$: the set of reachable states at instruction sequence I where $T(I,s)$ is maximal ($s \in IN_I$).

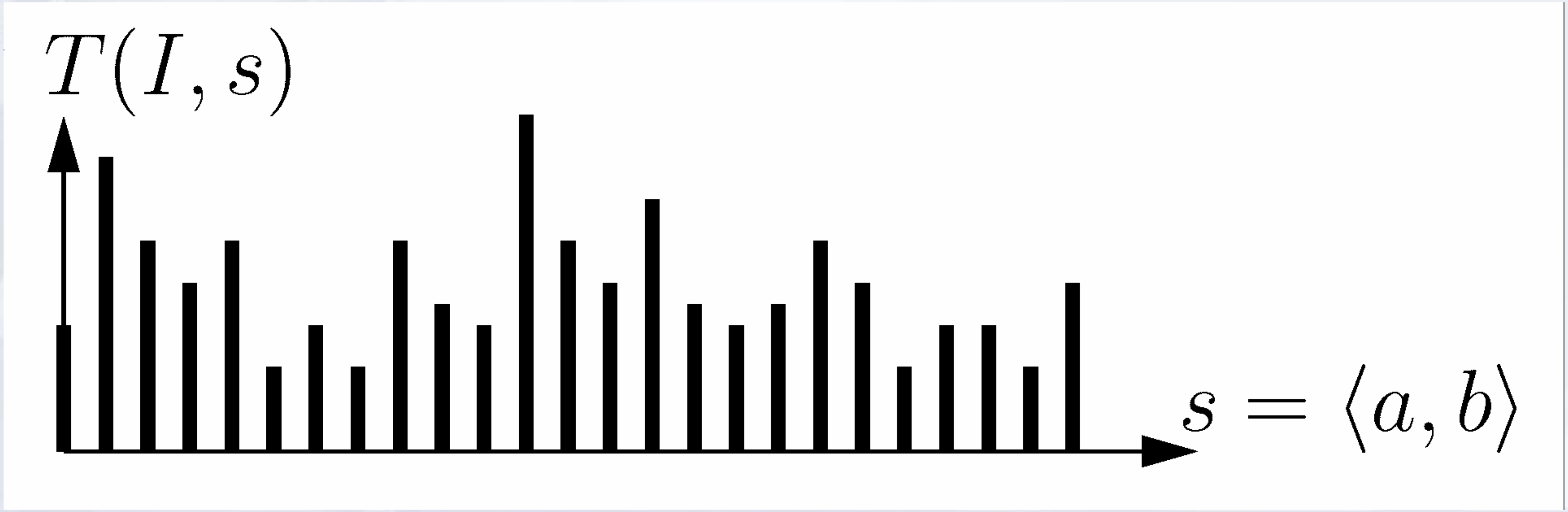
State Space Reduction – Series Decomposition

- Find the WCET of the composed instruction sequence I = A ° B:



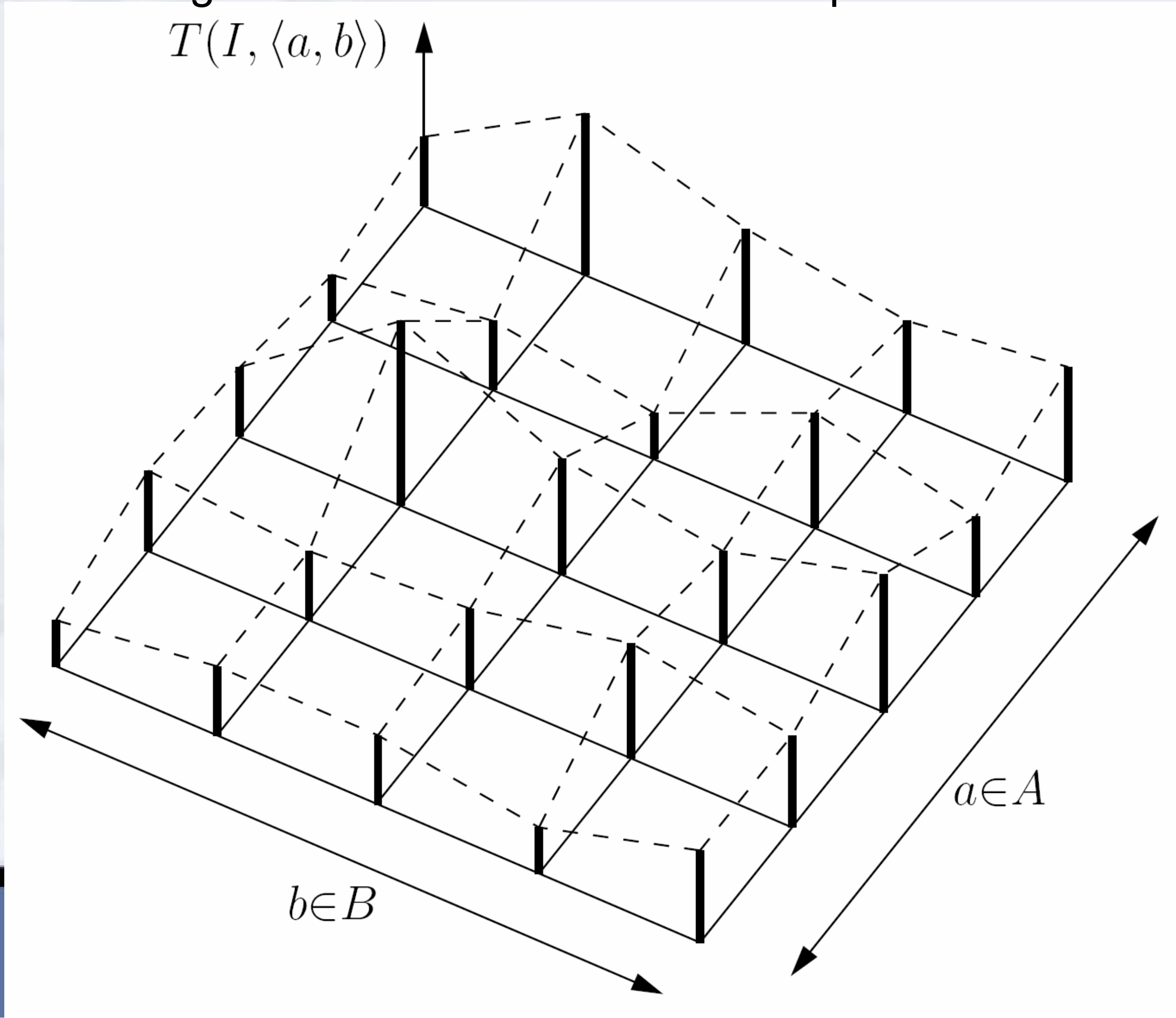
State Space Reduction – Parallel Decomposition

- The TRDCS of the hardware may be partitioned into A and B to analyze the timing of hardware component hw_A in isolation of hardware component hw_B
- Execution time of instruction sequence *I* depending on TRDCS *s*:



State Space Reduction – Parallel Decomposition

- Partitioning the TRDCS between HW component A and HW component B:



Challenge for Composition Techniques: Timing Anomalies (TAs)

- Timing anomalies are a violation of continuity properties
- Processor behavior analysis is much more complex in case of TAs.

Timing Anomalies – Definition by Lundqvist

- Terms
  - Δt … Latency variation of first instruction of instruction sequence S
  - ΔC … execution time change of whole instruction sequence S
- Timing Anomaly: one of the two following conditions must hold

  TA1: $\Delta t > 0: \rightarrow (\Delta C < 0)$ TA2: $\Delta t > 0: \rightarrow (\Delta C > \Delta t)$

  $\Delta t < 0: \rightarrow (\Delta C > 0)$ $\Delta t < 0: \rightarrow (\Delta C < \Delta t)$

Timing Anomalies – Definition by Reineke et al.

- Definition of TA is based on the hardware at micro-instruction level (modeled as state transition system)
- A timing anomaly occurs if the path taken for the global WCET does not go through one of the local worst-case paths.
- This definition of TA (based on the local worst-case paths) includes less behavior patterns than the original definition by Lundqvist!

Timing Anomalies – Definition by Kirner et al.

- Definition of TA is based on the state (TRDCS) and instruction sequence $I=A\circ B$
- Serial timing anomalies (generalization of Lundqvist's TA):
  - TA-S-I (series inversion):
    $\exists s,s'\in IN_I.\ \Delta(A,s,s') > 0 \wedge \Delta(A\circ B,s,s') < 0$
  - TA-S-A (series amplification):
    $\exists s,s'\in IN_I.\ 0 < \Delta(A,s,s') < \Delta(A\circ B,s,s')$
- Serial timing anomalies (restricted to local maxima):
  - TA-S-I (series inversion):
    $\exists s\in IN_I,\ \forall s'\in IN_{I,max}.\ \Delta(A,s,s') > 0 \wedge \Delta(A\circ B,s,s') < 0$
  - TA-S-A (series amplification):
    $\exists s\in IN_I,\ \forall s'\in IN_{I,max}.\ 0 < \Delta(A,s,s') < \Delta(A\circ B,s,s')$

Timing Anomalies – Definition by Kirner et al.

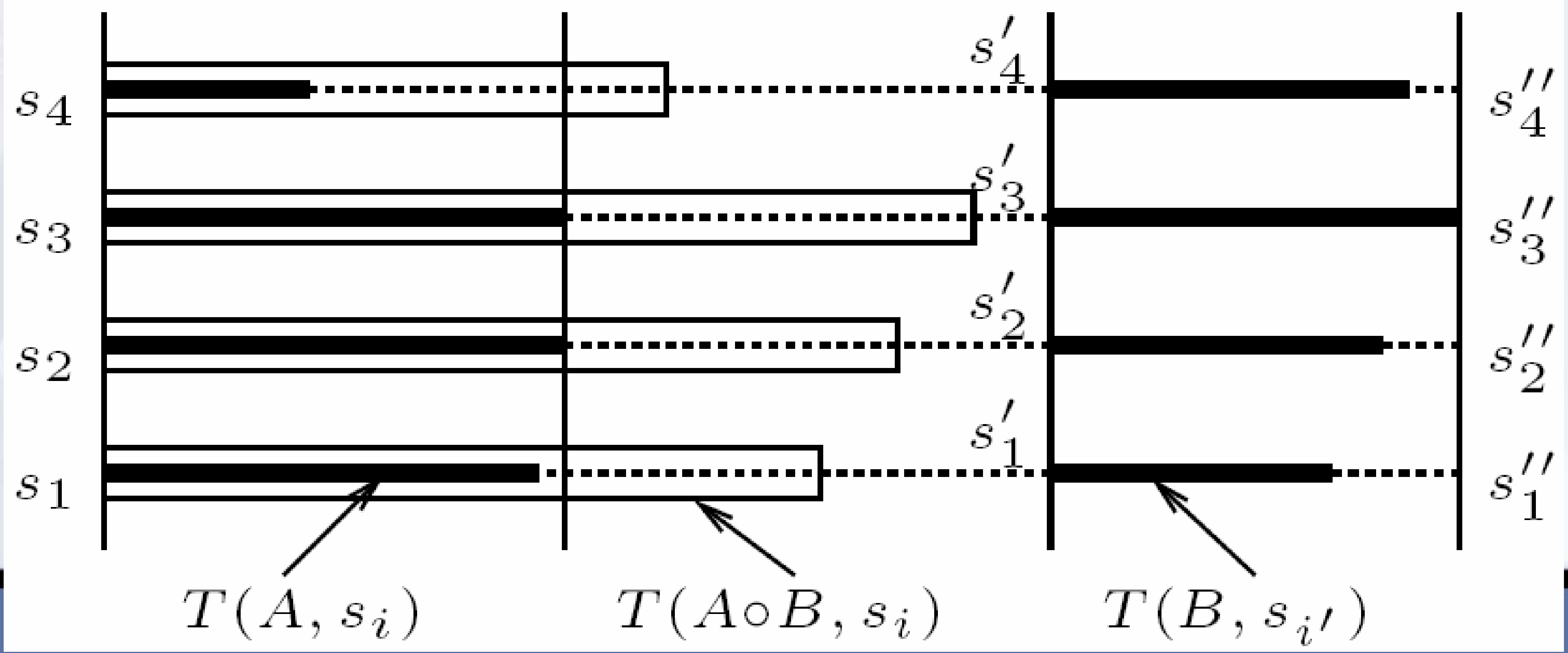
- Definition of TA is based on the state (TRDCS) $S = A \times B$ and instruction sequence I
- Parallel timing anomalies:
  - TA-P-I (parallel inversion):
    $\exists a,a' \in IN_{A,I},\ \exists b \in IN_{B,I}.$
    $\Delta_{hwA}(I,a,a') > 0\ \wedge\ \Delta(I,\langle a,b\rangle, \langle a',b\rangle) < 0$
  - TA-P-A (parallel amplification):
    $\exists a,a' \in IN_{A,I},\ \exists b \in IN_{B,I}.$
    $0 < \Delta_{hwA}(I,a,a') > 0\ < \Delta(I,\langle a,b\rangle, \langle a',b\rangle)$
- Parallel timing anomalies (restricted to local maxima):
  - same definition as above, but again use $IN_{A,I,max}$ and $IN_{A,I,max}$ as states.

Consequences of Timing Anomalies

- Knowledge of the execution history required to tightly bound the execution time
- Without knowledge of the execution history (e.g., it is too complex to take into account):
  - pessimistic overestimations in case of safe abstractions
  - potentially unsafe approximations in case of simplifications

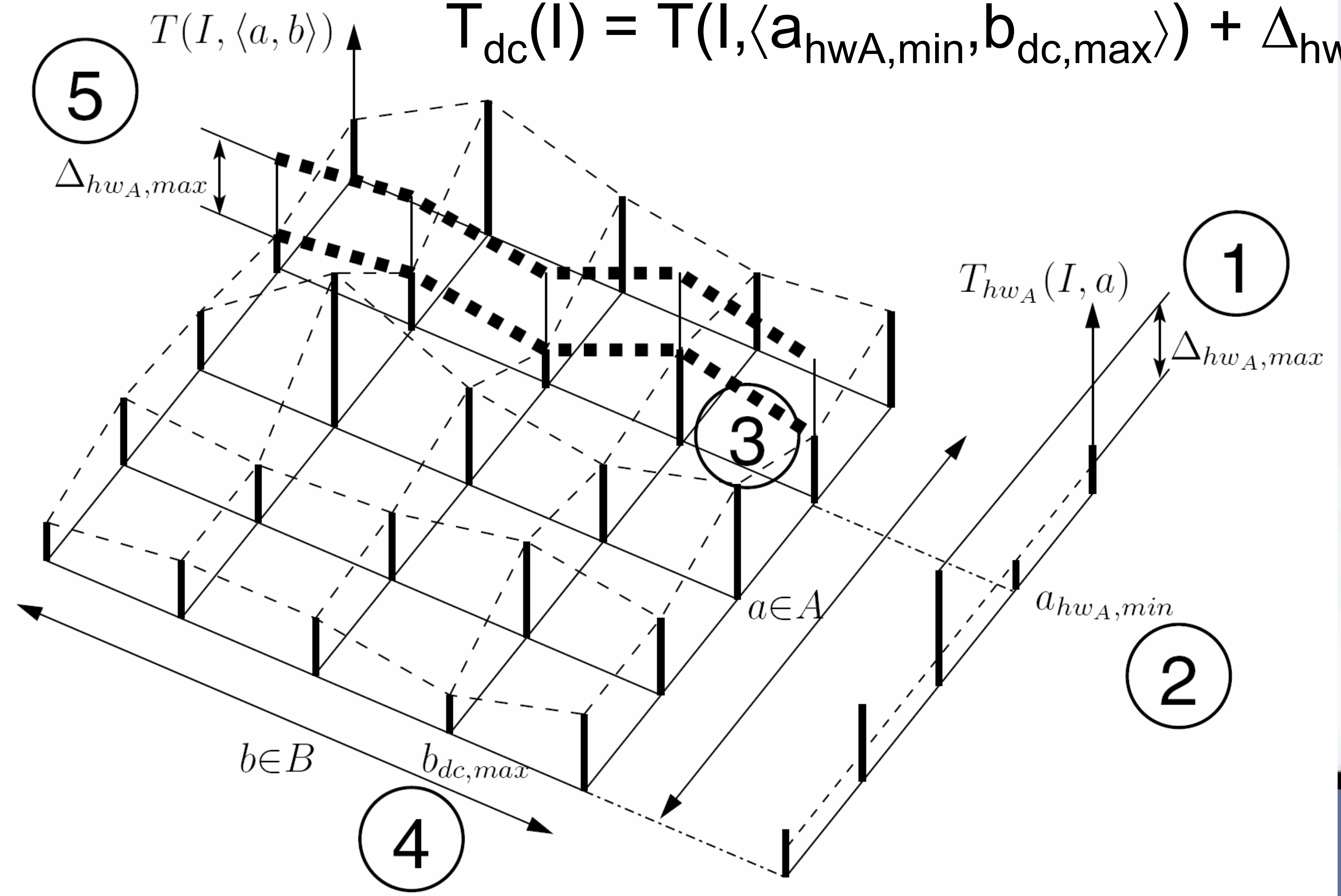
Series-Composition of TRDCS

$$T_{sc}(A \circ B) = \max T(A \circ B, s) \mid s \in IN_{l,max}$$



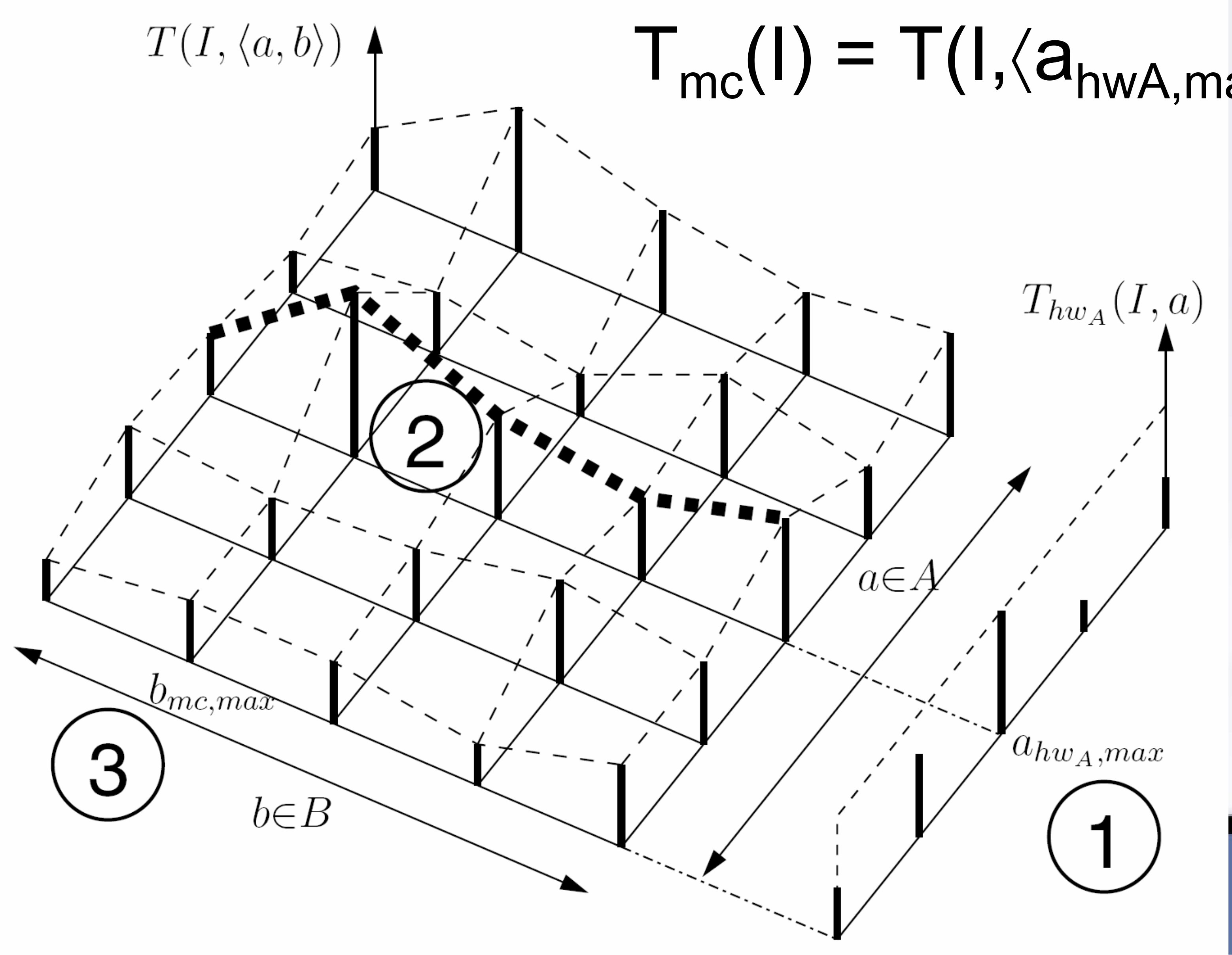
Delta-Composition of TRDCS

$$T_{dc}(I) = T(I,\langle a_{hwA,min},b_{dc,max}\rangle) + \Delta_{hwA,max}$$



Max-Composition of TRDCS

$T_{mc}(I) = T(I,\langle a_{hwA,max}, b_{mc,max}\rangle)$



Summary of Composition Techniques

- Series Composition:
  - only type TA-S-A: series composition gives safe bounds
  - only type TA-S-I: no safe composition technique known!
- Parallel Composition:
  - only type TA-P-I: delta-composition provides safe bounds
  - only type TA-P-A: max-composition provides safe bounds
  - only type TA-P-EIA:
    max(T_{dc},T_{mc}) provides safe WCET bounds
  - type TA-P-CIA (coupled dual parallel TA)
    no safe composition technique known!

Precondition for Timing Anomalies

- Common to shown patterns is a changed resource allocation sequence caused by a latency variation.

Resource Allocation Criterion (RAC):
A possible resource allocation decision for a hardware model is a necessary - but not sufficient - condition for the occurrence of timing anomalies. [Wenzel, MThesis 2003]

- Consequence: Hardware without possible *resource allocation decisions* does not allow timing anomalies to occur.
- Note: Occurrence of timing anomalies depends on hardware features as well as code structure.

Open Challenges

- Better understanding about the origins of timing anomalies:
  - Have a reliable indicator to detect potential TAs in a given hardware
    (the reliability of the RAC is not satisfying)
  - Construction of predictable HW:
    how to ensure that it is free of TAs?

Literature

- The content of the slides is mainly from

  Raimund Kirner, Albrecht Kadlec, and Peter Puschner; *Worst-Case Execution Time Analysis for Processors showing Timing Anomalies*; Research Report 01/2009, Technische Universität Wien, Institut für Technische Informatik, Treitlstraße 1-3/182-1, 1040 Vienna, Austria http://ti.tuwien.ac.at/rts/

http://www.wcet.at