Real-Time Systems

Anno accademico 2009/10
Laurea magistrale in informatica
Dipartimento di Matematica Pura e Applicata
Università di Padova
Tullio Vardanega

Outline

Bibliography

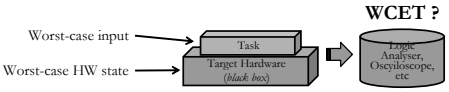
- J. Liu, "Real-Time Systems", Prentice Hall, 2000
- A. Burns, A. Wellings, "Concurrent and Real-Time Programming in Ada", Cambridge University Press, 2007
- A. Burns, A. Wellings, "Real Time Systems and Programming Languages: Ada 95, Real-Time Java and Real-Time C/POSIX", Addison-Wesley, 2009

8.a WCET analysis techniques

Enrico Mezzetti, emezzett@math.unipd.it

Computing the WCET – 1

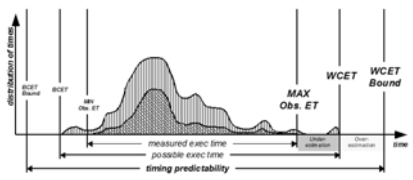
- Why not *measure* the WCET of a task on its target hardware?



- Triggering the WCET by test
  - *Worst-case input* covering all executions of a real program is intractable in practice
  - *Worst-case initial state* is difficult to determine due to complex HW features
    - Complex pipelines (out-of-order execution)
    - Caches
    - Branch predictors and other features allowing speculative execution
    - … increasingly used in modern processors

Computing the WCET – 2

- Exact WCET not generally computable (~ the *halting problem*)
- A WCET estimate or *bound* are key to predictability
  - Must be *safe* to be an upper bound to all possible executions
  - Must be *tight* to avoid costly over-dimensioning

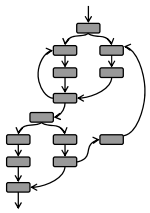


Static analysis – 1

- Analyze a program without executing it
  - On an **abstract model** of the target HW
  - With the actual executable
  - To determine safe and tight WCET bounds
- Execution time depends on execution path and HW
  - *High-level analysis* addresses the program behavior
    - Path analysis
  - *Low-level analysis* determines the timing behavior of individual instructions
    - Not constant due to complex HW
    - Must be aware of inner working of HW (pipeline, caches, etc.)

Static analysis – 2

- **High-level analysis**
  - Analyzes all possible execution paths of the program
    - Builds the Control-flow Graph (CFG)
    - Superset of all possible execution paths
    - *Basic block* is the unit of analysis
      - Sequence of instructions with no branches/loops
  - Issues related to path analysis
    - *Input-data dependency*
    - *Infeasible paths*
    - *Loop bounds* (and recursion depth)
    - *Dynamic calls* (through pointers)



Static analysis – 3

- **High-level analysis** (cont'd)
  - Several techniques are used
    - *Control-flow analysis* to compute execution paths
    - *Data-flow analysis* to find loop bounds
    - *Value analysis* to resolve memory accesses
    - CFG unit: *basic blocks*
  - Information automatically gathered is not exhaustive
    - *User annotation* of *flow-facts* is needed
      - To facilitate detection of *infeasible paths*
      - To refine *loop bounds*
      - To define *frequency relations* between basic blocks
      - To specify the target of *dynamic calls* and referenced *memory addresses*

Static analysis – 4

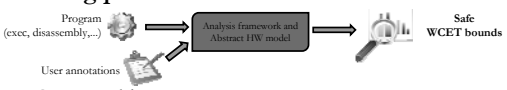
- **Low-level analysis**
  - Requires abstract modeling all hardware features
    - Processor, memory subsystem, buses, peripherals…
    - *Conservative* : never underestimate the concrete timing
    - All possible HW states should be accounted for
  - Issues related to HW modeling
    - *Precise modeling* of complex hardware is difficult
      - Inherent complexity (e.g. out-of-order pipelines)
      - Lack of comprehensive information (copyrights, patents, …)
      - Differences between specification and implementation (!)
    - *Representation* of all HW states is computationally infeasible

Static analysis – 5

- **Low-level analysis** (cont'd)
  - Concrete HW states
    - Determined by the execution history
    - Cannot compute all HW states for all possible executions
      - Invariant HW states are grouped into *execution contexts*
      - *Conservative overestimation* to reduce the research space
  - Applied techniques
    - *Abstract interpretation*
      - Computes *abstract states* and specific operators in the abstract domain
        - *Update function* to update the abstract state along the exec path
        - *Join function* to merge control-flow after a branch
    - Some techniques are specific to each HW feature

Static analysis – 6

- **The big picture**



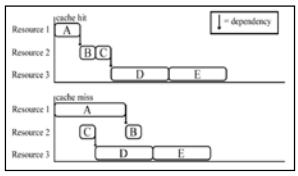
  - Open problems
    - Can we always trust HW modeling?
    - How much overestimation do we incur?
      - Inclusion of infeasible paths
      - Overestimation intrinsic in abstract state computation
    - Weaknesses of user annotations
      - Labor intensive and error prone

Static analysis – 7

- Also safeness can be hampered
  - **Local** worst case does not always lead to **global** worst case
  - Timing anomalies
    - Complex hardware architectures (e.g. out-of-order pipelines)
    - Even improper design choices (e.g. cache replacement policies)
    - *Counter-intuitive* timing behavior
    - Faster execution of a single instruction entails *long-term* negative effects
  - Very difficult to account for in static analysis

Scheduling anomaly: example

- Some dependence between instructions
- Shared resources (e.g. pipeline stages)



- Faster execution of A leads to a worse overall execution because of the order in which instructions are executed

Hybrid analysis (measurement based) – 1

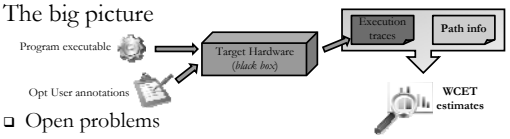
- To obtain *realistic* (less pessimistic) WCET estimates
  - On the real target processor
  - On the final executable
  - Safeness not guaranteed (!)
- Hybrid approaches exploit
  - Measures *basic blocks* on the real HW
    - Avoids pessimism from abstract modeling
  - Static analysis techniques to combine the obtained measures
    - Knowledge of the program execution paths

Hybrid analysis (measurement based) – 2

- Approaches to collect timing information
  - *Software instrumentation*
    - The program is augmented with instrumentation code
    - Instrumentation effects the timing behavior of the program
      - A.k.a.: *probe effect*
      - Cannot be simply removed at end of analysis
  - *Hardware instrumentation*
    - Depends on specialized HW features (e.g., debug interface)
- Confidence in the results contingent on the coverage of the executions
  - Exposed to the same problems as static analysis and measurement

Hybrid analysis (measurement based) – 3

- The big picture



  - Open problems
    - Can we trust the resulting estimates?
      - Contingent on worst-case input and worst-case HW state
      - Consideration of infeasible paths
    - Needs the real execution environment or an identical copy
      - Serious cost impact and inherent difficulty of exactness

Example tool: **a³** and aiT

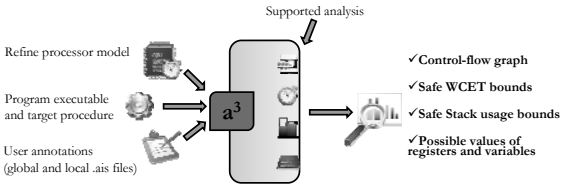
- **a³** stands for AbsInt Advanced Analyzer
  - Industrial-level commercial tool
    - Airbus, Daimler, Mitsubishi, Volkswagen, etc.
  - Developed by AbsInt GmbH (absint.com)
    - Based on *abstract interpretation*
    - Scientific basis developed at Saarlanden Universiteit, Saarbruecken, Germany
  - Supports various forms of static analysis
    - Stack usage analysis
    - Value analysis
    - WCET analysis – the **aiT** tool proper

WCET analysis with **a³**-aiT – 1

- A static analysis tool
  - Uses an abstract processor model
    - Specific to each processor
    - Different versions of the same tool are needed for different processors
  - Almost everything is modeled by *abstract interpretation*
    - *Loop analysis* : interval analysis and pattern matching
    - *Value analysis* : interval analysis
    - *Pipeline analysis* : integrates *cache analysis* by abstract interpretation
  - Results combined with path information in an ILP problem
    - Solution is the WCET bound

WCET analysis with **a³**-aiT – 2

- Overview of a³



WCET analysis with **a³**-aiT – 3

- The **a³-Leon2** tool
  - Targets the LEON2 processor family
    - Aeroflex-Gaisler (gaisler.com)
  - Configurable to apply to a specific processor
    - *Clock rate*
    - *FPU*
    - *Memory areas and relative access latency*
    - *Caches (size, associativity, line size,…)*
  - LEON2 is a quite simple processor
    - 5-stage pipeline
    - No branch predictors (delay slot)

Summary

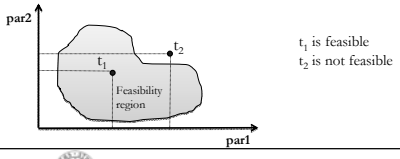
- Computing the WCET
- Static analysis
  - High-level analysis
  - Low-level analysis
- Hybrid analysis (measurement-based)
- Example tool and demo

8.b Feasibility analysis techniques

Marco Panunzio, panunzio@math.unipd.it

Feasibility region

- Geometrical region that represents the set of feasible systems (w.r.t. their workload model parameters)
  - N-dimensional space with N-parameter analysis
  - Function of the timing parameters
  - Specific to the scheduling policy in force

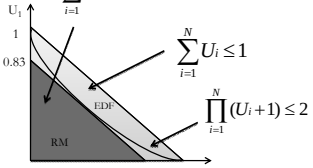


t_1 is feasible
t_2 is not feasible

Advanced utilization tests

- *Hyperbolic bound* improves Liu & Layland utilization test
  - For systems with periodic tasks under FPS and RM priority assignment
  - E. Bini, G. Buttazzo, and G. Buttazzo: "*A Hyperbolic Bound for the Rate Monotonic Algorithm*". Proceedings of the 13th Euromicro Conference on Real-Time Systems, 2001

$$\sum_{i=1}^{N} U_i \le N(2^{1/N} - 1)$$



Fine-grained response time analysis

$$R_i^{n+1} = B_i + CS1 + C_i + \sum_{j \in hp(i)} \left\lceil \frac{R_i^n + J_j^A}{T_j} \right\rceil (CS1 + C_j + TS + CS2) + I_{clock}^{R_i^n} + I_{extInt}^{R_i^n}$$

Blocking time (resource access protocol or *kernel*)

"In" context switch

"Activation" jitter

"Out" context switch

Interference from the clock

Interference from interrupts

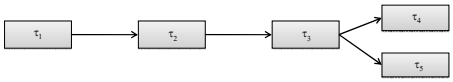
Time to issue a *suspension* call

$$R_i = B_i + CS1 + C_i$$

$$R_i = R_i^n + J^W \longleftarrow \text{"Wake-up" jitter}$$

Transactions – 1

- Considers causal relations between activities
  - Introduces information relevant to analysis that is not captured by classical workload models
    - Dependencies in the activation of jobs

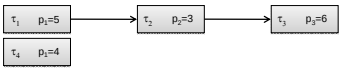


  - Originally introduced for the analysis of distributed systems
    - Also useful for the analysis of single-node "collaboration patterns"

Transactions – 2

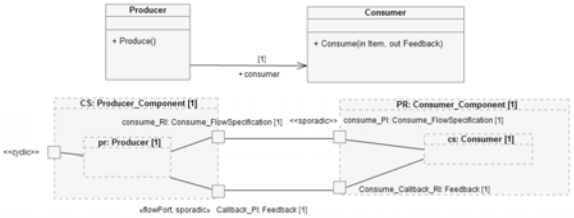
- Two (main) kinds of dependence
  - Direct precedence relation (e.g., producer-consumer)
    - τ_2 cannot proceed until τ_1 completes

  - Indirect priority relation
    - τ_4 does not suffer interference from τ_3 (under FPS and synchronous release of τ_1 and τ_4)

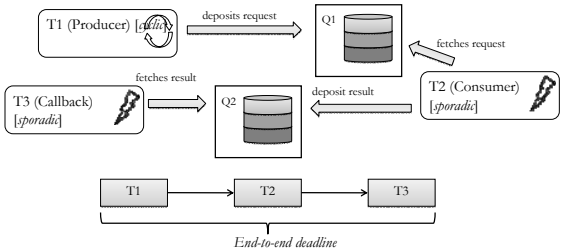


Example – 1

- A "*callback pattern*" to permit **in out** interactions between tasks in Ravenscar systems



Example – 2

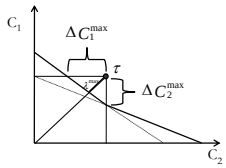


End-to-end deadline

The feasibility of the *end-to-end response time* against this deadline is the important information (!)

Sensitivity analysis – 1

- Investigates the changes in a given system that
  - Improve the fit of an already feasible system
  - Make feasible an infeasible system



τ	Position of the system in the feasibility region
ΔC_1^{max}	Maximum feasible variation for the WCET of t_1 (negative in the example)
ΔC_2^{max}	Maximum feasible variation for the WCET of t_2 (negative in the example)

Sensitivity analysis – 2

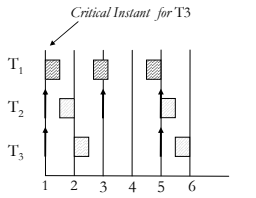
- Major computation complexity
- Theory still under development
  - Does not account for shared resources, multi-node systems, partitioned systems
- High potential
  - To explore solution space in the *dimensioning* phase of design
    - Presently only applicable to period/MIAT and WCET
  - To study the consequences of changes to timing parameters
    - To permit the inclusion of better functional value in the system
    - To renegotiate timing (or functional) parameters

MAST

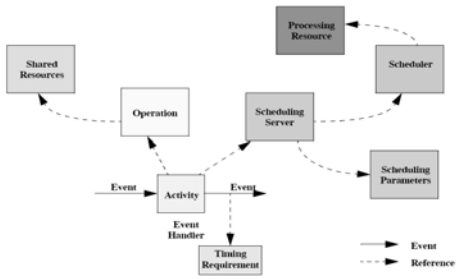
- Modeling and Analysis Suite for Real-Time Systems (MAST)
  - Developed at University of Cantabria, Spain
  - Open source
  - Implements several analysis techniques
    - To analyze uni-processor or multi-processor systems
    - Under Fixed-priority scheduling or EDF scheduling
  - http://mast.unican.es

Classic workload model

$\mathbf{T_1}$ (Sporadic) MIAT=1750 WCET=500
$\mathbf{T_2}$ (Cyclic) T=2000 WCET=500
$\mathbf{T_3}$ (Cyclic) T=2000 WCET=500

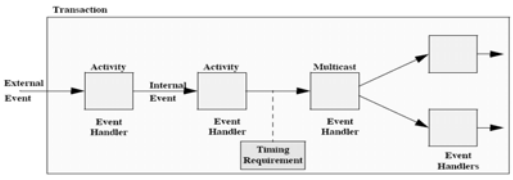


MAST – real-time model

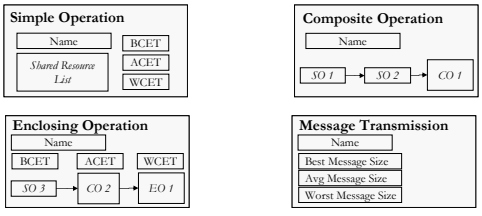


MAST – transaction

- To model causal relations between activities
  - Triggered by external events
    - Periodic, sporadic, aperiodic, etc…

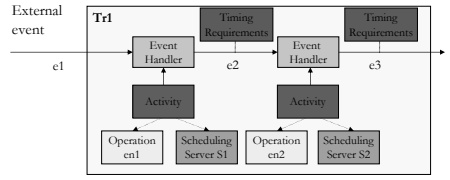


MAST – operations

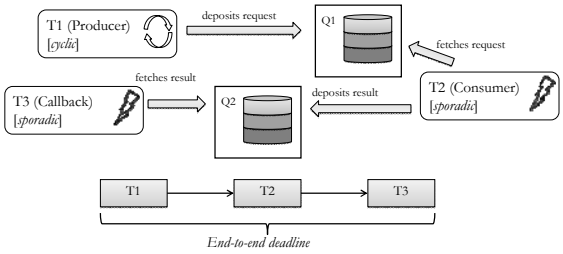


- The real-time model includes the description of all the operations in the system

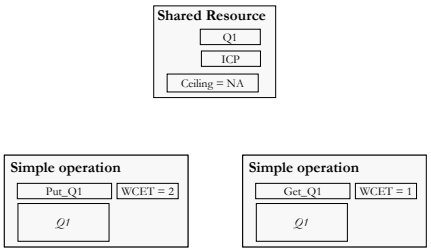
MAST – creation of a transaction



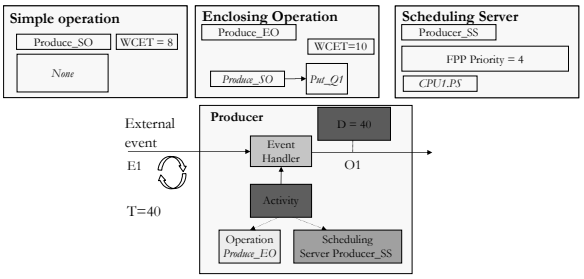
Example: Ravenscar callback



MAST – shared resources



MAST – modeling tasks



Example: timing attributes

Producer [1] (C) T_1=40 C_1=10 p_1=4

Consumer [2] (S) T_2=40 C_2=10 p_2=2

Callback [3] (S) T_3=40 C_3=5 p_3=5

Q1 Ceiling=4

Q2 Ceiling=5

Example: RTA results

Producer [1] (C) T_1=40 C_1=10 p_1=4

Consumer [2] (S) T_2=40 C_2=10 p_2=2

Callback [3] (S) T_3=40 C_3=5 p_3=5

Q1 Ceiling=4

Q2 Ceiling=5

⟹ B_1=2 B_2=0 B_3=2

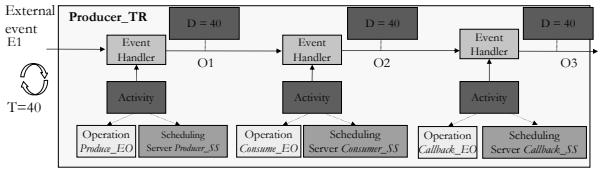
Classic RTA

R_1 = 17

R_2 = 25

R_3 = 7

Example: transaction



Example: end-to-end analysis

Producer [1] (C) T_1=40 C_1=10 p_1=4

Consumer [2] (S) T_2=40 C_2=10 p_2=2

Callback [3] (S) T_3=40 C_3=5 p_3=5

Q1 Ceiling=4

Q2 Ceiling=5

⇒ B_1=2 B_2=0 B_3=2

Classic RTA

R_1 = 17

R_2 = 25

R_3 = 7

Precedence and offset-based

R_1 (Tr) = 12

R_2 (Tr) = 20

R_3 (Tr) = 27

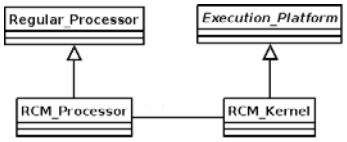
⇐ ***Response time* relative to the beginning of the transaction!**

MAST+

- Developed from MAST 1.3.6
- Extended real-time model and additional analysis techniques
  - Ravenscar systems
    - Uni-processor and multi-processor systems
      - Holistic analysis
- Output in XML

MAST+: extended real-time model

- Introduces the concept of "Execution platform"
  - To model Ravenscar-compliant execution platforms
    - By characterizing the timing cost of kernel operation



MAST+: implemented metrics

- ClockPeriod, PeriodicClockHandler, DemandedClockHandler
  - Overhead due to the Interrupt Service Routine (ISR) to serve the *hardware clock* and the *interval timer*
- Ready, Select, Switch
  - Context switch overhead
- SuspensionCall, WaitCall
  - Overhead due to task suspension
- KernelLongestCriticalSection
  - Maximum time duration in which the kernel disables interrupts

Summary

- Feasibility region
- Advanced utilization tests
- Fine-grained response time analysis
- Transactions
- Sensitivity analysis
- Example tool (MAST) and demo