Scalable (yet Precise) Timing Analysis

Wang Yi
Uppsala University
ETAPS/TACAS 2015

Can $P$ finish its execution within $D$ sec’s?
Joint work with

Nan Guan  Martin Stigge  Pontus Ekberg  Jakaria Abdullah
Embedded Systems

Timing Analysis

- What is the maximal delay at each component?
- What is the maximal end-to-end delay?

Example size of real applications:
- 80-100 tasks (Ind. Robots, ABB)
- 30-50 tasks (FMS, THALES)
The 1st TACAS, Aarhus, April 1995

UPPAAL

Johan Bengtsson
Kim Larsen
Fredrik Larsson
Paul Pettersson
Wang Yi

Photo: Kim Larsen, Aalborg Univ.
10 years ago ... ... my last TACAS paper:


2004

Mr. Industry

I can’t solve the problem, neither can all these famous Model-Checkers
... 10 years later, my latest TACAS paper:

Nan Guan, Yue Tang, Jakaria Abdullah, Martin Stigge, Wang Yi:
Scalable Timing Analysis with Refinement. TACAS 2015:3-18

The State-of-the-Practice in 2015

Have you solved the problem? I need a solution for these companies ...
Timed Systems

- **UPPAAL**, **UPPAAL-Tiga** (FUSC): Timed automata (Uppsala Univ., Aalborg Univ.)
  - manipulate **UPPAAL** XML (GPL-3, Python)
  - Yggdrasil (? ,?): UML (subset) -> **Uppaal**, intended for test generation (Aalborg Univ.)
- **METAMOC** (GPL-3, Python): WCET Analysis of ARM Processors using Real-Time model checking (Aalborg Univ.)
- **SARTS** (? , Java): Model Based Schedulability Analysis of Real-Time Systems (Aalborg Univ.)
- **OPAAL** (GPL-3, Python): distributed/parallel (discrete time) model checker for networks of timed automata using MPI
- **ECDAR** (FUSC): timed interface theory (Aalborg, INRIA, ITU)
- **PyECDAR** (GPL-2, Python): solve timed games based on timed automata models (ITU)
- **IOA** (MIT, Java): I/O automata formal language (MIT)
- **TEMPo** (closed, Java): Formal language for modeling distributed systems w/ w/o timing constraints as collections of interacting state machines, i.e., timed input/output automata (TIOA) (UIUC)
  - Tempo2HSal (? , Python): Tempo (.tioa) -> HSal (.hsal) translator (SRI)
- **ATAS** (GPL-3, Python): Alternating 1-clock (full-reachable) Timed Automata Solver
- **PPL binding** (GPL-2, Python): for Parma Polyhedral Lib features some specific methods for Timed Automata analysis
- **MCPTA** (FUSC, ?): Probabilistic Timed Automata model checker for MoDeST | UPPAAL | PRISM - maps on PRISM (Saarland Univ.)
- **SAAtRE** (?): Abstraction refinement model checker for Timed Automata based on extended SAT-solving, **UPPAAL**-like input format (Univ. Hamburg, CWI)
- **Fortuna** (GPL-3, C++/Eclipse): MC priced probabilistic timed automata (PPTAs) (Univ. Twente)
- **COSPAN** (? ,?): Automata-theoretic verification of coordinating processes with timing constraints (UPenn)
- **Romeo**: timed Petri nets (IRCCyN)
- **ExSched**: develop operating system schedulers for VxWorks and Linux w/o modifying the underlying kernel ([Mardalen Institute](http://www.es.mdh.se/staff/197-Mikael__berg))
- **RTComposer** (Java): classes and utilities for predictable real-time scheduling (BenGurion, UPenn)
- **ASTRAL**: MC of real-time systems (UCSB)
- **PAT** (? , C#): simulator, MC, refinement checker for concurrent and RT systems (Nanyang Tech. Univ.)
- **HCMC** (? , C++): Compositional model checking for real-time systems (ENS-Cachan)

Could these tools solve this problem?

![Graph showing the increase in the number of model checkers over time](image)
State-of-the-Practice

Mr. Industry

The tool never terminates ... ...

Mr. ModelChecker

Be patient!
The tool should be able to solve ALL problems 😊
State-of-the-Practice

Mr. Industry

Mr. ModelChecker

No No No!
Last night, it ran out of Memory 😞
The Analyzable Zone of "Models/Problems"

- **Decidable**
- **Analyzable**
- **Tractable (pseudo-p)**

**“Difficulty”**

- **Scalable**
- **Efficient**
- **Run & Pray**

**“Needed” for Interesting features**

**“Expressiveness”**

- **Ambition**
- **Precision**
- **RTAS**
- **ECRTS**
- **RTSS**
- **TACAS**
- **CAV**
- **ETAPS**

Tractable (pseudo-p) Analyzable Needed for Interesting features

Run & Pray
Timing Analysis

Sequential Case (WCET Analysis)

Concurrent Case (Response Time Analysis)

Non-deterministic releases
The WCET Analysis Problem

- A fundamental problem for embedded systems design
  - Worst-Case Execution Time (WCET) analysis
- Challenges ("termination" doesn’t make the problem easy)
  - "too many input" ➔ too many execution paths (difficult to find the worst-case)
  - hardware features e.g. caches ("the HW state" results in different execution times)
WCET Analysis

• Path Analysis
  – which path leads to the WCET?
  – well-known technique by ILP

  – need to know the timing delay of each instruction

• Architecture Analysis

  – Cache Analysis:
    Is a memory access hit or miss?

  – other factors like pipeline ...
WCET Analysis

• Path Analysis
  – which path leads to the WCET?
  – well-known technique by ILP
  – need to know the timing delay of each instruction

• Architecture Analysis [Survey 2015 wang et al]
  – Cache Analysis:
    Is a memory access hit or miss?
    • AH: always hit
    • FM: first miss, then always hit
    • AM: always miss
    • NC: not classified
  – other factors like pipeline ...
WCET Analysis

• Path Analysis
  – which path leads to the WCET?
  – well-known technique by ILP
  – need to know the timing delay of each instruction

• Architecture Analysis  [Survey 2015 wang et al]
  – Cache Analysis:
    Is a memory access hit or miss?
    • AH: always hit
    • FM: first miss, then always hit
    • AM: always miss
    • NC: not classified → always miss
  – other factors like pipeline ...

[aiT tool from AbsInt]
Wilhelm et al
Precision >> 95%
Timing Analysis

Sequential Case (WCET Analysis)

- Assume the WCET of each task is given (resource budget)
- How to estimate the Worst-Case Response Time of a task?

Concurrent Case (Response Time Analysis)

Non-deterministic releases

WCRT = WCET
Modeling for (System-Level) Timing Analysis

- The event arrival patterns e.g. using timed automata
- Synchronization between components,
- Resource arbitration, protocols and scheduling algorithms
- The resource demands or budget e.g. the WCET
- The timing constraints e.g. deadlines
Timed Models

- Timed Petri Nets, early 80s
  - Time Intervals over transition firing
- Process Algebras, 80s – 90s
  - Delays + untimed models e.g. Milner’s CCS
- Timed Automata, early 90s
  - finite automata + clock constraints
- Real-Time Task Models since 70s
  - Layland and Liu’s periodic tasks, 1973
  - The variants of L&L model [RTSS community]
- Real-Time Programming e.g. Ada 83
  - Delay, Tasking, Run-Time System
- Timed Game ... Learning etc ... yesterday tool demo
Liu and Layland’s Model, 1973

A system is a set of periodic tasks each described by two numbers:
- **e**: the worst case execution time (WCET)
- **P**: the minimum inter-release delay (implicit deadline)

- The workload of each task: \( e/p \)
- The system workload or utilization: \( U = \sum \frac{e_i}{p_i} \)

**Feasibility (i.e. EDF-schedulability):** no deadline miss if \( U \leq 1 \)

**Fixed-priority Schedulability:** no deadline miss if \( U \leq n(2^{1/n} - 1) \)

The well-known Rate-Monotonic Scheduling
Hierarchy of Models

Feasibility test

difficult

efficient

Expressiveness

high

low

Strongly (co)NP-hard
Pseudo-Polynomial

two integers
L&L
implicit deadline
ALL these models are “tractable” but have limited expressiveness
Example: Tree/DAG-task model

Restrictions of Non-Cyclic RRT

- Tasks are still *recurrent*
  - Always revisit source $J_1$
  - *No cycles allowed!*

- Consequences:
  - No *local loops*
  - *Not compositional* (for modes etc.)
Restrictions of Tree/DAG model

- Tasks are still *recurrent*
  - Always revisit source $J_1$
  - *No cycles allowed!*

Consequences:

- No *local loops*
Restrictions of Tree/DAG model

- Tasks are still **recurrent**
  - Always revisit source $J_1$
  - *No cycles allowed!*

Consequences:
- No **local loops**

- Not **composition**
  (for modes etc.)
Further extension without crossing the “tractable” borderline?
The Digraph Real-Time Model (DRT)

Pairs on nodes are the WCET and deadline on the task code e.g. A has WCET 2 and relative deadline 4
Numbers on edges are the minimum inter-release delays

The WCET, deadlines and release delays should be ensured by the Ada run-time system

In Ada Tasking:

Procedure PA
    "release A"
    Delay(2);
    PC

Procedure PB
    "release B"
    Delay(25);
    PA
If "condition"
    then Delay(10); PA
    else Delay(11); PB

[Stigge et al, RTAS 2011]
DRT: Semantics  (any path of the graph is a possible behavior)

Path $\pi = (v_4)$

Demand bound: $(10, 5)$
DRT: Semantics (any path of the graph is a possible behavior)

Path $\pi = (v_4, v_2)$

Demand bound : (10, 5)
Demand bound : (28, 6)
DRT: Semantics \hspace{1cm} (any path of the graph is a possible behavior)

Path $\pi = (v_4, v_2, v_3)$

Workload: (10, 5) \hspace{1cm} Workload: (28, 6) \hspace{1cm} Demand bound : (43, 9)
Workload of a DRT

Demand Bounds Function (dbf)
A system model = a set of DRT’s modeling the components

The system workload:
Hierarchy of Models

Feasibility test

difficult

efficient

Expressiveness

high

low

- arbitrary graph
- tree
- cycle graph
- three integers
- two integers

- DRT
- RB
- GMF
- sporadic
- L&L

branching, loops, ...
branching
different job types
explicit deadline
implicit deadline
Hierarchy of Models

Feasibility test

- arbitrary graph
- tree
- cycle graph
- three integers
- two integers

Expressiveness

- DRT: branching, loops, ...
- RB: branching
- GMF: different job types
- sporadic: explicit deadline
- L&L: implicit deadline

Strongly (co)NP-hard
Pseudo-Polynomial
Complexity Result \[\text{[RTAS 2011]}\]

Theorem (S. et al., 2011)

For DRT task systems $\tau$ with a utilization bounded by any $c < 1$, feasibility can be decided in pseudo-polynomial time.

Pseudo-polynomial time = Tractable/efficient

Ideas for feasibility analysis

- Characterize the system workload ...
- If the worst-case workload is over 100%, it is over-loaded, implying deadline miss

Units of work a CPU can compute over time (100%)
How to check this?

Of course, if the **BLUE line** is always below the **RED**, the system should work well without deadline miss!
Here is the intuition why “Pseudo-P”

If the utilization (long-term rates of DRT’s) of a system is bounded by a constant $c < 1$, any deadline miss, if exists, must appear before a pseudo-polynomial upper bound:
Calculating the Bound

\[ \sum \text{dbf}_\tau(t) \]

- Linear bound for \( \text{dbf}(t) \)
  - Slope: Less than 1
- Intersection with \( t \) gives bound \( D \)
- Check only up to \( D \)

\[ \text{dbf}(t) \leq t \cdot U(\tau) + e^{sum} \]

\[ D = \frac{e^{sum}}{1 - U(\tau)} \]
A system model = a set of DRT’s modeling the components.
Evaluation: Runtime vs. Utilization

Setting:
- Randomly generated task sets
- 1-30 tasks, 5-10 vertices per task, branching degree 1-3, ...
• How about synchronization?
  – the analysis without considering synchronization is SAFE!
  – Precise analysis possible with “Combinatorial Refinement”
• How about “static priority scheduling”?
Hierarchy of Models

[Stigge/Wang, ECRTS 2012]
# Summary

<table>
<thead>
<tr>
<th>Models</th>
<th>Analysis Complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Feasibility i.e. EDF-Schedulability</td>
</tr>
<tr>
<td>General graphs (Di-graph)</td>
<td>Pseudo-P</td>
</tr>
<tr>
<td>Trees/DAGs</td>
<td>Pseudo-P</td>
</tr>
<tr>
<td>Cyclic graphs (GMF)</td>
<td>Pseudo-P</td>
</tr>
<tr>
<td>Sporadic (L&amp;L, deadline≠period)</td>
<td>Pseudo-P</td>
</tr>
<tr>
<td>L&amp;L (periodic)</td>
<td>Linear</td>
</tr>
</tbody>
</table>

For systems with utilization bounded by a constant less than 1 (or below 100%)

Otherwise Strongly coNP-complete

!! The problem open for 25 years, theoretically interesting !!

[ECRTS 2015, Ekberg and Wang]
Combinatorial Refinement

solving “Combinatorial Problems”
(for timing analysis, it works very well!)
A system model = a set of DRT’s modeling the components

This works perfectly for feasibility checking: the global worst case can be constructed from the local worst cases

The system workload:
A system model = a set of DRT’s modeling the components

In general, each component may have a set of behaviors e.g. Paths or traces
A system model = a set of DRT’s modeling the components

Often, we have to check some property guaranteed by all the combinations of individual local behaviors and thus may have to enumerate ... (combinatorial explosion)
Construct an **Abstract Tree** for each individual component.
Construct an **Abstract Tree** for each individual component

Any non-leaf node **father** should be an over-approximation of its **sons** in the sense that

\[
(... \ldots \text{father} \ldots \ldots) \text{ sat } F \Rightarrow (\ldots \ldots \text{any son} \ldots \ldots) \text{ sat } F
\]
Construct an **Abstract Tree** for each individual component

For instance, the Combination of all roots satisfies the desired property implies that all combinations of the leaves satisfy the same property.

$$(\text{roots}) \text{ sat } F \implies (\text{any leave, any leave, ... any leave}) \text{ sat } F$$
Abstract Request Functions
Abstract Request Functions

$rf(t)$

$rf_{(v_4, v_2, v_3)}$

$rf_{(v_5, v_4, v_2)}$
Abstract Request Functions

\[ rf(t) \]

\[ rf(v_4, v_2, v_3) \]

\[ rf(v_5, v_4, v_2) \]

\[ arf \]
Abstraction Tree  for each DRT

Define an *abstraction tree* per task:
- Leaves are concrete *rf*
- Each node: maximum function of child nodes
- Root is maximum of *all rf*
Abstraction Tree for each DRT

Define an abstraction tree per task:

- Leaves are concrete \( rf \)
- Each node: maximum function of child nodes
- Root is maximum of all \( rf \)
Abstraction Tree for each DRT

Define an *abstraction tree* per task:

- Leaves are concrete \( rf \)
- Each node: maximum function of child nodes
- Root is \( mrf \), maximum of *all* \( rf \)
Combinatorial Abstraction Refinement

New Algorithm:
- Test one combination of all $mrf$.
- If fp-feasible: done
- Otherwise: Replace one $mrf$ with all child nodes, get 2 new combinations to test
- Repeat until:
  - All combinations show fp-feasibility, or
  - A combination of leaves shows non-fp-feasibility
Evaluation: Runtime vs. Utilization

Comparing runtimes of
- EDF-test using dbf (pseudo-polynomial)
- SP-test based on Combinatorial Abstraction Refinement
Evaluation: Tested vs. Total Combinations

\[ 10^5 \text{ samples of single-job tests.} \]
- Executed tests: in 99.9% of all cases, less than 100
- Total combinations possible: up to \( 10^{12} \)
Conclusions

“Code is Art” – Daniel Licata

• Model is “Abstract Art”, the key for scalable and precise analysis
  – it should be as simple as possible but not simpler
  – it should be as expressive as possible but not more

• Digraph Model instead of Timed Automata?
  – Expressive enough to capture Ada tasking
  – Efficient analysis possible: Pseudo-polynomial

• Combinatorial Refinement works well for timing problems
  – In particular when local search space can be abstracted & ordered
  – other verification problems?

• Current work
  – Synchronization and resource sharing
  – Multiprocessor mapping and scheduling
  – TIMES++, a new tool based on Digraph, aiming at industrial applications