A Novel WCET Semantics of Synchronous Programs

Michael Mendler[1] Partha S Roop[2,4] Bruno Bodin[3]

Bamberg University, Germany

University of Auckland, New Zealand

University of Edinburgh, United Kingdom

Mercator Fellow, Bamberg University, Germany

SYNCHRON'16, Bamberg (Germany),
07 December 2016

Reactive Systems and Synchronous Languages

Reactive systems are expected

- To have a **short delay** of reaction,
- and to be **correct**.

Synchronous programming languages capture this behaviour:

- **formal operational or denotational models for verification**
- **unambiguous semantics-preserving compilation**.

Time matters

Synchronous programs are highly time critical.

- This problem is modeled by the Worse-Case Execution Time.
- What is the longest reaction time of the system ?
- Also known as the Worst Case **Reaction** Time.

Numerous solutions exist, but those contribution solve the WCET for platform specific cases.
We miss a generalisation that considers time-abstract executions and the nuances of the underlying execution platform from the point of view of WCET.

Our proposition

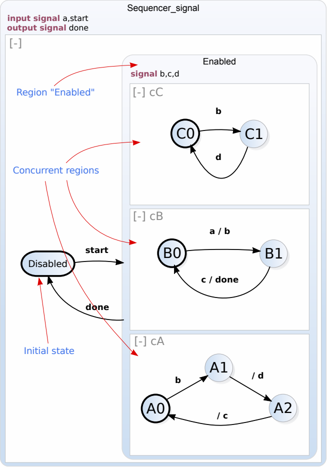
We propose a time-aware semantics for synchronous programs :

- An algebraic approach (min-max-plus)
- Based on formal power series
- Which combine
  - linear system theory for **timing**,
  - and Gödel-Dummet logic for **functional specification**,
- Compositional: can describe the WCET behaviour of individual threads, their concurrent and hierarchical compositions

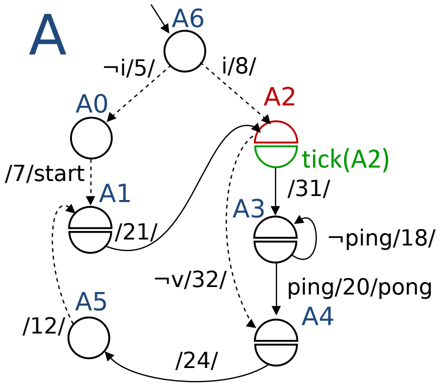
It can be used to integrate existing WCET analysis tools into functional compilation, to design new compositional timing analysis and to interface with temporal-logic based model checking.

Context

- SCCharts [vHDM+14]
- Precision timed architectures [EL07]
- Thread-interleaved pipelines

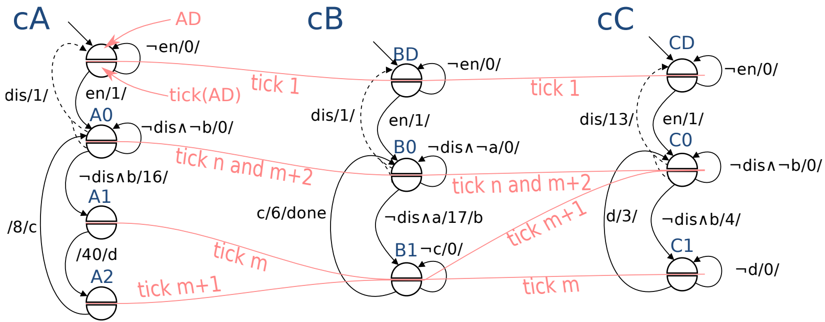


Definition



- States
- Transitions
- Ticks
- *guards*
- *signals*
- *delays*

Parallel composition



We have a **Tick Alignement Problem.**

semi-ring structure

Our timing analysis will be expressed in the discrete max-plus structured over natural numbers $(\mathbb{N}_\infty, \oplus, \odot, \mathbb{0}, \mathbb{1})$:

- $\mathbb{N}_\infty =_{df} \mathbb{N} \cup \{-\infty, +\infty\}$
- $\oplus$ stands for the maximum
- $\odot$ for the addition.
- $\mathbb{0} =_{df} -\infty$
- $\mathbb{1} =_{df} 0$,

A commutative and idempotent semi-ring on $\mathbb{N}_\infty$.

Example

$$
\begin{aligned}
4 \oplus (5 \odot 2) &= max(4, 5+2) = 7 \\
(4 \oplus 5) \odot (4 \oplus 2) &= max(4, 5) + max(4, 2) = 9
\end{aligned}
$$

Logical interpretation

The order structure $(\mathbb{N}_\infty, \leq, -\infty, +\infty)$ is a complete lattice.

- Max-plus is widely used for discrete event system analysis.
- But this lattice structure also supports **logical reasoning**

We can define a logical interpretation $(\mathbb{N}_\infty, \wedge, \vee, \supset, \bot, \top)$

- $\mathbb{N}_\infty$ measures the presence or absence of a signal
- $\bot$ or $\mathbb{0} = -\infty$ indicates that a signal is *absent*,
- $\top$ or $+\infty$ indicates *present eventually*,
- All other stabilisation values $d \in \mathbb{N}$ codify *bounded presence*

Constructive logic

We defined

- The semiring structure $(\mathbb{N}_\infty, \oplus, \odot, \mathbb{0}, \mathbb{1})$,
- and the logical interpretation $(\mathbb{N}_\infty, \wedge, \vee, \supset, \bot, \top)$

They are equally important.

- The former to calculate WCET timing
- and the latter to express signals and reaction behaviour.
- Both are overlapping with the identities $\oplus = \vee$ and $\mathbb{0} = \bot$.
- Every element in $\mathbb{N}_\infty$ is at the same time a delay value and a constructive truth value.

Formal Max-Plus Power Series

Definition (max-plus formal power series)

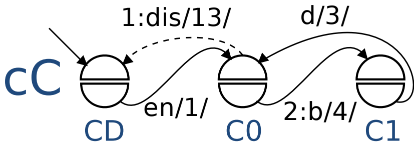
A *(max-plus) formal power series* is a (finite or ω-infinite) sequence

$$A \;=\; \bigoplus_{i \geq 0} a_i X^i \;=\; a_0 \oplus a_1 X \oplus a_2 X^2 \oplus a_3 X^3 \cdots \qquad (1)$$

with $a_i \in \mathbb{N}_\infty$ and where exponentiation is repeated multiplication, i.e., $X^0 = \mathbb{1}$ and $X^{k+1} = X\,X^k = X \odot X^k$. A formal power series stores an infinite sequence of numbers $a_0, a_1, a_2, a_3, \ldots$ as the scalar coefficients of the base polynomials X^i.

Such a power series may model an automaton's timing behaviour measuring the time cost to complete each tick or to reach a given state in given tick. However, A could also be used to model a signal.

Definition



Let us now consider the IO-BTCA cC,

$$\text{wcet}(\text{cC}) = \text{wcet}(CD) \oplus \text{wcet}(C0) \oplus \text{wcet}(C1).$$

Here is state CD:

$$\begin{aligned} \text{wcet}(CD)(0) &= \mathbb{1} \\ \text{wcet}(CD)(n+1) &= (\neg en(n+1) \wedge (0 \odot (\mathbb{1} \wedge \text{wcet}(CD)(n)))) \\ &\quad \oplus (dis(n+1) \wedge (13 \odot \text{wcet}(C0)(n+1))) \end{aligned}$$

The cost series $\mathrm{wcet}(\mathrm{En}) = \bigoplus_{i \geq 0} \mathrm{wcet}(\mathrm{En})(i)\, X^i$ is the parallel composition (tick-wise addition) of the constituent automata's tick cost series,

$$\mathrm{wcet}(\mathrm{En}) \quad = \quad \mathrm{wcet}(\mathrm{hC}) \parallel \mathrm{wcet}(\mathrm{cA}) \parallel \mathrm{wcet}(\mathrm{cB}) \parallel \mathrm{wcet}(\mathrm{cC}). \quad (2)$$

Approximations

This algebra introduce several approximation opportunities:

- Signal Abstraction
- Tick Alignement Abstraction
- Environment Abstraction
- ...

We already modeled two WCET computation methods:

- Max-Plus Approach (common approximation)
- **Tick Alignement Sensitive Approach** (closed to [WRA13])

Iterative feasibility analysis.

We define :

$$\mathrm{clk}(S) = \mathit{tick}(\mathrm{wcet}(S)) = X \odot (1^\omega \wedge \mathrm{wcet}(S))$$

The *clock* of S giving full reachability information for a state S across all ticks and depending on all signals.
Then with our algebra we can intersect two clocks

$$\mathrm{clk}(DisC) \wedge \mathrm{clk}(A1)$$

and find that $\mathrm{clk}(DisC) \wedge \mathrm{clk}(A1) = \mathbb{0}^\omega$, i.e., both clock are incompatible.

By applying this result in the approximated model :

...

We then are able to refine the approximation.

$$\begin{aligned} \mathrm{wcet}(En) &\leq (\mathrm{wcet}_{DisC}(hC) \parallel \mathrm{wcet}_{A0}(cA)) \parallel \mathrm{wcet}_{abs}(cB) \parallel \mathrm{wcet}_{abs}(cC)) \\ &= 0:12:26:41^{\omega} \parallel 0:2:17^{\omega} \parallel 0:14:14:16^{\omega} \\ &= 0:28:57:74^{\omega} \end{aligned}$$

Tighter than the max-plus result $0:28:57:83^{\omega}$.

Conclusion

Design of safety-critical systems need both functional and timing correctness.

- We developped a comprehensive semantics of synchronous languages using min-max-plus Gödel-Dummett algebra.
- This models, precisely, the tick-based lock-step execution of the threads, by formalising the *tick alignment problem*.
- Formalises the modelling of signals and the signal dependency between the threads.

Future works:

- Developement of a timing analysis tools for the SCCharts
- Link the semantics to existing approaches

Questions