Monitoring of the AUTOSAR Timing Extensions with TeSSLa

Hendrik Streichhahn

February 17, 2021

Motivation - Timing

- Timing fundamental for
  - Reliability
  - Availability
  - Safety and security

Motivation - Timing

- Timing fundamental for
  - Reliability
  - Availability
  - Safety and security
- Timing problems
  - Difficult to identify, debug and solve
  - Especially in Cyber-Physical Systems

AUTOSAR TIMEX Constraints

- *EventTriggeringConstraints*
  - *Periodic-*, *Sporadic-*, *ConcretePattern-*, *BurstPattern-*, *ArbitraryEventTriggering*

AUTOSAR TIMEX Constraints

- *EventTriggeringConstraints*
  - *Periodic-*, *Sporadic-*, *ConcretePattern-*, *BurstPattern-*, *ArbitraryEventTriggering*
- *LatencyTimingConstraint*
  - Time distance between *stimulus* and *response* events

AUTOSAR TIMEX Constraints

- *EventTriggeringConstraints*
  - *Periodic-*, *Sporadic-*, *ConcretePattern-*, *BurstPattern-*, *ArbitraryEventTriggering*
- *LatencyTimingConstraint*
  - Time distance between *stimulus* and *response* events
- *AgeConstraint*
  - Minimum and maximum age of received data

AUTOSAR TIMEX Constraints

- *EventTriggeringConstraints*
  - *Periodic-*, *Sporadic-*, *ConcretePattern-*, *BurstPattern-*, *ArbitraryEventTriggering*
- *LatencyTimingConstraint*
  - Time distance between *stimulus* and *response* events
- *AgeConstraint*
  - Minimum and maximum age of received data
- *SynchronizationTimingConstraint*
  - Synchronized event occurrences

AUTOSAR TIMEX Constraints

- *EventTriggeringConstraints*
  - *Periodic-*, *Sporadic-*, *ConcretePattern-*, *BurstPattern-*, *ArbitraryEventTriggering*
- *LatencyTimingConstraint*
  - Time distance between *stimulus* and *response* events
- *AgeConstraint*
  - Minimum and maximum age of received data
- *SynchronizationTimingConstraint*
  - Synchronized event occurrences
- *SynchronizationPointConstraint*
  - *Source* events must occur before *target* events

AUTOSAR TIMEX Constraints

- *EventTriggeringConstraints*
  - *Periodic-*, *Sporadic-*, *ConcretePattern-*, *BurstPattern-*, *ArbitraryEventTriggering*
- *LatencyTimingConstraint*
  - Time distance between *stimulus* and *response* events
- *AgeConstraint*
  - Minimum and maximum age of received data
- *SynchronizationTimingConstraint*
  - Synchronized event occurrences
- *SynchronizationPointConstraint*
  - *Source* events must occur before *target* events
- *OffsetTimingConstraint*
  - Minimal and maximal time distance between events

AUTOSAR TIMEX Constraints

- *EventTriggeringConstraints*
  - *Periodic-*, *Sporadic-*, *ConcretePattern-*, *BurstPattern-*, *ArbitraryEventTriggering*
- *LatencyTimingConstraint*
  - Time distance between *stimulus* and *response* events
- *AgeConstraint*
  - Minimum and maximum age of received data
- *SynchronizationTimingConstraint*
  - Synchronized event occurrences
- *SynchronizationPointConstraint*
  - *Source* events must occur before *target* events
- *OffsetTimingConstraint*
  - Minimal and maximal time distance between events
- *ExecutionOrderConstraint*
  - Order relation between events

AUTOSAR TIMEX Constraints

- *EventTriggeringConstraints*
  - *Periodic-*, *Sporadic-*, *ConcretePattern-*, *BurstPattern-*, *ArbitraryEventTriggering*
- *LatencyTimingConstraint*
  - Time distance between *stimulus* and *response* events
- *AgeConstraint*
  - Minimum and maximum age of received data
- *SynchronizationTimingConstraint*
  - Synchronized event occurrences
- *SynchronizationPointConstraint*
  - *Source* events must occur before *target* events
- *OffsetTimingConstraint*
  - Minimal and maximal time distance between events
- *ExecutionOrderConstraint*
  - Order relation between events
- *ExecutionTimeConstraint*
  - Minimal and maximal runtime of an executable (e.g. functions)

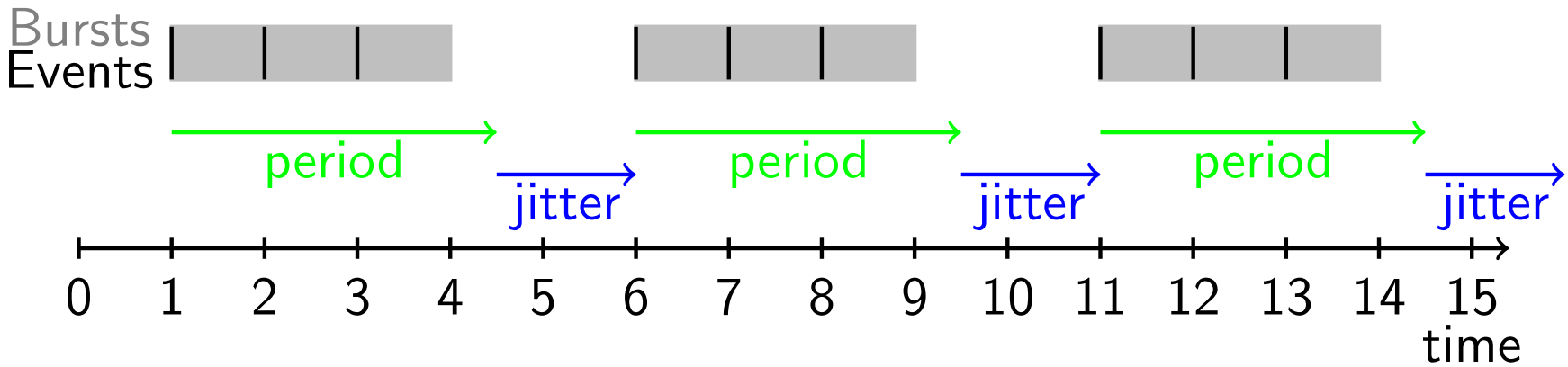
AUTOSAR TIMEX Constraints - Informal Definition

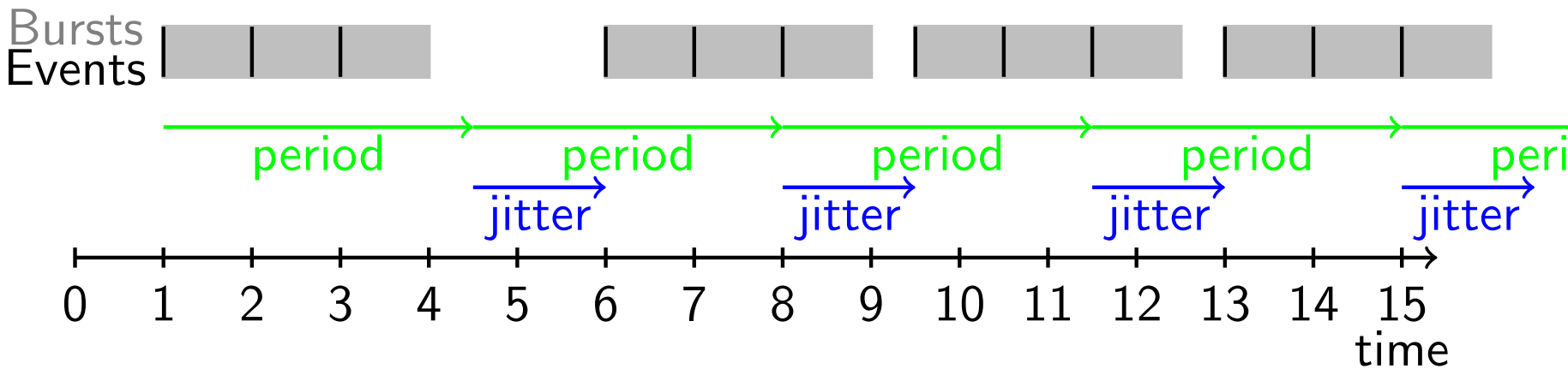
- Problem: Informal definitions, only textual often
  - Different interpretations possible
  - Unsuitable for automated monitoring

AUTOSAR TIMEX Constraints - Informal Definition

- Problem: Informal definitions, only textual often
  - Different interpretations possible
  - Unsuitable for automated monitoring
- Example *BurstPatternEventTriggering*
  - Parameter *patternPeriod* (time value)
    "The optional parameter "PatternPeriod" specifies the time distance between the beginnings of subsequent repetitions of the given burst pattern"[AUT18b]
  - Parameter *patternJitter* (time value)
    "The optional parameter "PatternJitter" specifies the deviation of the time interval's starting point from the beginning of the given period. This parameter is only applicable in conjunction with the parameter "Pattern Period"" [AUT18b]

BurstPatternEventTriggering





TADL2

- European ITEA2 Project TIMMO2USE (Timing Model, 2010-2012)[Blo+12]

TADL2

- European ITEA2 Project TIMMO2USE (Timing Model, 2010-2012)[Blo+12]
- **T**iming **A**ugmented **D**escription **L**anguage v. 2(TADL2)
  - Timing Extension for **E**lectronics **A**rchitecture and **S**oftware **T**echnology-**A**rchitecture **D**escription **L**anguage (EAST-ADL)

TADL2

- European ITEA2 Project TIMMO2USE (Timing Model, 2010-2012)[Blo+12]
- **T**iming **A**ugmented **D**escription **L**anguage v. 2(TADL2)
  - Timing Extension for **E**lectronics **A**rchitecture and **S**oftware **T**echnology-**A**rchitecture **D**escription **L**anguage (EAST-ADL)
- Constraints are strictly formally defined
  - TiCL (**Ti**ming **C**onstraint **L**ogic)

TADL2 Timing Constraints

- *Delay-*, *StrongDelay-*, *Reaction-* and *AgeConstraint*
  - Events occur as "response" to each other

TADL2 Timing Constraints

- *Delay-*, *StrongDelay-*, *Reaction-* and *AgeConstraint*
  - Events occur as "response" to each other
- *Repeat-*, *Repetition-*, *Sporadic-*, *Periodic-*, *Pattern-*, *Burst-* and *ArbitraryConstraint*
  - Time distances between event occurrences

TADL2 Timing Constraints

- *Delay-*, *StrongDelay-*, *Reaction-* and *AgeConstraint*
  - Events occur as "response" to each other
- *Repeat-*, *Repetition-*, *Sporadic-*, *Periodic-*, *Pattern-*, *Burst-* and *ArbitraryConstraint*
  - Time distances between event occurrences
- *Synchronization-*, *StrongSynchronization-*, *InputSynchronization-* and *OutputSynchronizationConstraint*
  - Synchronized occurrences of events

TADL2 Timing Constraints

- *Delay-*, *StrongDelay-*, *Reaction-* and *AgeConstraint*
  - Events occur as "response" to each other
- *Repeat-*, *Repetition-*, *Sporadic-*, *Periodic-*, *Pattern-*, *Burst-* and *ArbitraryConstraint*
  - Time distances between event occurrences
- *Synchronization-*, *StrongSynchronization-*, *InputSynchronization-* and *OutputSynchronizationConstraint*
  - Synchronized occurrences of events
- *ExecutionTimeConstraint*
  - Runtime of executables (e.g. functions)

TADL2 Timing Constraints

- *Delay-*, *StrongDelay-*, *Reaction-* and *AgeConstraint*
  - Events occur as "response" to each other
- *Repeat-*, *Repetition-*, *Sporadic-*, *Periodic-*, *Pattern-*, *Burst-* and *ArbitraryConstraint*
  - Time distances between event occurrences
- *Synchronization-*, *StrongSynchronization-*, *InputSynchronization-* and *OutputSynchronizationConstraint*
  - Synchronized occurrences of events
- *ExecutionTimeConstraint*
  - Runtime of executables (e.g. functions)
- *ComparisonConstraint*
  - Comparison between timestamps

TADL2 Timing Constraints

- *Delay-*, *StrongDelay-*, *Reaction-* and *AgeConstraint*
  - Events occur as "response" to each other
- *Repeat-*, *Repetition-*, *Sporadic-*, *Periodic-*, *Pattern-*, *Burst-* and *ArbitraryConstraint*
  - Time distances between event occurrences
- *Synchronization-*, *StrongSynchronization-*, *InputSynchronization-* and *OutputSynchronizationConstraint*
  - Synchronized occurrences of events
- *ExecutionTimeConstraint*
  - Runtime of executables (e.g. functions)
- *ComparisonConstraint*
  - Comparison between timestamps
- *OrderConstraint*
  - n^{th} *source* event must occur before n^{th} *target* event

AUTOSAR TIMEX 4.4.0 $\Leftrightarrow$ TADL2

- Most AUTOSAR TIMEX Constraints can be expressed in TADL2 Constraints:

AUTOSAR TIMEX	TADL2 Constraint	Complete Coverage
PeriodicEventTriggering	PeriodicConstraint	√
SporadicEventTriggering	SporadicConstraint	√
ConcretePatternEventTriggering	PatternConstraint	Minor differences
BurstPatternEventTriggering	BurstConstraint	Large differences
ArbitraryEventTriggering	ArbitraryConstraint	Minor differences
LatencyTimingConstraint	ReactionConstraint AgeConstraint	Minor differences
AgeConstraint	AgeConstraint	Minor differences
SynchronizationTimingConstraint	SynchronizationConstraint StrongSynchronizationConstraint OutputSynchronizationConstraint InputSynchronizationConstraint	√
SynchronizationPointConstraint	–	–
OffsetTimingConstraint	DelayConstraint	√
ExecutionOrderConstraint	multiple use of OrderConstraint	√
ExecutionTimeConstraint	ExecutionTimeConstraint	Minor differences

Monitorability

- Not every property can be infinitely monitored on infinite streams
  - Limited Resources (memory, time)

Monitorability

- Not every property can be infinitely monitored on infinite streams
  - Limited Resources (memory, time)
- Classification
  - Simple Monitorable
    - Worst case memory and runtime per event bounded independent of trace
    - No new timestamps required (*timestamp conservative*)

Monitorability

- Not every property can be infinitely monitored on infinite streams
  - Limited Resources (memory, time)
- Classification
  - Simple Monitorable
    - Worst case memory and runtime per event bounded independent of trace
    - No new timestamps required (*timestamp conservative*)
  - Simple Monitorable with Delay
    - Extension to Simple Monitorable
    - Exactly one new timestamp may be introduced

Monitorability

- Not every property can be infinitely monitored on infinite streams
  - Limited Resources (memory, time)
- Classification
  - Simple Monitorable
    - Worst case memory and runtime per event bounded independent of trace
    - No new timestamps required (*timestamp conservative*)
  - Simple Monitorable with Delay
    - Extension to Simple Monitorable
    - Exactly one new timestamp may be introduced
  - Not Simple Monitorable
    - Worst case memory or runtime per event cannot be bounded independently from trace

Timestamps

- Infinite traces $\Rightarrow$ infinite large timestamps
  - Cannot be used in simple monitorable setting

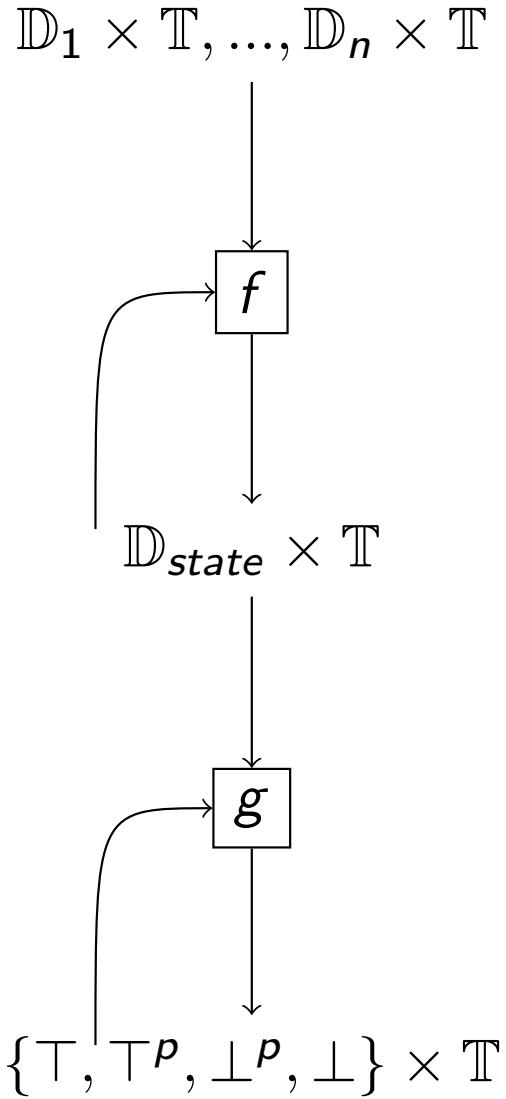
[1] for example, a 64-bit unsigned integer variable is enough, to cover nanoseconds for 584.55 years

Timestamps

- Infinite traces $\Rightarrow$ infinite large timestamps
  - Cannot be used in simple monitorable setting
- Restriction of Timestamps
  - Timestamps start at $t_0 = 0$
  - All used timestamps must be smaller than t_{max}.
    t_{max} must be big enough, so it is not reached in practical use [1]
  - Minimal distance between two subsequent time values is predetermined
  - Number of possible timestamps is significantly larger than the number of events

[1] for example, a 64-bit unsigned integer variable is enough, to cover nanoseconds for 584.55 years

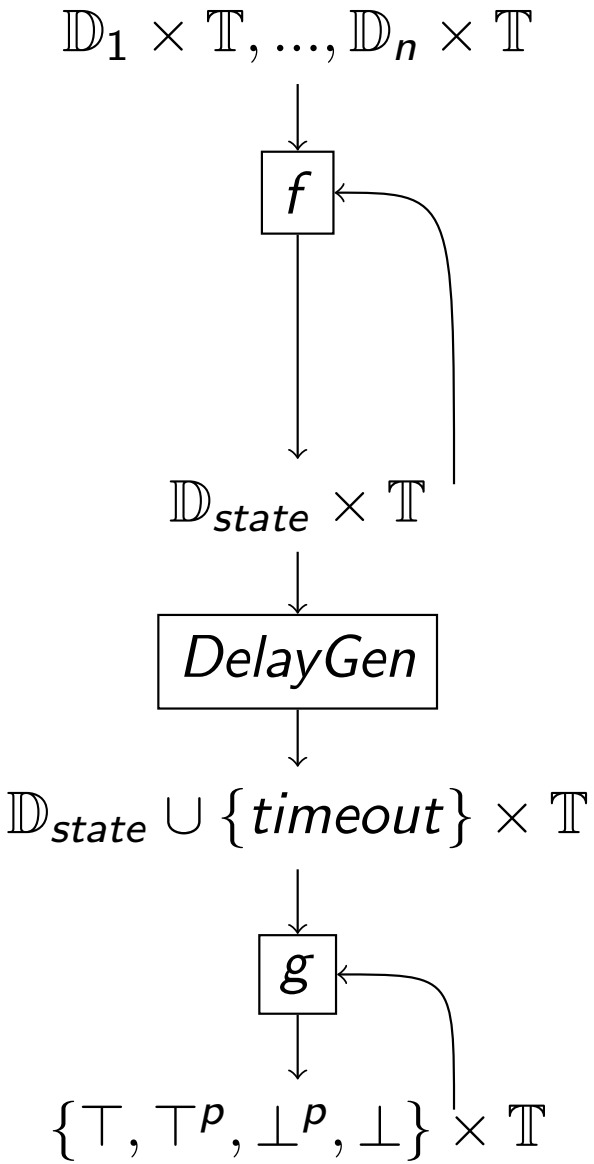
Simple Monitorability



- Non-Synchronized Input streams
- State transition function, worst case runtime independent from input streams
- State stream, worst case memory independent from input streams
- Evaluation Function, worst case runtime independent from input streams
- Output stream

- For given constraint parameters, a monitor can be build, which monitors the constraint infinitely with fixed resources

Simple Monitorability with Delay



- Non-Synchronized Input streams
- State transition function, worst case runtime independent from input streams
- State stream, worst case memory independent from input streams
- Delay Generator
- State stream including *timeouts*
- Evaluation function, worst case runtime independent from input streams
- Output stream

- For given constraint parameters, a monitor can be build, which monitors the constraint on infinitely with fixed resources

Simple Monitorable with Delay - Example

RepeatConstraint

- $RepeatConstraint(event, lower, upper, span) \Leftrightarrow$
  $\forall X \leq event : |X| = span + 1 \Rightarrow lower \leq \lambda([X]) \leq upper$

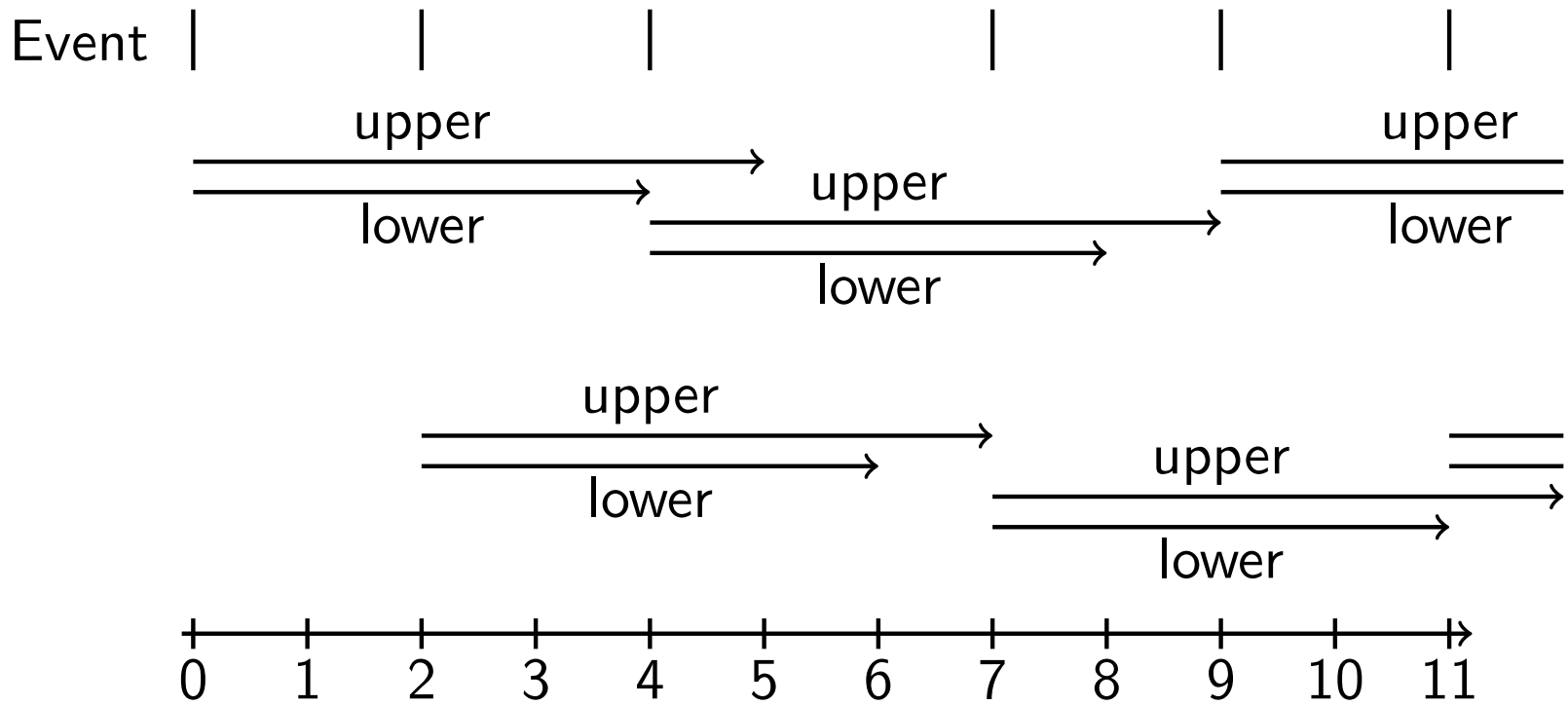


Figure: Example RepeatConstraint - $lower = 4$, $upper = 5$, $span = 2$

Not Simple Monitorable - Example *DelayConstraint*

- $DelayConstraint(source, target) \Leftrightarrow$
  $\forall x \in source : \exists y \in target : lower \leq y - x \leq upper$

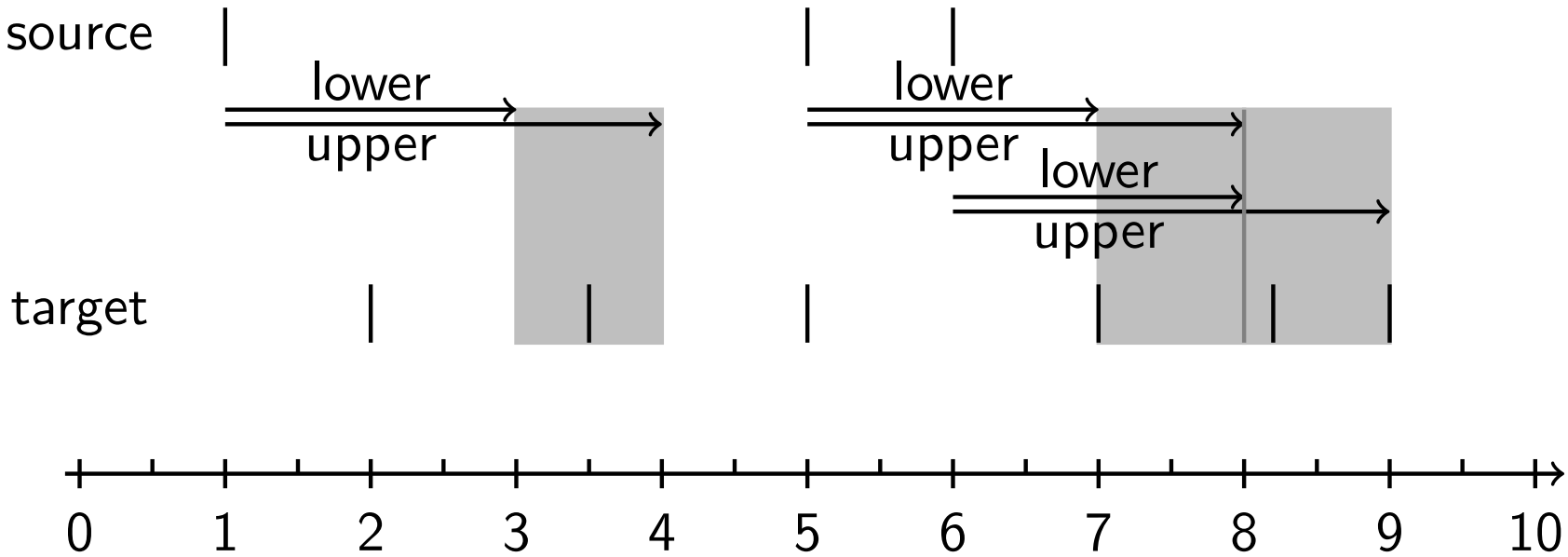


Figure: Example DelayConstraint - $lower = 2$, $upper = 3$

Not Simple Monitorable - Example *DelayConstraint*

- $\mathit{DelayConstraint}(\mathit{source}, \mathit{target}) \Leftrightarrow$
  $\forall x \in \mathit{source} : \exists y \in \mathit{target} : \mathit{lower} \leq y - x \leq \mathit{upper}$

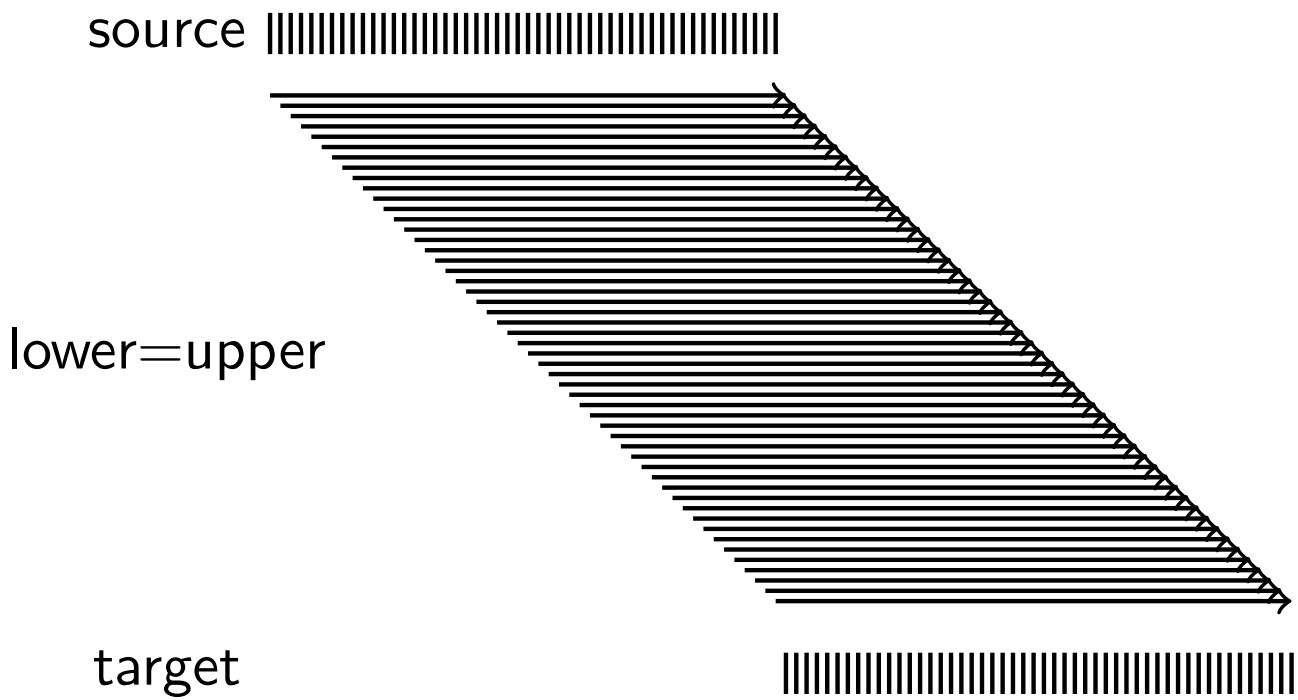


Figure: *DelayConstraint* with $\mathit{lower} = \mathit{upper} = 5$

- Worst case memory consumption is not bounded independently from input stream $\Rightarrow$ Not simple monitorable

Monitorability Analysis Results for the 18 TADL2 Constraints

Figure: Simple Monitorable

Monitorability Analysis Results for the 18 TADL2 Constraints

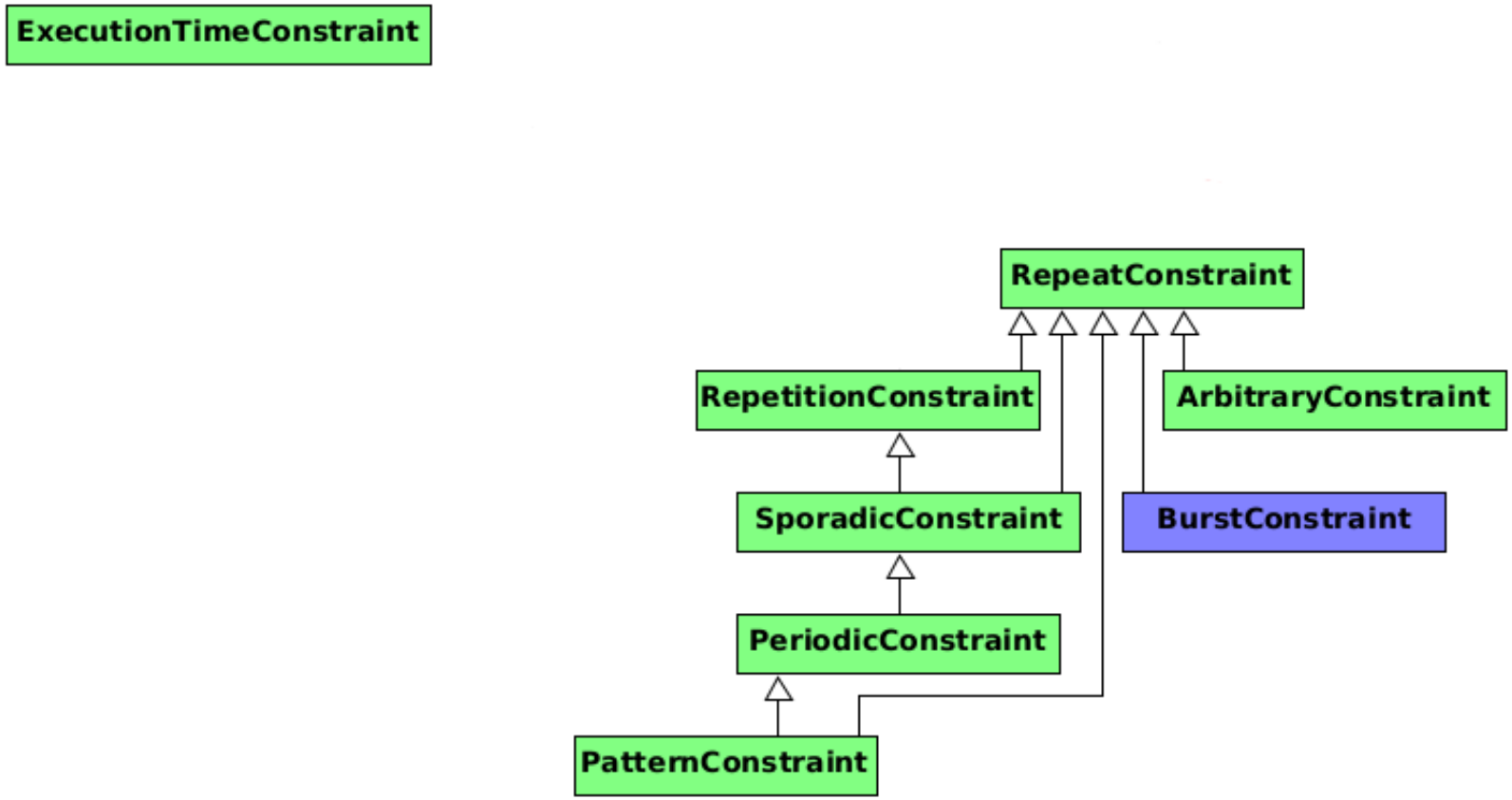


Figure: Simple Monitorable, Simple Monitorable With Delay

Monitorability Analysis Results for the 18 TADL2 Constraints

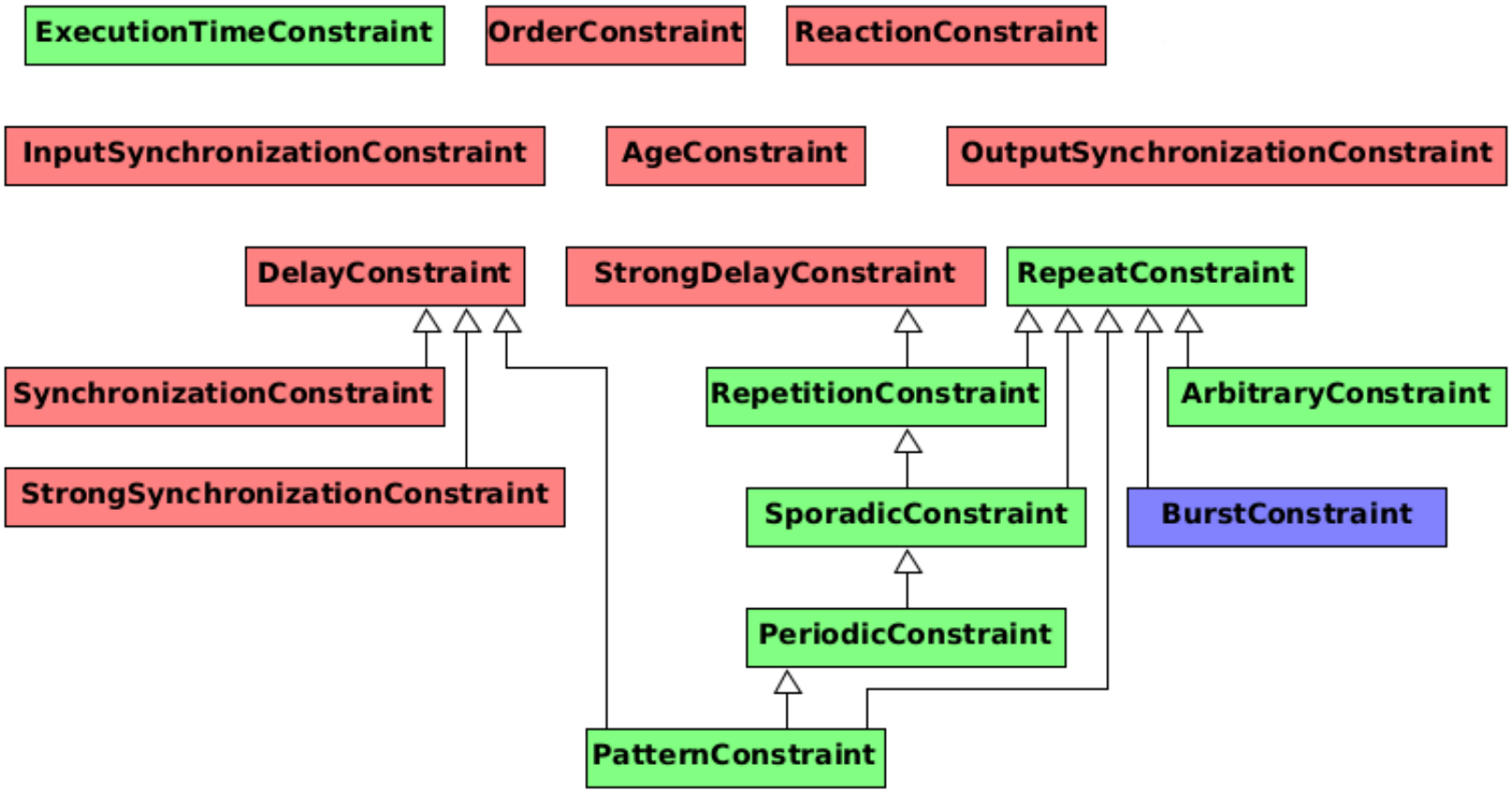


Figure: Simple Monitorable, Simple Monitorable With Delay, Not simple Monitorable

Monitorability Analysis Results for the 18 TADL2 Constraints

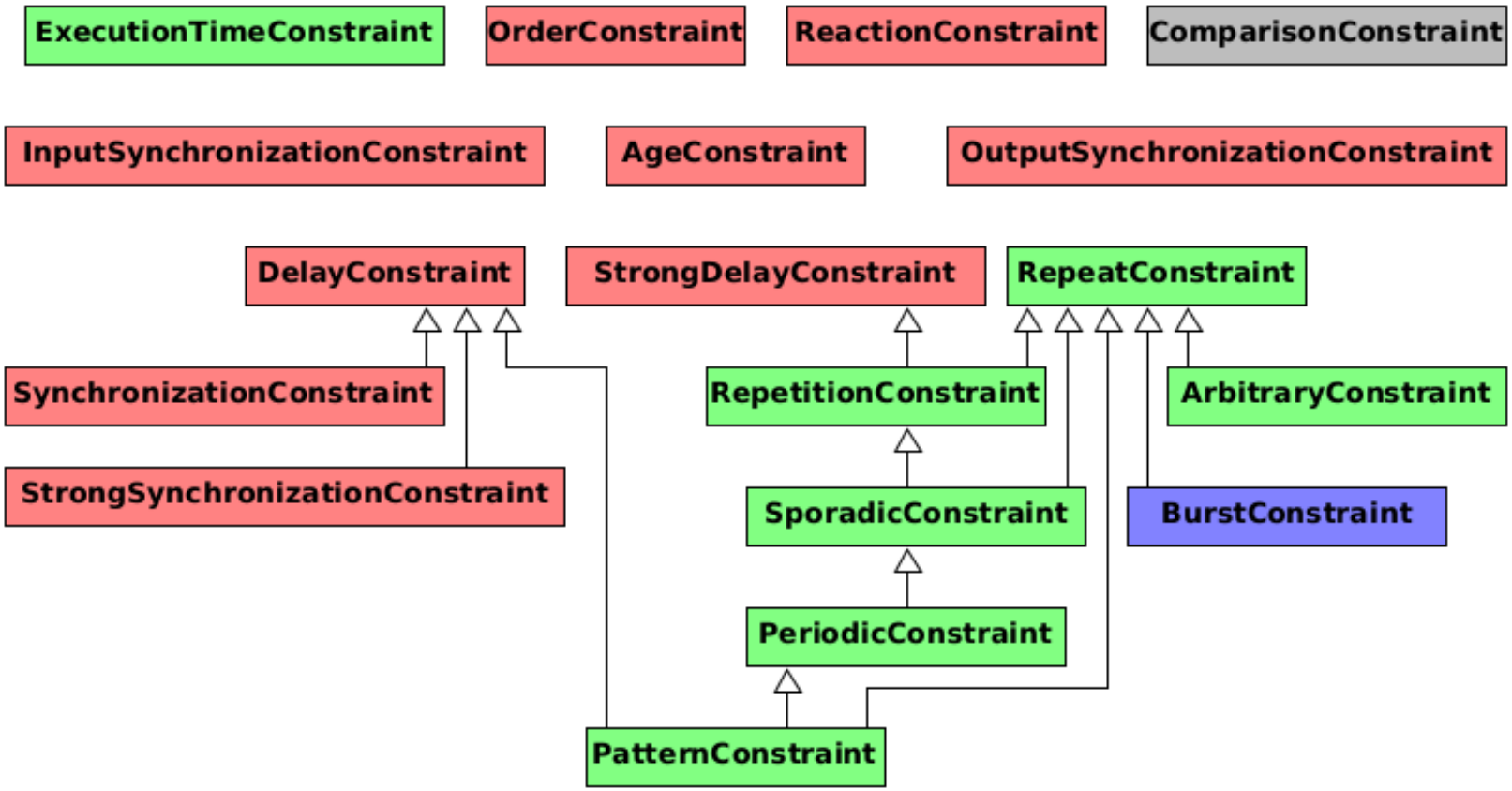


Figure: Simple Monitorable, Simple Monitorable With Delay, Not simple Monitorable, Not applicable

Implementation

- According to the scheme presented in *Simple Monitorability (with Delay)*
  - State transition function
  - State stream
  - use of *delay*, if needed
  - Evaluation function

Implementation

- According to the scheme presented in *Simple Monitorability (with Delay)*
  - State transition function
  - State stream
  - use of *delay*, if needed
  - Evaluation function
- If possible, implementations were reused. E.g.:
  - $\mathit{BurstConstraint}(\mathit{event}, \mathit{length}, \mathit{maxOccurences}, \mathit{minimum}) \Leftrightarrow$ $\mathit{RepeatConstraint}(\mathit{event}, \mathit{length}, \infty, \mathit{maxOccurrences})$ $\wedge\ \mathit{RepeatConstraint}(\mathit{event}, \mathit{minimum}, \infty, 1)$
  - ComparisonConstraint
    Comparison of timestamps already implemented in TeSSLa

Experimental Evaluation

- The implementations were tested on large Traces (10.000 Events), which were generated with different constraint parameters

Experimental Evaluation

- The implementations were tested on large Traces (10.000 Events), which were generated with different constraint parameters
- Edge cases tested seperately

Experimental Evaluation

- The implementations were tested on large Traces (10.000 Events), which were generated with different constraint parameters
- Edge cases tested seperately
- Runtime per input timestamp were measured
  - TeSSLa 1.2.2
  - Windows 10.0.19041.0
  - Intel i5-6600k, 4.3 GHz

Runtime - Constant Runtime

- Average Runtime per input timestamp

Constraint	**Dependencies**	**Measured Time**
ExecutionTimeConstraint	$\mathcal{O}(1)$	0.18-0.23ms
OrderConstraint	$\mathcal{O}(1)$	0.14-0.32ms
SporadicConstraint	$\mathcal{O}(1)$	0.36-0.42ms
PeridicConstraint	$\mathcal{O}(1)$	0.34-0.42ms
PatternConstraint	$\mathcal{O}(1)$	0.59-0.71ms
StrongDelayConstraint	$\mathcal{O}(1)$	0.21-0.38ms
RepeatConstraint	$\mathcal{O}(1)$	0.22-0.29ms
RepetitionConstraint	$\mathcal{O}(1)$	0.23-0.31ms
BurstConstraint	$\mathcal{O}(1)$	0.34-0.41ms

Runtime - Runtime Bounded by Parameters

- Average Runtime per input timestamp

Constraint	**Dependencies**	**measured Time**
DelayConstraint	$\mathcal{O}(upper)$	0.25-0.43ms
Synchronization Constraint	$\mathcal{O}(\lvert event \rvert * tolerance)$	0.82-8.55ms
StrongSynchronization Constraint	$\mathcal{O}(\lvert event \rvert * tolerance)$	0.34-2.33ms
ArbitraryConstraint	$\mathcal{O}(\lvert minimum \rvert)$	0.2ms-8.26ms
AgeConstraint	$\mathcal{O}(maximum)$	0.28-15.18ms
ReactionConstraint	$\mathcal{O}(maximum)$	0.28-26.66ms
OutputSynchronization Constraint	$\mathcal{O}(tolerance \lvert response \rvert^2)$	0.46-3.28ms
InputSynchronization Constraint	$\mathcal{O}(\lvert stimulus \rvert^2)$	0.33-143.76ms

Summary

- TADL2 as formal alternative to the AUTOSAR TIMEX constraints
- Monitorability of the TADL2 constraints
- Implementation of a monitor for each TADL2 constraint
  - experimental evaluation

References

AUTOSAR Basic Approach. https://web.archive.org/web/20170707082404/https://www.autosar.org/fileadmin/images/media_pictures/AUTOSAR_Basic_Approach.jpg. Accessed: 2020-12-06, archive from:2017-07-07.

AUTOSAR. *Recommended Methods and Practices for Timing Analysis and Design within the AUTOSAR Development Process*. Tech. rep. 4.4.0. AUTOSAR, 2018.

AUTOSAR. *Specification of Timing Extensions*. Tech. rep. 4.0. AUTOSAR, 2018.

Jean Berstel. *Transductions and Context-Free Languages* -. Wiesbaden: Vieweg+Teubner Verlag, 1979. ISBN: 978-3-519-02340-1.

Hans Blom et al. *TIMMO2USE Language syntax, semantics, metamodel V2*. Tech. rep. 1.2. ITEA2, 2012.