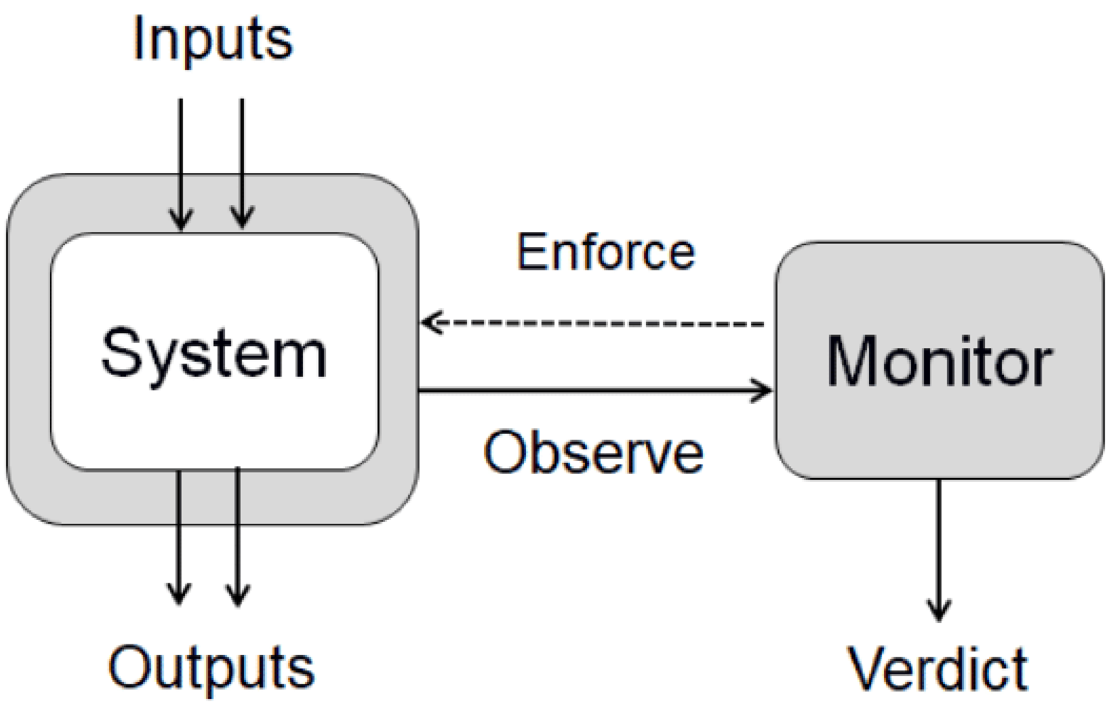
Quantitative and Approximate Monitoring

LICS'21

Thomas A. Henzinger   N. Ege Saraç

IST AUSTRIA
Institute of Science and Technology

Online Black-Box Monitoring



- Monitor runs in parallel and outputs a stream of verdicts
- Computation is deterministic and online/real-time[1]

[1] Rabin, M. O. (1963). Real time computation.

Motivation

- Increasing software complexity
  - systems cannot always be model-checked or modeled
  - static verification gap?
    - better tools but harder challenges
- Increasing hardware parallelism
  - not all hardware resources will go into performance
    - some will hopefully go into assurance

Motivation

- Increasing software complexity
  - systems cannot always be model-checked or modeled
  - static verification gap?
    - better tools but harder challenges
- Increasing hardware parallelism
  - not all hardware resources will go into performance
    - some will hopefully go into assurance

- Static verification $\rightarrow$ emptiness
  Runtime verification $\rightarrow$ membership
  - more expressive formalisms (beyond finite-state)
  - quantitative and approximate methods
    - distance measures between behaviors rather than systems

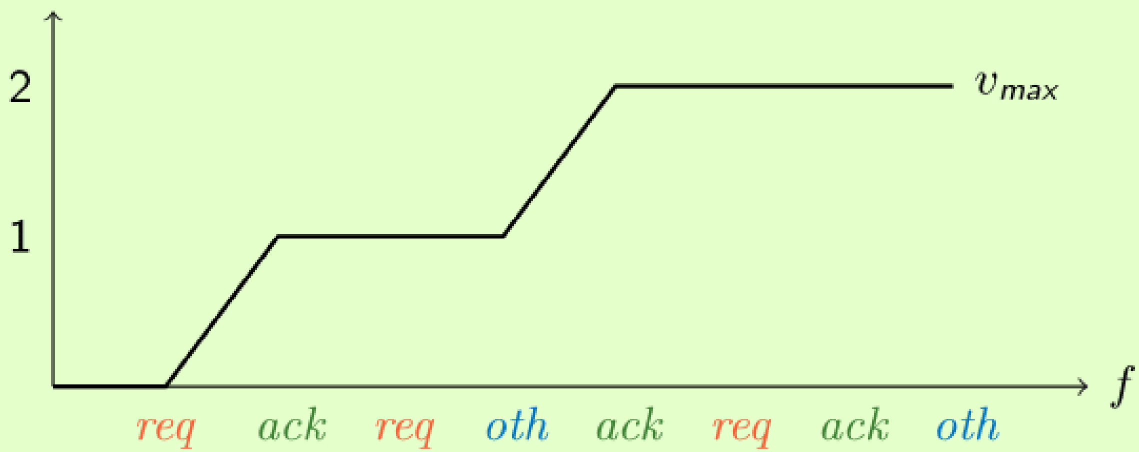
Our contribution

- A framework for runtime verification which
  - supports monitors that over- or under-approximate quantitative properties
  - enables comparison of such monitors w.r.t. precision and resource use

Example: Maximal Response Time

- Model: server with
  - $\Sigma = \{req, ack, oth\}$
  - $p_{max} : \Sigma^\omega \to \mathbb{N} \cup \{\infty\}$
- Verdict function:
  - $v_{max} : \Sigma^* \to \mathbb{N} \cup \{\infty\}$

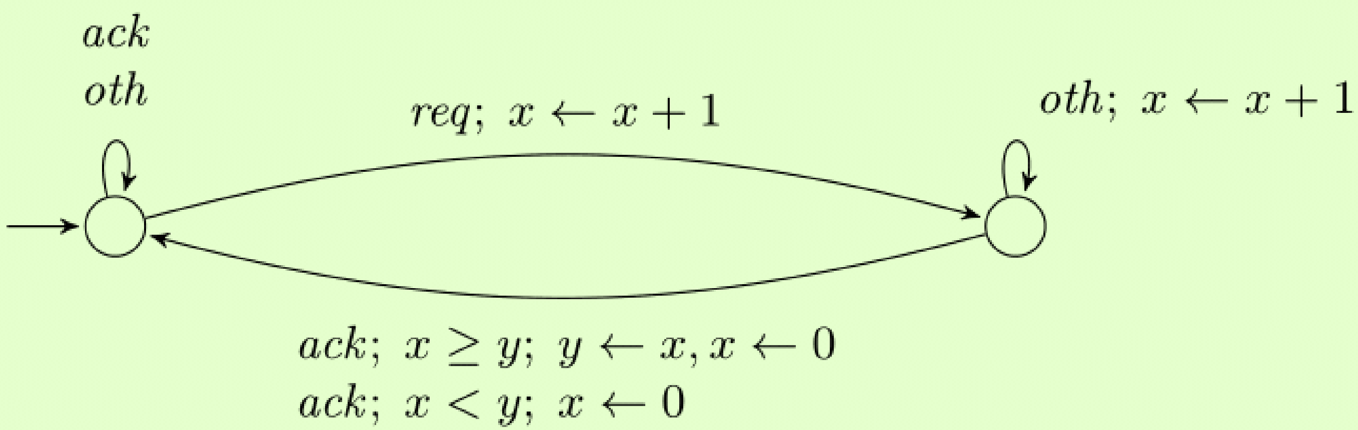
Example 1.



Example: Maximal Response Time

- Model: server with
  - $\Sigma = \{req, ack, oth\}$
  - $p_{max} : \Sigma^\omega \to \mathbb{N} \cup \{\infty\}$
- Verdict function:
  - $v_{max} : \Sigma^* \to \mathbb{N} \cup \{\infty\}$

Example 1.

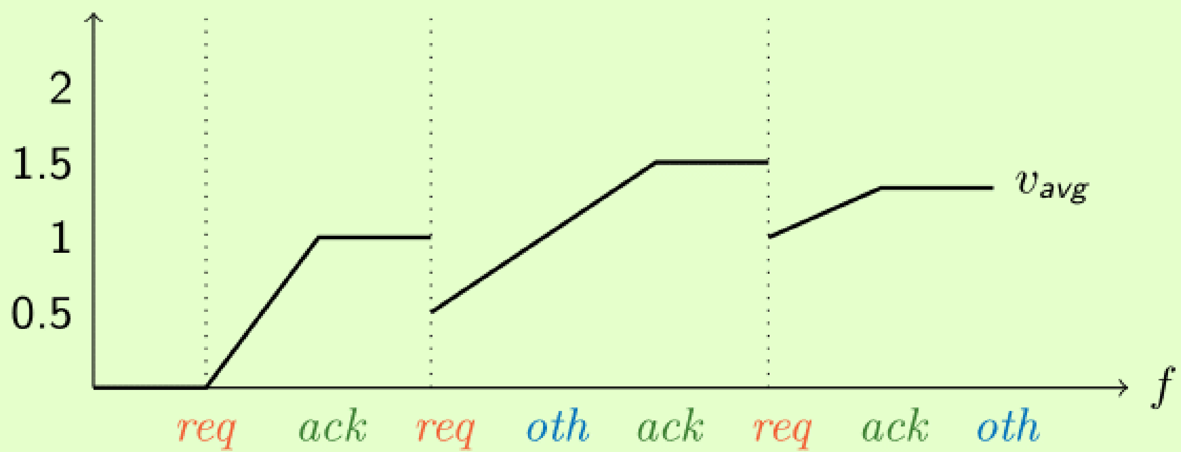


output: $\lambda(q, \mathsf{v}) = \max(\mathsf{v}(x), \mathsf{v}(y))$

Example: Average Response Time

- Model: server with
  - $\Sigma = \{req, ack, oth\}$
  - $p_{avg} : \Sigma^\omega \to \mathbb{Q} \cup \{\infty\}$
- Verdict function:
  - $v_{avg} : \Sigma^* \to \mathbb{Q} \cup \{\infty\}$

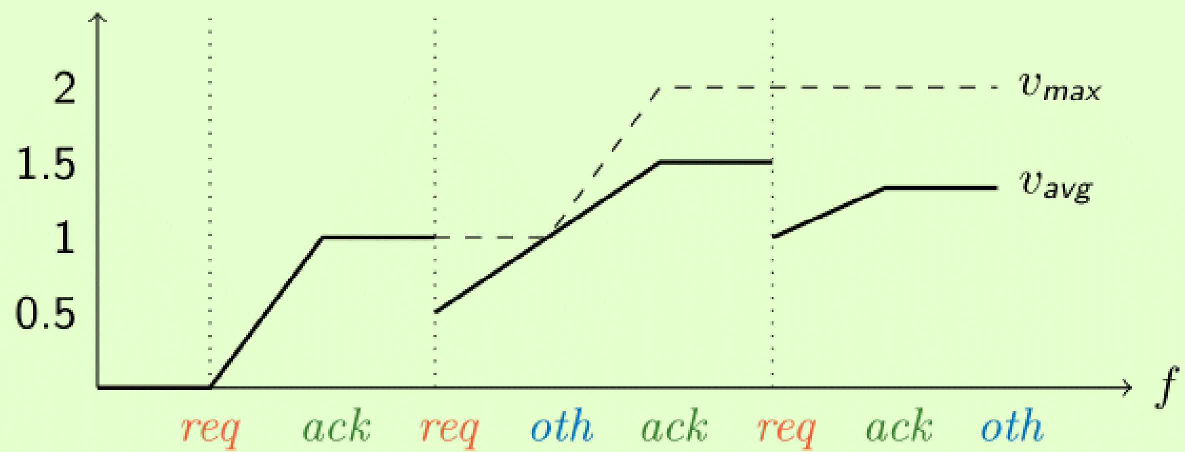
Example 2.



Example: Average Response Time

- Model: server with
  - $\Sigma = \{req, ack, oth\}$
  - $p_{avg} : \Sigma^\omega \to \mathbb{Q} \cup \{\infty\}$
- Verdict function:
  - $v_{avg} : \Sigma^* \to \mathbb{Q} \cup \{\infty\}$

Example 2.



Example: Pairwise Maximal Response Time

- Model: server with
  - $\Sigma = \{req_1, req_2, ack_1, ack_2, oth\}$
  - $p_{pair} : \Sigma^\omega \to (\mathbb{N} \cup \{\infty\}) \times (\mathbb{N} \cup \{\infty\})$

Example 3.

- 4 counters $\to$ exact for both
  3 counters $\to$ exact + under-approximate
  2 counters $\to$ under-approximate for both
- decreasing "precision"

Modalities of Quantitative Monitoring

For a quantitative property $p : \Sigma^\omega \to \mathbb{D}$ and a verdict function $v : \Sigma^* \to \mathbb{D}$

- p is universally monitorable from below by v iff
  - $\forall f \in \Sigma^\omega : \limsup_{n\to\infty} v(f_{0..n}) = p(f)$
- p is existentially monitorable from below by v iff
  - $\forall f \in \Sigma^\omega : \limsup_{n\to\infty} v(f_{0..n}) \leq p(f)$
  - $\forall s \in \Sigma^* : \exists f \in \Sigma^\omega : \limsup_{n\to\infty} v(sf_{0..n}) = p(sf)$
- p is approximately monitorable from below by v iff
  - $\forall f \in \Sigma^\omega : \limsup_{n\to\infty} v(f_{0..n}) \leq p(f)$

For verdict functions v, u that monitor p from below

- v is more precise than u iff
  - $\forall f \in \Sigma^\omega : \limsup_{n\to\infty} u(f_{0..n}) \leq \limsup_{n\to\infty} v(f_{0..n})$
  - $\exists g \in \Sigma^\omega : \limsup_{n\to\infty} u(g_{0..n}) < \limsup_{n\to\infty} v(g_{0..n})$

Modalities of Quantitative Monitoring

For a quantitative property $p : \Sigma^\omega \to \mathbb{D}$ and a verdict function $v : \Sigma^* \to \mathbb{D}$

- p is universally monitorable from above by v iff
  - $\forall f \in \Sigma^\omega : \liminf_{n\to\infty} v(f_{0..n}) = p(f)$
- p is existentially monitorable from above by v iff
  - $\forall f \in \Sigma^\omega : \liminf_{n\to\infty} v(f_{0..n}) \geq p(f)$
  - $\forall s \in \Sigma^* : \exists f \in \Sigma^\omega : \liminf_{n\to\infty} v(sf_{0..n}) = p(sf)$
- p is approximately monitorable from above by v iff
  - $\forall f \in \Sigma^\omega : \liminf_{n\to\infty} v(f_{0..n}) \geq p(f)$

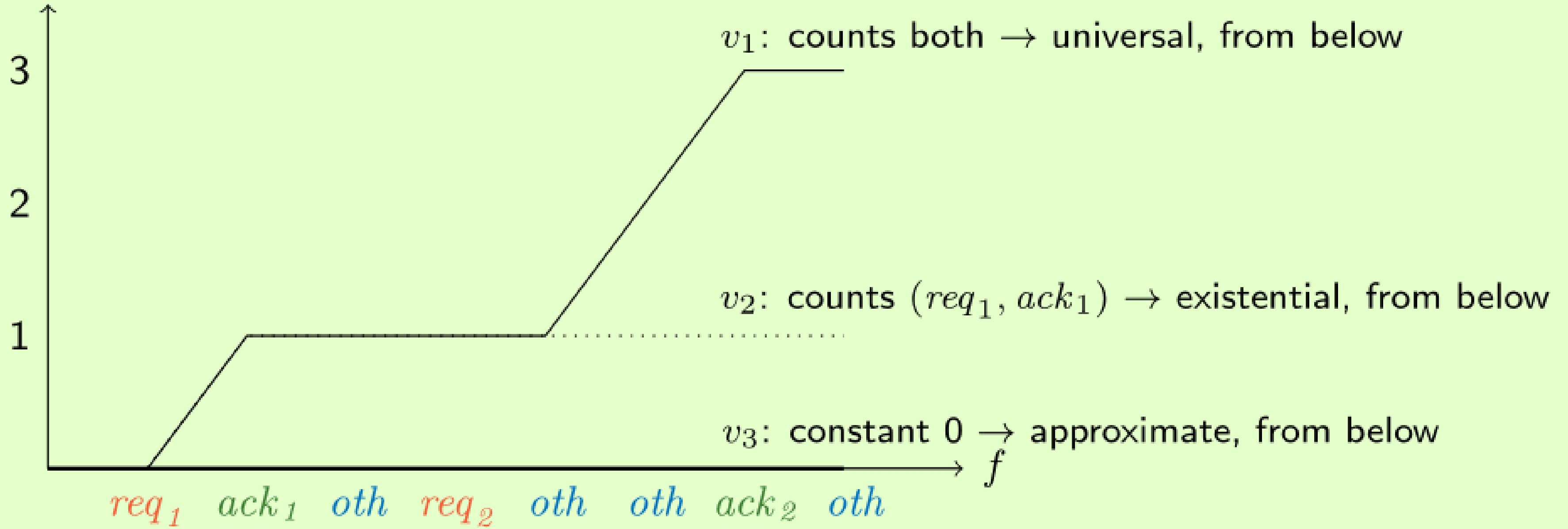
For verdict functions v, u that monitor p from above

- v is more precise than u iff
  - $\forall f \in \Sigma^\omega : \liminf_{n\to\infty} u(f_{0..n}) \geq \liminf_{n\to\infty} v(f_{0..n})$
  - $\exists g \in \Sigma^\omega : \liminf_{n\to\infty} u(g_{0..n}) > \liminf_{n\to\infty} v(g_{0..n})$

Example: Modalities of Quantitative Monitoring

- Model: server with
  - $\Sigma = \{req_1, req_2, ack_1, ack_2, oth\}$
  - p_i: maximal response time over (req_i, ack_i)
  - $p(f) = \max(p_1(f), p_2(f))$

Example 4.



The Power of Monotonicity

Monotonic verdicts:

- conservative estimates that improve in quality over time

- Model: server with
  - $\Sigma = \{req, ack, oth\}$
  - p_{min}: minimal response time
- $s = req\, oth\, oth\, ack$
  - $p_{min}(sf) \leq 3$ for all $f \in \Sigma^{\omega}$
- upper bound $\rightarrow$ property value

The Power of Monotonicity

Monotonic verdicts:

- conservative estimates that improve in quality over time

- Model: server with
  - $\Sigma = \{req, ack, oth\}$
  - p_{min}: minimal response time
- $s = req\,oth\,oth\,ack$
  - $p_{min}(sf) \leq 3$ for all $f \in \Sigma^\omega$
- upper bound $\rightarrow$ property value

- Such properties are *continuous*[2]
- Define *co-continuous* using lower bounds, e.g., maximal response time

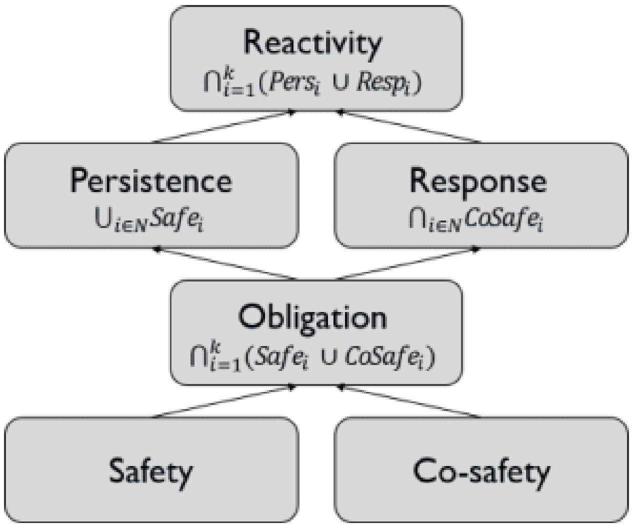
Theorem 5.

A quantitative property p is continuous (resp. co-continuous) iff p is universally monitorable by a monotonically decreasing (resp. increasing) verdict function.

[2] Weihrauch, K. (1987). Complete Partial Orders. In *Computability*.

Boolean Properties in Quantitative Setting

- Boolean monitorability[3,4,5,6]
- Safety-progress hierarchy[7]



Universal monitorability from below

$\mathbb{D}$	Mono. increasing	Unrestricted verdict
$\mathbb{B}$	$\emptyset$ or Σ^ω	Obl
$\mathbb{B}_\perp$	Safe $\cap$ CoSafe	Obl
$\mathbb{B}_t$	CoSafe	Resp
$\mathbb{B}_f$	Safe	Pers

Existential monitorability from below

$\mathbb{D}$	Mono. increasing	Unrestricted verdict
$\mathbb{B}$	$\emptyset$ or Σ^ω	Obl
$\mathbb{B}_\perp$	Mon	at least Mon $\cup$ React
$\mathbb{B}_t$	any $P \subseteq \Sigma^\omega$	any $P \subseteq \Sigma^\omega$
$\mathbb{B}_f$	any $P \subseteq \Sigma^\omega$	any $P \subseteq \Sigma^\omega$

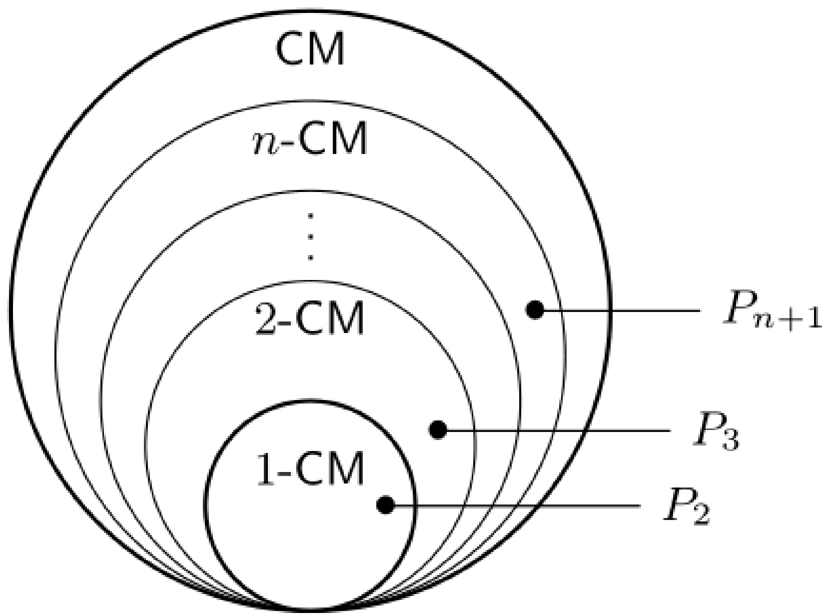
[3] Pnueli, A., & Zaks, A. (2006). PSL model checking and run-time verification via testers.
[4] Bauer, A., Leucker, M., & Schallhart, C. (2011). Runtime verification for LTL and TLTL.
[5] Falcone, Y., Fernandez, J. C., & Mounier, L. (2012). What can you verify and enforce at runtime?
[6] Aceto, L., Achilleos, A., Francalanza, A., Ingólfsdóttir, A., & Lehtinen, K. (2019). An operational guide to monitorability.
[7] Chang, E., Manna, Z., & Pnueli, A. (1993). The safety-progress classification.

Approximate Register Monitors

Real-time counter hierarchy[8]:

$T = \langle 0, +1, -1, \geq 0 \rangle$

$\Sigma_k = \{1, \ldots, k\}$ $\qquad P_k = \{f \in \Sigma_k^\omega \mid \forall\, 1 \leq i < k : \forall s \prec f : |s|_i \geq |s|_{i+1}\}$



[8] Ferrère, T., Henzinger, T. A., & Saraç, N. E. (2018). A theory of register monitors.

Approximate Register Monitors

$T = \langle 0, +1, -1, \geq 0 \rangle$

$\Sigma_k = \{1, \dots, k\}$ $\quad P_k = \{f \in \Sigma_k^\omega \mid \forall\, 1 \leq i < k : \forall s \prec f : |s|_i \geq |s|_{i+1}\}$

Theorem 6.

For every $k > 1$, there is a quantitative property q_k such that

- *q_k is universally monitorable by a k-counter monitor, and*
- *for every $\ell < k$ and approximate ℓ-counter monitor for q_k, there exists a more precise $(\ell + 1)$-counter monitor.*

Proof idea.

- Get a quantitative property q_k from P_k
  - $q_k(f) = \infty$ if $f \in P_k$
  - $q_k(f) = n$ if $f \notin P_k$ where $n :=$ len(shortest bad prefix of f)
- Approximate monitor makes "mistakes" $\rightarrow$ use the new counter to fix

□

Approximate Register Monitors

Observations: (i) The monitor needs to recognize the boolean property
(ii) No need to use Σ_k – encode using $\{0, 1, \#\}$

Theorem 7.

There is a quantitative property q such that

- *q is not universally monitorable by any counter monitor, and*
- *for every $k > 1$ and k-counter monitor for q, there exists a more precise $(k+1)$-counter monitor.*

Approximate Register Monitors

Observations: (i) The monitor needs to recognize the boolean property
(ii) No need to use Σ_k – encode using $\{0, 1, \#\}$

Theorem 7.

There is a quantitative property q such that

- *q is not universally monitorable by any counter monitor, and*
- *for every $k > 1$ and k-counter monitor for q, there exists a more precise $(k+1)$-counter monitor.*

Real-time monitors beyond counters:

- $P = \{\#s_0\#s_1\#s_2 \ldots \mid \forall i \in \mathbb{N} : s_i \in \{0,1\}^* \wedge \forall j \neq i : s_j \neq s_i\}$
  $\hookrightarrow$ no number repeats
  - $q(f) = \infty$ if $f \in P$
  - $q(f) = n$ if $f \notin P$ where $n :=$ len(shortest bad prefix of f)
- q is not universally monitorable by any $\langle 0, 1, +, \times, \geq \rangle$-monitor[8]

[8] Ferrère, T., Henzinger, T. A., & Saraç, N. E. (2018). A theory of register monitors.

Conclusion

Our contribution

- A framework for runtime verification which
  - supports monitors that over- or under-approximate quantitative properties
  - enables comparison of such monitors w.r.t. precision and resource use

Future work

- More on precision-resource tradeoffs
- Monitor synthesis problem
- Runtime enforcement