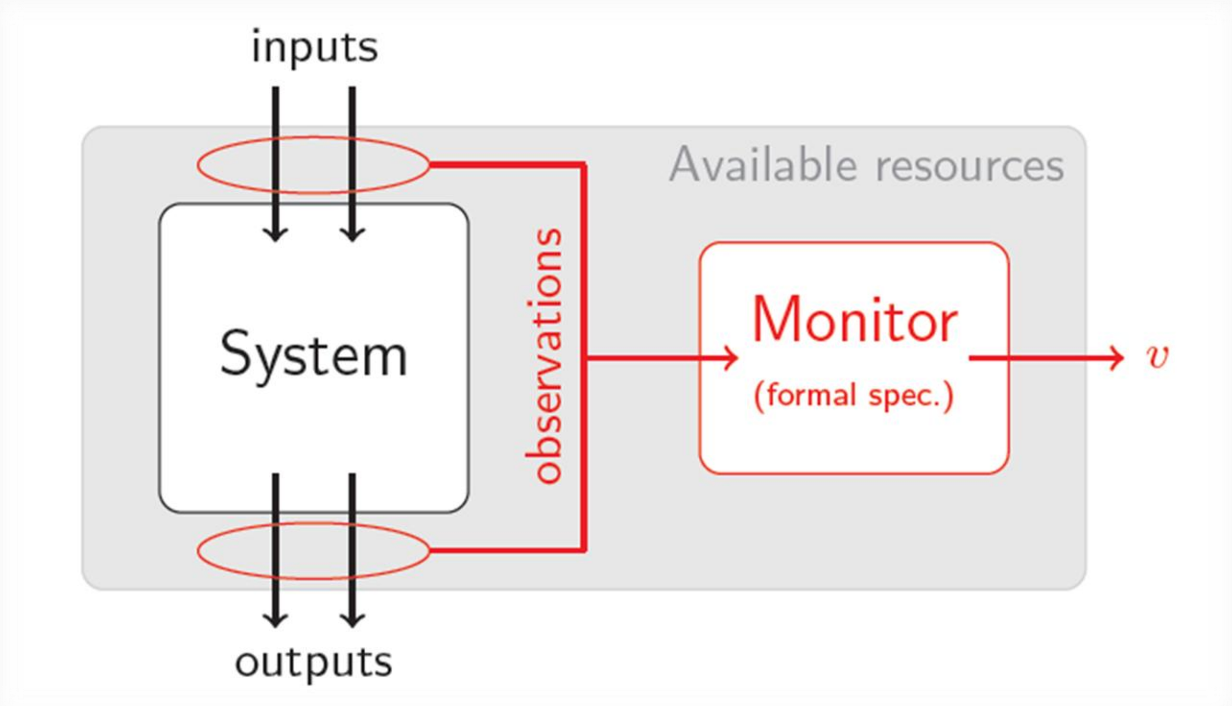
Quantitative Monitoring of Signal First-Order Logic

Marek Chalupa, Thomas A. Henzinger, N. Ege Saraç, Emily Yu

Online Black-Box Monitoring



- Monitor runs in parallel and outputs a stream of verdicts
- Monitor has no knowledge of the system's internals
- Monitor shares resources with the system

Why Monitoring Should Become Ubiquitous

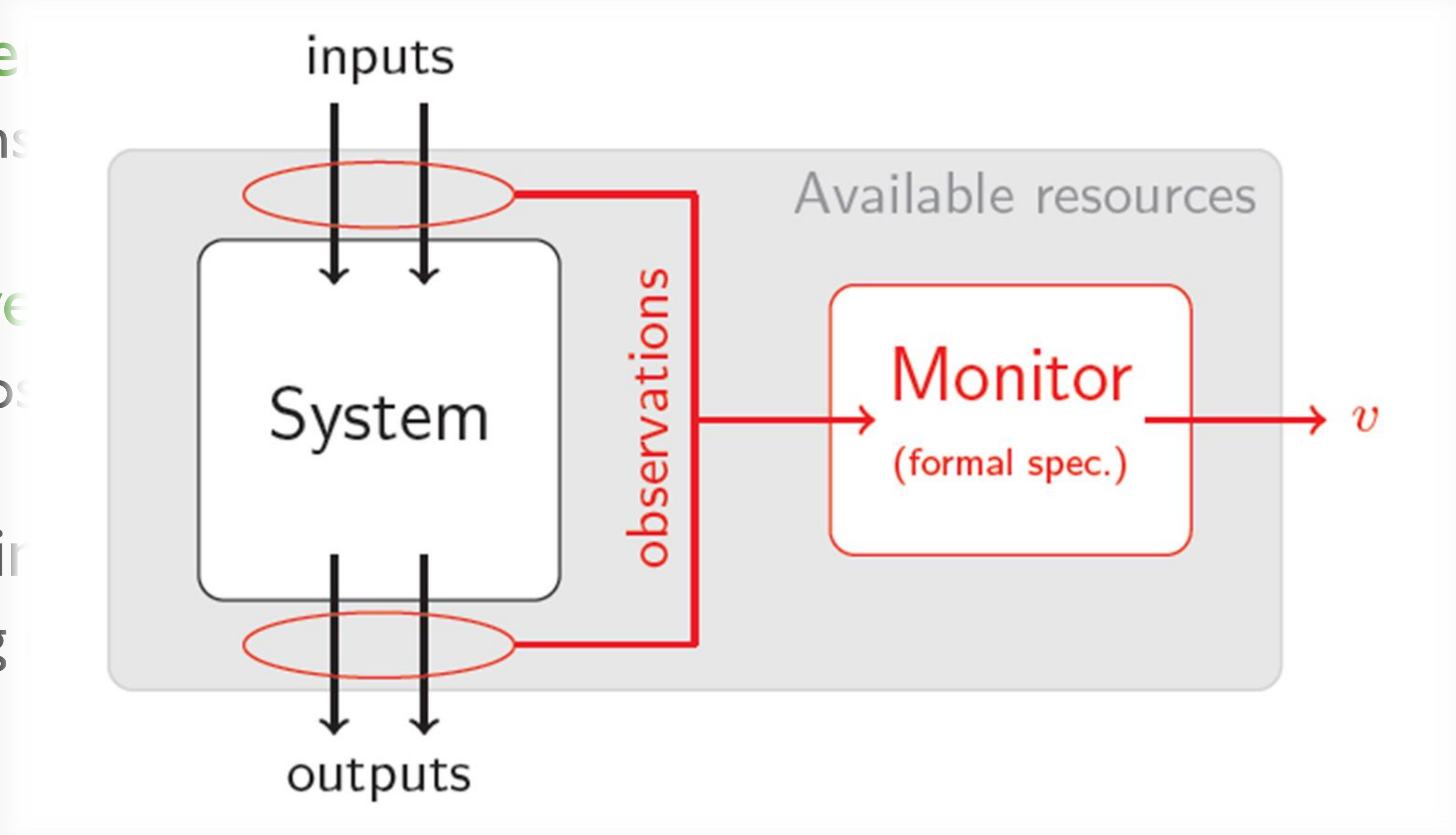
- Increasing software complexity
  - Verification gap
- Increasing hardware power
  - Some resources into assurance
- Inclusion vs. membership
  - More expressive formalisms

Why Monitoring Should be Quantitative

- More interesting specifications
  - Response time, power consumption…
- Fully universal monitoring
  - Best possible estimates at all times
- Natural approximate methods
  - Trading monitor precision against monitor resources

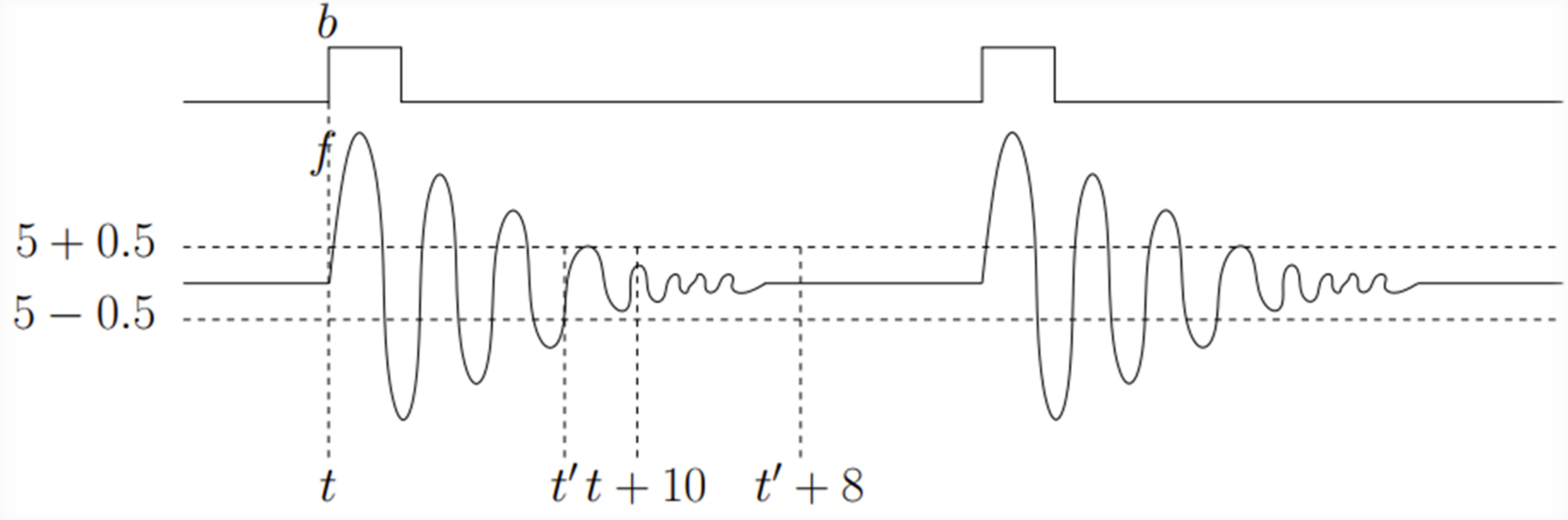
Why Monitoring Should be Quantitative

- More inte
  - Respons
- Fully unive
  - Best pos
- More fittin
  - Trading



Why Signal First-Order Logic (SFO)

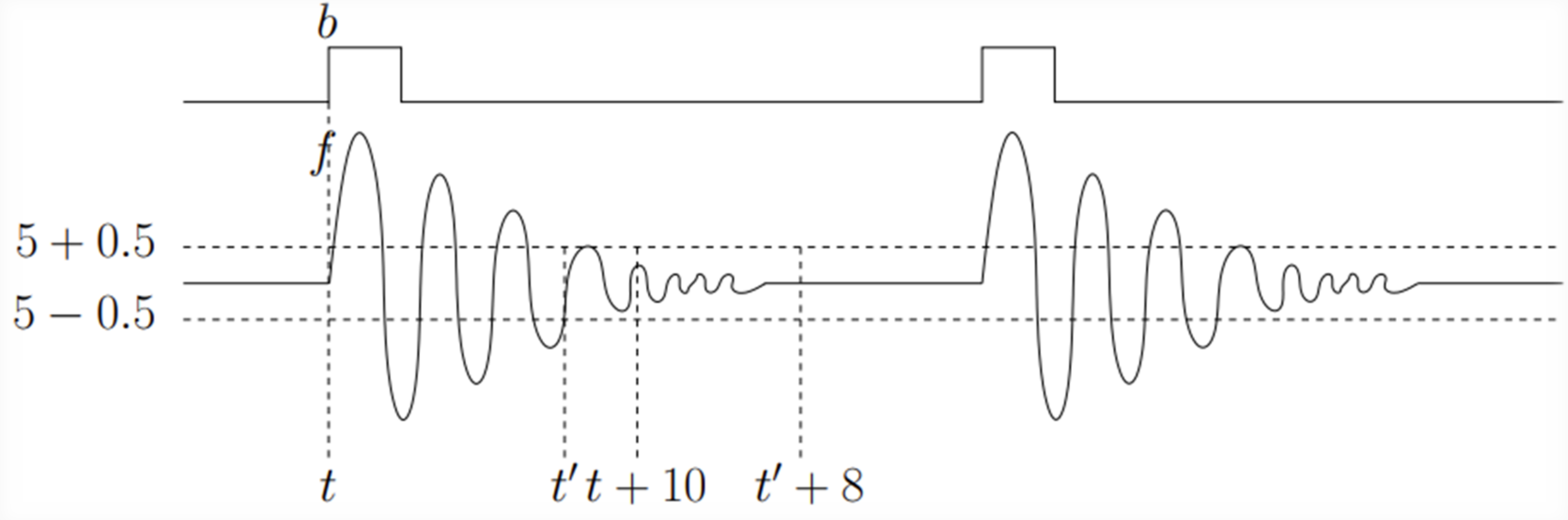
- STL: $\square(\uparrow b \rightarrow \diamond_{[0,10]} \square_{[0,8]}(|f-5| \leq 0.5))$



Maler and Ničković, "Monitoring Temporal Properties of Continuous Signals", FORMATS 2004.

Why Signal First-Order Logic (SFO)

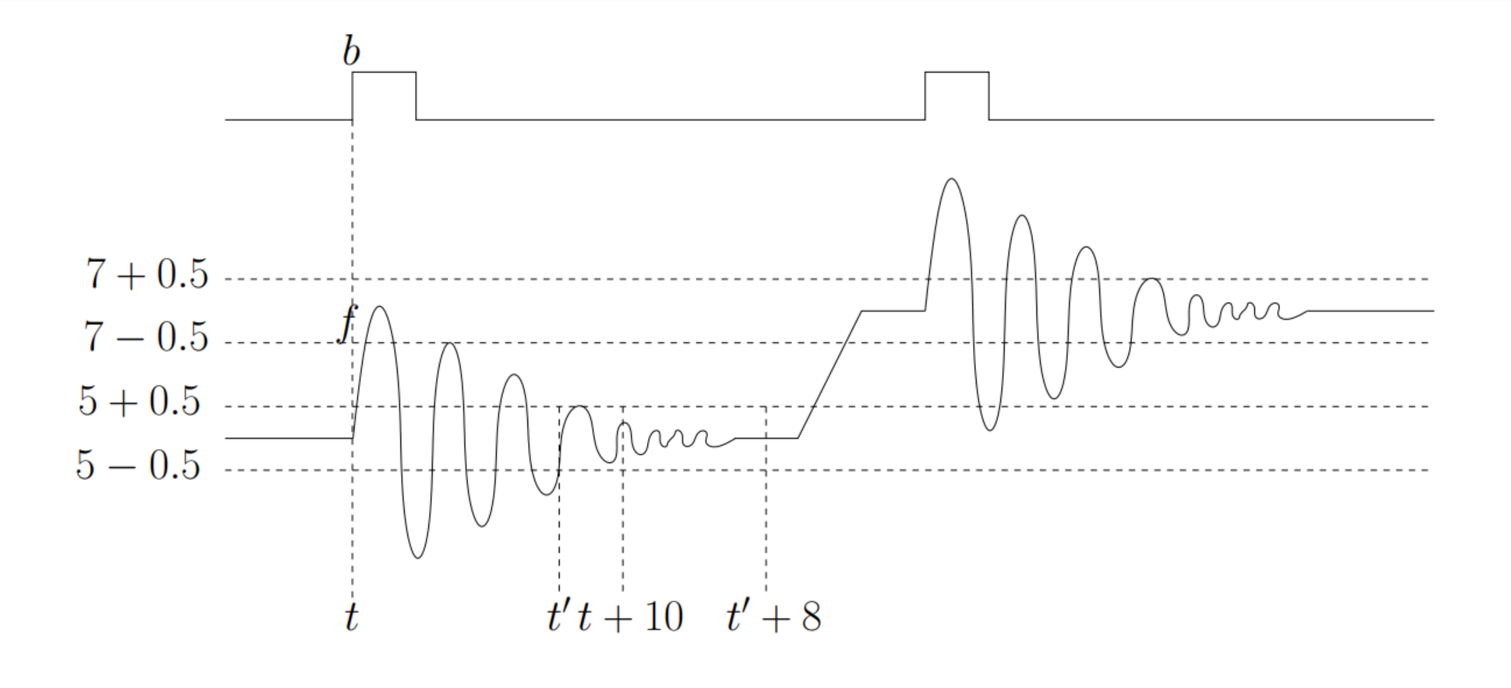
- STL: $\Box(\uparrow b \rightarrow \Diamond_{[0,10]} \Box_{[0,8]}(|f - 5| \leq 0.5)$



Maler and Ničković, "Monitoring Temporal Properties of Continuous Signals", FORMATS 2004.

Why Signal First-Order Logic (SFO)

- SFO: $\uparrow b[t] \rightarrow \exists r \in \mathbb{R}. \exists c \in [0, 10]. \forall d \in [0, 8]. |f(t + c + d) - r| \leq 0.5$



Bakhirkin, Ferrère, Henzinger, and Ničković, "The First-Order Logic of Signals", EMSOFT 2018.

Contributions and Overview

1. Quantitative semantics for SFO
2. Past-time fragment and pastification
3. Online monitoring algorithm
4. Implementation and experiments

Contributions and Overview

1. Quantitative semantics for SFO
2. Past-time fragment and pastification
3. Online monitoring algorithm
4. Implementation and experiments

SFO Boolean Semantics

$$\phi ::= \theta < \theta \mid \neg\phi \mid \phi \vee \phi \mid \exists r \in R.\, \phi \mid \exists s \in I.\, \phi$$

value variables　　time variables

$$\theta ::= \rho \mid \tau$$

$$\rho ::= r \mid f(\tau) \mid n \mid \rho - \rho \mid \rho + \rho$$

value terms

input signals

$$\tau ::= s \mid n \mid \tau - \tau \mid \tau + \tau$$

time terms

trace　　valuation

$$\begin{aligned}
w, \nu \models \theta_1 < \theta_2 &\Leftrightarrow [\![\theta_1]\!]_{w,\nu} < [\![\theta_2]\!]_{w,\nu} \\
w, \nu \models \neg\phi &\Leftrightarrow w, \nu \not\models \phi \\
w, \nu \models \phi_1 \vee \phi_2 &\Leftrightarrow w, \nu \models \phi_1 \ \mathit{or}\ w, \nu \models \phi_2 \\
w, \nu \models \exists r \in R.\, \phi &\Leftrightarrow \exists a \in R : w, \nu[r \leftarrow a] \models \phi \\
w, \nu \models \exists s \in I.\, \phi &\Leftrightarrow \exists a \in I : w, \nu[s \leftarrow a] \models \phi
\end{aligned}$$

$$\begin{aligned}
[\![n]\!]_{w,\nu} &= n \quad (n \in \mathbb{Q}) \\
[\![x]\!]_{w,\nu} &= \nu(x) \quad (x \in \mathcal{X}) \\
[\![\theta_1 \pm \theta_2]\!]_{w,\nu} &= [\![\theta_1]\!]_{w,\nu} \pm [\![\theta_2]\!]_{w,\nu} \\
[\![f(\tau)]\!]_{w,\nu} &= [\![f]\!]_w([\![\tau]\!]_{w,\nu})
\end{aligned}$$

Bakhirkin, Ferrère, Henzinger, and Ničković, "The First-Order Logic of Signals", EMSOFT 2018.

SFO Boolean Semantics

$$\phi ::= \theta < \theta \mid \neg\phi \mid \phi \vee \phi \mid \exists r \in R.\, \phi \mid \exists s \in I.\, \phi$$

value variables

time variables

$$\theta ::= \rho \mid \tau$$

$$\rho ::= r \mid f(\tau) \mid n \mid \rho - \rho \mid \rho + \rho$$

value terms

input signals

$$\tau ::= s \mid n \mid \tau - \tau \mid \tau + \tau$$

time terms

trace

valuation

$$w, \nu \models \theta_1 < \theta_2 \Leftrightarrow [\![\theta_1]\!]_{w,\nu} < [\![\theta_2]\!]_{w,\nu}$$

$$w, \nu \models \neg\phi \Leftrightarrow w, \nu \not\models \phi$$

$$w, \nu \models \phi_1 \vee \phi_2 \Leftrightarrow w, \nu \models \phi_1 \text{ } or \text{ } w, \nu \models \phi_2$$

$$w, \nu \models \exists r \in R.\, \phi \Leftrightarrow \exists a \in R : w, \nu[r \leftarrow a] \models \phi$$

$$w, \nu \models \exists s \in I.\, \phi \Leftrightarrow \exists a \in I : w, \nu[s \leftarrow a] \models \phi$$

$$[\![n]\!]_{w,\nu} = n \quad (n \in \mathbb{Q})$$

$$[\![x]\!]_{w,\nu} = \nu(x) \quad (x \in \mathcal{X})$$

$$[\![\theta_1 \pm \theta_2]\!]_{w,\nu} = [\![\theta_1]\!]_{w,\nu} \pm [\![\theta_2]\!]_{w,\nu}$$

$$[\![f(\tau)]\!]_{w,\nu} = [\![f]\!]_w\big([\![\tau]\!]_{w,\nu}\big)$$

Signal accesses must be well-defined

Bakhirkin, Ferrère, Henzinger, and Ničković, "The First-Order Logic of Signals", EMSOFT 2018.

SFO Quantitative Semantics

$$\phi ::= \theta < \theta \mid \neg\phi \mid \phi \vee \phi \mid \exists r \in R.\, \phi \mid \; \exists s \in I.\, \phi$$

value variables

time variables

$$\theta ::= \rho \mid \tau$$

$$\rho ::= r \mid f(\tau) \mid n \mid \rho - \rho \mid \rho + \rho$$

value terms

input signals

$$\tau ::= s \mid n \mid \tau - \tau \mid \tau + \tau$$

time terms

$$\begin{aligned}
\mu(w, \nu, \theta_1 < \theta_2) &= [\![\theta_2]\!]_{w,\nu} - [\![\theta_1]\!]_{w,\nu} \\
\mu(w, \nu, \neg\phi) &= -\mu(w, \nu, \phi) \\
\mu(w, \nu, \phi_1 \vee \phi_2) &= \max\{\mu(w, \nu, \phi_1), \mu(w, \nu, \phi_2)\} \\
\mu(w, \nu, \exists r \in R.\phi) &= \sup_{a \in R} \mu(w, \nu[r \leftarrow a], \phi) \\
\mu(w, \nu, \exists s \in I.\phi) &= \sup_{a \in I} \mu(w, \nu[s \leftarrow a], \phi)
\end{aligned}$$

SFO Quantitative Semantics

$$\phi ::= \theta < \theta \mid \neg\phi \mid \phi \vee \phi \mid \exists r \in R.\, \phi \mid \exists s \in I.\, \phi$$

value variables

time variables

$$\theta ::= \rho \mid \tau$$

$$\rho ::= r \mid f(\tau) \mid n \mid \rho - \rho \mid \rho + \rho$$

value terms

input signals

$$\tau ::= s \mid n \mid \tau - \tau \mid \tau + \tau$$

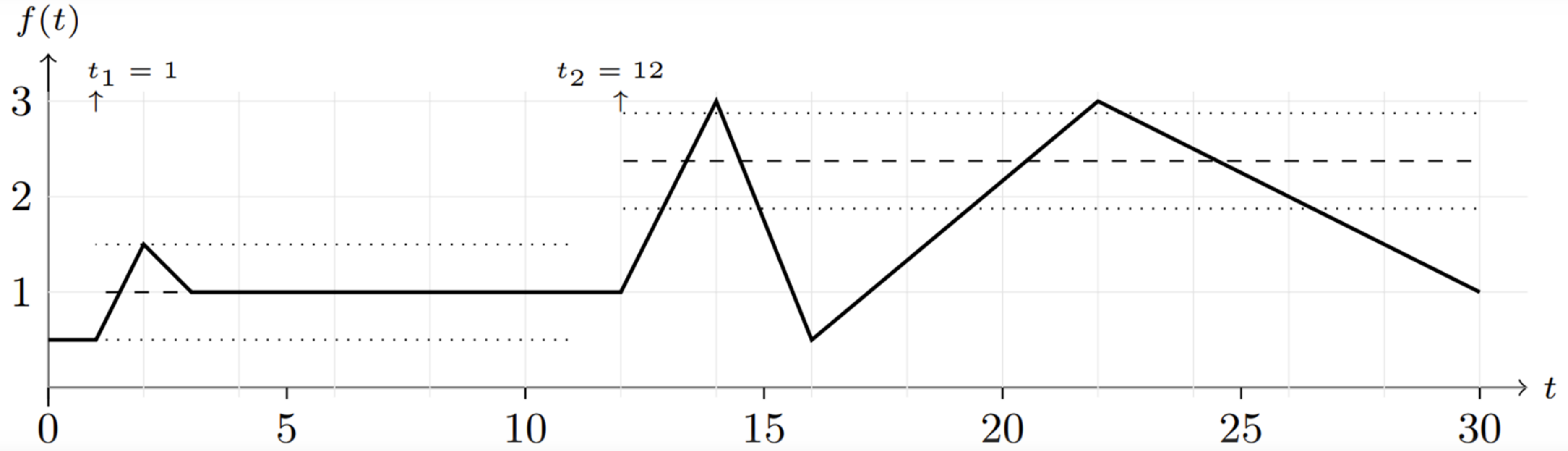
time terms

$$\mu(w, \nu, \theta_1 < \theta_2) = [\![\theta_2]\!]_{w,\nu} - [\![\theta_1]\!]_{w,\nu}$$
$$\mu(w, \nu, \neg\phi) = -\mu(w, \nu, \phi)$$
$$\mu(w, \nu, \phi_1 \vee \phi_2) = \max\{\mu(w, \nu, \phi_1), \mu(w, \nu, \phi_2)\}$$
$$\mu(w, \nu, \exists r \in R.\phi) = \sup_{a \in R} \mu(w, \nu[r \leftarrow a], \phi)$$
$$\mu(w, \nu, \exists s \in I.\phi) = \sup_{a \in I} \mu(w, \nu[s \leftarrow a], \phi)$$

Theorem.
If $\mu(w, \nu, \phi) > 0$, then $w, \nu \models \phi$.
If $\mu(w, \nu, \phi) < 0$, then $w, \nu \not\models \phi$.

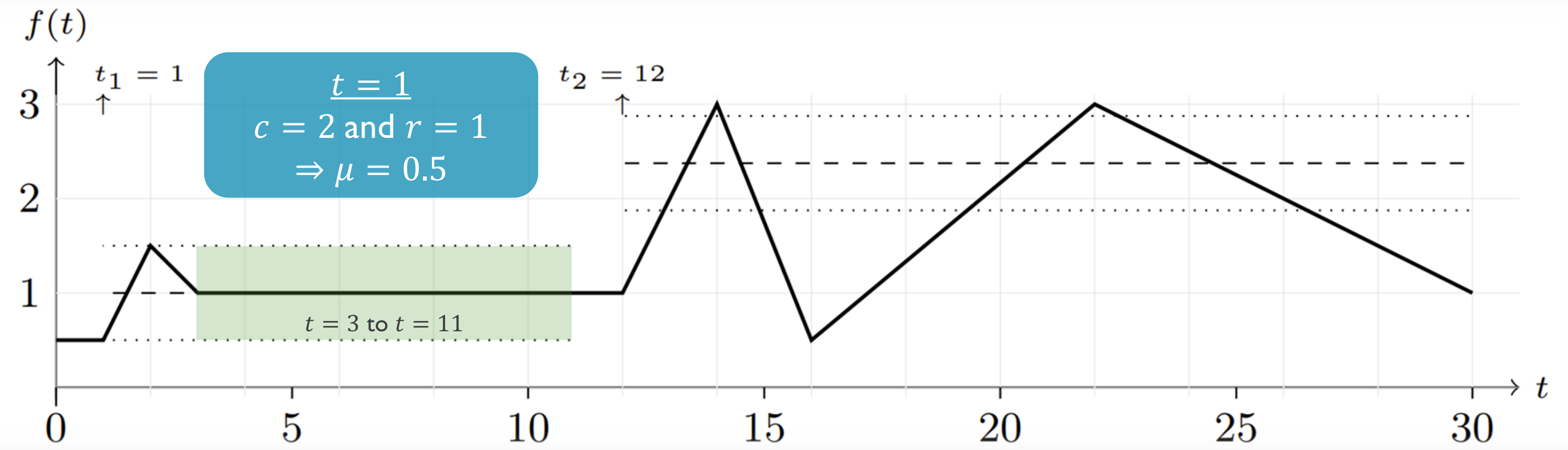
SFO Quantitative Semantics: Example

$$\uparrow b[t] \rightarrow \underbrace{\exists r \in \mathbb{R}. \exists c \in [0,10]. \forall d \in [0,8]. |f(t+c+d) - r| \leq 0.5}_{\sup_{r\in\mathbb{R}} \sup_{c\in[0,10]} \inf_{d\in[0,8]} (0.5 - |f(t+c+d) - r|)}$$



SFO Quantitative Semantics: Example

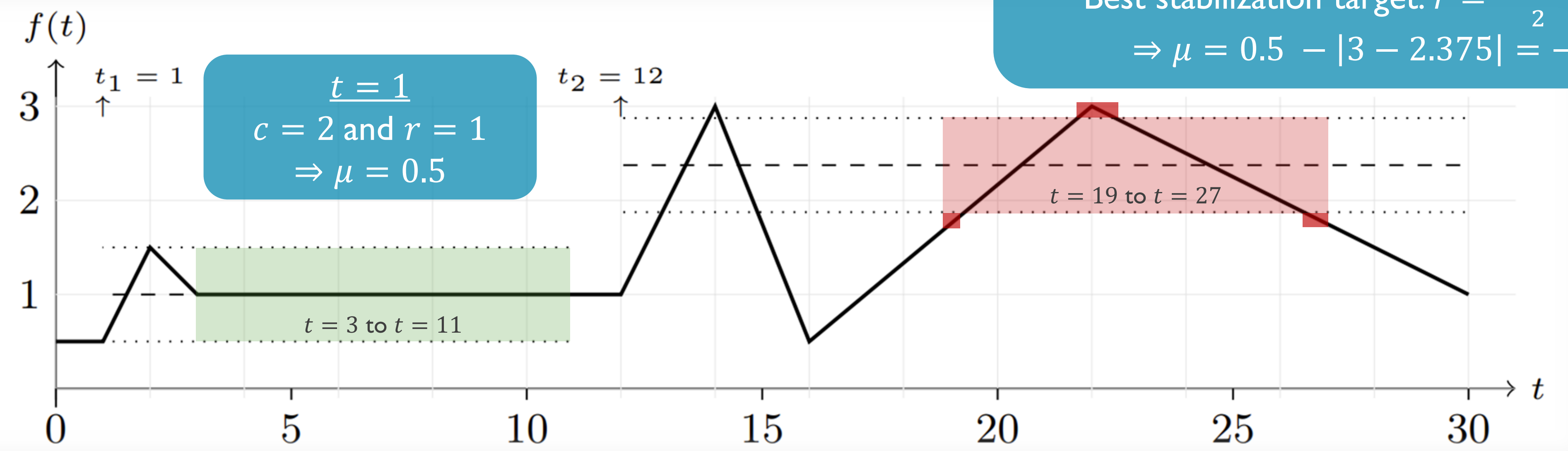
$$\uparrow b[t] \rightarrow \underbrace{\exists r \in \mathbb{R}.\exists c \in [0,10].\forall d \in [0,8].|f(t+c+d) - r| \leq 0.5}_{\sup_{r\in\mathbb{R}} \sup_{c\in[0,10]} \inf_{d\in[0,8]} (0.5 - |f(t+c+d) - r|)}$$



SFO Quantitative Semantics: Example

$$\uparrow b[t] \to \underbrace{\exists r \in \mathbb{R}.\exists c \in [0,10].\forall d \in [0,8].|f(t+c+d) - r| \leq 0.5}_{\sup_{r\in\mathbb{R}} \sup_{c\in[0,10]} \inf_{d\in[0,8]} (0.5 - |f(t+c+d) - r|)}$$

<u>$t = 12$</u>
Best delay: $c = 7$ with min $f = 1.75$ and max $f = 3$
Best stabilization target: $r = \frac{3+1.75}{2} = 2.375$
$\Rightarrow \mu = 0.5 - |3 - 2.375| = -0.125$



Online Quantitative Monitoring

- **Temporal** formulas
  - Exactly one free time variable t and all signal accesses are relative to t
- **Past-time** SFO (pSFO)
  - Evaluation at time t depends only on observations until time t
- **Piecewise-linear** signal interpolation
  - Represent constraints as polyhedra, optimize over them to compute μ

Online Quantitative Monitoring: Algorithm

Input: pSFO formula ϕ and signal stream $w_1, w_2, \ldots$

For $i \geq 1$:

1. Append to $\mathcal{P}_f$ the constraints from w_i; restrict t to current segment.
2. Compute μ recursively.

Require: pSFO formula ϕ; domain-constraints P_d for the current segment
Ensure: list of polyhedra $\mathcal{P}$ and robustness variable v for a subformula on the current segment

if $\phi \equiv (\theta_1 < \theta_2)$ **then**
  $(\mathcal{P}', v') \leftarrow \textsc{Term}(\theta_2 - \theta_1, P_d)$
  return $(\mathcal{P}', v')$
else if $\phi \equiv \neg\phi'$ **then**
  $(\mathcal{P}', v') \leftarrow \textsc{FormulaRobust}(\phi', P_d)$
  $v'' \leftarrow \textsc{FreshVar}()$
  $\mathcal{P}'' \leftarrow \mathcal{P}' \sqcap \{\, v'' = -v' \,\}$
  return $(\textsc{Eliminate}(\{v'\}, \mathcal{P}''), v'')$
else if $\phi \equiv \exists r \in R : \phi'$ **then**
  $(\mathcal{P}', v') \leftarrow \textsc{FormulaRobust}(\phi', P_d \sqcap \{r \in R\})$
  $(\mathcal{P}'', v'') \leftarrow \textsc{EliminateBySup}(\mathcal{P}', v', r, R)$
  return $(\mathcal{P}'', v'')$
else if $\phi \equiv \exists s \in I : \phi'$ **then**
  $(\mathcal{P}', v') \leftarrow \textsc{FormulaRobust}(\phi', P_d \sqcap \{s \in I\})$
  $(\mathcal{P}'', v'') \leftarrow \textsc{EliminateBySup}(\mathcal{P}', v', s, I)$
  return $(\mathcal{P}'', v'')$
else if $\phi \equiv \phi_1 \vee \phi_2$ **then**
  $(\mathcal{P}_1, v_1) \leftarrow \textsc{FormulaRobust}(\phi_1, P_d)$
  $(\mathcal{P}_2, v_2) \leftarrow \textsc{FormulaRobust}(\phi_2, P_d)$
  $v' \leftarrow \textsc{FreshVar}()$
  $\mathcal{P}^1_{\max} \leftarrow \mathcal{P}_1 \sqcap \mathcal{P}_2 \sqcap \{\, v_1 \geq v_2,\ v' = v_1 \,\}$
  $\mathcal{P}^2_{\max} \leftarrow \mathcal{P}_1 \sqcap \mathcal{P}_2 \sqcap \{\, v_1 < v_2,\ v' = v_2 \,\}$
  $\mathcal{P}' \leftarrow \textsc{Eliminate}(\{v_1, v_2\}, \mathcal{P}^1_{\max} \sqcup \mathcal{P}^2_{\max})$
  return $(\mathcal{P}', v')$

Online Quantitative Monitoring: Quantifiers

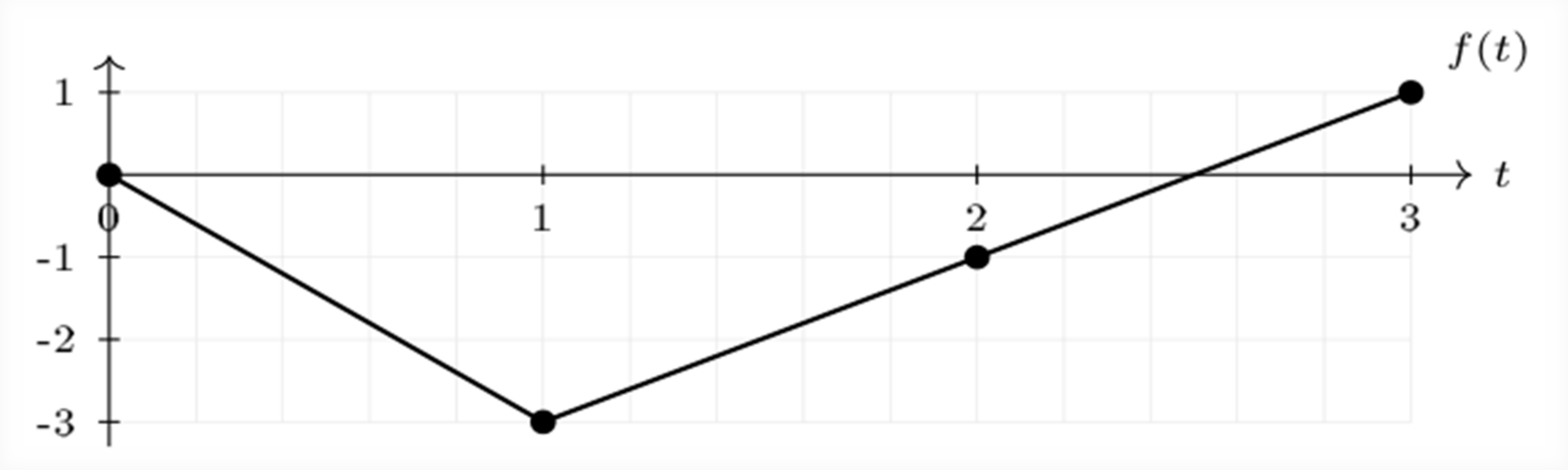
$$\exists x \in I : \phi$$

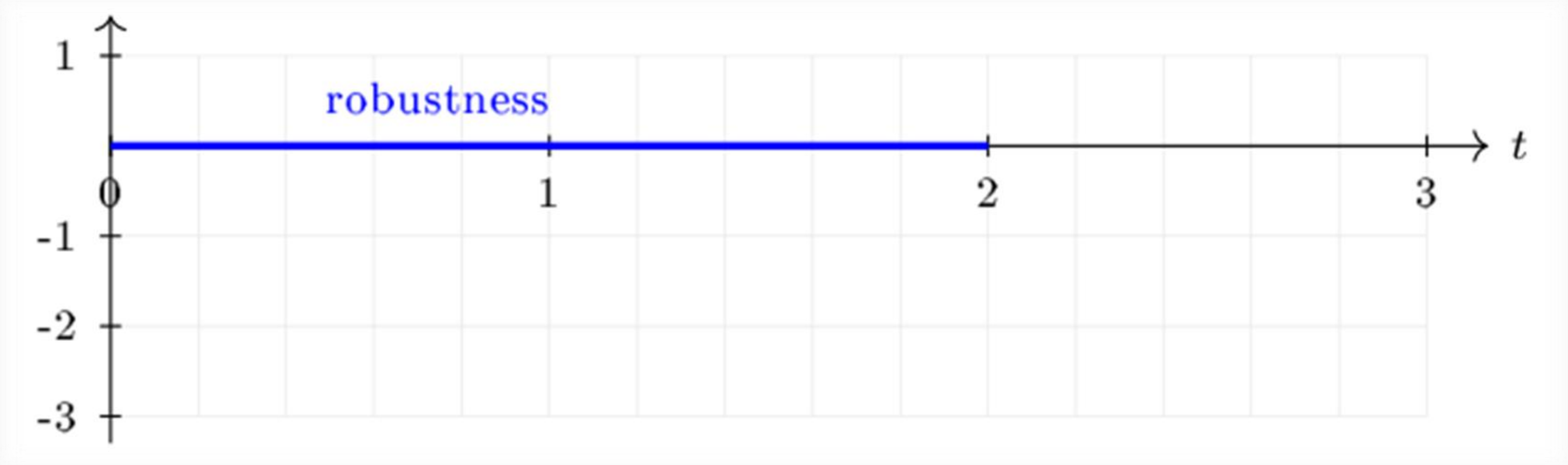
For each polyhedral piece P:

1. Restrict P with $x \in I$.
2. Write the robustness on P as $v = \alpha(Y) \cdot x + \beta(Y)$.
3. Extract the feasible bounds $\ell(Y) \leq x \leq u(Y)$ on x.
4. Choose the best endpoint:
    1. if $\alpha > 0$, choose the largest feasible x;
    2. if $\alpha < 0$, choose the smallest feasible x;
    3. if $\alpha = 0$, choose any feasible x.
5. Substitute the chosen value into v and eliminate x.
6. After processing all pieces, keep only the pointwise maximum.

Online Quantitative Monitoring: Example

$\exists c \in [0,2] : 0 < f(t-c)$

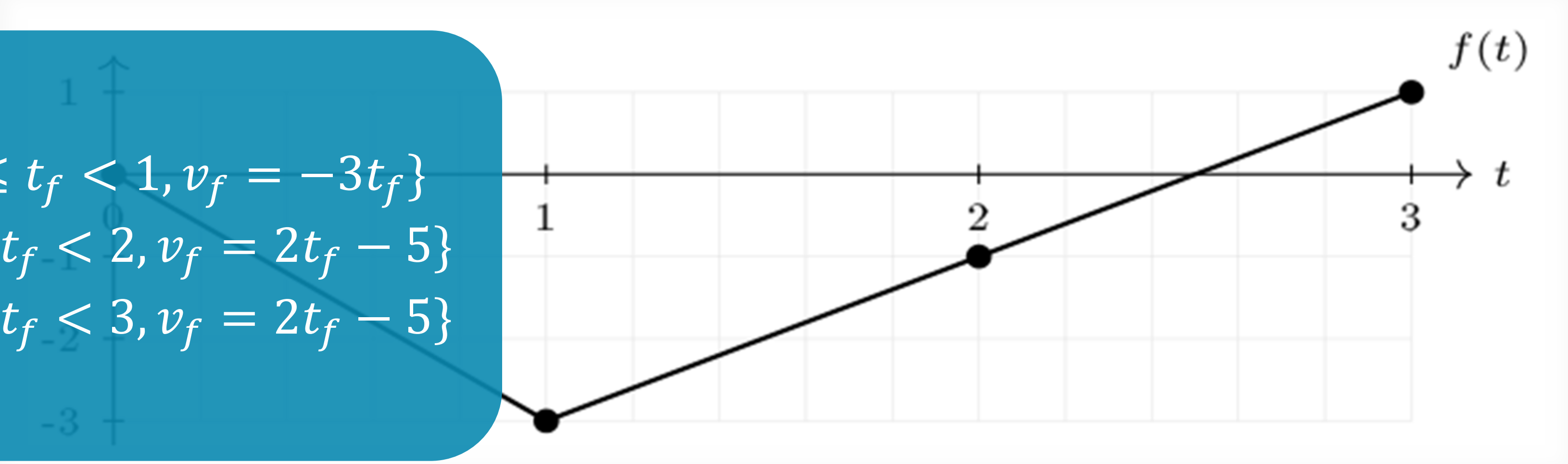


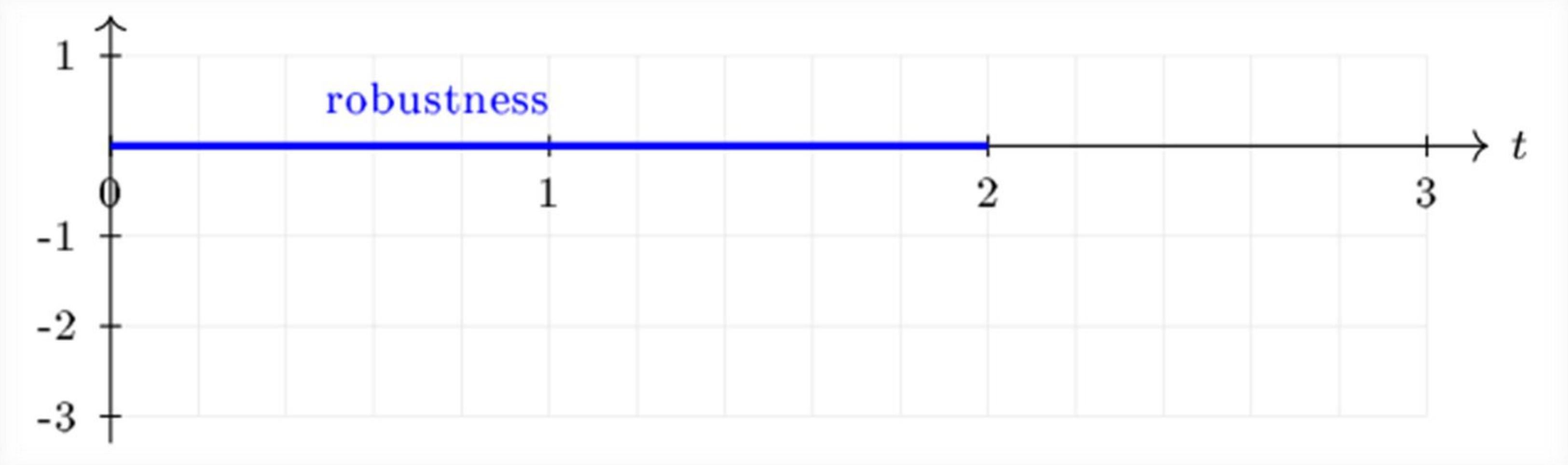


Online Quantitative Monitoring: Example

$\exists c \in [0,2] : 0 < f(t-c)$

$$P_f^1 = \{0 \le t_f < 1, v_f = -3t_f\}$$
$$P_f^2 = \{1 \le t_f < 2, v_f = 2t_f - 5\}$$
$$P_f^3 = \{2 \le t_f < 3, v_f = 2t_f - 5\}$$



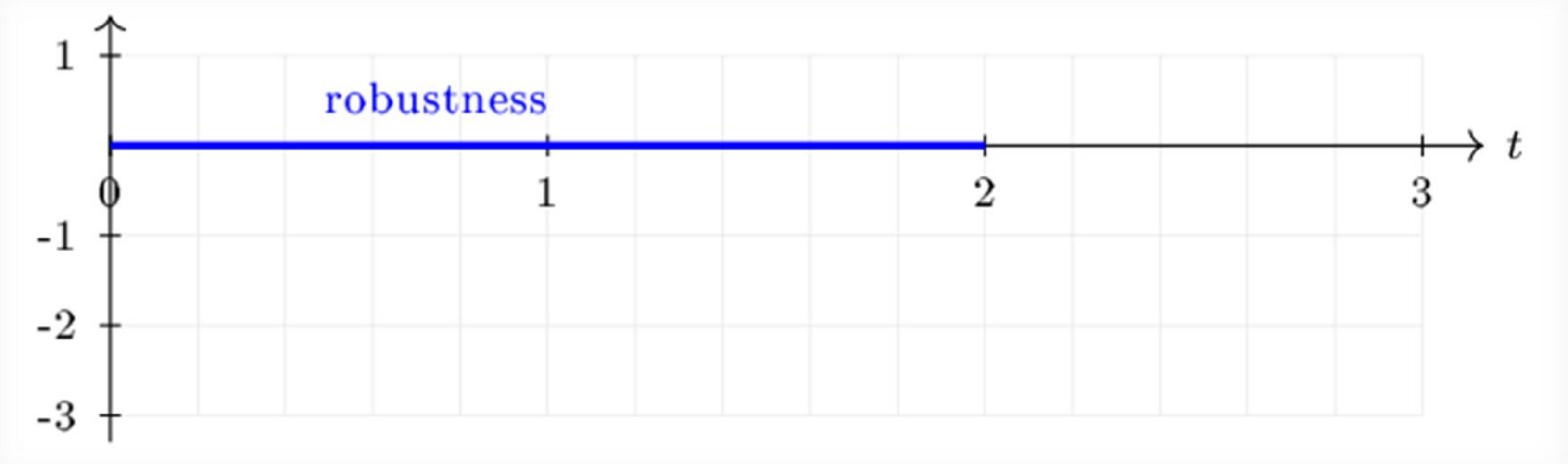


Online Quantitative Monitoring: Example

$\exists c \in [0,2] : 0 < f(t - c)$

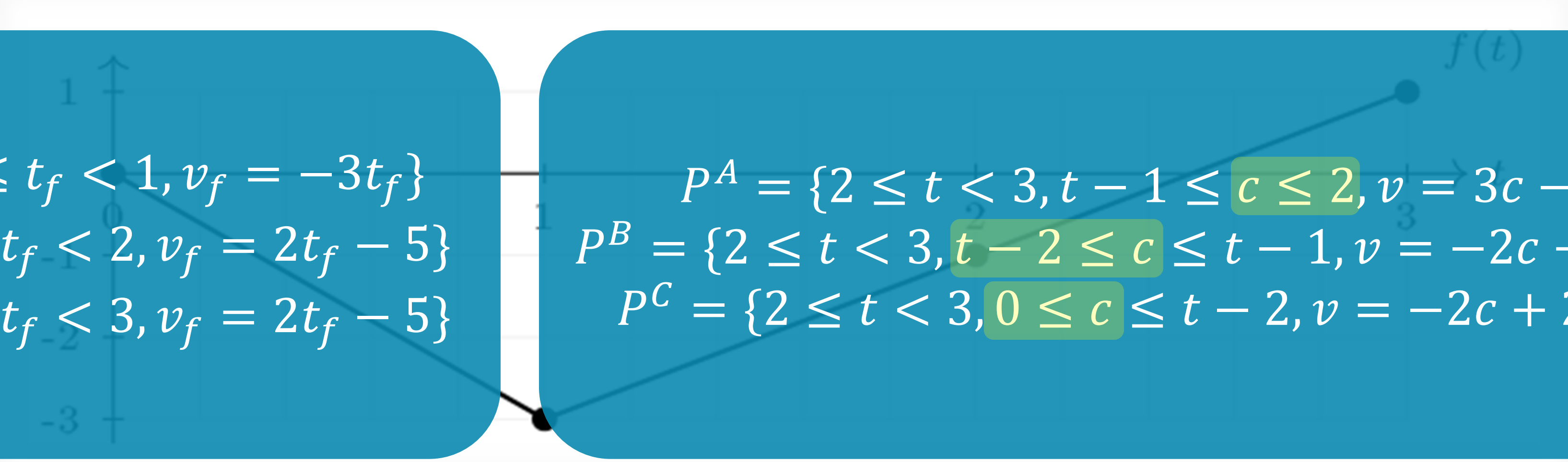
$$P_f^1 = \{0 \leq t_f < 1, v_f = -3t_f\}$$
$$P_f^2 = \{1 \leq t_f < 2, v_f = 2t_f - 5\}$$
$$P_f^3 = \{2 \leq t_f < 3, v_f = 2t_f - 5\}$$

$$P^A = \{2 \leq t < 3, t - 1 \leq c \leq 2, v = 3c - 3t\}$$
$$P^B = \{2 \leq t < 3, t - 2 \leq c \leq t - 1, v = -2c + 2t - 5\}$$
$$P^C = \{2 \leq t < 3, 0 \leq c \leq t - 2, v = -2c + 2t - 5\}$$



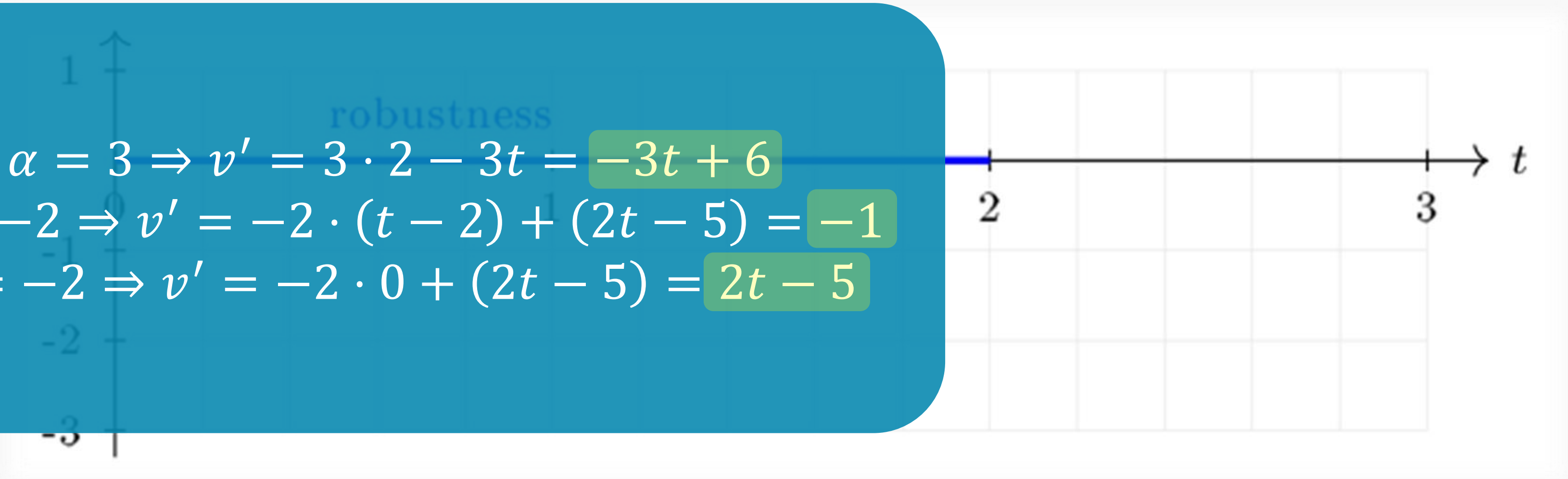
Online Quantitative Monitoring: Example

$\exists c \in [0,2] : 0 < f(t-c)$



$$P_f^1 = \{0 \le t_f < 1, v_f = -3t_f\}$$
$$P_f^2 = \{1 \le t_f < 2, v_f = 2t_f - 5\}$$
$$P_f^3 = \{2 \le t_f < 3, v_f = 2t_f - 5\}$$

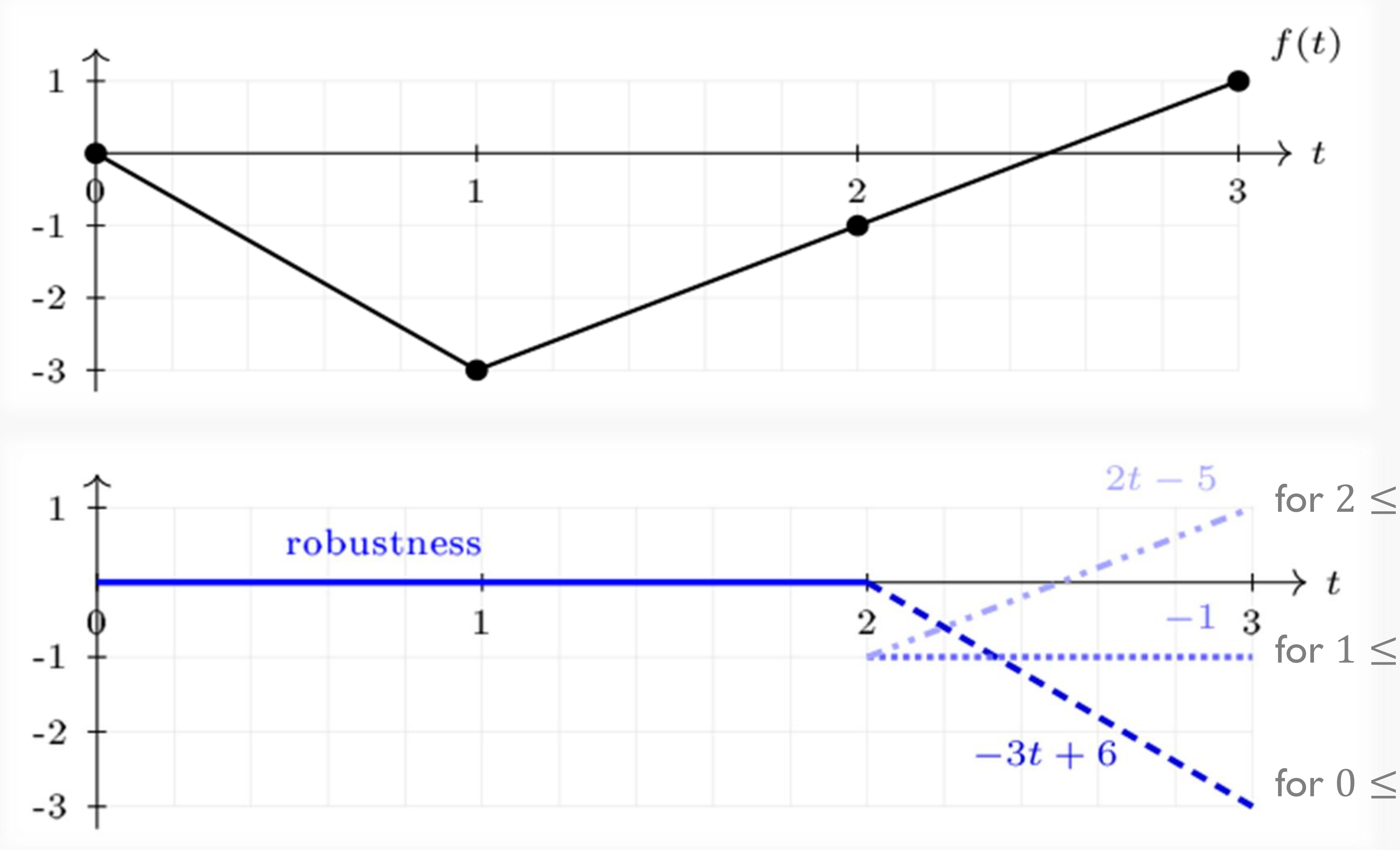
$$P^A = \{2 \le t < 3, t-1 \le c \le 2, v = 3c - 3t\}$$
$$P^B = \{2 \le t < 3, t-2 \le c \le t-1, v = -2c + 2t - 5\}$$
$$P^C = \{2 \le t < 3, 0 \le c \le t-2, v = -2c + 2t - 5\}$$



$$(A)\colon \alpha = 3 \Rightarrow v' = 3 \cdot 2 - 3t = -3t + 6$$
$$(B)\colon \alpha = -2 \Rightarrow v' = -2 \cdot (t-2) + (2t-5) = -1$$
$$(C)\colon \alpha = -2 \Rightarrow v' = -2 \cdot 0 + (2t-5) = 2t - 5$$

Online Quantitative Monitoring: Example

$\exists c \in [0,2] : 0 < f(t-c)$



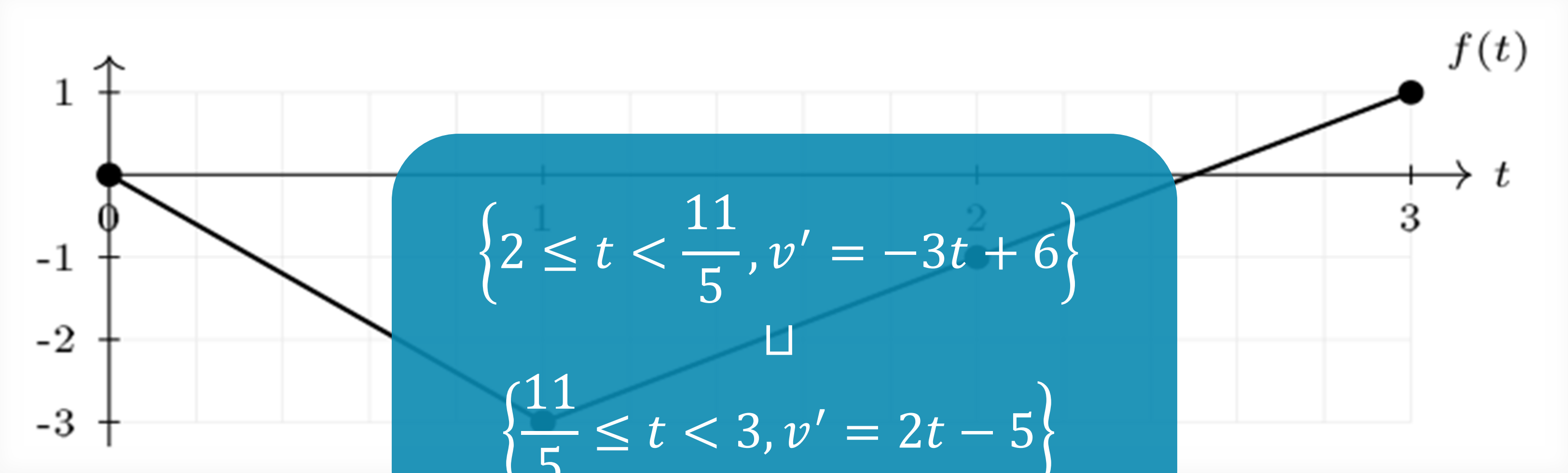
for $2 \leq t - c < 3$

for $1 \leq t - c < 2$

for $0 \leq t - c < 1$

Online Quantitative Monitoring: Example

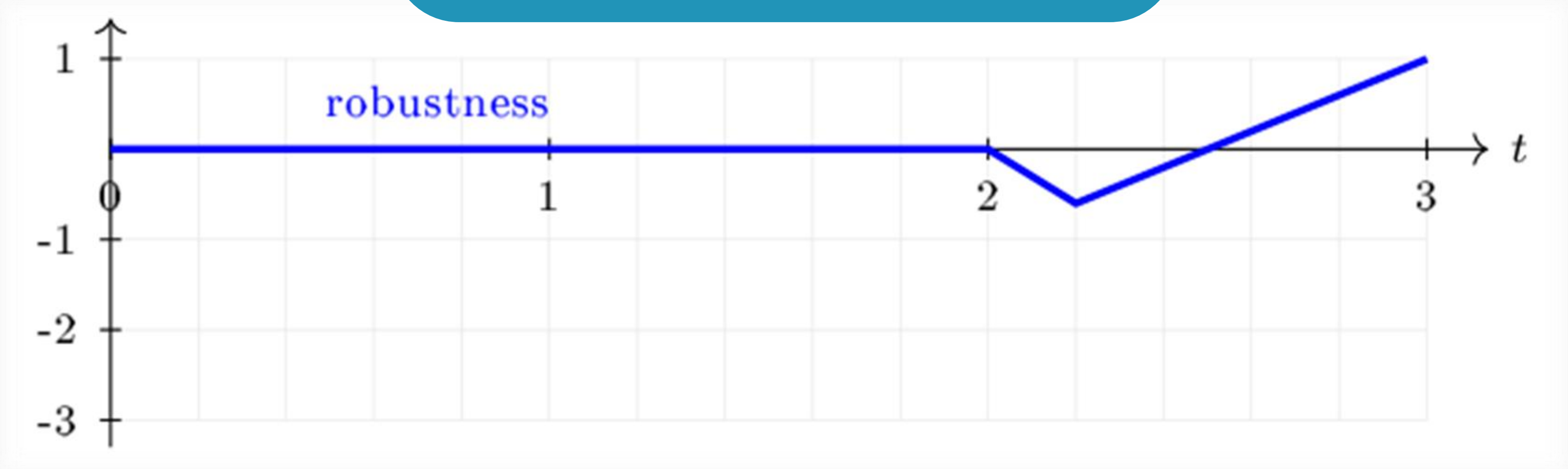
$\exists c \in [0,2] : 0 < f(t-c)$



$$\left\{2 \leq t < \frac{11}{5}, v' = -3t + 6\right\}$$

$$\sqcup$$

$$\left\{\frac{11}{5} \leq t < 3, v' = 2t - 5\right\}$$



Implementation

github.com/ista-vamos/artifact-fm-qsfo

- In Python, using pplpy and SymPy
- SFO parser and quantitative monitoring algorithm
- Some tricks:
  - Unions of convex polyhedra as lists
  - Robustness variable outside polyhedra
  - Fast output interval extraction

Experiments: Dynamic Obstacle Avoidance

	Sampling period: $0.1s$			
	Avoidance			
	P1	*P2*	*P3*	*P1 + P2 + P3*
Time (s) per segment:	0.002	0.005	0.014	0.021

- P1 (safe velocity): $t > 2 \Rightarrow \bigwedge_{i\in\{x,y,z\}} |v_i(t)| < 1$
- P2 (motion smoothness): $\bigwedge_{i\in\{x,y,z\}} |v_i(t) - v_i(t-0.1)| < 0.01$
- P3 (obstacle separation): $\bigwedge_{i\in\{x,y,z\}} \bigwedge_{1\le j\le 8} \left|pos_i(t) - obs_{i,j}(t)\right| > 0.5$

Qin, Zhang, Chen, Chen, and Fan, "Learning Safe Multi-Agent Control with Decentralized Neural Barrier Certificates", ICLR 2021.

Experiments: F16 Altitude Control

Sampling period: $0.033s$

	Altitude Control			
	$P1$	$P2$	$P3$	$P1 + P2 + P3$
Time (s) per segment:	0.002	0.002	0.210	0.532

- P1 (safe altitude): $1000 \leq alt(t) \leq 45000$
- P2 (safe airspeed): $150 \leq v(t) \leq 1500$
- P3 (altitude recovery): $alt(t) < 1640 \Rightarrow \exists t_r \in [0,10]: \forall t_h \in [0,10]: alt(t + t_r + t_h) \geq 2300$

Heidlauf, Collins, Bolender, and Bak, "Verification Challenges in F-16 Ground Collision Avoidance and Other Automated Maneuvers", ARCH 2018.

Experiments: F16 Altitude Control

Sampling period: $0.033s$

	Altitude Control			
	$P1$	$P2$	$P3$	$P1 + P2 + P3$
Time (s) per segment:	0.002	0.002	0.210	0.532

~98% of time spent on signal lookup
+
can be made ~40x faster by filtering empty intersections

- P1 (safe altitude): $1000 \leq alt(t) \leq 45000$
- P2 (safe airspeed): $150 \leq v(t) \leq 1500$
- P3 (altitude recovery): $alt(t) < 1640 \Rightarrow \exists t_r \in [0{,}10]: \forall t_h \in [0{,}10]: alt(t + t_r + t_h) \geq 2300$

Heidlauf, Collins, Bolender, and Bak, "Verification Challenges in F-16 Ground Collision Avoidance and Other Automated Maneuvers", ARCH 2018.

Conclusion

Contributions

1. Quantitative semantics for SFO
2. Past-time fragment and pastification
3. Online monitoring algorithm
4. Implementation and experiments

Future Work

1. SFO-based neural predictive control
2. Certified approximate monitoring

Thank you!