A Symbolic Execution Semantics for TopHat

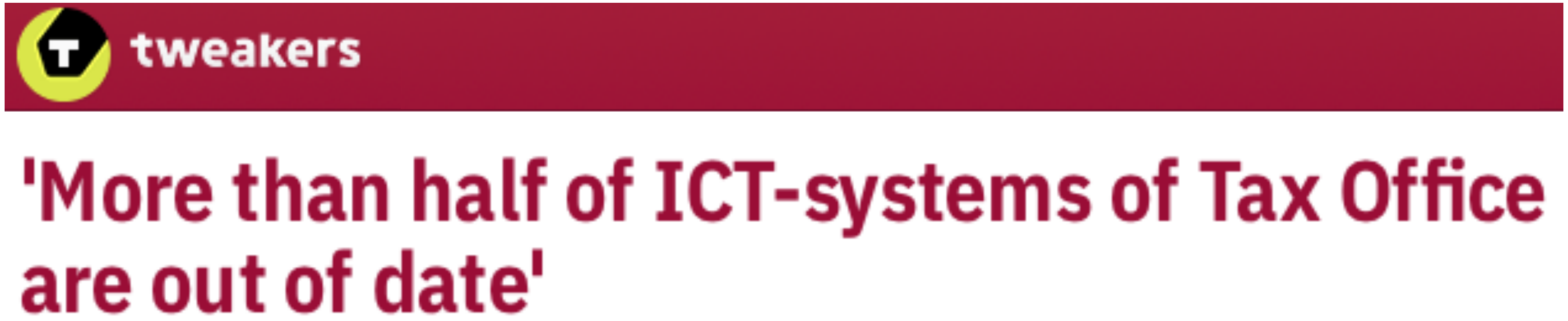
Markus Klinik
PhD Candidate
Radboud University

KUSTWACHT

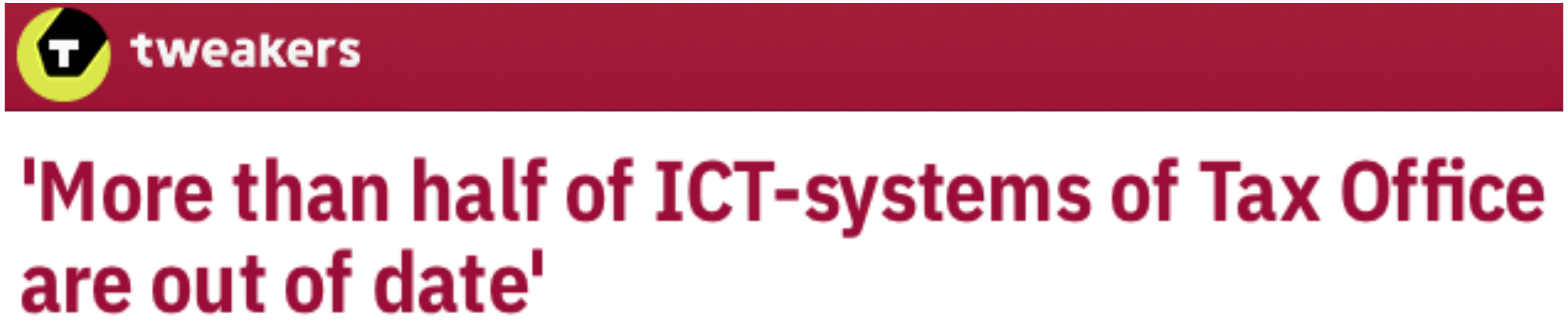
PHILIPS
ALPHATRON Medical
VUmc

Belastingdienst

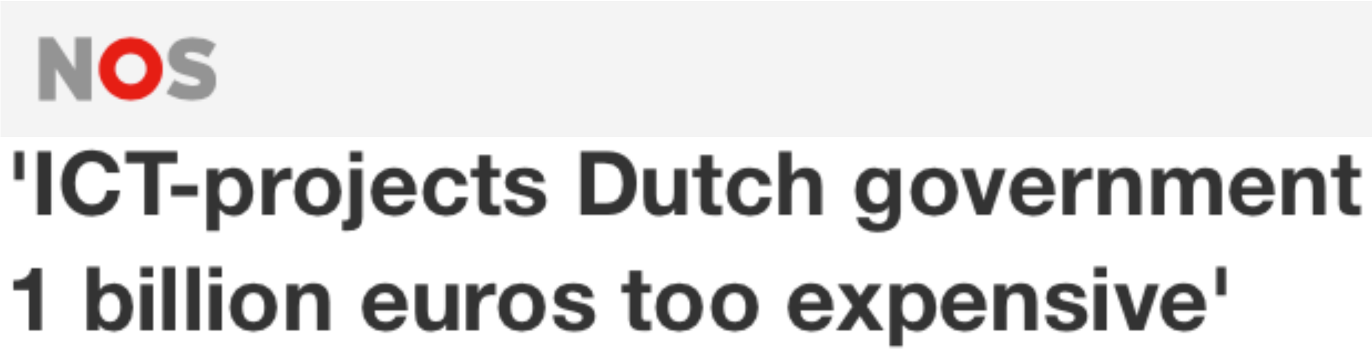
F802



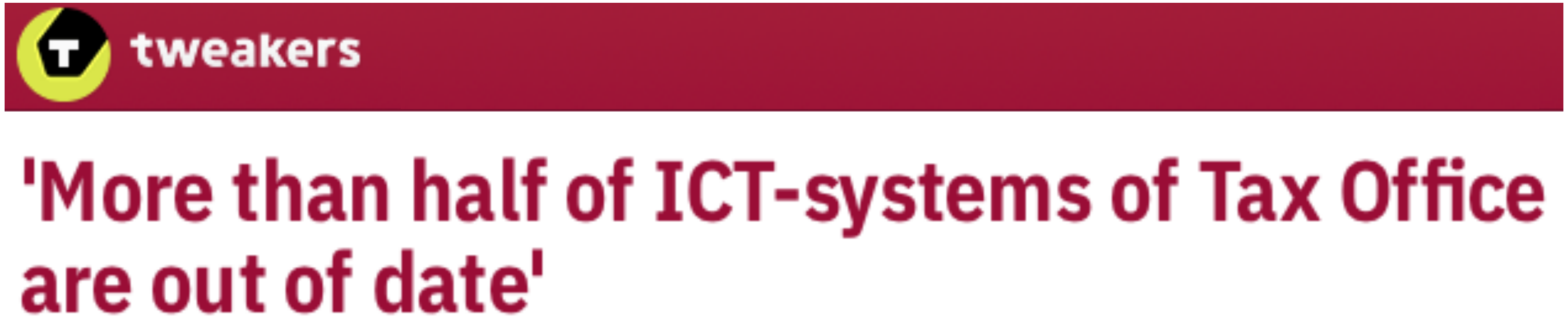
'More than half of ICT-systems of Tax Office are out of date'



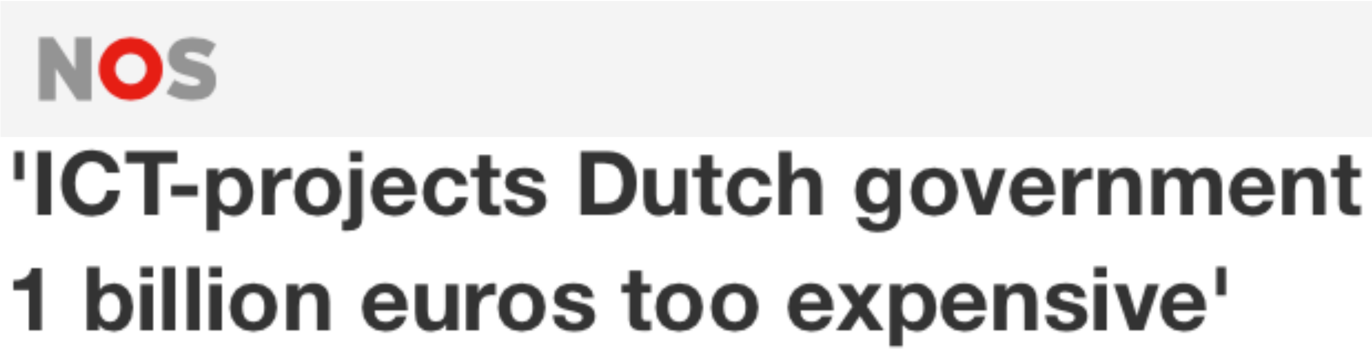
'More than half of ICT-systems of Tax Office are out of date'



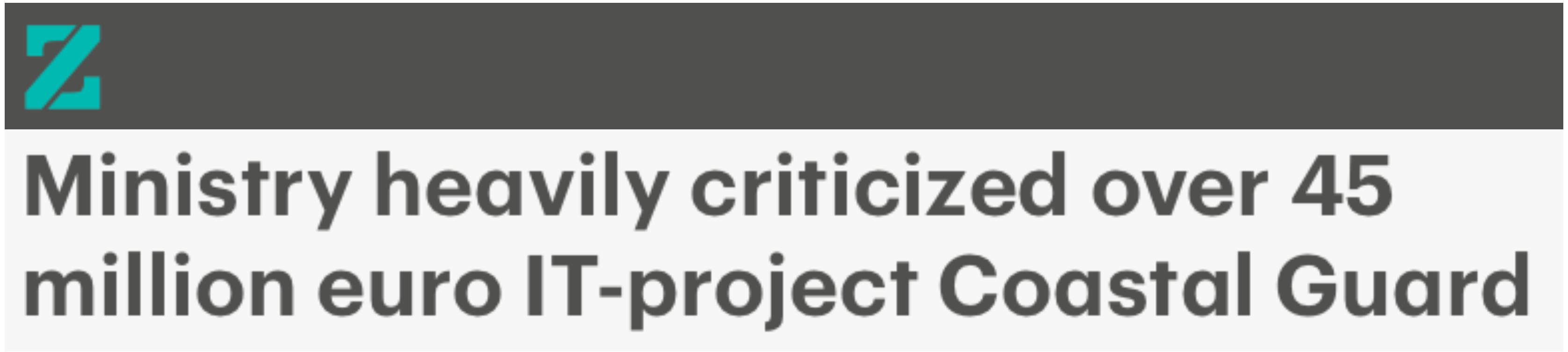
'ICT-projects Dutch government 1 billion euros too expensive'



'More than half of ICT-systems of Tax Office are out of date'

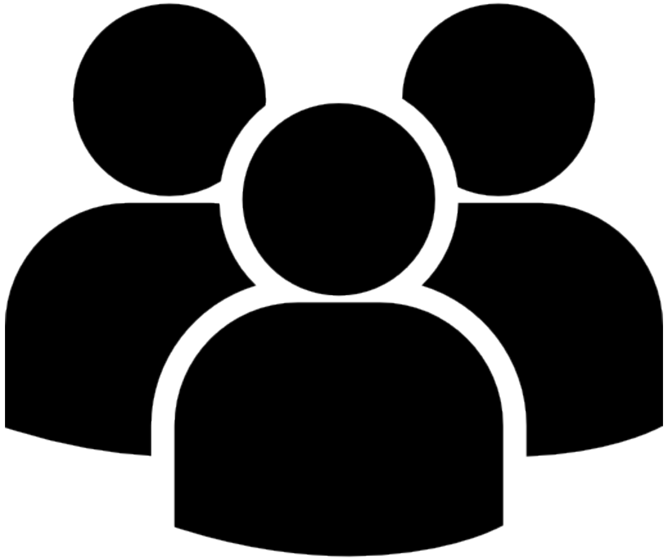


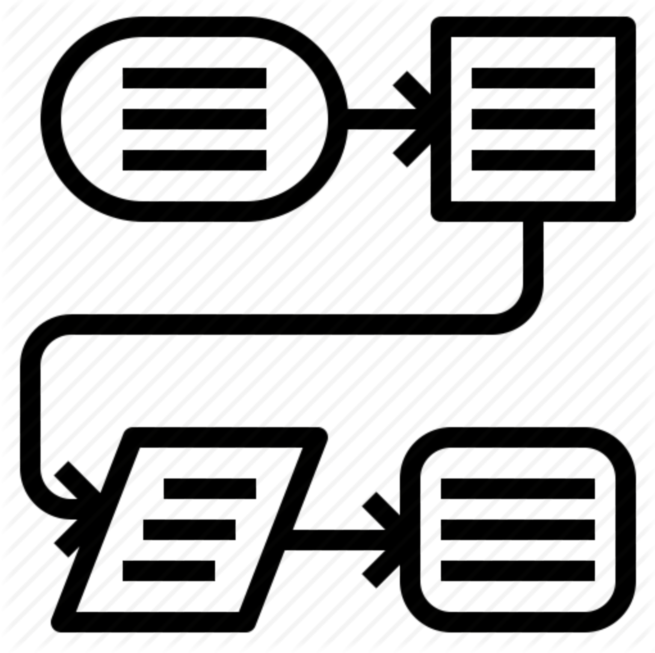
'ICT-projects Dutch government 1 billion euros too expensive'



Ministry heavily criticized over 45 million euro IT-project Coastal Guard

Workflow Systems





Task-Oriented Programming

TOP Languages

itasks

task-oriented programming framework

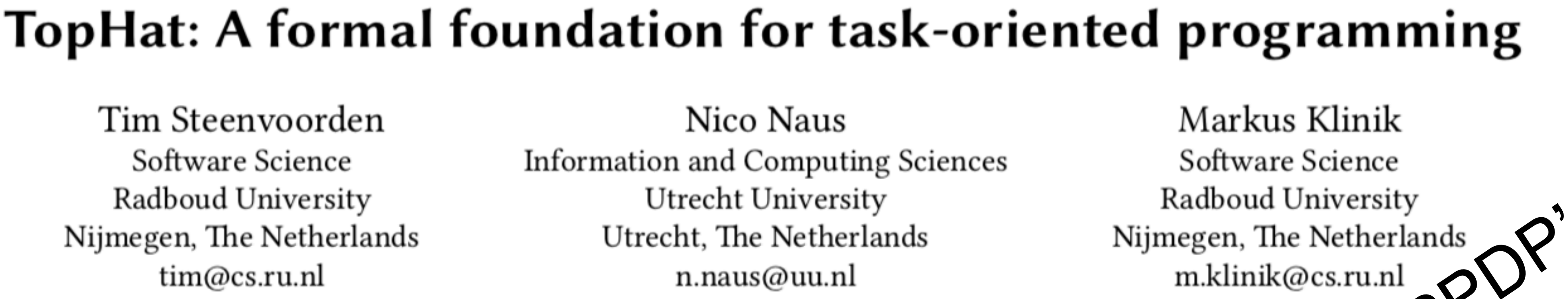
iTasks.org Rinus Plasmijer, Peter Achten, Bas Lijnse, and many more

TOP Languages

itasks

task-oriented programming framework

iTasks.org Rinus Plasmijer, Peter Achten, Bas Lijnse, and many more



TopHat: A formal foundation for task-oriented programming

Tim Steenvoorden
Software Science
Radboud University
Nijmegen, The Netherlands
tim@cs.ru.nl

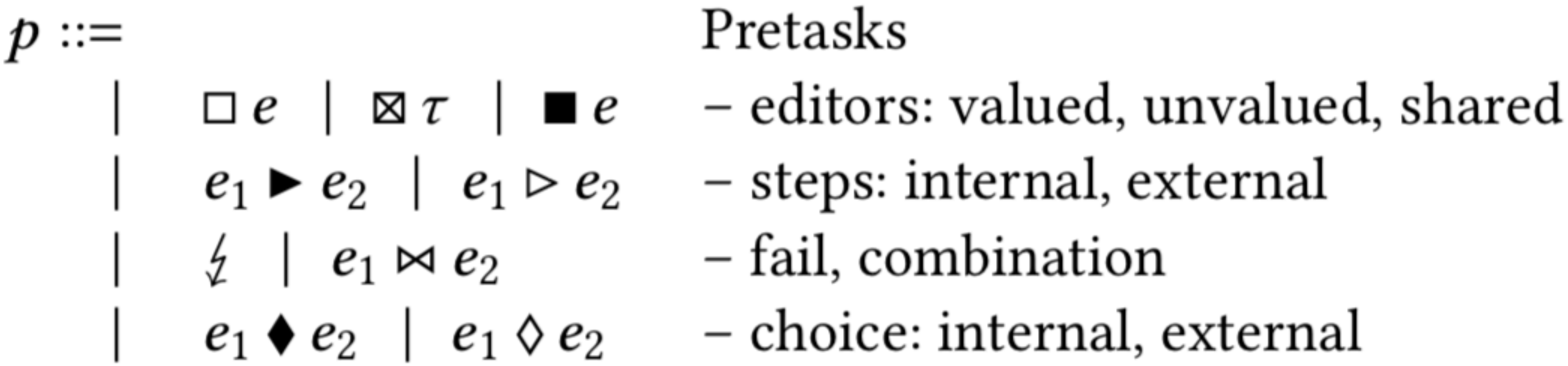
Nico Naus
Information and Computing Sciences
Utrecht University
Utrecht, The Netherlands
n.naus@uu.nl

Markus Klinik
Software Science
Radboud University
Nijmegen, The Netherlands
m.klinik@cs.ru.nl

PPDP’19

The TopHat Programming Language

TopHat



$$\begin{array}{lll}
p ::= & & \text{Pretasks} \\
\mid & \square\, e \mid \boxtimes\, \tau \mid \blacksquare\, e & \text{– editors: valued, unvalued, shared} \\
\mid & e_1 \blacktriangleright e_2 \mid e_1 \triangleright e_2 & \text{– steps: internal, external} \\
\mid & \lightning \mid e_1 \bowtie e_2 & \text{– fail, combination} \\
\mid & e_1 \blacklozenge e_2 \mid e_1 \Diamond e_2 & \text{– choice: internal, external}
\end{array}$$

Example

Example

- Within 365 days
- Confirmation from installation company
- Approval from tax office
- Maximum of 600 euros

Example

$$\textbf{let}\ \text{provideDocuments} = \boxtimes\text{Amount} \bowtie \boxtimes\text{Date}\ \textbf{in}$$

$$\textbf{let}\ \text{companyConfirm} = \square\text{True} \lozenge \square\text{False}\ \textbf{in}$$

$$\begin{aligned}&\textbf{let}\ \text{officerApprove} = \lambda \mathit{invoiceDate}.\ \lambda \mathit{today}.\ \lambda \mathit{confirmed}.\\ &\quad \square\text{False} \lozenge \textbf{if}\ (\mathit{today} - \mathit{invoiceDate} < 365 \wedge \mathit{confirmed})\ \ \textbf{then}\ \square\text{True}\ \textbf{else}\ \lightning\ \ \textbf{in}\end{aligned}$$

$$\begin{aligned}&\text{getCurrentDate} \blacktriangleright \lambda \mathit{today}.\\ &\text{provideDocuments} \bowtie \text{companyConfirm} \blacktriangleright\\ &\quad \lambda\langle\langle \mathit{invoiceAmount}, \mathit{invoiceDate}\rangle\ , \mathit{confirmed}\rangle\ .\\ &\quad \text{officerApprove}\ \mathit{invoiceDate}\ \mathit{today}\ \mathit{confirmed} \blacktriangleright \lambda \mathit{approved}.\end{aligned}$$

$$\textbf{let}\ \text{subsidyAmount} = \textbf{if}\ \mathit{approved}\ \textbf{then}\ \min 600\ (\mathit{invoiceAmount} / 10)\ \textbf{else}\ 0\ \textbf{in}$$

$$\square\langle \text{subsidyAmount}, \mathit{approved}, \mathit{confirmed}, \mathit{invoiceDate}, \mathit{today}\rangle$$

Symbolic Execution

```
λ (x,y) : (Int,Int) →
  if (x<y)
    then (y,x)
    else (x,y)
```

Symbolic Execution

```
λ (x,y) : (Int,Int) →
  if (x<y)
    then (y,x)
    else (x,y)
```

Path constraint: s1 < s2
(s2,s1)

Symbolic Execution

```
λ (x,y) : (Int,Int) →
  if (x<y)
    then (y,x)
    else (x,y)
```

Path constraint: s1 < s2
(s2,s1)

Path constraint: s1 >= s2
(s1,s2)

Symbolic Execution

```
λ (x,y) : (Int,Int) →
  if (x<y)
    then (y,x)
    else (x,y)
```

Path constraint: s1 < s2
(s2,s1)

Path constraint: s1 >= s2
(s1,s2)

$$\psi(a, b) = a \geq b$$

Symbolic TopHat

Symbolic TopHat

$$\textsc{H-Fill}\qquad \frac{}{\boxtimes\,\tau, \hat{\sigma} \xrightarrow{v} \square\, v, \hat{\sigma}}\; v : \tau$$

Symbolic TopHat

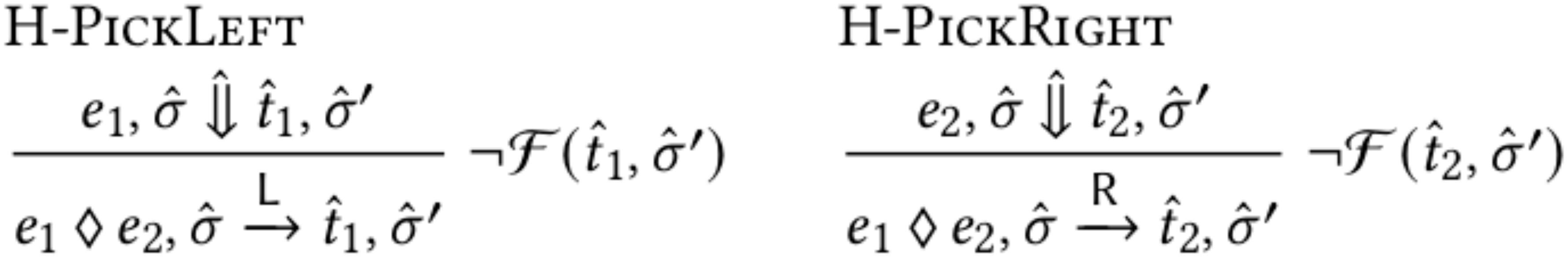
H-Fill

$$\frac{}{\boxtimes\, \tau, \hat{\sigma} \xrightarrow{v} \square\, v, \hat{\sigma}}\; v : \tau$$

SH-Fill

$$\frac{\text{fresh } s}{\boxtimes\, \tau, \sigma \;\rightarrow\; \square\, s, \sigma,\; s, \text{True}}\; s : \tau$$

Symbolic TopHat



H-PickLeft

$$\frac{e_1, \hat{\sigma} \mathrel{\hat{\Downarrow}} \hat{t}_1, \hat{\sigma}'}{e_1 \lozenge e_2, \hat{\sigma} \xrightarrow{\mathsf{L}} \hat{t}_1, \hat{\sigma}'} \; \neg\mathcal{F}(\hat{t}_1, \hat{\sigma}')$$

H-PickRight

$$\frac{e_2, \hat{\sigma} \mathrel{\hat{\Downarrow}} \hat{t}_2, \hat{\sigma}'}{e_1 \lozenge e_2, \hat{\sigma} \xrightarrow{\mathsf{R}} \hat{t}_2, \hat{\sigma}'} \; \neg\mathcal{F}(\hat{t}_2, \hat{\sigma}')$$

Symbolic TopHat

H-PickLeft

$$\frac{e_1, \hat{\sigma} \mathrel{\hat{\Downarrow}} \hat{t}_1, \hat{\sigma}'}{e_1 \Diamond e_2, \hat{\sigma} \xrightarrow{\mathsf{L}} \hat{t}_1, \hat{\sigma}'} \; \neg\mathcal{F}(\hat{t}_1, \hat{\sigma}')$$

H-PickRight

$$\frac{e_2, \hat{\sigma} \mathrel{\hat{\Downarrow}} \hat{t}_2, \hat{\sigma}'}{e_1 \Diamond e_2, \hat{\sigma} \xrightarrow{\mathsf{R}} \hat{t}_2, \hat{\sigma}'} \; \neg\mathcal{F}(\hat{t}_2, \hat{\sigma}')$$

SH-Pick

$$\frac{e_1, \sigma \;\Downarrow\; \overline{t_1, \; \sigma_1, \varphi_1} \qquad e_2, \sigma \;\Downarrow\; \overline{t_2, \; \sigma_2, \varphi_2}}{e_1 \Diamond e_2, \sigma \;\rightarrow\; \overline{t_1, \sigma_1, \mathsf{L}, \varphi_1} \cup \overline{t_2, \sigma_2, \mathsf{R}, \varphi_2}} \; \neg\mathcal{F}(t_1, \sigma_1) \wedge \neg\mathcal{F}(t_2, \sigma_2)$$

Symbolic TopHat

E-IfTrue

$$\frac{e_1, \hat{\sigma} \mathrel{\hat{\downarrow}} \mathsf{True}, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \mathrel{\hat{\downarrow}} \hat{v}_2, \hat{\sigma}''}{\textbf{if}\; e_1 \;\textbf{then}\; e_2 \;\textbf{else}\; e_3, \hat{\sigma} \mathrel{\hat{\downarrow}} \hat{v}_2, \hat{\sigma}''}$$

E-IfFalse

$$\frac{e_1, \hat{\sigma} \mathrel{\hat{\downarrow}} \mathsf{False}, \hat{\sigma}' \qquad e_3, \hat{\sigma}' \mathrel{\hat{\downarrow}} \hat{v}_3, \hat{\sigma}''}{\textbf{if}\; e_1 \;\textbf{then}\; e_2 \;\textbf{else}\; e_3, \hat{\sigma} \mathrel{\hat{\downarrow}} \hat{v}_3, \hat{\sigma}''}$$

Symbolic TopHat

E-IfTrue

$$\frac{e_1, \hat{\sigma} \mathrel{\hat{\downarrow}} \mathsf{True}, \hat{\sigma}' \qquad e_2, \hat{\sigma}' \mathrel{\hat{\downarrow}} \hat{v}_2, \hat{\sigma}''}{\textbf{if}\; e_1 \;\textbf{then}\; e_2 \;\textbf{else}\; e_3, \hat{\sigma} \mathrel{\hat{\downarrow}} \hat{v}_2, \hat{\sigma}''}$$

E-IfFalse

$$\frac{e_1, \hat{\sigma} \mathrel{\hat{\downarrow}} \mathsf{False}, \hat{\sigma}' \qquad e_3, \hat{\sigma}' \mathrel{\hat{\downarrow}} \hat{v}_3, \hat{\sigma}''}{\textbf{if}\; e_1 \;\textbf{then}\; e_2 \;\textbf{else}\; e_3, \hat{\sigma} \mathrel{\hat{\downarrow}} \hat{v}_3, \hat{\sigma}''}$$

SE-If

$$\frac{e_1, \sigma \;\downarrow\; \overline{v_1, \sigma', \varphi_1} \qquad e_2, \sigma' \;\downarrow\; \overline{v_2, \sigma'', \varphi_2} \qquad e_3, \sigma' \;\downarrow\; \overline{v_3, \sigma''', \varphi_3}}{\textbf{if}\; e_1 \;\textbf{then}\; e_2 \;\textbf{else}\; e_3, \sigma \;\downarrow\; \overline{v_2, \sigma'', \varphi_1 \wedge \varphi_2 \wedge v_1} \cup \overline{v_3, \sigma''', \varphi_1 \wedge \varphi_3 \wedge \neg v_1}}$$

Symbolic TopHat

$$\boxed{t, \sigma \ \Rightarrow\ \overline{t', \sigma', \ i, \varphi}}$$

$$\mathit{simulate} : \text{Tasks} \times \text{States} \times [\text{Inputs}] \times \text{Predicates} \rightarrow \mathcal{P}(\text{Values} \times [\text{Inputs}] \times \text{Predicates})$$

Example

- Within 365 days
- Confirmation from installation company
- Approval from tax office
- Maximum of 600 euros

Example

$$\psi(s, a, c, i, t) = s \geq 0 \supset c \tag{1}$$

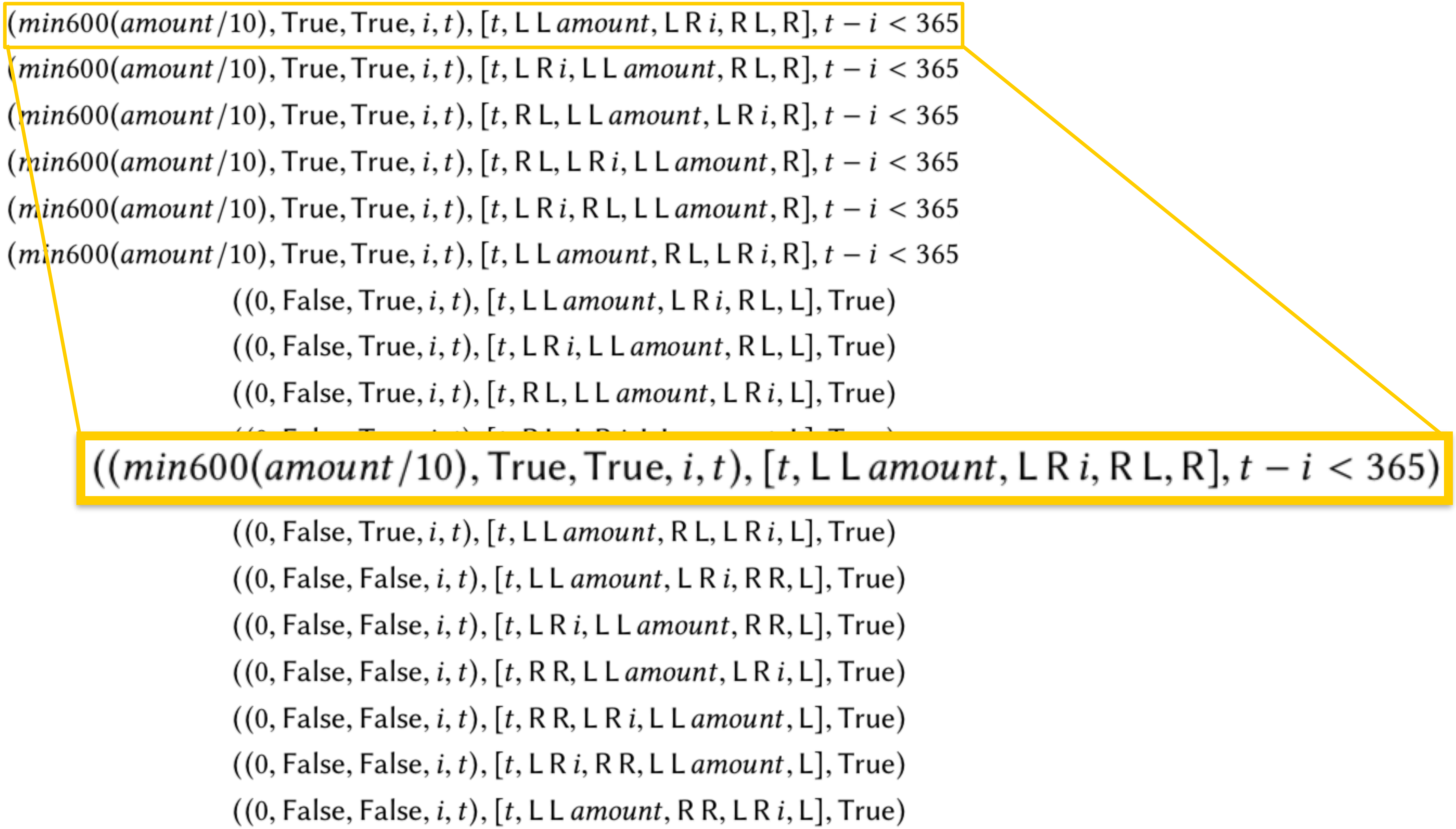
$$\wedge\ s \geq 0 \supset a \tag{2}$$

$$\wedge\ a \supset c \wedge t - i < 365 \tag{3}$$

$$\wedge\ s \leq 600 \tag{4}$$

$$\wedge\ \neg a \supset s \equiv 0 \tag{5}$$

Example



$(\mathit{min600}(\mathit{amount}/10), \mathrm{True}, \mathrm{True}, i, t), [t, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L\,R}\,i, \mathrm{R\,L}, \mathrm{R}], t - i < 365$

$(\mathit{min600}(\mathit{amount}/10), \mathrm{True}, \mathrm{True}, i, t), [t, \mathrm{L\,R}\,i, \mathrm{L\,L}\,\mathit{amount}, \mathrm{R\,L}, \mathrm{R}], t - i < 365$

$(\mathit{min600}(\mathit{amount}/10), \mathrm{True}, \mathrm{True}, i, t), [t, \mathrm{R\,L}, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L\,R}\,i, \mathrm{R}], t - i < 365$

$(\mathit{min600}(\mathit{amount}/10), \mathrm{True}, \mathrm{True}, i, t), [t, \mathrm{R\,L}, \mathrm{L\,R}\,i, \mathrm{L\,L}\,\mathit{amount}, \mathrm{R}], t - i < 365$

$(\mathit{min600}(\mathit{amount}/10), \mathrm{True}, \mathrm{True}, i, t), [t, \mathrm{L\,R}\,i, \mathrm{R\,L}, \mathrm{L\,L}\,\mathit{amount}, \mathrm{R}], t - i < 365$

$(\mathit{min600}(\mathit{amount}/10), \mathrm{True}, \mathrm{True}, i, t), [t, \mathrm{L\,L}\,\mathit{amount}, \mathrm{R\,L}, \mathrm{L\,R}\,i, \mathrm{R}], t - i < 365$

$((0, \mathrm{False}, \mathrm{True}, i, t), [t, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L\,R}\,i, \mathrm{R\,L}, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{True}, i, t), [t, \mathrm{L\,R}\,i, \mathrm{L\,L}\,\mathit{amount}, \mathrm{R\,L}, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{True}, i, t), [t, \mathrm{R\,L}, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L\,R}\,i, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{True}, i, t), [t, \mathrm{R\,L}, \mathrm{L\,R}\,i, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L}], \mathrm{True})$

$((\mathit{min600}(\mathit{amount}/10), \mathrm{True}, \mathrm{True}, i, t), [t, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L\,R}\,i, \mathrm{R\,L}, \mathrm{R}], t - i < 365)$

$((0, \mathrm{False}, \mathrm{True}, i, t), [t, \mathrm{L\,L}\,\mathit{amount}, \mathrm{R\,L}, \mathrm{L\,R}\,i, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{False}, i, t), [t, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L\,R}\,i, \mathrm{R\,R}, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{False}, i, t), [t, \mathrm{L\,R}\,i, \mathrm{L\,L}\,\mathit{amount}, \mathrm{R\,R}, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{False}, i, t), [t, \mathrm{R\,R}, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L\,R}\,i, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{False}, i, t), [t, \mathrm{R\,R}, \mathrm{L\,R}\,i, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{False}, i, t), [t, \mathrm{L\,R}\,i, \mathrm{R\,R}, \mathrm{L\,L}\,\mathit{amount}, \mathrm{L}], \mathrm{True})$

$((0, \mathrm{False}, \mathrm{False}, i, t), [t, \mathrm{L\,L}\,\mathit{amount}, \mathrm{R\,R}, \mathrm{L\,R}\,i, \mathrm{L}], \mathrm{True})$

KUSTWACHT

PHILIPS
ALPHATRON Medical
VUmc

Belastingdienst

F802