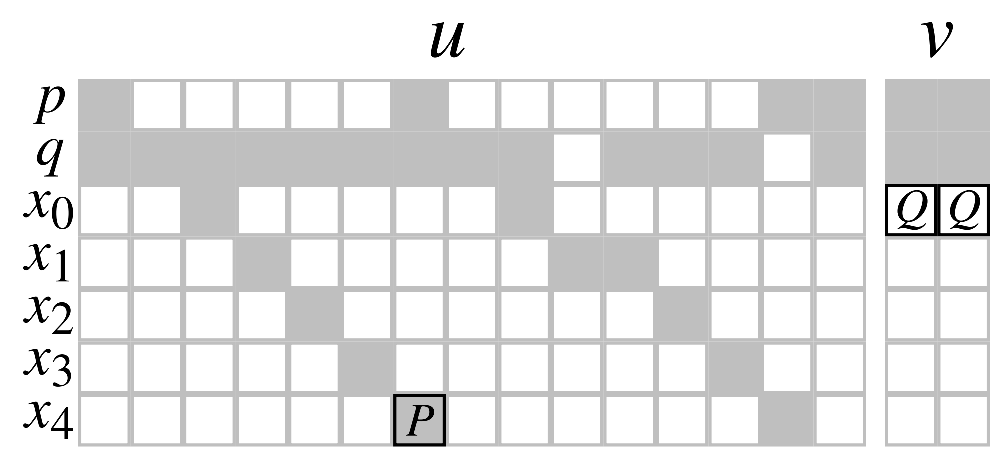
Optimal Proofs for LTL on Lasso Words

David Basin Bhargav Bhatt Dmitriy Traytel



ETH zürich

75 NRP Big Data
National Research Programme

Context

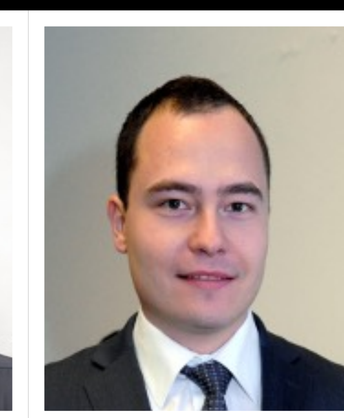
Big Data Monitoring

ETH zürich

Dmitriy Traytel

David Basin

Bhargav Bhatt



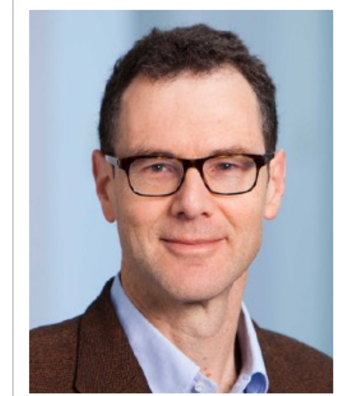
Srđan Krstić

Grand Challenge: scalable monitors for expressive policy specification languages

Big Data Monitoring

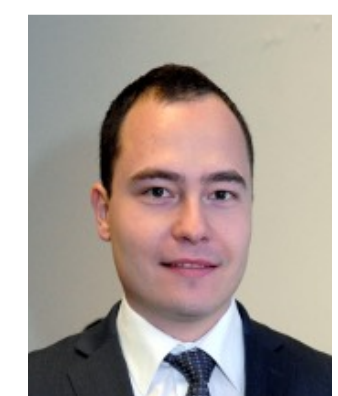
ETH zürich

Dmitriy Traytel



David Basin

Bhargav Bhatt



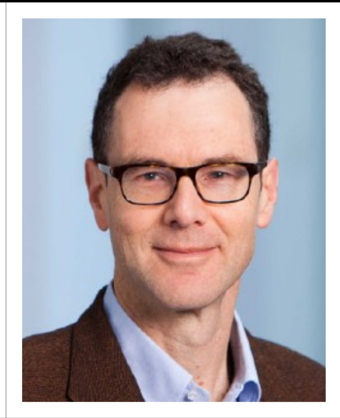
Srđan Krstić

SSH sessions must not last longer than 24h.

informal policy

Grand Challenge: scalable monitors for expressive policy specification languages

Big Data Monitoring

Dmitriy Traytel David Basin


Bhargav Bhatt Srđan Krstić

policy

$$\Box \forall c. \forall s. \mathit{ssh\_login}(c, s) \land ((\Diamond_{[1min,20min]} \mathit{net}(c)) \land \Box_{[0,1d]} (\blacksquare_{=0} \mathit{net}(c) \to \Diamond_{[1min,20min]} \mathit{net}(c))) \to \Diamond_{[0,1d)} \blacklozenge_{=0} \mathit{ssh\_logout}(c, s)$$

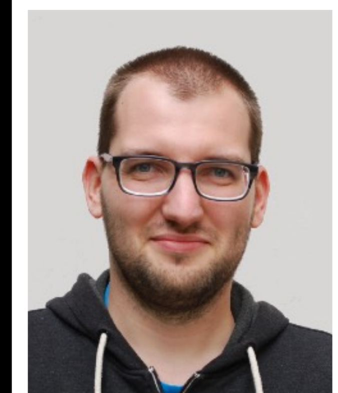
SSH sessions must not last longer than 24h.

informal policy

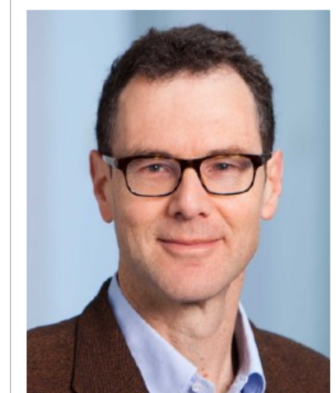
Grand Challenge: **scalable** monitors for **expressive** policy specification languages

Big Data Monitoring

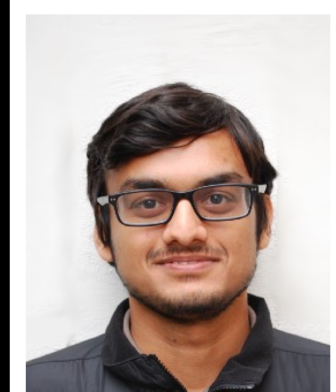
ETH zürich



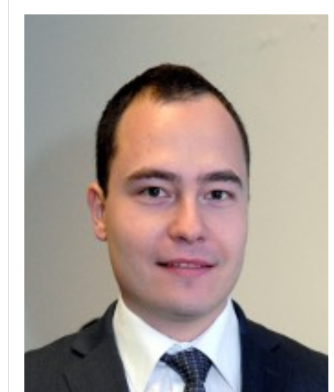
Dmitriy Traytel



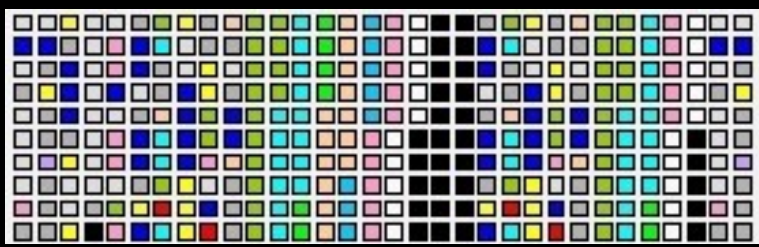
David Basin



Bhargav Bhatt



Srđan Krstić



event stream

policy

$$\Box \forall c.\ \forall s.\ ssh\_login(c,\ s) \land ((\Diamond_{[1min,20min]}\ net(c)) \land \Box_{[0,1d]}\ (\blacksquare_{=0}\ net(c) \to \Diamond_{[1min,20min]}\ net(c))) \to \Diamond_{[0,1d)}\ \blacklozenge_{=0}\ ssh\_logout(c,\ s)$$

↑

SSH sessions must not last longer than 24h.

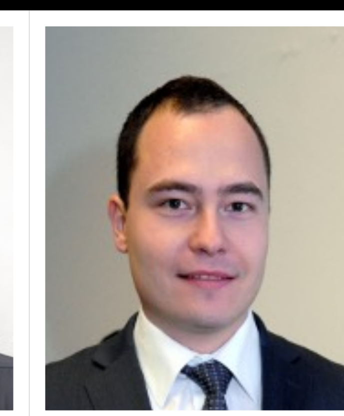
informal policy

Grand Challenge: **scalable** monitors for **expressive** policy specification languages

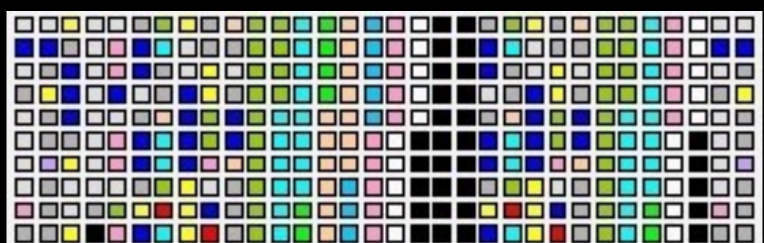
Big Data Monitoring

ETH zürich


Dmitriy Traytel David Basin

Bhargav Bhatt Srđan Krstić



event stream

monitor

policy

$$\square\, \forall c.\ \forall s.\ \mathit{ssh\_login}(c,\ s) \land \big((\lozenge_{[1min,20min]}\ \mathit{net}(c)) \land \square_{[0,1d]}\ (\blacksquare_{=0}\ \mathit{net}(c) \rightarrow \lozenge_{[1min,20min]}\ \mathit{net}(c))\big) \rightarrow \lozenge_{[0,1d)}\ \blacklozenge_{=0}\ \mathit{ssh\_logout}(c,\ s)$$

SSH sessions must not last longer than 24h.

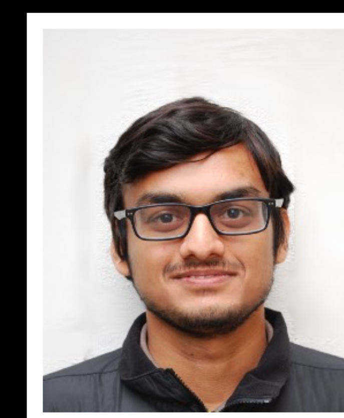
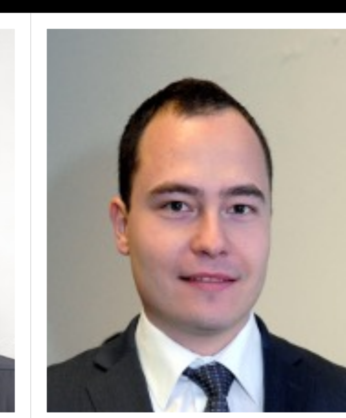
informal policy

Grand Challenge: **scalable** monitors for **expressive** policy specification languages

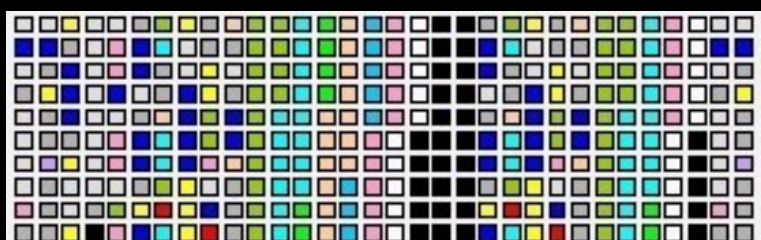
Big Data Monitoring

ETH zürich

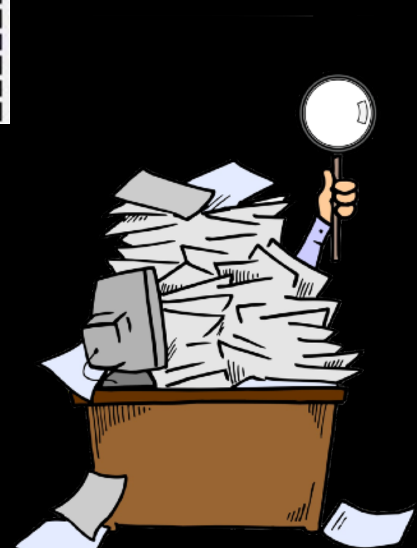

Dmitriy Traytel   David Basin

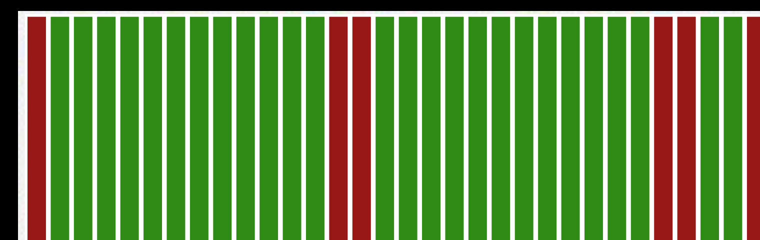
Bhargav Bhatt   Srđan Krstić



event stream



monitor



verdict stream

policy

$$\square\, \forall c.\ \forall s.\ \mathit{ssh\_login}(c,s) \land ((\Diamond_{[1min,20min]}\ \mathit{net}(c)) \land \square_{[0,1d]}\ (\blacksquare_{=0}\ \mathit{net}(c) \to \Diamond_{[1min,20min]}\ \mathit{net}(c))) \to \Diamond_{[0,1d)}\ \blacklozenge_{=0}\ \mathit{ssh\_logout}(c,s)$$

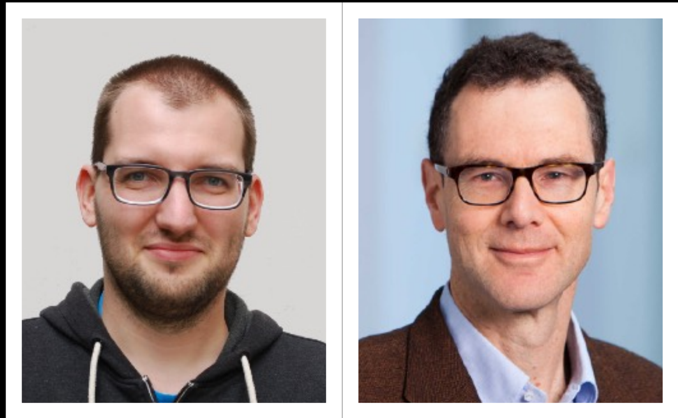
SSH sessions must not last longer than 24h.

informal policy

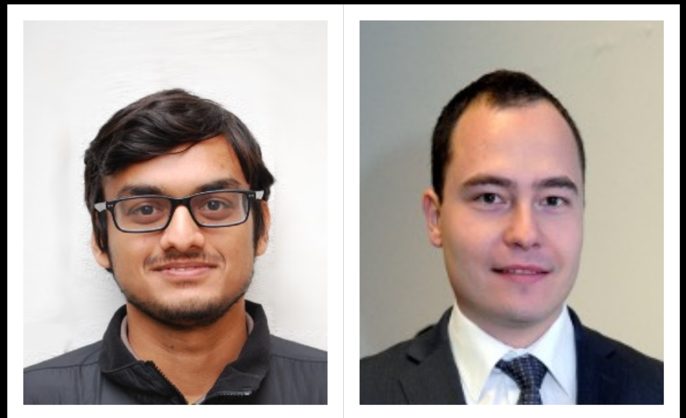
Grand Challenge: **scalable** monitors for **expressive** policy specification languages

Big Data Monitoring

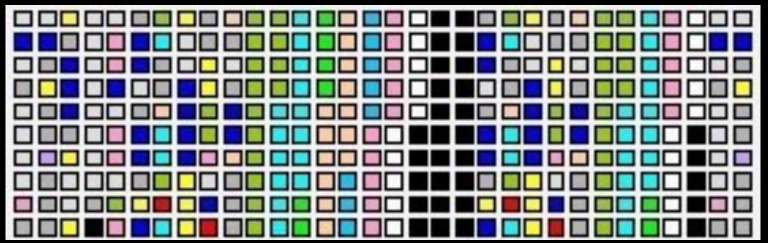
ETH zürich



Dmitriy Traytel | David Basin

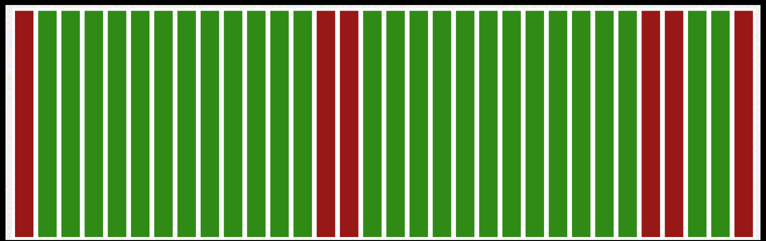


Bhargav Bhatt | Srđan Krstić



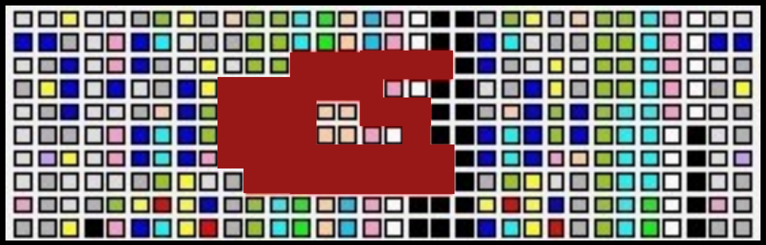
event stream

monitor



verdict stream

explanation



policy

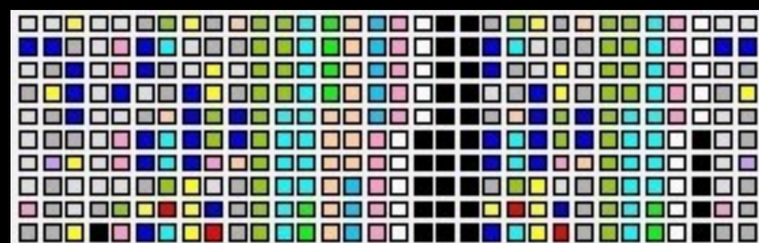
$$\square\, \forall c.\, \forall s.\; ssh\_login(c,\, s) \wedge \Big(\big(\Diamond_{[1min,20min]}\, net(c)\big) \wedge \square_{[0,1d]} \big(\blacksquare_{=0}\, net(c) \rightarrow \Diamond_{[1min,20min]}\, net(c)\big)\Big) \rightarrow \Diamond_{[0,1d)}\, \blacklozenge_{=0}\, ssh\_logout(c,\, s)$$

SSH sessions must not last longer than 24h.

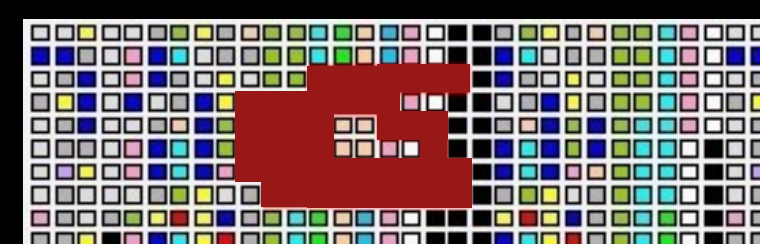
informal policy

Grand Challenge: **scalable** monitors for **expressive** policy specification languages

Ambitious Goal

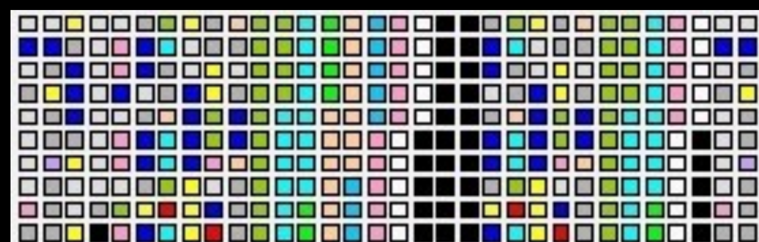


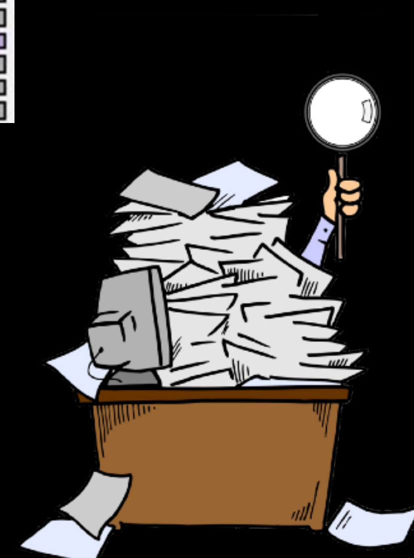
$$\Box \forall c.\ \forall s.\ ssh\_login(c, s) \wedge \big((\Diamond_{[1min,20min]}\, net(c)) \wedge \Box_{[0,1d]} (\blacksquare_{=0}\, net(c) \rightarrow \Diamond_{[1min,20min]}\, net(c))\big) \rightarrow \Diamond_{[0,1d)} \blacklozenge_{=0}\, ssh\_logout(c, s)$$

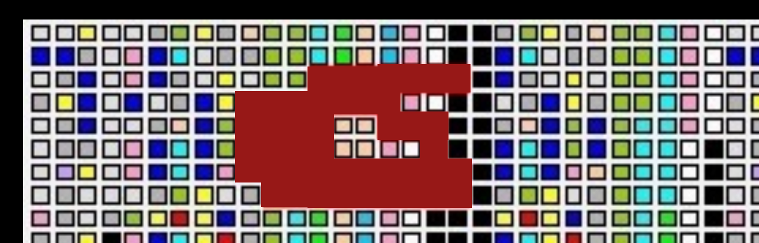


Ambitious Goal

infinite stream





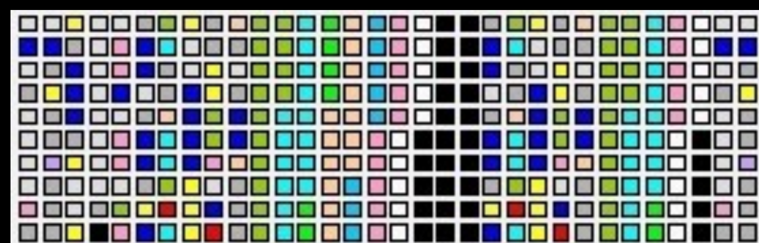


$$\begin{aligned}
&\square\, \forall c.\, \forall s.\, ssh_login(c, s) \wedge \\
&\quad ((\lozenge_{[1min,20min]}\, net(c)) \wedge \\
&\qquad \square_{[0,1d]}\, (\blacksquare_{=0}\, net(c) \rightarrow \lozenge_{[1min,20min]}\, net(c))) \rightarrow \\
&\quad \lozenge_{[0,1d)}\, \blacklozenge_{=0}\, ssh_logout(c, s)
\end{aligned}$$

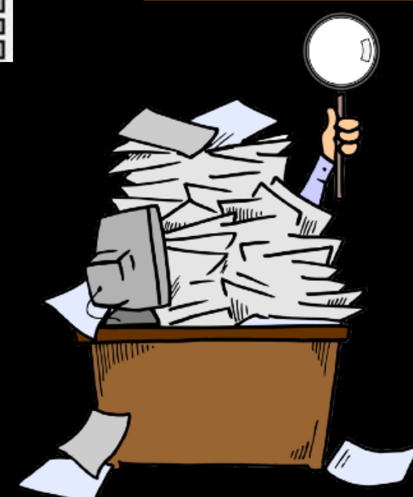
policy

Ambitious Goal

infinite stream

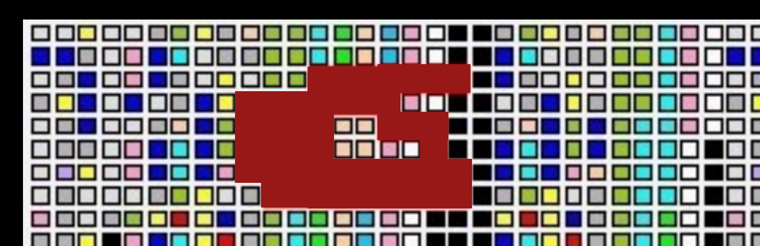


streaming algorithm



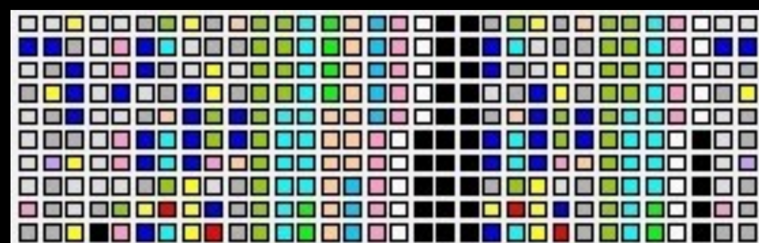
$$\Box\, \forall c.\ \forall s.\ ssh\_login(c, s) \land \left(\left(\Diamond_{[1min,20min]}\, net(c) \right) \land \Box_{[0,1d]} \left(\blacksquare_{=0}\, net(c) \rightarrow \Diamond_{[1min,20min]}\, net(c) \right) \right) \rightarrow \Diamond_{[0,1d)}\, \blacklozenge_{=0}\, ssh\_logout(c, s)$$

policy

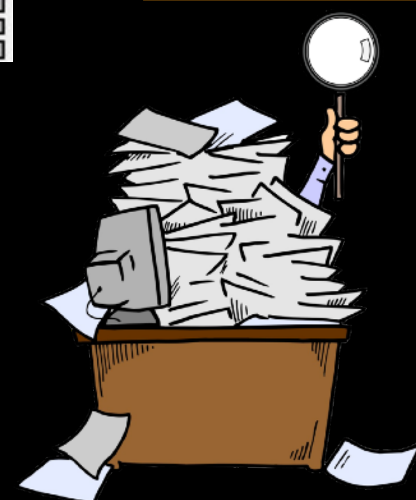


Ambitious Goal

infinite stream

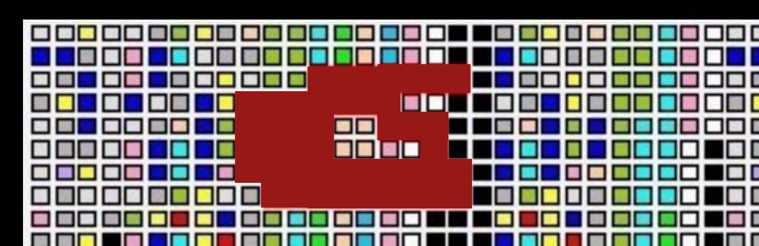


streaming algorithm



$$
\begin{aligned}
&\Box\, \forall c.\ \forall s.\ ssh\_login(c,\, s) \land \\
&\quad ((\Diamond_{[1min,20min]}\ net(c)) \land \\
&\qquad \Box_{[0,1d]}\ (\blacksquare_{=0}\ net(c) \to \Diamond_{[1min,20min]}\ net(c))) \to \\
&\quad \Diamond_{[0,1d)}\ \blacklozenge_{=0}\ ssh\_logout(c,\, s)
\end{aligned}
$$

policy

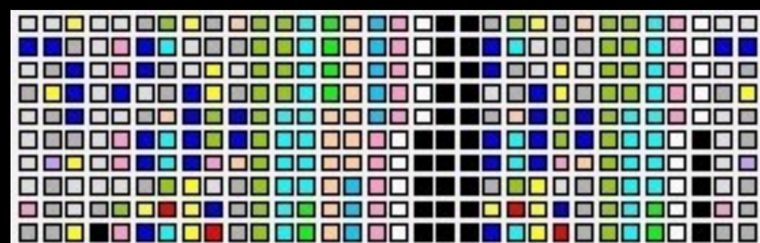


stream of explanations

Ambitious Goal

BIG DATA

infinite stream



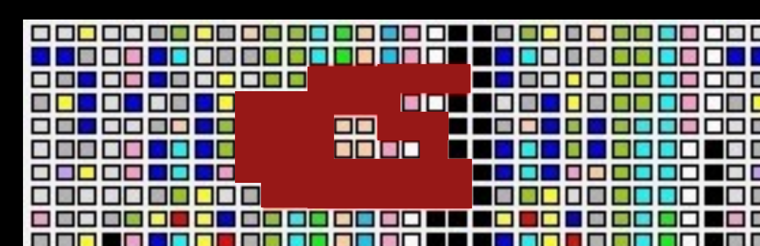
streaming algorithm

efficient

$$\Box\, \forall c.\, \forall s.\, \mathit{ssh\_login}(c, s) \land ((\Diamond_{[1min,20min]}\, \mathit{net}(c)) \land \Box_{[0,1d]}\, (\blacksquare_{=0}\, \mathit{net}(c) \to \Diamond_{[1min,20min]}\, \mathit{net}(c))) \to \Diamond_{[0,1d)}\, \blacklozenge_{=0}\, \mathit{ssh\_logout}(c, s)$$

policy

expressive language: MFOTL



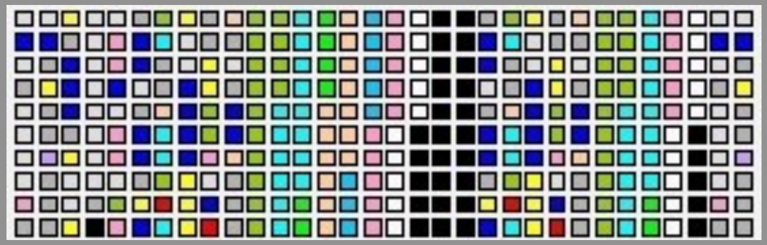
stream of explanations

small
understandable

Modest Goal

~~BIG DATA~~ small data

~~infinite~~ ~~stream~~ word



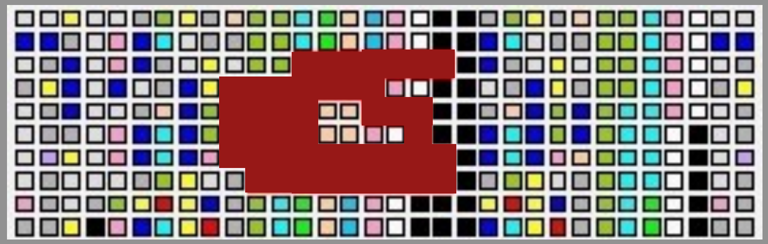
~~streaming~~ algorithm

efficient

$$\Box(req \rightarrow \Diamond ack)$$

policy

~~expressive language: MFOTL~~
simple language: LTL



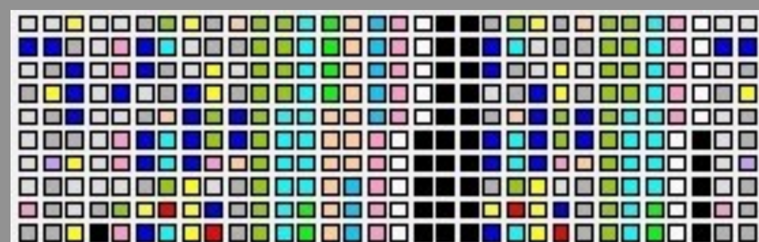
~~stream of~~ explanation~~s~~

small
~~understandable~~

Modest Goal

~~BIG DATA~~ small data

~~infinite~~ ~~stream~~ word



~~streaming~~ algorithm

efficient

Still useful?

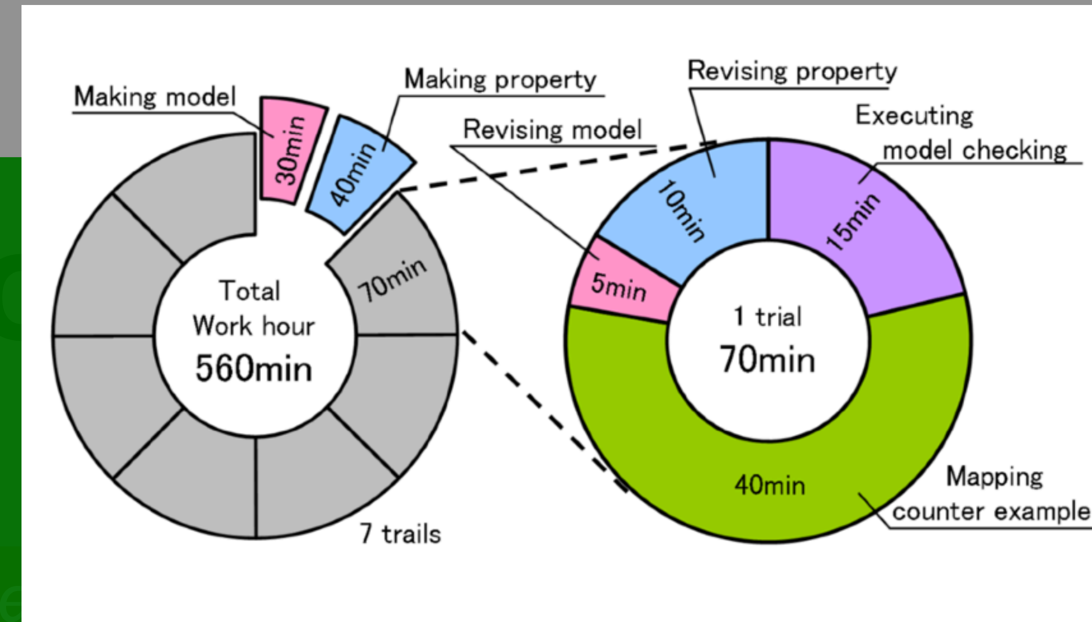
$$\Box(req \to \Diamond ack)$$

policy

~~expressive language: MFOTL~~
simple language: LTL

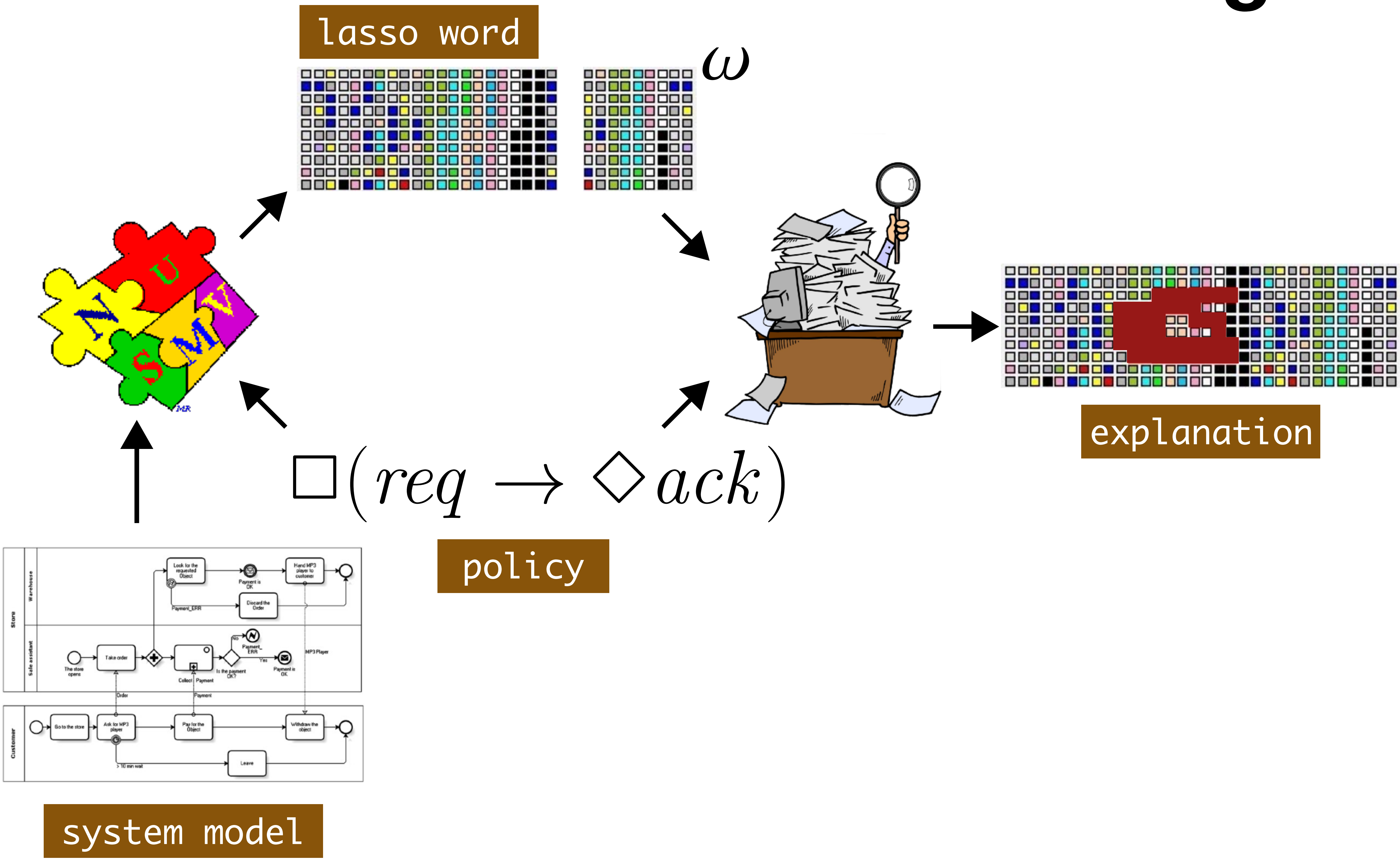
~~stream of~~ explanation~~s~~

small
~~understandable~~

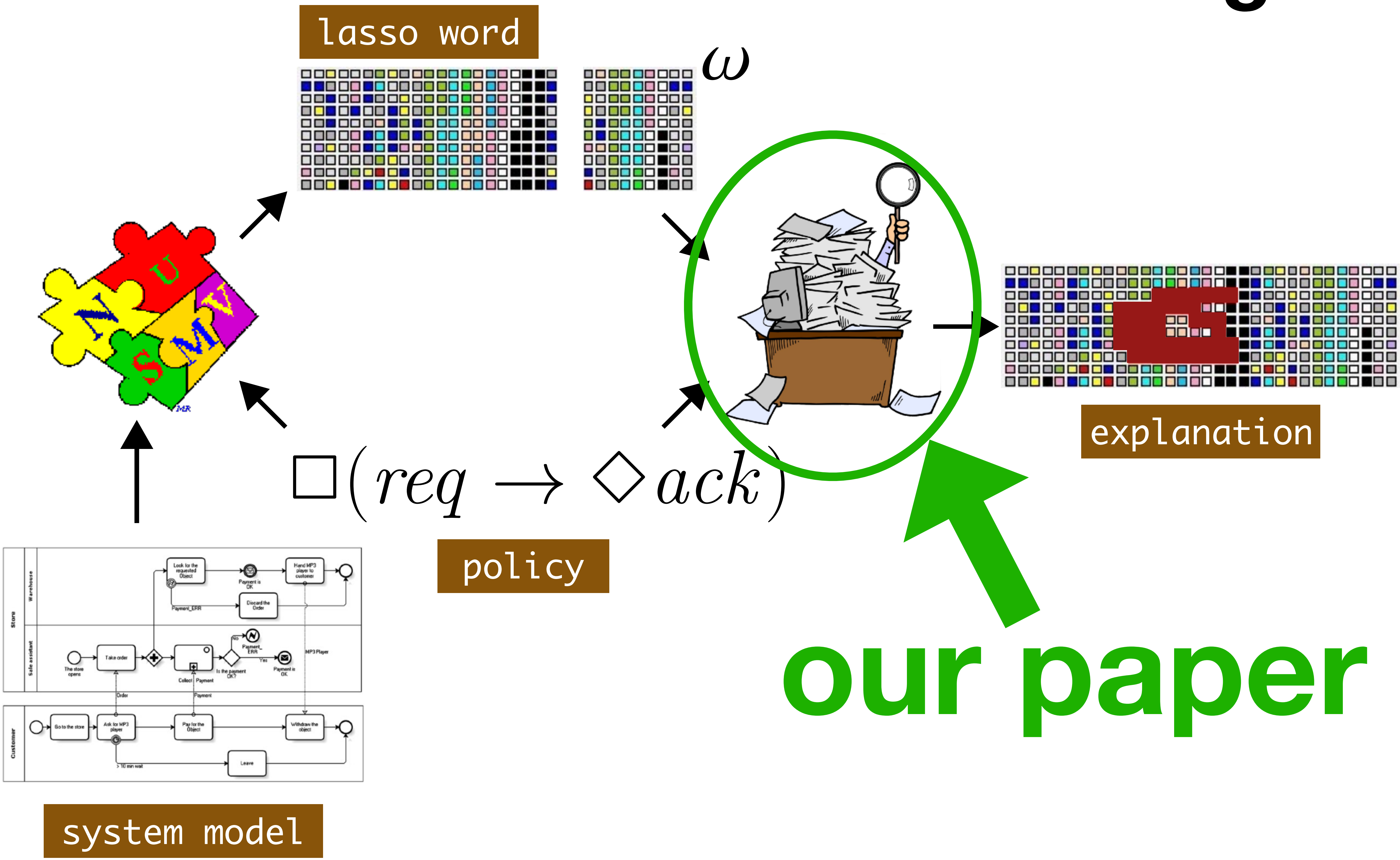


Yes!
For debugging model checking specifications.

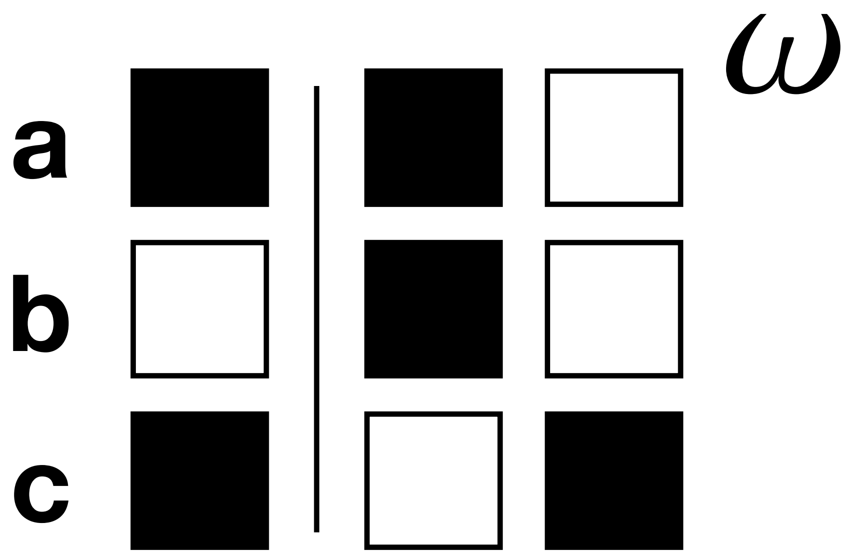
Concrete Setting

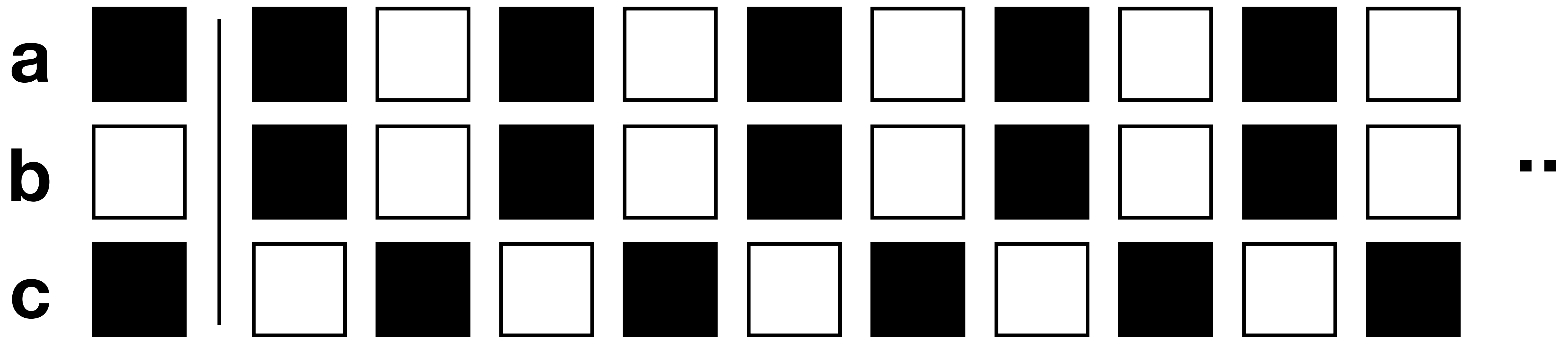


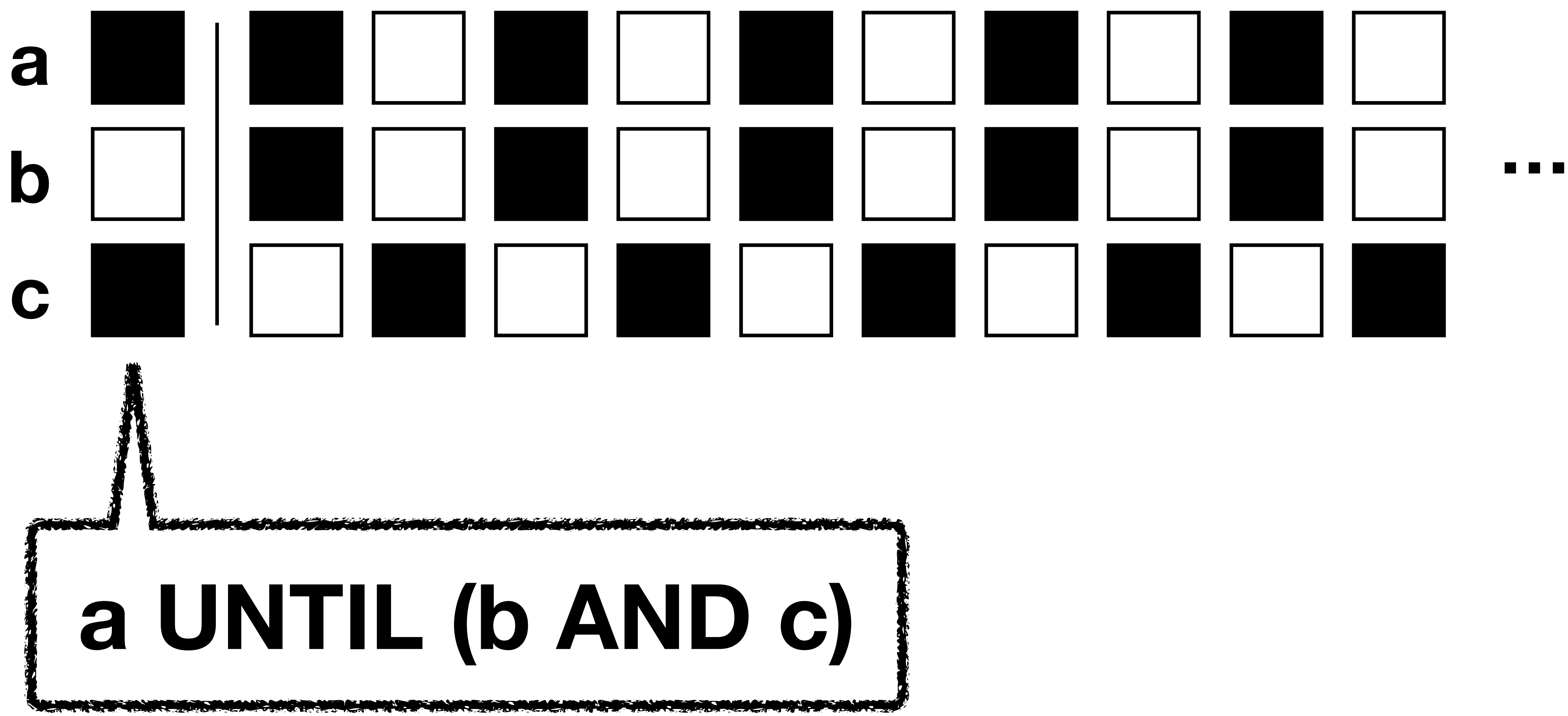
Concrete Setting

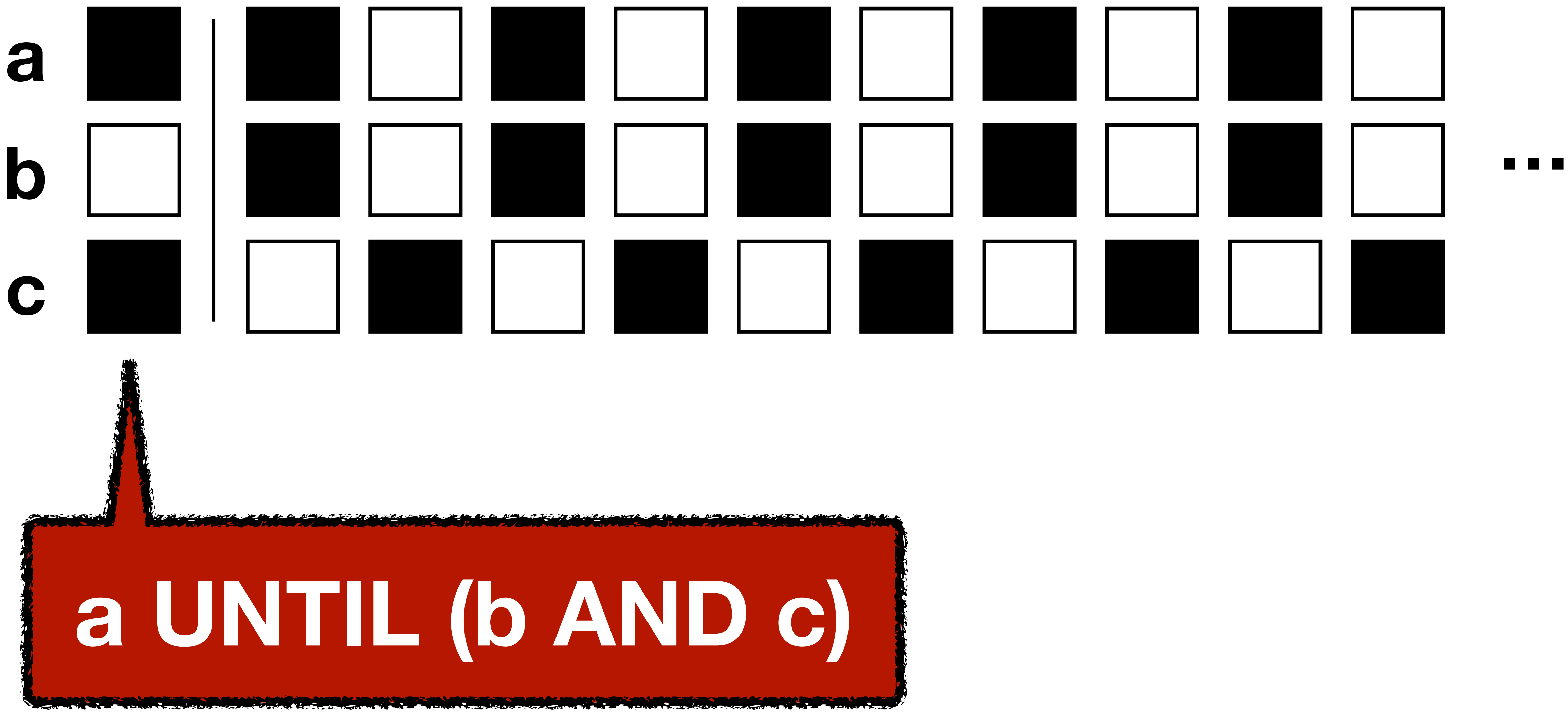


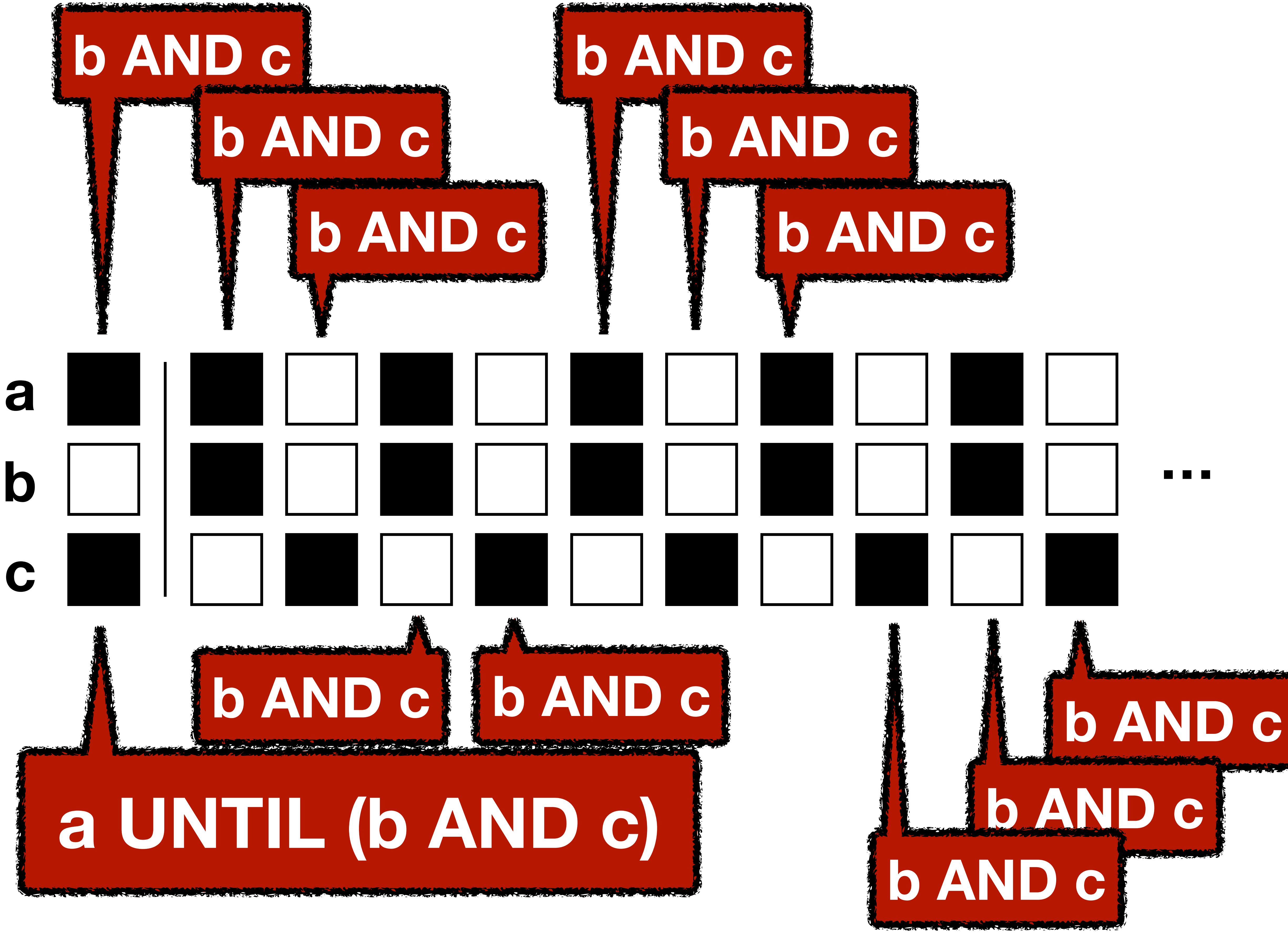
Explanations

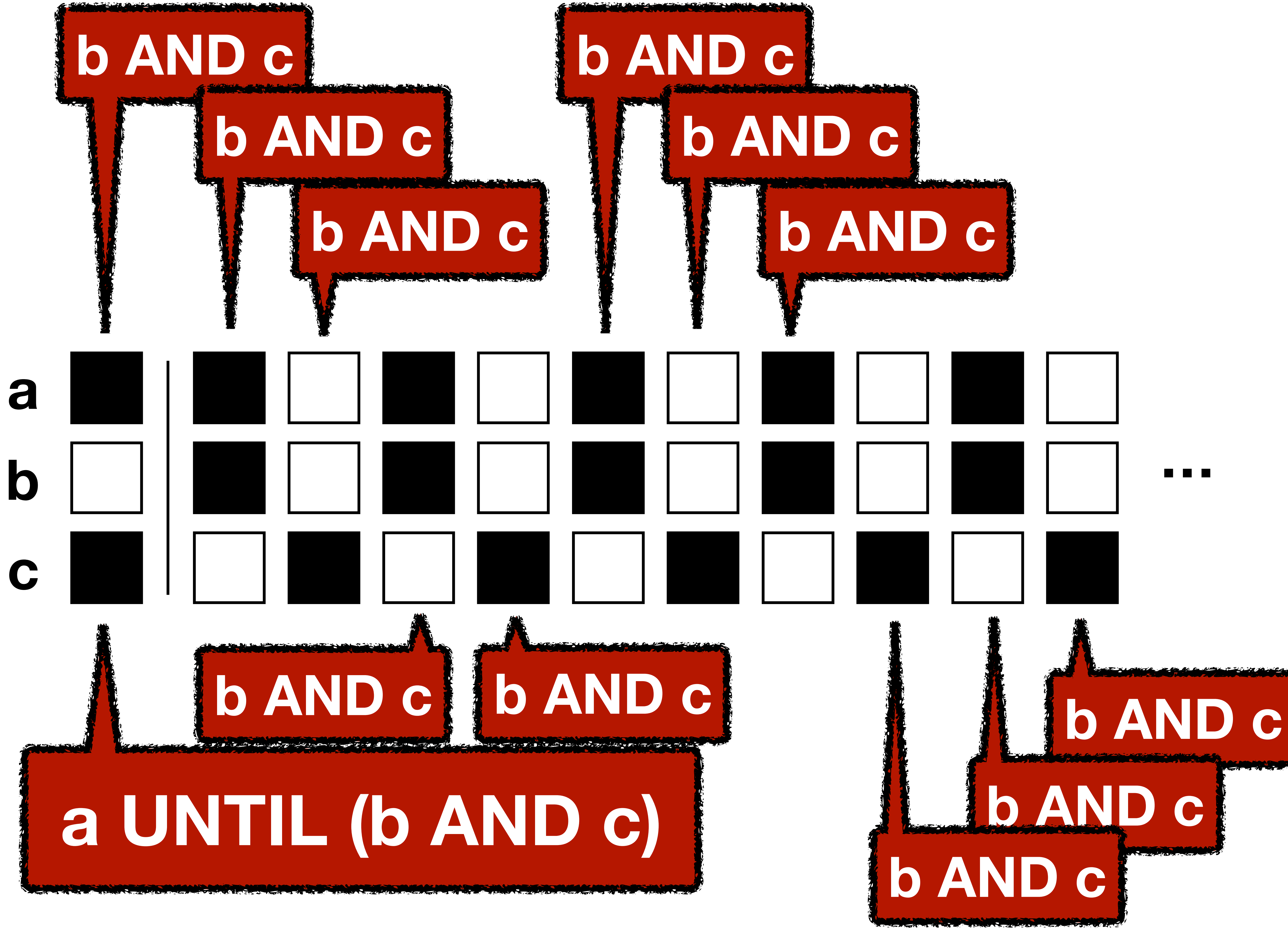

ω
a
b
c

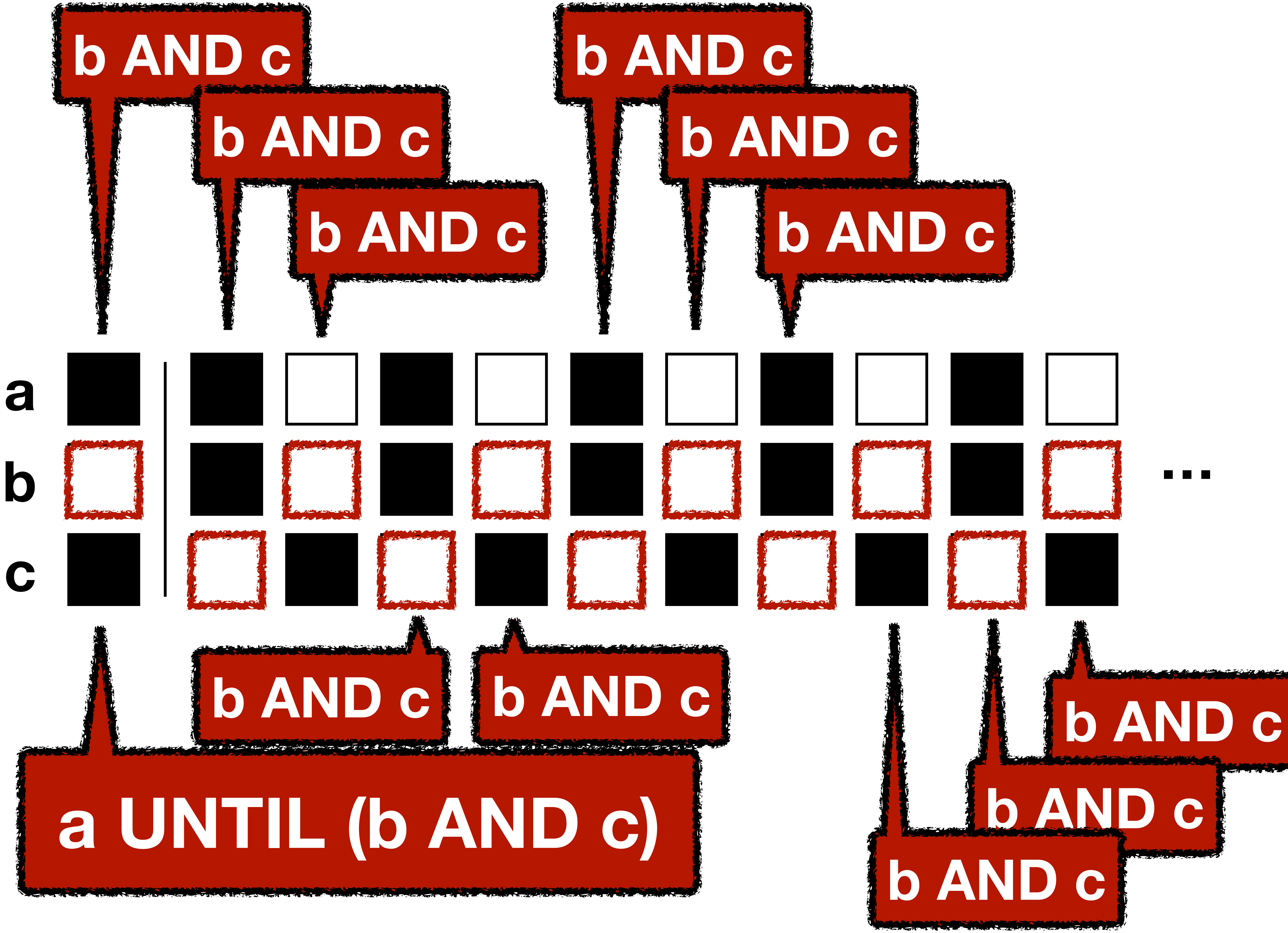

a
b
c
...


a
b
c
...
a UNTIL (b AND c)


a
b
c
...
a UNTIL (b AND c)


b AND c
b AND c
b AND c
b AND c
b AND c
b AND c
a
b
c
...
b AND c
b AND c
a UNTIL (b AND c)
b AND c
b AND c
b AND c


b AND c
b AND c
b AND c
b AND c
b AND c
b AND c
a
b
c
...
b AND c
b AND c
a UNTIL (b AND c)
b AND c
b AND c
b AND c


b AND c
b AND c
b AND c
b AND c
b AND c
b AND c
a
b
c
...
b AND c
b AND c
a UNTIL (b AND c)
b AND c
b AND c
b AND c

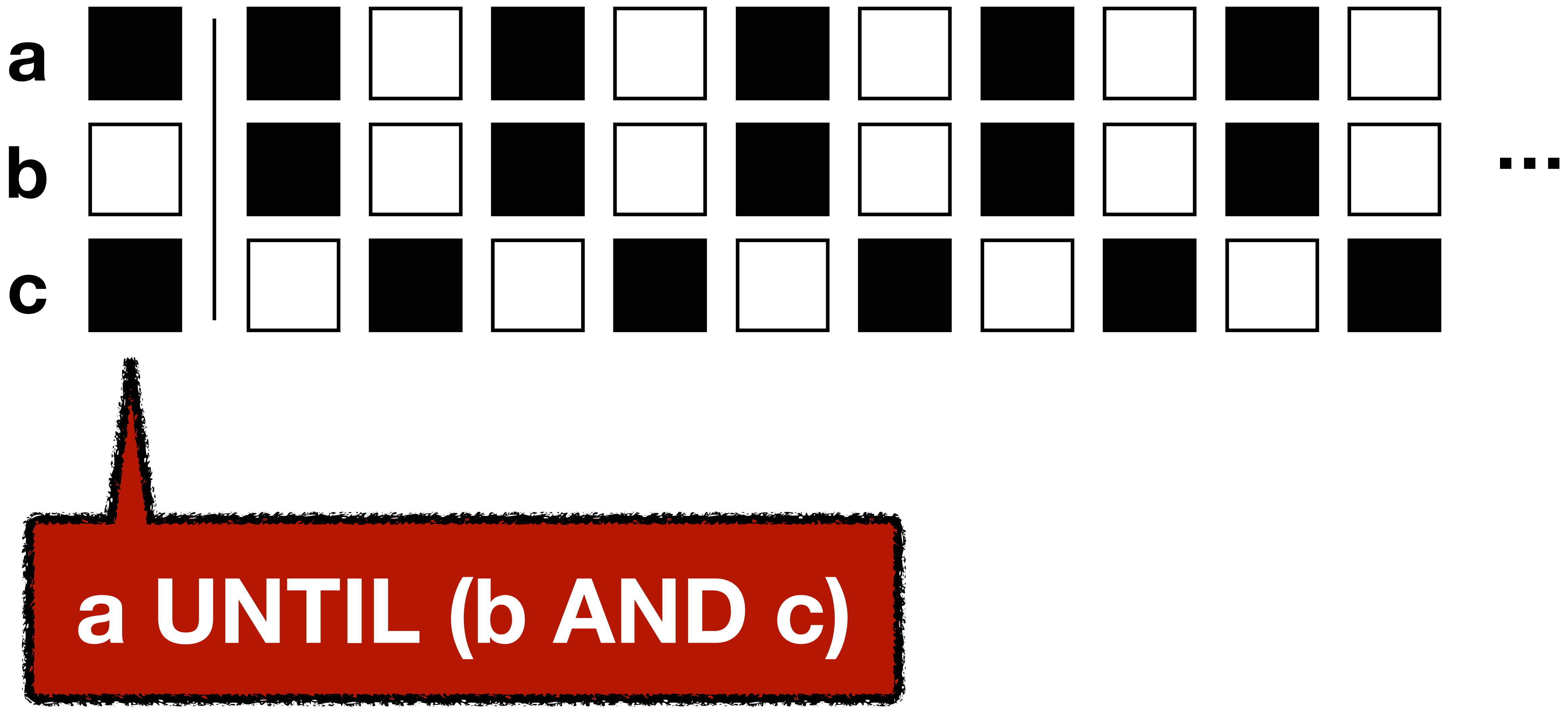
Observation 1

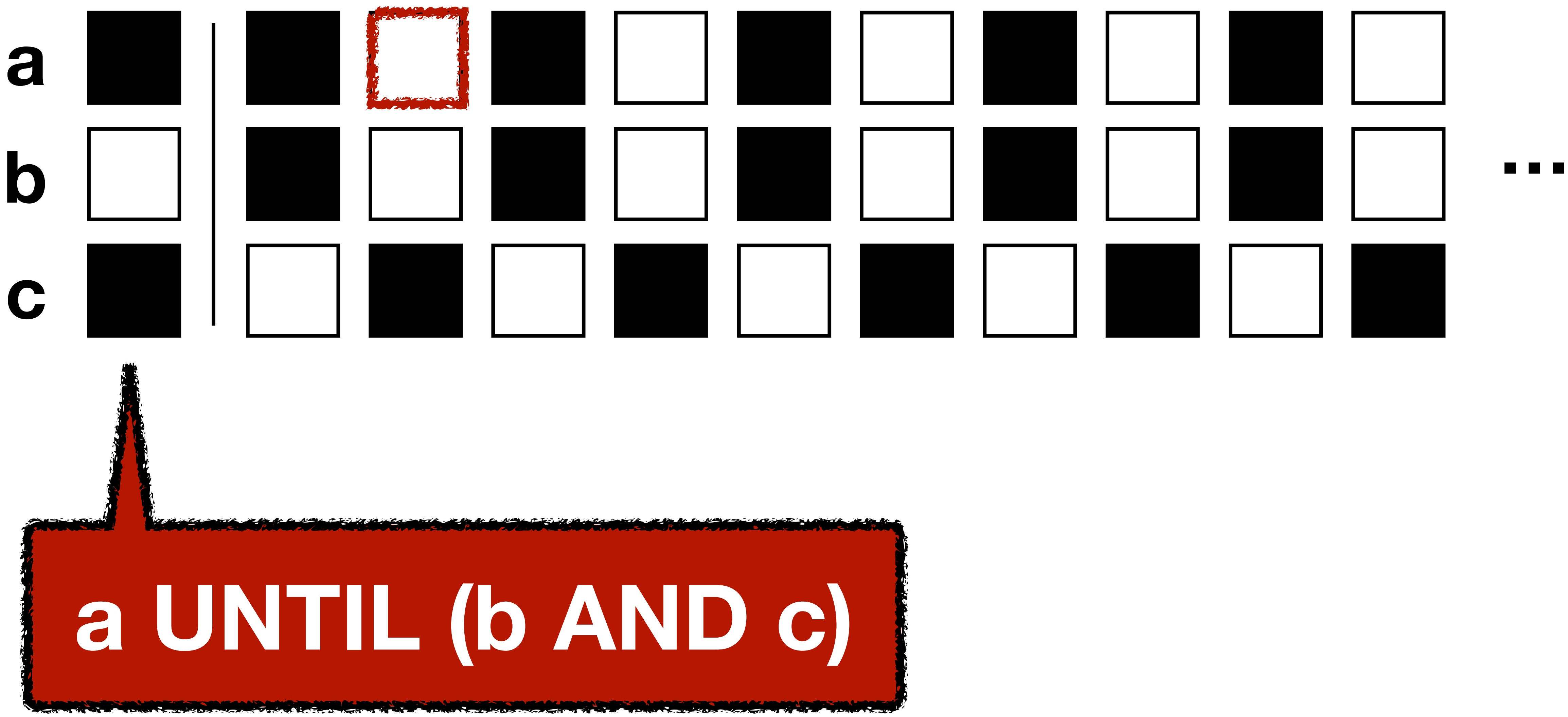
Explanations are recursive objects

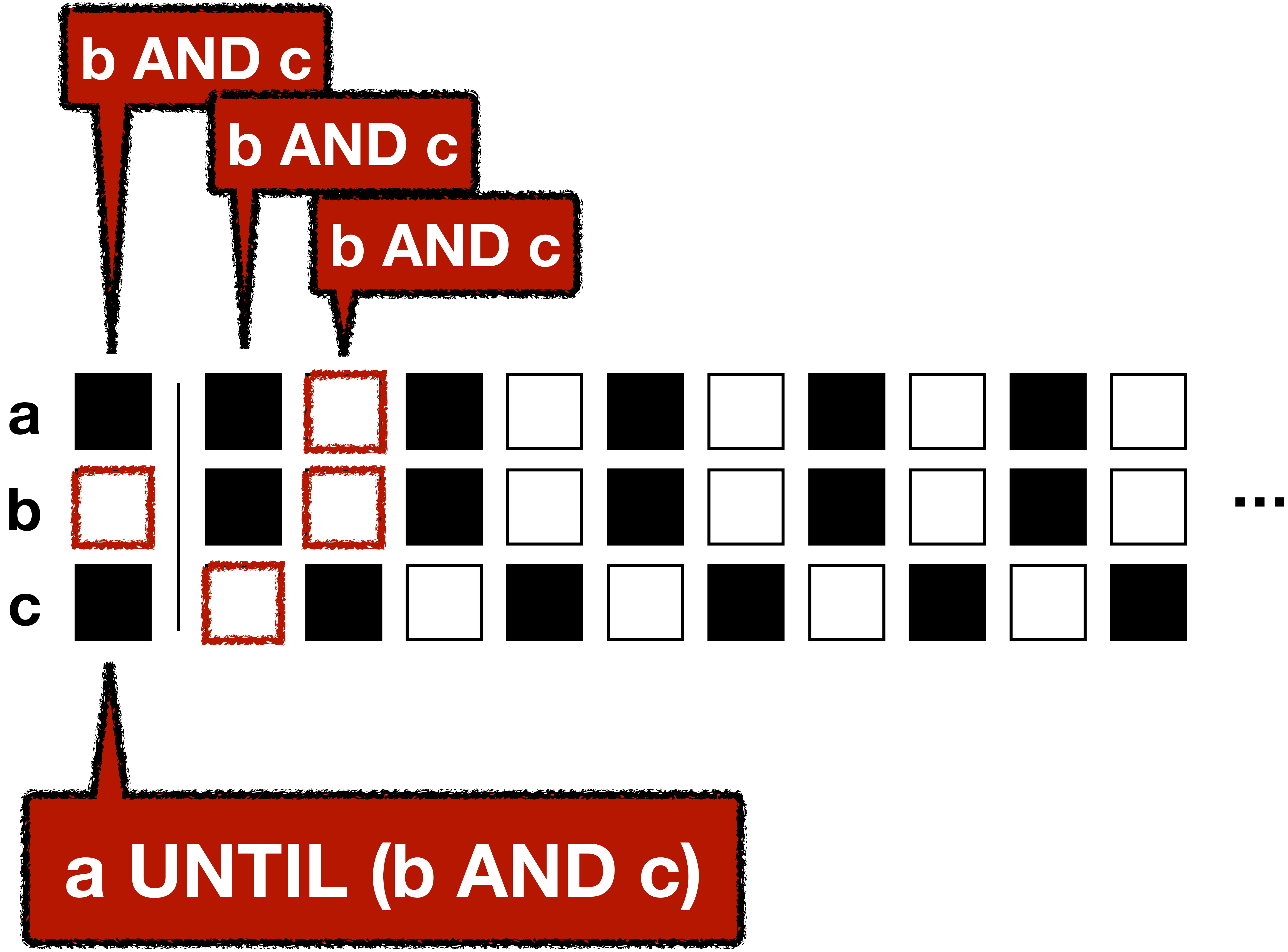
(which follow the formula structure)

Observation 2

Explanations
can be infinite
(but somehow repetitive)

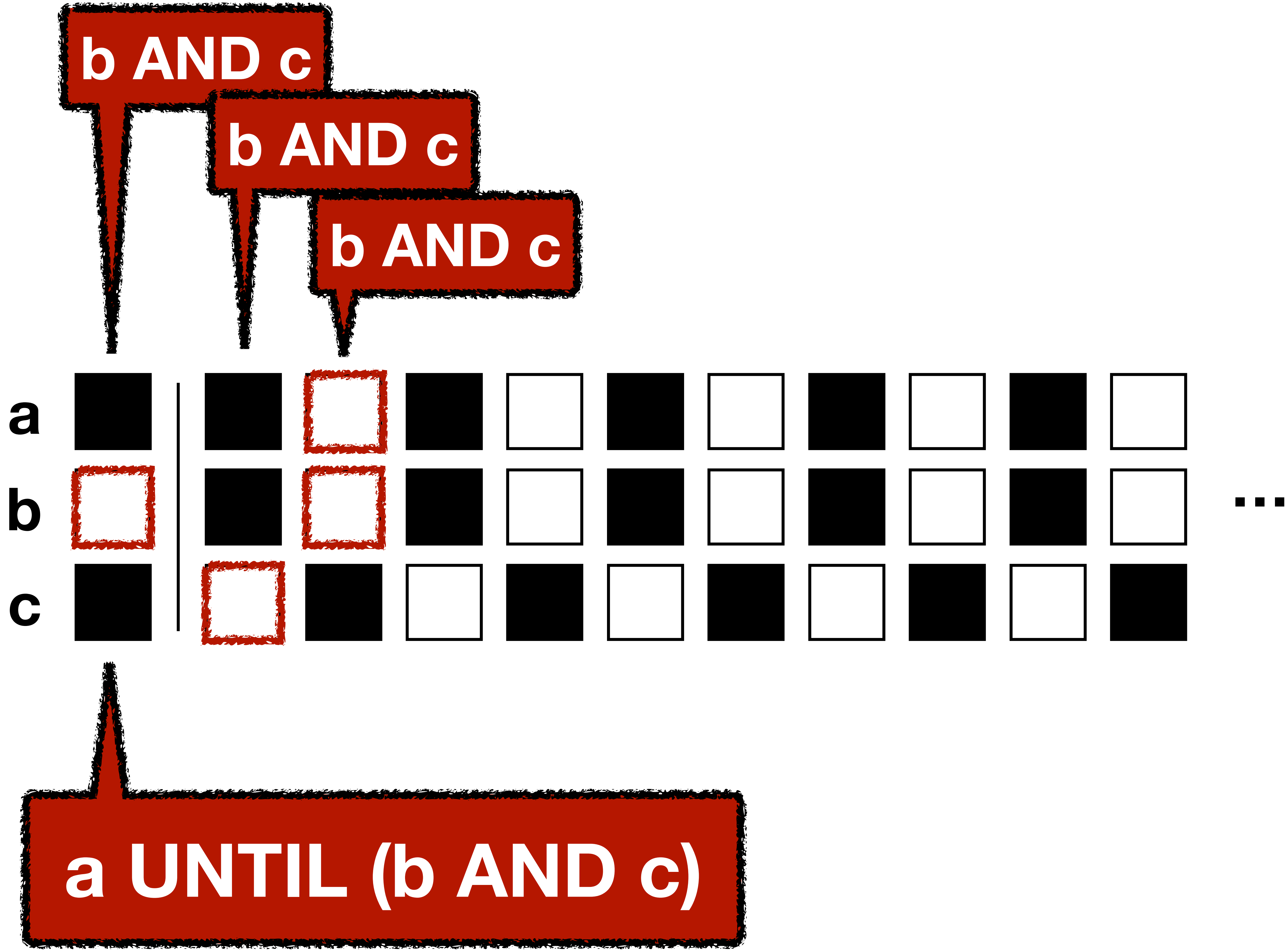

a
b
c
...
a UNTIL (b AND c)

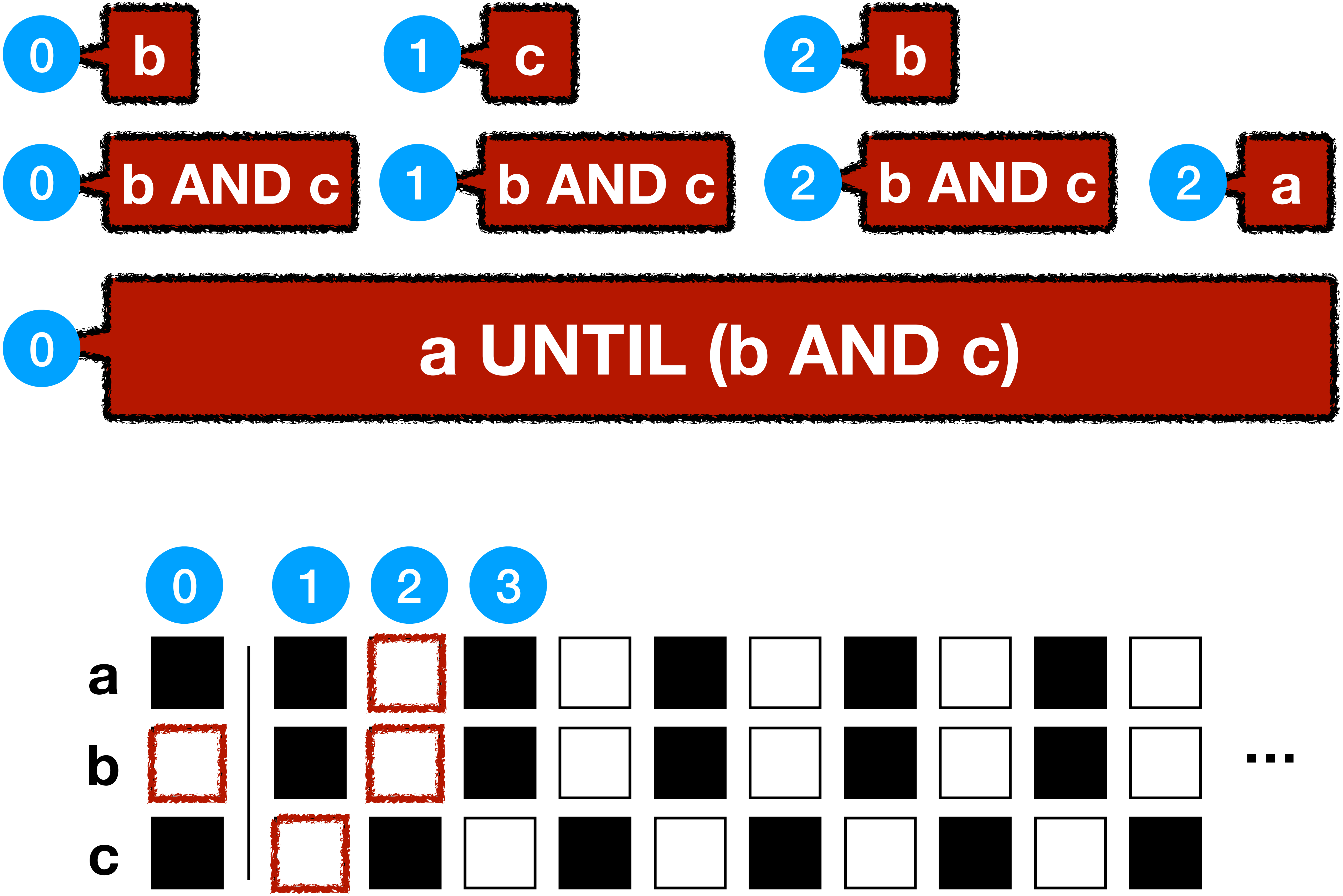

a
b
c
...
a UNTIL (b AND c)


b AND c
b AND c
b AND c
a
b
c
...
a UNTIL (b AND c)

Observation 3

Multiple explanations are possible


b AND c
b AND c
b AND c
a
b
c
...
a UNTIL (b AND c)


0 b
1 c
2 b
0 b AND c
1 b AND c
2 b AND c
2 a
0 a UNTIL (b AND c)
0
1
2
3
a
b
c
...

Explanations

=

Proof Trees

Proof System

$$\frac{a \in \rho(i)}{i \vdash^+ a}\ ap^+ \qquad \frac{i \vdash^- \varphi}{i \vdash^+ \neg\varphi}\ \neg^+ \qquad \frac{a \notin \rho(i)}{i \vdash^- a}\ ap^- \qquad \frac{i \vdash^+ \varphi}{i \vdash^- \neg\varphi}\ \neg^-$$

$$\frac{i \vdash^+ \varphi_1}{i \vdash^+ \varphi_1 \vee \varphi_2}\ \vee^+_L \qquad \frac{i \vdash^+ \varphi_2}{i \vdash^+ \varphi_1 \vee \varphi_2}\ \vee^+_R \qquad \frac{i \vdash^- \varphi_1 \quad i \vdash^- \varphi_2}{i \vdash^- \varphi_1 \vee \varphi_2}\ \vee^-$$

$$\frac{i \vdash^+ \varphi_1 \quad i \vdash^+ \varphi_2}{i \vdash^+ \varphi_1 \wedge \varphi_2}\ \wedge^+ \qquad \frac{i \vdash^- \varphi_1}{i \vdash^- \varphi_1 \wedge \varphi_2}\ \wedge^-_L \qquad \frac{i \vdash^- \varphi_2}{i \vdash^- \varphi_1 \wedge \varphi_2}\ \wedge^-_R$$

$$\frac{j \leq i \quad j \vdash^+ \varphi_2 \quad \forall k \in (j, i].\, k \vdash^+ \varphi_1}{i \vdash^+ \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^+ \qquad \frac{j \leq i \quad j \vdash^- \varphi_1 \quad \forall k \in [j, i].\, k \vdash^- \varphi_2}{i \vdash^- \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^-$$

$$\frac{j \geq i \quad j \vdash^+ \varphi_2 \quad \forall k \in [i, j).\, k \vdash^+ \varphi_1}{i \vdash^+ \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^+ \qquad \frac{j \geq i \quad j \vdash^- \varphi_1 \quad \forall k \in [i, j].\, k \vdash^- \varphi_2}{i \vdash^- \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^-$$

$$\frac{\forall k \in [0, i].\, k \vdash^- \varphi_2}{i \vdash^- \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^-_\infty \qquad \frac{\forall k \in [i, \infty).\, k \vdash^- \varphi_2}{i \vdash^- \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^-_\infty$$

Proof System

positive rules: satisfaction

$$\frac{a \in \rho(i)}{i \vdash^{+} a}\ ap^{+} \qquad \frac{i \vdash^{-} \varphi}{i \vdash^{+} \neg\varphi}\ \neg^{+}$$

$$\frac{i \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee_L^{+} \qquad \frac{i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee_R^{+}$$

$$\frac{i \vdash^{+} \varphi_1 \quad i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \wedge \varphi_2}\ \wedge^{+}$$

$$\frac{j \leq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in (j, i].\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{+}$$

$$\frac{j \geq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in [i, j).\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{+}$$

negative rules: violation

$$\frac{a \notin \rho(i)}{i \vdash^{-} a}\ ap^{-} \qquad \frac{i \vdash^{+} \varphi}{i \vdash^{-} \neg\varphi}\ \neg^{-}$$

$$\frac{i \vdash^{-} \varphi_1 \quad i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \vee \varphi_2}\ \vee^{-}$$

$$\frac{i \vdash^{-} \varphi_1}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge_L^{-} \qquad \frac{i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge_R^{-}$$

$$\frac{j \leq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [j, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}$$

$$\frac{j \geq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [i, j].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}$$

$$\frac{\forall k \in [0, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}_{\infty}^{-} \qquad \frac{\forall k \in [i, \infty).\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}_{\infty}^{-}$$

Proof System

$$\frac{a \in \rho(i)}{i \vdash^+ a}\ ap^+ \qquad \frac{i \vdash^- \varphi}{i \vdash^+ \neg\varphi}\ \neg^+ \qquad \frac{a \notin \rho(i)}{i \vdash^- a}\ ap^- \qquad \frac{i \vdash^+ \varphi}{i \vdash^- \neg\varphi}\ \neg^-$$

$$\frac{i \vdash^+ \varphi_1}{i \vdash^+ \varphi_1 \vee \varphi_2}\ \vee_L^+ \qquad \frac{i \vdash^+ \varphi_2}{i \vdash^+ \varphi_1 \vee \varphi_2}\ \vee_R^+ \qquad \frac{i \vdash^- \varphi_1 \quad i \vdash^- \varphi_2}{i \vdash^- \varphi_1 \vee \varphi_2}\ \vee^-$$

$$\frac{i \vdash^+ \varphi_1 \quad i \vdash^+ \varphi_2}{i \vdash^+ \varphi_1 \wedge \varphi_2}\ \wedge^+ \qquad \frac{i \vdash^- \varphi_1}{i \vdash^- \varphi_1 \wedge \varphi_2}\ \wedge_L^- \qquad \frac{i \vdash^- \varphi_2}{i \vdash^- \varphi_1 \wedge \varphi_2}\ \wedge_R^-$$

$$\frac{j \leq i \quad j \vdash^+ \varphi_2 \quad \forall k \in (j, i].\ k \vdash^+ \varphi_1}{i \vdash^+ \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^+ \qquad \frac{j \leq i \quad j \vdash^- \varphi_1 \quad \forall k \in [j, i].\ k \vdash^- \varphi_2}{i \vdash^- \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^-$$

$$\frac{j \geq i \quad j \vdash^+ \varphi_2 \quad \forall k \in [i, j).\ k \vdash^+ \varphi_1}{i \vdash^+ \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^+ \qquad \frac{j \geq i \quad j \vdash^- \varphi_1 \quad \forall k \in [i, j].\ k \vdash^- \varphi_2}{i \vdash^- \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^-$$

$$\frac{\forall k \in [0, i].\ k \vdash^- \varphi_2}{i \vdash^- \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}_\infty^- \qquad \frac{\forall k \in [i, \infty).\ k \vdash^- \varphi_2}{i \vdash^- \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}_\infty^-$$

$$\frac{a \notin \rho(i)}{i \vdash^{-} a}\ ap^{-} \qquad \frac{i \vdash^{+} \varphi}{i \vdash^{-} \neg\varphi}\ \neg^{-}$$

$$\frac{i \vdash^{-} \varphi_1 \quad i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \vee \varphi_2}\ \vee^{-}$$

$$\frac{i \vdash^{-} \varphi_1}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge_L^{-} \qquad \frac{i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge_R^{-}$$

fixed

$$\frac{a \notin \rho(i)}{i \vdash^{-} a}\ ap^{-}$$

$$\frac{i \vdash^{+} \varphi}{i \vdash^{-} \neg\varphi}\ \neg^{-}$$

$$\frac{i \vdash^{-} \varphi_1 \qquad i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \vee \varphi_2}\ \vee^{-}$$

$$\frac{i \vdash^{-} \varphi_1}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge_L^{-}$$

$$\frac{i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge_R^{-}$$

Proof System

$$\frac{a \in \rho(i)}{i \vdash^{+} a}\ ap^{+} \qquad \frac{i \vdash^{-} \varphi}{i \vdash^{+} \neg\varphi}\ \neg^{+} \qquad \frac{a \notin \rho(i)}{i \vdash^{-} a}\ ap^{-} \qquad \frac{i \vdash^{+} \varphi}{i \vdash^{-} \neg\varphi}\ \neg^{-}$$

$$\frac{i \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{L} \qquad \frac{i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{R} \qquad \frac{i \vdash^{-} \varphi_1 \quad i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \vee \varphi_2}\ \vee^{-}$$

$$\frac{i \vdash^{+} \varphi_1 \quad i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \wedge \varphi_2}\ \wedge^{+} \qquad \frac{i \vdash^{-} \varphi_1}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{L} \qquad \frac{i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{R}$$

$$\frac{j \leq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in (j, i].\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{+} \qquad \frac{j \leq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [j, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}$$

$$\frac{j \geq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in [i, j).\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{+} \qquad \frac{j \geq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [i, j].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}$$

$$\frac{\forall k \in [0, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}_{\infty} \qquad \frac{\forall k \in [i, \infty).\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}_{\infty}$$

$$\frac{j \geq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in [i, j).\, k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1 \,\mathcal{U}\, \varphi_2}\ \mathcal{U}^{+}$$

Proof System

$$\frac{a \in \rho(i)}{i \vdash^{+} a}\ ap^{+} \qquad \frac{i \vdash^{-} \varphi}{i \vdash^{+} \neg\varphi}\ \neg^{+} \qquad \frac{a \notin \rho(i)}{i \vdash^{-} a}\ ap^{-} \qquad \frac{i \vdash^{+} \varphi}{i \vdash^{-} \neg\varphi}\ \neg^{-}$$

$$\frac{i \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{L} \qquad \frac{i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{R} \qquad \frac{i \vdash^{-} \varphi_1 \quad i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \vee \varphi_2}\ \vee^{-}$$

$$\frac{i \vdash^{+} \varphi_1 \quad i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \wedge \varphi_2}\ \wedge^{+} \qquad \frac{i \vdash^{-} \varphi_1}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{L} \qquad \frac{i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{R}$$

$$\frac{j \leq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in (j, i].\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{+} \qquad \frac{j \leq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [j, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}$$

$$\frac{j \geq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in [i, j).\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{+} \qquad \frac{j \geq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [i, j].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}$$

$$\frac{\forall k \in [0, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}_{\infty} \qquad \frac{\forall k \in [i, \infty).\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}_{\infty}$$

$$\frac{j \geq i \quad j \vdash^- \varphi_1 \quad \forall k \in [i, j].\ k \vdash^- \varphi_2}{i \vdash^- \varphi_1 \,\mathcal{U}\, \varphi_2}\ \mathcal{U}^-$$

$$\frac{\forall k \in [i, \infty).\ k \vdash^- \varphi_2}{i \vdash^- \varphi_1 \,\mathcal{U}\, \varphi_2}\ \mathcal{U}^-_\infty$$

$$\rho = uv^{\omega}$$

$$\frac{j \geq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [i, j].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \mathcal{U} \varphi_2}\ \mathcal{U}^{-}$$

$$\frac{\forall k \in [i, \infty).\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \mathcal{U} \varphi_2}\ \mathcal{U}^{-}_{\infty}$$

$$\rho = uv^{\omega}$$

$$\frac{j \geq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [i, j].\, k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \, \mathcal{U} \, \varphi_2} \; \mathcal{U}^{-}$$

$$\frac{\forall k \in [i, max(i, |u| + h_p(\varphi_2) \times |v|) + |v|).\, k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \, \mathcal{U} \, \varphi_2} \; \mathcal{U}^{-}_{\infty}$$

$$\rho = uv^\omega$$

$$\frac{j \geq i \quad j \vdash^- \varphi_1 \quad \forall k \in [i, j].\, k \vdash^- \varphi_2}{i \vdash^- \varphi_1 \,\mathcal{U}\, \varphi_2}\ \mathcal{U}^-$$

$$\frac{\forall k \in [i, max(i, |u| + h_p(\varphi_2) \times |v|) + |v|).\, k \vdash^- \varphi_2}{i \vdash^- \varphi_1 \,\mathcal{U}\, \varphi_2}\ \mathcal{U}^-_\infty$$

soundness based on an argument from
[Markey & Schnoebelen, CONCUR 2003]

Proof System

$$\frac{a \in \rho(i)}{i \vdash^{+} a}\ ap^{+} \qquad \frac{i \vdash^{-} \varphi}{i \vdash^{+} \neg\varphi}\ \neg^{+} \qquad \frac{a \notin \rho(i)}{i \vdash^{-} a}\ ap^{-} \qquad \frac{i \vdash^{+} \varphi}{i \vdash^{-} \neg\varphi}\ \neg^{-}$$

$$\frac{i \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{L} \qquad \frac{i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{R} \qquad \frac{i \vdash^{-} \varphi_1 \quad i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \vee \varphi_2}\ \vee^{-}$$

$$\frac{i \vdash^{+} \varphi_1 \quad i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \wedge \varphi_2}\ \wedge^{+} \qquad \frac{i \vdash^{-} \varphi_1}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{L} \qquad \frac{i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{R}$$

$$\frac{j \leq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in (j, i].\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{+} \qquad \frac{j \leq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [j, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}$$

$$\frac{j \geq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in [i, j).\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{+} \qquad \frac{j \geq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [i, j].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}$$

$$\frac{\forall k \in [0, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}_{\infty} \qquad \frac{\forall k \in [i, max(i, |u| + h_p(\varphi_2) \times |v|) + |v|).\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}_{\infty}$$

Proof Syst

$$\frac{a \in \rho(i)}{i \vdash^{+} a}\ ap^{+} \qquad \frac{i \vdash^{-} \varphi}{i \vdash^{+} \neg\varphi}\ \neg^{+} \qquad \frac{a \notin}{i \vdash^{-}}\ ap^{-}$$

$$\frac{i \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{L} \qquad \frac{i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{R} \qquad \frac{i \qquad i}{i}$$

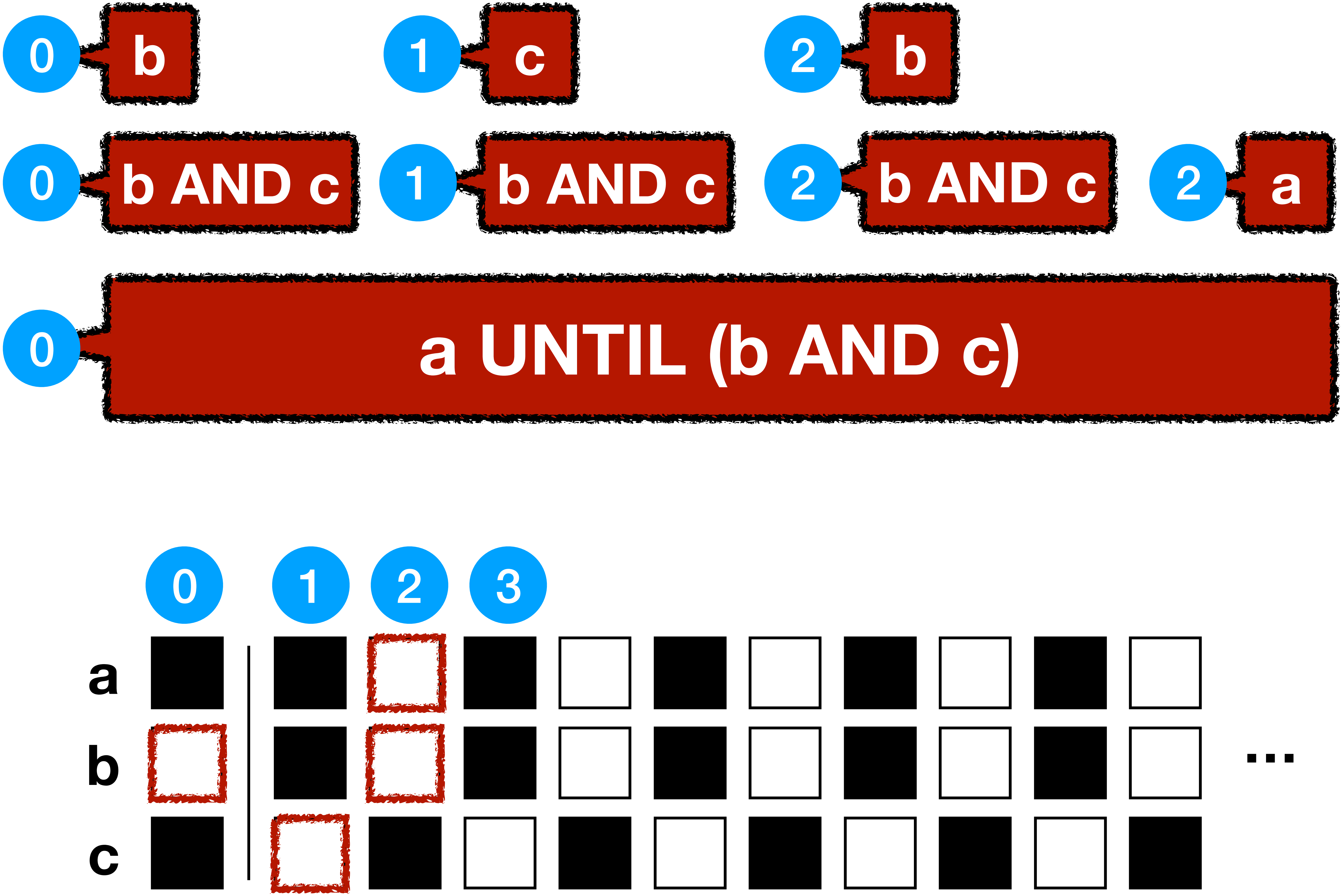
$$\frac{i \vdash^{+} \varphi_1 \quad i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \wedge \varphi_2}\ \wedge^{+} \qquad \frac{i \vdash^{-} \varphi_1}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{L} \qquad \frac{\varphi_2}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{R}$$

$$\frac{j \leq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in (j, i].\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{+} \qquad \frac{j \leq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [j, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}$$

$$\frac{j \geq i \quad j \vdash^{+} \varphi_2 \quad \forall k \in [i, j).\ k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{+} \qquad \frac{j \geq i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [i, j].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}$$

$$\frac{\forall k \in [0, i].\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}_{\infty} \qquad \frac{\forall k \in [i, max(i, |u| + h_p(\varphi_2) \times |v|) + |v|).\ k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}_{\infty}$$

Optimal Proofs

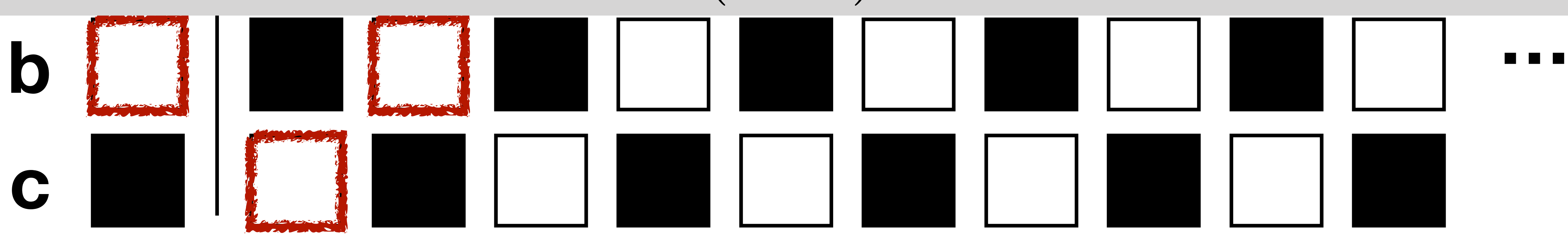

0 b
1 c
2 b
0 b AND c
1 b AND c
2 b AND c
2 a
0 a UNTIL (b AND c)
0
1
2
3
a
b
c
...

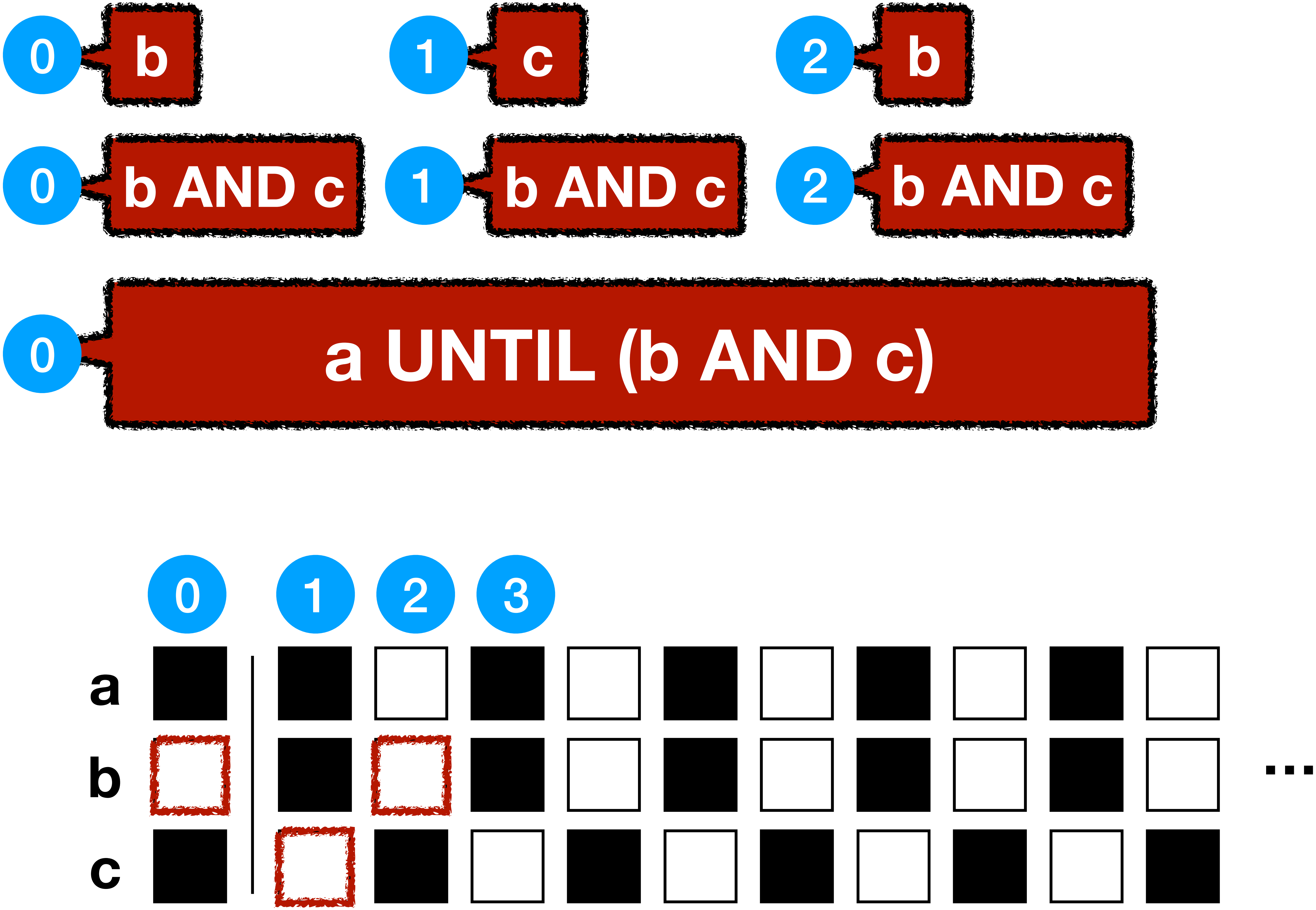
0 b   1 c   2 b

0 b AND c   1 b AND c   2 b AND c   2 a

0 a UNTIL (b AND c)

$$\dfrac{\dfrac{\dfrac{b \notin \{a,c\}}{0 \vdash^- b}\,ap^-}{0 \vdash^- b \wedge c}\,\wedge^-_L \quad \dfrac{\dfrac{c \notin \{a,b\}}{1 \vdash^- c}\,ap^-}{1 \vdash^- b \wedge c}\,\wedge^-_R \quad \dfrac{\dfrac{b \notin \{c\}}{2 \vdash^- b}\,ap^-}{2 \vdash^- b \wedge c}\,\wedge^-_L \quad \dfrac{a \notin \{c\}}{2 \vdash^- a}\,ap^-}{0 \vdash^- a\,\mathcal{U}\,(b \wedge c)}\,\mathcal{U}^-$$




0 b
1 c
2 b
0 b AND c
1 b AND c
2 b AND c
0 a UNTIL (b AND c)
0 1 2 3
a
b
c
...

0 b

1 c

2 b

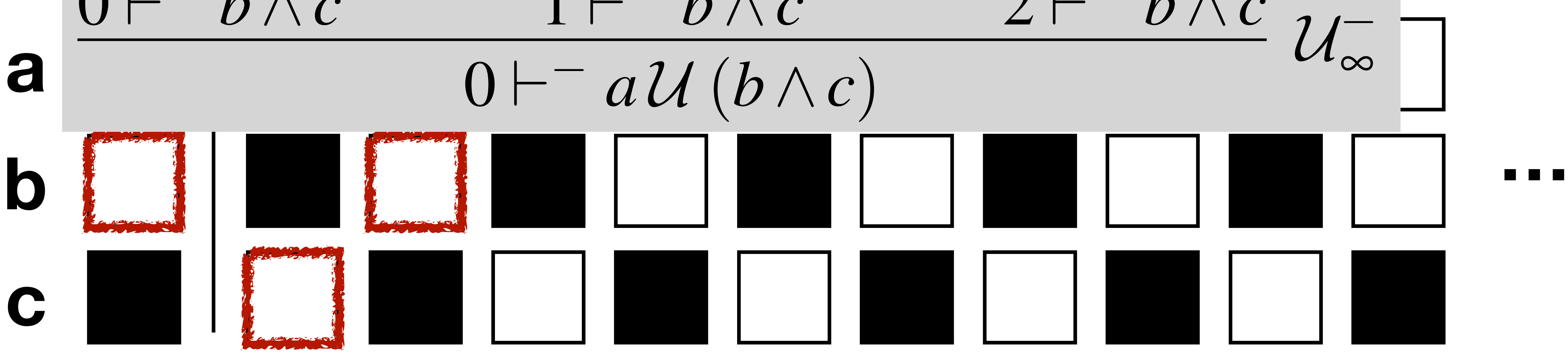
0 b AND c

1 b AND c

2 b AND c

0 a UNTIL (b AND c)

$$\dfrac{\dfrac{\dfrac{b \notin \{a,c\}}{0 \vdash^- b}\,ap^-}{0 \vdash^- b \wedge c}\,\wedge_L^- \qquad \dfrac{\dfrac{c \notin \{a,b\}}{1 \vdash^- c}\,ap^-}{1 \vdash^- b \wedge c}\,\wedge_R^- \qquad \dfrac{\dfrac{b \notin \{c\}}{2 \vdash^- b}\,ap^-}{2 \vdash^- b \wedge c}\,\wedge_L^-}{0 \vdash^- a\,\mathcal{U}\,(b \wedge c)}\,\mathcal{U}_\infty^-$$



$$
\dfrac{\dfrac{\dfrac{b \notin \{a,c\}}{0 \vdash^- b}\,ap^-}{0 \vdash^- b \wedge c}\,\wedge_L^- \qquad \dfrac{\dfrac{c \notin \{a,b\}}{1 \vdash^- c}\,ap^-}{1 \vdash^- b \wedge c}\,\wedge_R^- \qquad \dfrac{\dfrac{b \notin \{c\}}{2 \vdash^- b}\,ap^-}{2 \vdash^- b \wedge c}\,\wedge_L^- \qquad \dfrac{a \notin \{c\}}{2 \vdash^- a}\,ap^-}{0 \vdash^- a\,\mathcal{U}\,(b \wedge c)}\,\mathcal{U}^-
$$

$$
\dfrac{\dfrac{\dfrac{b \notin \{a,c\}}{0 \vdash^- b}\,ap^-}{0 \vdash^- b \wedge c}\,\wedge_L^- \qquad \dfrac{\dfrac{c \notin \{a,b\}}{1 \vdash^- c}\,ap^-}{1 \vdash^- b \wedge c}\,\wedge_R^- \qquad \dfrac{\dfrac{b \notin \{c\}}{2 \vdash^- b}\,ap^-}{2 \vdash^- b \wedge c}\,\wedge_L^-}{0 \vdash^- a\,\mathcal{U}\,(b \wedge c)}\,\mathcal{U}_\infty^-
$$

$$\dfrac{\dfrac{\dfrac{b \notin \{a,c\}}{0 \vdash^- b}\,ap^-}{0 \vdash^- b \wedge c}\,\wedge_L^- \quad \dfrac{\dfrac{c \notin \{a,b\}}{1 \vdash^- c}\,ap^-}{1 \vdash^- b \wedge c}\,\wedge_R^- \quad \dfrac{\dfrac{b \notin \{c\}}{2 \vdash^- b}\,ap^-}{2 \vdash^- b \wedge c}\,\wedge_L^- \quad \dfrac{a \notin \{c\}}{2 \vdash^- a}\,ap^-}{0 \vdash^- a\,\mathcal{U}\,(b \wedge c)}\,\mathcal{U}^-$$

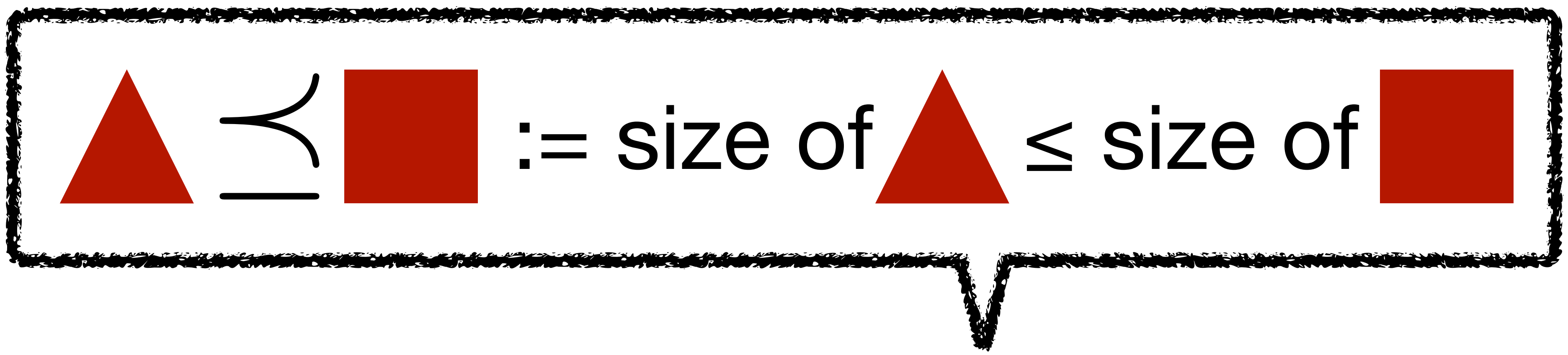
Which one is better?

$$\dfrac{\dfrac{\dfrac{b \notin \{a,c\}}{0 \vdash^- b}\,ap^-}{0 \vdash^- b \wedge c}\,\wedge_L^- \quad \dfrac{\dfrac{c \notin \{a,b\}}{1 \vdash^- c}\,ap^-}{1 \vdash^- b \wedge c}\,\wedge_R^- \quad \dfrac{\dfrac{b \notin \{c\}}{2 \vdash^- b}\,ap^-}{2 \vdash^- b \wedge c}\,\wedge_L^-}{0 \vdash^- a\,\mathcal{U}\,(b \wedge c)}\,\mathcal{U}^-_\infty$$

Well-Quasi-Order on Proofs

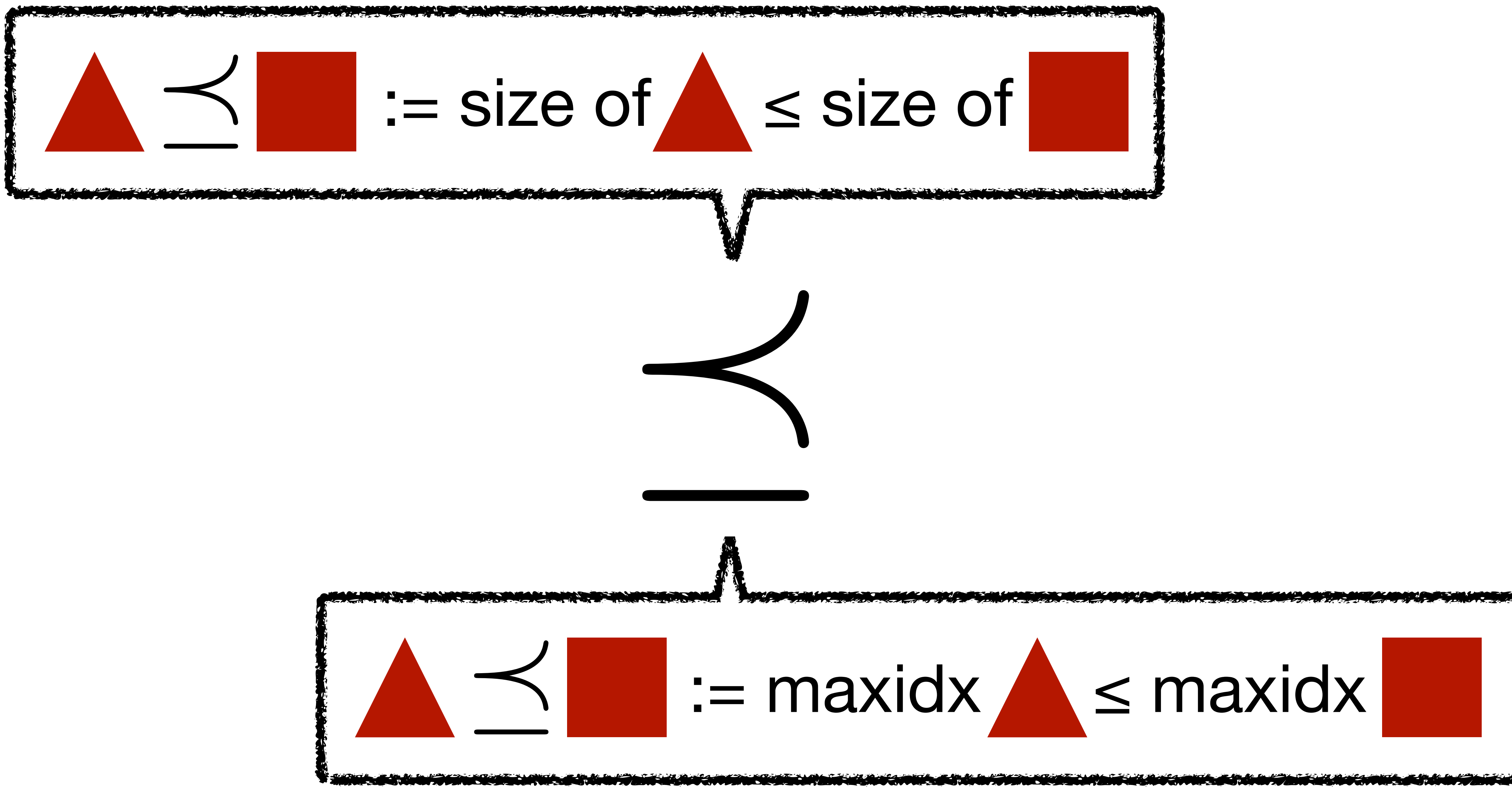
$$\preceq$$

Domain Specific “Better”



$$\preceq$$

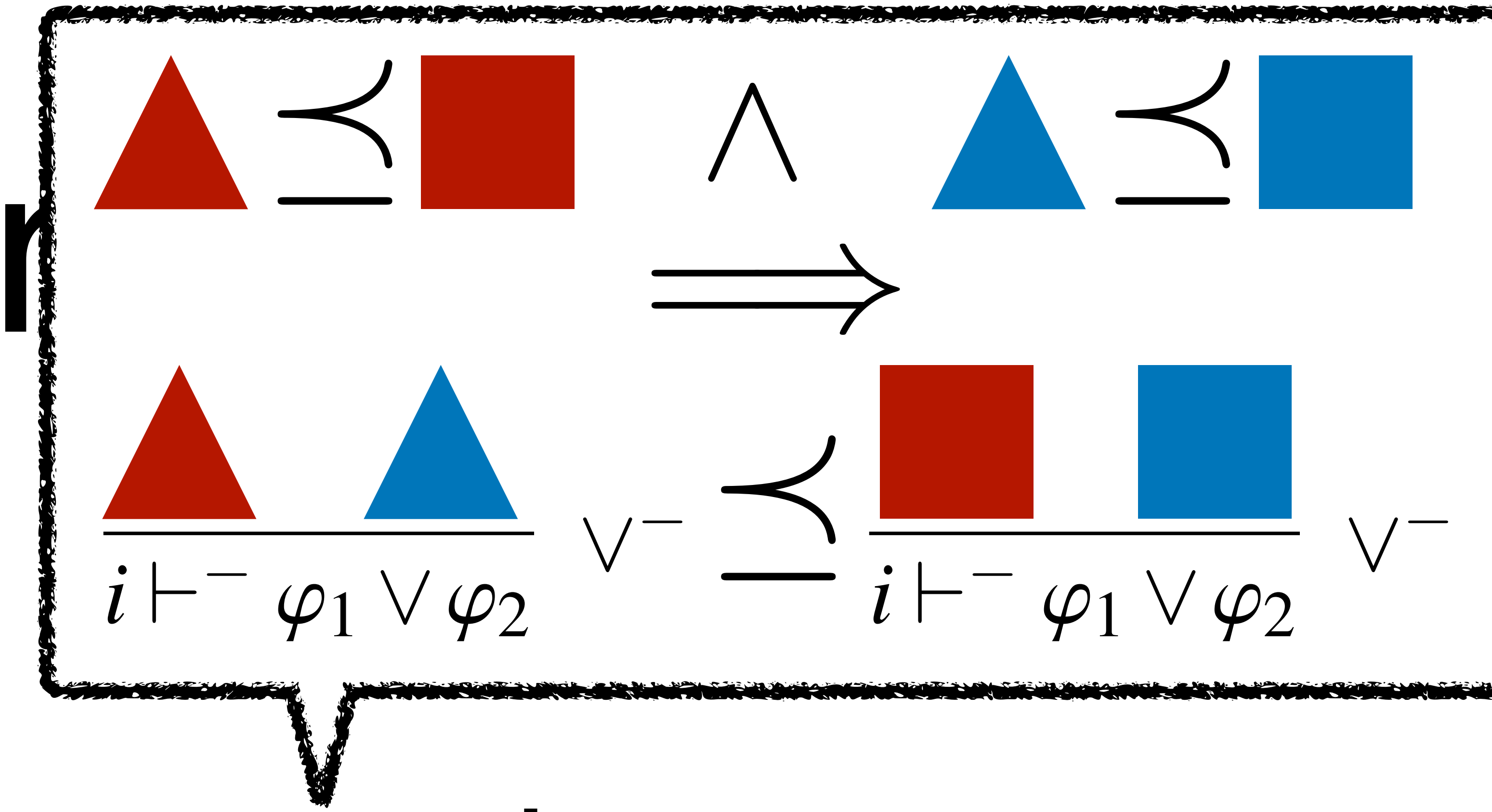
Domain Specific “Better”


⪯ := size of ≤ size of
⪯
⪯ := maxidx ≤ maxidx

Main Result

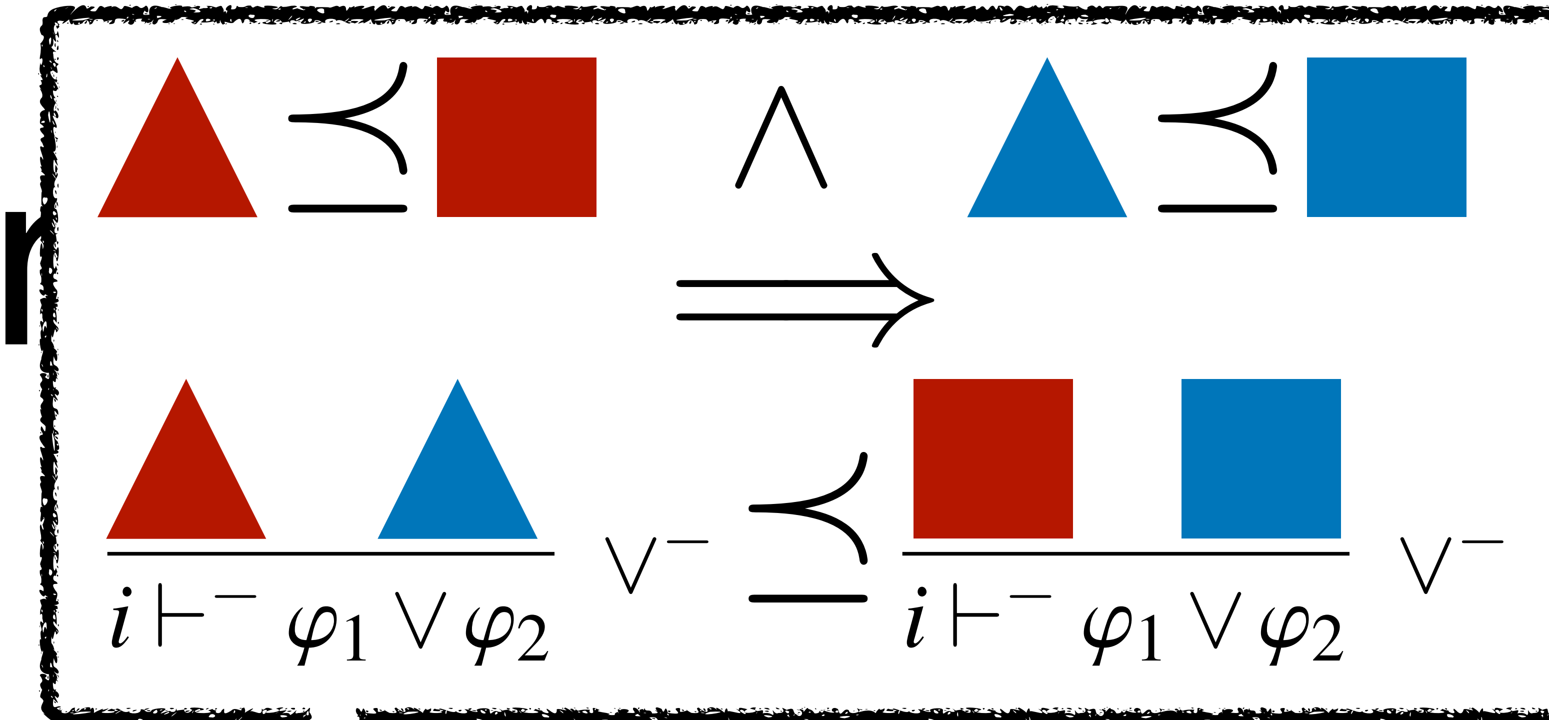
If $\preceq$ is monotone,
then we can compute
a $\preceq$-minimal proof efficiently

Main



If $\preceq$ is monotone,
then we can compute
a $\preceq$-minimal proof efficiently

Main



If $\preceq$ is monotone,
then we can compute
a $\preceq$-minimal proof efficiently

$$\mathcal{O}((|u| + h(\varphi) \cdot |v|) \cdot |\mathsf{SF}(\varphi)| \cdot f(\preceq) \cdot w(\preceq) \cdot |v|)$$

Related Work

Related Work

Chechik & Gurfinkel
***STTT* 2007**

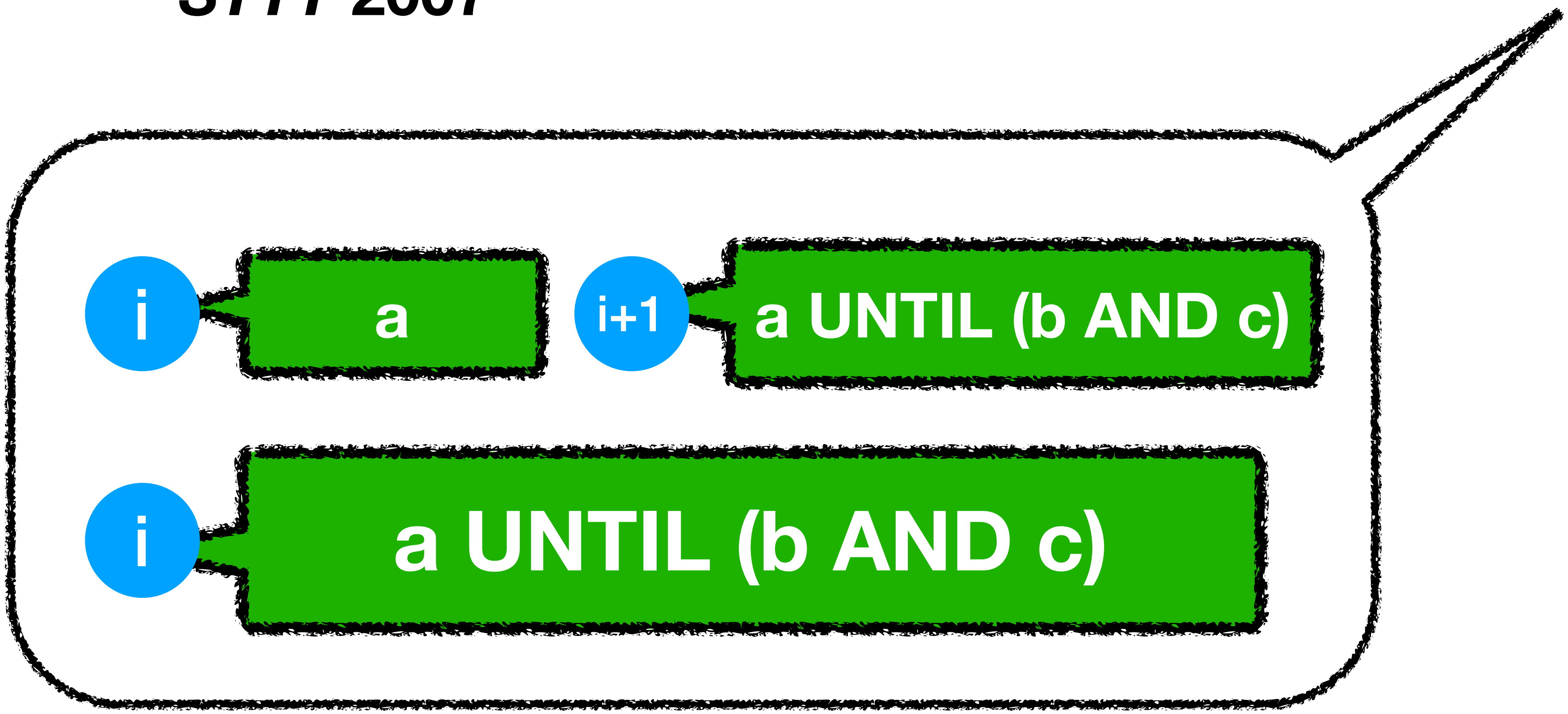
CTL

unrolling

Related Work

Chechik & Gurfinkel
***STTT* 2007**

CTL | **unrolling**



Related Work

	✓	✗
Chechik & Gurfinkel ***STTT* 2007**	**CTL**	**unrolling**
Sulzmann & Zechner **TAP 2012**	**optimal**	**no negation** **finite traces**
Cini & Francalanza **TACAS 2015**	**streaming**	**incomplete** **unrolling**

Prototype & Evaluation

https://bitbucket.org/traytel/explanator

```
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size
```

```
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size
Formula: ¬(◊ □ (¬res ∧ □ ◊ ena) ∧ □ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
Proof:
VNeg{0}
    SImplL{0}
        VConjR{0}
            VAlways{0}
                VEventually{15}
                    [ !x0{15}
                    ; !x0{16} ]
```

```
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size
Formula: ¬(◊ □ (¬res ∧ □ ◊ ena) ∧ □ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
Proof:
VNeg{0}
    SImplL{0}
        VConjR{0}
            VAlways{0}
                VEventually{15}
                    [ !x0{15}
                    ; !x0{16} ]
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O high
```

```
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size
Formula: ¬(◊ □ (¬res ∧ □ ◊ ena) ∧ □ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
Proof:
VNeg{0}
    SImplL{0}
        VConjR{0}
            VAlways{0}
                VEventually{15}
                    [ !x0{15}
                    ; !x0{16} ]
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O high
Formula: ¬(◊ □ (¬res ∧ □ ◊ ena) ∧ □ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
Proof:
VNeg{0}
    SImplR{0}
        SEventually{0}
            SSince{6}
                SSince{6}
                    SSince{6}
                        SSince{6}
                            x4{6}
                            []
                        []
                    []
                []
```

```
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size
Formula: ¬(◊ □ (¬res ∧ □ ◊ ena) ∧ □ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
Proof:
VNeg{0}
    SImplL{0}
        VConjR{0}
            VAlways{0}
                VEventually{15}
                    [ !x0{15}
                    ; !x0{16} ]
```

```
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size
Formula: ¬(◊ ◻ (¬res ∧ ◻ ◊ ena) ∧ ◻ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
Proof:
VNeg{0}
    SImplL{0}
        VConjR{0}
            VAlways{0}
                VEventually{15}
                    [ !x0{15}
                    ; !x0{16} ]
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size -ap
```

```
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size
Formula: ¬(◊ ▫ (¬res ∧ ▫ ◊ ena) ∧ ▫ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
Proof:
VNeg{0}
    SImplL{0}
        VConjR{0}
            VAlways{0}
                VEventually{15}
                    [ !x0{15}
                    ; !x0{16} ]
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size -ap
Formula: ¬(◊ ▫ (¬res ∧ ▫ ◊ ena) ∧ ▫ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
ena|XXXXXXXXX XXX X|XX|
res|X     X      XX|XX|
x0 |  X     X      |  |
x1 |   X     XX    |  |
x2 |    X      X   |  |
x3 |     X      X  |  |
x4 |      X      X |  |
```

Model	Spec	$\|u\|$	$\|v\|$	h_p	h_f	$\preceq_{size}$ $\|p\|$	$maxidx(p)$	$\preceq_{maxidx}$ $\|p\|$	$maxidx(p)$	$\preceq_{\times}$ $\|p\|$	$maxidx(p)$
srg5	φ_0	15	2	4	4	7	16	8	6	7	16
srg5	φ_1	0	16	4	4	621	70	621	33	621	33
dme2	φ_2	0	111	2	1	11	242	14	20	11	20
dme3	φ_2	0	216	2	1	11	494	14	62	11	62
dme4	φ_2	0	280	2	1	11	642	14	82	11	82
abp	φ_3	18	20	2	2	7	59	7	3	7	3
1394-3-2	φ_4	15	2	1	2	7	18	7	18	7	18

Model	Spec	$\|u\|$	$\|v\|$	h_p	h_f	$\preceq_{size}$ $\|p\|$	$\preceq_{size}$ $maxidx(p)$	$\preceq_{maxidx}$ $\|p\|$	$\preceq_{maxidx}$ $maxidx(p)$	$\preceq_{\times}$ $\|p\|$	$\preceq_{\times}$ $maxidx(p)$
srg5	φ_0	15	2	4	4	7	16	8	6	7	16
srg5	φ_1	0	16	4	4	621	70	621	33	621	33
dme2	φ_2	0	111	2	1	11	242	14	20	11	20
dme3	φ_2	0	216	2	1	11	494	14	62	11	62
dme4	φ_2	0	280	2	1	11	642	14	82	11	82
abp	φ_3	18	20	2	2	7	59	7	3	7	3
1394-3-2	φ_4	15	2	1	2	7	18	7	18	7	18

Model	Spec	$\|u\|$	$\|v\|$	h_p	h_f	$\preceq_{size}$ $\|p\|$	$\preceq_{size}$ $maxidx(p)$	$\preceq_{maxidx}$ $\|p\|$	$\preceq_{maxidx}$ $maxidx(p)$	$\preceq_{\times}$ $\|p\|$	$\preceq_{\times}$ $maxidx(p)$
srg5	φ_0	15	2	4	4	7	16	8	6	7	16
srg5	φ_1	0	16	4	4	621	70	621	33	621	33
dme2	φ_2	0	111	2	1	11	242	14	20	11	20
dme3	φ_2	0	216	2	1	11	494	14	62	11	62
dme4	φ_2	0	280	2	1	11	642	14	82	11	82
abp	φ_3	18	20	2	2	7	59	7	3	7	3
1394-3-2	φ_4	15	2	1	2	7	18	7	18	7	18

Model	Spec	$\|u\|$	$\|v\|$	h_p	h_f	$\preceq_{size}$ $\|p\|$	$\preceq_{size}$ $maxidx(p)$	$\preceq_{maxidx}$ $\|p\|$	$\preceq_{maxidx}$ $maxidx(p)$	$\preceq_{\times}$ $\|p\|$	$\preceq_{\times}$ $maxidx(p)$
srg5	φ_0	15	2	4	4	7	16	8	6	7	16
srg5	φ_1	0	16	4	4	621	70	621	33	621	33
dme2	φ_2	0	111	2	1	11	242	14	20	11	20
dme3	φ_2	0	216	2	1	11	494	14	62	11	62
dme4	φ_2	0	280	2	1	11	642	14	82	11	82
abp	φ_3	18	20	2	2	7	59	7	3	7	3
1394-3-2	φ_4	15	2	1	2	7	18	7	18	7	18

$$\varphi_0 = \neg((\Diamond\Box(\neg p) \wedge \Box\Diamond q) \wedge \Box\Diamond x_0) \rightarrow \Diamond(x_0\,\mathcal{S}\,(x_1\,\mathcal{S}\,(x_2\,\mathcal{S}\,(x_3\,\mathcal{S}\,x_4))))$$

Model	Spec	$\|u\|$	$\|v\|$	h_p	h_f	$\preceq_{size}$ $\|p\|$	$\preceq_{size}$ $maxidx(p)$	$\preceq_{maxidx}$ $\|p\|$	$\preceq_{maxidx}$ $maxidx(p)$	$\preceq_{\times}$ $\|p\|$	$\preceq_{\times}$ $maxidx(p)$
srg5	φ_0	15	2	4	4	7	16	8	6	7	16
srg5	φ_1	0	16	4	4	621	70	621	33	621	33
dme2	φ_2	0	111	2	1	11	242	14	20	11	20
dme3	φ_2	0	216	2	1	11	494	14	62	11	62
dme4	φ_2	0	280	2	1	11	642	14	82	11	82
abp	φ_3	18	20	2	2	7	59	7	3	7	3
1394-3-2	φ_4	15	2	1	2	7	18	7	18	7	18

$$\varphi_0 = \neg((\Diamond\Box(\neg p) \wedge \Box\Diamond q) \wedge \Box\Diamond x_0) \rightarrow \Diamond(x_0\, \mathcal{S}\, (x_1\, \mathcal{S}\, (x_2\, \mathcal{S}\, (x_3\, \mathcal{S}\, x_4))))$$

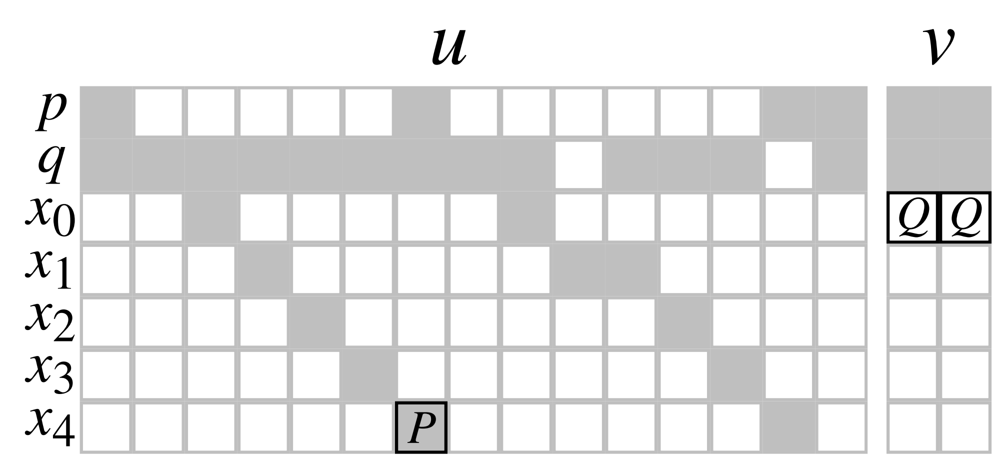
$$\begin{aligned} P = {} & \neg^-(\rightarrow_R^+(\Diamond^+ \\ & (\mathcal{S}^+(\mathcal{S}^+(\mathcal{S}^+(\mathcal{S}^+(ap^+(x_4, 6), []), []), []), [])))) \\ Q = {} & \neg^-(\rightarrow_L^+(\wedge_R^-(\Box^-(\Diamond^- \\ & ([ap^-(x_0, 15), ap^-(x_0, 16)]))))) \end{aligned}$$

Model	Spec	$\|u\|$	$\|v\|$	h_p	h_f	$\preceq_{size}$ $\|p\|$	$\preceq_{size}$ $maxidx(p)$	$\preceq_{maxidx}$ $\|p\|$	$\preceq_{maxidx}$ $maxidx(p)$	$\preceq_{\times}$ $\|p\|$	$\preceq_{\times}$ $maxidx(p)$
srg5	φ_0	15	2	4	4	7	16	8	6	7	16
srg5	φ_1	0	16	4	4	621	70	621	33	621	33
dme2	φ_2	0	111	2	1	11	242	14	20	11	20
dme3	φ_2	0	216	2	1	11	494	14	62	11	62
dme4	φ_2	0	280	2	1	11	642	14	82	11	82
abp	φ_3	18	20	2	2	7	59	7	3	7	3
1394-3-2	φ_4	15	2	1	2	7	18	7	18	7	18

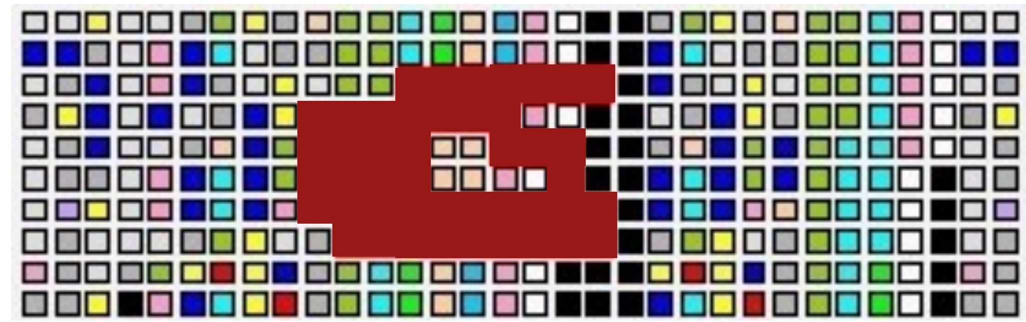
$$\varphi_0 = \neg((\Diamond\Box(\neg p) \wedge \Box\Diamond q) \wedge \Box\Diamond x_0) \rightarrow \Diamond(x_0\, \mathcal{S}\, (x_1\, \mathcal{S}\, (x_2\, \mathcal{S}\, (x_3\, \mathcal{S}\, x_4))))$$

$$P = \neg^-(\rightarrow_R^+(\Diamond^+ (\mathcal{S}^+(\mathcal{S}^+(\mathcal{S}^+(\mathcal{S}^+(ap^+(x_4,6),[]),[]),[]),[]))))$$

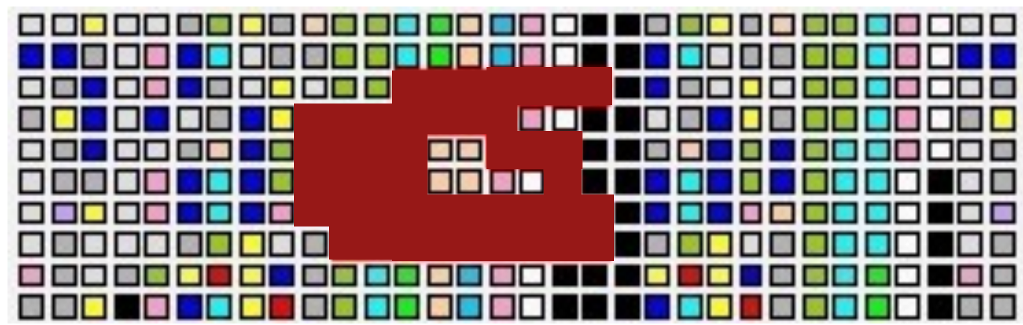
$$Q = \neg^-(\rightarrow_L^+(\wedge_R^-(\Box^-(\Diamond^- ([ap^-(x_0,15),ap^-(x_0,16)])))))$$



Vaporware



Vaporware



Theory

$$\frac{a\in\rho(i)}{i\vdash^+ a}\,ap^+ \qquad \frac{i\vdash^-\varphi}{i\vdash^+\neg\varphi}\,\neg^+ \qquad \frac{a\notin\rho(i)}{i\vdash^- a}\,ap^- \qquad \frac{i\vdash^+\varphi}{i\vdash^-\neg\varphi}\,\neg^-$$

$$\frac{i\vdash^+\varphi_1}{i\vdash^+\varphi_1\vee\varphi_2}\,\vee^+_L \qquad \frac{i\vdash^+\varphi_2}{i\vdash^+\varphi_1\vee\varphi_2}\,\vee^+_R \qquad \frac{i\vdash^-\varphi_1\quad i\vdash^-\varphi_2}{i\vdash^-\varphi_1\vee\varphi_2}\,\vee^-$$

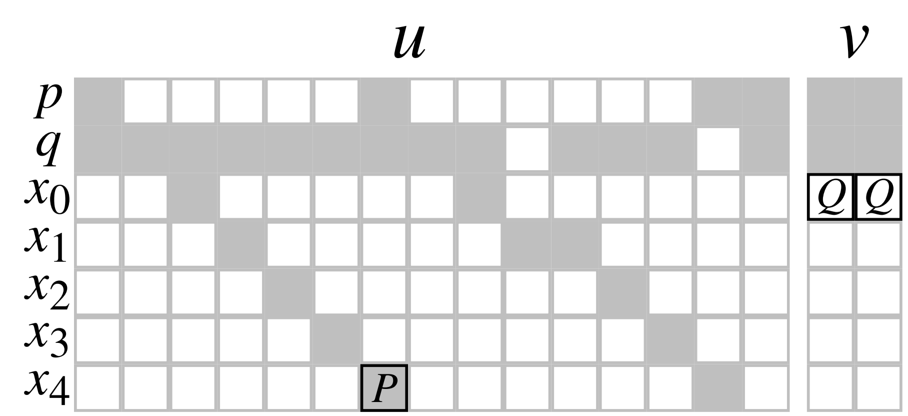
$$\frac{i\vdash^+\varphi_1\quad i\vdash^+\varphi_2}{i\vdash^+\varphi_1\wedge\varphi_2}\,\wedge^+ \qquad \frac{i\vdash^-\varphi_1}{i\vdash^-\varphi_1\wedge\varphi_2}\,\wedge^-_L \qquad \frac{i\vdash^-\varphi_2}{i\vdash^-\varphi_1\wedge\varphi_2}\,\wedge^-_R$$

$$\frac{j\le i\quad j\vdash^+\varphi_2\quad \forall k\in(j,i].\,k\vdash^+\varphi_1}{i\vdash^+\varphi_1\,\mathcal{S}\,\varphi_2}\,\mathcal{S}^+ \qquad \frac{j\le i\quad j\vdash^-\varphi_1\quad \forall k\in[j,i].\,k\vdash^-\varphi_2}{i\vdash^-\varphi_1\,\mathcal{S}\,\varphi_2}\,\mathcal{S}^-$$

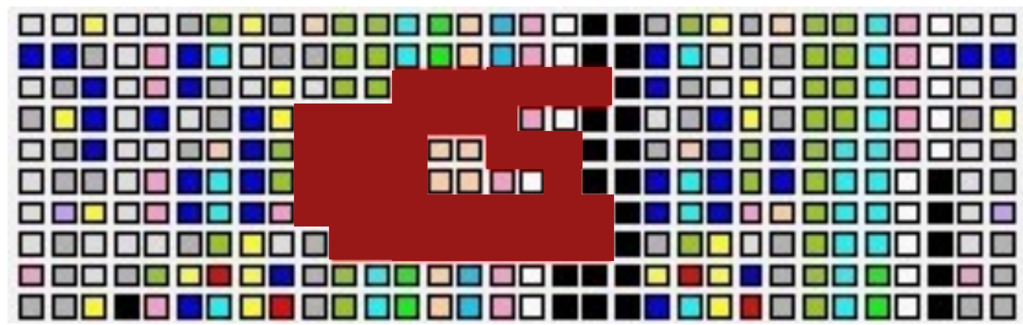
$$\frac{j\ge i\quad j\vdash^+\varphi_2\quad \forall k\in[i,j).\,k\vdash^+\varphi_1}{i\vdash^+\varphi_1\,\mathcal{U}\,\varphi_2}\,\mathcal{U}^+ \qquad \frac{j\ge i\quad j\vdash^-\varphi_1\quad \forall k\in[i,j].\,k\vdash^-\varphi_2}{i\vdash^-\varphi_1\,\mathcal{U}\,\varphi_2}\,\mathcal{U}^-$$

$$\frac{\forall k\in[0,i].\,k\vdash^-\varphi_2}{i\vdash^-\varphi_1\,\mathcal{S}\,\varphi_2}\,\mathcal{S}^-_\infty \qquad \frac{\forall k\in[i,max(i,|u|+h_p(\varphi_2)\times|v|)+|v|).\,k\vdash^-\varphi_2}{i\vdash^-\varphi_1\,\mathcal{U}\,\varphi_2}\,\mathcal{U}^-_\infty$$

$\preceq$



Vaporware



Theory

$$\frac{a \in \rho(i)}{i \vdash^{+} a}\ ap^{+} \qquad \frac{i \vdash^{-} \varphi}{i \vdash^{+} \neg\varphi}\ \neg^{+} \qquad \frac{a \notin \rho(i)}{i \vdash^{-} a}\ ap^{-} \qquad \frac{i \vdash^{+} \varphi}{i \vdash^{-} \neg\varphi}\ \neg^{-}$$

$$\frac{i \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{L} \qquad \frac{i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \vee \varphi_2}\ \vee^{+}_{R} \qquad \frac{i \vdash^{-} \varphi_1 \quad i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \vee \varphi_2}\ \vee^{-}$$

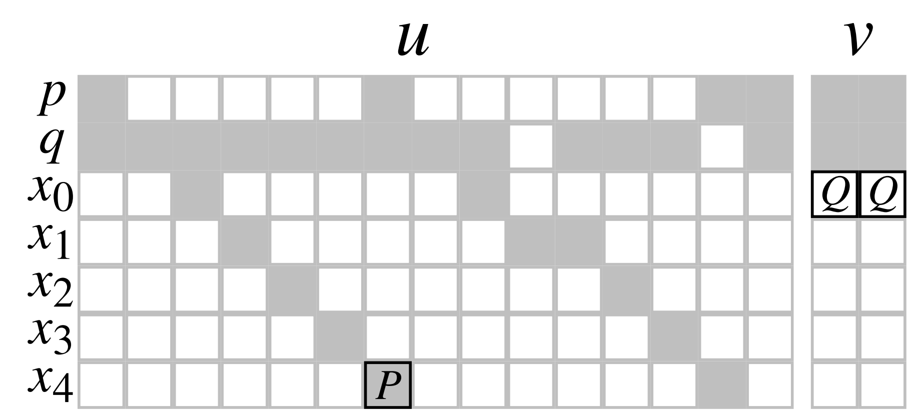
$$\frac{i \vdash^{+} \varphi_1 \quad i \vdash^{+} \varphi_2}{i \vdash^{+} \varphi_1 \wedge \varphi_2}\ \wedge^{+} \qquad \frac{i \vdash^{-} \varphi_1}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{L} \qquad \frac{i \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1 \wedge \varphi_2}\ \wedge^{-}_{R}$$

$$\frac{j \le i \quad j \vdash^{+} \varphi_2 \quad \forall k \in (j, i].\, k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{+} \qquad \frac{j \le i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [j, i].\, k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}$$

$$\frac{j \ge i \quad j \vdash^{+} \varphi_2 \quad \forall k \in [i, j).\, k \vdash^{+} \varphi_1}{i \vdash^{+} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{+} \qquad \frac{j \ge i \quad j \vdash^{-} \varphi_1 \quad \forall k \in [i, j].\, k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}$$

$$\frac{\forall k \in [0, i].\, k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{S}\, \varphi_2}\ \mathcal{S}^{-}_{\infty} \qquad \frac{\forall k \in [i, max(i, |u| + h_p(\varphi_2) \times |v|) + |v|).\, k \vdash^{-} \varphi_2}{i \vdash^{-} \varphi_1\, \mathcal{U}\, \varphi_2}\ \mathcal{U}^{-}_{\infty}$$

$$\preceq$$



Prototype

```
> explanator -nusmv -log nusmv-runs/srg5.ptimoneg.ltl.txt -O size -ap
Formula: ¬(◊ □ (¬res ∧ □ ◊ ena) ∧ □ ◊ x0 → ◊ (x0 S (x1 S (x2 S (x3 S x4)))))
ena|XXXXXXXXX XXX X|XX|
res|X     X      XX|XX|
x0 |  X     X      |  |
x1 |   X     XX    |  |
x2 |    X      X   |  |
x3 |     X      X  |  |
x4 |      X      X |  |
```

Read the proofs.

Read the proofs.
They explain things!

Optimal Proofs for LTL on Lasso Words

David Basin Bhargav Bhatt Dmitriy Traytel

ETH zürich

75 NRP
Big Data
National Research Programme