Runtime verification of fixpoint logic: Synthesis of optimal monitors

Karoliina Lehtinen

University of Kiel

January 2018
Runtime monitoring

Karoliina Lehtinen

Synthesis of optimal monitors
The set-up

- A process $p$ (described by a CCS process)

$$p, p' := \text{end} \mid \alpha.p \mid \text{rec}x.p \mid x \mid p + p'$$
The set-up

- A process $p$ (described by a CCS process)

$$p, p' := \text{end} \mid \alpha.p \mid \text{rec}x.p \mid x \mid p + p'$$

- A system specification $\psi$ in your favourite logic: Hennessy–Milner logic with recursion

$$\psi := \top \mid \bot \mid \langle \alpha \rangle \psi \mid [\alpha] \psi \mid \psi \lor \psi' \mid \psi \land \psi' \mid X \mid \mu X.\psi \mid \nu X.\psi$$
The set-up

- A process \( p \) (described by a CCS process)

\[
p, p' := \text{end} \mid \alpha.p \mid \text{rec}x.p \mid x \mid p + p'
\]

- A system specification \( \psi \) in your favourite logic: Hennessy–Milner logic with recursion

\[
\psi := T \mid \bot \mid \langle \alpha \rangle \psi \mid [\alpha] \psi \mid \psi \lor \psi' \mid \psi \land \psi' \mid X \mid \mu X.\psi \mid \nu X.\psi
\]

- A monitor \( m \) (also described by a CCS process)

\[
p, p' := \text{yes} \mid \text{no} \mid \text{end} \mid \alpha.p \mid \text{rec}x.p \mid x \mid p + p'
\]
The set-up

- A process $p$ (described by a CCS process)

\[ p, p' := \text{end} \mid \alpha.p \mid \text{rec}x.p \mid x \mid p + p' \]

- A system specification $\psi$ in your favourite logic: Hennessy–Milner logic with recursion

\[ \psi := \top \mid \bot \mid \langle \alpha \rangle \psi \mid [\alpha] \psi \mid \psi \lor \psi' \mid \psi \land \psi' \mid X \mid \mu X. \psi \mid \nu X. \psi \]

- A monitor $m$ (also described by a CCS process)

\[ p, p' := \text{yes} \mid \text{no} \mid \text{end} \mid \alpha.p \mid \text{rec}x.p \mid x \mid p + p' \]

- An instrumentation $m \triangleright p$

  - $m$ can accept $p$,
  - $m$ can reject $p$,
  - $m$ can be indecisive about $p$. 

Goal: Given $\psi$, find a good monitor for $\psi$. 

Karoliina Lehtinen  |  Synthesis of optimal monitors
The set-up

- A process $p$ (described by a CCS process)

$$ p, p' := \text{end} \mid \alpha.p \mid \text{rec}.x.p \mid x \mid p + p' $$

- A system specification $\psi$ in your favourite logic: Hennessy–Milner logic with recursion

$$ \psi := \top \mid \bot \mid \langle \alpha \rangle \psi \mid [\alpha] \psi \mid \psi \lor \psi' \mid \psi \land \psi' \mid X \mid \mu X.\psi \mid \nu X.\psi $$

- A monitor $m$ (also described by a CCS process)

$$ p, p' := \text{yes} \mid \text{no} \mid \text{end} \mid \alpha.p \mid \text{rec}.x.p \mid x \mid p + p' $$

- An instrumentation $m \triangleleft p$
  - $m$ can accept $p$,
  - $m$ can reject $p$,
  - $m$ can be indecisive about $p$.

Goal: Given $\psi$, find a **good** monitor for $\psi$. 
A good monitor is sound

The monitor $m$ is a sound monitor for $\psi$ if:
- $\text{acc}(m, p)$ implies $p \in \psi$, and
- $\text{rej}(m, p)$ implies $p \notin \psi$.

Note: only uni-verdict monitors are sound.

A great monitor is complete

The monitor $m$ is violation-complete for $\psi$ if
- $p \notin \psi$ implies $\text{rej}(m, p)$.

The monitor $m$ is satisfaction-complete for $\psi$ if
- $p \in \psi$ implies $\text{acc}(m, p)$.

A monitor is complete for if it is violation- or satisfaction-complete.
Sound and complete monitors

Theorem (Francalanza, Aceto, Ingólfsdóttir 2015)

A $\mu$HML formula has a **sound and violation complete** monitor if and only if it is in the **safety** fragment of $\mu$HML.

$$\psi, \psi' := \top \mid \bot \mid [\alpha]\psi \mid \nu X.\psi \mid \psi \land \psi'$$

What if $\psi$ is not in this fragment?
Sound and complete monitors

Theorem (Francalanza, Aceto, Ingólfdóttir 2015)

A $\mu$HML formula has a sound and violation complete monitor if and only if it is in the safety fragment of $\mu$HML.

$$\psi, \psi' := \top | \bot | [\alpha]\psi | \nu X.\psi | \psi \land \psi'$$

What if $\psi$ is not in this fragment?

Good, better and optimal monitors

A monitor $m$ is optimal for $\psi$ if:

- $m$ is sound for $\psi$;
- If $m'$ is sound for $\psi$, then $\text{rej}(m', p)$ implies $\text{rej}(m, p)$. 
Problem: Given a $\mu$HML formula, what is its optimal monitor?

Solution

- Reduce the problem to finding the strongest safety consequence of $\psi$.
- Find the strongest safety consequence of $\psi$.
Problem: Given a $\mu$HML formula, what is its optimal monitor?

Solution

- Reduce the problem to finding the strongest safety consequence of $\psi$.
- Find the strongest safety consequence of $\psi$. 
Contributions

Problem: Given a $\mu$HML formula, what is its optimal monitor?

Solution

- Reduce the problem to finding the strongest safety consequence of $\psi$.
- Find the strongest safety consequence of $\psi$. 

![Diagram showing $\psi$ and $\mu$HML with Safety and crosses indicating violations]
**Theorem**

*Finding the optimal rejection-monitor of $\psi$ reduces to finding the strongest consequence of $\psi$ in the safety fragment of $\mu$HML.*
Finding the optimal rejection-monitor of $\psi$ reduces to finding the strongest consequence of $\psi$ in the safety fragment of $\mu$HML.

The strongest safety consequence of $\psi$ is a formula $\theta$ such that:

- $\theta$ is a safety formula,
- $\psi$ implies $\theta$, and
- If $\psi$ implies $\theta'$ and $\theta'$ is a safety formula, then $\theta$ implies $\theta'$
Finding the optimal rejection-monitor of $\psi$ reduces to finding the strongest consequence of $\psi$ in the safety fragment of $\mu$HML.

**Definition**

The **strongest safety consequence** of $\psi$ is a formula $\theta$ such that:

- $\theta$ is a safety formula,
- $\psi$ implies $\theta$, and
- If $\psi$ implies $\theta'$ and $\theta'$ is a safety formula, then $\theta$ implies $\theta'$

**Proof.**

- Optimal monitor for $\psi$ is sound and complete for strongest safety consequence $\theta$ of $\psi$. 
Synthesis of the strongest safety consequence

The problem

Given \( \psi \), find \( \theta \) such that

- \( \theta \) is a safety formula,
- \( \psi \) implies \( \theta \), and
- If \( \psi \) implies \( \theta' \) and \( \theta' \) is a safety formula, then \( \theta \) implies \( \theta' \)

The solution

Formula transformation:
Synthesis of the strongest safety consequence

The problem

Given $\psi$, find $\theta$ such that
- $\theta$ is a safety formula,
- $\psi$ implies $\theta$, and
- If $\psi$ implies $\theta'$ and $\theta'$ is a safety formula, then $\theta$ implies $\theta'$

The solution

Formula transformation:

1. Eliminate $\langle \alpha \rangle$-subformulas.

While preserving safety consequences.
The problem

Given $\psi$, find $\theta$ such that

- $\theta$ is a safety formula,
- $\psi$ implies $\theta$, and
- If $\psi$ implies $\theta'$ and $\theta'$ is a safety formula, then $\theta$ implies $\theta'$

The solution

Formula transformation:

1. Eliminate $\langle \alpha \rangle$-subformulas.
2. Turn $\mu$-operators into $\nu$-operators.

While preserving safety consequences.
Synthesis of the strongest safety consequence

The problem

Given \( \psi \), find \( \theta \) such that
- \( \theta \) is a safety formula,
- \( \psi \) implies \( \theta \), and
- If \( \psi \) implies \( \theta' \) and \( \theta' \) is a safety formula, then \( \theta \) implies \( \theta' \)

The solution

Formula transformation:

1. Eliminate \( \langle \alpha \rangle \)-subformulas.
2. Turn \( \mu \)-operators into \( \nu \)-operators.
3. Turn \( [\alpha] \psi \lor [\alpha] \psi' \) into \( [\alpha] \psi \lor \psi' \)

While preserving safety consequences.
Step 1: Eliminating $\langle \alpha \rangle$

**Lemma**

Let $\Psi$ be a formula in **disjunctive normal form**. Obtain $\Psi'$ from $\Psi$ by replacing subformulas $\langle \alpha \rangle \phi$ with:

- $\bot$ if $\phi$ is unsatisfiable, $\top$ otherwise.

$\Psi$ has the same safety consequences as $\Psi'$.

**Proof (idea).**

$\bot$-substitution preserves semantics, trivially correct.
For $\top$-substitution, look at counterexample:

- Safety consequence $\theta$ of $\Psi$
- $T$ such that $T \models \neg \theta \land \Psi'$
- Build $T'$ such that $T' \models \Psi \land \neg \theta$, a contradiction.
Proof of: If $\Psi \implies \theta$ then $\Psi' \implies \theta$ for safety $\theta$.

- Assume $T \models \neg \theta \land \Psi'$.
Step 1: Eliminating $\langle \alpha \rangle$

Proof of: If $\Psi \implies \theta$ then $\Psi' \implies \theta$ for safety $\theta$.

- Assume $T \models \neg \theta \land \Psi'$.
- Find nodes at which the $\Psi'$-proof proves $\top$ (from $\langle \alpha \rangle \phi$ in $\Psi$).
Step 1: Eliminating $\langle \alpha \rangle$

Proof of: If $\Psi \implies \theta$ then $\Psi' \implies \theta$ for safety $\theta$.

- Assume $T \models \neg \theta \land \Psi'$.
- Find nodes at which the $\Psi'$-proof proves $\top$ (from $\langle \alpha \rangle \phi$ in $\Psi$).
- Build $T'$ from $T$: Add $\alpha$-successors that satisfy $\phi$ for every $\langle \alpha \rangle \phi$ in $\Psi$. 

Karoliina Lehtinen  Synthesis of optimal monitors
Step 1: Eliminating $\langle \alpha \rangle$

Proof of: If $\Psi \Rightarrow \theta$ then $\Psi' \Rightarrow \theta$ for safety $\theta$.

- Assume $T \models \neg \theta \land \Psi'$.
- Find nodes at which the $\Psi'$-proof proves $\top$ (from $\langle \alpha \rangle \phi$ in $\Psi$).
- Build $T'$ from $T$: Add $\alpha$-successors that satisfy $\phi$ for every $\langle \alpha \rangle \phi$ in $\Psi$.
- $\Psi'$-proof in $T$ becomes $\Psi$-proof in $T'$: $T' \models \Psi$
Step 1: Eliminating $\langle \alpha \rangle$

Proof of: If $\Psi \implies \theta$ then $\Psi' \implies \theta$ for safety $\theta$.

- Assume $T \models \neg \theta \land \Psi'$.
- Find nodes at which the $\Psi'$-proof proves $\top$ (from $\langle \alpha \rangle \phi$ in $\Psi$).
- Build $T'$ from $T$: Add $\alpha$-successors that satisfy $\phi$ for every $\langle \alpha \rangle \phi$ in $\Psi$.
- $\Psi'$-proof in $T$ becomes $\Psi$-proof in $T'$: $T' \models \Psi$
- $\neg \theta$ is not affected by adding successors: $T \not\models \theta$
Step 1: Eliminating $\langle \alpha \rangle$

Proof of: If $\Psi \Rightarrow \theta$ then $\Psi' \Rightarrow \theta$ for safety $\theta$.

- Assume $T \models \neg \theta \land \Psi'$.
- Find nodes at which the $\Psi'$-proof proves $\top$ (from $\langle \alpha \rangle \phi$ in $\Psi$).
- Build $T'$ from $T$: Add $\alpha$-successors that satisfy $\phi$ for every $\langle \alpha \rangle \phi$ in $\Psi$.
- $\Psi'$-proof in $T$ becomes $\Psi$-proof in $T'$: $T' \models \Psi$
- $\neg \theta$ is not affected by adding successors: $T \not\models \theta$
- A contradiction. $\Psi' \Rightarrow \theta$. 

Karoliina Lehtinen
Synthesis of optimal monitors
Lemma

Let $\Psi$ be a formula without $\langle \alpha \rangle$-subformulas. Obtain $\Psi'$ from $\Psi$ by replacing $\mu$-operators with $\nu$-operators. $\Psi$ has the same safety consequences as $\Psi'$.

Proof

Let $\theta$ be a safety consequence of $\Psi$: $\neg \theta \implies \neg \Psi$.

Therefore $\neg \theta \implies \neg \Psi'$.
Lemma

Let $\Psi$ be a formula without $\langle \alpha \rangle$-subformulas. Obtain $\Psi'$ from $\Psi$ by replacing $\mu$-operators with $\nu$-operators. $\Psi$ has the same safety consequences as $\Psi'$.

Proof

Let $\theta$ be a safety consequence of $\Psi$: $\neg \theta \implies \neg \Psi$.

- If $T \models \neg \theta$, then there is a finite prefix $T'$ of $T$ such that no completion of $T'$ satisfies $\theta$.

Therefore $\neg \theta \implies \neg \Psi'$.
Step 2: Eliminating $\mu$

**Lemma**

Let $\Psi$ be a formula without $\langle \alpha \rangle$-subformulas. Obtain $\Psi'$ from $\Psi$ by replacing $\mu$-operators with $\nu$-operators. $\Psi$ has the same safety consequences as $\Psi'$.

**Proof**

Let $\theta$ be a safety consequence of $\Psi$: $\neg \theta \implies \neg \Psi$.

- If $T \models \neg \theta$, then there is a finite prefix $T'$ of $T$ such that no completion of $T'$ satisfies $\theta$.
- $\Psi$ and $\Psi'$ agree on finite models: $T' \models \neg \Psi \land \neg \Psi'$.

Therefore $\neg \theta \implies \neg \Psi'$.
Step 2: Eliminating $\mu$

Lemma

Let $\Psi$ be a formula without $\langle \alpha \rangle$-subformulas. Obtain $\Psi'$ from $\Psi$ by replacing $\mu$-operators with $\nu$-operators. $\Psi$ has the same safety consequences as $\Psi'$.

Proof

Let $\theta$ be a safety consequence of $\Psi$: $\neg \theta \iff \neg \Psi$.

- If $T \models \neg \theta$, then there is a finite prefix $T'$ of $T$ such that no completion of $T'$ satisfies $\theta$.
- $\Psi$ and $\Psi'$ agree on finite models: $T' \models \neg \Psi \land \neg \Psi'$.
- $\Psi'$ has no $\langle \alpha \rangle$, therefore $\neg \Psi'$ has no $[\alpha]$.
  A proof of $\neg \Psi'$ in $T'$ is a proof of $\neg \Psi'$ in $T$.

Therefore $\neg \theta \iff \neg \Psi'$.
Step 3: Eliminate $\lor$

**Idea**

- Push disjunctions between matching modalities inwards: $[\alpha] \psi \lor [\alpha] \psi'$ becomes $[\alpha] (\psi \lor \psi')$;
- Eliminate non-matching modalities: $[\alpha] \psi \lor [\beta] \psi'$ becomes $\top$.

**Execution**

- Tableau-construction
- Almost dual to transformation into disjunctive normal form

**Output**

Strongest safety consequence.
Example

\[ \nu X. [\alpha]([\alpha]X \land [\beta]\perp) \lor [\alpha]([\alpha]\perp \land [\gamma]\perp) \]
Example

$$\forall X. [\alpha]([\alpha]X \land [\beta]\bot) \lor [\alpha]([\alpha]\bot \land [\beta]X)$$
Example

$$\frac{[\alpha](\left[\alpha\right]X \land [\beta] \perp) \lor [\alpha](\left[\alpha\right] \perp \land [\beta]X)}{\nu X.\left[\alpha\right]([\alpha]X \land [\beta] \perp) \lor [\alpha](\left[\alpha\right] \perp \land [\beta]X)}$$
Example

\[
\begin{align*}
[\alpha](\left[\alpha\right]X \land [\beta]\bot),
[\alpha]([\alpha]\bot \land \left[\beta\right]X)
\end{align*}
\] 

\[
[\alpha]([\alpha]X \land [\beta]\bot) \lor [\alpha]([\alpha]\bot \land \left[\beta\right]X)
\] 

\[
\nu X.\left[\alpha\right]([\alpha]X \land [\beta]\bot) \lor [\alpha]([\alpha]\bot \land \left[\beta\right]X)
\] 

(\forall)

(\forall)
Example

\[
\frac{[\alpha]X \land [\beta]\bot, [\alpha]\bot \land [\beta]X}{[\alpha]([\alpha]X \land [\beta]\bot), [\alpha]([\alpha]\bot \land [\beta]X)}
\]

\[
\frac{[\alpha]([\alpha]X \land [\beta]\bot) \lor [\alpha]([\alpha]\bot \land [\beta]X)}{\nu X. [\alpha]([\alpha]X \land [\beta]\bot) \lor [\alpha]([\alpha]\bot \land [\beta]X)}
\]
Example

\[
\begin{align*}
[\alpha]X, [\alpha] \bot \land [\beta]X & \quad [\beta] \bot, [\alpha] \bot \land [\beta]X \\
[\alpha]X \land [\beta] \bot, [\alpha] \bot \land [\beta]X & \quad ([\alpha]) \\
[\alpha]([\alpha]X \land [\beta] \bot), [\alpha]([\alpha] \bot \land [\beta]X) & \quad (\lor) \\
[\alpha]([\alpha]X \land [\beta] \bot) \lor [\alpha]([\alpha] \bot \land [\beta]X) & \quad (\nu) \\
\nu X. [\alpha]([\alpha]X \land [\beta] \bot) \lor [\alpha]([\alpha] \bot \land [\beta]X) & \quad (\nu)
\end{align*}
\]
Example

\[
\begin{align*}
\alpha X, \alpha & \perp \Rightarrow \alpha X, \beta X \quad (\wedge) \\
\alpha X, \alpha \perp \wedge \beta X & \Rightarrow \beta \perp, \alpha \perp \wedge \beta X \\
\alpha X \wedge \beta \perp, \alpha \perp \wedge \beta X & \Rightarrow \alpha (\alpha X \wedge \beta \perp), [\alpha]([\alpha] \perp \wedge \beta X) \\
\alpha (\alpha X \wedge \beta \perp) \vee [\alpha]([\alpha] \perp \wedge \beta X) & \Rightarrow \nu X. \alpha (\alpha X \wedge \beta \perp) \vee [\alpha]([\alpha] \perp \wedge \beta X) \\
\end{align*}
\]
Example

\[
\frac{X}{[\alpha]X, [\alpha] \perp} (\{\alpha\}) \quad \frac{[\alpha]X, [\beta]X}{(\wedge)} \quad \frac{[\alpha]X, [\alpha] \perp \wedge [\beta]X}{(\wedge)} \quad \frac{[\beta] \perp, [\alpha] \perp \wedge [\beta]X}{(\wedge)}
\]

\[
\frac{[\alpha]X \wedge [\beta] \perp, [\alpha] \perp \wedge [\beta]X}{([\alpha])} \quad \frac{[\alpha]([\alpha]X \wedge [\beta] \perp), [\alpha]([\alpha] \perp \wedge [\beta]X)}{([\alpha])} \quad \frac{[\alpha]([\alpha]X \wedge [\beta] \perp) \lor [\alpha]([\alpha] \perp \wedge [\beta]X)}{(\lor)} \quad \frac{\nu X. [\alpha]([\alpha]X \wedge [\beta] \perp) \lor [\alpha]([\alpha] \perp \wedge [\beta]X)}{(\nu)}
\]
Example

\[
\frac{X}{[\alpha]X, [\alpha] \perp} (\lbrack \alpha \rbrack) \quad \frac{\top}{[\alpha]X, [\beta]X} (\wedge) \quad \frac{[\alpha]X \wedge [\beta] \perp, [\alpha] \perp \wedge [\beta]X}{[\alpha]X \wedge [\beta] \perp, [\alpha] \perp \wedge [\beta]X} (\wedge) \quad \frac{[\alpha]([\alpha]X \wedge [\beta] \perp), [\alpha]([\alpha] \perp \wedge [\beta]X)}{[\alpha]([\alpha]X \wedge [\beta] \perp) \lor [\alpha]([\alpha] \perp \wedge [\beta]X)} (\lor) \quad \frac{\nu X. [\alpha]([\alpha]X \wedge [\beta] \perp) \lor [\alpha]([\alpha] \perp \wedge [\beta]X)}{\nu X. [\alpha]([\alpha]X \wedge [\beta] \perp) \lor [\alpha]([\alpha] \perp \wedge [\beta]X)} (\nu)
\]
Example

\[
\begin{align*}
\frac{X}{[\alpha]X, [\alpha] \bot} & \quad ([\alpha]) \\
\frac{T}{[\alpha]X, [\beta]X} & \quad (\land) \\
\frac{[\alpha]X, [\alpha] \bot \land [\beta]X}{[\alpha]X \land [\beta] \bot, [\alpha] \bot \land [\beta]X} & \quad ([\alpha]) \\
\frac{T}{[\beta] \bot, [\alpha] \bot} & \quad ([\beta] \bot, [\beta]X) \\
\frac{T}{[\beta] \bot, [\alpha] \bot \land [\beta]X} & \quad ([\beta] \bot, [\beta]X) \\
\frac{[\alpha](([\alpha]X \land [\beta] \bot), [\alpha]([\alpha] \bot \land [\beta]X))}{[\alpha]([\alpha]X \land [\beta] \bot) \lor [\alpha]([\alpha] \bot \land [\beta]X)} & \quad ([[\alpha]]) \\
\frac{[[\alpha]])}{[[\alpha]]} & \quad (\lor) \\
\frac{[[\alpha]])}{[[\alpha]]} & \quad (\lor) \\
\frac{\nu X.[\alpha]([\alpha]X \land [\beta] \bot) \lor [\alpha]([\alpha] \bot \land [\beta]X)}{\nu X.[\alpha]([\alpha]X \land [\beta] \bot) \lor [\alpha]([\alpha] \bot \land [\beta]X)} & \quad (\nu)
\end{align*}
\]
Example

\[
\begin{align*}
\frac{X}{[\alpha]X, [\alpha]\bot} ([\alpha]) & \\
\frac{T}{[\alpha]X, [\beta]X} (\wedge) & \\
\frac{T}{[\beta]\bot, [\alpha]\bot} & \\
\frac{X}{[\beta]\bot, [\beta]X} (\wedge) & \\
\frac{[\alpha]X \land [\beta]\bot, [\alpha]\bot \land [\beta]X}{[\alpha]([\alpha]X \land [\beta]\bot), [\alpha]([\alpha]\bot \land [\beta]X)} ([\alpha]) & (\lor) \\
\frac{\nu X. [\alpha]([\alpha]X \land [\beta]\bot) \lor [\alpha]([\alpha]\bot \land [\beta]X)}{\nu X. [\alpha]([\alpha]X \land [\beta]\bot) \lor [\alpha]([\alpha]\bot \land [\beta]X)} (\nu)
\end{align*}
\]
Example

\[ X ([\alpha]) \quad \top ([\alpha/\beta]) \quad \top ([\alpha/\beta]) \quad X ([\beta]) \]
\[ \land \quad \land \quad \land \quad \land \]
\[ ([\alpha]) \quad ([\beta]) \quad (\top) \quad (\top) \]
\[ \lor \quad \lor \quad \lor \quad \lor \]
\[ (X) \quad (\nu) \quad (\nu) \quad (\nu) \]
Example

\[
\frac{X}{[\alpha]X} \quad \frac{[\alpha]}{[\alpha/\beta]} \quad \frac{T}{T} \quad \frac{[\alpha/\beta]}{\wedge} \quad \frac{T}{T} \quad \frac{[\alpha/\beta]}{\wedge} \quad \frac{X}{[\beta]X} \quad \frac{[\beta]}{\wedge}
\]

\[
\frac{\text{([\alpha])}}{(\wedge)} \quad \frac{\text{([\alpha/\beta])}}{(\wedge)}
\]

\[
\frac{\text{([\alpha])}}{(\wedge)} \quad \frac{\text{([\alpha/\beta])}}{(\wedge)} \quad \frac{X}{[\beta]X} \quad \frac{([\beta])}{(\wedge)}
\]

\[
\frac{\text{([\alpha])}}{(\wedge)} \quad \frac{\text{([\alpha/\beta])}}{(\wedge)} \quad \frac{X}{[\beta]X} \quad \frac{([\beta])}{(\wedge)}
\]

Karoliina Lehtinen  Synthesis of optimal monitors
Example

\[
\begin{align*}
\frac{X}{[\alpha]X} \quad ([\alpha]) & \quad \frac{T}{T} \quad ([\alpha/\beta]) & \quad \frac{T}{T} \quad ([\alpha/\beta]) & \quad \frac{X}{[\beta]X} \quad ([\beta]) \\
\frac{[\alpha]X \land T}{[\alpha]X \land T} & \quad (\land) & \quad (\land) \\
\frac{(\land)}{([\alpha])} & \quad (\lor) & \quad (\lor) \\
\frac{(X)}{(X)} & \quad (\nu)
\end{align*}
\]
Example

\[
\frac{X}{[\alpha]X} (\alpha) \quad \frac{T}{T} ([\alpha/\beta]) \quad \frac{T}{T} ([\alpha/\beta]) \quad \frac{X}{[\beta]X} ([\beta])
\]

\[
\frac{[\alpha]X \land T}{[\alpha]X \land T} (\land)
\]

\[
\frac{T \land [\beta]X}{T \land [\beta]X} (\land)
\]

\[
\frac{[\alpha]X \land T \land [\beta]X}{[\alpha]X \land T \land [\beta]X} (\land)
\]

\[
\frac{([\alpha])}{([\alpha])} (\lor)
\]

\[
\frac{([\beta])}{([\beta])} (\lor)
\]

\[
(X)
\]
Example

\[
\begin{align*}
\frac{X}{[\alpha]X} & (\lbrack \alpha \rbrack) & \frac{T}{T} & (\lbrack \alpha / \beta \rbrack) & \frac{T}{T} & (\lbrack \alpha / \beta \rbrack) & \frac{X}{[\beta]X} & (\lbrack \beta \rbrack) \\
[\alpha]X \land T & (\land) & T \land [\beta]X & (\land) & [\alpha]X \land T \land [\beta]X & (\land) & [\alpha]([\alpha]X \land T \land [\beta]X) & (\land) \\
[\alpha]X \land T \land [\beta]X & (\land) & \frac{[\alpha]([\alpha]X \land T \land [\beta]X)}{([\alpha])} & (\land) & \frac{X}{\nu} & (\nu) & \frac{[\alpha]X \land T \land [\beta]X}{(X)} & (\nu)
\end{align*}
\]
Example

\[
\frac{X}{[\alpha]X} \quad ([\alpha]) \quad \frac{T}{T} \quad ([\alpha/\beta]) \quad \frac{T}{T} \quad ([\alpha/\beta]) \quad \frac{X}{[\beta]X} \quad ([\beta]) \quad \frac{T}{T} \quad ([\alpha/\beta])
\]

\[
\frac{[\alpha]X \land T}{[\alpha]X \land T} \quad (\land)
\]

\[
\frac{[\alpha]X \land T \land [\beta]X}{[\alpha]X \land T \land [\beta]X} \quad (\land)
\]

\[
\frac{[\alpha]([\alpha]X \land T \land [\beta]X)}{[\alpha]([\alpha]X \land T \land [\beta]X)} \quad ([\alpha])
\]

\[
\frac{[\alpha](T \land [\beta]X)}{[\alpha](T \land [\beta]X)} \quad (\lor)
\]

\[
\frac{([\alpha]X \land T \land [\beta]X)}{([\alpha]X \land T \land [\beta]X)} \quad (\lor)
\]

\[
\frac{X}{X} \quad ([\alpha])
\]

\[
\frac{[\alpha](X \land T \land [\beta]X)}{[\alpha](X \land T \land [\beta]X)} \quad (\lor)
\]

\[
\frac{([\alpha]X \land T \land [\beta]X)}{([\alpha]X \land T \land [\beta]X)} \quad (\lor)
\]
Example

\[
\frac{X}{[\alpha]X} \quad ([\alpha]) \quad \frac{T}{T} \quad ([\alpha/\beta]) \quad \frac{T}{T} \quad ([\alpha/\beta]) \quad \frac{X}{[\beta]X} \quad ([\beta])
\]

\[
\frac{[\alpha]X \land T}{[\alpha]X \land T} \quad (\land)
\]

\[
\frac{T \land [\beta]X}{T \land T} \quad (\land)
\]

\[
\frac{[\alpha]X \land T \land [\beta]X}{[\alpha](([\alpha]X \land T \land [\beta]X))} \quad ([\alpha])
\]

\[
\frac{[\alpha](([\alpha]X \land T \land [\beta]X))}{[\alpha](([\alpha]X \land T \land [\beta]X))} \quad (\lor)
\]

\[
\frac{\nu X.[\alpha](([\alpha]X \land T \land [\beta]X))}{\nu X.[\alpha](([\alpha]X \land T \land [\beta]X))} \quad (\nu)
\]
Example

Original formula:

\[ \nu X. [\alpha]([\alpha] X \land [\beta] \bot) \lor [\alpha]([\alpha] \bot \land [\beta] X) \]

Strongest safety consequence:

\[ \nu X. [\alpha]([\alpha] X \land [\beta] X) \equiv \top \]

Original formula:

\[ \nu X. [\alpha]([\alpha] X \land [\beta] \bot \land [\gamma] \bot) \lor [\alpha]([\alpha] X \land [\gamma] \bot \land [\epsilon] \bot) \]

Strongest safety consequence:

\[ \nu X. [\alpha]([\alpha] X \land [\gamma] \bot) \]
Synthesis of the optimal monitor for $\psi$ via synthesis of its strongest safety consequence.

The resulting monitors are deterministic

$2\text{Exptime}$ complexity
Can the $2\text{-EXPTIME}$ upper bound be improved by generating non-deterministic monitors?
Can the $2\text{-Exptime}$ upper bound be improved by generating non-deterministic monitors?

Some formulas have only trivial monitors. Can this be checked in Exptime?
Open questions

- Can the 2-\textit{EXPTIME} upper bound be improved by generating non-deterministic monitors?
- Some formulas have only trivial monitors. Can this be checked in \textit{EXPTIME}?
- Hybrid verification: $\Psi = \Psi' \land \text{ssc}$?
Open questions

- Can the 2-Exptime upper bound be improved by generating non-deterministic monitors?
- Some formulas have only trivial monitors. Can this be checked in Exptime?
- Hybrid verification: $\Psi = \Psi' \land ssc$?
- Monitoring CTL specifications?
Open questions

- Can the $2^{\text{EXPTIME}}$ upper bound be improved by generating non-deterministic monitors?
- Some formulas have only trivial monitors. Can this be checked in $\text{EXPTIME}$?
- Hybrid verification: $\Psi = \Psi' \land \text{ssc}$?
- Monitoring CTL specifications?
- [Insert your $\mu$HML problem here]