Christian-Albrechts-Universität zu Kiel

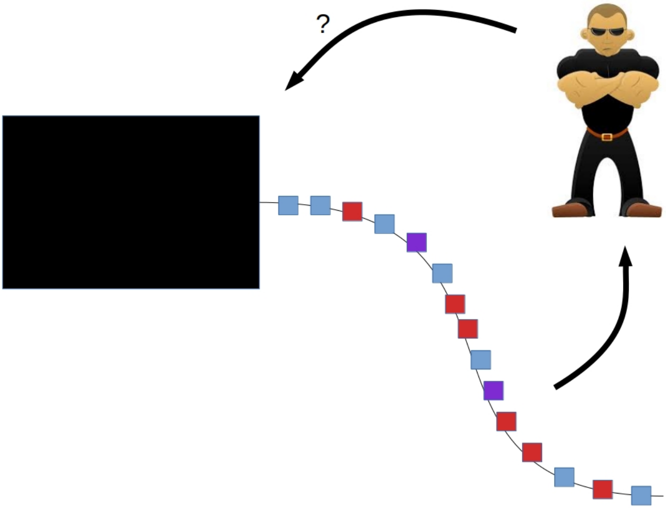
Runtime verification of fixpoint logic: Synthesis of optimal monitors

Karoliina Lehtinen

University of Kiel

January 2018

Runtime monitoring



The set-up

- A process p (described by a CCS process)

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

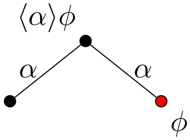
The set-up

- A process p (described by a CCS process)

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

- A system specification ψ in your favourite logic: Hennessy–Milner logic with recursion

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



The set-up

- A process p (described by a CCS process)

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

- A system specification ψ in your favourite logic: Hennessy–Milner logic with recursion

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

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

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

The set-up

- A process p (described by a CCS process)

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

- A system specification ψ in your favourite logic: Hennessy–Milner logic with recursion

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

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

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

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

The set-up

- A process p (described by a CCS process)

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

- A system specification ψ in your favourite logic: Hennessy–Milner logic with recursion

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

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

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

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

Goal: Given ψ, find a **good** monitor for ψ.

What is a good monitor?

A good monitor is sound

The monitor m is a sound monitor for ψ if:

- **acc**(m, p) implies $p \in \psi$, and
- **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 ψ if

- $p \notin \psi$ implies **rej**(m, p).

The monitor m is satisfaction-complete for ψ if

- $p \in \psi$ implies **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 μHML formula has a **sound and violation complete** *monitor if and only if it is in the* **safety** *fragment of μHML.*

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

What if ψ is not in this fragment?

Sound and complete monitors

Theorem (Francalanza, Aceto, Ingólfsdóttir 2015)

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

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

What if ψ is not in this fragment?

Good, better and optimal monitors

A monitor m is optimal for ψ if:

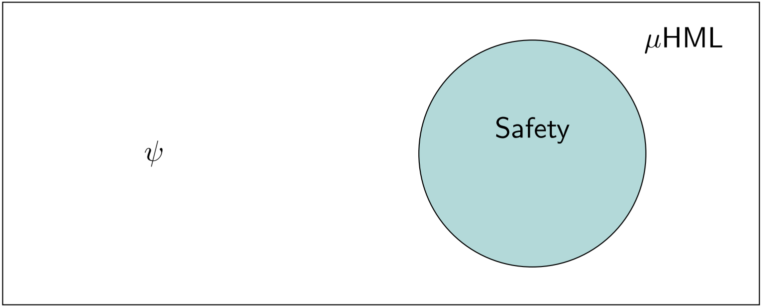
- m is sound for ψ;
- If m' is sound for ψ, then $\mathbf{rej}(m', p)$ implies $\mathbf{rej}(m, p)$.

Contributions

Problem: Given a μHML formula, what is its optimal monitor?

Solution

- Reduce the problem to finding the **strongest safety consequence** of ψ.
- Find the **strongest safety consequence** of ψ.

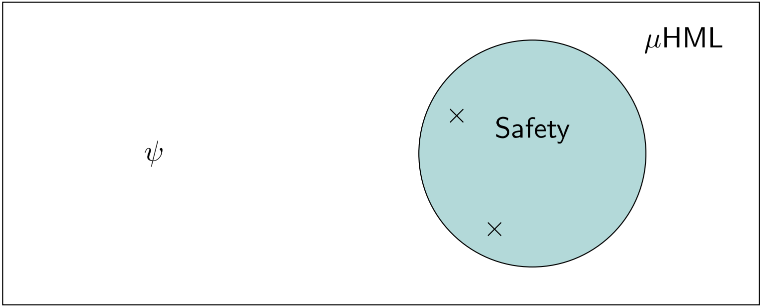


Contributions

Problem: Given a μHML formula, what is its optimal monitor?

Solution

- Reduce the problem to finding the **strongest safety consequence** of ψ.
- Find the **strongest safety consequence** of ψ.

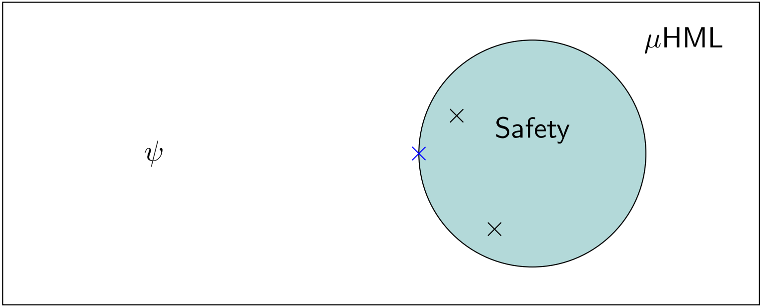


Contributions

Problem: Given a μHML formula, what is its optimal monitor?

Solution

- Reduce the problem to finding
  the **strongest safety consequence** of ψ.
- Find the **strongest safety consequence** of ψ.



μHML phrasing of the problem

Theorem

Finding the optimal rejection-monitor of ψ reduces to finding the strongest consequence of ψ in the safety fragment of μHML.

μHML phrasing of the problem

Theorem

Finding the optimal rejection-monitor of ψ reduces to finding the strongest consequence of ψ in the safety fragment of μHML.

Definition

The **strongest safety consequence** of ψ is a formula θ such that:

- θ is a safety formula,
- ψ implies θ, and
- If ψ implies θ' and θ' is a safety formula, then θ implies θ'

μHML phrasing of the problem

Theorem

Finding the optimal rejection-monitor of ψ reduces to finding the strongest consequence of ψ in the safety fragment of μHML.

Definition

The **strongest safety consequence** of ψ is a formula θ such that:

- θ is a safety formula,
- ψ implies θ, and
- If ψ implies θ' and θ' is a safety formula, then θ implies θ'

Proof.

- Optimal monitor for ψ is sound and complete for strongest safety consequence θ of ψ.

$\square$

Synthesis of the strongest safety consequence

The problem

Given ψ, find θ such that

- θ is a safety formula,
- ψ implies θ, and
- If ψ implies θ' and θ' is a safety formula, then θ implies θ'

The solution

Formula transformation:

Synthesis of the strongest safety consequence

The problem

Given ψ, find θ such that

- θ is a safety formula,
- ψ implies θ, and
- If ψ implies θ' and θ' is a safety formula, then θ implies θ'

The solution

Formula transformation:

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

While preserving safety consequences.

Synthesis of the strongest safety consequence

The problem

Given ψ, find θ such that

- θ is a safety formula,
- ψ implies θ, and
- If ψ implies θ' and θ' is a safety formula, then θ implies θ'

The solution

Formula transformation:

1. Eliminate $\langle\alpha\rangle$-subformulas.
2. Turn μ-operators into ν-operators.

While preserving safety consequences.

Synthesis of the strongest safety consequence

The problem

Given ψ, find θ such that

- θ is a safety formula,
- ψ implies θ, and
- If ψ implies θ' and θ' is a safety formula, then θ implies θ'

The solution

Formula transformation:

1. Eliminate $\langle\alpha\rangle$-subformulas.
2. Turn μ-operators into ν-operators.
3. Turn $[\alpha]\psi \vee [\alpha]\psi'$ into $[\alpha]\psi \vee \psi'$
   Eliminate $[\alpha]\psi \vee [\beta]\psi$

While preserving safety consequences.

Step 1: Eliminating $\langle\alpha\rangle$

Lemma

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

- *$\perp$ if ϕ is unsatisfiable, $\top$ otherwise.*

Ψ has the same safety consequences as Ψ'.

Proof (idea).

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

- Safety consequence θ of Ψ
- T such that $T \models \neg\theta \wedge \Psi'$
- Build T' such that $T' \models \Psi \wedge \neg\theta$, a contradiction.

$\square$

Step 1: Eliminating $\langle \alpha \rangle$

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

- Assume $T \models \neg\theta \wedge \Psi'$.

$\square$

Step 1: Eliminating $\langle\alpha\rangle$

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

- Assume $T \models \neg\theta \wedge \Psi'$.
- Find nodes at which the Ψ'-proof proves $\top$ (from $\langle\alpha\rangle\phi$ in Ψ).

$\square$

Step 1: Eliminating $\langle\alpha\rangle$

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

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

$\square$

Step 1: Eliminating $\langle \alpha \rangle$

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

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

$\square$

Step 1: Eliminating $\langle\alpha\rangle$

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

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

$\square$

Step 1: Eliminating $\langle\alpha\rangle$

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

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

$\square$

Step 2: Eliminating μ

Lemma

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

Proof

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

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

Step 2: Eliminating μ

Lemma

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

Proof

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

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

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

Step 2: Eliminating μ

Lemma

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

Proof

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

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

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

Step 2: Eliminating μ

Lemma

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

Proof

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

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

Step 3: Eliminate $\vee$

Idea

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

Execution

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

Ouput

Strongest safety consequence.

Example

$$\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\gamma]\bot)$$

Example

$$\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)$$

Example

$$\frac{[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}{\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\ (\nu)$$

Example

$$\dfrac{\dfrac{[\alpha]([\alpha]X \wedge [\beta]\bot), [\alpha]([\alpha]\bot \wedge [\beta]X)}{[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\vee)}{\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\nu)$$

Example

$$\dfrac{\dfrac{\dfrac{[\alpha]X \wedge [\beta]\bot, [\alpha]\bot \wedge [\beta]X}{[\alpha]([\alpha]X \wedge [\beta]\bot), [\alpha]([\alpha]\bot \wedge [\beta]X)}\,([\alpha])}{[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\vee)}{\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\nu)$$

Example

$$\cfrac{\cfrac{\cfrac{\cfrac{[\alpha]X, [\alpha]\bot \wedge [\beta]X \qquad [\beta]\bot, [\alpha]\bot \wedge [\beta]X}{[\alpha]X \wedge [\beta]\bot, [\alpha]\bot \wedge [\beta]X}\,(\wedge)}{[\alpha]([\alpha]X \wedge [\beta]\bot), [\alpha]([\alpha]\bot \wedge [\beta]X)}\,([\alpha])}{[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\vee)}{\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\nu)$$

Example

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{[\alpha]X, [\alpha]\bot \qquad [\alpha]X, [\beta]X}{[\alpha]X, [\alpha]\bot \wedge [\beta]X}\,(\wedge) \qquad [\beta]\bot, [\alpha]\bot \wedge [\beta]X}{[\alpha]X \wedge [\beta]\bot, [\alpha]\bot \wedge [\beta]X}\,(\wedge)}{[\alpha]([\alpha]X \wedge [\beta]\bot), [\alpha]([\alpha]\bot \wedge [\beta]X)}\,([\alpha])}{[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\vee)}{\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\nu)$$

Example

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{
        \dfrac{
          \dfrac{X}{[\alpha]X, [\alpha]\bot}\,([\alpha]) \qquad [\alpha]X, [\beta]X
        }{
          [\alpha]X, [\alpha]\bot \wedge [\beta]X
        }\,(\wedge)
        \qquad
        [\beta]\bot, [\alpha]\bot \wedge [\beta]X
      }{
        [\alpha]X \wedge [\beta]\bot, [\alpha]\bot \wedge [\beta]X
      }\,(\wedge)
    }{
      [\alpha]([\alpha]X \wedge [\beta]\bot), [\alpha]([\alpha]\bot \wedge [\beta]X)
    }\,([\alpha])
  }{
    [\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)
  }\,(\vee)
}{
  \nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)
}\,(\nu)
$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{X}{[\alpha]X,[\alpha]\bot}\,([\alpha]) \qquad \dfrac{\top}{[\alpha]X,[\beta]X}}{[\alpha]X,[\alpha]\bot\wedge[\beta]X}\,(\wedge) \qquad [\beta]\bot,[\alpha]\bot\wedge[\beta]X}{[\alpha]X\wedge[\beta]\bot,[\alpha]\bot\wedge[\beta]X}\,(\wedge)}{[\alpha]([\alpha]X\wedge[\beta]\bot),[\alpha]([\alpha]\bot\wedge[\beta]X)}\,([\alpha])}{[\alpha]([\alpha]X\wedge[\beta]\bot)\vee[\alpha]([\alpha]\bot\wedge[\beta]X)}\,(\vee)}{\nu X.[\alpha]([\alpha]X\wedge[\beta]\bot)\vee[\alpha]([\alpha]\bot\wedge[\beta]X)}\,(\nu)$$

Example

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{X}{[\alpha]X, [\alpha]\bot}\,([\alpha]) \qquad \dfrac{\top}{[\alpha]X, [\beta]X}
    }{[\alpha]X, [\alpha]\bot \wedge [\beta]X}\,(\wedge)
    \qquad
    \dfrac{
      \dfrac{\top}{[\beta]\bot, [\alpha]\bot} \qquad [\beta]\bot, [\beta]X
    }{[\beta]\bot, [\alpha]\bot \wedge [\beta]X}\,(\wedge)
  }{
    \dfrac{
      [\alpha]X \wedge [\beta]\bot, [\alpha]\bot \wedge [\beta]X
    }{
      \dfrac{[\alpha]([\alpha]X \wedge [\beta]\bot), [\alpha]([\alpha]\bot \wedge [\beta]X)}{[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\vee)
    }\,([\alpha])
  }\,(\wedge)
}{\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\nu)
$$

Example

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{X}{[\alpha]X, [\alpha]\bot}\,([\alpha]) \qquad \dfrac{\top}{[\alpha]X, [\beta]X}}{[\alpha]X, [\alpha]\bot \wedge [\beta]X}\,(\wedge) \qquad \dfrac{\dfrac{\top}{[\beta]\bot, [\alpha]\bot} \qquad \dfrac{X}{[\beta]\bot, [\beta]X}}{[\beta]\bot, [\alpha]\bot \wedge [\beta]X}\,(\wedge)}{[\alpha]X \wedge [\beta]\bot, [\alpha]\bot \wedge [\beta]X}\,(\wedge)}{[\alpha]([\alpha]X \wedge [\beta]\bot), [\alpha]([\alpha]\bot \wedge [\beta]X)}\,([\alpha])}{[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\vee)}{\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)}\,(\nu)}{}
$$

Example

$$
\begin{prooftree}
\AxiomC{X}
\RightLabel{$([\alpha])$}
\UnaryInfC{}
\AxiomC{$\top$}
\RightLabel{$([\alpha/\beta])$}
\UnaryInfC{}
\RightLabel{$(\wedge)$}
\BinaryInfC{}
\AxiomC{$\top$}
\RightLabel{$([\alpha/\beta])$}
\UnaryInfC{}
\AxiomC{X}
\RightLabel{$([\beta])$}
\UnaryInfC{}
\RightLabel{$(\wedge)$}
\BinaryInfC{}
\RightLabel{$(\wedge)$}
\BinaryInfC{}
\RightLabel{$([\alpha])$}
\UnaryInfC{}
\RightLabel{$(\vee)$}
\UnaryInfC{}
\RightLabel{(ν)}
\UnaryInfC{(X)}
\end{prooftree}
$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{X}{[\alpha]X}\,([\alpha]) \qquad \dfrac{\top}{\top}\,([\alpha/\beta])}{}\,(\wedge) \qquad \dfrac{\dfrac{\top}{\top}\,([\alpha/\beta]) \qquad \dfrac{X}{[\beta]X}\,([\beta])}{}\,(\wedge)}{}\,(\wedge)}{}\,([\alpha])}{}\,(\vee)}{(X)}\,(\nu)$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{X}{[\alpha]X}\,([\alpha]) \quad \dfrac{\top}{\top}\,([\alpha/\beta])}{[\alpha]X \wedge \top}\,(\wedge) \qquad \dfrac{\dfrac{\top}{\top}\,([\alpha/\beta]) \quad \dfrac{X}{[\beta]X}\,([\beta])}{}\,(\wedge)}{}\,(\wedge)}{}\,([\alpha])}{}\,(\vee)}{(X)}\,(\nu)$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{X}{[\alpha]X}([\alpha]) \quad \dfrac{\top}{\top}([\alpha/\beta])}{[\alpha]X \wedge \top}(\wedge) \qquad \dfrac{\dfrac{\top}{\top}([\alpha/\beta]) \quad \dfrac{X}{[\beta]X}([\beta])}{\top \wedge [\beta]X}(\wedge)}{[\alpha]X \wedge \top \wedge [\beta]X}(\wedge)}{\quad}([\alpha])}{\quad}(\vee)}{(X)}(\nu)$$

Example

$$
\cfrac{
  \cfrac{
    {\cfrac{
      {\cfrac{
        {\cfrac{X}{[\alpha]X}\,([\alpha])} \quad {\cfrac{\top}{\top}\,([\alpha/\beta])}
      }{[\alpha]X \wedge \top}\,(\wedge)}
      \quad
      {\cfrac{
        {\cfrac{\top}{\top}\,([\alpha/\beta])} \quad {\cfrac{X}{[\beta]X}\,([\beta])}
      }{\top \wedge [\beta]X}\,(\wedge)}
    }{
      \cfrac{[\alpha]X \wedge \top \wedge [\beta]X}{[\alpha]([\alpha]X \wedge \top \wedge [\beta]X)}\,([\alpha])
    }\,(\wedge)}
  }{}\,(\vee)
}{(X)}\,(\nu)
$$

Example

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{X}{[\alpha]X}\,([\alpha]) \qquad \cfrac{\top}{\top}\,([\alpha/\beta])}{[\alpha]X \wedge \top}\,(\wedge) \qquad \cfrac{\cfrac{\top}{\top}\,([\alpha/\beta]) \qquad \cfrac{X}{[\beta]X}\,([\beta])}{\top \wedge [\beta]X}\,(\wedge)}{[\alpha]X \wedge \top \wedge [\beta]X}\,(\wedge)}{[\alpha]([\alpha]X \wedge \top \wedge [\beta]X)}\,([\alpha])}{[\alpha]([\alpha]X \wedge \top \wedge [\beta]X)}\,(\vee)}{(X)}\,(\nu)
$$

Example

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{X}{[\alpha]X}\,([\alpha]) \qquad \dfrac{\top}{\top}\,([\alpha/\beta])}{[\alpha]X \wedge \top}\,(\wedge) \qquad \dfrac{\dfrac{\top}{\top}\,([\alpha/\beta]) \qquad \dfrac{X}{[\beta]X}\,([\beta])}{\top \wedge [\beta]X}\,(\wedge)}{[\alpha]X \wedge \top \wedge [\beta]X}\,(\wedge)}{[\alpha]([\alpha]X \wedge \top \wedge [\beta]X)}\,([\alpha])}{[\alpha]([\alpha]X \wedge \top \wedge [\beta]X)}\,(\vee)}{\nu X.[\alpha]([\alpha]X \wedge \top \wedge [\beta]X)}\,(\nu)$$

Example

Original formula:

$$\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot) \vee [\alpha]([\alpha]\bot \wedge [\beta]X)$$

Strongest safety consequence:

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

Original formula:

$$\nu X.[\alpha]([\alpha]X \wedge [\beta]\bot \wedge [\gamma]\bot) \vee [\alpha]([\alpha]X \wedge [\gamma]\bot \wedge [\epsilon]\bot)$$

Strongest safety consequence:

$$\nu X.[\alpha]([\alpha]X \wedge [\gamma]\bot)$$

Summary

- Synthesis of the optimal monitor for ψ via synthesis of its strongest safety consequence.
- The resulting monitors are deterministic
- $2\textsc{Exptime}$ complexity

Open questions

- Can the 2-EXPTIME upper bound be improved by generating non-deterministic monitors?

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?

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: $\Psi = \Psi' \wedge \mathtt{ssc}$?

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: $\Psi = \Psi' \wedge \mathtt{ssc}$?
- Monitoring CTL specifications?

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: $\Psi = \Psi' \wedge \mathtt{ssc}$?
- Monitoring CTL specifications?
- [Insert your μHML problem here]