Computing Minimal Distinguishing Formulas for Bisimulation

Computing minimal distinguishing Hennessy-Milner formulas is NP-hard, but variants are tractable, Jan Martens, Jan Friso Groote

Minimal Depth Distinguishing Formulas Without Until for Branching Bisimulation, Jan Martens, Jan Friso Groote

Remco van Os 21 January 2025

Labelled Transition Systems

Formalization

Definition

A Labelled Transition System or LTS $L = (S, Act, \rightarrow)$ is:

- a finite set of states S
- a finite set of action labels Act
- a transition relation $\rightarrow \subseteq S \times Act \times S$

We write $s \xrightarrow{a} s'$ when $(s, a, s') \in \rightarrow$

Equivalence

Bisimulation

Definition

Given an LTS $L = (S, Act, \rightarrow)$, a relation $R \subseteq S \times S$ is called a bisimulation relation iff for all $s, t \in S$ such that sRt holds, it also holds for all actions $a \in Act$ that:

- if $s \xrightarrow{a} s'$, then there is $t' \in S$ such that $t \xrightarrow{a} t'$ and $s'Rt'$
- if $t \xrightarrow{a} t'$, then there is $s' \in S$ such that $s \xrightarrow{a} s'$ and $s'Rt'$

$$\begin{tikzcd}
s \arrow[r, squiggly, no head, "R"] \arrow[d, "a"] & t \arrow[d, dotted, "a"] \\
s' \arrow[r, squiggly, no head, "R"] & t'
\end{tikzcd}
\qquad
\begin{tikzcd}
t \arrow[r, squiggly, no head, "R"] \arrow[d, "a"] & s \arrow[d, dotted, "a"] \\
t' \arrow[r, squiggly, no head, "R"] & s'
\end{tikzcd}$$

We say s is bisimilar to t, denoted $s \mathrel{\underline{\leftrightarrow}} t$ if there is such a relation R with sRt

---

Modeling and Analysis of Communicating Systems Jan Friso Groote, Mohammed Reza Mousavi

Hennessy-Milner Logic

Higher level way to talk about states
Formulas that capture the behavior of a state

Hennessy-Milner Logic

Definition

For $a \in Act$ a label, we define the Hennessy-Milner Logic:

$$\phi ::= tt \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \langle a\rangle\phi$$

For $s \in S$, we write $s \models \phi$ if ϕ holds in s:

True	$s \models tt$	always holds
Negations	$s \models \neg\phi$	iff $s \not\models \phi$
Conjunctions	$s \models \phi_1 \wedge \phi_2$	iff $s \models \phi_1$ and $s \models \phi_2$
Observations	$s \models \langle a\rangle\phi$	iff $\exists s' \in S$ such that $s \xrightarrow{a} s'$ and $s' \models \phi$

Hennessy-Milner Logic

Hennessy-Milner Theorem

Given an LTS $L = (S, Act, \rightarrow)$ and two states $s, t \in S$, we have:

$$s \leftrightarroweq t \iff \forall \phi \in HML, s \models \phi \leftrightarrow t \models \phi$$

On Observing Nondeterminism and Concurrency Matthew Hennessy and Robin Milner

Distinguishing Formulas

Corollary

$$s \not\leftrightarrow t \quad \iff \quad \exists \phi \in \mathit{HML} \text{ such that } s \models \phi \text{ and } t \not\models \phi$$

This ϕ is called the distinguishing formula

Size

Definition

We inductively define the size of a formula in *HML*

- $|tt| = 0$
- $|\langle a\rangle\phi| = |\phi| + 1$
- $|\neg\phi| = |\phi|$
- $|\phi_1 \wedge \phi_2| = |\phi_1| + |\phi_2|$

Intuitively: count the number of observations in the whole formula

Computing minimal size distinguishing formulas

Given an LTS $L = (S, Act, \rightarrow)$ and two states $s, t \in S$

MIN-DIST

There is a formula $\phi \in HML$ with less observations than $|S|$ such that ϕ distinguishes s and t, and $|\phi| \leq \ell$ for some $\ell \in \mathbb{N}$

Computing minimal size distinguishing formulas

Given an LTS $L = (S, Act, \rightarrow)$ and two states $s, t \in S$

MIN-DIST

There is a formula $\phi \in HML$ with less observations than $|S|$ such that ϕ distinguishes s and t, and $|\phi| \leq \ell$ for some $\ell \in \mathbb{N}$

This decision problem is NP-hard

- Reduction from CNF-SAT
- NP-complete depending on representation of ϕ

Observation Depth

Definition

We inductively define the observation-depth of a formula in *HML*

- $d_\diamond(tt) = 0$
- $d_\diamond(\langle a\rangle\phi) = d_\diamond(\phi) + 1$
- $d_\diamond(\neg\phi) = d_\diamond(\phi)$
- $d_\diamond(\phi_1 \wedge \phi_2) = \max(d_\diamond(\phi_1), d_\diamond(\phi_2))$

Intuitively: the largest number of nested observations

k-bisimilarity

Definition

Given an LTS $L = (S, Act, \rightarrow)$ and $k \in \mathbb{N}$, k-bisimilarity, denoted $\leftrightarroweq_l$, is defined inductively:

$$\begin{aligned} \leftrightarroweq_0 &= \{(s,t) \mid s,t \in S\} \\ \leftrightarroweq_k &= \{(s,t) \mid \forall\, s \xrightarrow{a} s' \exists\, t \xrightarrow{a} t' \text{ such that } s' \leftrightarroweq_{k-1} t' \text{ and} \\ &\qquad \forall\, t \xrightarrow{a} t' \exists\, s \xrightarrow{a} s' \text{ such that } t' \leftrightarroweq_{k-1} s'\} \end{aligned}$$

We can prove $\leftrightarroweq\ = \bigcap_{k \in \mathbb{N}} \leftrightarroweq_k$

Deltas

Definition

Define the minimal observation depth $\Delta : S \times S \to \mathbb{N} \cup \infty$ by

$$\Delta(s,t) = \begin{cases} i & \text{if } s \not\leftrightarrow_i t \text{ and } s \leftrightarrow_{i-1} t \\ \infty & \text{if } s \leftrightarrow t \end{cases}$$

Computing minimal distinguishing Hennessy-Milner formulas is NP-hard, but variants are tractable Jan Martens, Jan Friso Groote

Deltas

Definition

Define the minimal observation depth $\Delta : S \times S \to \mathbb{N} \cup \infty$ by

$$\Delta(s,t) = \begin{cases} i & \text{if } s \not\leftrightarrow_i t \text{ and } s \leftrightarrow_{i-1} t \\ \infty & \text{if } s \leftrightarrow t \end{cases}$$

Define a function δ_i that gives the set of witnesses of this minimal observation depth, i.e. of s and t being i-distinguishable.

$$\delta_i(s,t) = \{(a,s')|\, s \xrightarrow{a} s' \text{ and } \forall\, t \xrightarrow{a} t', \Delta(s',t') \leq i-1\}$$

Computing minimal distinguishing Hennessy-Milner formulas is NP-hard, but variants are tractable Jan Martens, Jan Friso Groote

Algorithm 1: Minimal observations

Input: Two states $s, t \in S$ such that $s \not\leftrightarrow t$
Output: A HM-formula ϕ such that $s \models \phi$ and $t \not\models \phi$

```
function $\phi(s, t)$
    $i := \Delta(s, t)$
    if $\delta_i(s, t) = \emptyset$ then
        return $\neg\phi(t, s)$
    Select $(a, s') \in \delta_i(s, t)$
    $T := \{t' \mid t \xrightarrow{a} t'\}$                ▷ $\Delta(s', t') \leq i - 1$
    return $\langle a \rangle \left(\bigwedge_{t' \in T} \phi(s', t')\right)$
end
```

Optimization: Removing unnecessary conjuncts

```
$T := \{t' \mid t \xrightarrow{a} t'\}$
return $\langle a \rangle \left( \bigwedge_{t' \in T} \phi(s', t') \right)$
```

We create a distinguishing formula between each $t' \in T$ and s'

One formula can be a distinguishing formula for multiple t'
So, after each recursive call, check whether the formula holds for the other t' and remove unnecessary conjuncts

```
$T := \{t' \mid t \xrightarrow{a} t'\}$
while $T \neq \emptyset$ do
    Select $t_{max} \in T$ s.t. $\Delta(s, t_{max}) \geq \Delta(s, t') \; \forall t' \in T$
    $\phi_{t_{max}} := \phi(s, t_{max})$
    $\Phi := \Phi \wedge \phi_{t_{max}}$
    $T := \{t' \in T \mid t' \models \phi_{t_{max}}\}$
return $\langle a \rangle \Phi$
```

Silent steps

Definition

We introduce the internal or silent transition τ

In the definition of the LTS we change $Act \Rightarrow Act \cup \{\tau\} = Act_\tau$

We write $\xrightarrow{\tau}\!\!\!\!\rightarrow$ for zero or more combined τ steps and $\xrightarrow{(a)}$ for zero or one a steps.

Silent steps

Definition

We introduce the internal or silent transition τ

In the definition of the LTS we change $Act \Rightarrow Act \cup \{\tau\} = Act_\tau$

We write $\overset{\tau}{\twoheadrightarrow}$ for zero or more combined τ steps and $\xrightarrow{(a)}$ for zero or one a steps.

Are these strongly bisimilar?

Branching Bisimulation

Definition

Given an LTS $L = (S, \mathrm{Act}_\tau, \rightarrow)$. A symmetric relation $R \subseteq S \times S$ is called a branching bisimulation, iff for all sRt and $s \xrightarrow{a} s'$, either

- there are $t', t'' \in S$ such that $t \overset{\tau}{\twoheadrightarrow} t' \xrightarrow{a} t''$, sRt', and $s'Rt''$
- $a = \tau$ and $s'Rt$

$$\begin{tikzcd}
s \arrow[r, no head, squiggly, "R"] \arrow[d, "a"] \arrow[dr, no head, squiggly, "R"] & t \arrow[d, dotted, two heads, "\tau^*"] \\
s' \arrow[dr, no head, squiggly, "R"] & t' \arrow[d, dotted, "a"] \\
 & t''
\end{tikzcd}
\qquad
\begin{tikzcd}
s \arrow[r, no head, squiggly, "R"] \arrow[d, "\tau"'] & t \\
s' \arrow[ur, no head, squiggly, "R"] &
\end{tikzcd}$$

Two states $s, t \in S$ are said to be branching bisimilar, written as $s \leftrightarroweq_b t$, iff there is a branching bisimulation R such that sRt.

Branching Apartness

We want something like

$$s \not\leftrightarrow_b t \iff s \# t$$

Definition

Like k-bisimilarity, we define inductively a relation $\#_i$. Let $\#_0 = \emptyset$ and $s \#_{i+1} t$ if either:

- $s \#_i t$
- there is a path $s \xrightarrow{\tau} \!\!\!\!\!\rightarrow s' \xrightarrow{a} s''$ such that for all paths $t \xrightarrow{\tau} \!\!\!\!\!\rightarrow t' \xrightarrow{(a)} t''$ either $s' \#_i t'$ or $s'' \#_i t''$
- symmetrically, there is a path $t \xrightarrow{\tau} \!\!\!\!\!\rightarrow t' \xrightarrow{a} t''$ such that for all paths $s \xrightarrow{\tau} \!\!\!\!\!\rightarrow s' \xrightarrow{(a)} s''$ either $t' \#_i s'$ or $t'' \#_i s''$

We define the branching apartness relation $\# \subseteq S \times S$ by $\# = \bigcup_{i \in \mathbb{N}} \#_i$

Hennessy-Milner Logic without Until

Definition

Adapting *HML* for branching bisimulation, we restrict ourselves to formulas of the shape:

$$\phi ::= tt \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \langle\tau^*\rangle(\langle a\rangle\psi \wedge \phi)$$

Here $a \in Act \ \cup \{\hat{\tau}\}$, where $\langle\hat{\tau}\rangle\phi := \langle\tau\rangle\phi \vee \phi$

We call this Hennessy-Milner Logic without Until, or *HMLU*

A Hennessy-Milner Theorem

A Hennessy-Milner Theorem

Given an LTS $L = (S, Act_\tau, \rightarrow)$ and two states $s, t \in S$, we have:

$$s \leftrightarroweq_b t \quad \Longleftrightarrow \quad \forall \phi \in HMLU, s \models \phi \leftrightarrow t \models \phi$$

Distinguishing Formulas

We now have:

$$s \# t \iff \exists\phi \in HMLU, s \models \phi \wedge t \not\models \phi$$

And also:

$$s \#_i t \iff \exists\phi \in HMLU \text{ with } d_\diamond(\phi) = i, s \models \phi \wedge t \not\models \phi$$

Theorem 12. *Minimal Depth Distinguishing Formulas Without Until for Branching Bisimulation* Jan Martens, Jan Friso Groote

Deltas for Branching Bisimulation

We again need the minimal observation depth and suitable witnesses

$$\Delta(s, t) = \begin{cases} i & \text{if } s \#_i t \text{ and } \neg(s \#_{i-1} t) \\ \infty & \text{otherwise} \end{cases}$$

Deltas for Branching Bisimulation

We again need the minimal observation depth and suitable witnesses

$$\Delta(s,t) = \begin{cases} i & \text{if } s \#_i t \text{ and } \neg(s \#_{i-1} t) \\ \infty & \text{otherwise} \end{cases}$$

$$\delta_i(s,t) = \{(a, s', s'') \mid s \overset{\tau}{\twoheadrightarrow} s' \xrightarrow{a} s'' \text{ and } \forall t \overset{\tau}{\twoheadrightarrow} t' \xrightarrow{a} t'', \text{ it holds that } t' \#_{i-1} s' \text{ or } t'' \#_{i-1} s''\}$$

Algorithm 2: Minimal Depth for Branching Bisimulation

Input: Two states $s, t \in S$ such that $s \# t$.

Output: A formula $\phi \in HMLU$ such that $s \models \phi$ and $t \not\models \phi$.

```
function $\phi(s, t)$
    $i := \Delta(s, t)$
    if $\delta_i(s, t) = \emptyset$ then
        return $\neg\phi(t, s)$
    Select $(a, s', s'') \in \delta_i(s, t)$
    $\hat{a} := \hat{\tau}$ if $a = \tau$
    $\hat{a} := a$ otherwise
    $T_\tau := \{t' \mid t \overset{\tau}{\twoheadrightarrow} t'\}$
    $T := \{t'' \mid t' \in T_\tau, t' \xrightarrow{(a)} t''$ and $t'' \#_{i-1} s''\}$
    $\Phi_T := \textsc{Dist}(s'', T)$
    $T_\tau := \{t \in T_\tau \mid t \models \langle\hat{a}\rangle\Phi_T\}$
    $\Phi_{T_\tau} := \textsc{Dist}(s', T_\tau)$
    return $\langle\tau^*\rangle(\langle\hat{a}\rangle\Phi_T \wedge \Phi_{T_\tau})$
```

Algorithm 3: Removing unnecessary conjuncts

Input: a state $s \in S$, a set $T \subseteq S$ such that $s \# t$ for all $t \in T$.
Output: a formula $\phi \in HMLU$ s.t. $s \models \phi$ and $\forall t \in T, t \not\models \phi$.

```
function $\textsc{Dist}(s, T)$
    while $T \neq \emptyset$ do
        Select $t_{max} \in T$ s.t. $\Delta(s, t_{max}) \geq \Delta(s, t') \ \forall t' \in T$
        $\phi_{t_{max}} := \phi(s, t_{max})$
        $\Phi := \Phi \wedge \phi_{t_{max}}$
        $T := \{t' \in T \mid t' \models \phi_{t_{max}}\}$
    return $\Phi$
```

Proof MIN-DIST NP-Hard

Given an LTS $L = (S, Act, \rightarrow)$ and two states $s, t \in S$

MIN-DIST

There is a formula $\phi \in HML$ with less observations than $|S|$ such that ϕ distinguishes s and t, and $|\phi| \leq l$ for some $l \in \mathbb{N}$

Proof MIN-DIST NP-Hard

Theorem

Given a CNF formula $C = C_1 \ \wedge \ \dots \ \wedge \ C_n$ with propositions $p_1, \dots, p_k$ we construct an LTS such that there is a distinguishing formula $\phi \in HML$ between s and t with $|\phi| \leq k + 2$ if and only if C is satisfiable.

Proof MIN-DIST NP-Hard

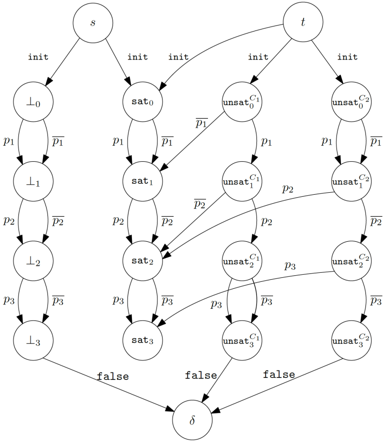


Figure: The LTS for the formula $C = (\neg p_1 \vee \neg p_2) \wedge (p_2 \vee p_3)$

Representation

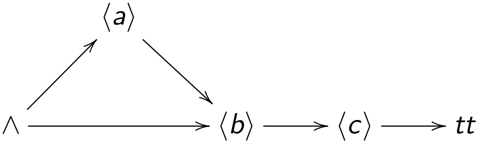
It can be shown that there is an exponential lower bound on the size of the minimal distinguishing formula. MIN-DIST is therefore not in NP. If we change the representation, a polynomial witness does exist.

For example, for the term $\langle a\rangle\langle b\rangle\langle c\rangle tt \wedge \langle b\rangle\langle c\rangle tt$

Equations:

- $\phi_1 = \langle a\rangle\phi_2 \wedge \phi_2$
- $\phi_2 = \langle b\rangle\langle c\rangle tt$

Shared Term:



Hennessy-Milner Logic with Until

Adapting *HML* for branching bisimulation, we introduce the Until

Definition

$$s \models \phi\langle a\rangle\psi \iff \text{there is } s \xrightarrow{\tau}\!\!\!\!\rightarrow s' \xrightarrow{a} s'' \text{ such that in all states from } s \text{ to } s', \phi \text{ holds and } s'' \models \psi$$

We define:

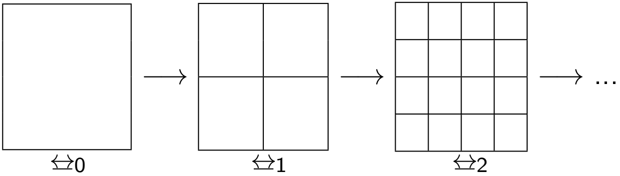
$$\phi ::= tt \mid \phi\langle a\rangle\psi \mid \neg\phi \mid \phi_1 \wedge \phi_2$$

- Until $\phi\langle a\rangle\psi$
- Negations $\neg\phi$
- Conjunctions $\phi_1 \wedge \phi_2$
- tt always holds

Partition Refinement

How do we obtain Δ and δ_i? Via a partition refinement algorithm

For each $a \in Act$ and other block B' split B into $split_a(B, B')$ and $B \setminus split_a(B, B')$ where $split_a(B, B') = \{s \in B \mid \exists s' \in B', s \xrightarrow{a} s'\}$



For apartness, observe that $s \# t \iff \forall B$ blocks, $s \notin B$ or $t \notin B$

Minimal Negation Depth

Definition

We inductively define the negation-depth of a formula in *HML*

- $d_\neg(tt) = 0$
- $d_\neg(\langle a \rangle \phi) = d_\neg(\phi)$
- $d_\neg(\neg \phi) = d_\neg(\phi) + 1$
- $d_\neg(\phi_1 \wedge \phi_2) = \max(d_\neg(\phi_1), d_\neg(\phi_2))$

Intuitively: the largest number of nested negations

Minimal Negation Depth

Combining observation (k) and negation depth (m)

Definition

We define *m-nested k-similarity inclusion*, denoted $\overset{\rightsquigarrow}{-}{}^{m}_{k}$, inductively. For all $s, t \in S$ we have $s \overset{\rightsquigarrow}{-}{}^{m}_{0} t$. If $s \overset{\rightsquigarrow}{-}{}^{m}_{k} t$ then

- if $s \xrightarrow{a} s'$ there is a $t \xrightarrow{a} t'$ such that $s' \overset{\rightsquigarrow}{-}{}^{m}_{k-1} t'$
- if $m > 0$ and $t \xrightarrow{a} t'$, then there is a $s \xrightarrow{a} s'$ such that $t' \overset{\rightsquigarrow}{-}{}^{m-1}_{k-1} s'$

Minimal Negation Depth

We again need the minimal depth and suitable witnesses (before: Δ and δ_i)

$$\overrightarrow{\Delta}_i(s,t) = \begin{cases} j & \text{if } s \not\underline{\rightsquigarrow}^{j}_{i} \ t \text{ and } s \ \underline{\rightsquigarrow}^{j-1}_{i} \ t \\ \infty & \text{if } s \ \underline{\leftrightarrow}_i \ t \end{cases}$$

$$\hat{\delta}^j_i(s,t) = \{(a,s') | \, s \xrightarrow{a} s' \text{ and}$$

$$\forall \, t \xrightarrow{a} t', \Delta(s',t') \leq i-1 \text{ and } \overrightarrow{\Delta}_i(s',t') \leq j\}$$

Minimal Negation Depth

Input: Two states $s, t \in S$ such that $s \not\underline{\leftrightarrow}_i t$ for some $i \in \mathbb{N}$
Output: A HM-formula ϕ such that $d_\diamond(\phi) = i$, $s \models \phi$ and $t \not\models \phi$

```
function $\varphi_i(s, t)$
    $j := \overrightarrow{\Delta}_i(s, t)$
    $\mathcal{X} := \hat{\delta}_i^j(s, t)$
    if $\mathcal{X} = \emptyset$ then
        return $\neg\varphi_i(t, s)$
    Select $(a, s') \in \mathcal{X}$
    $T := \{t' \mid t \xrightarrow{a} t'\}$
    while $T \neq \emptyset$ do
        Select $t_{\max} \in T$ s.t. $\overrightarrow{\Delta}_{i-1}(s', t_{\max})$ is maximal
        $\varphi_{t_{\max}} := \varphi_{i-1}(s', t_{\max})$
        $\Phi := \Phi \cup \{\varphi_{t_{\max}}\}$
        $T := \{t' \in T | t' \models \phi_{t_{max}}\}$
    return $\langle a \rangle \bigwedge_{\varphi \in \Phi} \varphi$
```