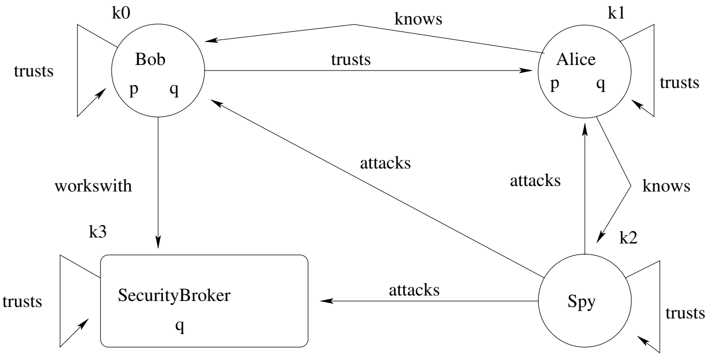
Hybrid logics, abstraction, and probabilities

Michael Huth[1]

[1]Department of Computing
Imperial College London

UCL, Intelligent Systems Seminar, 5 October 2005

Hybrid models and logics



- nominals, e.g. Bob, true at exactly one world
- formulas may refer to nominals n, e.g. "at n, ϕ" or "there is a cycle: $\exists n$, $EF\ n$" (not expressible in modal logic)
- an abstraction of the model above

Applications of abstraction through under-specification

- **state:** "a .NET component may have a `main` method"

Applications of abstraction through under-specification

- **state:** "a .NET component may have a `main` method"
- **behavior:** "an audio plug-in may be present in a browser"

Applications of abstraction through under-specification

- **state:** "a .NET component may have a `main` method"
- **behavior:** "an audio plug-in may be present in a browser"
- **interface:** "`requires balance >= 0`"

Applications of abstraction through under-specification

- **state:** "a .NET component may have a `main` method"
- **behavior:** "an audio plug-in may be present in a browser"
- **interface:** "`requires balance >= 0`"
- **topology:** "a node may have no neighbor in its broadcast range"

Applications of abstraction through under-specification

- **state:** "a .NET component may have a `main` method"
- **behavior:** "an audio plug-in may be present in a browser"
- **interface:** "`requires balance >= 0`"
- **topology:** "a node may have no neighbor in its broadcast range"
- **space-time:** "packets will get through in an ad-hoc network if no node is ever hostile."

Under-specifying propositional models

- models $M\colon \mathit{AtomicProp} \to \{0, 1/2, 1\}$, e.g. $[p \mapsto 1/2, q \mapsto 0]$

Under-specifying propositional models

- models $M\colon AtomicProp \rightarrow \{0, 1/2, 1\}$, e.g. $[p \mapsto 1/2, q \mapsto 0]$
- M' refines M iff $\forall p\colon M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$, e.g. $[p \mapsto 1, q \mapsto 0]$ refines $[p \mapsto 1/2, q \mapsto 0]$

Under-specifying propositional models

- models $M\colon \mathit{AtomicProp} \to \{0, 1/2, 1\}$, e.g. $[p \mapsto 1/2, q \mapsto 0]$
- M' refines M iff $\forall p\colon M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$, e.g. $[p \mapsto 1, q \mapsto 0]$ refines $[p \mapsto 1/2, q \mapsto 0]$
- thorough: $M \models^{th} \phi$ iff all 2-valued refinements of M satisfy ϕ

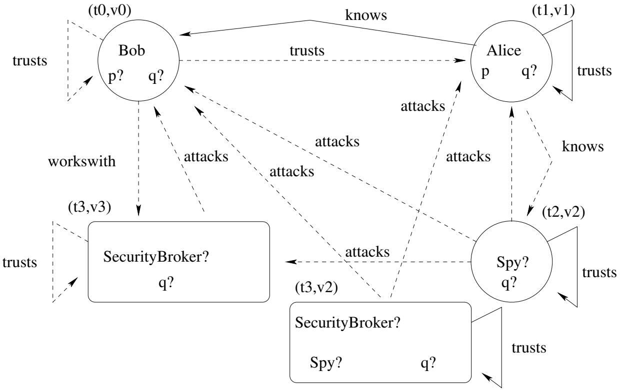
Under-specifying propositional models

- models $M\colon \mathit{AtomicProp} \to \{0, 1/2, 1\}$, e.g. $[p \mapsto 1/2, q \mapsto 0]$
- M' refines M iff $\forall p\colon M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$, e.g. $[p \mapsto 1, q \mapsto 0]$ refines $[p \mapsto 1/2, q \mapsto 0]$
- thorough: $M \models^{th} \phi$ iff all 2-valued refinements of M satisfy ϕ
- compositional: $M \models^{val} \phi$ interprets $1/2$ as 0 (1) in positive (negative) contexts, implies $M \models^{th} \phi$

Under-specifying propositional models

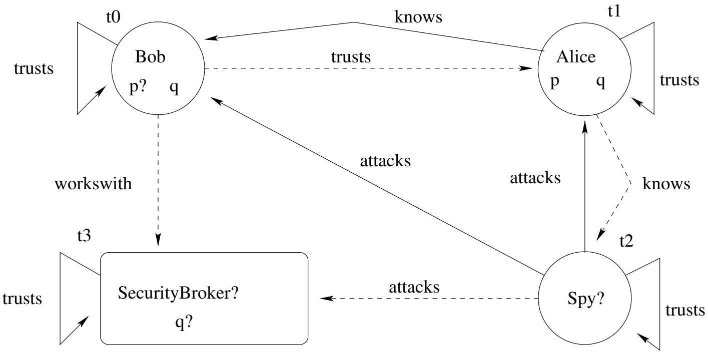
- models $M\colon \mathit{AtomicProp} \to \{0, 1/2, 1\}$, e.g. $[p \mapsto 1/2, q \mapsto 0]$
- M' refines M iff $\forall p\colon M(p) \neq 1/2 \Rightarrow M(p) = M'(p)$, e.g. $[p \mapsto 1, q \mapsto 0]$ refines $[p \mapsto 1/2, q \mapsto 0]$
- thorough: $M \models^{th} \phi$ iff all 2-valued refinements of M satisfy ϕ
- compositional: $M \models^{val} \phi$ interprets $1/2$ as 0 (1) in positive (negative) contexts, implies $M \models^{th} \phi$
- loss of precision: $[p \mapsto 1/2] \models^{th} p \vee \neg p$ but $[p \mapsto 1/2] \not\models^{val} p \vee \neg p$

Under-specifying temporal models



- abstracts ▸ initial model, abstracts ▸ another model
- ? and dashed lines $\equiv 1/2$, solid lines and atoms with no ? $\equiv 1$
- SecurityBroker possibly true at two worlds, refinement can only realize one choice

Refinement



a refinement of the model on previous slide, refinement preserves guarantees and introduces no “new” possibilities

Compositional and thorough semantics

- compositional: $M \models^{val} \phi$ again interprets $1/2$ as 0 (1) in negative (positive) contexts, noting $[\alpha]\phi = \neg\langle\alpha\rangle\neg\phi$

Compositional and thorough semantics

- compositional: $M \models^{val} \phi$ again interprets $1/2$ as 0 (1) in negative (positive) contexts, noting $[\alpha]\phi = \neg\langle\alpha\rangle\neg\phi$
- thorough: $M \models^{th} \phi$ iff all 2-valued refinements of M satisfy ϕ

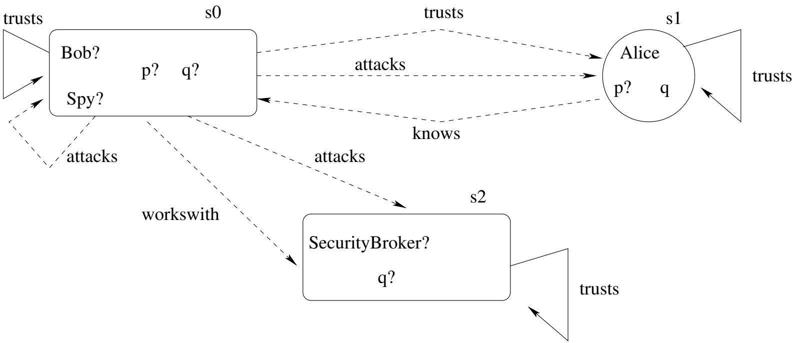
Compositional and thorough semantics

- compositional: $M \models^{val} \phi$ again interprets 1/2 as 0 (1) in negative (positive) contexts, noting $[\alpha]\phi = \neg\langle\alpha\rangle\neg\phi$
- thorough: $M \models^{th} \phi$ iff all 2-valued refinements of M satisfy ϕ
- compositional semantics sound: $M \models^{val} \phi \Rightarrow M \models^{th} \phi$ for all M, ϕ

Compositional and thorough semantics

- compositional: $M \models^{val} \phi$ again interprets $1/2$ as 0 (1) in negative (positive) contexts, noting $[\alpha]\phi = \neg\langle\alpha\rangle\neg\phi$
- thorough: $M \models^{th} \phi$ iff all 2-valued refinements of M satisfy ϕ
- compositional semantics sound: $M \models^{val} \phi \Rightarrow M \models^{th} \phi$ for all M, ϕ
- compositional semantics incomplete: inherited from propositional logic, e.g. $\langle\alpha\rangle\phi \vee \neg\langle\alpha\rangle\phi$

Example re-visited



- $s_0 \not\models^{val} \langle \mathrm{attacks} \rangle Alice \vee \neg \langle \mathrm{attacks} \rangle Alice$ as $(s_0, \mathrm{attacks}, s_1)$ possible but $(s_0, \mathrm{attacks}, \cdot)$ not guaranteed

Predicate (functional) abstraction

- $M = (S, R \subseteq S \times S, L\colon (AP + Nom) \to \mathbb{P}(S))$ hybrid Kripke structure

Predicate (functional) abstraction

- $M = (S, R \subseteq S \times S, L\colon (AP + Nom) \to \mathbb{P}(S))$ hybrid Kripke structure
- equivalence relation $s \equiv s'$ iff for all $i = 1, \ldots, n$ $(s \models \phi_i \Leftrightarrow s' \models \phi_i)$

Predicate (functional) abstraction

- $M = (S, R \subseteq S \times S, L\colon (AP + Nom) \to \mathbb{P}(S))$ hybrid Kripke structure
- equivalence relation $s \equiv s'$ iff for all $i = 1, \ldots, n$ $(s \models \phi_i \Leftrightarrow s' \models \phi_i)$
- abstract model $(S/\equiv, R^{\exists\exists}, R^{\forall\exists}, L^{\exists}, L^{\forall})$

Predicate (functional) abstraction

- $M = (S, R \subseteq S \times S, L\colon (AP + Nom) \to \mathbb{P}(S))$ hybrid Kripke structure
- equivalence relation $s \equiv s'$ iff for all $i = 1, \ldots, n$ $(s \models \phi_i \Leftrightarrow s' \models \phi_i)$
- abstract model $(S/\equiv, R^{\exists\exists}, R^{\forall\exists}, L^{\exists}, L^{\forall})$
- $tR^{\exists\exists}t'$ iff $\exists s \in t\, \exists s' \in t' \colon sRs'$, possible transitions $\in \{1/2, 1\}$;
  $tR^{\forall\exists}t'$ iff $\forall s \in t\, \exists s' \in t' \colon sRs'$, guaranteed transitions $\in \{1\}$

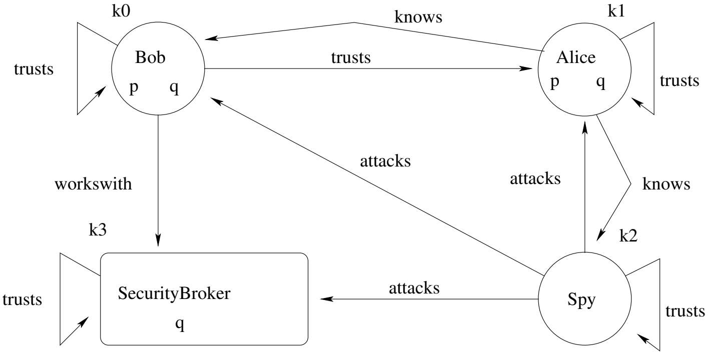
Predicate (functional) abstraction

- $M = (S, R \subseteq S \times S, L\colon (AP + Nom) \to \mathbb{P}(S))$ hybrid Kripke structure
- equivalence relation $s \equiv s'$ iff for all $i = 1, \ldots, n$ $(s \models \phi_i \Leftrightarrow s' \models \phi_i)$
- abstract model $(S/{\equiv}, R^{\exists\exists}, R^{\forall\exists}, L^{\exists}, L^{\forall})$
- $tR^{\exists\exists}t'$ iff $\exists s \in t\, \exists s' \in t'\colon sRs'$, possible transitions $\in \{1/2, 1\}$;
  $tR^{\forall\exists}t'$ iff $\forall s \in t\, \exists s' \in t'\colon sRs'$, guaranteed transitions $\in \{1\}$
- $t \in L^{\exists}(q)$ iff $\exists s \in t\colon s \in L(q)$, possible labels $\in \{1/2, 1\}$;
  $t \in L^{\forall}(q)$ iff $\forall s \in t\colon s \in L(q)$, guaranteed labels $\in \{1\}$

Predicate (functional) abstraction

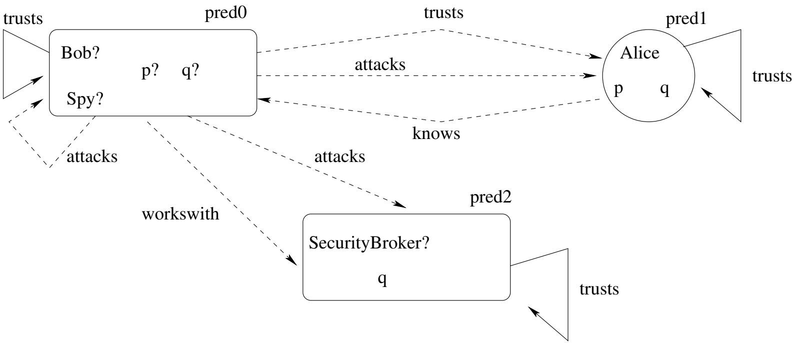
- $M = (S, R \subseteq S \times S, L\colon (AP + Nom) \to \mathbb{P}(S))$ hybrid Kripke structure
- equivalence relation $s \equiv s'$ iff for all $i = 1, \ldots, n$ $(s \models \phi_i \Leftrightarrow s' \models \phi_i)$
- abstract model $(S/\equiv, R^{\exists\exists}, R^{\forall\exists}, L^{\exists}, L^{\forall})$
- $tR^{\exists\exists}t'$ iff $\exists s \in t\, \exists s' \in t'\colon sRs'$, possible transitions $\in \{1/2, 1\}$;
  $tR^{\forall\exists}t'$ iff $\forall s \in t\, \exists s' \in t'\colon sRs'$, guaranteed transitions $\in \{1\}$
- $t \in L^{\exists}(q)$ iff $\exists s \in t\colon s \in L(q)$, possible labels $\in \{1/2, 1\}$;
  $t \in L^{\forall}(q)$ iff $\forall s \in t\colon s \in L(q)$, guaranteed labels $\in \{1\}$
- obtain: $\forall n \in Nom\colon L^{\forall}(n)$ empty or singleton; if singleton, then $L^{\exists}(n) = L^{\forall}(n)$;
  morale: turn these constraints into model axioms, even for relational abstractions

Example of predicate abstraction



- predicate abstraction of the model above with $\phi_1 = Alice$ and $\phi_2 = SecurityBroker$ results in ▸ this abstraction

Example of predicate abstraction con't



- the predicate abstraction of the ▸ concrete model with $\phi_1 = \mathit{Alice}$ and $\phi_2 = \mathit{SecurityBroker}$

Interlude: multiple-model checking

(Ongoing work with Altaf Hussain.)

- $M \models^{val} \phi$ and $M \models^{th} \phi$ reason about set $\mathcal{C}(M) = \{N \text{ 2-valued} \mid N \text{ refines } M\}$, link to "abstract interpretation."

Interlude: multiple-model checking

(Ongoing work with Altaf Hussain.)

- $M \models^{val} \phi$ and $M \models^{th} \phi$ reason about set $\mathcal{C}(M) = \{N \text{ 2-valued} \mid N \text{ refines } M\}$, link to "abstract interpretation."
- Requirements engineering, version control etc reason about

$$\bigcap_{i=1}^{k} \mathcal{C}(M_i)\,. \tag{1}$$

Interlude: multiple-model checking

(Ongoing work with Altaf Hussain.)

- $M \models^{val} \phi$ and $M \models^{th} \phi$ reason about set $\mathcal{C}(M) = \{N \text{ 2-valued} \mid N \text{ refines } M\}$, link to "abstract interpretation."
- Requirements engineering, version control etc reason about

$$\bigcap_{i=1}^{k} \mathcal{C}(M_i)\,. \tag{1}$$

- For fixed k: have efficient check for consistency, i.e. (1) $\neq \{\}$?

Interlude: multiple-model checking

(Ongoing work with Altaf Hussain.)

- $M \models^{val} \phi$ and $M \models^{th} \phi$ reason about set $\mathcal{C}(M) = \{N \text{ 2-valued} \mid N \text{ refines } M\}$, link to "abstract interpretation."
- Requirements engineering, version control etc reason about

$$\bigcap_{i=1}^{k} \mathcal{C}(M_i)\,. \tag{1}$$

- For fixed k: have efficient check for consistency, i.e. $(1) \neq \{\}$?
- If all M_i deterministic, (1) representable as $\mathcal{C}(\hat{M})$; not true for non-deterministic M_i, requires tree-automata-like models.

Interlude: multiple-model checking

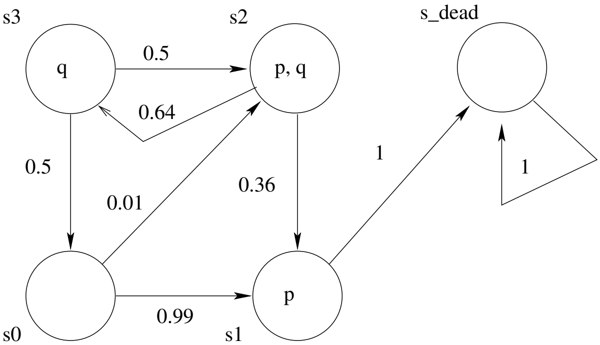
(Ongoing work with Altaf Hussain.)

- $M \models^{val} \phi$ and $M \models^{th} \phi$ reason about set $\mathcal{C}(M) = \{N \text{ 2-valued} \mid N \text{ refines } M\}$, link to "abstract interpretation."
- Requirements engineering, version control etc reason about

$$\bigcap_{i=1}^{k} \mathcal{C}(M_i)\,. \tag{1}$$

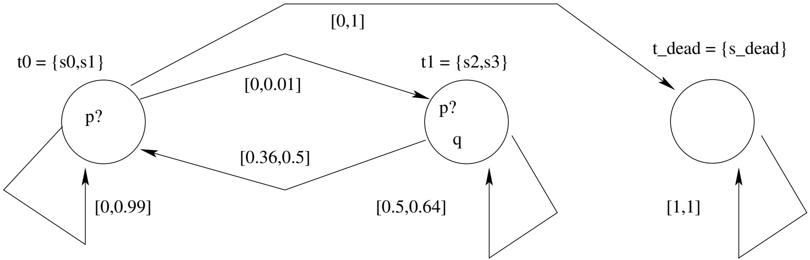
- For fixed k: have efficient check for consistency, i.e. $(1) \neq \{\}$?
- If all M_i deterministic, (1) representable as $\mathcal{C}(\hat{M})$; not true for non-deterministic M_i, requires tree-automata-like models.
- Seek good analogue of efficient $M \models^{val} \phi$ in this setting.

A probabilistic system



- discrete-time labeled Markov chain
- transition = probability measure over state space

An abstraction of that probabilistic system



- predicate abstraction of model on previous slide
- intervals approximate non-additive Choquet capacities
- nominals (if present) are treated as before

Probabilities and abstraction

- Probabilistic model checking is expensive.

Probabilities and abstraction

- Probabilistic model checking is expensive.
- Predicate abstraction and CEGAR for probabilistic systems possible?

Probabilities and abstraction

- Probabilistic model checking is expensive.
- Predicate abstraction and CEGAR for probabilistic systems possible?
- Right abstract structures: measures, Choquet capacities, etc?

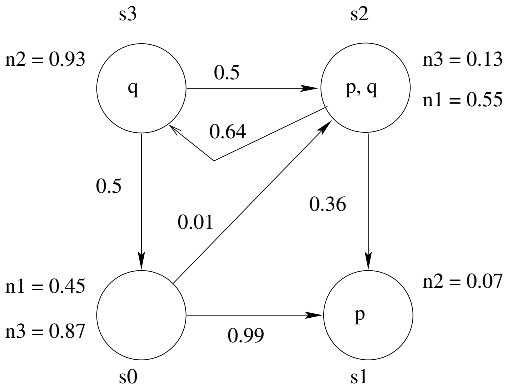
Probabilities and abstraction

- Probabilistic model checking is expensive.
- Predicate abstraction and CEGAR for probabilistic systems possible?
- Right abstract structures: measures, Choquet capacities, etc?
- Complete (i.e. finite state) abstractions for probabilistic CTL or modal mu-calculus?

Probabilities and abstraction

- Probabilistic model checking is expensive.
- Predicate abstraction and CEGAR for probabilistic systems possible?
- Right abstract structures: measures, Choquet capacities, etc?
- Complete (i.e. finite state) abstractions for probabilistic CTL or modal mu-calculus?
- Optimal finite state abstractions for finite set of properties of some probabilistic logic?

Probabilistic nominals



- probabilistic system as before
- but now nominals governed by probability distribution
- atomic events for nominals of the form “*n* is at state *s*”

Hybrid probabilistic computation tree logic

$$\phi ::= \ldots\ PCTL\ \ldots \mid @_n^{\sqsupseteq p}.\phi \mid \downarrow(n,\delta).\phi \mid \exists(n,\Delta').\phi$$

$\Delta' \subseteq \Delta$ set of probability measures

- "at n, ϕ holds with probability $\sqsupseteq p$:" $s \models_L @_n^{\sqsupseteq p}.\phi$ iff $\sum\{L(n,s') \mid s' \models_{L[n\mapsto\delta_{s'}]} \phi\} \sqsupseteq p$; reflects conditional probabilities of n's being at s'; where $L[n \mapsto \delta](n) = \delta$ and $L[n \mapsto \delta](m) = L(m)$ if $m \neq n$

Hybrid probabilistic computation tree logic

$$\phi ::= \ldots \; PCTL \; \ldots \mid @_n^{\sqsupseteq p}.\phi \mid \downarrow(n,\delta).\phi \mid \exists(n,\Delta').\phi$$

$\Delta' \subseteq \Delta$ set of probability measures

- "at n, ϕ holds with probability $\sqsupseteq p$:"
  $s \models_L @_n^{\sqsupseteq p}.\phi$ iff $\sum\{L(n,s') \mid s' \models_{L[n \mapsto \delta_{s'}]} \phi\} \sqsupseteq p$; reflects conditional probabilities of n's being at s'; where $L[n \mapsto \delta](n) = \delta$ and $L[n \mapsto \delta](m) = L(m)$ if $m \neq n$
- "if n is rebound to δ, ϕ holds:"
  $s \models_L \downarrow(n,\delta).\phi$ iff $s \models_{L[n \mapsto \delta]} \phi$

Hybrid probabilistic computation tree logic

$$\phi ::= \ldots\ PCTL\ \ldots \mid @_n^{\sqsupseteq p}.\phi \mid \downarrow(n,\delta).\phi \mid \exists(n,\Delta').\phi$$

$\Delta' \subseteq \Delta$ set of probability measures

- "at n, ϕ holds with probability $\sqsupseteq p$:"
  $s \models_L @_n^{\sqsupseteq p}.\phi$ iff $\sum\{L(n,s') \mid s' \models_{L[n \mapsto \delta_{s'}]} \phi\} \sqsupseteq p$; reflects conditional probabilities of n's being at s'; where $L[n \mapsto \delta](n) = \delta$ and $L[n \mapsto \delta](m) = L(m)$ if $m \neq n$
- "if n is rebound to δ, ϕ holds:"
  $s \models_L \downarrow(n,\delta).\phi$ iff $s \models_{L[n \mapsto \delta]} \phi$
- "it is possible to rebind n in Δ' such that ϕ holds:"
  $s \models_L \exists(n,\Delta').\phi$ iff for some $\delta \in \Delta'$: $s \models_{L[n \mapsto \delta]} \phi$

expressiveness of hybrid PCTL

- subsumes $(M, s) \models_L \downarrow n.\phi$ through $(M, s) \models_L \downarrow (n, \delta_s).\phi$

expressiveness of hybrid PCTL

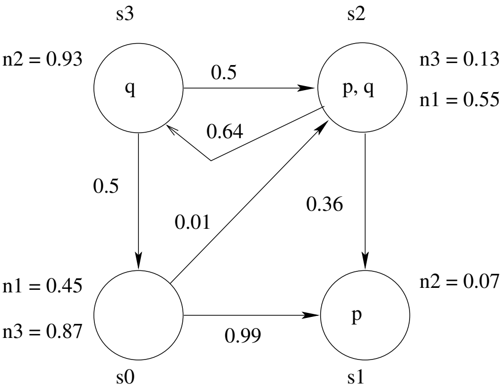
- subsumes $(M, s) \models_L \downarrow n.\phi$ through $(M, s) \models_L \downarrow (n, \delta_s).\phi$
- subsumes $(M, s) \models_L \exists n.\phi$ through $(M, s) \models_L \exists (n, \{\delta_t \mid t \in \Sigma\}).\phi$

expressiveness of hybrid PCTL

- subsumes $(M, s) \models_L \downarrow n.\phi$ through $(M, s) \models_L \downarrow(n, \delta_s).\phi$
- subsumes $(M, s) \models_L \exists n.\phi$ through $(M, s) \models_L \exists(n, \{\delta_t \mid t \in \Sigma\}).\phi$
- can express probabilistic recurrence, e.g. that state s is on a cycle with probability at least .9999, as

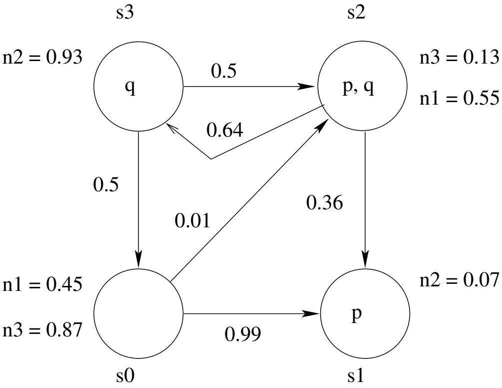
$$s \models_L \downarrow(n, \delta_s).[\mathit{true}\,\mathrm{U}\,n]_{\geq .9999}$$

Example probabilistic check



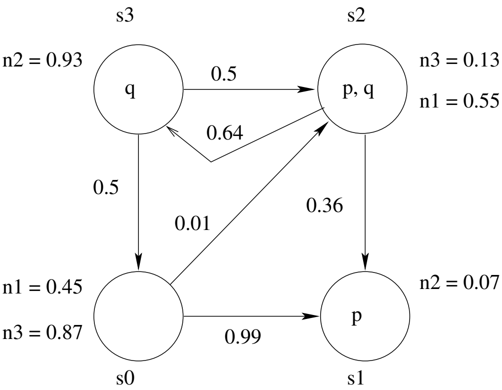
check $s_3 \models_L @^{>0.1}_{n_3}[true \, \mathrm{U} \, n_3]_{\geq 0.01}$ i.e.
is sum of all $L(n_3, s)$, with $s \models_{L[s \mapsto \delta_s]} [true \, \mathrm{U} \, n_3]_{\geq 0.01}$, > 0.1?
only s_0 and s_2 are relevant states s here

Example probabilistic check (2)



at s_0 for $L[n_3 \mapsto \delta_{s_0}]$, the probability that s_0 is on a cycle is $0.01 \cdot 0.64 \cdot 0.5 \cdot (\sum_{i=0}^{\infty}(0.64 \cdot 0.5)^i) = 0.00948529 \cdots \not\geq 0.01$ so $L(s_0, n_3) = 0.87$ does not contribute to that sum

Example probabilistic check (3)



at s_2 for $L[n_3 \mapsto \delta_{s_2}]$, the probability that s_2 is on a cycle is $0.64 \cdot 0.5 + 0.64 \cdot 0.5 \cdot 0.01 = 0.3232 \geq 0.01$ so $L(s_2, n_3) = 0.13$ is only contributor to that sum $\Rightarrow s_3 \models_L @_{n_3}^{>0.1}[\mathit{true}\ \mathrm{U}\ n_3]_{\geq 0.01}$ holds as $0.13 > 0.1$

Some references

- Huth, M. Abstraction and Probabilities for Hybrid Logics. *Electronic Notes in Theoretical Computer Science* 112 (2005) 61–76.
- Huth, M. On Finite-State Approximants for Probabilistic Computation Tree Logic. To appear in *Theoretical Computer Science*, 2005.
- Hussain, A. & Huth, M. On model checking multiple hybrid views. Extended version of paper given at the 1th International Symposium on Leveraging Applications of Formal Methods, Paphos, Cyprus, October 2004. Invited journal submission.

- Detailed references to related and originating work (e.g. by Kim Larsen) can be found in these papers.