

abstraction and probabilities for hybrid logics

Michael Huth

Department of Computing
Imperial College London

Acknowledgments: www.hylo.net

outline of talk

- 0 motivation
- 1 hybrid computation tree logic
- 2 relational abstraction for hybrid CTL
- 3 hybrid probabilistic CTL
- 4 conclusions

0 motivation

hybrid logics = temporal logics + ability to (re)bind names to unique states

applications: temporal logic for Pi-calculus, mobility, multiple agents, security etc

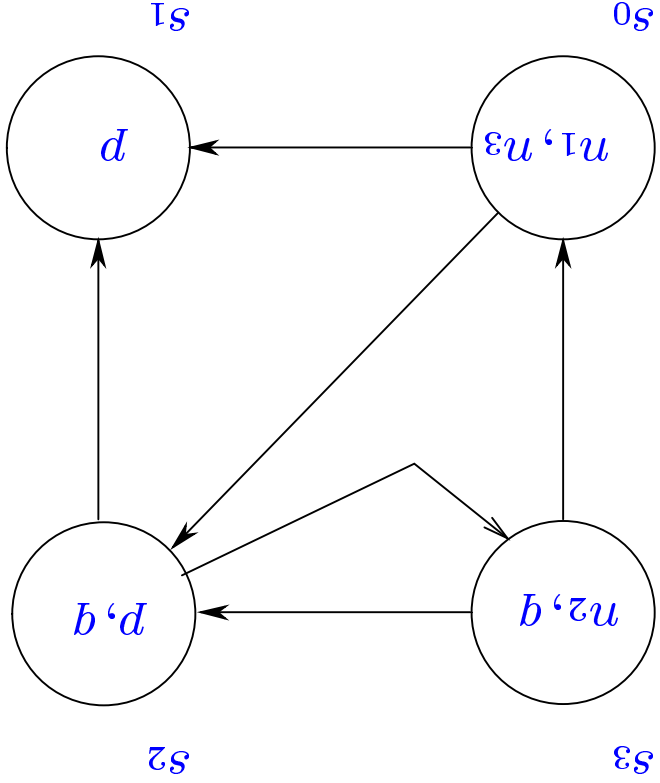
model-checking algorithms developed in [Franceschet & Rijke'03]

our contribution

1. hybrid CTL and its **relational abstraction**
2. hybrid PCTL and hybrid labelled Markov chains
1. \rightsquigarrow 2. : transfer of abstraction techniques
2. \rightsquigarrow 1. : relations as abstractions of probabilities

1 hybrid computation tree logic

a hybrid Kripke structure:



$$AP = \{p, q\}, \text{Nom} = \{n_1, n_2, n_3\}$$

all nominals are true at exactly one state

validity & correspondence theory

validity: $\text{EX } (n \wedge p) \wedge \text{EX } (n \wedge q) \rightarrow \text{EX } (p \wedge q)$
 not valid over Kripke structures ($n \in \text{AP}$)

but valid over hybrid Kripke structures ($n \in \text{Nom}$)

correspondence: “ $R \subseteq \Sigma \times \Sigma$ is irreflexive”

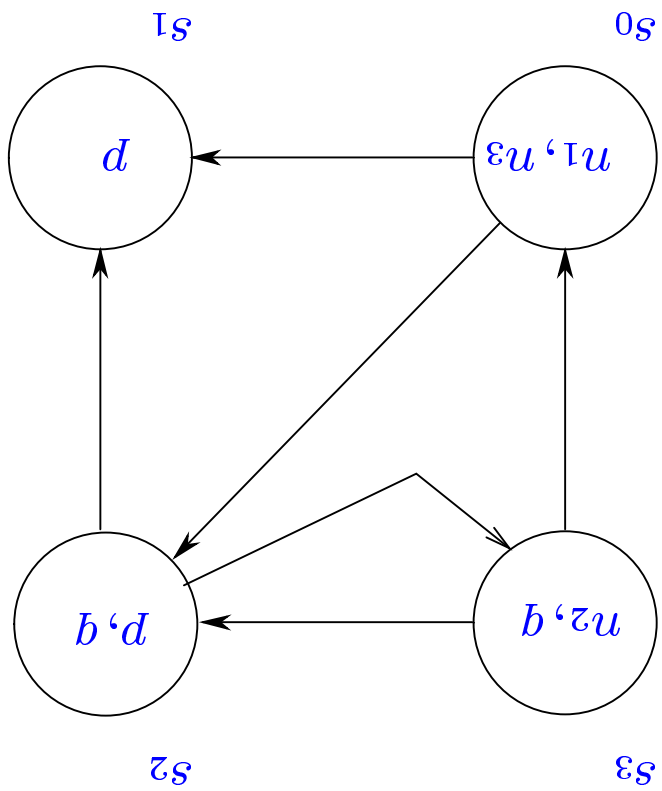
not expressible as Kripke frame satisfaction ($\Sigma, R \models \phi$ over

propositional modal logic

($\Sigma, R \models \phi$ means “for all labelling functions L , ($\Sigma, R, L \models \phi$)”)

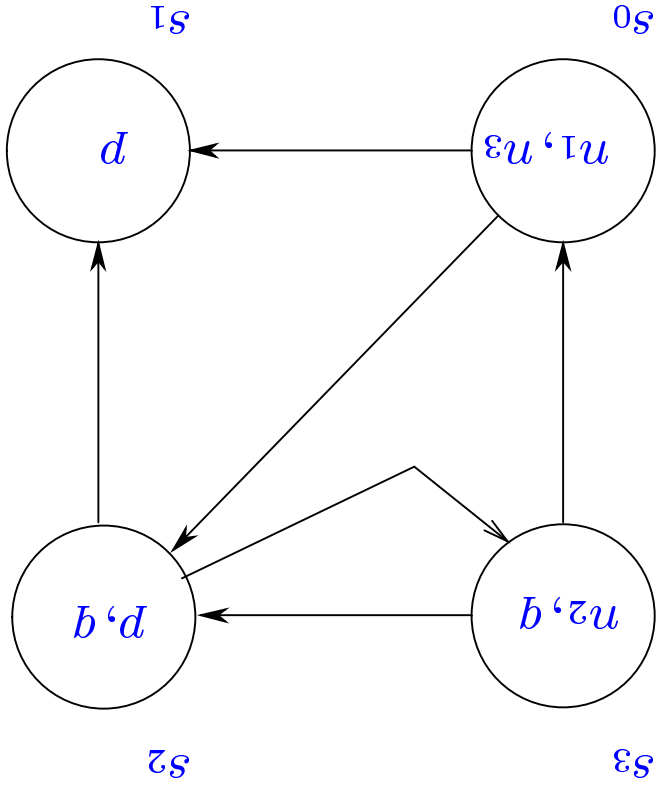
but $n \rightarrow \neg \text{EX } n$ captures this over hybrid models ($n \in \text{Nom}$)

since $(M, s_3) \models_T \text{EX } \neg d$ holds
 $(M, s_0) \models_T \text{EX } \neg d$ holds for T as in the picture



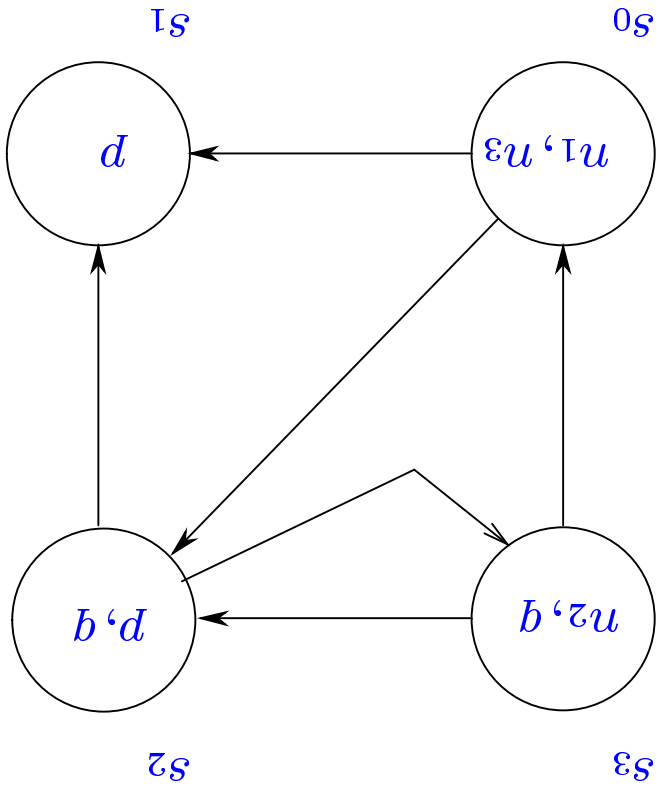
“at n , ϕ holds.”

“if n is rebound to current state, ϕ holds:”



$(M, s_0) \models_L \uparrow n_2. \neg \text{EX } n_2$ holds for L as in the picture since $(M, s_0) \models_{L[n_2 \mapsto s_0]} \neg \text{EX } n_2$ holds, for $(s_0, s_0) \notin R$

$(M, s_0) \models \exists n_1. \exists n_2. \exists n_3. d \wedge \neg \text{EX } d$ holds for L as in the picture
 as, e.g., $(M, s_0) \models L[n_1 \mapsto s_3] \wedge \neg \text{EX } d$



“it is possible to rebind n such that ϕ holds:”

2 relational abstraction for hybrid CTL

given: hybrid model $M = (\Sigma, R, L)$ and relation $\rho \subseteq \Sigma \times \hat{\Sigma}$

construct: abstract hybrid model \hat{M} with state set $\hat{\Sigma}$ such that for all spt and $\phi \in CTL(@, \uparrow, \exists)$, $(\hat{M}, t) \models \phi$ implies $(M, s) \models \phi$

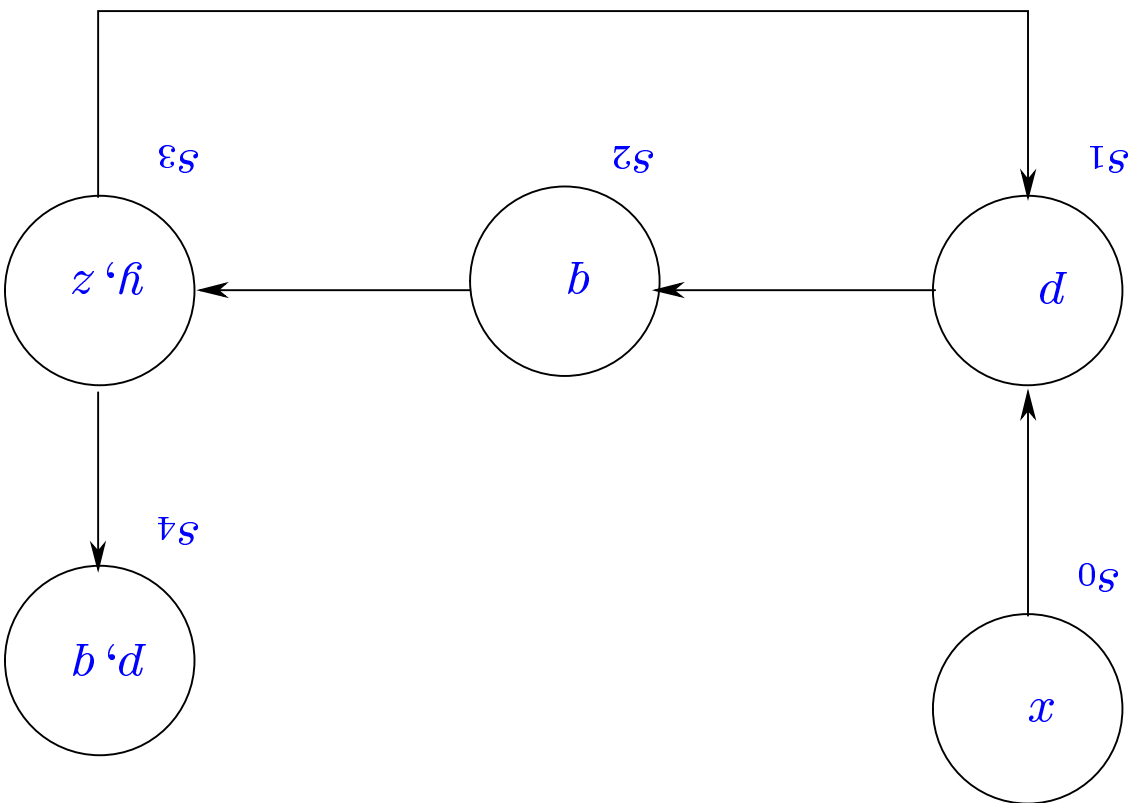
requires: ρ is left- and right-total, R and L have two components (“may” and “must”) such that for all $n \in \text{Nom}$:

$$1. \hat{L}^{must}(n) \subseteq L^{may}(n),$$

$$2. |\hat{L}^{must}(n)| \leq 1, \text{ and}$$

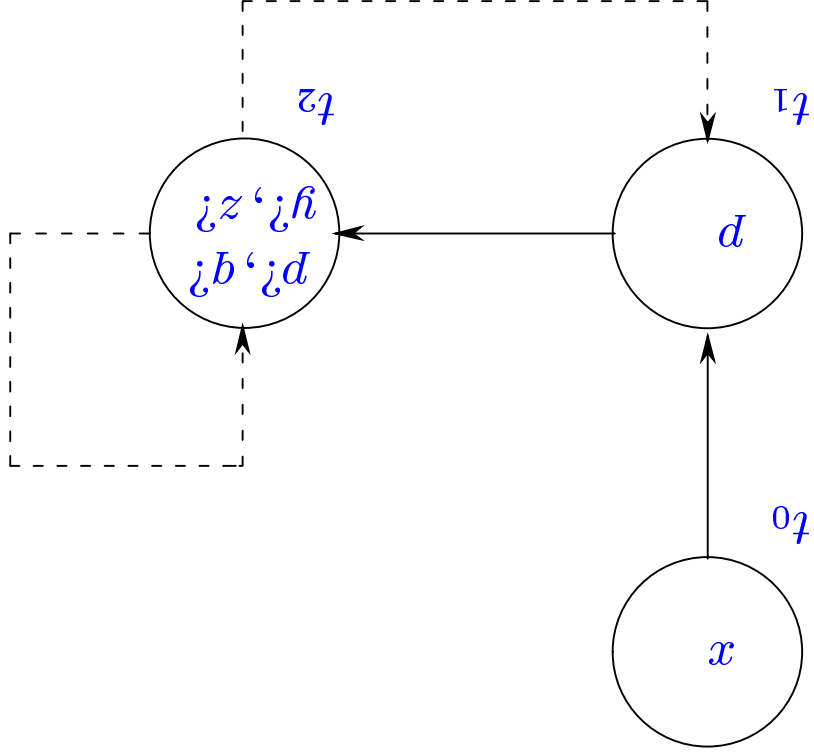
$$3. \hat{L}^{must}(n) \neq \{\} \Leftrightarrow L^{may}(n) = \hat{L}^{must}(n)$$

a shape graph



program identifiers x , y , and $z \in \text{Nom}$ point to heap cells
 d and b are atomic propositions about heap cells, e.g. $x * y >= -5$

“may” information = dashed lines and observables o with a $?$
 “must” information = solid lines and observables o without a $?$

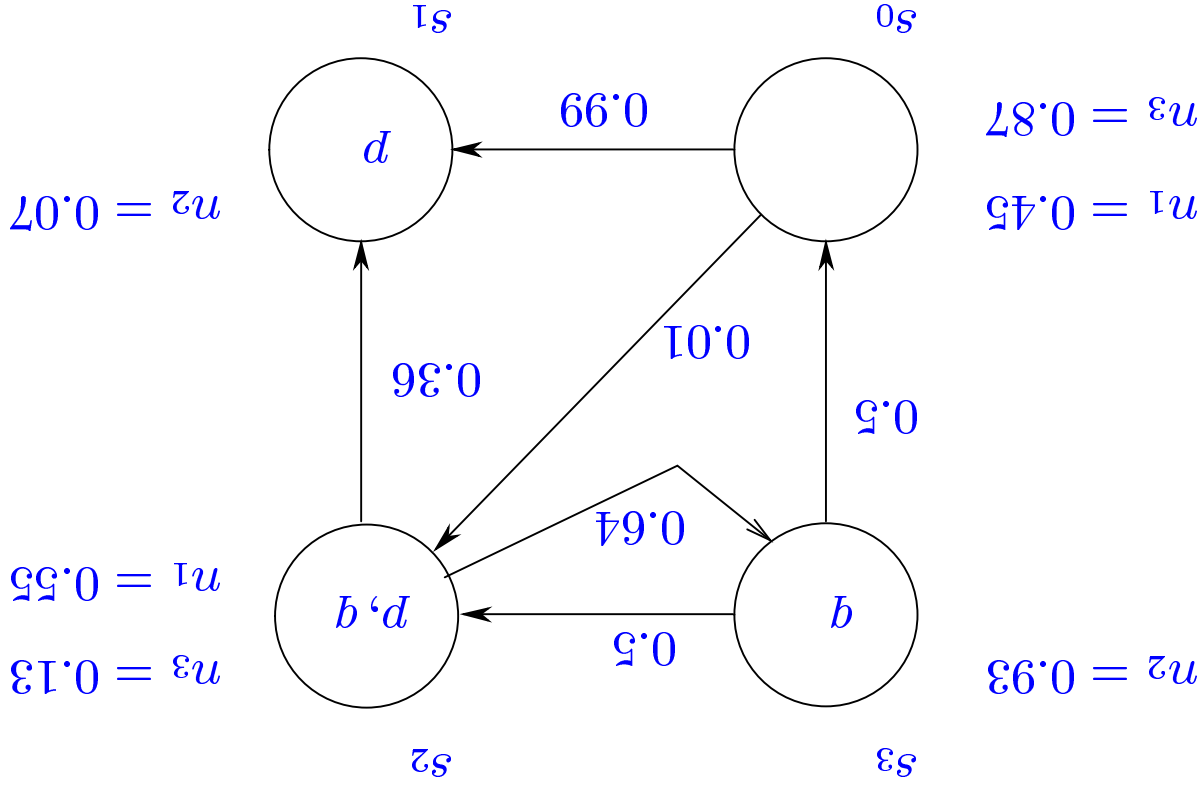


abstract shape graph of depth 2

3 hybrid PCTL

1. how should hybrid logics adapt to quantities and probabilities?
2. are model-checking back-ends and their data-structures affected by hybrid operators, if so how?
3. do relational abstraction techniques models transfer smoothly to quantities and probabilities?
4. how complex is model checking over labelled Markov chains on hybrid extensions of probabilistic computation tree logic?
first question on labelled Markov chains is a natural starting point

hybrid labelled Markov chains



R and labelling for AP give us a labelled Markov chain for each $n \in \text{Nom}$, $L(n)$ is a probability measure of n 's whereabouts and δ_s is a point measure

hybrid PCTL

$$\phi ::= \dots \text{PCTL} \dots \mid \text{@}_{\square p}^u \phi \mid \uparrow(n, \delta) \cdot \phi \mid \exists(n, \Delta') \cdot \phi$$

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

1. “at n , ϕ holds with probability $\square p$.”
 $(M, s) \models_T \text{@}_{\square p}^u \phi \iff \sum \{T(n, s') \mid (M, s') \models_T [n \leftrightarrow \delta'] \phi\} \subseteq p$

reflects conditional probabilities of n 's being at s' ; where
 $T[n \leftrightarrow \delta](n) = \delta$ and $T[n \leftrightarrow u] = T(m)$ if $m \neq n$

2. “if n is rebound to δ , ϕ holds.”
 $(M, s) \models_T \uparrow(n, \delta) \cdot \phi \iff (M, s) \models_T [n \leftrightarrow \delta] \phi$

3. “it is possible to rebound n in Δ' such that ϕ holds.”
 $(M, s) \models_T \exists(n, \Delta') \cdot \phi \iff$ for some $\delta \in \Delta'$: $(M, s) \models_T [n \leftrightarrow \delta] \phi$

expressiveness of hybrid PCTL

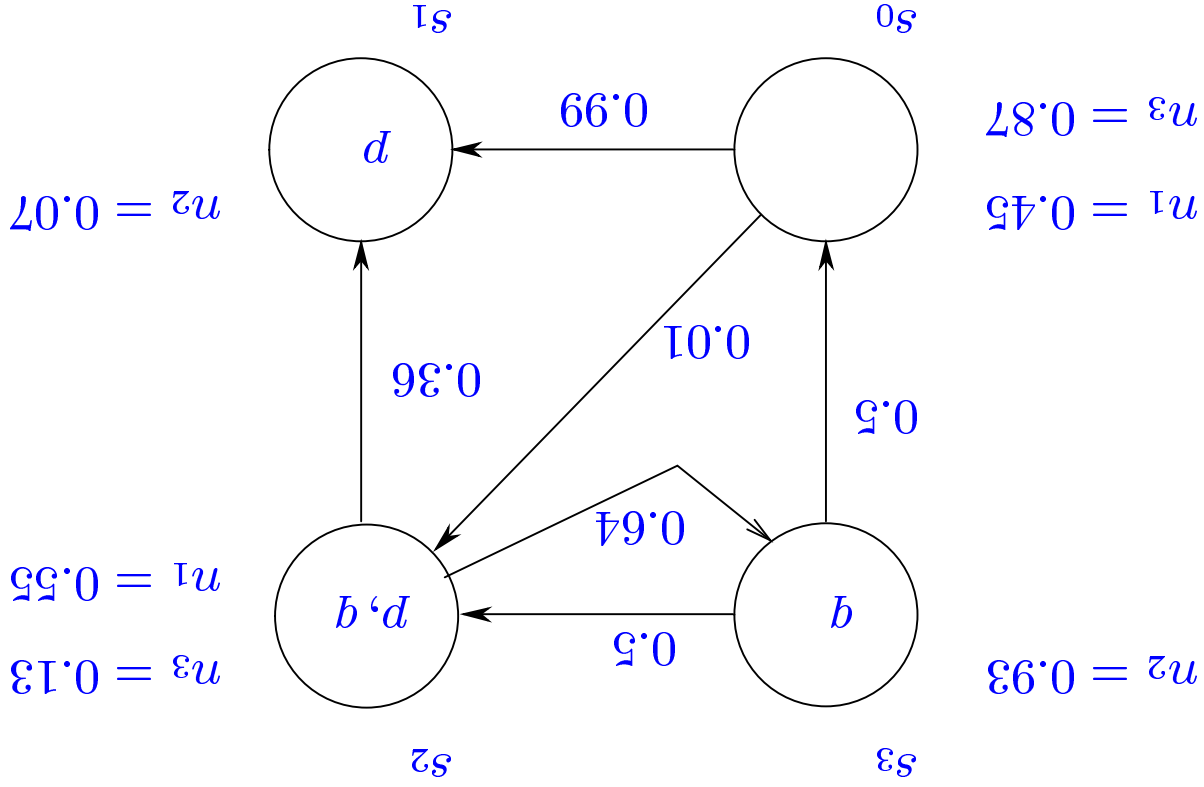
subsumes $(M, s) \models_T \uparrow n. \phi$ through $(M, s) \models_T \uparrow (n, \delta_s) \cdot \phi$

subsumes $(M, s) \models_T \exists n. \phi$ through $(M, s) \models_T \exists (n, \delta_t) \{ t \in \Sigma \} \cdot \phi$

can express probabilistic recurrence, e.g. that state s is on a cycle with probability at least $.9999$, as

$$(M, s) \models_T \uparrow (n, \delta_s) \cdot [true \cup n]_{\geq .9999}$$

example check

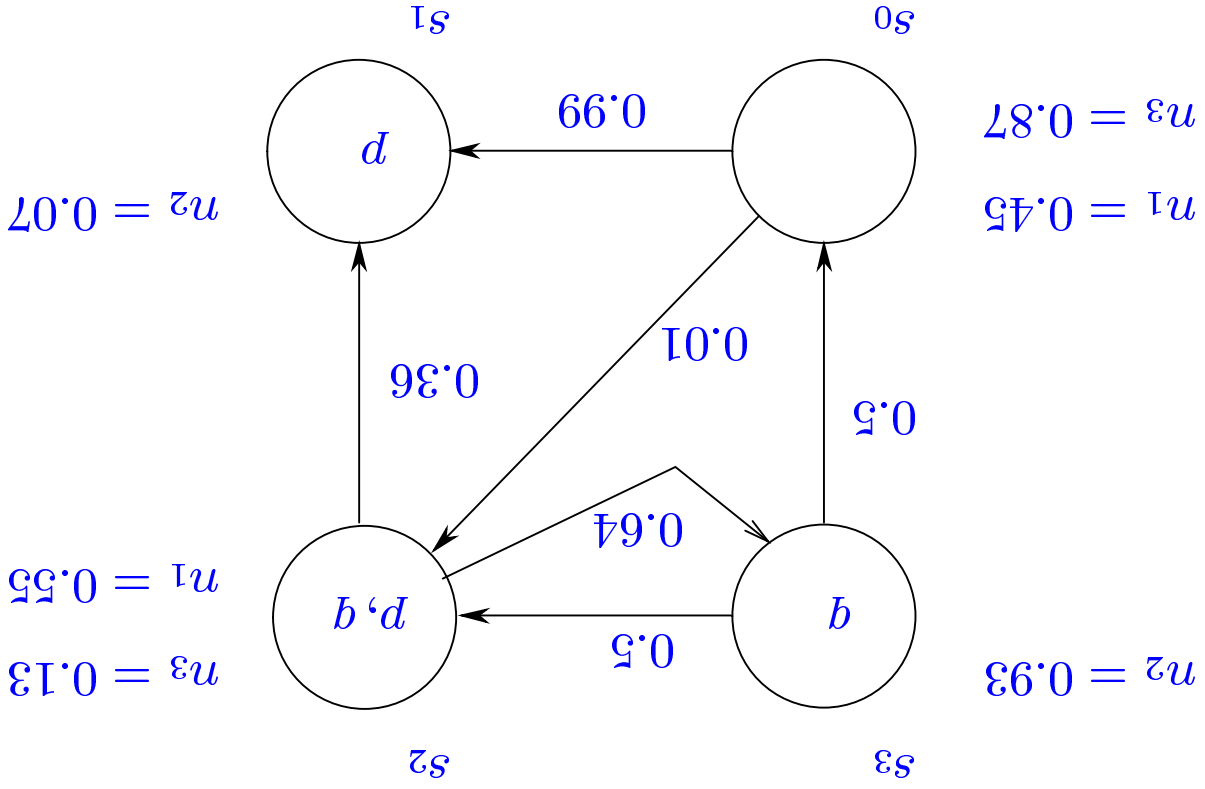


check $(M, s_3) \models_{L} \textcircled{>0.1}^{n_3} [true \cup n_3]_{\geq 0.01}$ i.e.

is sum of all $L(n_3, s)$, with $(M, s) \models_{L[s \leftrightarrow \delta_s]} [true \cup n_3]_{\geq 0.01}$, > 0.1 ?

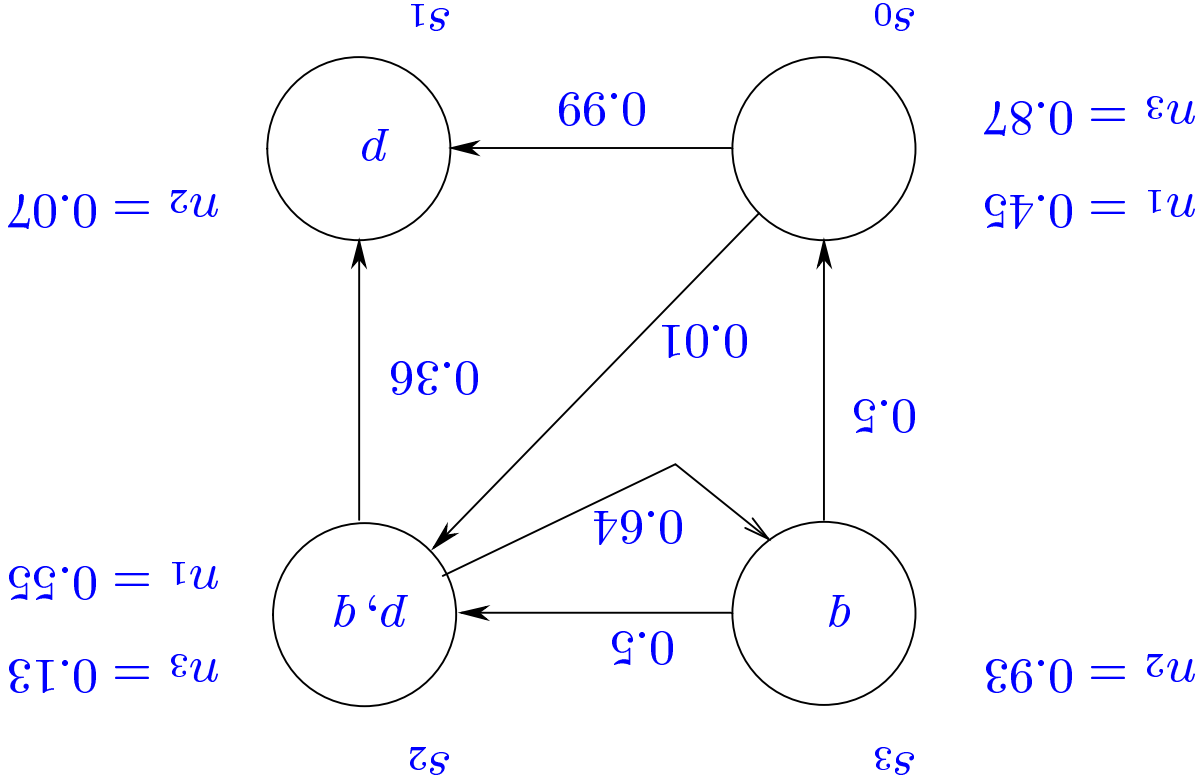
only s_0 and s_2 are relevant states s here

example check (2)



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

example 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 $\Leftrightarrow (M, s_3) \models_L \textcircled{a}_{>0.1} [true \cup n_3 \geq 0.01]$ holds as $0.13 > 0.1$

conclusions

(this page is intentionally left blank)