UNIVERSITY OF OXFORD

Quantitative verification techniques for probabilistic software

Marta Kwiatkowska

Oxford University Computing Laboratory

Summer School on Model Checking, Beijing, October 2010

Course overview

- 3 sessions (Mon/Tue/Thur): 6 $\times$ 50 minute lectures
  - 1: Markov decision processes (MDPs)
  - 2: Probabilistic LTL model checking
  - 3: Compositional probabilistic verification
  - 4: Abstraction, refinement and probabilistic software
  - 5: Probabilistic timed automata (PTAs)
  - 6: Software with time and probabilities
- For additional background material
  - and an accompanying list of references
  - see: http://www.prismmodelchecker.org/lectures/

Part 2

Probabilistic LTL model checking

Overview (Part 2)

- Linear temporal logic (LTL) for DTMCS/MDPs
- Strongly connected components (DTMCs)
- ω-automata (Büchi, Rabin)
- LTL model checking for DTMCs
- LTL model checking for MDPs

Limitations of PCTL

- PCTL, although useful in practice, has limited expressivity
  - essentially: probability of reaching states in X, passing only through states in Y (and within k time-steps)

- One useful approach: extend models with costs/rewards
  - see last lecture

- Another direction: Use more expressive logics. e.g.:
  - LTL [Pnu77] – (non-probabilistic) linear-time temporal logic
  - PCTL* [ASB+95,BdA95] – which subsumes both PCTL and LTL
  - both allow temporal (path) operators to be combined
  - (in PCTL, $P_{\sim p}$ [...] always contains a single temporal operator)

LTL – Linear temporal logic

- LTL syntax (path formulae only)
  - $\psi ::= \text{true} \mid a \mid \psi \wedge \psi \mid \neg\psi \mid X\,\psi \mid \psi\,U\,\psi$
  - where $a \in AP$ is an atomic proposition
  - usual equivalences hold: $F\,\phi \equiv \text{true}\;U\,\phi$, $G\,\phi \equiv \neg(F\,\neg\phi)$

- LTL semantics (for a path ω)
  - $\omega \vDash \text{true}$ always
  - $\omega \vDash a \quad\Leftrightarrow\quad a \in L(\omega(0))$
  - $\omega \vDash \psi_1 \wedge \psi_2 \quad\Leftrightarrow\quad \omega \vDash \psi_1$ and $\omega \vDash \psi_2$
  - $\omega \vDash \neg\psi \quad\Leftrightarrow\quad \omega \nvDash \psi$
  - $\omega \vDash X\,\psi \quad\Leftrightarrow\quad \omega[1\ldots] \vDash \psi$
  - $\omega \vDash \psi_1\,U\,\psi_2 \quad\Leftrightarrow\quad \exists k{\geq}0 \text{ s.t. } \omega[k\ldots] \vDash \psi_2 \wedge \forall i{<}k\ \omega[i\ldots] \vDash \psi_1$

  where $\omega(i)$ is i^{th} state of ω, and $\omega[i\ldots]$ is suffix starting at $\omega(i)$

LTL examples

- $(\mathrm{F}\ tmp\_fail_1) \wedge (\mathrm{F}\ tmp\_fail_2)$
  - “both servers suffer temporary failures at some point”
- GF ready
  - “the server always eventually returns to a ready-state”
- FG error
  - “an irrecoverable error occurs”
- G (req → X ack)
  - “requests are always immediately acknowledged”

LTL for DTMCs and MDPs

- Same idea as PCTL: probabilities of sets of path formulae
  - for a state s of a DTMC and an LTL formula ψ:
  - $Pr_s(\psi) = Pr_s \{ \omega \in Path_s \mid \omega \models \psi \}$
  - all such path sets are measurable [Var85]
  - and for an MDP: we have $Pr_s^{min}(\psi)$, $Pr_s^{max}(\psi)$ over adversaries

- A (probabilistic) LTL specification often comprises an LTL (path) formula and a probability bound
  - e.g. $P_{\geq 1}$ [GF ready] – "with probability 1, the server always eventually returns to a ready-state"
  - e.g. $P_{\leq 0.01}$ [FG error] – "with probability at most 0.01, an irrecoverable error occurs"

- PCTL* subsumes both LTL and PCTL
  - e.g. $P_{>0.5}$ [GF $crit_1$] $\wedge$ $P_{>0.5}$ [GF $crit_2$]

Overview (Part 2)

- Linear temporal logic (LTL) for DTMCS/MDPs
- Strongly connected components (DTMCs)
- ω-automata (Büchi, Rabin)
- LTL model checking for DTMCs
- LTL model checking for MDPs

Strongly connected components

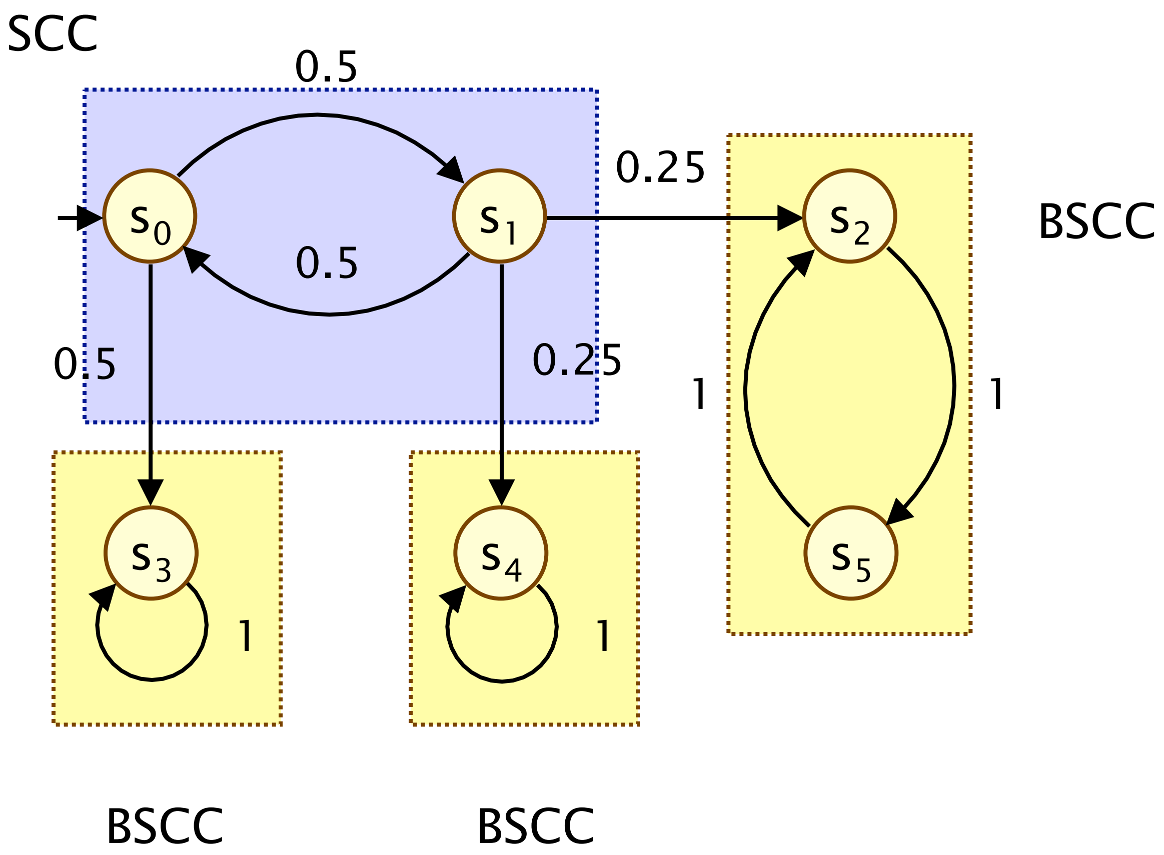
- Long-run properties of DTMCs rely on an analysis of their underlying graph structure (i.e. ignoring probabilities)

- Strongly connected set of states T
  - for any pair of states s and s’ in T, there is a path from s to s’, passing only through states in T

- Strongly connected component (SCC)
  - a maximally strongly connected set of states
    (i.e. no superset of it is also strongly connected)

- Bottom strongly connected component (BSCC)
  - an SCC T from which no state outside T is reachable from T

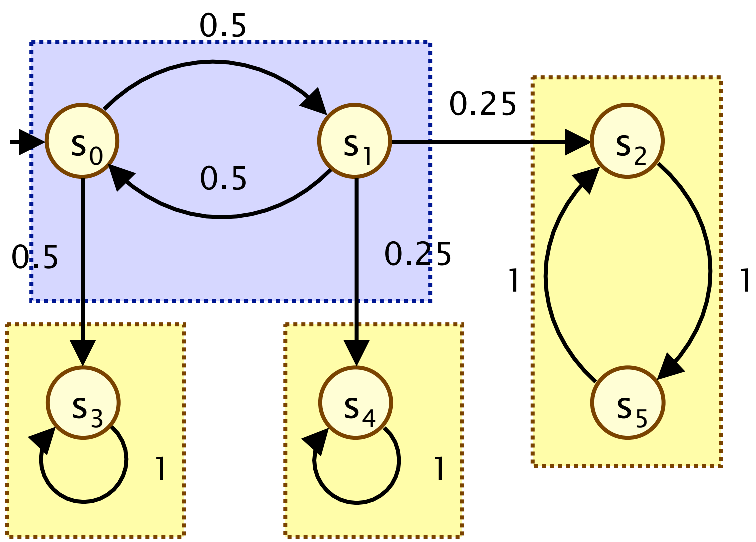
Example – (B)SCCs



Fundamental property of DTMCs

- Fundamental property of (finite) DTMCs…

- With probability 1,
  a BSCC will be reached
  and all of its states
  visited infinitely often



- Formally:
  - $\color{red}{Pr_s}$ $\{\ \omega \in Path_s \mid \exists\ i \geq 0,\ \exists$ BSCC T such that $\forall\ j \geq i\ \ \omega(i) \in T$ and $\forall\ s' \in T\ \ \omega(k) = s'$ for infinitely many $k\ \}$ $\color{red}{=\ 1}$

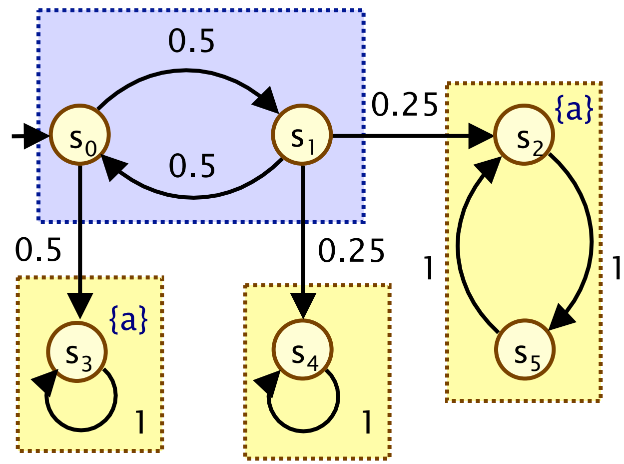
LTL model checking for DTMCs

- LTL model checking for DTMCs relies on:
  - computing the probability $Pr_s(\psi)$ for LTL formula ψ
  - reduces to probability of reaching a set of “accepting” BSCCs
  - 2 simple cases: GF a and FG a…

- $Pr_s(GF\ a) = Pr_s(F\ T_{GFa})$
  - where T_{GFa} = union of all BSCCs containing some state satisfying a

- $Pr_s(FG\ a) = Pr_s(F\ T_{FGa})$
  - where T_{FGa} = union of all BSCCs containing only a-states

- To extend this idea to arbitrary LTL formula, we use ω-automata…



Example:

$Pr_{s0}(GF\ a)$

$= Pr_{s0}(F\ T_{GFa})$

$= Pr_{s0}(F\ \{s_3,s_2,s_5\})$

$= 2/3 + 1/6 = 5/6$

Overview (Part 2)

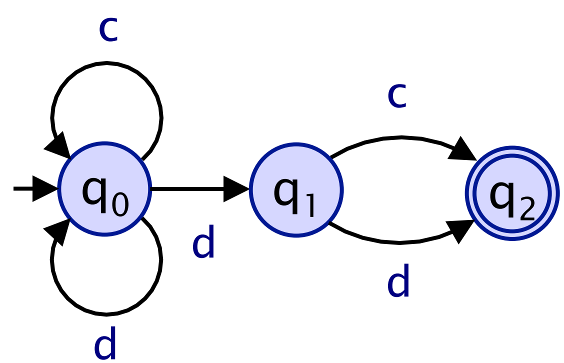
- Linear temporal logic (LTL) for DTMCS/MDPs
- Strongly connected components (DTMCs)
- ω-automata (Büchi, Rabin)
- LTL model checking for DTMCs
- LTL model checking for MDPs

Reminder – Finite automata

- A regular language over alphabet α
  - is a set of finite words $L \subseteq \alpha^*$ such that either:
  - $L = L(E)$ for some regular expression E
  - $L = L(A)$ for some nondeterministic finite automaton (NFA) A
  - $L = L(A)$ for some deterministic finite automaton (DFA) A

- Example:

  Regexp: $(c+d)^*d(c+d)$ NFA A:



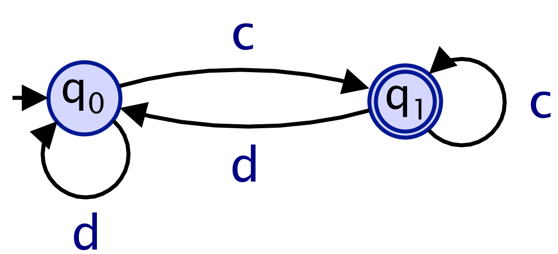
- NFAs and DFAs have the same expressive power
  - we can always determinise an NFA to an equivalent DFA
  - (with a possibly exponential blow-up in size)

Büchi automata

- ω-automata represent sets of infinite words $L \subseteq \alpha^\omega$
  - e.g. Büchi automata, Rabin automata, Streett, Muller, …

- A nondeterministic Büchi automaton (NBA) is…
  - a tuple $A = (Q, Q_{init}, \alpha, \delta, F)$ where:
  - Q is a finite set of states
  - $Q_{init} \subseteq Q$ is a set of initial states
  - α is an alphabet
  - $\delta : Q \times \alpha \to 2^Q$ is a transition function
  - $F \subseteq Q$ is a set of “accept” states

Example:
words $w \in \{c,d\}^\omega$
with infinitely many c



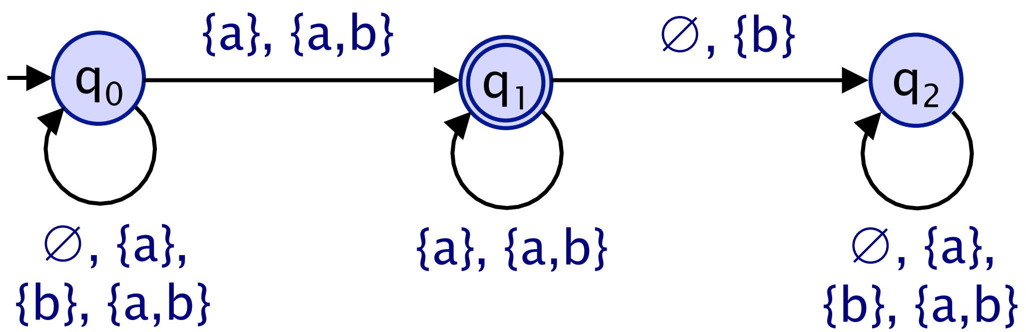
- NBA acceptance condition
  - language $L(A)$ for A contains $w \in \alpha^\omega$ if there is a corresponding run in A that passes through states in F infinitely often

ω-regular properties

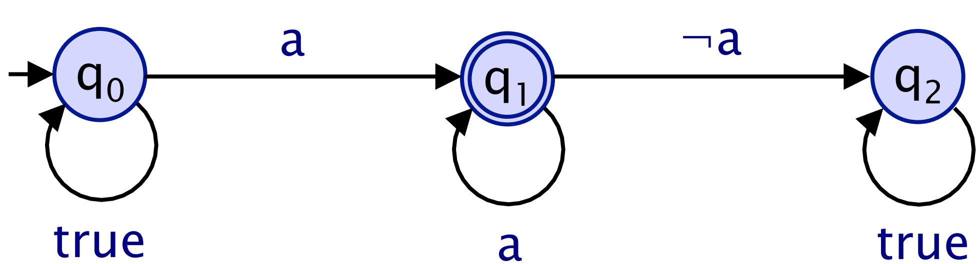
- Consider a model, i.e. an LTS/DTMC/MDP/…
  - for example: DTMC $D = (S, s_{init}, P, Lab)$
  - where labelling Lab uses atomic propositions from set AP
- We can capture properties of these using ω-automata
  - let $\omega \in Path_{D,s}$ be some infinite path in D
  - $trace(\omega) \in (2^{AP})^{\omega}$ denotes the projection of state labels of ω
  - i.e. $trace(s_0 s_1 s_2 s_3 \ldots) = Lab(s_0)Lab(s_1)Lab(s_2)Lab(s_3)\ldots$
  - can specify a set of paths of D with an ω-automata over 2^{AP}
- Let $Pr_{D,s}(A)$ denote the probability…
  - from state s in a discrete-time Markov chain D
  - of satisfying the property specified by automaton A
  - i.e. $Pr_{D,s}(A) = Pr_{D,s}\{ \omega \in Path_{D,s} \mid trace(\omega) \in L(A) \}$

Example

- Nondeterministic Büchi automaton
  - for LTL formula FG a, i.e. “eventually always a”
  - for a DTMC with atomic propositions AP = {a,b}



- We abbreviate this to just:



Büchi automata + LTL

- Nondeterministic Büchi automata (NBAs)
  - define the set of ω-regular languages
- ω-regular languages are more expressive than LTL
  - can convert any LTL formula ψ over atomic propositions AP
  - into an equivalent NBA A_ψ over 2^{AP}
  - i.e. $\omega \vDash \psi \Leftrightarrow trace(\omega) \in L(A_\psi)$ for any path ω
  - for LTL-to-NBA translation, see e.g. [VW94], [DGV99], [BK08]
  - worst-case: exponential blow-up from $|\psi|$ to $|A_\psi|$
- But deterministic Büchi automata (DBAs) are less expressive
  - e.g. there is no DBA for the LTL formula FG a
  - for probabilistic model checking, need deterministic automata
  - so we use deterministic Rabin automata (DRAs)

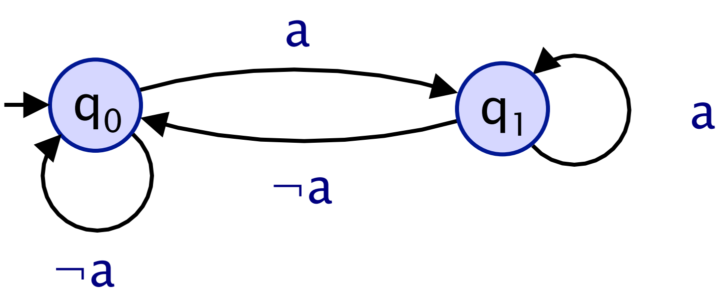
Deterministic Rabin automata

- A deterministic Rabin automaton is a tuple $(Q,q_{init},\alpha,\delta,Acc)$:
  - Q is a finite set of states, $q_{init} \in Q$ is an initial state
  - α is an alphabet, $\delta : Q \times \alpha \rightarrow Q$ is a transition function
  - $Acc = \{ (L_i, K_i) \}_{i=1..k} \subseteq 2^Q \times 2^Q$ is an acceptance condition

- A run of a word on a DRA is accepting iff:
  - for some pair (L_i, K_i), the states in L_i are visited finitely often and (some of) the states in K_i are visited infinitely often

  - or in LTL: $\bigvee_{1 \leq i \leq k} (\mathrm{FG}\, \neg L_i \wedge \mathrm{GF}\, K_i)$

- Example: DRA for FG a
  - acceptance condition is $Acc = \{ (\{q_0\},\{q_1\}) \}$

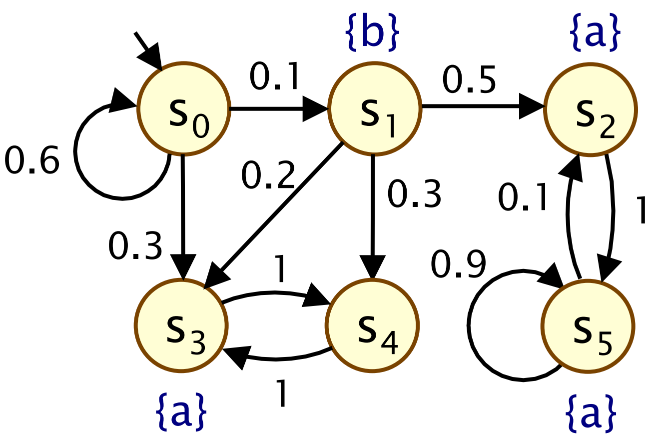


Overview (Part 2)

- Linear temporal logic (LTL) for DTMCS/MDPs
- Strongly connected components (DTMCs)
- ω-automata (Büchi, Rabin)
- LTL model checking for DTMCs
- LTL model checking for MDPs

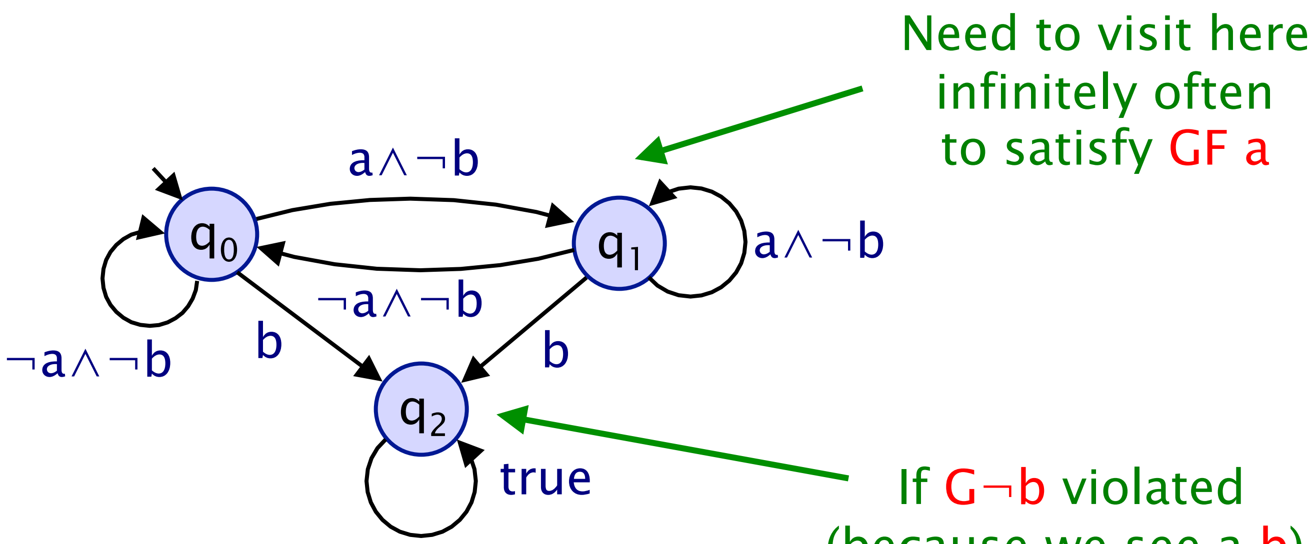
LTL model checking for DTMCs

- LTL model checking for DTMC D and LTL formula ψ
- 1. Construct DRA A_ψ for ψ
- 2. Construct product $D \otimes A$ of DTMC D and DRA A_ψ
- 3. Compute $Pr_{D,s}(\psi)$ from DTMC $D \otimes A$
- Running example:
  - compute probability of satisfying LTL formula $\psi = G\neg b \wedge GF\ a$ on:



Example - DRA

- DRA A_ψ for $\psi = G\neg b \wedge GF\, a$ is shown below
  - acceptance condition is Acc = { ({},{q_1}) }
  - (i.e. this is actually a deterministic Büchi automaton)



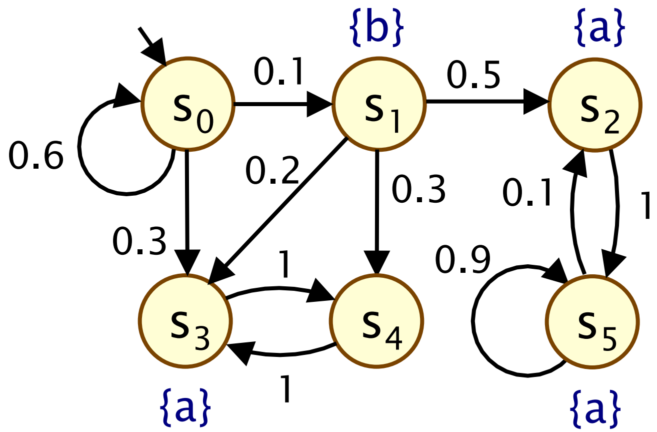
Product DTMC for a DRA

- We construct the product DTMC
  - for DTMC D and DRA A, denoted $D \otimes A$
  - $D \otimes A$ can be seen as an unfolding of D with states (s,q), where q records state of automata A for path fragment so far
  - since A is deterministic, $D \otimes A$ is a also a DTMC
  - each path in D has a corresponding (unique) path in $D \otimes A$
  - the probabilities of paths in D are preserved in $D \otimes A$

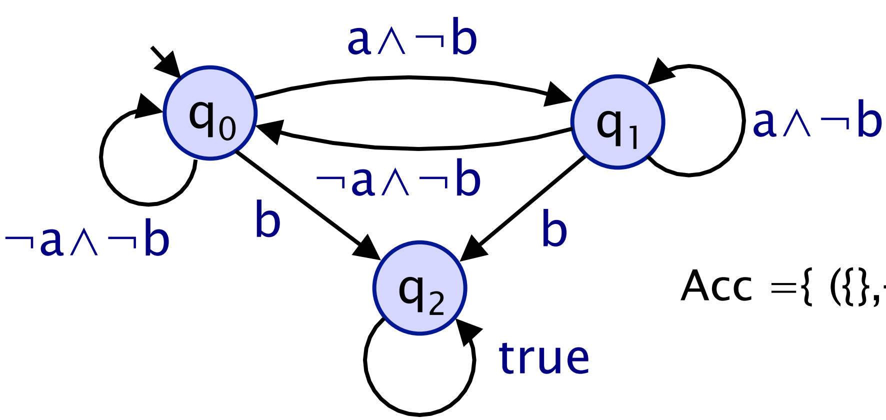
- Formally, for $D = (S,s_{init},P,L)$ and $A = (Q,\alpha,\delta,q_{init},\{(L_i,K_i)\}_{i=1..k})$
  - $D \otimes A$ is the DTMC $(S \times Q, (s_{init},q_{s_{init}}), P', L')$ where:
  - $q_{s_{init}} = \delta(q_{init},L(s_{init}))$
  - $P'((s_1,q_1),(s_2,q_2)) = \begin{cases} P(s_1,s_2) & \text{if } q_2 = \delta(q_1,L(s_2)) \\ 0 & \text{otherwise} \end{cases}$
  - $l_i \in L'(s,q)$ if $q \in L_i$ and $k_i \in L'(s,q)$ if $q \in K_i$

Example - Product DTMC

DTMC D

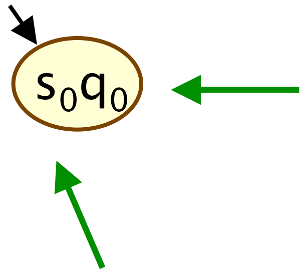


DRA A_ψ for $\psi = G\neg b \wedge GF\ a$



Acc ={ ({},{q_1}) }

Product DTMC $D \otimes A_\psi$

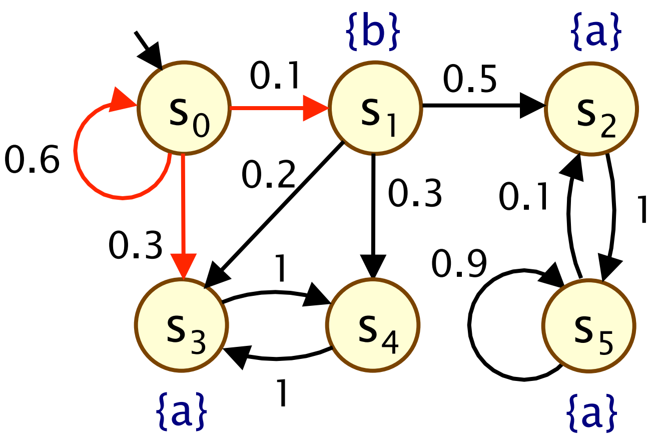


s_0 satisfies neither a or b
so we stay in q_0 in DRA A_ψ

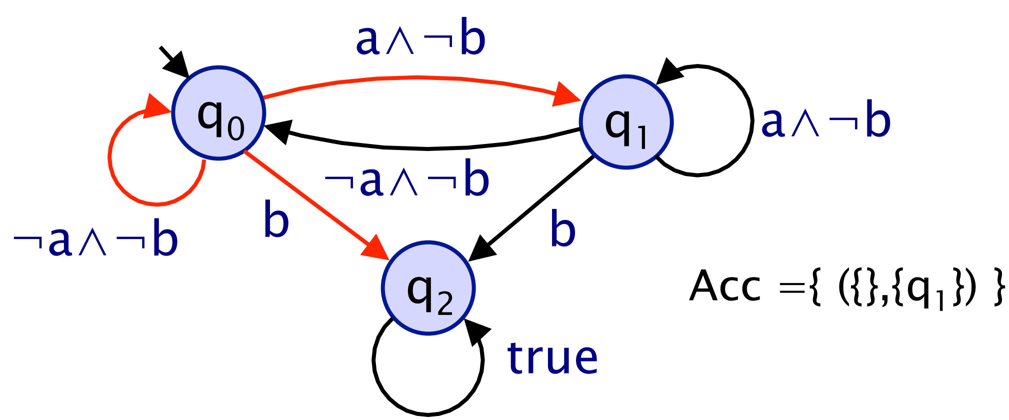
s_0 is initial
state of DTMC D

Example – Product DTMC

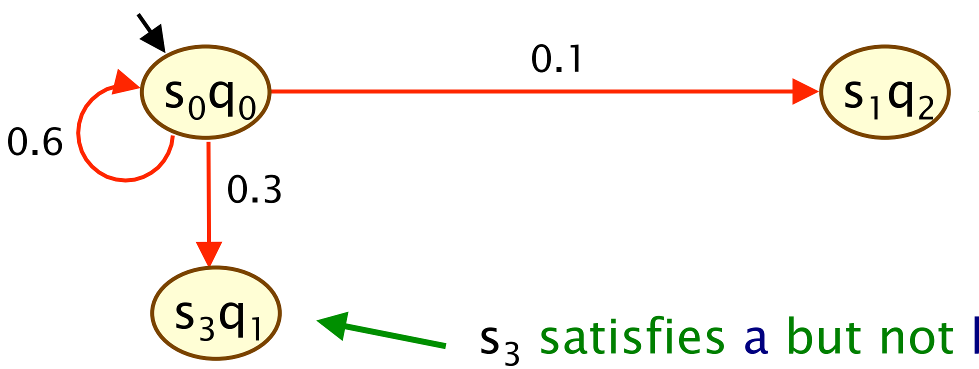
DTMC D



DRA A_ψ for $\psi = G\neg b \wedge GF\, a$



Product DTMC $D \otimes A_\psi$

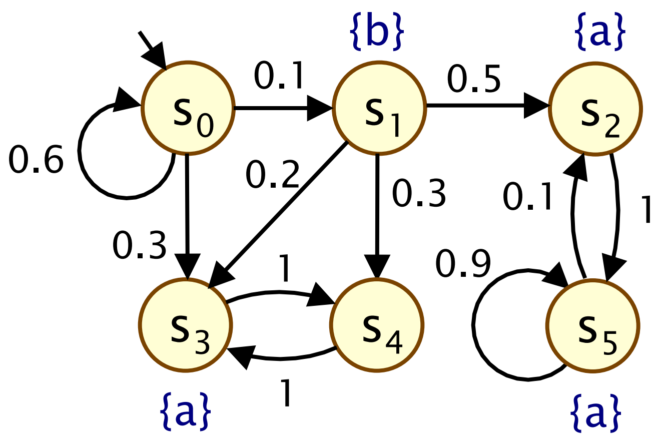


s_1 satisfies b so
we move to q_2 in A_ψ

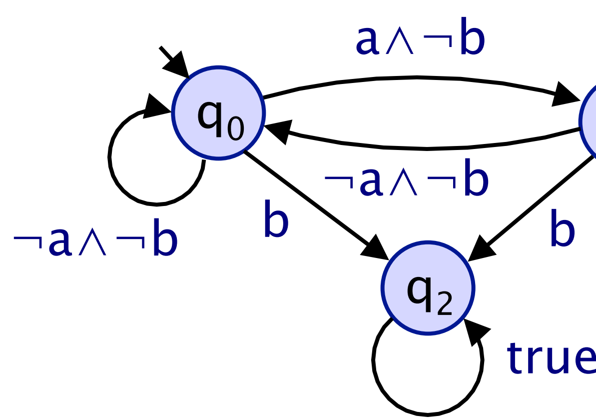
s_3 satisfies a but not b
so we move to q_1 in A_ψ

Example – Product DTMC

DTMC D



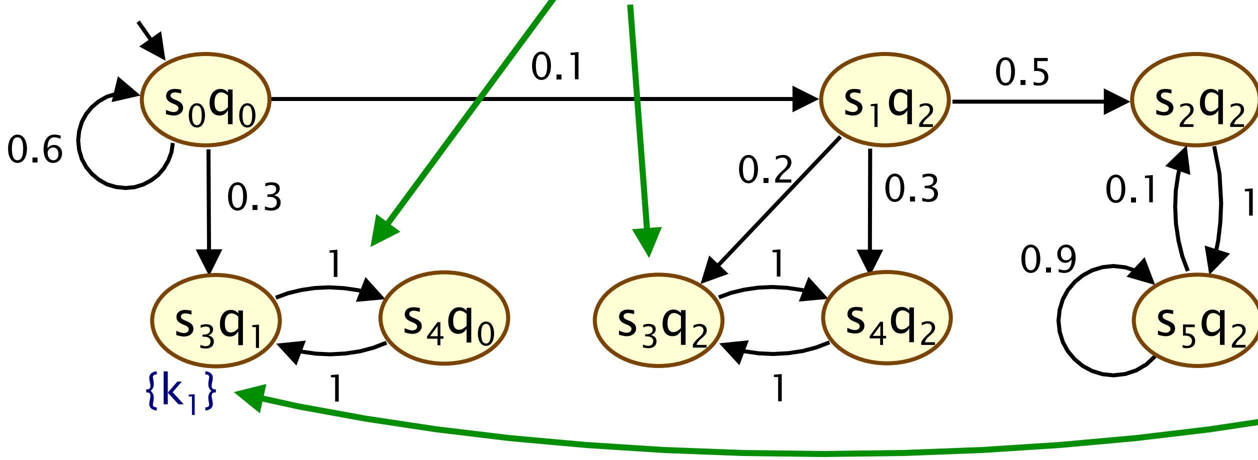
DRA A_ψ for $\psi = G\neg b \wedge GF\ a$



Acc $=\{ (\{\},\{q_1\}) \}$

Product DTMC $D \otimes A_\psi$

2 copies of s_3/s_4, one after seeing a b and one no b's



label states satisfying acceptance pair (L_1,K_1)

Product DTMC for a DRA

- For DTMC D and DRA A

$$\boxed{Pr_{D,s}(A) = Pr_{D \otimes A,(s,q_s)}(\vee_{1 \leq i \leq k} (FG \neg l_i \wedge GF k_i))}$$

  – where $q_s = \delta(q_{init}, L(s))$

- Hence:

$$\boxed{Pr_{D,s}(A) = Pr_{D \otimes A,(s,q_s)}(F\ T_{Acc})}$$

  – where T_{Acc} is the union of all accepting BSCCs in $D \otimes A$

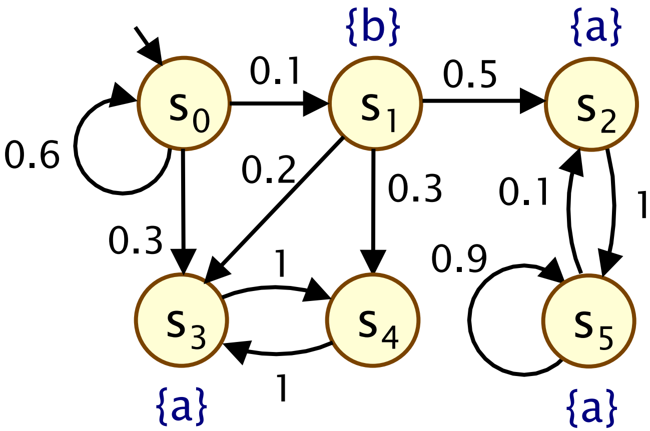
  – an accepting BSCC T of $D \otimes A$ is such that, for some $1 \leq i \leq k$, no states in T satisfy l_i and some state in T satisfies k_i

- Reduces to computing BSCCs and reachability probabilities

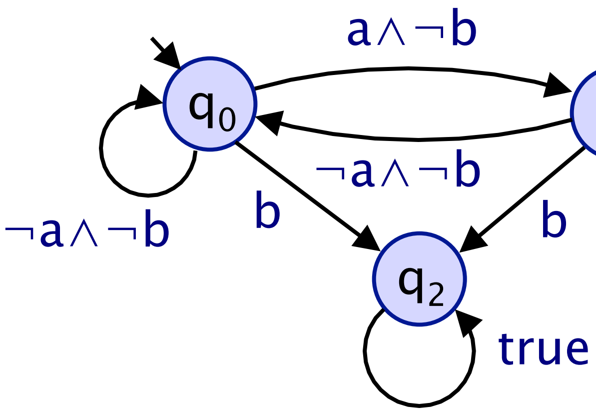
Example: LTL for DTMCs

- Compute $Pr_{D,s_0}(G\neg b \wedge GF\ a)$ for DTMC D:

DTMC D



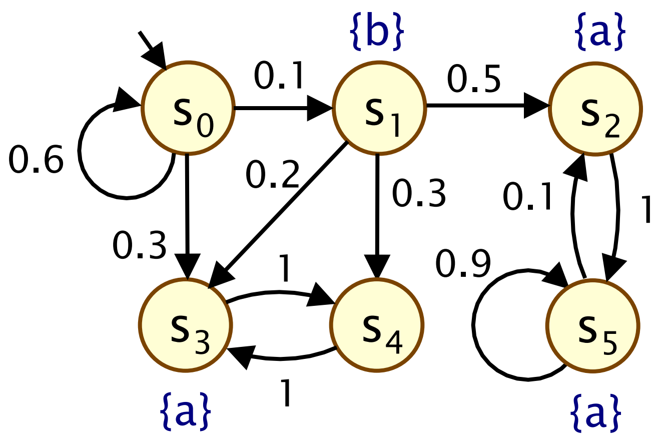
DRA A_ψ for $\psi = G\neg b \wedge GF\ a$



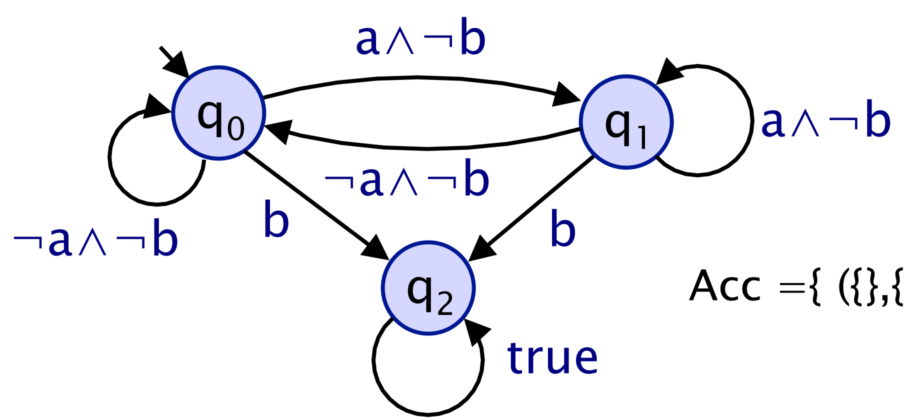
Acc ={ ({},{q_1}) }

Example: LTL for DTMCs

DTMC D

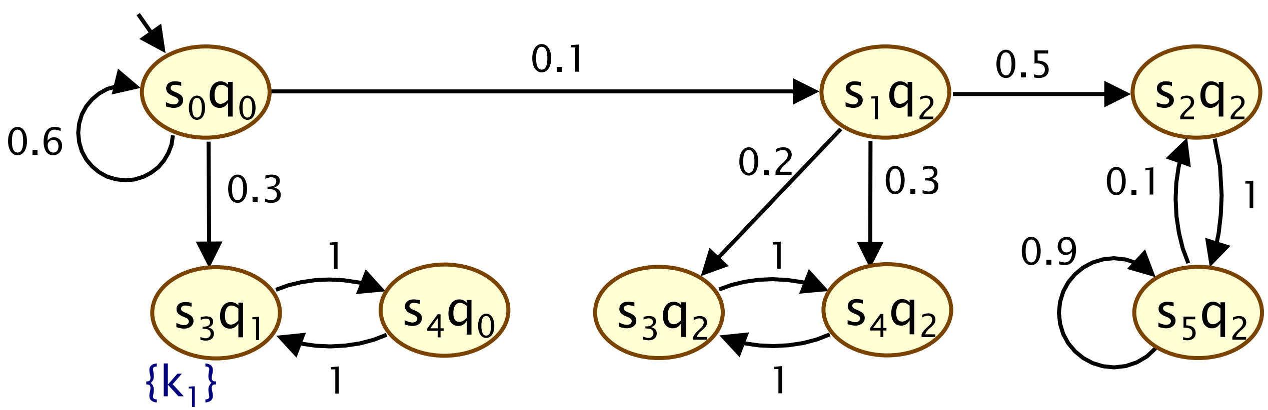


DRA A_ψ for $\psi = G\neg b \wedge GF\, a$



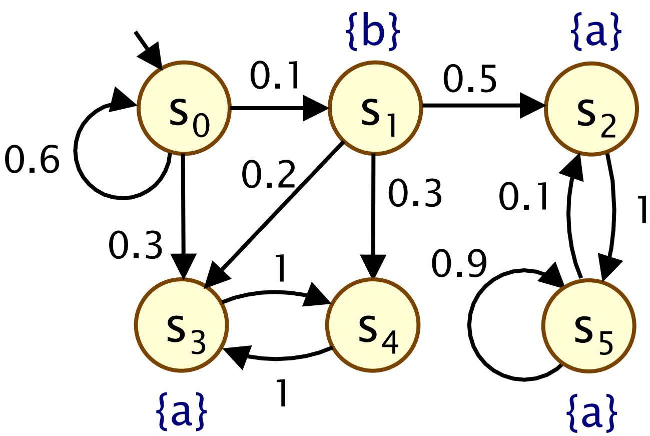
Acc $=\{\ (\{\},\{q_1\})\ \}$

Product DTMC $D \otimes A_\psi$

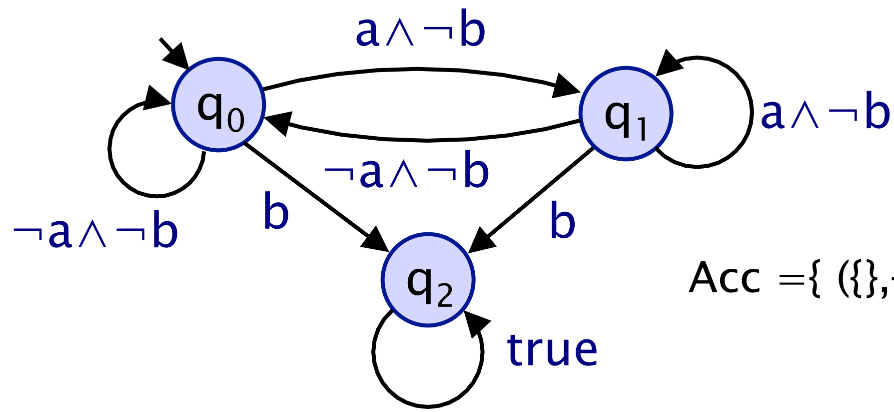


Example: LTL for DTMCs

DTMC D



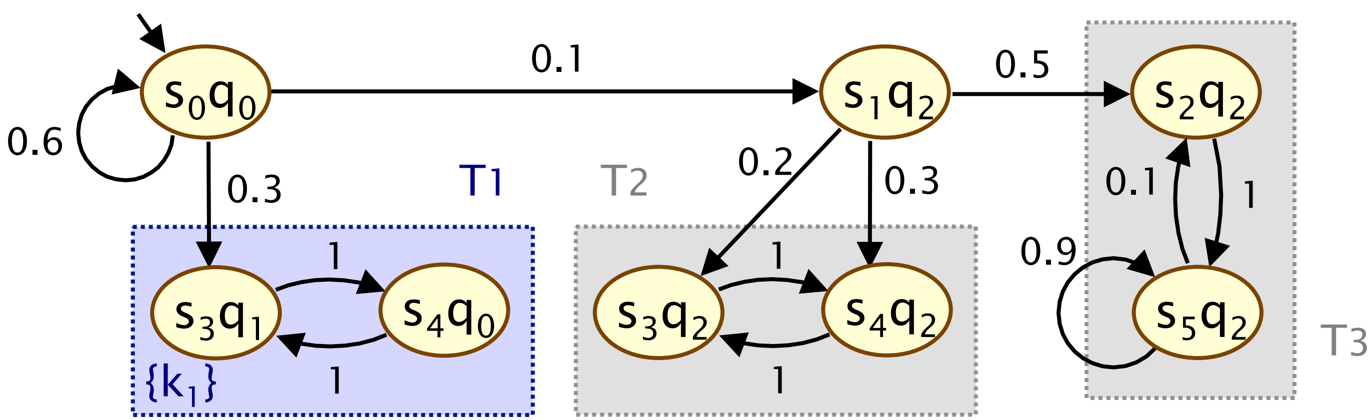
DRA A_ψ for $\psi = G\neg b \wedge GF\ a$



Acc $= \{ (\{\},\{q_1\}) \}$

Product DTMC $D \otimes A_\psi$

$Pr_{D,s_0}(\psi) = Pr_{D\otimes A_\psi,(s_0,q_0)}(F\ T_1) = 3/4$



Complexity of LTL model checking

- Complexity of model checking LTL formula ψ on DTMC D
  - is doubly exponential in |ψ| and polynomial in |D|
  - (for the algorithm presented in these lectures)
- Double exponential blow-up comes from use of DRAs
  - size of NBA can be exponential in |ψ|
  - and DRA can be exponentially bigger than NBA
  - in practice, this does not occur and ψ is small anyway
- Polynomial-time operations required on product model
  - BSCC computation – linear in (product) model size
  - probabilistic reachability – cubic in (product) model size
- In total: $O(poly(|D|,|A_\psi|))$

- Complexity can be reduced to single exponential in |ψ|
  - see e.g. [CY88,CY95]

PCTL* model checking

- PCTL* syntax:
  - ϕ ::= true | a | $\phi \wedge \phi$ | $\neg\phi$ | $P_{\sim p}$ [ψ]
  - ψ ::= ϕ | $\psi \wedge \psi$ | $\neg\psi$ | X ψ | ψ U ψ
- Example:
  - $P_{>p}$ [GF (send $\rightarrow$ $P_{>0}$ [F ack])]

- PCTL* model checking algorithm
  - bottom-up traversal of parse tree for formula (like PCTL)
  - to model check $P_{\sim p}$ [ψ]:
    - replace maximal state subformulae with atomic propositions
    - (state subformulae already model checked recursively)
    - modified formula ψ is now an LTL formula
    - which can be model checked as for LTL

Overview (Part 2)

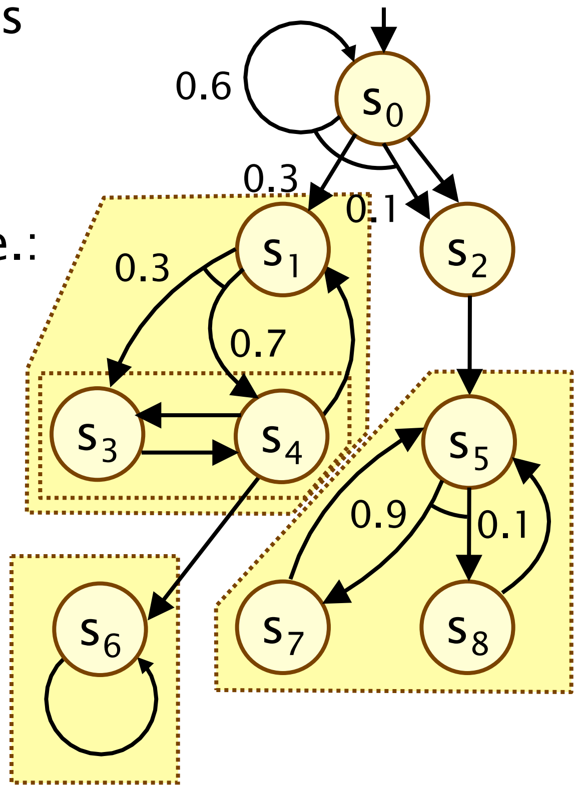
- Linear temporal logic (LTL) for DTMCS/MDPs
- Strongly connected components (DTMCs)
- ω-automata (Büchi, Rabin)
- LTL model checking for DTMCs
- LTL model checking for MDPs

End components

- Consider an MDP M = $(S,s_{init},\alpha_M,\delta_M,L)$

- A sub-MDP of M is a pair (T,δ_T) where:
  - $T \subseteq S$ is a (non-empty) subset of M's states
  - $\delta_T(s) \subseteq \delta(s)$ for each $s \in T$
- which:
  - is closed under probabilistic branching, i.e.:
  - $\{ s' \mid \mu(s')>0 \text{ for some } (a,\mu)\in\delta_T(s) \} \subseteq T$

- An end component of M is a strongly connected sub-MDP



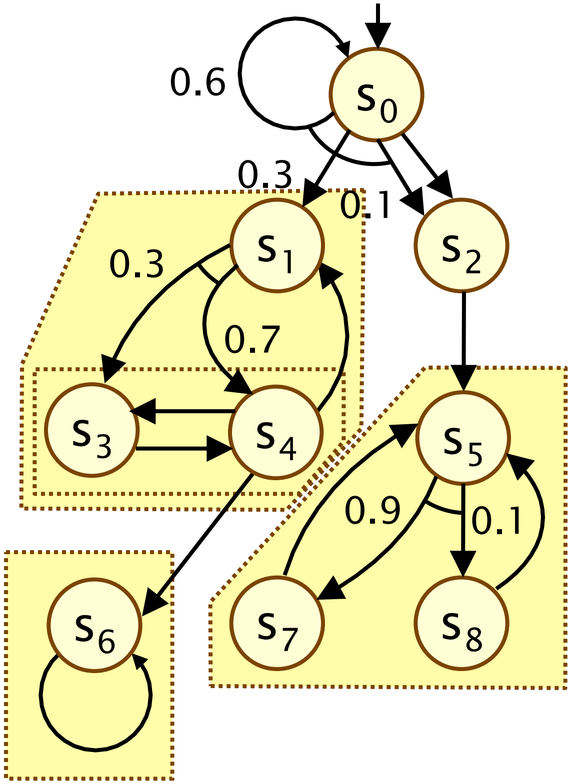
End components

- For finite MDPs…

- For every end component, there is an adversary which, with probability 1, forces the MDP to remain in the end component and visit all its states infinitely often

- Under every adversary A, with probability 1 an end component will be reached and all of its states visited infinitely often

  - (analogue of fundamental property of finite DTMCs)



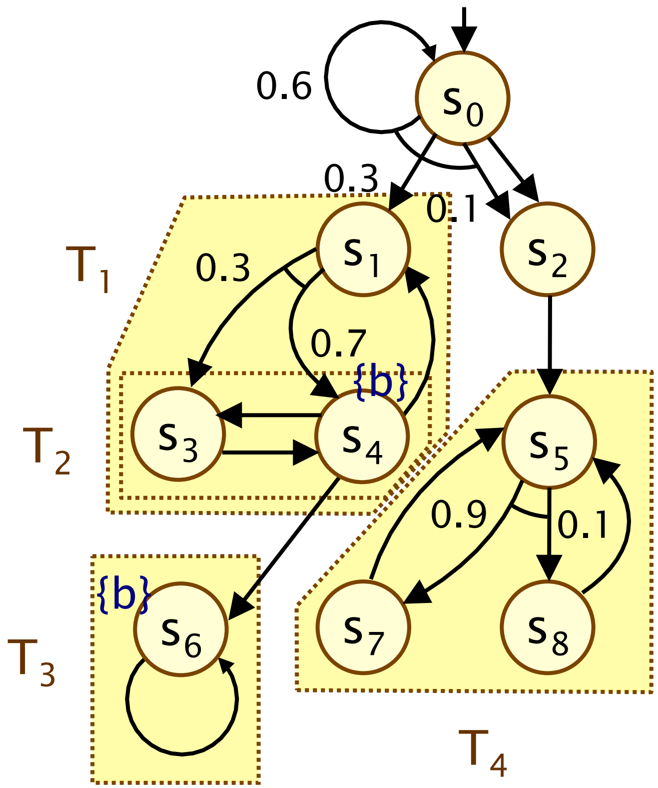
Long-run properties of MDPs

- Maximum probabilities
  - $Pr_s^{max}(GF\ a) = Pr_s^{max}(F\ T_{GFa})$
    - where T_{GFa} is the union of sets T for all end components (T,δ_T) with $T \cap Sat(a) \neq \varnothing$
  - $Pr_s^{max}(FG\ a) = Pr_s^{max}(F\ T_{FGa})$
    - where T_{FGa} is the union of sets T for all end components (T,δ_T) with $T \subseteq Sat(a)$
- Minimum probabilities
  - need to compute from maximum probabilities…
  - $Pr_s^{min}(GF\ a) = 1 - Pr_s^{max}(FG\neg a)$
  - $Pr_s^{min}(FG\ a) = 1 - Pr_s^{max}(GF\neg a)$

Example

- Model check: $P_{<0.8}$ [GF b] for s_0

- Compute $Pr_{s_0}^{max}(GF\ b)$
  - $Pr_{s_0}^{max}(GF\ b) = Pr_{s_0}^{max}(F\ T_{GFb})$
  - T_{GFb} is the union of sets T for all end components with $T \cap Sat(b) \neq \emptyset$
  - $Sat(b) = \{ s_4, s_6 \}$
  - $T_{GFb} = T_1 \cup T_2 \cup T_3 = \{ s_1, s_3\ s_4, s_6 \}$
  - $Pr_{s_0}^{max}(F\ T_{GFb}) = 0.75$
  - $Pr_{s_0}^{max}(GF\ b) = 0.75$



- Result: $s_0 \vDash P_{<0.8}$ [GF b]

Automata-based properties for MDPs

- For an MDP M and automaton A over alphabet 2^{AP}
  - consider probability of "satisfying" language $L(A) \subseteq (2^{AP})^\omega$
  - $Pr_{M,s}^{\sigma}(A) = Pr_{M,s}^{\sigma} \{ \omega \in Path_{M,s}^{\sigma} \mid trace(\omega) \in L(A) \}$
  - $Pr_{M,s}^{max}(A) = sup_{\sigma \in Adv}\ Pr_{M,s}^{\sigma}(A)$
  - $Pr_{M,s}^{min}(A) = inf_{\sigma \in Adv}\ Pr_{M,s}^{\sigma}(A)$

- Might need minimum or maximum probabilities
  - e.g. $s \vDash P_{\geq 0.99} [\ \psi_{good}\ ] \Leftrightarrow Pr_{M,s}^{min}(\psi_{good}) \geq 0.99$
  - e.g. $s \vDash P_{\leq 0.05} [\ \psi_{bad}\ ] \Leftrightarrow Pr_{M,s}^{max}(\psi_{bad}) \leq 0.05$
- But, ψ-regular properties are closed under negation
  - as are the automata that represent them
  - so can always consider maximum probabilities…
  - $Pr_{M,s}^{max}(\psi_{bad})$ or $1 - Pr_{M,s}^{max}(\neg\psi_{good})$

LTL model checking for MDPs

- Model check LTL specification $P_{\sim p}$ [ψ] against MDP M

- 1. Convert problem to one needing maximum probabilities
  - e.g. convert $P_{>p}$ [ψ] to $P_{<1-p}$ [¬ψ]
- 2. Generate a DRA for ψ (or ¬ψ)
  - build nondeterministic Büchi automaton (NBA) for ψ [VW94]
  - convert the NBA to a DRA [Saf88]
- 3. Construct product MDP M⊗A
- 4. Identify accepting end components (ECs) of M⊗A
- 5. Compute max. probability of reaching accepting ECs
  - from all states of the D⊗A
- 6. Compare probability for (s, q_s) against p for each s

Product MDP for a DRA

- For an MDP $M = (S, s_{init}, \alpha_M, \delta_M, L)$
- and a (total) DRA $A = (Q, q_{init}, \alpha_A, \delta_A, Acc)$
  - where $Acc = \{ (L_i, K_i) \mid 1 \leq i \leq k \}$

- The product MDP $M \otimes A$ is:
  - the MDP $(S \times Q, (s_{init}, q_{s_{init}}), \alpha_M, \delta_\otimes, L_\otimes)$ where:

    $q_{s_{init}} = \delta(q_{init}, L(s_{init}))$

    $\delta_\otimes(s,q) = \{ (a, \mu^q) \mid (a,\mu) \in \delta_M(s) \}$

    $$\mu^q(s',q') = \begin{cases} \mu(s') & \text{if } q' = \delta_A(q, L(s)) \\ 0 & \text{otherwise} \end{cases}$$

    $l_i \in L_\otimes(s,q)$ if $q \in L_i$ and $k_i \in L_\otimes(s,q)$ if $q \in K_i$

    (i.e. state sets of acceptance condition used as labels)

Product MDP for a DRA

- For MDP M and DRA A

$$\boxed{Pr_{M,s}^{max}(A) = Pr_{M\otimes A,(s,q_s)}^{max}(\vee_{1\leq i\leq k} (FG\ \neg l_i \wedge GF\ k_i))}$$

  – where $q_s = \delta_A(q_{init},L(s))$

- Hence:

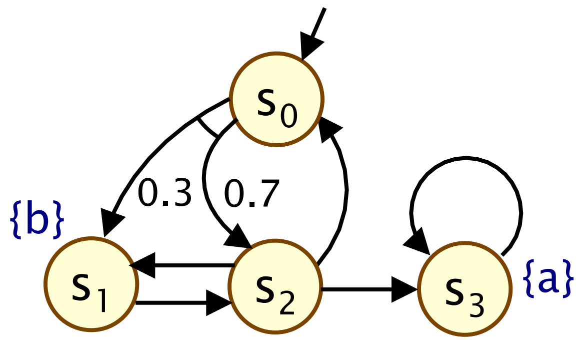
$$\boxed{Pr_{M,s}^{max}(A) = Pr_{M\otimes A,(s,q_s)}^{max}(F\ T_{Acc})}$$

  – where T_{Acc} is the union of all sets T for accepting end components (T,δ_T) in $D\otimes A$
  – an accepting end components is such that, for some $1\leq i\leq k$:
    - $(s,q) \vDash \neg l_i$ for all $(s,q) \in T$ and $(s,q) \vDash k_i$ for some $(s,q) \in T$
    - i.e. $T \cap (S \times L_i) = \varnothing$ and $T \cap (S \times K_i) \neq \varnothing$

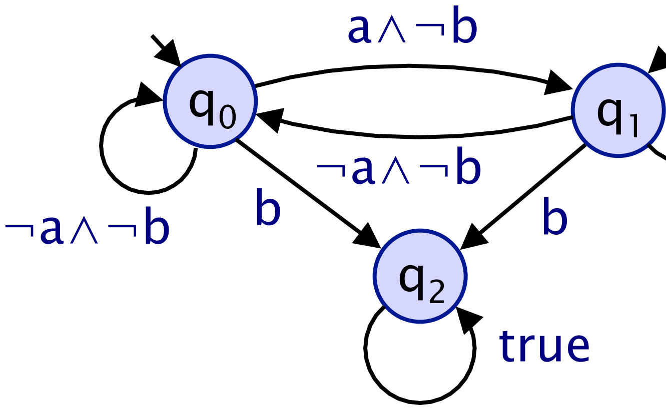
Example: LTL for MDPs

- Model check $P_{<0.8}$ [G ¬b ∧ GF a] for state s_0 in MDP M:
  - need to compute $Pr_{M,s_0}{}^{max}(G\ \neg b \wedge GF\ a)$

MDP M



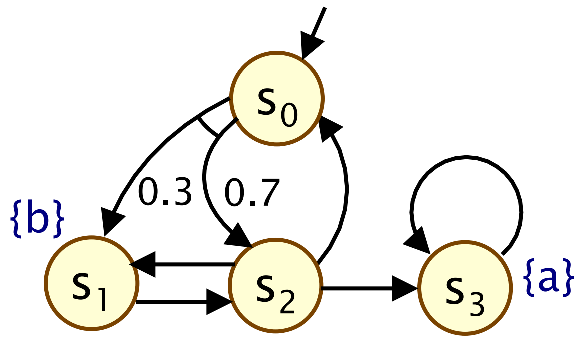
DRA A_ψ for ψ = G¬b ∧ GF a



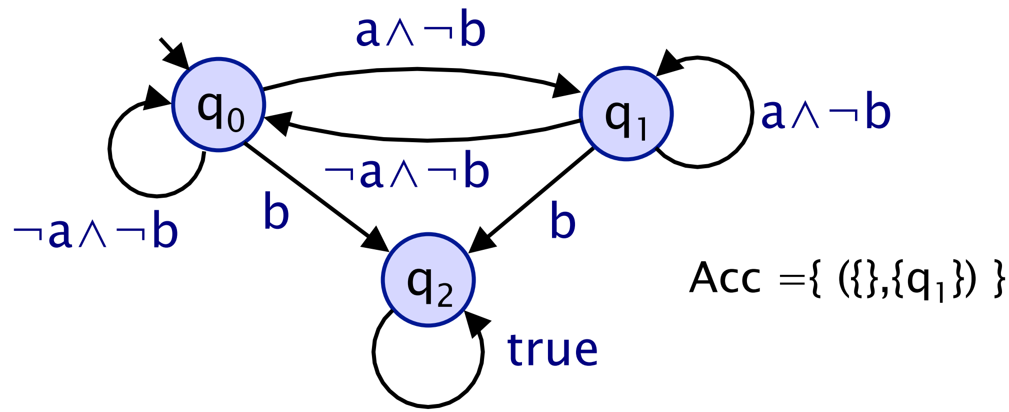
Acc ={ ({},{q_1}) }

Example: LTL for MDPs

MDP M

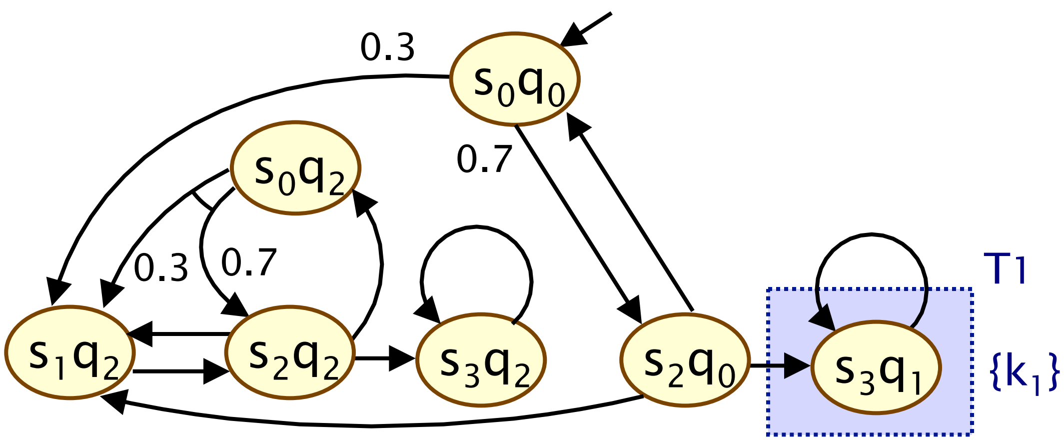


DRA A_ψ for $\psi = G\neg b \wedge GF\ a$



Product MDP $M \otimes A_\psi$

$Pr_{M,s_0}^{max}(\psi) = Pr_{M \otimes A_\psi,(s_0,q_0)}^{max}(F\ T_1) = 0.7$



LTL model checking for MDPs

- Complexity of model checking LTL formula ψ on MDP M
  - is doubly exponential in |ψ| and polynomial in |M|
  - unlike DTMCs, this cannot be improved upon
- PCTL* model checking
  - LTL model checking can be adapted to PCTL*, as for DTMCs
- Maximal end components
  - can optimise LTL model checking using maximal end components (there may be exponentially many ECs)
- Optimal adversaries for LTL formulae
  - e.g. memoryless adversary always exists for $Pr_{M,s}^{max}(GF\ a)$, but not for $Pr_{M,s}^{max}(FG\ a)$

Summary (Part 2)

- Linear temporal logic (LTL)
  - combines path operators; PCTL* subsumes LTL and PCTL
- ω-automata: represent ω-regular languages/properties
  - can translate any LTL formula into a Büchi automaton
  - for deterministic ω-automata, we use Rabin automata
- Long-run properties of DTMCs
  - need bottom strongly connected components (BSCCs)
- LTL model checking for DTMCs
  - construct product of DTMC and Rabin automaton
  - identify accepting BSCCs, compute reachability probability
- LTL model checking for MDPs
  - MDP-DRA product, reachability of accepting end components

- Next: Compositional probabilistic verification