Game-based abstraction of Markov decision processes

Marta Kwiatkowska
Gethin Norman
Dave Parker

University of Birmingham

QEST'06

Overview

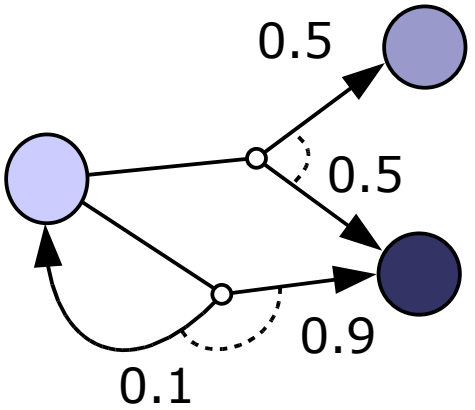
- Markov decision processes (MDPs)
- Simple stochastic games (SSGs)
- Abstraction of MDPs using SSGs
- Case study: Zeroconf protocol

Markov decision processes (MDPs)

- Model both probabilistic and nondeterministic choice
  - concurrency: parallel composition of stochastic components

    e.g. communication protocols, randomised algorithms, ...
  - unknown environment: e.g. probabilistic security protocols

- MDP M = (S,Steps) where:
  - set of states S
  - Steps : $S \rightarrow 2^{Dist(S)}$
    mapping from states to sets of probability distributions



Probabilistic verification of MDPs

- Formal analysis of quantitative properties of MDPs
  - probabilistic extensions of temporal logic, e.g. PCTL
- Adversaries (also known as schedulers, policies)
  - adversary A = resolution of all nondeterminism in MDP
  - A is a mapping from finite paths to probability distributions
- Probabilistic reachability (for a set of goal states F)
  - $p_A(F)$ = probability of reaching states F under adversary A
  - minimum/maximum probabilities over all adversaries
    - $pmin(F) = inf_A\ p_A(F)$
    - $pmax(F) = sup_A\ p_A(F)$

Probabilistic verification of MDPs...

- Analysis of best/worst-case scenarios for MDP:
  - "maximum probability of an error occurring"
  - "minimum probability of termination within T seconds"
  - "maximum expected time for completion"
  - "minimum expected number of rounds required"
- Probabilistic model checking algorithms
  - solution of linear optimisation problems
  - iterative numerical methods (dynamic programming)
  - efficient symbolic implementations, tools (e.g. PRISM)
  - but... state space explosion still a major issue

Abstraction

- Very successful in (non-probabilistic) model checking
- Construct abstract model M' of concrete model M
  - details not relevant to property of interest removed
  - merge states according to a given partition of state space
  - e.g. from set of predicates (predicate abstraction)
- Counterexample guided abstraction and refinement
  - conservative: satisfaction in M' implies satisfaction in M
  - converse does not hold, but...
  - information from model checking process (counterexample) can be used to refine the abstraction

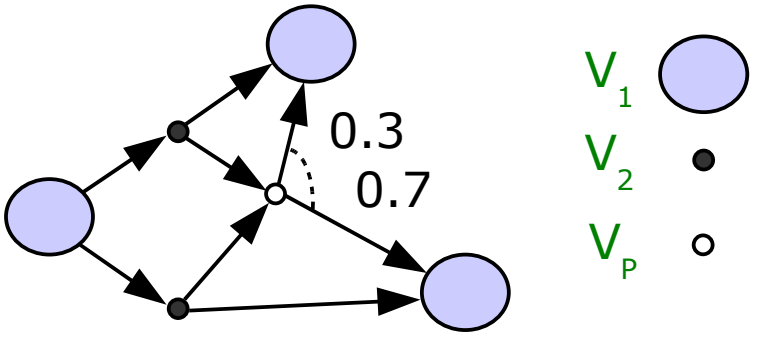
Abstraction of MDPs

- Abstraction increases degree of nondeterminism
  - minimum probability will be lower, and maximum higher
- Key idea: separate two forms of nondeterminism
  - (a) from abstraction and (b) from original MDP
- Generate separate lower/upper bounds for min/max

- Gives quantitative measure of utility of abstraction
  - if lower/upper bounds not close enough...
  - refine abstraction and repeat

Simple stochastic games (SSGs)

- Simple stochastic two-player games [Condon]
- Game G = ((V,E), v_{init}, (V_1,V_2,V_P), δ)
  - (V,E) is a finite directed graph
  - v_{init} is the initial vertex
  - (V_1,V_2,V_P) is a partition of V:
    'player 1', 'player 2', 'probabilistic'
  - δ : $V_P \rightarrow$ Dist(V) is a probabilistic transition function



- Execution of G: successor in each vertex chosen...
  - by player 1/2 for V_1/V_2 vertices
  - at random (δ) for V_P vertices

Analysis of SSGs

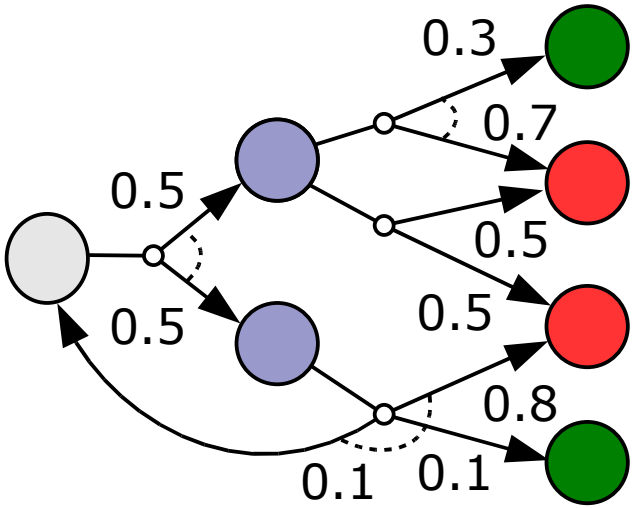
- Probabilistic reachability of vertex goal set F
  - strategies a1, a2 are resolutions of choices for players 1, 2
  - $p_{a1,a2}(F)$ = probability of reaching F under strategies a1, a2
  - optimal probabilities for player 1 and player 2:
  - $\sup_{a1} \inf_{a2} p_{a1,a2}(F)$ and $\sup_{a2} \inf_{a1} p_{a1,a2}(F)$
  - computable via simple iterative methods, similar to MDPs

Abstract MDP

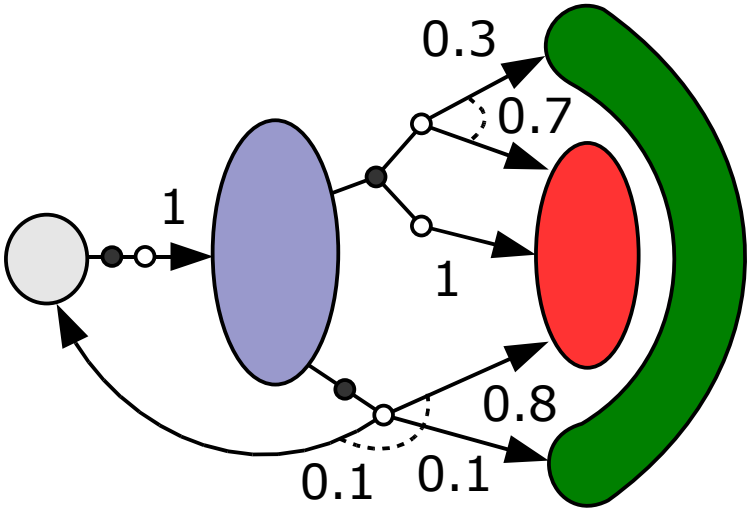
- Abstract MDP is a simple stochastic game
  - based on a partition P of MDP state space S
  - V_1 states are elements of P (subsets of S)
  - V_2 states are sets of prob. distributions ("states of MDP")
  - V_P states are single probability distributions (now over V_1)
  - strict alternation between V_1, V_2, V_P vertices
- Player 1 controls nondeterminism from abstraction
  - selects a state of the original MDP from a subset of S (in P)
- Player 2 controls nondeterminism from original MDP
  - selects a single probability distribution from a set

Simple example

Original MDP



Abstract MDP
(simple stochastic game)



Analysis of abstract MDP

- For set of goal states/vertices F in MDP/SSG...
- Compute lower/upper bounds for pmin(F), pmax(F) on MDP using abstract MDP (SSG):

$$\inf_{a1,a2} p_{a1,a2}(F) \leq \text{pmin}(F) \leq \sup_{a1} \inf_{a2} p_{a1,a2}(F)$$

$$\sup_{a2} \inf_{a1} p_{a1,a2}(F) \leq \text{pmax}(F) \leq \sup_{a1,a2} p_{a1,a2}(F)$$

Analysis of abstract MDP

- For set of goal states/vertices F in MDP/SSG...
- Compute lower/upper bounds for pmin(F), pmax(F) on MDP using abstract MDP (SSG):

$$\inf_{a1,a2} p_{a1,a2}(F) \leq \text{pmin}(F) \leq \sup_{a1} \inf_{a2} p_{a1,a2}(F)$$

$$\sup_{a2} \inf_{a1} p_{a1,a2}(F) \leq \text{pmax}(F) \leq \sup_{a1,a2} p_{a1,a2}(F)$$

min/max reachability probabilities for original MDP

Analysis of abstract MDP

- For set of goal states/vertices F in MDP/SSG...
- Compute lower/upper bounds for pmin(F), pmax(F) on MDP using abstract MDP (SSG):

$$\inf_{a1,a2} p_{a1,a2}(F) \leq \text{pmin}(F) \leq \sup_{a1} \inf_{a2} p_{a1,a2}(F)$$

$$\sup_{a2} \inf_{a1} p_{a1,a2}(F) \leq \text{pmax}(F) \leq \sup_{a1,a2} p_{a1,a2}(F)$$

optimal probabilities for player 1, player 2 in abstract MDP

Analysis of abstract MDP

- For set of goal states/vertices F in MDP/SSG...
- Compute lower/upper bounds for pmin(F), pmax(F) on MDP using abstract MDP (SSG):

$$\inf_{a1,a2} p_{a1,a2}(F) \leq \text{pmin}(F) \leq \sup_{a1} \inf_{a2} p_{a1,a2}(F)$$

$$\sup_{a2} \inf_{a1} p_{a1,a2}(F) \leq \text{pmax}(F) \leq \sup_{a1,a2} p_{a1,a2}(F)$$

equivalent to normal analysis of min/max probs for MDP

(but performed on abstract MDP)

Implementation

- Prototype implementation in Java
  - construction of SSGs (abstract MDPs)
  - iterative numerical analysis of SSGs
- Based on reduction of full original MDP
  - constructed and exported in PRISM

Case study: Zeroconf protocol

- Decentralised self configuration of local IP addresses
  - new node joining network of N existing nodes, M addresses
  - probabilistic: based on random selection of IP address
  - nondeterministic: concurrency from scheduling, unknown message propagation delays (different range for each node)
- Abstraction
  - abstract M IP addresses to 2 values: in-use/fresh
  - abstract messages: just store type of message, not sender
  - consequently, we lose information about message timings
  - provided by user in terms of PRISM model variables
  - see paper for more details

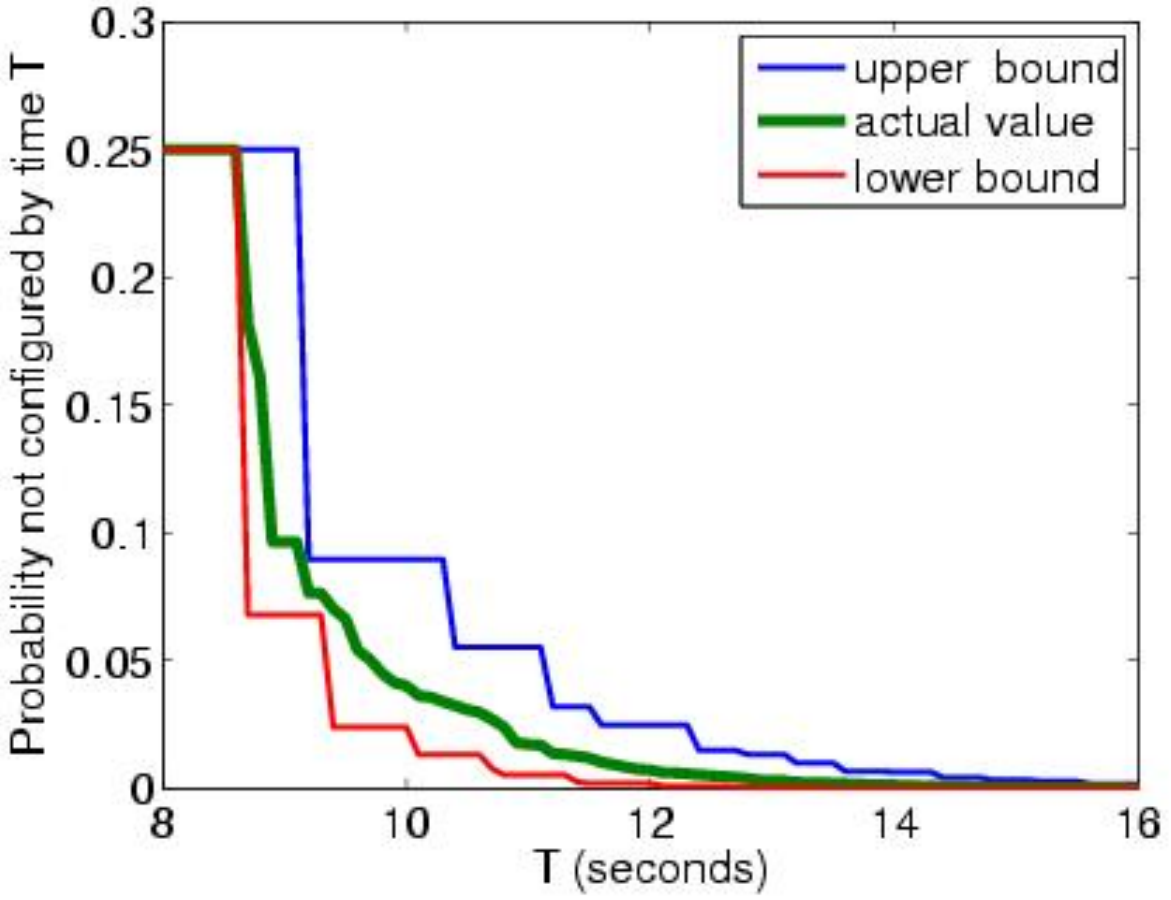
Results

- Substantial reduction in model size (MDP vs. SSG)

N	States		Transitions	
	MDP	Abs	MDP	Abs
4	26,121	737	50,624	1,594
5	58,497	785	139,104	1,678
6	145,801	833	432,944	1,762
7	220,513	857	614,976	1,806
8	432,185	881	1,254,480	1,850

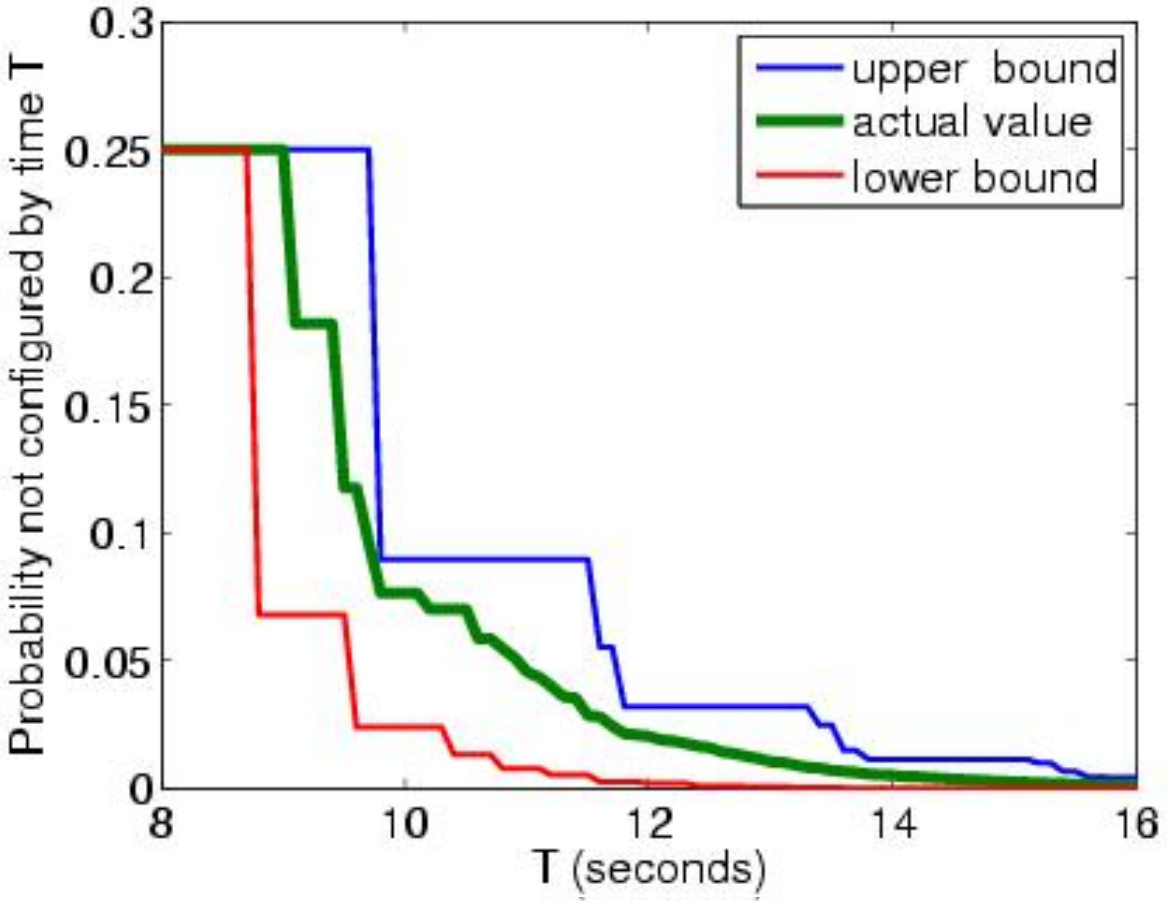
Results

- Minimum probability not configured by time T:



Results

- Maximum probability not configured by time T:



Conclusions

- Novel abstraction approach for MDPs using SSGs
  - separation of nondeterminism from MDP/abstraction
  - both lower/upper bounds for min/max probabilities
  - quantitative measure of utility of abstraction
  - promising results: model reduction, quantitative results
- Future work
  - perform abstraction at PRISM language level (not on MDP)
  - efficient symbolic implementation of SSG algorithms
  - automatic/semi-automatic generation of partitions
  - more case studies, comparison with related work