Analysis of Software Artifacts

Probabilistic Systems (Lecture 21)
MIBDDs

Probabilistic Verus and Symbolic Model Checking with

Model Checking for PCTL

Probabilistic CTL

Markov chains: notions and analysis
Probabilistic Systems

Examples: manufacturing systems, controllers, environments, etc.

Stochastic systems: events occur with certain probabilities.
Properties of interest

• Probability of reaching a state after a given time

• Reliability

• Average lifetime

• Mean time to failure

• Steady-state probability
Stochastic Processes

A stochastic process is a collection of random variables indexed by time, $\mathcal{F}$, where $I = (\infty+) \cup I = (\infty-) \cup I = (x) \cup \mathcal{F}$.

Continuous random variable: cumulative distribution function

$$[x > X]d = (x) \cup \mathcal{F}$$

Discrete random variable: probability mass function

$$[x = X]d = (x) \cup \mathcal{F}$$
\[ \gamma x = (\gamma \mu) X | \gamma x = (1 + \gamma \mu) X \]_{d} = [0 = (0 \mu) X \cdots ; \gamma x = (1 + \gamma \mu) X]_{d} \\

For discrete state space: Markov chain:

\[ \gamma x = (\gamma \mu) X | \gamma x \geq (1 + \gamma \mu) X \]_{d} = [0 = (0 \mu) X \cdots ; \gamma x = (1 + \gamma \mu) X]_{d}

independent of past, future probabilistically determined by present, property:

future process iff is has the memoryless property:

\[ \{(\mu) X\} \]

\[ (\mathbb{R} = \mathcal{L}) \]

discrete-time process or continuous-time process

Stochastic and Markov Processes
\[
\begin{align*}
\text{(Chapman-Kolmogorov equation)} \\
\sum_{n} (u + \gamma)(u + \gamma, n) \mathcal{P}(n, \gamma) \mathcal{P}(\gamma, u) \mathcal{P}(u, \gamma) = (u + \gamma, \gamma) \mathcal{P}(\gamma, u) \\
\cdot \mathbb{P}[\gamma = \gamma \, X | \cdot = u + \gamma \, X] I = (u + \gamma, \gamma) \mathcal{P}(\gamma, u) \\
\text{n-step transition probability:} \\
\mathbb{P}[\gamma = \gamma \, X | \cdot = \cdot + \gamma \, X] I = (\gamma) \mathcal{P}(\gamma, u) \\
\text{Define: state space:} \\
\text{Consider: discrete-time Markov chain with integers as state space:} \\
\end{align*}
\]
All rows sum up to 1: stochastic matrix.

\[ p \cdot d \] = \text{Define transition probability matrix} \ L \sim \ \text{Homogeneous Markov chain if } p \cdot d \ (y) \ \text{independent of } k \]

\[ \Rightarrow \text{Transition Probabilities} \]
occurs at time of call completion
• process call arrival if it
• if phone busy, call is lost
  \( \mathcal{G} \) calls complete with probability \( \mathcal{G} \) 
  \( \mathcal{G} \) at most one call in one slot, probability \( \mathcal{G} \) 
Telephone call process with discrete time slots:

Example: A Simple Markov Chain
State transition diagram

\[ g' \sigma + (g' - 1) \]

\[ 1 \quad 0 \]

\[ (\sigma - 1) g' \]

\[ \sigma - 1 \]
Classification of states:

- Reachable from any other
- Irreducible closed set if any state
  \[ I = \pi_d \iff \text{state is absorbing} \]
- State set $S' \not\ni \exists S \ni \exists \omega A^0 = \pi_d \iff \text{closed set} \]
- State $\not\ni$ reachable from if $\exists \pi_d < (\forall \gamma)(\exists \gamma)$ for some $\gamma$

Analyzing Markov Chains
Analyzing Markov Chains

- With these notions, can analyze steady-state behavior

  - Positive recurrent state: periodic or aperiodic

    - $\infty > \infty$ > mean recurrence time

      - Transient state is not recurrent

      - Recurrent state is probability of returning to it is 1

Analyzing Markov Chains
Steady-State Analysis

The initial state probability vector $\pi$ always exists and is independent of the initial state. Let $\pi^\infty$ be the unique solution to the equation $\pi = \pi P$.

Theorem: In an irreducible aperiodic Markov chain, the limiting distribution $\pi^\infty$ exists.

Question: Does $\lim_{n \to \infty} \pi^n$ exist?

$[\cdots, (\pi)_{n-1}, (\pi)_{n}, (\pi)_{n+1}] = (\pi)_{n+1}$

State probability vector $\pi$ exists.

$[c = \pi^\infty X]d = (\pi)^c$ state probability vector $\pi$.
\[ I = (s', s) \models L \models_{s \models} \exists \models_{s \models} \]  

transition relation with \([I, 0] \leftarrow S \times S \models L \models \]  

initial state \(i \]  

finite state space \(S \models \]  

where: \(\eta, \eta' \models L \models_0 S, S \models \) 

Computation model: Labelled Markov chain

Temporal Logic Analysing Computation Model
Temporal Logic Analysis: Computation Model

Traces \( \Rightarrow \) induces probability measure on set of execution (propositions)

\( \text{Labeling function} = \mathcal{d}(A) \) set of atomic

\( \mathcal{d}(A) \) \( \leftarrow \) \( S : n \) •

Temporal Logic Analysis: Computation Model
Probabilistic CTL

\[ \exists_f s \implies \forall_f s \mid \exists_f s \implies \forall_f s =:: fd \]
\[ d^<[fd] \mid d^<[fd] \mid \exists_f s \lor \forall_f s \mid f s \rightarrow \mid do_f d =:: fs \]

Syntax: State formulas and path formulas \( fs \) and \( f s \).

[Hansson and Jonsson, RTSS89]
Probabilistic CTL

$d$ exceeds $f_d$ by the measure of paths that satisfy $d<[fd] \models s$.

$\begin{align*}
1fs &\models [\ell] \diamond [\ell',0] \in \ell A \\
\text{or} & \\
\neg fs \cap \bigwedge fs &\models \diamond \bigwedge fs \models \bigwedge fs = \models \diamond \bullet \\
\text{and} & \\
\neg fs &\models [\ell] \diamond \ell' \geq \exists \in \bigwedge fs \models \bigwedge fs = \models \diamond \bullet
\end{align*}$
Properties in PCTL

- Probability of an alarm occurring at least $d$ times

- There is no failure for $\tau$ time units with probability at least $d$

- Becomes true in $\tau$ units and that $\neg \text{reg}$ stays true until $\text{ack}$

- An $\text{ack}$ within $\tau$ units and that $\neg \text{reg}$ stays true until $\text{ack}$

- There is probability at least $d$ that there is

Examples:

$$fs^{d-\tau}_\geq \neg P = fs^{\geq d}_\geq \neg C$$

$$fs^{\geq d}_\geq \bigcup \neg \text{reg} \text{true} = fs^{\geq d}_\geq \neg P$$
within time $t$
/* Recursive */

*/

*/

/* Direct */

*/

*/

/* Inductively */

Probability of a path from state $s$ satisfying $s I f \cup f ^ I f$ defined

---

Model Checking for PCTL: Until Operator
Model Checking

- compute vector $\overline{p}(s, t) = P^t \overline{p}(s, 0)$
- $M = f_1 \cup f_2$ iff $\overline{p}(s^0, t) \geq p$
- \[ P[s, s] = 0 \text{ otherwise} \]
- $P[s, s] = 1$ if $s_k = f_1 \land s_k \models f_2$ (same)
- $P[s, s] = \overline{f_2}$ (recursive case)
- $P[s, s] = \overline{T[s, s]}$ if $s_k \models f_1 \land s_k \models \overline{f_2}$
- build transition probability matrix $P$ from $T$ as follows:

```plaintext
Model Checking
```
fully symbolic efficient representation and algorithms

multi-terminal (multi-terminal BDDs)

implemented symbolically using MIBDDs

matrix

compilation of programs yields probabilistic transition

\[ I = \sum_{d \in \mathbb{D}} \bigwedge_I \]

with \( p \in \{ 0, 1 \} \), \( I \)

select (select)

Introduce probabilistic selection statement:

[Harroons-Garmhausen, Campos, Clarke 1998]

Probabilistic Verus
representation

- If matrix is sparse or presents regularity compact
- Terminal values are matrix elements
- Column indices
- Matrix representation: BDD variables are row and
- Matrix representation: BDD variables are row and
- (from a finite set) in the terminal nodes
- Values
- MTBDDs are binary decision diagrams with arbitrary

Multi-Terminal BDDs
Multi-Terminal BDDs

apply operator

matrix operation implemented recursively using BDD

Multi-Terminal BDDs
Practical Results with ProbVersus

- Reaching unsafe states
- Safety, liveliness, response times, probabilities of
- Stations
- Largest example: a safety-critical system for railway
- Control
- Also transportation; fault-tolerant industrial process
- Probabilities
- Manufacturing systems: very downtime

Practical Results with ProbVersus
Practical Results with ProbVersus

counterexample trace

deadlock discovered and located throughout

specification

complexity: 10^{27} states; about 5 minutes per