Probabilistic Plan Verification through Acceptance Sampling

Håkan L. S. Younes  David J. Musliner
Carnegie Mellon University  Honeywell Laboratories
Introduction

- Probabilistic extension to CIRCA
- Efficient plan verification algorithm
  - Monte Carlo simulation
  - Acceptance sampling
- Guaranteed error bounds
Planning via Model Checking

Planner

Model checker

objectives, environment

candidate plan

verification result

safety constraints
World Model

- States...

- normal path no threat
- evasive path no threat
- evasive path radar threat
- normal path radar threat
- FAILURE
World Model

- States + events = environment

Diagram:
- Normal path
  - No threat
  - Radar threat
- Evasive path
  - No threat
- Failure
  - Hit: Exp(50) + 120
  - Exp(150)

U(50,100)
A plan maps states to actions

- World Model
  - A plan maps states to actions

- Diagram showing transitions between states:
  - Normal path (no threat) to evasive path (radar threat) to failure
  - Evasive path (no threat) to normal path (radar threat)
  - Normal path (radar threat) to failure

- Probabilities and actions:
  - End evasive path: U(25,50)
  - Safe: U(50,100)
  - Begin evasive path: U(25,50)
  - Hit: Exp(50) + 120
  - Radar threat: Exp(150)
Sample Execution Paths

radar threat  begin evasive  safe  end evasive

normal path  no threat  normal path  radar threat  evasive path  radar threat  evasive path  no threat  normal path  no threat

41.9  45.8  93.5  43.4  ...

radar threat  begin evasive  hit

normal path  no threat  normal path  radar threat  evasive path  radar threat  FAILURE

44.1  48.7  92.2
Plan Safety

- Two parameters
  - Failure probability threshold: $\theta$
  - Maximum execution time: $t_{\text{max}}$

- A plan is safe if the probability of reaching a failure state within $t_{\text{max}}$ time units is at most $\theta$
Safety Over Sample Execution

Paths

Given $t_{\text{max}} = 200$:

- normal path
- radar threat
- begin evasive
- safe
- end evasive
- normal path
- no threat

41.9 + 45.8 + 93.5 + 43.4 > 200 ...

Safe!
Safety Over Sample Execution Paths

- Given $t_{\text{max}} = 200$:

```
radar threat  begin evasive  hit
normal path no threat  +  44.1  48.7  +  92.2  ≤ 200
normal path radar threat
(evasive path radar threat
FAILURE

Not safe!
(safe if $t_{\text{max}} < 185$)
Verifying Plan Safety

- **Symbolic Methods**
  - **Pro:** Exact solution
  - **Con:** Works only for **restricted** class of models

- **Sampling**
  - **Pro:** Works for **any** model that can be simulated
  - **Con:** Uncertainty in correctness of solution
Our Approach

- Use simulation to generate sample execution paths
- Use sequential acceptance sampling to verify plan safety
Error Bounds

- Probability of false negative: $\leq \alpha$
  - We say that a plan is not safe when it is

- Probability of false positive: $\leq \beta$
  - We say that a plan is safe when it is not
Acceptance Sampling

- Test hypothesis $\Pr_{\leq \theta}(X)$
- In our case
  - $\theta$ is the failure probability threshold
  - $X$ is the proposition that a failure state is reached within the time limit
Sequential Acceptance Sampling

- Test hypothesis $\Pr_{\leq \theta}(X)$
Performance of Test

\[ \Pr_{\leq \theta}(X) \text{ as true} \]

\[ 1 - \alpha \]

\[ \beta \]

\[ \theta \]

Actual failure probability of plan
Ideal Performance

Actual failure probability of plan

Probability of accepting $Pr_{\leq \theta}(X)$ as true

$1 - \alpha$

$\beta$

False positives

False negatives
Actual Performance

Actual failure probability of plan

\[ \Pr_{\leq \theta}(X) \text{ as true} \]

1 - \( \alpha \)

\( \beta \)

Actual failure probability of plan

\[ \theta - \delta \quad \theta \quad \theta + \delta \]

False negatives

Indifference region

False positives
Graphical Representation of Sequential Test

Number of negative samples

Number of samples
Graphical Representation of Sequential Test

- We can find an acceptance line and a rejection line given $\theta$, $\delta$, $\alpha$, and $\beta$.
Graphical Representation of Sequential Test

- Accept hypothesis

The graph shows the relationship between the number of samples and the number of negative samples.

- Reject
- Continue sampling
- Accept
Graphical Representation of Sequential Test

- Reject hypothesis
Example

- Verify plan with $\theta=0.05$, $\delta=0.01$, $\alpha=\beta=0.05$, $t_{\text{max}}=200$
Example

- Verify plan with $\theta=0.05$, $\delta=0.01$, $\alpha=\beta=0.05$, $t_{\text{max}}=200$
Performance

Failure probability

Average number of samples

\[\delta = 0.01, \alpha = \beta = 0.05\]

\[\delta = 0.01, \alpha = \beta = 0.10\]

\[\delta = 0.02, \alpha = \beta = 0.05\]

\[\delta = 0.02, \alpha = \beta = 0.10\]
Summary

- Probabilistic extension to CIRCA
  - Allows for plans with non-zero failure probability
- Efficient plan verification algorithm based on acceptance sampling
- Guaranteed error bounds
- Easy to trade efficiency for accuracy
Future Work

- Sensitivity analysis
- Using verification result to guide plan generation
- “Generalized semi-Markov Decision Processes”