Compositional Solution Space Quantification for Probabilistic Software Analysis

Mateus Borges, Marcelo d’Amorim (UFPE)  
Antonio Filieri (Stuttgart)  
Corina Pasareanu (CMU SV and NASA Ames)  
Willem Visser (Stellenbosch)
Uncertain Environments
Uncertain Environments
Quantitative Properties

Not restricted to boolean values

Establish non-functional requirements

→ Reliability, performance...
Probabilistic Model Checking

Probabilistic Model + Property Specification

PMC Engine (e.g. PRISM...)

Violation Probability
Probabilistic Model Checking

Problem: can be expensive!

➔ You need to learn a new modelling language
➔ You need to model the system

We would like to analyze code
Probabilistic Software Analysis

Target Event
+ Program
+ Input Profile

Analysis Engine

Event Probability
+ Accuracy
Probabilistic Software Analysis

- Source Code
- Target Event
- Input Profile
- Symbolic Execution
- PCs
- Probabilistic Analysis

Probability + Accuracy
Collect path conditions leading to target event
Obstacle: Quantification
Integration Methods

Symbolic
➔ very expensive, restricted

Numerical
➔ expensive with multi-dimensional domains

Statistical
➔ approximate results
Challenge

Quantifying the solution space of complex mathematical functions

Example constraint from TSAFE module (Tactical Separation Assisted Flight Environment)

\[ \sqrt{\text{pow}\left(\left(x_1 + \left(e_1 \cdot \cos(x_4) - \cos(\left(x_4 + \left(\left(1.0 \cdot \left(\left(c_1 \cdot x_5\right) \cdot \left(e_2/c_2\right)\right) / x_6\right) \cdot x_2 / e_1\right)\right)\right) - \left(\left(e_2/c_2\right) \cdot (1.0 - \cos(\left(c_1 \cdot x_5\right))\right), 2.0\right) > 999.0 \& (c_1 \cdot x_5) > 0.0 \& x_3 > 0.0 \& x_6 > 0.0 \& c_1 = 0.017... \& c_2 = 68443.0 \& e_1 = ((\text{pow}(x_2,2.0) / \text{tan}(\left(c_1\cdot x_3\right))/c_2) \& e_2 = \text{pow}(x_6,2.0) / \text{tan}(c_1\cdot x_3) \right) }\]
Contribution

Path Conditions + Input Profile

qCoral

Event Probability + Accuracy

Supports arbitrarily complex constraints
Computes accurate estimates efficiently
High Level View: Divide

Path Conditions

\[ PC^1 \]

\[ PC^2 \]

\[ PC^3 \]
High Level View: Divide

Path Conditions

Input Profile

PC<sup>1</sup> → PC<sup>2</sup> → PC<sup>3</sup>

pt<sup>1</sup> → pt<sup>2</sup> → pt<sup>3</sup> → pt<sup>4</sup> → pt<sup>5</sup> → pt<sup>6</sup> → pt<sup>7</sup>
High Level View: Divide

Path Conditions

$PC^1$

$PC^2$

$PC^3$

Input Profile

$pt^1$

$pt^2$

$pt^3$

$pt^4$

$pt^5$

$pt^6$

$pt^7$

Monte Carlo

$e_{pt}^1$

$e_{pt}^2$

$e_{pt}^3$

$e_{pt}^4$

$e_{pt}^5$

$e_{pt}^6$

$e_{pt}^7$
High Level View: Conquer
High Level View: Conquer

\[ e_{pt}^1 \quad e_{pt}^2 \quad e_{pt}^3 \quad e_{pt}^4 \quad e_{pt}^5 \quad e_{pt}^6 \quad e_{pt}^7 \]

\[ \rightarrow \]

\[ e_{PC}^1 \quad e_{PC}^2 \quad e_{PC}^3 \]
High Level View: Conquer

- $e_{pt}^1$
- $e_{pt}^2$
- $e_{pt}^3$
- $e_{pt}^4$
- $e_{pt}^5$
- $e_{pt}^6$
- $e_{pt}^7$

- $e_{PC}^1$
- $e_{PC}^2$
- $e_{PC}^3$

Probability Estimate
Working With Disjunctions

All elements in $PC^T$ are disjoint

Estimates can be computed individually
Working With Conjunctions

\[ PC_1 \]

\[
\begin{array}{c}
c1 \\
c2
\end{array}
\]

\[ PC_2 \]

\[
\begin{array}{c}
c2 \\
c3
\end{array}
\]

\[ PC_3 \]

\[
\begin{array}{c}
c4 \\
c3
\end{array}
\]

\[ \ldots \]
Working With Conjunctions

\[ PC^1 \]
\[
\begin{array}{c}
  c1 \\
  c2 \\
\end{array}
\]

\[ PC^2 \]
\[
\begin{array}{c}
  c2 \\
  c3 \\
\end{array}
\]

\[ PC^3 \]
\[
\begin{array}{c}
  c4 \\
  c3 \\
\end{array}
\]

\[ \ldots \]
Working With Conjunctions

\[ PC^1 \]
- \( c1 \)
- \( c2 \)

\[ PC^2 \]
- \( c2 \)
- \( c3 \)

\[ PC^3 \]
- \( c4 \)
- \( c3 \)

Contains dependent variables

pt1: \( c1 \)
pt2: \( c2 \)
pt3: \( c3 \)
pt4: \( c3 \land c4 \)
Working With Conjunctions

Partitions can be analyzed faster

Estimates can be efficiently re-used

pt1: c1
pt2: c2
pt3: c3
pt4: c3 && c4

Contains dependent variables
Quantifying Constraints
Quantifying Constraints

Domain

Solution Space

c2
Hit-or-Miss Monte Carlo

\[ E[X] = \frac{\# \text{hits}}{\# \text{samples}} \]
Stratified Sampling

Remove infeasible areas with RealPaver

Domain

c2 Solution Space

Boxes returned by RealPaver

c2 Solution Space
Stratified Sampling

Remove infeasible areas with RealPaver

Increase precision with Stratified Sampling
SPF Toolchain (with qCORAL)
Illustrative Example

// 0 <= x,y,z <= 9
f(x,y,z):
    if x < 5:
        if y < 3:
            abort()
        elif z + y > 10:
            abort()

Probability that f(x,y,z) calls abort()?
Illustrative Example

// 0 <= x,y,z <= 9

\( f(x,y,z) \):
  
  if \( x < 5 \):
    
    if \( y < 3 \):
      abort()
    
    elif \( z + y > 10 \):
      abort()

Probability that \( f(x,y,z) \) calls abort()?

pc1: \( x < 5 \) && \( y < 3 \)

pc2: \( x < 5 \) && \( y \geq 3 \)
    && \( z + y > 10 \)
Illustrative Example

//0 <= x,y,z <= 9
pc1: x < 5
    && y < 3
pc2: x < 5
    && y >= 3
    && z + y > 10

qCORAL
### Illustrative Example

<table>
<thead>
<tr>
<th>Condition 1</th>
<th>Condition 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x &lt; 5$</td>
<td>$x &lt; 5$</td>
</tr>
<tr>
<td>$y &lt; 3$</td>
<td>$y \geq 3$</td>
</tr>
<tr>
<td></td>
<td>$z + y &gt; 10$</td>
</tr>
</tbody>
</table>

- **pc1**: $x < 5 \land y < 3$
- **pc2**: $x < 5 \land y \geq 3 \land z + y > 10$
Illustrative Example

pc1: \( x < 5 \) && \( y < 3 \)

pc2: \( x < 5 \) && \( y \geq 3 \) && \( z + y > 10 \)
pc1: \( x < 5 \) && \( y < 3 \)

pc2: \( x < 5 \) && \( y \geq 3 \) && \( z + y > 10 \)
pc1: $x < 5 \land y < 3$

pc2: $x < 5 \land y \geq 3 \land z + y > 10$

pt1: $E = 0.5001$
Var = 0.00008

pt2: $E = 0.3000$
Var = 0.00003

pt3: $E = 0.3806$
Var = 0.00009
Illustrative Example

\[ pc1: \ x < 5 \ \&\& \ y < 3 \]
\[ pc2: \ x < 5 \ \&\& \ y \geq 3 \ \&\& \ z + y > 10 \]

\[ pt1: \]
\[ E = 0.5001 \]
\[ Var = 0.00008 \]

\[ pt2: \]
\[ E = 0.3000 \]
\[ Var = 0.00003 \]

\[ pt3: \]
\[ E = 0.3806 \]
\[ Var = 0.00009 \]
Illustrative Example

\[ \text{pt1:} \]
\[ E = 0.5001 \]
\[ Var = 0.00008 \]
\[ \text{pt2:} \]
\[ E = 0.3000 \]
\[ Var = 0.00003 \]
\[ \text{pt3:} \]
\[ E = 0.3806 \]
\[ Var = 0.00009 \]

\[ \text{pc1:} \]
\[ E = 0.1501 \]
\[ Var = 0.00013 \]
\[ \text{pc2:} \]
\[ E = 0.1927 \]
\[ Var = 0.00022 \]

\[ \text{pc1: } x < 5 \land y < 3 \]
\[ \text{pc2: } x < 5 \land y \geq 3 \land z + y > 10 \]
Illustrative Example

\[ \text{pc1: } x < 5 \land y < 3 \]
\[ \text{pc2: } x < 5 \land y \geq 3 \land z + y > 10 \]

\[ \begin{align*}
\text{pt1:} & \quad E = 0.5001 \\
& \quad \text{Var} = 0.00008 \\
\text{pt2:} & \quad E = 0.3000 \\
& \quad \text{Var} = 0.00003 \\
\text{pt3:} & \quad E = 0.3806 \\
& \quad \text{Var} = 0.00009
\end{align*} \]

\[ \begin{align*}
\text{pc1:} & \quad E = 0.1501 \\
& \quad \text{Var} = 0.00013 \\
\text{pc2:} & \quad E = 0.1927 \\
& \quad \text{Var} = 0.00022
\end{align*} \]

\[ \begin{align*}
\text{Estimate:} & \quad 0.3403 \\
\text{Variance:} & \quad \leq 0.0005
\end{align*} \]
Illustrative Example

// 0 <= x, y, z <= 9
pc1: x < 5
    && y < 3
pc2: x < 5
    && y >= 3
    && z + y > 10

qCORAL

Estimate: 0.3403
Variance: <= 0.0005
Evaluation

RQ1: qCORAL is competitive with other tools?

RQ2: qCORAL features help with complex constraints?
RQ1: qCORAL is competitive?

VolComp Benchmark (PLDI’13)

Techniques/Tools:

➔ Mathematica (*NIntegrate*)
➔ VolComp
➔ qCORAL
RQ1: qCORAL is competitive?

VolComp Benchmark (PLDI'13)

Techniques/Tools:

➔ Mathematica (*NIntegrate*)
➔ VolComp
➔ qCORAL
### RQ1: qCORAL is competitive?

<table>
<thead>
<tr>
<th></th>
<th>NIntegrate</th>
<th>VolComp</th>
<th>qCORAL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>solution</strong></td>
<td></td>
<td><strong>bounds</strong></td>
<td><strong>avg. est.</strong></td>
</tr>
<tr>
<td><strong>ARTRIAL</strong></td>
<td>0.9350</td>
<td>[0.9340, 0.9364]</td>
<td>0.9352</td>
</tr>
<tr>
<td><strong>CART</strong></td>
<td>0.9826</td>
<td>[0.9470, 1.0000]</td>
<td>0.9818</td>
</tr>
<tr>
<td><strong>CORONARY</strong></td>
<td>0.0001</td>
<td>[0.0001, 0.0001]</td>
<td>0.0001</td>
</tr>
<tr>
<td><strong>EGFR-EPI</strong></td>
<td>0.1264</td>
<td>[0.1264, 0.1264]</td>
<td>0.1262</td>
</tr>
<tr>
<td><strong>PACK</strong></td>
<td>0.2462</td>
<td>[0.2522, 0.2800]</td>
<td>0.2663</td>
</tr>
<tr>
<td><strong>VOL</strong></td>
<td>1.0005</td>
<td>[0.0000, 1.0000]</td>
<td>1.0001</td>
</tr>
</tbody>
</table>
## RQ1: qCORAL is competitive?

<table>
<thead>
<tr>
<th>Dataset</th>
<th>NIntegrate</th>
<th>VolComp</th>
<th>qCORAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>solution</td>
<td>bounds</td>
<td>avg. est.</td>
</tr>
<tr>
<td>ARTRIAL</td>
<td>0.9350</td>
<td>[0.9340, 0.9364]</td>
<td>0.9352</td>
</tr>
<tr>
<td>CART</td>
<td>0.9826</td>
<td>[0.9470, 1.0000]</td>
<td>0.9818</td>
</tr>
<tr>
<td>CORONARY</td>
<td>0.0001</td>
<td>[0.0001, 0.0001]</td>
<td>0.0001</td>
</tr>
<tr>
<td>EGFR-EPI</td>
<td>0.1264</td>
<td>[0.1264, 0.1264]</td>
<td>0.1262</td>
</tr>
<tr>
<td>PACK</td>
<td>0.2462</td>
<td>[0.2522, 0.2800]</td>
<td>0.2663</td>
</tr>
<tr>
<td>VOL</td>
<td>1.0005</td>
<td>[0.0000, 1.0000]</td>
<td>1.0001</td>
</tr>
</tbody>
</table>
**RQ1: qCORAL is competitive?**

<table>
<thead>
<tr>
<th></th>
<th>NIntegrate</th>
<th>VolComp</th>
<th>qCORAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>solution</td>
<td>bounds</td>
<td>avg. est.</td>
</tr>
<tr>
<td>ARTRIAL</td>
<td>0.9350</td>
<td>[0.9340, 0.9364]</td>
<td>0.9352</td>
</tr>
<tr>
<td>CART</td>
<td>0.9826</td>
<td>[0.9470, 1.0000]</td>
<td>0.9818</td>
</tr>
<tr>
<td>CORONARY</td>
<td>0.0001</td>
<td>[0.0001, 0.0001]</td>
<td>0.0001</td>
</tr>
<tr>
<td>EGFR-EPI</td>
<td>0.1264</td>
<td>[0.1264, 0.1264]</td>
<td>0.1262</td>
</tr>
<tr>
<td>PACK</td>
<td>0.2462</td>
<td>[0.2522, 0.2800]</td>
<td>0.2663</td>
</tr>
<tr>
<td>VOL</td>
<td>1.0005</td>
<td>[0.0000, 1.0000]</td>
<td>1.0001</td>
</tr>
</tbody>
</table>
## RQ1: qCORAL is competitive?

<table>
<thead>
<tr>
<th></th>
<th>NIntegrate</th>
<th>VolComp</th>
<th>qCORAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>time</td>
<td>time</td>
<td>avg. time</td>
</tr>
<tr>
<td>ARTRIAL</td>
<td>4,179.36</td>
<td>771.10</td>
<td>4.14</td>
</tr>
<tr>
<td>CART</td>
<td>7.66</td>
<td>33.74</td>
<td>4.39</td>
</tr>
<tr>
<td>CORONARY</td>
<td>0.86</td>
<td>1.99</td>
<td>0.57</td>
</tr>
<tr>
<td>EGFR EPI</td>
<td>1.98</td>
<td>0.60</td>
<td>1.61</td>
</tr>
<tr>
<td>PACK</td>
<td>5,066.20</td>
<td>104.80</td>
<td>68.79</td>
</tr>
<tr>
<td>VOL</td>
<td>1,245.30</td>
<td>3.76</td>
<td>821.11</td>
</tr>
</tbody>
</table>
RQ1: Observations

qCORAL estimates:

→ are very close to the results reported by NIntegrate

→ almost always fall within the VolComp interval
RQ2: Evaluation

- Subjects from the aerospace domain
- Picked 70% of the paths to avoid bias
- Reported results for 30 executions (avg. estimate and standard error)
RQ2: Evaluated configurations

- qCORAL \{\}
- qCORAL \{STRAT\}
- qCORAL \{STRAT, PCACHE\}

Steps:
1. qCORAL \{\} + ICP: Stratified Sampling
2. qCORAL \{STRAT\} + Partitioning Caching
## RQ2: Subjects Considered

<table>
<thead>
<tr>
<th>Subject</th>
<th>LOC</th>
<th>#pcs analyzed (70%)</th>
<th>complex functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apollo</td>
<td>~2,600</td>
<td>5,779</td>
<td>sqrt</td>
</tr>
<tr>
<td>TSAFE - Conflict</td>
<td>~50</td>
<td>23</td>
<td>cos,pow, sin, sqrt,tan</td>
</tr>
<tr>
<td>TSAFE - Turnlogic</td>
<td>~50</td>
<td>225</td>
<td>atan2</td>
</tr>
</tbody>
</table>
RQ2: Conclusions

Impact of features depends on the subject

\{STRAT\} can reduce variance (x50 in Conflict)

➔ There is a time overhead, however

\{PCACHE\} can reduce time (x2 in Apollo)

➔ Savings increase with number of samples
Sankaranarayanan et al. (PLDI’13) ➔ Supports only linear constraints

Adje et al. (VSTTE’13) ➔ Supports only the four basic arithmetic operations
Conclusions

qCoral

New approach to solution space quantification

Acceleration procedure improves accuracy

More details at pan.cin.ufpe.br/qcoral
Extra Slides
Probability of a Target Event

\[ P(\text{event}) = \sum \text{probabilities of the paths that lead to the event} \]

\[ P(\text{path}) = \frac{\text{size of solution space}}{\text{size of domain}} \]

And if the number of paths is infinite?

Bound the symbolic execution and measure the confidence!

(see Filieri et al, ICSE 2013)
And the Variance?

Use Chebyshev’s inequality:

“...at least $1 - 1/k^2$ of the distribution's values are within $k$ standard deviations of the mean”
Target application

Sometimes knowing only if an event happens is not very useful!

➔ randomized behavior
➔ probabilistic profile of the environment