Steering Symbolic Execution to Less Traveled Paths

You Li

Joint with Zhendong Su, Linzhang Wang, Xuandong Li
Background and Motivations

- Testing is important, but can be ineffective
  - Software is complex with large or infinite state space
  - Manual testing is tedious and ad hoc
  - Random testing is not systematic

- Symbolic execution is promising
  - Systematically explores a program
  - Generates test cases with high coverage
Symbolic Execution

- Uses symbolic values for inputs to explore a program
- Forks at branch conditions
- Follows both directions by updating path constraints
- Solves path constraints to generate test cases
Main Challenges

- Complex constraints
- Path explosion

Goal: Guide Symbolic Execution to Profitable Paths
Key issue: How to guide toward profitable paths?
Less Traveled Paths

- **Benefits**
  - Cover the program better
  - Locate more bugs

- **Difficulties**
  - Define "footprints"
  - Use "footprints" to guide path exploration
Subpath-Guided Path Exploration

- How to define “footprints”?
  - *Length-n* Subpath Program Spectra

- How to use "footprints" to guide path exploration?
  - Subpath-Guided Search (SGS)
Program Spectra

- **Program profiling**
  - Counting different program execution events

- **Profiling of different events provides various program spectra**
  - Branch Hit Spectra
  - Branch Count Spectra
  - Complete Path Spectra
  - Path Spectra
  - Path Count Spectra
Length-\(n\) Subpath Program Spectra

- Each subpath has \(n\) branches
- Contiguous sub-sequences of execution paths
- Varying \(n\) leads to a spectrum of modeling precision
- Fills the gap between branch coverage & complete path coverage
Subpath Guided Search (SGS)

- Maintain a structure $e = \langle \pi_n, f \rangle$
  - $\pi_n$ is a length $n$ subpath
  - $f$ is the frequency of $\pi_n$

- For each execution, track the most recent length-$n$ path segment

- Pick a pending execution with the lowest $f$ to explore next
  - Break ties randomly
Example

\[
\text{main (x, y)} \{
\begin{align*}
\text{s0: } & \quad \text{if } (x > y) \\
\text{s1: } & \quad x = f(x); \\
\text{else } & \\
\text{s2: } & \quad ; \\
\text{s3: } & \quad g (x, y); \\
\text{s4: } & \quad \text{return;}
\end{align*}
\}
\]

\[
\text{int f (a)} \{
\begin{align*}
\text{s5: } & \quad \text{if } (a > 0) \\
\text{s6: } & \quad \text{ABORT;} \\
\text{else } & \\
\text{s7: } & \quad \text{return -a;}
\end{align*}
\}
\]

\[
\text{g (a, b)} \{
\begin{align*}
\text{s8: } & \quad \text{if } (a == 0) \\
\text{s9: } & \quad \text{if } (b == 0) \\
\text{s10: } & \quad \text{ABORT;} \\
\text{else } & \\
\text{s11: } & \quad ; \\
\text{else } & \\
\text{s12: } & \quad \text{print a/b;} \\
\text{s13: } & \quad \text{return;}
\end{align*}
\}
\]
Sub-path Frequency

- $S_{0t}, 0$
- $S_{0f}, 1$
- $S_{0fS_{8t}}, 0$
- $S_{0fS_{8f}}, 0$
Entry

Sub-path Frequency

\( S_{0t, 0} \)

\( S_{0f, 0} \)

\( S_{0fS_8t, 0} \)

\( S_{0fS_8t, 1} \)

\( S_{0fS_8f, 1} \)

2013/10/31
Sub-path Frequency

- $S_{0t}, 0^*$
- $S_{0f}, 1$
- $S_{0f}S_{8t}, 1$
- $S_{0f}S_{8f}, 1$
- $S_{8t}S_{9t}, 0^*$
- $S_{8t}S_{9f}, 0^*$
### Sub-path Frequency

<table>
<thead>
<tr>
<th>Sub-path</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_{0t}, 0$</td>
<td></td>
</tr>
<tr>
<td>$S_{0f}, 1$</td>
<td></td>
</tr>
<tr>
<td>$S_{0f}S_{8t}, 1$</td>
<td></td>
</tr>
<tr>
<td>$S_{0f}S_{8f}, 1$</td>
<td></td>
</tr>
<tr>
<td>$S_{8t}S_{9t}, 0$</td>
<td></td>
</tr>
<tr>
<td>$S_{8t}S_{9f}, 1$</td>
<td></td>
</tr>
</tbody>
</table>

Flowchart:
- Entry
  - $S_{0t}, 0$
    - $S_0$
      - $S_5$
        - $S_{6}$
          - $S_{10}$
            - $S_{8t}S_{9t}, 0$
              - $S_{9}$
                - $S_{0f}S_{8t}S_{9f}S_4$
                  - $S_{0f}S_{8f}S_4$
                    - $S_4$
Sub-path Frequency

- \( S_{0t}, 0^* \)
- \( S_{0f}, 1 \)
- \( S_{0fS_8t}, 1 \)
- \( S_{0fS_8f}, 1 \)
- \( S_{8tS_9t}, 1 \)
- \( S_{8tS_9f}, 1 \)
Sub-path Frequency

- $S_{0t}, 1$
- $S_{0f}, 1$
- $S_{0t}S_{8t}, 1$
- $S_{0f}S_{8f}, 1$
- $S_{8t}S_{9t}, 1$
- $S_{8t}S_{9f}, 1$
- $S_{0t}S_{5t}, 0^*$
- $S_{0t}S_{5f}, 0^*$

Entries:

- $S_0$
- $S_5$
- $S_6$
- $S_8$
- $S_9$
- $S_{10}$

Paths:

- $S_{0t}S_{5t}, 0$
- $S_{0t}S_{5f}, 0$

Date: 2013/10/31
Sub-path Frequency

$S_{0t}, 1$
$S_{0f}, 1$
$S_{0f}S_{8t}, 1$
$S_{0f}S_{8f}, 1$
$S_{8t}S_{9t}, 1^*$
$S_{8t}S_{9f}, 1^*$
$S_{0t}S_{5t}, 0^*$
$S_{0t}S_{5f}, 1$
$S_{5f}S_{8t}, 1$
$S_{5f}S_{8f}, 1$

2013/10/31
Evaluation: Research Questions

- What impact do different choices of $n$ have?
- Can they be effectively combined?
- How does our strategy compare to existing strategies?
Evaluation Setup

- Implement SGS in KLEE
- Evaluation subjects: GNU core utilities
- Evaluated search strategies
  - Length-n SGS with varying n (n = 1, 2, 4, 8)
  - Existing strategies implemented in KLEE
- Evaluation metrics
  - How well a program is covered?
  - How effective in locating bugs?
KLEE Strategies

- DFS
- Random State
- Random Path
- Non-Uniform Random Selection
  - covnew
  - depth
  - icnt
  - md2u
Program Coverage

- 75 programs (2K - 10K LOC in size)
- Run each strategy for 1 hour
- Output test cases exploring new statements or triggering errors
- Re-execute test cases to measure statement coverage
Coverage Distribution

- SGS-1
- SGS-2
- SGS-4
- SGS-8

- 90%-100%
- 80%-90%
- 70%-80%
- 60%-70%
- 60%-

- RSS
- DFS
- RPS
- NURS covernew
- NURS depth
- NURS icnt
- NURS md2u

2013/10/31
Average Coverage (%)
### "Best" Counts

<table>
<thead>
<tr>
<th></th>
<th>SGS-1</th>
<th>SGS-2</th>
<th>SGS-4</th>
<th>SGS-8</th>
<th>RSS</th>
<th>DFS</th>
<th>RPS</th>
<th>NURS cn</th>
<th>NURS depth</th>
<th>NURS icnt</th>
<th>NURS md2u</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Best</strong></td>
<td>25</td>
<td>38</td>
<td>29</td>
<td>24</td>
<td>20</td>
<td>16</td>
<td>23</td>
<td>14</td>
<td>21</td>
<td>14</td>
<td>15</td>
</tr>
</tbody>
</table>

2013/10/31
Results Recap

- Result 1: SGS yields higher coverage
- Result 2: No uniform best $n$ for SGS
Combined SGS

- Run SGS with length 1, 2, 4, 8 for 15 minutes each
- Combine all the generated test cases
Average Coverage (%)

- SGS-1
- SGS-2
- SGS-4
- SGS-8
- Com

For 60min and 15min

2013/10/31
Coverage Distribution

SGS-1 | SGS-2 | SGS-4 | SGS-8 | Com

RSS DFS RPS NURS cover new NURS depth NURS icnt NURS md2u

- 90%-100%
- 80%-90%
- 70%-80%
- 60%-70%
- 60%-

2013/10/31
Average Coverage (%)
"Best" Counts

<table>
<thead>
<tr>
<th></th>
<th>SGS-1</th>
<th>SGS-2</th>
<th>SGS-4</th>
<th>SGS-8</th>
<th>Com</th>
<th>RSS</th>
<th>DFS</th>
<th>RPS</th>
<th>NURS cn</th>
<th>NURS depth</th>
<th>NURS icnt</th>
<th>NURS md2u</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best</td>
<td>25</td>
<td>38</td>
<td>29</td>
<td>24</td>
<td>57</td>
<td>20</td>
<td>16</td>
<td>23</td>
<td>14</td>
<td>21</td>
<td>14</td>
<td>15</td>
</tr>
</tbody>
</table>

2013/10/31
Results Recap

- Result 3: Combined SGS performs uniformly the best
Result 4: SGS yields more bug reports

Result 5: SGS has acceptable overhead
Bug Detection: Killing Mutants

- 40 programs (which produce deterministic output)
- Run each different strategy for 1 hour
- Output all terminated test cases
- Generate mutants of the 40 programs
- Re-execute test cases on both original program and mutants
- Compare their outputs to see if mutants were killed
### Average Kill Rate (%)

<table>
<thead>
<tr>
<th></th>
<th>SGS-1</th>
<th>SGS-2</th>
<th>SGS-4</th>
<th>SGS-8</th>
<th>Combined</th>
<th>RSS</th>
<th>DFS</th>
<th>RPS</th>
<th>NURS cn</th>
<th>NURS depth</th>
<th>NURS icnt</th>
<th>NURS md2u</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>26</td>
<td>27.65</td>
<td>26.04</td>
<td>26.96</td>
<td>32.17</td>
<td>23.03</td>
<td>18.63</td>
<td>25.16</td>
<td>19.58</td>
<td>21.8</td>
<td>19.23</td>
<td>18.44</td>
</tr>
</tbody>
</table>

Date: 2013/10/31
Total Kill Number

2013/10/31
"Best" Counts

Result 6: SGS kills more mutants
Impact of Different Length $n$

- Shorter length => less contextual information

- Longer length => more contextual information

- Combined SGS strikes a good balance
  - Efficiency
  - Effectiveness
Summary

- Introduced length-n path spectra to guide path exploration
  - Uniform, parameterized technique
  - Steering toward less traveled paths
- Implemented in KLEE and extensively evaluated
  - SGS outperforms existing search strategies
  - SGS exhibits different behavior with varying length $n$
  - Combined SGS performs the best

Thanks!