VeriAbs

Afzal, Asia, Avriti Chauhan, Bharti Chimdyalwar, Priyanka Darke, Advaita Datar, Shrawan Kumar, Charles Babu M, Tanha Shah, R Venkatesh

Tata Consultancy Services, Chennai Mathematical Institute

March 28, 2019
Techniques in VeriAbs

- Ideas to prove properties
  - Loop Abstraction to scale Bounded Model Checking (LABMC)
    - Abstract Acceleration + split case k induction
  - Invariants from program behavior and syntax
  - Shrinking and pruning for array loops

- Ideas to falsify properties
  - Test generation by fuzzing
  - Bounded model checking

<table>
<thead>
<tr>
<th>Category</th>
<th># Programs</th>
<th>Score (# prgs. verified)</th>
<th>Highest score (# prgs. verified)</th>
<th>VeriAbs Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReachSafety</td>
<td>3831</td>
<td>4638 (3173)</td>
<td>-</td>
<td>Gold</td>
</tr>
<tr>
<td>SoftwareSystems</td>
<td>2809</td>
<td>1061 (1757)</td>
<td>1185 (2202)</td>
<td>Bronze</td>
</tr>
</tbody>
</table>

[DATE'15, FM'15, ICST'17, LCTES'18]
[Prabhu et al SAS'18]
[Kumar et al TACAS'18]
Invariant Synthesis using Syntax & Behaviours

```c
int x = 0, y = 0;
while(*){
    x = x + 1;
    y = y + x;
}
assert (y >= 0);
```

```c
int n, sum = 0, i = 1;
assume (1 <= n <= 1000);
while(i <= n){
    sum = sum + i;
    i = i + 1;
}
assert (2*sum = n*(n+1));
```

- Data candidates are learned from program behaviors [Prabhu et al SAS’18]
- Guess and check framework
- Highest score in ECA

\[
x \geq 0 \land y \geq 0
\]

\[
2*sum = i*(i-1) \land (i \leq n+1)
\]
Array Pruning

1. #define N 100000
2. 3. void computeMin(){
4. int i, min, a[N]
5. 6. min = a[0]
7. 8. for (i = 1; i < N; i++)
9.   if(min > a[i]){
10.      min = a[i]
11.  }
12. 13. assert (
14.   forall j in [0,N)
15.     a[j] >= min
16.   exists j in [0,N)
17.     a[j] == min
18. )
19. }

- Initialized with non-deterministic values (or initialized programmatically)
- Constant loop bound and increment steps
- Indices must have a constant offset from the counter
- Limited support for multiple and nested loops
- Second in arrays category
- In collaboration with IIT Bombay

<table>
<thead>
<tr>
<th>Programs</th>
<th>Safe</th>
<th>Unsafe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>123</td>
<td>44</td>
</tr>
<tr>
<td>Not pruneable</td>
<td>85</td>
<td>34</td>
</tr>
<tr>
<td>Pruneable</td>
<td>38</td>
<td>10</td>
</tr>
<tr>
<td>By shrinkability [TACAS’18]</td>
<td>65</td>
<td>17</td>
</tr>
<tr>
<td>By pruning</td>
<td>22</td>
<td>01</td>
</tr>
<tr>
<td>By both</td>
<td>16</td>
<td>09</td>
</tr>
</tbody>
</table>
Thank you