1. Problem : Find an invariant \( I \) for the Loop 

\[
\{ \delta \} \text{ while } \rho \text{ do } S \text{ end } \{ \epsilon \}
\]

Invariant must satisfy the following conditions:

(A) \( \delta \Rightarrow I \) \hspace{1cm} (B) \( I \land \rho \Rightarrow \text{Pre}(I, S) \) \hspace{1cm} (C) \( I \land \lnot \rho \Rightarrow \epsilon \)

Example:

precondition 
\[
\delta = (i = 0)
\]

loop guard \( \beta \)

while \( i < 10 \) do

\[
\text{ret} := \text{random}();
\]

if \( \text{ret} != 0 \) then \( i := i + 1 \)
end

postcondition 
\[
\epsilon = (i = 10 \land \text{ret})
\]

Invariant: \( i < 10 \lor (i = 10 \land \text{ret}) \)

2. Idea : Using the CDNF Algorithm

Exact Learning Algorithm for Boolean formula

Asks two types of queries:

1) Membership Query \( \text{MEM}(\mu) \) asks 
if the truth assignment \( \mu \) satisfies \( \lambda \).

\[
\text{MEM}(\mu) = \begin{cases} 
\text{Yes} & \text{if } \mu \models \lambda \\
\text{No} & \text{if } \mu \nmodels \lambda
\end{cases}
\]

2) Equivalence Query \( \text{EQ}(\beta) \) asks 
if the Boolean formula \( \beta \) is equivalent to \( \lambda \),
If not, the teacher returns a truth assignment as a counterexample \( \mu \).

\[
\text{EQ}(\beta) = \begin{cases} 
\text{Yes} & \text{if } \beta \equiv \lambda \\
\text{No} & \text{with } \mu \text{ if } \beta \not\equiv \lambda \land (\mu \models \beta \equiv \lambda)
\end{cases}
\]

3. Solution: Implementing a Teacher to Answer Queries

Overview

- **SMT Solver**: Formula
  - SAT with CE / UNSAT
- **Static Analyzer**: Under/Over Approximation of Invariants
- **Algorithmic Learning**: Propositional Formula
  - \( i < 10 \lor (i = 10 \land \text{ret}) \)
- **Predicate Abstraction**: Boolean Formula
  - \( b_{L<10} \lor (b_{L=10} \lor \text{ret}) \)

**Resolving Equivalence Query: EQ(\beta)**

1. **Yes**, if the guess \( \beta \) meets the three conditions [A,B,C] to be an invariant.
2. Try to answer "No" with a counterexample.
   - If not possible, then restart.

**Guess 5**: No, with found a counterexample.

**Guess 5**: Restart!

**Guess 5**: Cannot find a counterexample.

**Resolving Membership Query: MEM(\mu)**

1. Try to find an answer.
2. If not possible choose a random answer.
   - It is still sound since we always check the three conditions in equivalence query resolution.

**Guess 5**: Yes

**Guess 5**: No

**Guess 5**: Unknown

Random Answer

4. Experiment Results

For some Linux device drivers and SPEC2000 benchmarks.

<table>
<thead>
<tr>
<th>Program</th>
<th>LOC</th>
<th>AP</th>
<th>MEM</th>
<th>EQ</th>
<th>Randoms</th>
<th>Restart</th>
<th>Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>lde-lde-tape</td>
<td>16</td>
<td>18.2</td>
<td>5.2</td>
<td>4.4</td>
<td>1.2</td>
<td>0.005</td>
<td></td>
</tr>
<tr>
<td>lde-std-tape</td>
<td>9</td>
<td>216.1</td>
<td>111.8</td>
<td>47.2</td>
<td>9.9</td>
<td>0.002</td>
<td></td>
</tr>
<tr>
<td>parser</td>
<td>3</td>
<td>6654.3</td>
<td>319.4</td>
<td>990.4</td>
<td>12.5</td>
<td>0.120</td>
<td></td>
</tr>
<tr>
<td>unix-messsage</td>
<td>18</td>
<td>20.1</td>
<td>6.8</td>
<td>1.0</td>
<td>1.0</td>
<td>0.128</td>
<td></td>
</tr>
<tr>
<td>vpr</td>
<td>8</td>
<td>14.9</td>
<td>8.9</td>
<td>11.8</td>
<td>2.9</td>
<td>0.005</td>
<td></td>
</tr>
</tbody>
</table>

The data are the averages of 50 runs and collected on a 2.6GHz Intel E5500 Duo Core with 3GB memory running Linux 2.6.28.

5. Conclusion

* Novel approach to invariants generation.
* Multitude of invariants is the reason why this approach is working with random answers.
* We are currently working on its extension supporting quantified invariants.