SMT-based Formal Analysis of the ECMAScript Shared Memory Model

Cristian Mattarei, PhD
mattarei@stanford.edu

The problem of JavaScript Engine Correctness

94.5% of front-end web-based applications use JavaScript

<table>
<thead>
<tr>
<th>Programming Language</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>5.4%</td>
</tr>
<tr>
<td>JavaScript</td>
<td>94.5%</td>
</tr>
<tr>
<td>Flash</td>
<td>6.9%</td>
</tr>
<tr>
<td>Silverlight</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

Multi-Core Processors

Shared Memory Operations Extension

Correct JavaScript Engines Implementation Concerns

Correct Output?

All Possible Valid Executions

JavaScript Program (Shared Memory)

JavaScript engine

FM.JS Project Approach

SMT-based Formal Analyses

EMME

CVC4