JSCert: Certified JavaScript

November 2012

INRIA:

- Martin Bodin
- Arthur Charguéraud
- Alan Schmitt

Imperial College:

- Daniele Filaretti
- Philippa Gardner
- Sergio Maffeis
- Daiva Naudziuniene
- Gareth Smith

Certified JavaScript

Our project:

- JSCert: JavasScript specification in Coq
- JSRef: a reference interpreter and testing
- JSVerify: certified automated reasoning
- Library plugins for JSVerify: e.g. DOM plugin
- JSTools: e.g., security analysis of browser extensions

Other applications:

- Verified compilation from other languages into JS
- Verification of virtual machines

JSCert and JSRef

Goal: a Coq formalization of JavaScript semantics

- an operational semantics very faithful to the official reference
- an interpreter proved correct w.r.t. the operational semantics

Previous and related work:

- Small-step semantics for the entire language (jssec.net)
- Big-step semantics and program logic for the core language (POPL'12)
- λ_{JS}: small-step semantics via translation into a λ-calculus with refs
- Pretty-big-step semantics for avoiding duplication in rules

Progress

Subset of JavaScript formalized so far:

- variable declaration, scopes, prototype chains,
- function call, new, delete, access, assignment,
- unary and binary operators (most useful ones),
- sequence, conditional, while loop,
- with construct, this construct,
- throw, try construct,
- break and continue (almost complete)
- type conversions (almost complete)

Main missing features:

- switch, arrays, for loops
- parsing, eval
- extensions: regexp, ...