

The Essence of JavaScript

Arjun Guha, Claudiu Saftoiu and Shriram
Krishnamurthi

Department of Computer Science
Brown University
Providence, Rhode Island 02912

CS-09-10
December 2009

The Essence of JavaScript

Arjun Guha, Claudiu Saftoiu, and Shriram Krishnamurthi

Brown University

Abstract. We reduce JavaScript to a core calculus structured as a small-step operational semantics. We present several peculiarities of the language and show that our calculus models them. We explicate the desugaring process that turns JavaScript programs into ones in the core. We demonstrate faithfulness to JavaScript using real-world test suites. Finally, we illustrate utility by defining a security property, implementing it as a type system on the core, and extending it to the full language.

1 The Need for A(nother) JavaScript Semantics

The growing use of JavaScript, which is the scripting language of Web browsers, has created whole new technical and business models of program construction and deployment. Unfortunately, JavaScript is a feature-rich language with many quirks, and these quirks are often exploited to create security and privacy attacks. This is especially true in cases where JavaScript has a familiar syntax but unconventional semantics.

Due to its popularity and shortcomings, companies and researchers have tried to tame JavaScript via program analyses [4, 9, 10, 13], language subsets [5, 7, 17], and more. These works claim but do not demonstrate soundness. In part, this is due to the difficulty of obtaining a tractable account of the language: the standard [6] is capacious and informal, while one major formal semantics [15] is large, not amenable to conventional proof techniques, and inherits the standard’s complexities, as we discuss in section 5. In contrast:

- We present a core language, λ_{JS} , that embodies JavaScript’s essential features (sans `eval`). λ_{JS} fits on three pages and lends itself well to proofs techniques such as subject reduction.
- We show that we can desugar JavaScript into λ_{JS} . In particular, desugaring handles notorious JavaScript features such as `this` and `with`, so λ_{JS} itself remains simple (and thus simplifies proofs that utilize it).
- We have mechanized both λ_{JS} and desugaring.
- To show compliance with reality, we have successfully tested λ_{JS} and desugaring against the actual Mozilla JavaScript test suite.
- Finally, we demonstrate the use of our semantics by building a safe subset of JavaScript. This application highlights how our partitioning of JavaScript into core and syntactic sugar lends structure to proofs.

Our supplemental materials (full desugaring, tools, etc.) are available at

<http://www.cs.brown.edu/research/plt/dl/CS-09-10>

$$\begin{aligned}
c &= \text{num} \mid \text{str} \mid \text{bool} \mid \text{undefined} \mid \text{null} \\
v &= c \mid \text{func}(x \cdots) \{ \text{return } e \} \mid \{ \text{str}: v \cdots \} \\
e &= x \mid v \mid \text{let } (x = e \cdots) e \mid e(e \cdots) \mid e[e] \mid e[e] = e \mid \text{delete } e[e] \\
E &= \bullet \mid \text{let } (x = v \cdots \mid x = E, x = e \cdots) e \mid E(e \cdots) \mid v(v \cdots \mid E, e \cdots) \\
&\quad \mid \{ \text{str}: v \cdots \mid \text{str}: E, \text{str}: e \cdots \} \mid E[e] \mid v[E] \mid E[e] = e \mid v[E] = e \\
&\quad \mid v[v] = E \mid \text{delete } E[e] \mid \text{delete } v[E]
\end{aligned}$$

$$\begin{aligned}
&\text{let } (x = v \cdots) e \hookrightarrow e[x/v] \cdots & (\text{E-LET}) \\
&(\text{func}(x_1 \cdots x_n) \{ \text{return } e \})(v_1 \cdots v_n) \hookrightarrow e[x_1/v_1 \cdots x_n/v_n] & (\text{E-APP}) \\
&\{ \cdots \text{str}: v \cdots \}[\text{str}] \hookrightarrow v & (\text{E-GETFIELD}) \\
&\frac{\text{str}_x \notin (\text{str}_1 \cdots \text{str}_n)}{\{ \text{str}_1: v_1 \cdots \text{str}_n: v_n \} [\text{str}_x] \hookrightarrow \text{undefined}} & (\text{E-GETFIELD-NOTFOUND}) \\
&\frac{\{ \text{str}_1: v_1 \cdots \text{str}_i: v_i \cdots \text{str}_n: v_n \} [\text{str}_i] = v}{\hookrightarrow \{ \text{str}_1: v_1 \cdots \text{str}_i: v \cdots \text{str}_n: v_n \}} & (\text{E-UPDATEFIELD}) \\
&\frac{\text{str}_x \notin (\text{str}_1 \cdots)}{\{ \text{str}_1: v_1 \cdots \} [\text{str}_x] = v_x \hookrightarrow \{ \text{str}_x: v_x, \text{str}_1: v_1 \cdots \}} & (\text{E-CREATEFIELD}) \\
&\frac{\text{delete } \{ \text{str}_1: v_1 \cdots \text{str}_i: v_x \cdots \text{str}_x: v_n \} [\text{str}_x]}{\hookrightarrow \{ \text{str}_1: v_1 \cdots \text{str}_i: v \cdots \text{str}_n: v_n \}} & (\text{E-DELETEFIELD}) \\
&\frac{\text{str}_x \notin (\text{str}_1 \cdots)}{\text{delete } \{ \text{str}_1: v_1 \cdots \} [\text{str}_x] \hookrightarrow \{ \text{str}_1: v_1 \cdots \}} & (\text{E-DELETEFIELD-NOTFOUND})
\end{aligned}$$

Fig. 1. Functions and Objects

2 λ_{JS} : A Tractable Semantics for JavaScript

In the following sections, we present λ_{JS} incrementally. Figures 1, 2, 4, 8, and 9 specify the syntax and semantics of λ_{JS} . We use a Felleisen-Hieb small-step operational semantics with evaluation contexts [8].

Alongside the semantics we also present examples of JavaScript’s behavior, some of which might strike the reader—especially one used to a more traditional interpretation of the same syntax—as unconventional. These help demonstrate how λ_{JS} truly can explain the behavior of JavaScript.

$l = \dots$	Locations
$v = \dots \mid l$	Values
$\sigma = \langle (l, v) \dots \rangle$	Stores
$e = \dots \mid \mathbf{e} = \mathbf{e} \mid \mathbf{ref} \ \mathbf{e} \mid \mathbf{deref} \ \mathbf{e}$	Expressions
$E = \dots \mid \mathbf{E} = \mathbf{e} \mid \mathbf{v} = \mathbf{E} \mid \mathbf{ref} \ \mathbf{E} \mid \mathbf{deref} \ \mathbf{E}$	Evaluation Contexts

$$\begin{array}{c}
\frac{e_1 \hookrightarrow e_2}{\sigma E[e_1] \rightarrow \sigma E[e_2]} \\
\\
\frac{l \notin \text{dom}(\sigma) \quad \sigma' = \sigma, (l, v)}{\sigma E[\mathbf{ref} \ v] \rightarrow \sigma' E[\mathbf{1}]} \quad (\text{E-REF}) \\
\\
\sigma E[\mathbf{deref} \ l] \rightarrow \sigma E[\sigma(l)] \quad (\text{E-DEREF}) \\
\\
\sigma E[\mathbf{1} = \mathbf{v}] \rightarrow \sigma[l/v] E[l] \quad (\text{E-SETREF})
\end{array}$$

Fig. 2. Mutable References in λ_{JS}

2.1 Functions, Objects and State

We begin with a small subset of λ_{JS} specified in figure 1 that includes just functions and objects. We model operations on objects via functional update. This seemingly trivial fragment already exhibits some of JavaScript's quirks:

- In field lookup, the name of the field need not be specified statically; instead, it may be computed at runtime (E-GETFIELD):

```

let (obj = { "x" : 500, "y" : 100 })
  let (select = func(name) { return obj[name] })
    select("x") + select("y")
 $\hookrightarrow^*$  600

```

- A program that looks up a non-existent field does not result in an error; instead, JavaScript returns the value `undefined` (E-GETFIELD-NOTFOUND):

```

{ "x" : 7 }["y"]  $\hookrightarrow$  undefined

```

- Field update in JavaScript is conventional (E-UPDATEFIELD)—

```

{ "x" : 0 }["x"] = 10  $\hookrightarrow$  { "x" : 10 }

```

—but the same syntax also creates new fields (E-CREATEFIELD):

```

{ "x" : 0 }["z"] = 20  $\hookrightarrow$  { "z" : 20, "x" : 10 }

```

- Finally, JavaScript lets us delete fields from objects:

```

delete { "x": 7, "y": 13 }["x"]  $\hookrightarrow$  { "y": 13 }

```

```

function sum(arr) {
  var r = 0;
  for (var i = 0; i < arr["length"]; i = i + 1) {
    r = r + arr[i] };
  return r };

sum([1,2,3]) // returns 6
var a = [1,2,3,4];
delete a["3"];
sum(a) // returns NaN!

```

Fig. 3. Array Processing in JavaScript

Of course, JavaScript also supports a more conventional dotted-field notation: `obj.x` is valid in JavaScript, and is equivalent to `obj["x"]`. To keep λ_{JS} small, we omit the dotted-field notation in favor of the more general computed lookup, and instead explicitly treat dotted fields as syntactic sugar.

Assignment and Imperative Objects JavaScript has two forms of state: objects are mutable, and variables are assignable. We model both variables and imperative objects with conventional mutable references (figure 2). We desugar JavaScript to explicitly allocate and dereference heap-allocated values in λ_{JS} .

Example: JavaScript Arrays JavaScript has arrays that developers can process in a traditional imperative style. However, JavaScript arrays are really objects, and this can lead to unexpected behavior. Figure 3 shows a small example of the use of arrays, which is conventional until just before the end. Deleting the field `a["3"]` (E-DELETEFIELD) does not affect `a["length"]` or shift the array elements. Therefore, in the loop body, `arr["3"]` evaluates to `undefined` (E-GETFIELD-NOTFOUND). Finally, adding `undefined` results in `NaN`; we discuss other quirks of addition in section 2.6.

2.2 Prototype-Based Objects

JavaScript supports *prototype inheritance* [3]. For example, in the following code, `animal` is the prototype of `dog`:

```

var animal = { "length": 13, "width": 7 };
var dog = { "__proto__": animal, "barks": true };

```

Prototypes affect field lookup:

```

dog["length"] // returns 13
dog["width"] // returns 7

var lab = { "__proto__": dog, "length": 2 }

```

$$\begin{array}{c}
\frac{str_x \notin (str_1 \cdots str_n) \quad \text{"_proto_"} \notin (str_1 \cdots str_n)}{\{ str_1 : v_1, \dots, str_n : v_n \} [str_x] \hookrightarrow \text{undefined}} \text{(E-GETFIELD-NOTFOUND)} \\
\\
\frac{str_x \notin (str_1 \cdots str_n)}{\{ str_1 : v_1 \cdots \text{"_proto_"} : p \cdots str_n : v_n \} [str_x] \hookrightarrow (\text{deref } p)[str_x]} \text{(E-GETFIELD-PROTO)}
\end{array}$$

Fig. 4. Prototype-Based Objects

```

lab["length"] // returns 2
lab["width"]  // returns 7
lab["barks"]  // returns true

```

Prototype inheritance does not affect field update. The code below creates the field `dog["width"]`, but it does not affect `animal["width"]`, which `dog` had previously inherited:

```

dog["width"] = 19
dog["width"] // returns 19
animal["width"] // returns 7

```

However, `lab` now inherits `dog["width"]`:

```

lab["width"] // returns 19

```

We specify prototype inheritance with a single reduction rule (figure 4). However, we modify E-GETFIELD-NOTFOUND so that it applies only when the `"_proto_"` field is missing.

Prototype inheritance is simple, but it is obfuscated by JavaScript's syntax. The examples in this section are not standard JavaScript because the `"_proto_"` field is not directly accessible by JavaScript programs.¹ In the next section, we unravel and desugar JavaScript's intended interface to prototypes.

2.3 Prototypes

JavaScript allows programmers to manipulate prototypes indirectly using operators that are reminiscent of class-based languages like Java. In this section, we explain this syntax and its actual semantics. In our semantic treatment of the source language, we account for this syntax by desugaring it to directly manipulate prototypes (section 2.2). Therefore, this section does not grow λ_{JS} and only describes desugaring. Figure 5 specifies the portion of desugaring that is relevant for the rest of this section.²

¹ Some browsers, such as Firefox, can run these examples.

² Figure 5 omits details like variable-arity functions, which aren't relevant here.

```

desugar[[{prop : e ...}]] = ref {
  prop : desugar[[e]]...,
  "__proto__": (deref Object)["prototype"]
}

desugar[[function(x...) { stmt... }]] = ref {
  "code": func(this, x...) { return desugar[[stmt...]] },
  "prototype": ref { "__proto__":
    (deref Object)["prototype"]
  } }

desugar[[new ef(e...)]] =
  let (constr = deref desugar[[ef]]
    obj = ref { "__proto__" : constr["prototype"] })
  constr["code"](obj, desugar[[e]]...);
  obj

desugar[[obj[field](e...)]] =
  let (obj = desugar[[obj]])
  let (f = (deref obj)[field])
  f["code"](obj, desugar[[e]]...)

desugar[[ef(e...)]] =
  let (obj = desugar[[ef]])
  let (func = deref obj)
  func["code"](window, desugar[[e]]...)

desugar[[obj instanceof constr]] =
  let (obj = ref (deref desugar[[obj]]),
    constr = deref desugar[[constr]])
  done: {
    while (deref obj !== null) {
      if ((deref obj).__proto__ === constr.prototype) {
        break done true }
      else { obj = (deref obj).__proto__ } };
    false }

desugar[[this]] = this (an ordinary identifier, bound by functions)

```

Fig. 5. Desugaring JavaScript's Object Syntax


```

var obj = {
  "x" : 0,
  "setX": function(x) { this.x = x } };

window.x // produces undefined
obj.setX(10);
obj.x // produces 10
var f = obj.setX;
f(90);
obj.x // still produces 10!
window.x // produces 90

```

Fig. 6. Implicit `this` Parameter

The `this` Keyword JavaScript does not have conventional methods. Function-valued fields are informally called “methods”, and provide an interpretation for a `this` keyword, but both are quite different from those of, say, Java.

For example, in figure 6, when `obj.setX(10)` is applied, `this` is bound to `obj` in the body of the function. However, in the same figure, although `f` is bound to `obj.setX`, `f(90)` does not behave like a traditional method call. In fact, the function is applied with `this` bound to the *global object* [6, Section 10.1.5].

In general, `this` is an implicit parameter to all JavaScript functions. Its value is determined by the syntactic shape of function applications. Thus, when we desugar functions to λ_{JS} , we make `this` an explicit argument. Moreover, we desugar function calls to explicitly supply a value for `this`.

Functions as Objects In JavaScript, functions are objects with fields:

```

f = function(x) { return x + 1 }
f.y = 90
f(f.y)  $\rightarrow$  91

```

We desugar JavaScript’s `function` to objects in λ_{JS} with a distinguished “`code`” field that refers to the actual function. Therefore, we also desugar application to lookup the “`code`” field.

We could design λ_{JS} so that functions truly are objects, making this bit of desugaring unnecessary. In our experience, JavaScript functions are rarely used as objects. Therefore, our design lets us reason about simple functions when possible, and functions as objects only when necessary.

In addition to the `code` field, which we add by desugaring, and any other fields that may have been created by the programmer, all functions also have a distinguished field called `prototype`. As figure 5 shows, this is a reference to an object that eventually leads to the prototype of `Object`. Unlike the `__proto__` field, `prototype` is accessible and can be mutated by programmers. The combination of its mutability and its use in `instanceof` leads to unpredictable behavior, as we show below.

```

function Dog() { this.barks = "woof" };
function Cat() { this.purrs = "meow" };
dog = new Dog();
cat = new Cat();
dog.barks; // produces "woof"
cat.purrs; // produces "meow"

function animalThing(obj) {
  if (obj instanceof Cat) { return obj.purrs }
  else if (obj instanceof Dog) { return obj.barks }
  else { return "unknown animal" } };

animalThing(dog); // returns "woof"
animalThing(cat); // returns "meow"
animalThing(4234); // returns "unknown animal"

Cat.prototype = Dog.prototype;
animalThing(cat); // returns "unknown animal"
animalThing(dog) // looks up dog.purrs (E-GETFIELD-NOTFOUND)

```

Fig. 7. Using `instanceof`

Constructors and Prototypes JavaScript does not have explicit constructors, but it does have a `new` keyword. `new` invokes a function with `this` bound to a new object. For example, the following code—

```

function Point(x, y) {
  this.x = x;
  this.y = y }

pt = new Point(50, 100)

```

—applies the function `Point`, with its arguments bound as follows:

```

this = { "__proto__": Point.prototype }, x = 50, y = 100

```

Therefore, the prototype of `pt` is `Point.prototype`. We can now observe prototype inheritance, since `new` implicitly set `pt.__proto__`:

```

Point.prototype.getX = function() { return this.x }
pt.getX() → pt.__proto__.getX() → 50

```

In standard JavaScript, because the `__proto__` field is not exposed, the only way to set up a prototype hierarchy is via a function's `prototype` field.

The `instanceof` Operator JavaScript's `instanceof` operator has an unconventional semantics that reflects the peculiar notion of constructors that we have already discussed. In most languages, a programmer might expect that if `x` is

bound to the value created by `new Constr(...)`, then `x instanceof Constr` is true. In JavaScript, however, this invariant does not apply.

For example, in figure 7, `animalThing` dispatches on the type of its argument using `instanceof`. However, after we set `Cat.prototype = Dog.prototype`, the type structure seems to break down. The resulting behavior might appear unintuitive in JavaScript, but it is straightforward when we desugar `instanceof` into λ_{JS} . In essence, `cat instanceof Cat` is `cat.__proto__ === Cat.prototype`. In the figure, before `Cat.prototype = Dog.prototype` is evaluated, the following are true:

```
cat.__proto__ === Cat.prototype
dog.__proto__ === Dog.prototype
Cat.prototype !== Dog.prototype
```

However, after we update `Cat.prototype`, we have:

```
cat.__proto__ === the previous value of Cat.prototype
dog.__proto__ === Dog.prototype
Cat.prototype === Dog.prototype
```

Hence, `cat instanceof Cat` becomes `false`. Furthermore, since `animalThing` first tests for `Cat`, the test `dog instanceof Cat` succeeds.

2.4 Statements and Control Operators

JavaScript has a plethora of control statements. Many map directly to λ_{JS} 's control operators (figure 8), while the rest are easily desugared.

For example, consider JavaScript's `return` and `break` statements. `break` transfers control to a local label. `return` transfers control to the end of the local function and produces a result. Instead of two control operators that are almost identical, λ_{JS} has a single `break` expression that produces a value.

Concretely, we elaborate JavaScript's functions to begin with a label `ret`:

```
desugar[function(x...) { stmt... }] =
  func(this x...) { return ret: { desugar[stmt...] } }
```

Thus, `return` statements can be desugared to `break ret`:

$$desugar[\text{return } e] = \text{break ret } desugar[e]$$

while `break` statements are desugared to produce `undefined`:

$$desugar[\text{break label}] = \text{break label undefined}$$

2.5 Static Scope in JavaScript

The JavaScript standard specifies identifier lookup in an unconventional manner [6, Section 10.1.4]. It uses neither substitution nor environments, but *scope objects*. A scope object is akin to an activation record, but is a conventional JavaScript object. The fields of this object are interpreted as variable bindings.

$$\begin{aligned}
& \text{label} = (\text{Labels}) \\
& e = \dots \mid \text{if } (e) \{ e \} \text{ else } \{ e \} \mid e; e \mid \text{while}(e) \{ e \} \mid \text{label}:\{ e \} \\
& \quad \mid \text{break label } e \mid \text{try } \{ e \} \text{ catch } (x) \{ e \} \mid \text{try } \{ e \} \text{ finally } \{ e \} \\
& \quad \mid \text{err } v \\
& E = \dots \mid \text{if } (E) \{ e \} \text{ else } \{ e \} \mid E; e \mid \text{label}:\{ E \} \\
& \quad \mid \text{try } \{ E \} \text{ catch } (x) \{ e \} \mid \text{try } \{ E \} \text{ finally } \{ e \} \\
& \quad \mid \text{delete } E[e] \mid \text{delete } v[E] \\
& E' = \bullet \mid \text{let } (x = v \dots x = E', x = e \dots) e \mid E'(e \dots) \mid v(v \dots E', e \dots) \\
& \quad \mid \text{if } (E') \{ e \} \text{ else } \{ e \} \mid \{ \text{str}: v \dots \text{str}: E', \text{str}: e \dots \} \\
& \quad \mid E'[e] \mid v[E'] \mid E'[e] = e \mid v[E'] = e \mid v[v] = E' \mid E' = e \mid v = E' \\
& \quad \mid \text{delete } E'[e] \mid \text{delete } v[E'] \mid \text{ref } E' \mid \text{deref } E' \mid E'; e \\
& F = E' \mid \text{label}:\{ F \} \quad (\text{Exception Contexts}) \\
& G = E' \mid \text{try } \{ G \} \text{ catch } (x) \{ e \} \quad (\text{Local Jump Contexts})
\end{aligned}$$

$$\begin{aligned}
& \text{if } (\text{true}) \{ e_1 \} \text{ else } \{ e_2 \} \hookrightarrow e_1 & (\text{E-IFTRUE}) \\
& \text{if } (\text{false}) \{ e_1 \} \text{ else } \{ e_2 \} \hookrightarrow e_2 & (\text{E-IFFALSE}) \\
& v; e \hookrightarrow e & (\text{E-BEGIN-DISCARD}) \\
& \text{while}(e_1) \{ e_2 \} \hookrightarrow \text{if } (e_1) \{ e_2; \text{while}(e_1) \{ e_2 \} \} \text{ else } \{ \text{undefined} \} & (\text{E-WHILE}) \\
& \text{throw } v \hookrightarrow \text{err } v & (\text{E-THROW}) \\
& \text{try } \{ F[\text{err } v] \} \text{ catch } (x) \{ e \} \hookrightarrow e[x/v] & (\text{E-CATCH}) \\
& \sigma F[\text{err } v] \rightarrow \sigma \text{err } v & (\text{E-UNCAUGHT-EXCEPTION}) \\
& \text{try } \{ F[\text{err } v] \} \text{ finally } \{ e \} \hookrightarrow e; \text{err } v & (\text{E-FINALLY-ERROR}) \\
& \text{try } \{ G[\text{break } v] \} \text{ finally } \{ e \} \hookrightarrow e; \text{break } v & (\text{E-FINALLY-BREAK}) \\
& \text{try } \{ v \} \text{ finally } \{ e \} \hookrightarrow e; v & (\text{E-FINALLY-POP}) \\
& \text{label}:\{ G[\text{break label } v] \} \hookrightarrow v & (\text{E-BREAK}) \\
& \frac{\text{label}_1 \neq \text{label}_2}{\text{label}_1:\{ G[\text{break label}_2 v] \} \hookrightarrow \text{break } v} & (\text{E-BREAK-POP}) \\
& \text{label}:\{ v \} \hookrightarrow v & (\text{E-LABEL-POP})
\end{aligned}$$

Fig. 8. Control operators for λ_{JS}

In addition, a scope object has a distinguished parent-field that references another scope object (the global scope object’s parent-field is `null`). This linked list of scope objects is called a *scope chain*. The value of an identifier `x` is the value of the first `x`-field in the *current scope chain*. When a new variable `y` is defined, the field `y` is added to the scope object at the head of the scope chain.

Since scope objects are ordinary JavaScript objects, JavaScript’s `with` statement (discussed below) lets us add arbitrary objects to the scope chain. Given `with`, and other features discussed below, it is not clear whether JavaScript is lexically scoped. In this section, we describe how JavaScript’s scope-manipulation statements are desugared into λ_{JS} , which is obviously lexically scoped. Therefore, we present a complete, lexical account of JavaScript.

Local Variables In JavaScript, functions close over their current scope chain (intuitively, their static environment). Applying a closure sets the current scope chain to be that in the closure. In addition, an empty scope object is added to the head of the scope chain. The function’s arguments and local variables (introduced using `var`) are properties of this scope object.

Local variables are automatically lifted to the top of the function. As a result, in a fragment such as this—

```
function foo() {
  if (true) { var x = 10; }
  return x }

foo() // returns 10
```

—the `return` statement has access to the variable that appeared to be defined inside a branch of the `if`. This can result in somewhat unintuitive answers:

```
function bar() {
  x = 10;
  var x = x * x;
  return x }

bar() // returns 100
x // error: unbound identifier
```

The programmer might expect that the first statement of the function sets the value of the top-level `x` (and creates it if it doesn’t exist). However, the lifting of the second statement results in the function application evaluating to 100 and there being no `x` added to the top-level.

We can easily give a lexical account of this behavior. All local variable declarations `var x = e` are desugared into simple assignments, `x = e`. Furthermore, locals are desugared to let-bindings at the top of functions:

```
let (x = ref undefined) ...
```

Global Variables Global variables are more subtle. Global variables are properties of the root scope object, called `window` in Web browsers. `window` has a field `window.window` that references itself:

```
window.window === window // returns true
```

Therefore, a program can obtain a reference to the global scope object by simply writing `window`.³

As a consequence, globals seem to break lexical scope, since we can observe that they are properties of `window`:

```
var x = 0;
window.x = 50;
x // returns 50
x = 100;
window.x // returns 100
```

However, `window` is the only scope object that is directly accessible to JavaScript programs [6, Section 10.1.6]. We can maintain lexical scope by abandoning global variables. That is, we simply desugar the obtuse code above to the following:

```
window.x = 0;
window.x = 50;
window.x // returns 50
window.x = 100;
window.x // returns 100
```

Although global variables observably manipulate `window`, local variables are still lexically scoped. We can thus reason about local variables using substitution, α -renaming, and other standard techniques.

With Statements The `with` statement is a widely-acknowledged JavaScript wart. `with` adds an arbitrary object to the front of the scope chain:

```
function(x, obj) {
  with(obj) {
    x = 50; // if obj.x exists, then obj.x = 50, else x = 50
    return y } } // similarly, return either obj.y, or window.y
```

We can desugar `with` by turning the comments above into code:

```
function(x, obj) {
  if (obj.hasOwnProperty("x")) {
    obj.x = 50 }
  else {
    x = 50 }
  if (obj.hasOwnProperty("y")) {
    return obj.y }
  else {
    return window.y } }
```

³ In addition, `this` is bound to `window` in function applications (figure 5).

$$\begin{aligned}
e &= \dots \mid op_n(e_1 \dots e_n) \\
E &= \dots \mid op_n(v \dots E \ e \dots) \\
E' &= \dots \mid op_n(v \dots E' e \dots) \\
\delta_n &: op_n \times v_1 \dots v_n \rightarrow c + err \\
op_n(v_1 \dots v_n) &\hookrightarrow \delta_n(op_n, v_1 \dots v_n) \quad (\text{E-PRIM})
\end{aligned}$$

Fig. 9. Primitive Operators

Nested `with`s require a little more care, but are essentially the same. Desugaring `with` in this manner is correct, but is non-compositional. We will return to this point in section 4.3.

What are Scope Objects? Various authors (including ourselves) have developed JavaScript tools that assume JavaScript is lexically scoped (e.g., [2, 10, 11]). Other tools restrict themselves to a subset of JavaScript that is intuitively lexically scoped (e.g., [5, 7, 17]). We show that JavaScript is lexically scoped, validating these assumptions. As a result, we no longer need scope objects in the specification; they may instead be viewed as an implementation strategy.⁴

2.6 Type Conversions and Primitive Operators

JavaScript is not a pure object language. We can observe the difference between primitive numbers and number objects:

```

x = 10;
y = new Number(7)
typeof x // returns "number"
typeof y // returns "object"

```

Moreover, JavaScript's operators include implicit casts and type conversions between primitives and corresponding objects:

```

x + y // returns 17

```

However, we can redefine basic type conversions:

```

Number.prototype.valueOf = function() { return 0 }
x + y // returns 10

```

The object `y` still contains the value 7. Also, `+` is overloaded to concatenate strings, and both `+` and `*` perform implicit coercions:

```

y.toString() // returns "7"
x + y.toString() // returns "107" (x converted to string)
x * y.toString() // returns 70 ("7" converted to number)

```

⁴ Scope objects are especially well suited for implementing `with`. Our desugaring strategy for `with` increases code-size linearly in the number of nested `with`s.

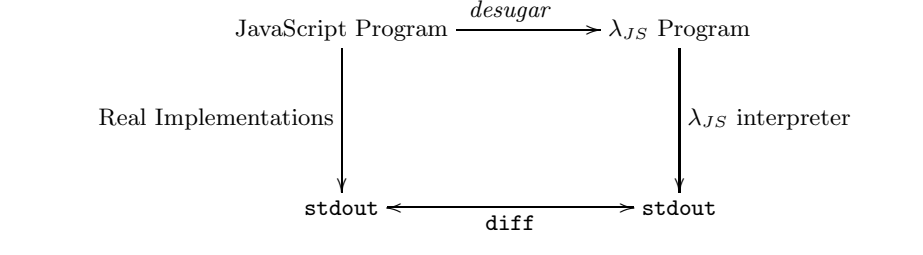


Fig. 10. Testing Strategy for λ_{JS}

This suggests that JavaScript’s operators are complicated. Indeed, $x + y$ is specified by a 15-step algorithm that refers to three pages of metafunctions. Buried in these details are four primitive operators: primitive addition, string concatenation, and number-to-string and string-to-number type coercions.

These four primitives are essential and intuitive. We therefore model them with a conventional δ function (figure 9). The remaining details of operators are simply type-tests and method invocations: as the examples above suggest, JavaScript internally performs operations such as `y.valueOf()` and `typeof x`. In λ_{JS} we desugar JavaScript’s operators, making these type-tests and method calls explicit.

This paper does not enumerate all the primitives that λ_{JS} needs. Instead, the type of δ constrains their behavior significantly, which often lets us reason with arbitrary δ functions.

3 Soundness and Adequacy of λ_{JS}

Soundness We mechanize λ_{JS} with PLT Redex. The process of mechanization did help us find errors in our semantics, particularly in the interactions of control operators (figure 8). We use our mechanized semantics to test λ_{JS} for safety [14]:

Property 1 (Progress) *If σe is a closed, well-formed configuration, then either:*

- $e \in v$,
- $e = \mathbf{err} v$, or
- $\sigma e \rightarrow \sigma' e$, where $\sigma' e$ is a closed, well-formed configuration.

This property requires additional evaluation rules for runtime type errors, and definitions of well-formedness. We elide them from the paper, as they are conventional. The supplemental material contains these details.

Adequacy λ_{JS} is a semantics for the core of JavaScript. We have described how it models many aspects of the language’s semantics, warts and all. Ultimately, however, a small core language has limited value to those who want to reason about programs written in JavaScript, with its many syntactic forms.

Syntactic Form	Occurrences (approx.)
with blocks	15
var statements	500
try blocks	20
functions	200
if and switch statements	90
typeof and instanceof	35
new expressions	50
Math library functions	15

Fig. 11. Test Suite Coverage

As the paper has discussed, we employ an explicit desugaring operation to map JavaScript into λ_{JS} , with full details given in the supplemental material. Given this method of handling all of JavaScript, we are now obliged to show that desugaring and the semantics enjoy two properties. First, we should show that all of JavaScript is handled in this manner:

Claim 1 (Desugaring is Total) *For all JavaScript programs e , $\text{desugar}\llbracket e \rrbracket$ is defined.*

We must also demonstrate that our semantics corresponds to what JavaScript implementations actually do:

Claim 2 (Desugar Commutes with Eval) *For all JavaScript programs e , $\text{desugar}\llbracket \text{eval}_{JavaScript}(e) \rrbracket = \text{eval}_{\lambda_{JS}}(\text{desugar}\llbracket e \rrbracket)$.*

We could try to prove the latter claim, but that just begs the question: What is $\text{eval}_{JavaScript}$? A semantics based on the specification would itself require evidence of its adequacy.

In practice, JavaScript is truly defined by its major implementations. Open-source Web browsers are accompanied by extensive JavaScript test suites. These test suites help the tacit standardization of JavaScript across major implementations.⁵ We use these test suites to *test* our semantics.

Figure 10 outlines our testing strategy. We first define an interpreter for λ_{JS} . This is a straightforward exercise; the interpreter is a mere 100 LOC, and easy to inspect since it is based directly on the semantics. Then, for any JavaScript program, we should be able to to run it both directly and in our semantics. For direct execution we employ three JavaScript implementations: SpiderMonkey (used by Firefox), V8 (used by Chrome), and Rhino (an implementation in Java). We desugar the same program into λ_{JS} and run the result through our interpreter. We then check whether our λ_{JS} interpreter produces the same output as each JavaScript implementation.

Our tests cases are a significant portion of the Mozilla JavaScript test suite. We omit the following tests:

⁵ For example, the Firefox JavaScript test suite is also found in the Safari source.

- Those that target Firefox-specific JavaScript extensions.
- Those that use `eval`.
- Those that target corner cases of library details, such as regular expressions.

The remaining tests are about 5,000 LOC. We make absolutely no modifications to these files.

Our λ_{JS} interpreter produces exactly the same output as Rhino, V8, and SpiderMonkey. Figure 11 indicates that these tests employ many interesting syntactic forms, including statements like `with` and `switch` that are considered complicated. We make the following observations:

- No prior semantics for JavaScript accounts for all these forms (e.g., Maffei et al. [15] do not model `switch`).
- We account for much of JavaScript by desugaring. Therefore, these tests validate both our core semantics and our desugaring strategy.
- These tests give us confidence that our implemented tools are correct.

In the next section, we demonstrate that λ_{JS} is *useful*. We give a succinct proof that a safe subset with a “security wrapper” preserves the desired property.

4 Example: Language-Based Sandboxing

Web platforms often combine programs from several different sources on the same page. For instance, on a portal page like iGoogle, a user can combine a weather widget with a stock ticker widget; on Facebook, users can run applications. Unfortunately, this means programs from different authors can in principle examine data from one another, which creates the possibility that a malicious application may steal data or create other harm. To prevent both accidents and malice, these sites need to run each widget or application in a sandbox.

To this end, corporations have defined *safe subsets* of JavaScript like Caja [17] and Facebook JavaScript (FBJS) [7]. These are designed as subsets—rather than as whole new languages with, perhaps, security types—to target developers who already know how to write JavaScript Web applications. These subsets disallow blatantly dangerous features such as `eval`. However, these subsets intend to also establish more subtle security properties, which they attempt to enforce using runtime checks that they insert into untrusted code. Naturally, this raises the question of whether these subsets function as advertised.

Let us consider the following property, which is inspired by FBJS and Caja: we wish to prevent code in the sandbox from communicating with a server. For instance, we intend to block the `XMLHttpRequest` object:

```
var x = new window.XMLHttpRequest()
x.open("GET", "/get_confidential", false)
x.send("");
var result = x.responseText
```

For simplicity, we will construct a subset that only disallows access to `XMLHttpRequest`. A complete solution would use our techniques to block other communication mechanisms, such as `document.write` and `Element.innerHTML`.

```

lookup = func(obj, field) {
  return if (field === "XMLHttpRequest") { undefined }
        else { (deref obj)[field] }
}

```

Fig. 12. Safe Wrapper for λ_{JS}

4.1 Isolating JavaScript

Let us begin with short, type-based proofs that exploit the compactness of λ_{JS} . We will then use our tools to migrate from λ_{JS} to JavaScript.

First, we need to precisely state “disallow access to XMLHTTPRequest”. In JavaScript, `window.XMLHttpRequest` references the XMLHTTPRequest constructor, where `window` names the global object. We make two assumptions:

- In λ_{JS} , we allocate the global object at location 0. This is a convenient convention that is easily ensured by desugaring.
- We assume that the XMLHTTPRequest constructor is only accessible as a property of the global object. This assumption is valid as long as we do not use untrusted libraries (or can analyze their code).

Given these two assumptions, we can formally state “disallow access to XMLHTTPRequest” as a property of λ_{JS} programs:

Definition 1 (Safety) *e is safe if $e \neq E[(\text{deref } (\text{ref } 0))][\text{"XMLHttpRequest"}]$.*

Note that in the definition above, the active expression is `(deref (ref 0))`, and the evaluation context is $E[\bullet[\text{"XMLHttpRequest"}]]$.

Intuitively, ensuring safety appears to be easy. Given an untrusted λ_{JS} program, we can elaborate property accesses, $e_1[e_2]$, to $\text{lookup}(e_1, e_2)$, where lookup is defined in Figure 12.

This technique⁶ has two problems. First, this elaboration does not allow access to the `"XMLHttpRequest"` property of *any* object, rather than the property of that name of `window`. Second, lookup may appear “obviously correct”. However, the actual wrapping in Caja, FBJS, and other subsets occurs in the source language, not in a core calculus like λ_{JS} ; but lookup does not directly correspond to any JavaScript function. We could write a JavaScript function that loosely resembles lookup , but it would be wrought with various implicit type conversions and method calls (section 2.6) that could break its intended behavior. Thus, we will first prove safety for λ_{JS} before tackling JavaScript’s details.

4.2 Types for Securing λ_{JS}

Our goal is to determine whether a λ_{JS} program is safe (definition 1). We wish to do this without making unnecessary assumptions. In particular, we do not assume that lookup (figure 12) is itself safe.

⁶ Maffei et al.’s blacklisting [16], based on techniques used in FBJS, has this form.

$T = \mathbf{JS}$

$$\Gamma \vdash \text{string} : \mathbf{JS} \quad (\text{T-STRING})$$

$$\frac{\Gamma(x) = T}{\Gamma \vdash x : T} \quad (\text{T-ID})$$

$$\frac{\Gamma, x_1 : \mathbf{JS}, \dots, x_n : \mathbf{JS} \vdash e : \mathbf{JS}}{\Gamma \vdash \text{func } (x_1 \dots x_n) \{ \text{return } e \} : \mathbf{JS}} \quad (\text{T-FUN})$$

$$\frac{\Gamma \vdash e_1 : \mathbf{JS} \quad \dots \quad \Gamma \vdash e_n : \mathbf{JS}}{\Gamma \vdash \delta_n(\text{op}_n, e_1 \dots e_n) : \mathbf{JS}} \quad (\text{T-PRIM})$$

The type judgements for remaining forms are similar to T-PRIM and T-FUN: namely, $\Gamma \vdash e : \mathbf{JS}$ if all subexpressions of e have type \mathbf{JS} . However, $e_1[e_2]$ is not typable.

Fig. 13. Type System that Disallows Field Lookup

We begin by statically disallowing *all* field accesses. The trivial type system in Figure 13 achieves this, since it excludes a typing rule for $e_1[e_2]$. This type system does not catch conventional type errors. Instead, it has a single type, \mathbf{JS} , of statically safe JavaScript expressions (definition 1). The following theorem is evidently true:

Theorem 1 *For all λ_{JS} expressions e , if $\cdot \vdash e : T$, and $e \rightarrow e'$, then $e' \neq E[(\text{deref } 0)]["XMLHttpRequest"]$.*

We need to extend our type system to account for *lookup*, taking care not to violate theorem 1. Note that *lookup* is currently untypable, since field access is untypable. However, the conditional in *lookup* seems to ensure safety; our goal is to prove that it does.

Our extended type system is shown in figure 14. The new type, **NotXHR**, is for expressions that provably do not evaluate to the string "XMLHttpRequest". Since primitives like string concatenation yield values of type \mathbf{JS} (T-PRIM in figure 13), programs cannot manufacture unsafe strings with type **NotXHR**. (Of course, trusted primitives could yield values of type **NotXHR**.)

Note this important peculiarity: *These new typing rules are purpose-built for lookup*. There are other ways to establish safe access to fields. However, since we will rewrite all expressions $e_1[e_2]$ to $\text{lookup}(e_1, e_2)$, our type system need only account for the syntactic structure of *lookup*.

Our extended type system admits *lookup*, but we must prove theorem 1. It is sufficient to prove the following lemmas:⁷

Lemma 1 (Safety) *If $\cdot \vdash e : \mathbf{JS}$, then $e \neq E[v["XMLHttpRequest"]]$, for any value v .*

⁷ Additional proof details are in the supplemental material.

$T = \dots \mid \text{NotXHR}$

$$\begin{array}{c}
\text{NotXHR} <: \text{JS} \quad (\text{SUB-SAFE}) \\
\\
\frac{v \neq \text{"XMLHttpRequest"}}{\Gamma \vdash v : \text{NotXHR}} \quad (\text{T-SAFEVALUE}) \\
\\
\frac{\Gamma \vdash e_1 : \text{JS} \quad \Gamma \vdash e_2 : \text{NotXHR}}{\Gamma \vdash e_1[e_2] : \text{JS}} \quad (\text{T-GETFIELD}) \\
\\
\frac{x \in \text{dom}(\Gamma) \quad \Gamma \vdash e_2 : \text{JS} \quad \Gamma[x : \text{NotXHR}] \vdash e_3 : \text{JS}}{\Gamma \vdash \text{if } x === \text{"XMLHttpRequest"} \text{ then } e_2 \text{ else } e_3 : \text{JS}} \quad (\text{T-IFSAFE})
\end{array}$$

Fig. 14. Type System for Blocking Access to XMLHttpRequest

$$\begin{array}{c}
\frac{\Gamma \vdash e_2 : \text{JS}}{\Gamma \vdash \text{if } (\text{"XMLHttpRequest"} === \text{"XMLHttpRequest"}) \{ e_2 \} \text{ else } \{ e_3 \} : \text{JS}} \quad (\text{T-IFTRUE-XHR}) \\
\\
\frac{\Gamma \vdash e_2 : \text{JS}}{\Gamma \vdash \text{if } (\text{true}) \{ e_2 \} \text{ else } \{ e_3 \} : \text{JS}} \quad (\text{T-IFTRUE})
\end{array}$$

Fig. 15. Auxiliary Typing Rules for Blocking Access to XMLHttpRequest

The proof of this lemma is by induction on typing derivations, given the typing rules in figure 13 and figure 14. This lemma also holds for the typing rules in figure 15, which we introduce below.

Lemma 2 (Subject Reduction) *If $\cdot \vdash e : \text{JS}$, and $e \rightarrow e'$, then $\cdot \vdash e' : \text{JS}$.*

Proof Technique This is a conventional subject reduction proof. However, the typing rules for *lookup* (figure 14) require a technique introduced in *occurrence typing* for Typed Scheme [18].

Note that *lookup* is typable, but subject reduction requires all expressions in this reduction sequence to be typable:

```

lookup(window, "XMLHttpRequest")
→ if ("XMLHttpRequest" === "XMLHttpRequest") { undefined }
  else { (deref window)["XMLHttpRequest"] }
→ if (true) { undefined }
  else { (deref window)["XMLHttpRequest"] }
→ undefined

```

The intermediate expressions above are not typable, although they are intuitively safe. We can make them typable by extending our type system with the typing rules in figure 15, which let us prove subject reduction.

However, we have to ensure that our new typing rules do not violate safety (lemma 1). Intuitively, lemma 1 still holds, since our newly-typable expressions are not of the form $v["XMLHttpRequest"]$.

Our type system may appear ad hoc, but it simply reflects the nature of JavaScript security solutions. Note that our type system is merely a means to an end: the main result is the conclusion of theorem 1, which is a property of the runtime semantics.

4.3 Scaling to JavaScript

Since we can easily implement a checker for our type system,⁸ we might claim we have a result for JavaScript as follows: desugar JavaScript into λ_{JS} and type-check the resultant λ_{JS} code. This strategy is, however, unsatisfying because seemingly harmless changes to a JavaScript source that type-checks may result in a program that fails to type-check, due to the effects of desugaring. This would make the language appear whimsical to the widget developer.

Instead, our goal is to define a safe sub-language (just as, say, Caja and FBJS do). This safe sub-language would provide syntactic safety criteria, such as:

- The JavaScript expression $e_1 + e_2$ is safe when its subexpressions are safe.
- $e_1[e_2]$, when rewritten to $lookup(e_1, e_2)$, is safe, but will fail if e_2 evaluates to `"XMLHttpRequest"`.

Our plan is as follows. We focus on the *structure* of the desugaring rules and show that a particular kind of compositionality in these rules suffices for showing safety. We will illustrate this process by extending the λ_{JS} result to include JavaScript's addition (which, as we explained in section 2.6, is non-trivial). We will then generalize this process to the rest of the language.

Safety for e_1+e_2 By theorem 1, it is sufficient to determine whether $\Gamma \vdash desugar[e_1+e_2] : \mathbf{JS}$. Proving this, however, would benefit from some constraints on e_1 and e_2 . Consider the following proposition:

Proposition 1 *If $\Gamma \vdash desugar[e_1] : \mathbf{JS}$ and $\Gamma \vdash desugar[e_2] : \mathbf{JS}$, then $\Gamma \vdash desugar[e_1+e_2] : \mathbf{JS}$.*

By lemma 1, this proposition entails that if e_1 and e_2 are safe, then e_1+e_2 is safe. But is the proposition true? $desugar[e_1+e_2]$ produces an unwieldy λ_{JS} expression with explicit type-conversions and method calls. Still, a quick inspection of our implementation shows that:

$$desugar[e_1 + e_2] = \text{let } (x = desugar[e_1], y = desugar[e_2])$$

...

⁸ The supplemental material includes a 150-line implementation.

$\text{desugar}[[e_1 + e_2]]$ simply recurs on its subexpressions and does not examine the result of $\text{desugar}[[e_1]]$ and $\text{desugar}[[e_2]]$. Moreover, the elided body does not contain additional occurrences of $\text{desugar}[[e_1]]$ and $\text{desugar}[[e_2]]$. Thus, we can write the right-hand side as a two-holed *program context*:⁹

$$\begin{aligned} C_+ &= \text{let } (\mathbf{x} = \bullet_1, \mathbf{y} = \bullet_2) \\ &\quad \dots \\ \text{desugar}[[e_1 + e_2]] &= C_+[\text{desugar}[[e_1]], \text{desugar}[[e_2]]] \end{aligned}$$

Therefore, desugaring $e_1 + e_2$ is *compositional*.

A simple replacement lemma [20] holds for our type system:

Lemma 3 (Replacement) *If:*

- i. \mathcal{D} is a deduction concluding $\Gamma \vdash C[e_1, e_2] : \mathbf{JS}$,
- ii. Subdeductions $\mathcal{D}_1, \mathcal{D}_2$ prove that $\Gamma_1 \vdash e_1 : \mathbf{JS}$ and $\Gamma_2 \vdash e_2 : \mathbf{JS}$ respectively,
- iii. \mathcal{D}_1 occurs in \mathcal{D} , at the position corresponding to \bullet_1 , and \mathcal{D}_2 at the position corresponding to \bullet_2 , and
- iv. $\Gamma_1 \vdash e'_1 : \mathbf{JS}$ and $\Gamma_2 \vdash e'_2 : \mathbf{JS}$,

then $\Gamma \vdash C[e'_1, e'_2] : \mathbf{JS}$.

Replacement, along with weakening of environments, gives us:

Lemma 4 *If:*

- $x : \mathbf{JS}, y : \mathbf{JS} \vdash C_+[x, y] : \mathbf{JS}$, and
- $\Gamma \vdash \text{desugar}[[e_1]] : \mathbf{JS}$ and $\Gamma \vdash \text{desugar}[[e_2]] : \mathbf{JS}$,

then $\Gamma \vdash C_+[\text{desugar}[[e_1]], \text{desugar}[[e_2]]] : \mathbf{JS}$.

The conclusion of lemma 4 is the conclusion of proposition 1. The second hypothesis of lemma 4 is the only hypothesis of proposition 1. Therefore, to prove proposition 1, we simply need to prove $x : \mathbf{JS}, y : \mathbf{JS} \vdash C_+[x, y] : \mathbf{JS}$.

We establish this using our tools. We assume \mathbf{x} and \mathbf{y} are safe (i.e., have type \mathbf{JS}), and desugar and type-check the expression $\mathbf{x} + \mathbf{y}$. Because this succeeds, the machinery above—in particular, the replacement lemma—tells us that we may admit $+$ into our safe subset.

A Safe Subset of JavaScript The proofs of lemma 3 and 4 do not rely on the definition of C_+ . For each construct, we must thus ensure that the desugaring rule can be written as a program context, which we easily verify by inspection. We find this true for all syntactic forms other than **with**, which we omit from our safe subset (as do other subsets such as Caja and FBJS). If **with** were considered important, we could extend our machinery to find under what circumstances, or with what wrapping, it too could be considered safe.

⁹ Due to lack of space, we do not formally define program contexts for λ_{JS} in this paper, but evaluation contexts offer a strong hint.

Having checked the structure of the desugaring rules, we must still establish that their expansion does no harm. We mechanically populate a type environment with placeholder variables, create expressions of each kind, and type-check. All forms pass type-checking, except for the following:

- `x[y]` and `x.XMLHttpRequest` do not type—happily, as they are unsafe! This is acceptable because these unsafe forms will be wrapped in *lookup*.
- However, `x[y]++`, the corresponding pre-increment, and corresponding decrementing versions, also fail to type due to the structure of code they generate on desugaring. Yet, we believe these forms are safe; we can account for them with additional typing rules, as employed below for *lookup*.

Safety for *lookup* As section 4.2 explained, we designed our type system to account for *lookup* (figure 12). However, *lookup* is in λ_{JS} , whereas we need a corresponding wrapper in JavaScript. A direct translation of *lookup* into JavaScript would yield this:

```
lookupJS = function(obj, field) {
  if (field === "XMLHttpRequest") { return undefined }
  else { return obj[field] } }
```

Since *lookupJS* is a closed expression that is inserted as-is into untrusted scripts, we can desugar and type-check it in isolation. When we did so, however, we were surprised to find that *desugar*[[*lookupJS*]] did not type...

When we examine the generated λ_{JS} code, we see that `obj[field]` is desugared into an expression that explicitly converts `field` to a string. (Recall that field names are strings.) If, however, `field` is itself an object, this conversion includes the method call `field.toString()`. Working backward, we see that the following exploit would succeed:

```
lookupJS(window,
  {toString: function() {return "XMLHttpRequest"}})
```

where the second argument to *lookupJS* (i.e., the expression in the field position) is a literal object that has a single method, `toString`, which returns "XMLHttpRequest". Thus, not only does *lookupJS* not type, it truly is unsafe!

Our type system successfully caught a bug in our JavaScript implementation of *lookup*. The fix is simple: ensure that `field` is a primitive string:

```
safeLookup = function(obj, field) {
  if (field === "XMLHttpRequest") { return undefined }
  else if (typeof field === "string") { return obj[field] }
  else { return undefined } }
```

This code truly is safe, though to prove it we need to extend our type system. We design the extension by studying the result of desugaring *safeLookup*.¹⁰

¹⁰ Desugaring produces 200 LOC of pretty-printed λ_{JS} . We omit this code from the paper, but make it available online.

We have noted that desugaring evinces the unsafe call to `field.toString()`. However, `toString` cannot be applied indiscriminately: if `field` is a primitive constant and not an object, the application will fail. Therefore, in the desugared λ_{JS} code, `field.toString()` is guarded by a conditional inserted *by desugaring*:

```
if (typeof field === "location") { ... field.toString() ... }
else { field }
```

Thus, the second if in *safeLookup* desugars to:

```
if (typeof field === "string") {
  obj[if (typeof field === "location")
    { ... field.toString() ... }
    else { field }] }
```

To now reach `field.toString()`, both conditions must hold. This cannot happen in λ_{JS} because identifiers are immutable. Therefore, the unsafe code block truly is unreachable.

Recall, however, that we designed our type system for λ_{JS} around the syntactic structure of the lookup guard. With this more complex guard, we must extend our type system to employ if-splitting—which we already used in section 4.2—a second time. As long as our extension does not violate safety (lemma 1) and subject reduction (lemma 2), the arguments in this section still hold.

4.4 Perspective

In the preceding sections, we rigorously developed a safe subset of JavaScript that disallows access to `XMLHttpRequest`. In addition, we proved that inserted runtime “wrappers” are correct. To enhance isolation, we have to disallow access to a few other properties, such as `document.write` and `Element.innerHTML`. Straightforward variants of the statements and proofs in this section could verify such systems. We believe our approach can scale to tackle more sophisticated security properties as well.

Nevertheless, our primary goal in this section is not to define a subset with some security property, but rather to showcase our semantics and tools:

- λ_{JS} is small. It is much smaller than other definitions and semantics for JavaScript. Therefore, our proofs are tractable.
- λ_{JS} is adequate and tested. This gives us confidence that our arguments are applicable to real-world JavaScript.
- λ_{JS} is conventional, so we are free to use standard type-soundness techniques [20]. In contrast, working with JavaScript’s scope objects would be onerous. This section is littered with statements of the form $\Gamma \vdash e : \mathbf{JS}$. The heap-allocated scope objects would preclude the straightforward use of Γ , thus complicating the proof effort (and perhaps requiring new techniques).
- Finally, *desugar* is compositional. Although we developed a type system for λ_{JS} , we were able to apply our results to most of JavaScript by exploiting the compositionality of *desugar*.

5 Related Work

Types for JavaScript There are various proposed type systems for JavaScript that are accompanied by semantics. However, these semantics are only defined for small subsets of JavaScript, not the language in its entirety. For example, Anderson et al. [2] develop a type system and a type inference algorithm for JS_0 , a subset of JavaScript that excludes prototypes and first-class functions. Heidegger and Thiemann’s recency types [11] admit prototypes and first-class functions, but omit assignment. Moreover, their language is syntactically restricted to A-normal form. We have found it non-obvious to define a semantics-preserving transformation from JavaScript’s surface syntax to ANF. In contrast, λ_{JS} and desugaring account for all of JavaScript.

JavaScript Semantics JavaScript is specified in 200 pages of prose and pseudocode [6]. This specification is barely amenable to informal study, let alone proofs. Maffeis, Mitchell, and Taly [15] present a 30-page operational semantics, based directly on the JavaScript specification. Their semantics covers most of JavaScript directly, but does omit a few syntactic forms.

Our approach is drastically different. λ_{JS} is a semantics for the core of JavaScript, though we desugar the rest of JavaScript into λ_{JS} . In section 3, we present evidence that our strategy is correct. λ_{JS} and desugaring together are much smaller and simpler than the semantics presented by Maffeis, et al. Yet, we cover all of JavaScript (other than `eval`) and account for a substantial portion of the standard libraries as well.

Maffeis, et al. demonstrate adequacy by following the standard, though they discuss various differences between the standard and implementations. In section 3, we demonstrate adequacy by running 3rd-party JavaScript tests in λ_{JS} and comparing results with mainstream JavaScript implementations.

A technical advantage of our semantics is that it is conventional. For example, we use substitution instead of scope objects (section 2.5). Therefore, we can use conventional techniques, such as subject reduction, to reason in λ_{JS} . It is unclear how to build type systems with proofs for a semantics that uses scope objects.

David Herman defines a CEKS machine for a small portion of JavaScript [12]. This machine is also based on the standard and inherits some of its complexities, such as implicit type conversions.

CoreScript [21] models an imperative subset of JavaScript, along with portions of the DOM, but omits essentials such as functions and objects. Moreover, their big-step semantics is not easily amenable to typical type safety proofs.

Object Calculi λ_{JS} is an untyped, object-based language with prototype inheritance. However, λ_{JS} does not have methods as defined in object calculi. Without methods, most object calculi cease to be interesting. However, we do desugar JavaScript’s method invocation syntax to self-application in λ_{JS} [1, Chapter 18].

λ_{JS} and JavaScript do not support cloning, which is a crucial element of other prototype-based languages, such as Self [19]. JavaScript does support Self’s prototype inheritance, but the surface syntax of JavaScript does not permit

direct access to an object’s prototype (section 2.3). Without cloning, and without direct access to the prototype, JavaScript programmers cannot use techniques such as dynamic inheritance and mode-switching [1].

References

1. M. Abadi and L. Cardelli. *A Theory of Objects*. Springer-Verlag, 1996.
2. C. Anderson, P. Giannini, and S. Drossopoulou. Towards type inference for JavaScript. In *European Conference on Object-Oriented Programming*, 2005.
3. A. Borning. Classes versus prototypes in object-oriented languages. In *ACM Fall Joint Computer Conference*, 1986.
4. R. Chugh, J. A. Meister, R. Jhala, and S. Lerner. Staged information flow for JavaScript. In *ACM SIGPLAN Conference on Programming Language Design and Implementation*, 2009.
5. D. Crockford. JSLint. www.jshint.com.
6. ECMAScript language specification, 1999.
7. Facebook. FBJS. wiki.developers.facebook.com/index.php/FBJS.
8. M. Felleisen and R. Hieb. The revised report on the syntactic theories of sequential control and state. *Theoretical Computer Science*, 103(2), 1992.
9. S. Guarnieri and B. Livshits. GateKeeper: Mostly static enforcement of security and reliability policies for JavaScript code. In *USENIX Security Symposium*, 2009.
10. A. Guha, S. Krishnamurthi, and T. Jim. Static analysis for Ajax intrusion detection. In *International World Wide Web Conference*, 2009.
11. P. Heidegger and P. Thiemann. Recency types for dynamically-typed, object-based languages: Strong updates for JavaScript. In *ACM SIGPLAN International Workshop on Foundations of Object-Oriented Languages*, 2009.
12. D. Herman. ClassicJavaScript. www.ccs.neu.edu/home/dherman/javascript/.
13. S. H. Jensen, A. Møller, and P. Thiemann. Type analysis for JavaScript. In *International Static Analysis Symposium*, 2009.
14. C. Klein and R. B. Finder. Randomized testing in PLT Redex. In *ACM SIGPLAN Workshop on Scheme and Functional Programming*, 2009.
15. S. Maffei, J. C. Mitchell, and A. Taly. An operational semantics for JavaScript. In *Asian Symposium on Programming Languages and Systems*, 2008.
16. S. Maffei, J. C. Mitchell, and A. Taly. Isolating JavaScript with filters, rewriting, and wrappers. In *European Symposium on Research in Computer Security*, 2009.
17. M. S. Miller, M. Samuel, B. Laurie, I. Awad, and M. Stay. Caja: Safe active content in sanitized JavaScript. Technical report, Google Inc., 2008. <http://google-caja.googlecode.com/files/caja-spec-2008-06-07.pdf>.
18. S. Tobin-Hochstadt and M. Felleisen. The design and implementation of Typed Scheme. In *ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, 2008.
19. D. Ungar and R. B. Smith. SELF: The power of simplicity. In *ACM SIGPLAN Conference on Object-Oriented Programming Systems, Languages & Applications*, 1987.
20. A. Wright and M. Felleisen. A syntactic approach to type soundness. *Information and Computation*, 115(1), 1994.
21. D. Yu, A. Chander, N. Islam, and I. Serikov. Javascript instrumentation for browser security. In *ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, 2007.