The Essence of JavaScript
Proof Details

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

Proof. By induction on the typing derivation $\cdot \vdash e : \textbf{JS}$.

We only need to consider cases where $e = E[e']$. e is typable, there exist Γ, T such that $\Gamma \vdash e' : T$.

We only need to consider cases where $e' =$ e_1`[`e_2`]`. The only typing rule for expressions of this form is T-GetField. By hypothesis of T-GetField, $\Gamma \vdash e_2 : \textbf{NotXHR}$. By inversion, we conclude $\Gamma \vdash e_2 : \textbf{NotXHR}$ by either T-Id or T-SafeValue[1] Consider each case:

- By T-Id, $e_2 = x$, for some identifier x. By defintiion of evaluation contexts, e_2 is a value, but identifiers are not values by definition. Hence, we have a contradiction.
- By the antecedent of T-SafeValue, $e_2 \neq$ `"XMLHttpRequest"`.

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

Proof. By induction on the typing derivation $\cdot \vdash e : \textbf{JS}$ followed by case analysis on $e \rightarrow e'$. The interesting cases are:

- T-IfSafe, which cannot occur, since the consequent is an open term.
- T-IfTrue-XHR, where:

  $e =$ `if ("XMLHttpRequest" === "XMLHttpRequest") {` e_2 `} else {` e_3 `}`

  in which the active expression is:

  $e = E[$`"XMLHttpRequest" === "XMLHttpRequest"`$]$

  Evaluation proceeds by:

  $$\frac{\texttt{"XMLHttpRequest"===\ "XMLHttpRequest"} \hookrightarrow \texttt{true}}{e \rightarrow E[\texttt{true}]}$$

[1] This inversion lemma needs to be proved by induction, due to subsumption.

$e' = E[\texttt{true}]$
$e' = \texttt{if (true) \{ } e_2 \texttt{ \} else \{ } e_3 \texttt{ \}}$

e' is typable by T-IfTrue, since $\Gamma \vdash e_2 : \mathbf{JS}$, by the hypothesis of T-IfTrue-XHR.

- T-IfTrue, where:

  $e = \texttt{if (true) \{ } e_2 \texttt{ \} else \{ } e_3 \texttt{ \}}$
  $e = [\texttt{if (true) \{ } e_2 \texttt{ \} else \{ } e_3 \texttt{ \}}]$
  $\texttt{if (true) \{ } e_2 \texttt{ \} else \{ } e_3 \texttt{ \}} \hookrightarrow e_2$
  $e' = e_2$

  e_2 is typable by hypothesis of T-IfTrue.

Subject reduction for the remaining typing rules are conventional. We require a substitution lemma for evaluation of function applications and let-bindings. Since λ_{JS} is call-by-value, we can assume that in the lemma below, v is a value.

Lemma 3 (Substitution) *If $\Gamma, x : S \vdash e : T$ and $\Gamma \vdash v : S$, then $\Gamma \vdash e[x/v] : T$.*

Proof. By induction on the typing derivation $\Gamma, x : S \vdash e : T$.
The interesting case is is T-IfSafe, reproduced below:

$$\frac{y \in dom(\Gamma) \qquad \Gamma \vdash e_2 : \mathbf{JS} \qquad \Gamma[y : \mathbf{NotXHR}] \vdash e_3 : \mathbf{JS}}{\Gamma \vdash \texttt{if } y \texttt{ === "XMLHttpRequest"then } e_2 \texttt{ else } e_3 : \mathbf{JS}} \text{ (T-IfSafe)}$$

Above, $e = \texttt{if } y \texttt{ === "XMLHttpRequest"then } e_2 \texttt{ else } e_3$.
Our inductive hypotheses are:

1. If $\Gamma, x : S \vdash e_2 : \mathbf{JS}$, then $\Gamma \vdash e_2[x/v]$.
2. If $\Gamma[y/\mathbf{NotXHR}], x : S \vdash e_3 : \mathbf{JS}$, then $\Gamma[y/\mathbf{NotXHR}] \vdash e_3[x/v] : \mathbf{JS}$.

We have two cases:

- If $x \neq y$, then $\Gamma \vdash e[x/v] : \mathbf{JS}$ by T-IfSafe.
- If $x = y$, then:

  $e[x/v] = \texttt{if (} v \texttt{ === "XMLHttpRequest") \{ } e_2[x/v] \texttt{ \} else \{ } e_3[x/v] \texttt{ \}}$

  We consider two subcases:

  – $v = \texttt{"XMLHttpRequest"}$. $e[x/v]$ is typable by T-IfTrue-XHR.

– $v \neq$ `"XMLHttpRequest"`, so $v : \mathbf{NotXHR}$ by T-SafeValue.

Since $\Gamma, x : S$ is an environment, $x \notin dom(\Gamma)$ by convention. Therefore, since $x = y$, in the second inductive hypothesis, $\Gamma[y/\mathbf{NotXHR}] = \Gamma$.

Thus, we can rewrite the second inductive hypothesis as: If $\Gamma, x : S \vdash e_3 : \mathbf{JS}$, then $\Gamma \vdash e_3[x/v] : \mathbf{JS}$.

In addition, the third hypothesis of our instantiation of T-IfSafe is simply $\Gamma \vdash e_2 : \mathbf{JS}$.

Therefore, both inductive hypotheses apply and $\Gamma \vdash e[x/v] : \mathbf{JS}$ by T-If.