An Information Flow Monitor for a Core of DOM

Introducing references and live primitives

Ana Almeida Matos[1,2], José Fragoso Santos[3], and Tamara Rezk[3]

[1] SQIG–Instituto de Telecomunicações, Lisbon, Portugal
[2] Instituto Superior Técnico, Universidade de Lisboa, Lisbon, Portugal
[3] Inria, Sophia Antipolis, France

Abstract. We propose and prove sound a novel, purely dynamic, flow-sensitive monitor for securing information flow in an imperative language extended with DOM-like tree operations, that we call Core DOM. In Core DOM, as in the DOM API, tree nodes are treated as first-class values. We take advantage of this feature in order to implement an information flow control mechanism that is finer-grained than previous approaches in the literature. Furthermore, we extend Core DOM with additional constructs to model the behavior of *live collections* in the DOM Core Level 1 API. We show that this kind of construct effectively augments the observational power of an attacker and we modify the proposed monitor so as to tackle newly introduced forms of information leaks.

1 Introduction

Interaction between client-side JavaScript programs and the HTML document is done *via* the DOM API [11]. In contrast to the ECMA Standard [1] that specifies in full detail the internals of objects created during the execution, the DOM API only specifies the behavior that DOM interfaces are supposed to exhibit when a program interacts with them. Hence, browser vendors are free to implement the DOM API as they see fit. In fact, in all major browsers, the DOM is not managed by the JavaScript engine but by a separate engine whose role is to do so. Therefore, the design of an information flow monitor for client-side JavaScript Web applications must take into account the DOM API.

Russo et al. [13] first studied the problem of information flow control in dynamic tree structures, for a model where programs are assumed to operate on a single current working node. However, in real client-side JavaScript, tree nodes are first-class values, which means that a program can store in memory several references to different nodes in the DOM forest at the same time. We present a flow-sensitive monitor for tracking information flow in a DOM-like language, that we call Core DOM. In Core DOM, tree nodes are treated as first-class values and thus they support all operations available to other types of values, such as assignment to variables. Interestingly, this language design feature enables us to implement a more fine-grained information flow control mechanism, since it becomes possible to distinguish the security level of the node itself from both the security level of the value that is stored in the node and from the level of its

position in the DOM forest. We prove that the proposed monitor is sound with respect to a standard definition of noninterference.

Live collections are a special kind of data structure featured in the DOM API that automatically reflects the changes that occur in the document. There are several types of live collections. For instance, the method `getElementsByTagName` returns a live collection containing the DOM nodes that match a given *tag*. In the following example, after retrieving the initial collection of **DIV** nodes, the program iterates over the *current* size of this collection, while introducing a new **DIV** node at each step:

```
divs = document.getElementsByTagName("DIV"); i = 0;
while(i <= divs.length){
  document.appendChild(document.createElement("DIV")); i++; }
```

Every time a new **DIV** node is inserted in the `document` (no matter where in its structure), it is also inserted in the live collection bound to `divs`. Due to the live update of the loop condition, if the initial `document` contains at least one **DIV** node, the program does not terminate.

Live collections can be exploited to encode new types of information leaks. Therefore, we extend Core DOM with two additional constructs that model the behavior of `getElementsByTagName` in the DOM API. We demonstrate that these constructs effectively augment the observational power of an attacker and we show how to modify the proposed monitor so as to tackle this issue.

In the remainder of the paper, we start by formally introducing the target language Core DOM (Section 2). We then present a mechanism that controls information flows by means of a flow-sensitive monitor (Section 3). The scenario is then extended with live collections, for which we propose a modified mechanism (Section 4). Finally, we discuss related work and conclude. Due to space restrictions, proofs are presented in the article's full version [2].

2 Core DOM

We now present Core DOM – a simple imperative language extended with primitives for operating on tree structures. Its syntax is given by the following:

$e ::= v$	literal value	$\mid \underline{v}$	runtime value
$\mid x$	identifier	$\mid \mathsf{if}(e_0)\{e_1\}\ \mathsf{else}\ \{e_2\}$	conditional
$\mid \mathsf{while}(e_0)\{e_1\}$	loop	$\mid \mathsf{while}^{e_0}(e_1)\{e_2\}$	internal loop
$\mid e_0; e_1$	sequence	$\mid \mathsf{move}_{\uparrow}(e)$	move upward
$\mid \mathsf{move}_{\downarrow}(e, e)$	move downward	$\mid \mathsf{remove}(e, e)$	remove node
$\mid \mathsf{insert}(e, e, e)$	insert node	$\mid \mathsf{new}^{\sigma_0,\sigma_1,\sigma_2}(e)$	new node
$\mid \mathsf{value}(e)$	node value	$\mid \mathsf{store}(e, e)$	store value
$\mid \mathsf{len}(e)$	node length	$\mid \mathsf{end}(e)$	end

Every tree node has a type, called its *tag* (for instance, **DIV**) and can store a single value taken from a set $\mathcal{P}rim$ containing integers, strings, booleans, and a special value *null*. All the nodes in memory form a *forest*, meaning that every node has a possibly empty list of *children* and at most a single *parent*. We define the *index* of a node as the position it occupies in the list of children of its parent.

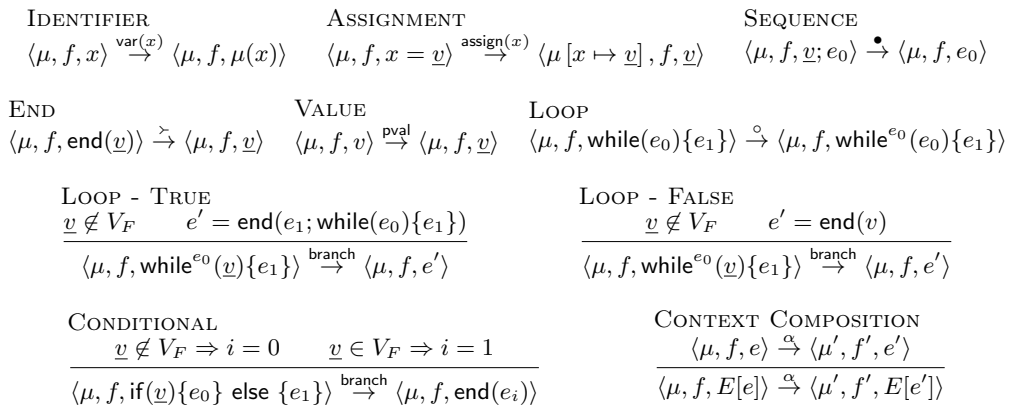


Fig. 1. Core DOM Semantics - Imperative Fragment

New nodes are created using the primitive new, which expects as input the tag of the node to be created and is annotated with three security levels that are explained later. When given a node as input, the primitive $\mathsf{move}_{\uparrow}$ evaluates to its parent in the DOM forest. Complementarily, the primitive $\mathsf{move}_{\downarrow}$ expects as input a node n and an integer i and evaluates to the i^{th} child of n. The primitive insert is used for inserting an *orphan node* (that is, a node with no parent) in the list of children of another node, whereas the primitive remove is used for removing a node from the list of children of its parent. Concretely, insert expects as input two nodes n_0 and n_1 and an integer i and inserts n_1 in the i^{th} position of the list of children of n_0 right-shifting by one all the children of n_0 whose indexes are greater than or equal to i. The primitive remove expects as input a node n and an integer i and removes the i^{th} child of n from its list of children left-shifting the right siblings of the removed node by one position. When given as input a node, the keyword len evaluates to its number of children. The keyword value expects as input a node and evaluates to the value that it stores, whereas the keyword store expects as input a node n and a value v and stores v in n. Finally, the syntax of Core DOM includes two special primitives: **(1)** end [12,14] (not available for the programmer) that is used by the semantics to signal the end of a structure block and **(2)** an internal while primitive used by the semantics for bookkeeping the guard of the loop currently executing.

We model a DOM forest $f : \mathcal{R}ef \rightarrow \mathcal{N}$ as a partial mapping from a set of references to the set of DOM nodes. A DOM node is a tuple of the form: $\langle m, \underline{v}, r, \omega \rangle$, where: **(1)** m is the node's tag, **(2)** $\underline{v}$ the runtime value that it stores, **(3)** r the reference pointing to its parent, and **(4)** ω its list of children. For simplicity, given a DOM node n, we denote by $n.\mathsf{tag}$, $n.\mathsf{value}$, $n.\mathsf{parent}$, and $n.\mathsf{children}$ its tag, value, parent, and list of children, respectively. The semantics of Core DOM makes use of a semantic function $\mathcal{R}_{Ancestor}$ that, given a forest f, outputs a binary relation in $\mathcal{R}ef \times \mathcal{R}ef$ such that $\langle r_0, r_1 \rangle \in \mathcal{R}_{Ancestor}(f)$ iff the node pointed to by r_0 is an ancestor of that pointed to by r_1. The set V_F contains the runtime values that cause the guard of a conditional or loop to fail.

Figures 1 and 2 present the small-step semantics of Core DOM. Configurations have the form: $\langle \mu, f, e \rangle$, where μ is a mapping from variables to values, f

$$\textsc{Move Upward}\quad \frac{f(r).\mathsf{parent} = r'}{\langle \mu, f, \mathsf{move}_{\uparrow}(r)\rangle \overset{\uparrow(r)}{\rightarrow} \langle \mu, f, r'\rangle} \qquad \textsc{Move Downward}\quad \frac{f(r).\mathsf{children}(i) = r'}{\langle \mu, f, \mathsf{move}_{\downarrow}(r,i)\rangle \overset{\downarrow(r')}{\rightarrow} \langle \mu, f, r'\rangle}$$

$$\textsc{New}\quad \frac{r = fresh(f, \sigma_0) \qquad f' = f\left[r \mapsto \langle m, null, null, \epsilon\rangle\right]}{\langle \mu, f, \mathsf{new}^{\sigma_0,\sigma_1,\sigma_2}(m)\rangle \overset{\mathsf{new}(r,\sigma_0,\sigma_1,\sigma_2)}{\rightarrow} \langle \mu, f', r\rangle}$$

$$\textsc{Remove}\quad \frac{f(r) = \langle m, \underline{v}, \hat{r}, \omega\rangle \qquad f(\omega(i)) = \langle m', \underline{v}', r, \omega'\rangle \qquad r' = \omega(i) \qquad f' = f\begin{bmatrix} r \mapsto \langle m, \underline{v}, \hat{r}, Shift_L(\omega, i)\rangle, \\ r' \mapsto \langle m', \underline{v}', null, \omega'\rangle \end{bmatrix}}{\langle \mu, f, \mathsf{remove}(r,i)\rangle \overset{-(r,r')}{\rightarrow} \langle \mu, f', r'\rangle}$$

$$\textsc{Insert}\quad \frac{\langle r', r\rangle \notin \mathcal{R}_{Ancestor}(f) \qquad f(r) = \langle m, \underline{v}, \hat{r}, \omega\rangle \qquad f(r') = \langle m', \underline{v}', null, \omega'\rangle \qquad f' = f\left[r \mapsto \langle m, \underline{v}, \hat{r}, Shift_R(\omega, i, r')\rangle, r' \mapsto \langle m', \underline{v}', r, \omega'\rangle\right]}{\langle \mu, f, \mathsf{insert}(r, r', i)\rangle \overset{+(r,r',\omega(i))}{\rightarrow} \langle \mu, f', r'\rangle}$$

$$\textsc{Length}\quad \frac{i = |f(r).\mathsf{children}|}{\langle \mu, f, \mathsf{len}(r)\rangle \overset{\mathsf{len}(r)}{\rightarrow} \langle \mu, f, i\rangle} \qquad \textsc{Value}\quad \frac{f(r).\mathsf{value} = \underline{v}}{\langle \mu, f, \mathsf{value}(r)\rangle \overset{\mathsf{val}(r)}{\rightarrow} \langle \mu, f, \underline{v}\rangle} \qquad \textsc{Store}\quad \frac{f(r) = \langle m, \underline{v}, \hat{r}, \omega\rangle \qquad f' = f\left[r \mapsto \langle m, \underline{v}', \hat{r}, \omega\rangle\right]}{\langle \mu, f, \mathsf{store}(r, \underline{v}')\rangle \overset{\mathsf{store}(r)}{\rightarrow} \langle \mu, f', \underline{v}'\rangle}$$

Fig. 2. Core DOM Semantics - Primitives for Tree Operations

a DOM forest, and e the expression to evaluate. References can be viewed as pointers to nodes, in the sense that the creation of a node yields a new reference that points to it. As in [6], the semantics makes use of a *parametric allocator*, $fresh$, that given a DOM forest f and a security level σ, generates a new reference r, such that $r \notin dom(f)$. The semantic transitions are annotated with *internal events* [12] to be used by the monitored semantics.

The evaluation order is specified by writing expressions using *evaluation contexts*. We write $E[e]$ to denote the expression obtained by replacing the occurrence of [] in the context E with e. The syntax of evaluation contexts is given by:

$$\begin{aligned} E ::= {} & [] \mid x = E \mid \mathsf{if}(E)\{e\}\ \mathsf{else}\ \{e\} \mid \mathsf{while}^{e}(E)\{e\} \mid E; e \mid \mathsf{end}(E) \mid \mathsf{len}(E) \mid \mathsf{value}(E) \\ & \mid \mathsf{move}_{\uparrow}(E) \mid \mathsf{move}_{\downarrow}(E, e) \mid \mathsf{move}_{\downarrow}(\underline{v}, E) \mid \mathsf{remove}(E, \underline{v}) \mid \mathsf{remove}(\underline{v}, E) \mid \mathsf{insert}(\underline{v}, E, e) \\ & \mid \mathsf{insert}(E, e, e) \mid \mathsf{insert}(\underline{v}, \underline{v}, E) \mid \mathsf{new}^{\sigma_0,\sigma_1,\sigma_2}(E) \mid \mathsf{store}(E, e) \mid \mathsf{store}(\underline{v}, E) \end{aligned}$$

Given a list ω, an integer i, and an arbitrary element a, we denote by: **(1)** $\omega(i)$ the i^{th} element of ω if it is defined and *null* otherwise, **(2)** $|\omega|$ the number of elements of ω, **(3)** ϵ the empty list, **(4)** $Shift_L(\omega, i)$ the list obtained by removing from ω its i^{th} element (provided that it is defined), **(5)** $Shift_R(\omega, a, i)$ the list obtained by inserting a in the i^{th} position of ω (provided that i is smaller than or equal to the number of elements of ω), **(6)** $\omega :: a$ the list obtained by appending a to ω, and **(7)** $\omega_0 \oplus \omega_1$ the concatenation of ω_0 and ω_1. We use the notation $f\left[a \mapsto b\right]$ for the function that coincides with f everywhere except in a that it maps to b.

3 Dynamic IFC in Core DOM

Before proceeding to describe the monitor for securing information flow in Core DOM, we discuss the main challenges imposed by the particular features of this

API and how we propose to tackle them. As usual, the specification of security policies relies on a lattice $\mathcal{L}$ of security levels and a labeling that maps resources to security levels. In examples and informal explanations, we use $\mathcal{L} = \{H, L\}$ with $L \sqsubseteq H$, meaning that resources labeled L (*low*, *visible*) are less confidential than those labeled H (*high*, *invisible*). Hence, H-labeled resources can depend on L-labeled resources, but not the contrary, as that would entail a *security leak*.

3.1 Challenges for IFC in Core DOM

The range of tree operations offered by Core DOM allows information to be stored and inspected from arbitrary nodes in several ways: **(1)** A node can be created and its existence tested; **(2)** A value can be stored and read from a node; **(3)** A child node can be inserted at/removed from a certain position, and both the number of children and their positions can be retrieved. (The *position* of a node can be understood as the pair consisting of its parent in the DOM forest and its index.) These operations can be used to encode security leaks via the different information components that are associated with every node. We now examine these leaks and introduce the formal techniques we use for tackling them. In the examples, we assume three initial nodes, div_0, div_1 and div_2, created as follows:

$$div_0 = \mathsf{new}(\text{"DIV"});\ div_1 = \mathsf{new}(\text{"DIV"});\ div_2 = \mathsf{new}(\text{"DIV"}) \tag{1}$$

Differentiating information components. Each node in a DOM forest can be seen to carry four main information components: its existence, its value, its position and its number of children. To some degree, these components can be manipulated separately, and there is value in treating them separately by the security analysis. For instance, in the following program, the final position of div_2 carries *high* information (because it is inserted in a *high* context), despite the fact that it contains the *low* level value l_0:

$$\mathsf{store}(div_2, l_0);\ \mathsf{if}(h)\{\mathsf{insert}(div_0, div_2, 0)\}\ \mathsf{else}\ \{\mathsf{insert}(div_1, div_2, 0)\} \tag{2}$$

After the execution of this program, the position of div_2 should not be revealed to a low observer. Its value, however, can be made public. Hence, while the evaluation of $\mathsf{move}_{\uparrow}(div_2)$ should yield a high value, the evaluation of the expression $\mathsf{value}(div_2)$ in the final memory can yield a low value. Similarly, there is no reason why the position of a node that stores a secret value should not be public.

By treating tree nodes as first-class values, we can naturally differentiate the security levels that are associated to each of the node's information components. We propose to associate every tree node with four security levels. The *value level* of a node is the level of the value that it stores. The *position level* of a node is the level of its position in the DOM forest. Hence, the position level of a node constitutes an upper bound on the levels of the contexts in which its position in the DOM forest can change (such as by its insertion/removal). The *structure security level* [10] of a node is associated to the node's number of children. It serves as an upper bound on the levels of the contexts in which the number of children of a node can be changed (such as by insertion/removal of nodes in/from its list of children). Finally, the *node level* is the level associated to information about the existence of the node itself. It is used as an upper bound on the levels

of the contexts in which the node can be created or a lower bound on its own value and structure level, and on its children's position levels.

New forms of security leaks. When inserting/removing a node in/from the list of children of a given node, the indexes of its right siblings change, thereby entailing a new kind of implicit flow. Consider the following example:

$$\mathsf{insert}(div_0, div_1, 0);\ \mathsf{if}(h)\{\mathsf{insert}(div_0, div_2, 0)\}\ \mathsf{else}\ \{null\};\ l_0 = \mathsf{move}_{\downarrow}(div_0, 0) \quad (3)$$

The program above prepends div_1 to the list of children of div_0 (which is originally empty). Then, depending on the value of h, the program prepends div_2 to the list of children of div_0. Hence, depending on the value of h, the program assigns either div_1 or div_2 to the *low* variable l_0. We refer to these forms of security leaks as *order leaks*, as they leverage information about the order of the nodes in the list of children. Order leaks can also be obtained by removing a child node when a second sibling node of higher index exists. Program 3 shows that, when changing the position of a node in the DOM forest, the positions of its right siblings also change. Therefore, the monitor enforces the position levels of the right siblings of a given node to be equal to or higher than its own position level. Furthermore, when moving from one node to another information about the position of the child node is leaked. For instance, for Program 3 to be legal, the position levels of div_1 and div_2 must be H. Therefore, the value associated with the evaluation of the instruction $\mathsf{move}_{\downarrow}(div_0, 0)$ is H.

The fact that a program can inspect the number of children of a given node can be exploited to encode implicit information flows. If we add the low assignment $l_1 = \mathsf{len}(div_0)$ to the end of Program 3, the value of l_1 will be set to 2 or 1 depending on the value of the *high* variable h. The *structure security level* is meant to control this kind of leaks. If a node has *low* structure security level, one cannot insert/remove nodes in/from its list of children in *high* contexts. Therefore, the level associated with looking-up the number of children of a given node corresponds to its structure security level. For instance, for Program 3 to be legal, the structure security level of div_0 must be H. Hence, the level associated with the evaluation of $\mathsf{len}(div_0)$ is H independently of the original value of h.

Flow-sensitive versus flow-insensitive IF monitoring. The *no-sensitive-upgrade* discipline [3] has been widely used in the design of *purely dynamic monitors*. This discipline establishes that visible resources cannot be upgraded in invisible contexts, since such upgrades cause the visible domain of a program to change depending on secret values. Hence, flow-sensitive monitors that implement the no-sensitive-upgrade discipline abort executions that encode illegal implicit flows. Since both the structure security level and the position level of a node are used to control the implicit flows that can be encoded by inserting/removing nodes in/from the DOM forest, these levels cannot be upgraded. This point is illustrated in the following table, which represents four monitored executions of a program (represented on the left) in two distinct memories, by showing how the variable labeling Γ and the node labeling Σ evolve during each execution. The initial memories are such that div_0 and div_1 each bind an orphan node with *low* structure security level, and are pointed to by r_0 and r_1, respectively, but differ in the value of *high* variable h.

While the monitor following the *naive approach* raises the structure security level of div_0 to H (allowing the execution to go through), the monitor following the *no-sensitive-upgrade* discipline blocks the execution when the program tries to add div_1 to the list of children of div_0 in a *high* context. The case regarding the position level can be seen by replacing the test of the second `if` instruction with $\mathsf{move}_{\uparrow}(div_1) == div_0$, assuming that the original position level of div_1 is *low*. In contrast to the position level and to the structure security level, the value level of a node can be upgraded, as the value stored in a node is set explicitly. However, such upgrades cannot be caused by implicit information flows.

	Both Approaches	*Naive Approach*	*No-Sensitive-Upgrade*
Initial High Memory:	$h = \mathsf{false}$	$h = \mathsf{true}$	$h = \mathsf{true}$
$l = \mathsf{true}$	$\Gamma(l) := L$	$\Gamma(l) := L$	$\Gamma(l) := L$
$\mathsf{if}(h)$	branch not taken	branch taken	branch taken
$\mathsf{insert}(div_0, div_1, 0)$	—	$\Sigma(r_0).\mathsf{struct} := H$	*stuck*
$\mathsf{if}(\mathsf{len}(div_0) == 0)$	branch taken	branch not taken	—
$l = \mathsf{false}$	$\Gamma(l) := L$	—	—
Final Low Memory:	$l = \mathsf{false}$	$l = \mathsf{true}$	—

3.2 The Attacker Model

We assume a generic lattice $\mathcal{L}$ of security levels, and use $\sqcup$, $\sqcap$, $\bot$, and $\top$ for the greatest lower bound, the least upper bound, the *bottom* level, and the *top* level, respectively. We consider two types of labelings: *variable labelings* and *node labelings*. While a variable labeling $\Gamma : \mathcal{V}ar \to \mathcal{L}$ maps each variable to a single security level, a node labeling $\Sigma : \mathcal{R}ef \to \mathcal{L}^4$ associates each reference with a tuple of four security levels. Hence, given a reference r and a labeling Σ, $\Sigma(r) = \langle \sigma_n, \sigma_v, \sigma_e, \sigma_s \rangle$, where: **(1)** σ_n is the node level, **(2)** σ_v is the value level, **(3)** σ_e is the the position level, and **(4)** σ_s is the structure security level. For clarity, given a node n pointed to by a reference r and a labeling Σ, we denote by $\Sigma(r).\mathsf{node}$, $\Sigma(r).\mathsf{value}$, $\Sigma(r).\mathsf{pos}$, and $\Sigma(r).\mathsf{struct}$ its node level, value level, position level, and structure security level, respectively. For simplicity, we impose four restrictions on the levels assigned to a given node. First, one cannot store a visible value in an invisible node. Second, an invisible node cannot have a visible position. Third, an invisible node cannot have a visible number of children. Fourth, an invisible node cannot have a visible node in its list of children (in practice, this means that we cannot insert a visible node in an invisible node). Formally, for every reference $r \in dom(\Sigma)$, it holds that: $\Sigma(r).\mathsf{node} \sqsubseteq \Sigma(r).\mathsf{value} \sqcap \Sigma(r).\mathsf{pos} \sqcap \Sigma(r).\mathsf{struct}$. Additionally, for every two references r and r' in a forest f such that: $r, r' \in dom(\Sigma)$ and $f(r).\mathsf{children}(i) = r'$ for some integer i, it holds that $\Sigma(r).\mathsf{node} \sqsubseteq \Sigma(r').\mathsf{node}$.

In order to formally characterize the observational power of an attacker, we take the standard approach of defining a notion of *low-projection* of a memory/forest at a given level σ, which corresponds to the part of the memory/-forest that an attacker at level σ can observe. The low-projection of a memory μ with respect to a variable labeling Γ at level σ is simply given by: $\mu \restriction^{\Gamma,\sigma} = \{(x, \mu(x), \Gamma(x)) \mid x \in dom(\Gamma) \wedge \Gamma(x) \sqsubseteq \sigma\}$. Accordingly, two memories μ_0 and μ_1, respectively labeled by Γ_0 and Γ_1 are said to be *low-equal* at

$$\textsc{Identifier}\quad \frac{\sigma = level(o) \sqcup \Gamma(x)}{\langle \Gamma, \Sigma, o, \zeta\rangle \overset{\mathsf{var}(x)}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \sigma\rangle} \qquad \textsc{Assignment}\quad \frac{level(o) \sqsubseteq \Gamma(x) \qquad \sigma' = level(o) \sqcup \sigma}{\langle \Gamma, \Sigma, o, \zeta :: \sigma\rangle \overset{\mathsf{assign}(x)}{\rightarrow} \langle \Gamma\left[x \mapsto \sigma'\right], \Sigma, o, \zeta :: \sigma'\rangle}$$

$$\textsc{Literal Value}\quad \langle \Gamma, \Sigma, o, \zeta\rangle \overset{\mathsf{pval}}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: level(o)\rangle \qquad \textsc{Branch}\quad \langle \Gamma, \Sigma, o, \zeta :: \sigma\rangle \overset{\mathsf{branch}}{\rightarrow} \langle \Gamma, \Sigma, o :: \sigma, \zeta\rangle$$

$$\textsc{End}\quad \langle \Gamma, \Sigma, o :: \sigma, \zeta\rangle \overset{\succ}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta\rangle \qquad \textsc{Discharge}\quad \langle \Gamma, \Sigma, o, \zeta :: \sigma\rangle \overset{\bullet}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta\rangle \qquad \textsc{Empty}\quad \langle \Gamma, \Sigma, o, \zeta\rangle \overset{\circ}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta\rangle$$

Fig. 3. Core DOM Monitor - Imperative Fragment

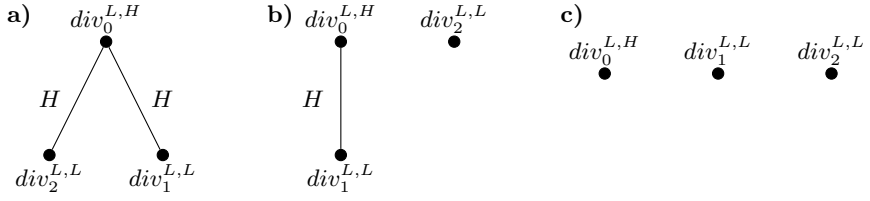
security level σ, written $\mu_0, \Gamma_0 \sim_\sigma \mu_1, \Gamma_1$, if they coincide in their respective low-projections, $\mu_0 \restriction^{\Gamma_0,\sigma} = \mu_1 \restriction^{\Gamma_1,\sigma}$. Definition 1 extends the notion of low-projection to forests. Informally, an attacker at level σ can see: **(1)** the references whose corresponding nodes are associated with levels $\sqsubseteq \sigma$ as well as their tags, **(2)** the values stored in visible nodes whose value level is $\sqsubseteq \sigma$, **(3)** the positions of visible nodes (with visible parents) whose levels are $\sqsubseteq \sigma$, and **(4)** the number of children of visible nodes whose structure security level is $\sqsubseteq \sigma$.

Definition 1 (Low-Projection and Low-Equality). *The low-projection of a forest f w.r.t. a security level σ and a labeling Σ is given by:*

$$\begin{aligned} f \restriction^{\Sigma,\sigma} = \ & \{(r, f(r).\mathsf{tag}, \Sigma(r).\mathsf{node}, \Sigma(r).\mathsf{pos}, \Sigma(r).\mathsf{struct}) \mid \Sigma(r).\mathsf{node} \sqsubseteq \sigma\} \\ \cup \ & \{(r, f(r).\mathsf{value}, \Sigma(r).\mathsf{value}) \mid \ \Sigma(r).\mathsf{value} \sqsubseteq \sigma\} \\ \cup \ & \{(r, i, r') \mid \ f(r).\mathsf{children}(i) = r' \ \wedge \ \Sigma(r').\mathsf{pos} \sqsubseteq \sigma\} \\ \cup \ & \{(r, null) \mid \ f(r).\mathsf{parent} = null \ \wedge \ \Sigma(r).\mathsf{pos} \sqsubseteq \sigma\} \\ \cup \ & \{(r, |f(r).\mathsf{children}|) \mid \ \Sigma(r).\mathsf{struct} \sqsubseteq \sigma\} \end{aligned}$$

Two forests f_0 and f_1, respectively labeled by Σ_0 and Σ_1 are said to be low-equal at security level σ, written $f_0, \Sigma_0 \sim_\sigma f_1, \Sigma_1$, if $f_0 \restriction^{\Sigma_0,\sigma} = f_1 \restriction^{\Sigma_1,\sigma}$.

In the following figures, **a)** and **b)** represent the final forests obtained from the execution of Program 3 in two distinct memories that initially map the *high* variable h to 1 and to 0, respectively. Forest **c)** represents their (coinciding) low-projection. Nodes are labeled with their node level and structure security level, while edges are labeled with the child's position level. The position levels of div_1 and div_2 as well as the structure security level of div_0 are assumed to be originally *high*. All other levels are assumed to be originally *low*.



3.3 Enforcement

We define a monitored semantics in the style of Russo et al. [12, 14]. A configuration of the monitored semantics is obtained by pairing up a configuration

of the unmonitored semantics with a configuration of the security monitor. At each computation step, the security monitor uses the internal event generated by the unmonitored semantics to determine its corresponding transition. Hence, the transitions of the monitored semantics are defined as follows:

$$\frac{\langle \mu, f, e\rangle \xrightarrow{\alpha} \langle \mu', f', e'\rangle \quad \langle \Gamma, \Sigma, o, \zeta\rangle \xrightarrow{\alpha} \langle \Gamma', \Sigma', o', \zeta'\rangle}{\langle\langle \mu, f, e\rangle, \langle \Gamma, \Sigma, o, \zeta\rangle\rangle \to \langle\langle \mu', f', e'\rangle, \langle \Gamma', \Sigma', o', \zeta'\rangle\rangle}$$

The arrow $\to$ denotes the transition relation (whilst $\to^*$ its reflexive-transitive closure), and the configurations of the security monitor have the form $\langle \Gamma, \Sigma, o, \zeta\rangle$, where: **(1)** Γ is the variable labeling, **(2)** Σ is the node labeling, **(3)** o is the *control context*, that is, a list containing the levels of the expressions on which the program branched in order to reach the expression that is currently executing, and **(4)** ζ is the *expression context*, that is, a list consisting of the levels of the expressions of the current evaluation context that were already computed. The control context and the expression context lists are used as stacks. Concretely, each time the evaluation enters the body of an `if` or a `while` expression, the level of the expression that was tested is appended to the control context. Conversely, when the control flow leaves the body of an `if` or a `while` expression, the monitor removes the last element of the control context. Similarly, after the evaluation of an expression that is nested inside another expression, its level is appended to the expression context and, whenever an expression is no longer nested inside another expression, its level is removed from the expression context. The transitions of the monitor are presented in Figures 3 and 4. We are only concerned with monitored executions beginning with $\langle \Gamma_0, \Sigma_0, \epsilon, \epsilon\rangle$, where Γ_0 and Σ_0 are the original variable and node labelings. Furthermore, letting μ_0 and f_0 be the initial memory and the initial forest, we require that: $dom(\mu_0) = dom(\Gamma_0)$ and $dom(f_0) = dom(\Sigma_0)$. Given a list ω, we use the $level(\omega)$ as an abbreviation for $\sqcup\{\omega(i) \mid 0 \leq i < |\omega|\}$.

Let us briefly explain the rules of the proposed information flow monitor. Rules [Move Upward] and [Move Downward] update the expression context ζ with the levels of the current expression's subexpression(s) (that are retrieved from ζ), of the program counter, and of the departing/arriving node's position. Observe that the levels of the nodes that the traversed edge connects are ignored, as they are assumed to be lower than or equal to the child's position level. Analogously, rule [Length] updates the expression context ζ with the levels of the current expression's subexpression, of the program counter, and of the structure security level of the node whose number of children is being inspected. Rules [Remove] and [Insert] prevent the removal/insertion of a node with a visible position in an invisible context. Furthermore, they prevent the semantics from inserting/removing a node in/from a node with a visible number of children in an invisible context. Since changing the position of a node causes the position of its right siblings to change, Rule [Insert] ensures that the position levels of the children of every DOM node are always in increasing order. Finally, rules [Store] and [Assignment] update the security level of the corresponding value, provided that it does not constitute a sensitive-upgrade. Hence, updates of visible values in invisible contexts cause the execution to abort.

$$\textsc{Move Upward}\quad \frac{\sigma' = level(o) \sqcup \Sigma(r).\mathsf{pos} \sqcup \sigma}{\langle \Gamma, \Sigma, o, \zeta :: \sigma\rangle \overset{\uparrow(r)}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \sigma'\rangle}$$

$$\textsc{Move Downward}\quad \frac{\sigma' = level(o) \sqcup \Sigma(r).\mathsf{pos} \sqcup \sigma_0 \sqcup \sigma_1}{\langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1\rangle \overset{\downarrow(r)}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \sigma'\rangle}$$

$$\textsc{Length}\quad \frac{\sigma' = \sigma \sqcup level(o) \sqcup \Sigma(r).\mathsf{struct}}{\langle \Gamma, \Sigma, o, \zeta :: \sigma\rangle \overset{\mathsf{len}(r)}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \sigma'\rangle}$$

$$\textsc{Remove}\quad \frac{level(o) \sqcup \sigma_0 \sqcup \sigma_1 \sqsubseteq \Sigma(r).\mathsf{struct} \sqcap \Sigma(r').\mathsf{pos}}{\langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1\rangle \overset{-(r,r')}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \Sigma(r').\mathsf{pos}\rangle}$$

$$\textsc{Insert}\quad \frac{\begin{array}{c} r'' = null \vee \Sigma(r').\mathsf{pos} \sqsubseteq \Sigma(r'').\mathsf{pos} \\ level(o) \sqcup \sigma_0 \sqcup \sigma_1 \sqcup \sigma_2 \sqsubseteq \Sigma(r).\mathsf{struct} \sqcap \Sigma(r').\mathsf{pos}\end{array}}{\langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1 :: \sigma_2\rangle \overset{+(r,r',r'')}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \Sigma(r').\mathsf{pos}\rangle}$$

$$\textsc{Value}\quad \frac{\sigma' = \sigma \sqcup \Sigma(r).\mathsf{value}}{\langle \Gamma, \Sigma, o, \zeta :: \sigma\rangle \overset{\mathsf{val}(r)}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \sigma'\rangle}$$

$$\textsc{Store}\quad \frac{\begin{array}{c} \sigma = level(o) \sqcup \sigma_0 \sqcup \sigma_1 \sqcup \Sigma(r).\mathsf{node} \\ level(o) \sqcup \sigma_0 \sqsubseteq \Sigma(r).\mathsf{value} \\ \Sigma' = \Sigma\,[r \mapsto \langle \Sigma(r).\mathsf{node}, \sigma, \Sigma(r).\mathsf{pos}, \Sigma(r).\mathsf{struct}\rangle]\end{array}}{\langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1\rangle \overset{\mathsf{store}(r)}{\rightarrow} \langle \Gamma, \Sigma', o, \zeta :: \sigma_1\rangle}$$

$$\textsc{New}\quad \frac{\begin{array}{c} level(o) \sqcup \sigma \sqsubseteq \sigma_0 \sqsubseteq \sigma_1 \sqcap \sigma_2 \\ \Sigma' = \Sigma\,[r \mapsto \langle \sigma_0, \sigma_0, \sigma_1, \sigma_2\rangle]\end{array}}{\langle \Gamma, \Sigma, o, \zeta :: \sigma\rangle \overset{\mathsf{new}(r,\sigma_0,\sigma_1,\sigma_2)}{\rightarrow} \langle \Gamma, \Sigma', o, \zeta :: \sigma_0\rangle}$$

Fig. 4. Core DOM Monitor - Primitives for Tree Operations

Informally, a monitor is said to be *noninterferent* (NI) if, whenever the monitored execution of a program on two low-equal memories/forests terminates successfully, it also produces two low-equal memories/forests. Hence, an attacker cannot use the monitored execution of a program as a means to disclose information about the confidential contents of a memory. Theorem 1 states that the monitored successfully-terminating execution of a program on two low-equal memories/forests always yields two low-equal memories/forests.

Theorem 1 (Noninterference). *For any expression e, memories μ_0 and μ_1, forests f_0 and f_1, variable labelings Γ_0 and Γ_1, node labelings Σ_0 and Σ_1, and security level σ such that $\mu_0, \Gamma_0 \sim_\sigma \mu_1, \Gamma_1$ and $f_0, \Sigma_0 \sim_\sigma f_1, \Sigma_1$, and also:*

- $\langle\langle \mu_0, f_0, e\rangle, \langle \Gamma_0, \Sigma_0, \epsilon, \epsilon\rangle\rangle \rightarrow^* \langle\langle \mu_0', f_0', v_0\rangle, \langle \Gamma_0', \Sigma_0', \epsilon, \epsilon :: \sigma_0\rangle\rangle$
- $\langle\langle \mu_1, f_1, e\rangle, \langle \Gamma_1, \Sigma_1, \epsilon, \epsilon\rangle\rangle \rightarrow^* \langle\langle \mu_1', f_1', v_1\rangle, \langle \Gamma_1', \Sigma_1', \epsilon, \epsilon :: \sigma_1\rangle\rangle$

It holds that: $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ and $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$. Furthermore, if either $\sigma_0 \sqsubseteq \sigma$ or $\sigma_1 \sqsubseteq \sigma$, then: $\sigma_0 \sqcup \sigma_1 \sqsubseteq \sigma$ and $v_0 = v_1$.

4 Extension to Live Primitives

The DOM API includes several methods that return live collections. For instance, the method `getElementsByTagName` returns a live collection containing all the nodes in the document tree whose tag matches the string given as input. The distinctive feature of live collections is that they automatically reflect modifications to the document. Hence, every time a node matching the query that generated a given live collection is inserted/removed in/from the document, it is also automatically inserted/removed in/from the corresponding live collection. Therefore, a live collection is in fact a dynamic query to the document.

$$\textsc{Live Move}\quad \frac{f \vdash r \rightsquigarrow_m \omega \qquad \omega(i) = r'}{\langle \mu, f, \mathsf{move}_\ell\,(r, m, i)\rangle \overset{\ell\,(f,r')}{\rightarrow} \langle \mu, f, r'\rangle} \qquad \textsc{Live Length}\quad \frac{f \vdash r \rightsquigarrow_m \omega}{\langle \mu, f, \mathsf{len}_\ell\,(r, m)\rangle \overset{\mathsf{len}_\ell\,(f,r,m)}{\rightarrow} \langle \mu, f, |w|\rangle}$$

Fig. 5. Extension of the Semantics to Live Primitives

4.1 Formal Syntax and Semantics

The nodes of a live collection are always arranged in *document order*. The document order is an ordering $\leq$ on the nodes of the DOM forest such that for every two nodes n_0 and n_1 in the same DOM tree, $n_0 \leq n_1$ if and only if n_0 is found before n_1 in a depth-first left-to-right search starting from the root of the tree. In order to model the live collections returned by the method `getElementsByTagName`, we extend Core DOM with two additional constructs:

$$e ::= ... \mid \mathsf{move}_\ell\,(e, e, e) \mid \mathsf{len}_\ell\,(e, e)$$

The *live move* primitive receives as input a node n, a tag name m, and an integer i and evaluates to the i^{th} node with tag m in the tree rooted at n when traversed in document order. The *live length* primitive receives as input a node n and a tag name m and evaluates to the number of nodes with tag m in the tree rooted at n. The example given in Section 1 can be rewritten in Core DOM as:

$$i = 0;\ \mathsf{while}(i < \mathsf{len}_\ell\,(\mathsf{doc}, \text{“}DIV\text{”}))\{\mathsf{insert}(\mathsf{doc}, \mathsf{new}(\text{“}DIV\text{”}), \mathsf{len}(\mathsf{doc}));\ i = i + 1\} \quad (4)$$

where doc is assumed to be a special identifier bound to the root of the *document*. The syntax of the evaluation contexts is extended to take into account the new syntactic constructs:

$$E ::= ... \mid \mathsf{move}_\ell\,(E, e, e) \mid \mathsf{move}_\ell\,(\underline{v}, E, e) \mid \mathsf{move}_\ell\,(\underline{v}, \underline{v}, E) \mid \mathsf{len}_\ell\,(E, e) \mid \mathsf{len}_\ell\,(\underline{v}, E)$$

The extension of the semantics to live primitives is presented in Figure 5. The semantics makes use of a search predicate of the form $f \vdash r \rightsquigarrow_m \omega$ (given in appendix), that formalizes the search for the nodes matching a given tag in a tree. Intuitively, given a forest f, a reference to a node r, a tag name m, and a list of DOM references ω, $f \vdash r \rightsquigarrow_m \omega$ holds iff ω is the list of all the nodes with tag m found when traversing the tree of f rooted at r in document order.

4.2 Information Leaks due to Live Primitives

The *live* constructs introduced in this section can be exploited to encode new types of information leaks.

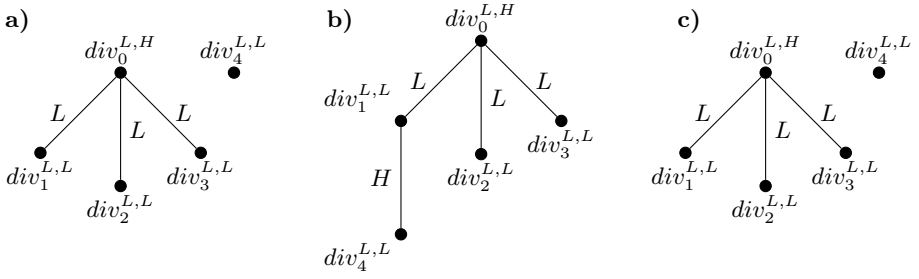
Leaks via len_ℓ. Consider the program below, which is to be executed in a forest that originally contains five orphan **DIV** nodes respectively bound to the variables: div_0, div_1, div_2, div_3, and div_4.

$$\begin{array}{l}\mathsf{insert}(div_0, div_1, 0);\ \mathsf{insert}(div_0, div_2, 1);\ \mathsf{insert}(div_0, div_3, 2);\\ \mathsf{if}(h)\{\mathsf{insert}(div_1, div_4, 0)\}\ \mathsf{else}\ \{null\};\ l = \mathsf{len}_\ell\,(div_0)\end{array} \quad (5)$$

Depending on the value of h, l may be set either to 4 or 5. In order to tackle this type of leak, we require the programmer to pre-establish for each possible tag name m an upper bound on the position levels of the nodes with that tag name, that we denote by σ_m and call *global position level*. For instance, $\sigma_{\mathbf{DIV}}$

corresponds to the pre-established upper bound on the position levels of DIV nodes. In order to allow the execution of $\mathsf{len}_{\not z}$ to go through, the monitor checks whether the position levels of all nodes in the forest are lower than or equal to the global position level, in which case the level associated with the expression is the global position level. Therefore, for Program 5 to be legal $\sigma_{\mathbf{DIV}}$ must be set to H. Accordingly, the expression $\mathsf{len}_{\not z}(div_0)$ yields a value of level H.

Leaks via $\mathsf{move}_{\not z}$. As the primitive $\mathsf{move}_{\not z}$ traverses the tree in document order, it can be used to encode a new type of *order leak*. Let us modify Program 5 by replacing the last instruction with $l = \mathsf{move}_{\not z}(div_0, \text{“}DIV\text{”}, 3)$. Then, depending on the value of the *high* variable h, l is assigned to div_3 or div_2. A NI monitor must detect this information flow and raise the level of the originally *low* variable l to H. In particular, for this program to be legal (according to the current enforcement mechanism), the position level of div_4 as well as the structure security level of div_1 must be *high*. All other levels can be set to L. In the following figures, **a)** and **b)** represent the final forests obtained from the execution of this program in two distinct memories that initially map the h to 0 and to 1, respectively. Forest **c)** represents their (coinciding) low-projection. Observe that in spite of being evaluated in two low-equal memories and only manipulating visible values, the evaluation of $\mathsf{move}_{\not z}(div_0, \text{“}DIV\text{”}, 3)$ yields two different values.



The key insight for securing the new information flows introduced by the $\mathsf{move}_{\not z}$ primitive is that this primitive allows an attacker to operate on the nodes with the same tag in the same tree as if they were siblings. Hence, it is necessary to adjust the notion of a node's position in order to take into account this new way of traversing the DOM forest. Let the *live index* of a node be its position in the list of nodes obtained by searching its corresponding tree for the nodes with its tag in document order. The position of a node is now understood as the triple consisting of its parent, its index, and its live index. Hence, changing the position of a node in a tree causes the positions of the nodes with the same tag in the same tree with higher live indexes to change. In order to deal with this kind of flow, the proposed enforcement mechanism guarantees that the execution of a live move only goes through if, for every tag name m and node n, the position levels of the nodes with tag m in the tree rooted at n monotonically increase in document order. For instance, in the figure above, the final forest **b)** obtained when $h = 1$ does not comply with this requirement because the position level of div_4 is not lower than or equal to the position level of div_2, while the live index of div_4 is lower than the live index of div_2.

4.3 Revised Attacker Model and Enforcement Mechanism

At the formal level, the introduction of the new live primitives poses two separate problems. First, the low-equality definition must be restated so as to correctly capture the observational power of an attacker disposing of these new primitives. Second, the monitor must be extended in such a way that it remains noninterferent. We modify the definition of low-projection so that an attacker at level σ can additionally see: **(1)** the live indexes of the nodes whose position levels are $\sqsubseteq \sigma$ and **(2)** the number of descendants of visible nodes with a given tag m such that $\sigma_m \sqsubseteq \sigma$. Formally:

$$f \restriction_{\not\iota}^{\Sigma,\sigma} = f \restriction^{\Sigma,\sigma} \cup \{(r, m, i, r') \mid \ f \vdash r \rightsquigarrow_m \omega \ \wedge \ \omega(i) = r' \ \wedge \ \Sigma(r').\mathsf{pos} \sqsubseteq \sigma\}$$
$$\cup \ \{(r, m, n) \mid \ f \vdash r \rightsquigarrow_m \omega \ \wedge \ |\omega| = n \ \wedge \ \sigma_m \sqcup \Sigma(r).\mathsf{node} \sqsubseteq \sigma\}$$

As expected, two labeled forests are low-equal at a given level σ, written $f_0, \Sigma_0 \sim_\sigma^{\not\iota} f_1, \Sigma_1$, if they coincide in their respective low-projections.

We do not modify the previous monitor so that the new low-equality is preserved by monitored executions. Instead, we establish a predicate – $\mathcal{WL}(f, \Sigma)$ – for labeled forests, such that any two labeled forests verifying this predicate and related by the first low-equality are also related by the new low-equality. This is formally stated as follows:

Theorem 2 (Low-Equality Strengthening). *Given two forests f_0 and f_1 respectively labeled by Σ_0 and Σ_1 and a security level σ such that $\mathcal{WL}(f_0, \Sigma_0)$ and $\mathcal{WL}(f_1, \Sigma_1)$ and $f_0, \Sigma_0 \sim_\sigma f_1, \Sigma_1$, it holds that: $f_0, \Sigma_0 \sim_\sigma^{\not\iota} f_1, \Sigma_1$.*

Informally, $\mathcal{WL}(f, \Sigma)$ holds if and only if: **(1)** the position levels of all the nodes in f are lower than or equal to the respective global position levels, **(2)** the position levels of the nodes with the same tag monotonically increase in document order, and **(3)** the position level of every node is higher than or equal to the position levels of all its descendants (meaning that if the position of a node is secret, the positions of all its descendants are also secret). The predicate $\mathcal{WL}(f, \Sigma)$ is defined with the help of a predicate $\mathcal{WL}_{f,\Sigma} \vdash^r \phi_{\not\iota} \rightsquigarrow \phi'_{\not\iota}$, defined below, that holds if the tree rooted at r is well-labeled. The function $\phi_{\not\iota}$ maps each tag name to the position level of the last node with that tag name preceding the node pointed to by r in f in document order. The function $\phi'_{\not\iota}$ maps each tag name to the position level of the last node with that tag name in the tree rooted at r (if no such node exists, $\phi'_{\not\iota}$ coincides with $\phi_{\not\iota}$). Formally, the predicate $\mathcal{WL}(f, \Sigma)$ holds if and only if for all orphan nodes pointed to by a reference r there are two functions $\phi_{\not\iota}$ and $\phi'_{\not\iota}$ such that $\mathcal{WL}_{f,\Sigma} \vdash^r \phi_{\not\iota} \rightsquigarrow \phi'_{\not\iota}$.

Orphan Node

$$\frac{\begin{array}{c} f(r).\mathsf{tag} = m \\ |f(r).\mathsf{children}| = 0 \\ \phi_{\not\iota}(m) \sqsubseteq \Sigma(r).\mathsf{pos} \sqsubseteq \sigma_m \\ \phi'_{\not\iota} = \phi_{\not\iota}\,[m \mapsto \Sigma(r).\mathsf{pos}] \end{array}}{\mathcal{WL}_{f,\Sigma} \vdash^r \phi_{\not\iota} \rightsquigarrow \phi'_{\not\iota}}$$

Non-Orphan Node

$$\frac{\begin{array}{c} f(r).\mathsf{tag} = m \qquad \phi_{\not\iota}(m) \sqsubseteq \Sigma(r).\mathsf{pos} \sqsubseteq \sigma_m \\ |f(r).\mathsf{children}| = n > 0 \qquad \phi^0_{\not\iota} = \phi_{\not\iota}\,[m \mapsto \Sigma(r).\mathsf{pos}] \\ \forall_{0 \le i < n} \ \Sigma(r).\mathsf{pos} \sqsubseteq \Sigma(f(r).\mathsf{children}(i)).\mathsf{pos} \\ \forall_{0 \le i < n} \ \mathcal{WL}_{f,\Sigma} \vdash^{f(r).\mathsf{children}(i)} \phi^i_{\not\iota} \rightsquigarrow \phi^{i+1}_{\not\iota} \end{array}}{\mathcal{WL}_{f,\Sigma} \vdash^r \phi_{\not\iota} \rightsquigarrow \phi^n_{\not\iota}}$$

Finally, the extension of the security monitor to the new live primitives is given in Figure 6. The evaluation of these primitives only goes through if the corresponding forest is well-labeled.

$$\textsc{Live Move}\quad \frac{\sigma' = \sigma_0 \sqcup \sigma_1 \sqcup \sigma_2 \sqcup \Sigma(r).\mathsf{pos} \qquad \mathcal{WL}(f,\Sigma)}{\langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1 :: \sigma_2 \rangle \overset{\natural\,(f,r)}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \sigma' \rangle}$$

$$\textsc{Live Length}\quad \frac{\sigma' = \sigma_0 \sqcup \sigma_1 \sqcup \sigma_m \sqcup \Sigma(r).\mathsf{node} \qquad \mathcal{WL}(f,\Sigma)}{\langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1 \rangle \overset{\mathsf{len}_\natural\,(f,r,m)}{\rightarrow} \langle \Gamma, \Sigma, o, \zeta :: \sigma' \rangle}$$

Fig. 6. Extension of the Monitor to Live Primitives

5 Related Work and Conclusions

The increasing popularity of scripting languages has motivated further research on runtime mechanisms for securing information flow, such as *monitors*. In contrast to *purely dynamic monitors* [3–5] that do not rely on any kind of static analysis, *hybrid monitors* [8, 15, 16] use static analysis to reason about the implicit flows that arise due to untaken execution paths. Given the dynamic nature of tree operations, designing such a static analysis for Core DOM is far from trivial. Hence, we have chosen to present a purely dynamic monitor and we leave the design of its hybrid version for future work.

Russo et al. [13] were the first to study the problem of securing information flow in DOM-like dynamic tree structures. They present a monitor for a WHILE language with primitives for manipulating DOM-like trees and prove it sound. However, references are not modeled in this language; instead, program configurations include the current working node of the program. This is, as the authors point out, the main difference with respect to JavaScript DOM operations, since in JavaScript tree nodes are treated as first-class values. In particular, in [13] it is not possible to change the position of a node in the DOM forest without deleting and re-creating it – its position remains the same during its whole "lifetime". Consequently, the *position level* of a node coincides with its *node level*. By treating nodes as first-class values we were able to give separate treatment to position leaks, which cannot be directly expressed in the language of [13].

Hedin et al. [9] implemented the first information flow monitor for fully-fledged JavaScript together with "statefull information-flow models" for the standard API, as well as several APIs that are present in a browser environment such as the DOM API. The presentation includes an informal explanation on how the problem of live collections returned by the method `getElementsByName` is dealt with. Their approach for dealing with live leaks coincides with the technique we employ to the particular case of the $\mathsf{len}_\natural$ primitive.

Gardner et al. [7] propose a compositional and concise formal specification of the DOM called Minimal DOM. The authors show that their semantics has no redundancy and that it is sufficient to describe the structural kernel of DOM Core Level 1. Additionally, they apply local reasoning based on Separation Logic and prove invariant properties of simple JavaScript programs that interact with the DOM. Given that our aim is to track information flow in the DOM, we use a simplified semantics that allows us to label DOM resources in a natural way. Like Minimal DOM, Core DOM is also compositional. Furthermore, all the primitives of Minimal DOM can be easily translated to Core DOM. Hence, we expect the authors' sufficiency claim to be applicable to Core DOM.

This paper contributes to the challenge of enforcing secure information flow in client-side Web applications by presenting a provably sound flow-sensitive security monitor that enforces noninterference over Core DOM, an expressive

representative subset of the DOM API. The proposed solution tackles open issues in IF security such as references and live collections in dynamic tree structures. By including references and live collections, Core DOM offers the expressive power of the DOM in the form of a simple language that is well tailored for automatic program analysis. We thus believe that it could be re-used in future research on security aspects of the DOM API.

Acknowledgments. This work was partially supported by the Portuguese Government via the PhD grant SFRH/BD/71471/2010.

References

1. The 5th edition of ECMA 262 June 2011. ECMAScript Language Specification. Technical report, ECMA, 2011.
2. A. Almeida Matos, J. Fragoso Santos, and T. Rezk. An IF monitor for a core of DOM. http://web.ist.utl.pt/∼ana.matos/14-AFR-if+monitor+coredom-full.pdf.
3. T. H. Austin and C. Flanagan. Efficient purely-dynamic information flow analysis. In *PLAS*, 2009.
4. T. H. Austin and C. Flanagan. Permissive dynamic information flow analysis. In *PLAS*, 2010.
5. T. H. Austin and C. Flanagan. Multiple facets for dynamic information flow. In *POPL*, 2012.
6. A. Banerjee and D. A. Naumann. Secure information flow and pointer confinement in a Java-like language. In *CSFW*, 2002.
7. P. Gardner, G. Smith, M. J. Wheelhouse, and U. Zarfaty. DOM: Towards a formal specification. In *PLAN-X*, 2008.
8. G. Le Guernic. *Confidentiality Enforcement Using Dynamic Information Flow Analyses*. PhD thesis, Kansas State University, 2007.
9. D. Hedin, B. Birgisson, L. Bello, and A. Sabelfeld. Jsflow: Tracking information flow in JavaScript and its APIs. In *SAC*, 2014.
10. D. Hedin and A. Sabelfeld. Information-flow security for a core of JavaScript. In *CSF*, 2012.
11. W3C Recommendation. DOM: Document Object Model (DOM). Technical report, W3C, 2005.
12. A. Russo and A. Sabelfeld. Dynamic vs. static flow-sensitive security analysis. In *CSF*, 2010.
13. A. Russo, A. Sabelfeld, and A. Chudnov. Tracking information flow in dynamic tree structures. In *ESORICS*, 2009.
14. A. Sabelfeld and A. Russo. From dynamic to static and back: Riding the roller coaster of information-flow control research. In *Ershov Memorial Conference*, 2009.
15. P. Shroff, S. F. Smith, and M. Thober. Dynamic dependency monitoring to secure information flow. In *CSF*, 2007.
16. V. N. Venkatakrishnan, W. Xu, D. C. DuVarney, and R. Sekar. Provably correct runtime enforcement of non-interference properties. In *ICICS*, 2006.

A Proofs of Section 3

A.1 Allocator

Definition 2 formalizes the notion of *parametric allocator*. An allocator is a function (with internal state) that given a forest and a security level produces a new reference r. An allocator is said to be *parametric* if given two low-equal forests and the same security level, it produces the same new reference.

Definition 2 (Parametric Allocator). *An allocator $fresh$ is said to be parametric if given two forests f_0 and f_1 respectively labeled by Σ_0 and Σ_1 and a security level σ such that the number of nodes in $\{r \mid \Sigma_0(r).\mathsf{node} \sqsubseteq \sigma\}$ coincides with the number of nodes in $\{r \mid \Sigma_1(r).\mathsf{node} \sqsubseteq \sigma\}$, it follows that: $fresh(f_0, \sigma) = fresh(\sigma_1, \sigma)$.*

Lemma 1 (Node Creation in Low-Equal Forests). *Given two forests f_0 and f_1 respectively labeled by Σ_0 and Σ_1 and a security level σ such that $f_0, \Sigma_0 \sim_\sigma f_1, \Sigma_1$, it follows that: $fresh(f_0, \sigma) = fresh(f_1, \sigma)$.*

Proof. If $f_0, \Sigma_0 \sim_\sigma f_1, \Sigma_1$, we conclude that the number of visible nodes in f_0 (that is, nodes with an observable node level) coincides with the number of visible nodes in f_1. Hence, it follows that: $fresh(f_0, \sigma) = fresh(f_1, \sigma)$. □

A.2 Low-Equality for Lists

Informally, two lists of labeled values are low-equal with respect to a given security level σ, if for each position of both sequences, either the two values in that position coincide, or the levels that are associated with both of them are $\not\sqsubseteq \sigma$. Definition 3 formalizes this notion.

Definition 3 (Low-Equality for Sequences). *Two lists of values ω and ω' respectively labeled by two lists of security levels ζ and ζ' are said to be low-equal w.r.t. a security level σ, written $\omega, \zeta \sim_\sigma \omega', \zeta'$ if the following hold:* **(1)** $\forall_{0 \leq i < n}\ \zeta(i) \sqcap \zeta'(i) \sqsubseteq \sigma \Rightarrow \omega(i) = \omega'(i) \ \wedge\ \zeta(i) = \zeta'(i) \sqsubseteq \sigma$, **(2)** $\forall_{n < i < |\zeta|}\ \zeta(i) \not\sqsubseteq \sigma$, *and* **(3)** $\forall_{n < i < |\zeta'|}\ \zeta'(i) \not\sqsubseteq \sigma$, *where* $n = \mathsf{min}(|\zeta|, |\zeta'|)$.

Given a list of security levels used as a control context o, we define the low-projection of o w.r.t. a given security level σ, written $o \restriction^\sigma$ as the prefix of o that only contains levels $\sqsubseteq \sigma$.

A.3 Contexts and Low-Equality for Contexts

We introduce a new function $\mathsf{pvalues}$ that given a context, returns the list containing the values in that context that were already evaluated in *evaluation order*. Definition 4 formalizes this notion.

Definition 4 (Context Parsed Values). *Given a context E, we recursively define* $\mathsf{pvalues}(E)$ *as follows:*

$$
\begin{array}{llll}
\mathsf{pvalues}([]) & = \epsilon & \mathsf{pvalues}(x = E) & = \mathsf{pvalues}(E) \\
\mathsf{pvalues}(\mathsf{if}(E)\{e\}\ \mathsf{else}\ \{e\}) & = \mathsf{pvalues}(E) & \mathsf{pvalues}(\mathsf{while}^e(E)\{e\}) & = \mathsf{pvalues}(E) \\
\mathsf{pvalues}(E; e) & = \mathsf{pvalues}(E) & \mathsf{pvalues}(\mathsf{end}(E)) & = \mathsf{pvalues}(E) \\
\mathsf{pvalues}(\mathsf{move}_{\uparrow}(E)) & = \mathsf{pvalues}(E) & \mathsf{pvalues}(\mathsf{move}_{\downarrow}(E, e)) & = \mathsf{pvalues}(E) \\
\mathsf{pvalues}(\mathsf{move}_{\downarrow}(\underline{v}, E)) & = \underline{v} :: \mathsf{pvalues}(E) & \mathsf{pvalues}(\mathsf{remove}(E, e)) & = \mathsf{pvalues}(E) \\
\mathsf{pvalues}(\mathsf{remove}(\underline{v}, E)) & = \underline{v} :: \mathsf{pvalues}(E) & \mathsf{pvalues}(\mathsf{insert}(\underline{v}, E, e)) & = \underline{v} :: \mathsf{pvalues}(E) \\
\mathsf{pvalues}(\mathsf{new}^{\sigma_0,\sigma_1,\sigma_2}(E)) & = \mathsf{pvalues}(E) & \mathsf{pvalues}(\mathsf{insert}(\underline{v}_0, \underline{v}_1, e)) & = \underline{v}_0 :: \underline{v}_1 :: \mathsf{pvalues}(E) \\
\mathsf{pvalues}(\mathsf{value}(E)) & = \mathsf{pvalues}(E) & \mathsf{pvalues}(\mathsf{store}(E, e)) & = \mathsf{pvalues}(E) \\
\mathsf{pvalues}(\mathsf{store}(\underline{v}, E)) & = \underline{v} :: \mathsf{pvalues}(E) & \mathsf{pvalues}(\mathsf{len}(E)) & = \mathsf{pvalues}(E)
\end{array}
$$

We extend the notion of low-projection to contexts paired up with a list of security levels corresponding to the control context. Hence, given an execution context E and a control context ζ, $E \upharpoonright^{o,\sigma}$ denotes the context obtained from E by removing its subcontext that is not observable. For instance, $(\mathsf{end}(\mathsf{end}(x = []); x = 1)) \upharpoonright^{L::H,L} = \mathsf{end}([]; x = 1)$.

Definition 5 (Context Low-Projection). *Given a context E and control context o, we define the low-projection of E at a level σ w.r.t. o recursively as follows:*

$$E \upharpoonright^{o::\sigma',\sigma} = \begin{cases} E & \text{if } \sigma' \sqsubseteq \sigma \\ \mathsf{flush}(E) \upharpoonright^{o,\sigma} & \text{otherwise} \end{cases}$$

where $\mathsf{flush}(E) = E'$ *if and only if* $E = E'[\mathsf{end}(E'')]$ *and there are no contexts* $\hat{E}$ *and* $\hat{E}'$ *such that* $E'' = \hat{E}[\mathsf{end}(\hat{E}')]$.

Using the definition of low-projection for contexts, we extend the definition of low-equality for contexts paired up with the corresponding control and expression contexts. In the following, we use **(1)** $|E|$ as an abbreviation for $|\mathsf{pvalues}(E)|$, **(2)** $\lceil\omega\rceil_n$ for the list containing the first n elements of ω, **(3)** $\lfloor\omega\rfloor_n$ for the list containing the last n elements of ω, and **(4)** $\omega.\mathsf{last}$ for the last element of ω.

Definition 6 (Low-Equality for Contexts). *Given two contexts E_0 and E_1 each paired up with two lists of security levels o_0 and ζ_0 and o_1 and ζ_1 and a security level σ, we say that E_0 is low-equal to E_1 w.r.t. o_0, ζ_0, o_1, and ζ_1 and σ, written $E_0, o_0, \zeta_0 \sim_\sigma E_1, o_1, \zeta_1$, if and only if* $\mathsf{pvalues}(E_0'), \lceil\zeta_0\rceil_{|E_0'|} \sim_\sigma \mathsf{pvalues}(E_1'), \lceil\zeta_1\rceil_{|E_1'|}$, *where* $E_0' = E_0 \upharpoonright^{o_0,\sigma}$ *and* $E_1' = E_1 \upharpoonright^{o_1,\sigma}$.

A.4 Redexes and Low-Equality for Redexes

Let us define a *redex* as an expression $\bar{e}$ for which there is no context E different from $[]$ and expression e such that $\bar{e} = E[e]$. Definition 7 extends $\mathsf{pvalues}$ to rexedes.

Definition 7 (Runtime Values of a Redex). *Given a redex $\bar{e}$, we define* $\mathsf{pvalues}(\bar{e})$ *as follows:*

$$
\begin{array}{llll}
\mathsf{pvalues}(v) & = \epsilon & \mathsf{pvalues}(x) & = \epsilon \\
\mathsf{pvalues}(x = \underline{v}) & = \epsilon :: \underline{v} & \mathsf{pvalues}(\underline{v}; e_0) & = \epsilon :: \underline{v} \\
\mathsf{pvalues}(\mathsf{end}(\underline{v})) & = \epsilon :: \underline{v} & \mathsf{pvalues}(\mathsf{while}(e_0)\{e_1\}) & = \epsilon \\
\mathsf{pvalues}(\mathsf{while}^{e_0}(\underline{v})\{e_1\}) & = \epsilon :: \underline{v} & \mathsf{pvalues}(\mathsf{if}(\underline{v})\{e_0\}\ \mathsf{else}\ \{e_1\}) & = \epsilon :: \underline{v} \\
\mathsf{pvalues}(\mathsf{move}_{\uparrow}(r)) & = \epsilon :: r & \mathsf{pvalues}(\mathsf{move}_{\downarrow}(r, i)) & = \epsilon :: r :: i \\
\mathsf{pvalues}(\mathsf{len}(r)) & = \epsilon :: r & \mathsf{pvalues}(\mathsf{remove}(r, i)) & = \epsilon :: r :: i \\
\mathsf{pvalues}(\mathsf{insert}(r, r', i)) & = \epsilon :: r :: r' :: i & \mathsf{pvalues}(\mathsf{value}(r)) & = \epsilon :: r \\
\mathsf{pvalues}(\mathsf{store}(r, \underline{v})) & = \epsilon :: r :: \underline{v} & \mathsf{pvalues}(\mathsf{new}^{\sigma_0,\sigma_1,\sigma_2}(m)) & = \epsilon :: m
\end{array}
$$

We say that two redexes $\bar{e}$ and $\bar{e}'$ are *equal up to runtime-values*, written $\bar{e} \equiv \bar{e}'$, if they only differ in runtime values. We use $|\bar{e}|$ as an abbreviaton for $|\mathsf{pvalues}(\bar{e})|$.

We extend the definition of low-equality to redexes, each paired up with a list of security levels in the following way. Two redexes $\bar{e}_0$ and $\bar{e}_1$ paired up with two lists of security levels ζ_0 and ζ_1 respectively are said to be low-equal at level σ, written $\bar{e}_0, \zeta_0 \sim_\sigma \bar{e}_1, \zeta_1$, if and only if $\bar{e}_0 \equiv \bar{e}_1$ and $\mathsf{pvalues}(\bar{e}_0), \zeta_0 \sim_\sigma \mathsf{pvalues}(\bar{e}_1), \zeta_1$.

A.5 Low-Equality for Configurations

We say that a monitored configuration *cfgm* is *final* if there exist a memory μ, a forest f, a runtime value $\underline{v}$, a variable labeling Γ, a node labeling Σ, and a security level σ, such that:

$$cfgm = \langle\langle \mu, f, \underline{v}\rangle, \langle \Gamma, \Sigma, \epsilon, \epsilon :: \sigma\rangle\rangle$$

A configuration *cfgm* is *convergent* if there is a final configuration $cfgm'$ such that: $cfgm \rightarrow^* cfgm'$.

Finally, Definitions 8 and 9 extend the notion of low-equality for intermediate and final configurations respectively. An intermediate configuration is never low-equal to a final configuration.

Definition 8 (Low-Equality for Monitored Intermediate Confs). *Two monitored confs. $\langle\langle \mu, f, E[\bar{e}]\rangle, \langle \Gamma, \Sigma, o, \zeta\rangle\rangle$ and $\langle\langle \mu', f', E'[\bar{e}']\rangle, \langle \Gamma', \Sigma', o', \zeta'\rangle\rangle$ are said to be low-equal at level σ, written:*

$$\langle\langle \mu, f, E[\bar{e}]\rangle, \langle \Gamma, \Sigma, o, \zeta\rangle\rangle \sim_\sigma \langle\langle \mu', f', E'[\bar{e}']\rangle, \langle \Gamma', \Sigma', o', \zeta'\rangle\rangle$$

if: **(1)** $\mu, \Gamma \sim_\sigma \mu', \Gamma'$, **(2)** $f, \Sigma \sim_\sigma f', \Sigma'$, **(3)** $E, o, \zeta \sim_\sigma E', o', \zeta'$, **(4)** $o \restriction^\sigma = o' \restriction^\sigma$, *and* **(5)** $level(o) \sqcap level(o') \sqsubseteq \sigma \Rightarrow level(o) \sqcup level(o') \sqsubseteq \sigma \wedge \bar{e}, \lfloor\zeta\rfloor_{|\bar{e}|} \sim_\sigma \bar{e}', \lfloor\zeta'\rfloor_{|\bar{e}'|}$.

Definition 9 (Low-Equality for Monitored Final Confs). *Two monitored final confs. $\langle\langle \mu, f, \underline{v}\rangle, \langle \Gamma, \Sigma, \epsilon, \epsilon :: \hat{\sigma}\rangle\rangle$ and $\langle\langle \mu', f', \underline{v}'\rangle, \langle \Gamma', \Sigma', \epsilon, \epsilon :: \hat{\sigma}'\rangle\rangle$ are said to be low-equal at level σ, written:*

$$\langle\langle \mu, f, \underline{v}\rangle, \langle \Gamma, \Sigma, \epsilon, \epsilon :: \hat{\sigma}\rangle\rangle \sim_\sigma \langle\langle \mu', f', \underline{v}'\rangle, \langle \Gamma', \Sigma', \epsilon, \epsilon :: \hat{\sigma}'\rangle\rangle$$

if: **(1)** $\mu, \Gamma \sim_\sigma \mu', \Gamma'$, **(2)** $f, \Sigma \sim_\sigma f', \Sigma'$, *and* **(3)** $\hat{\sigma} \sqcap \hat{\sigma}' \sqsubseteq \sigma \Rightarrow \hat{\sigma} \sqcup \hat{\sigma}' \sqsubseteq \sigma \wedge \underline{v} = \underline{v}'$.

A.6 Confinement Lemmas

Here we present all the confinement lemmas used in the proof of noninterference. Intuitively, a transition of the monitored semantics is *confined* if, whenever it occurs in a *high* context, it produces a configuration that is *low-equal* to the initial configuration.

Lemma 2 (Strong Confinement for Storing). *Given a memory μ labeled by Γ, a forest f labeled by Σ, a control context o, an expression context ζ, an evaluation context E, a reference r_0, a runtime value $\underline{v}_1$, and three security levels σ_0, σ_1, and σ such that: $level(o) \sqcup \sigma_0 \not\sqsubseteq \sigma$ (hyp.1) and:*

$$\langle\langle \mu, f, E[\mathsf{store}(r_0, \underline{v}_1)]\rangle, \langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1\rangle\rangle \rightarrow \langle\langle \mu, f', E[\underline{v}_1]\rangle, \langle \Gamma, \Sigma, o, \zeta :: \sigma_1\rangle\rangle$$

(hyp.2), it holds that $f \upharpoonright^{\Sigma,\sigma} = f' \upharpoonright^{\Sigma,\sigma}$.

Proof. Letting $\omega_0 = f(r_0).\mathsf{children}$, $m_0 = f(r_0).\mathsf{tag}$, $\underline{v}_0 = f(r_0).\mathsf{value}$, $\hat{r} = f(r_0).\mathsf{parent}$, and $\sigma' = level(o) \sqcup \sigma_0 \sqcup \sigma_1 \sqcup \Sigma(r_0).\mathsf{node}$, we conclude that:

- $f' = f\,[r_0 \mapsto \langle m_0, \underline{v}_1, \hat{r}, \omega_0\rangle]$ — (1) - (hyp.2)
- $\Sigma' = \Sigma\,[r_0 \mapsto \langle \Sigma(r_0).\mathsf{node}, \sigma', \Sigma(r_0).\mathsf{pos}, \Sigma(r_0).\mathsf{struct}\rangle]$ — (2) - (hyp.2)
- $level(o) \sqcup \sigma_0 \sqsubseteq \Sigma(r_0).\mathsf{value}$ — (3) - (hyp.2)
- $\Sigma(r).\mathsf{value} \not\sqsubseteq \sigma$ — (4) - (hyp.1) + (3)
- $(r, \underline{v}_0, \Sigma(r_0).\mathsf{value}) \notin f \upharpoonright^{\Sigma,\sigma}$ — (5) - (4)
- $\sigma' \not\sqsubseteq \sigma$ — (6) - (hyp.1)
- $(r, \underline{v}_1, \Sigma'(r_0).\mathsf{value}) \notin f' \upharpoonright^{\Sigma',\sigma}$ — (7) - (hyp.2) + (6)
- $f \upharpoonright^{\Sigma,\sigma} = f' \upharpoonright^{\Sigma',\sigma}$ — **(10)** - (hyp.2)+(5)+(7)

□

Lemma 3 (Strong Confinement for Removal). *Given a memory μ labeled by Γ, a forest f labeled by Σ, a control context o, an expression context ζ, an evaluation context E, a reference r_0, a runtime integer i, and three security levels σ_0, σ_1, and σ such that: $level(o) \sqcup \sigma_0 \sqcup \sigma_1 \not\sqsubseteq \sigma$ (hyp.1) and:*

$$\langle\langle \mu, f, E[\mathsf{remove}(r_0, i)]\rangle, \langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1\rangle\rangle \rightarrow \langle\langle \mu, f', E[r']\rangle, \langle \Gamma, \Sigma, o, \zeta :: \sigma'\rangle\rangle$$

for some reference r' (hyp.2), it holds that $f \upharpoonright^{\Sigma,\sigma} = f' \upharpoonright^{\Sigma,\sigma}$.

Proof. Letting $\omega_0 = f(r_0).\mathsf{children}$, $m_0 = f(r_0).\mathsf{tag}$, $\underline{v}_0 = f(r_0).\mathsf{value}$, $\hat{r} = f(r_0).\mathsf{parent}$, $m' = f(r').\mathsf{tag}$, $\underline{v}' = f(r').\mathsf{value}$, $\omega' = f(r').\mathsf{children}$, we conclude that:

- $\omega_0(i) = r'$ — (1) - (hyp.2)
- $f' = f\,[r_0 \mapsto \langle m_0, \underline{v}_0, \hat{r}, Shift_L(\omega_0, i)\rangle, r' \mapsto \langle m', \underline{v}', null, \omega'\rangle]$ — (2) - (hyp.2)
- $level(o) \sqcup \sigma_0 \sqcup \sigma_1 \sqcup \sigma_2 \sqsubseteq \Sigma(r).\mathsf{struct} \sqcap \Sigma(r').\mathsf{pos}$ — (3) - (hyp.2)
- $\Sigma(r).\mathsf{struct} \sqcap \Sigma(r').\mathsf{pos} \not\sqsubseteq \sigma$ — (4) - (hyp.1) + (3)
- $(r_0, i, r') \notin f \upharpoonright^{\Sigma,\sigma}$ and $(r', null) \notin f' \upharpoonright^{\Sigma,\sigma}$ — (5) - (4)
- $(r_0, |\omega_0|) \notin f \upharpoonright^{\Sigma,\sigma}$ and $(r_0, Shift_L(\omega_0, i)) \notin f' \upharpoonright^{\Sigma,\sigma}$ — (6) - (4)
- $\forall_{i \leq j \leq |\omega_0|}\ \Sigma(\omega_0(j)).\mathsf{pos} \not\sqsubseteq \sigma$ — (7) - (4) + *indexes invariant*
- $\forall_{i \leq j \leq |\omega_0|}\ (r_0, j, \omega_0(j)) \notin f \upharpoonright^{\Sigma,\sigma}$ — (8) - (7)

– $\forall_{i \leq j \mid Shift_L(\omega_0,i)\mid}\ (r_0, j, Shift_L(\omega_0, i)(j)) \notin f' \restriction^{\Sigma,\sigma}$ (9) - (4) + (7)
– $f \restriction^{\Sigma,\sigma} = f' \restriction^{\Sigma,\sigma}$ **(10)** - (5)+(6)+(8)+(9)

□

Lemma 4 (Strong Confinement for Insertion). *Given a memory μ labeled by Γ, a forest f labeled by Σ, a control context o, an expression context ζ, an evaluation context E, two references r_0 and r_1, a runtime integer i, and four security levels σ_0, σ_1, σ_2, and σ such that: $level(o) \sqcup \sigma_0 \sqcup \sigma_1 \sqcup \sigma_2 \not\sqsubseteq \sigma$ (hyp.1) and:*

$$\langle\langle \mu, f, E[\mathsf{insert}(r_0, r_1, i)]\rangle, \langle \Gamma, \Sigma, o, \zeta :: \sigma_0 :: \sigma_1 :: \sigma_2\rangle\rangle \rightarrow \langle\langle \mu, f', E[r_1]\rangle, \langle \Gamma, \Sigma, o, \zeta :: \sigma_1\rangle\rangle$$

(hyp.2), it holds that $f \restriction^{\Sigma,\sigma} = f' \restriction^{\Sigma,\sigma}$.

Proof. Letting $\omega_0 = f(r_0).\mathsf{children}$, $m_0 = f(r_0).\mathsf{tag}$, $\underline{v}_0 = f(r_0).\mathsf{value}$, $\hat{r} = f(r_0).\mathsf{parent}$, $m_1 = f(r_1).\mathsf{tag}$, $\underline{v}_1 = f(r_1).\mathsf{value}$, $\omega_1 = f(r_1).\mathsf{children}$, we conclude that:

– $f(r_1).\mathsf{parent} = null$ (1) - (hyp.2)
– $f' = f\,[r_0 \mapsto \langle m_0, \underline{v}_0, \hat{r}, Shift_R(\omega_0, i, r_1)\rangle, r_1 \mapsto \langle m_1, \underline{v}_1, r_0, \omega_1\rangle]$ (2) - (hyp.2)
– $level(o) \sqcup \sigma_0 \sqcup \sigma_1 \sqcup \sigma_2 \sqsubseteq \Sigma(r_0).\mathsf{struct} \sqcap \Sigma(r_1).\mathsf{pos}$ (3) - (hyp.2)
– $\Sigma(r_0).\mathsf{struct} \sqcap \Sigma(r_1).\mathsf{pos} \not\sqsubseteq \sigma$ (4) - (hyp.1) + (3)
– $(r_1, null) \notin f \restriction^{\Sigma,\sigma}$ and $(r_0, i, r_1) \notin f' \restriction^{\Sigma,\sigma}$ (5) - (4)
– $(r_0, |\omega_0|) \notin f \restriction^{\Sigma,\sigma}$ and $(r_0, Shift_R(\omega_0, i, r_1)) \notin f' \restriction^{\Sigma,\sigma}$ (6) - (4)
– $\forall_{i \leq j \mid \omega_0 \mid}\ \Sigma(\omega_0(j)).\mathsf{pos} \not\sqsubseteq \sigma$ (7) - (4) + *indexes invariant*
– $\forall_{i \leq j \mid \omega_0 \mid}\ (r_0, j, \omega_0(j)) \notin f \restriction^{\Sigma,\sigma}$ (8) - (7)
– $\forall_{i \leq j \mid Shift_R(\omega_0,i,r_1)\mid}\ (r_0, j, Shift_R(\omega_0, i, r_1)(j)) \notin f' \restriction^{\Sigma,\sigma}$ (9) - (4) + (7)
– $f \restriction^{\Sigma,\sigma} = f' \restriction^{\Sigma,\sigma}$ **(10)** - (5)+(6)+(8)+(9)

□

Lemma 5 (Strong Confinement for Node Creation). *Given a memory μ labeled by Γ, a forest f labeled by Σ, a control context o, an expression context ζ, an evaluation context E, a strings m, and five security levels σ_0, σ_1, σ_2, σ', and σ such that: $level(o) \sqcup \sigma' \not\sqsubseteq \sigma$ (hyp.1) and:*

$$\langle\langle \mu, f, E[\mathsf{new}^{\sigma_0,\sigma_1,\sigma_2}(m)]\rangle, \langle \Gamma, \Sigma, o, \zeta :: \sigma'\rangle\rangle \rightarrow \langle\langle \mu, f', E[r]\rangle, \langle \Gamma, \Sigma, o, \zeta :: \sigma_0\rangle\rangle$$

(hyp.2), it holds that $f \restriction^{\Sigma,\sigma} = f' \restriction^{\Sigma,\sigma}$.

Proof. We conclude that:

– $r = fresh(f, \sigma_0)$, $f' = f\,[r \mapsto \langle m, null, null, \epsilon\rangle]$, $\Sigma' = \Sigma\,[r \mapsto \langle \sigma_0, \sigma_0, \sigma_1, \sigma_2\rangle]$, $level(o) \sqcup \sigma' \sqsubseteq \sigma_0 \sqsubseteq \sigma_1 \sqcap \sigma_2$ (1) - (hyp.2)
– $\sigma_0 \sqcap \sigma_1 \sqcap \sigma_2 \not\sqsubseteq \sigma$ (2) - (hyp.1) + (1)
– $f \restriction^{\Sigma,\sigma} = f' \restriction^{\Sigma,\sigma}$ (3) - (1) + (2)

□

Lemma 6 (Confined Value Generating One-Step Transition). *Given a monitored configuration $\langle\langle \mu, f, E[\bar{e}]\rangle, \langle \Gamma, \Sigma, o, \zeta\rangle\rangle$ such that $level(o) \not\sqsubseteq \sigma$ (hyp.1) and:*

$$\langle\langle \mu, f, E[\bar{e}]\rangle, \langle \Gamma, \Sigma, o, \zeta\rangle\rangle \rightarrow \langle\langle \mu', f', E[\underline{v}]\rangle, \langle \Gamma', \Sigma', o, \zeta' :: \sigma'\rangle\rangle$$

(hyp.2), it holds that: **(1)** $\mu \restriction^{\Gamma,\sigma} = \mu' \restriction^{\Gamma',\sigma}$, **(2)** $f \restriction^{\Sigma,\sigma} = f' \restriction^{\Sigma',\sigma}$, *and* **(3)** $\sigma' \not\sqsubseteq \sigma$.

Proof. The interesting cases are those that modify the memory: [Store], [Remove], [Insert], [New], and [Assignment]. The first four were dealt separately in Lemmas 2 to 5. Since, all other cases do not modify the memory, we only give the proof for the case [Assignment].

[Assignment] $\bar{e} = x = \underline{v}$ for a given variable x and a runtime value $\underline{v}$.

- $\mu' = \mu\,[x \mapsto \underline{v}]$, $f' = f$, $\Sigma' = \Sigma$, $level(o) \sqsubseteq \Gamma(x)$, and $\Gamma' = \Gamma\,[x \mapsto level(o) \sqcup \sigma]$ (1) - (hyp.2)
- $\Gamma(x) \not\sqsubseteq \sigma$ (2) - (hyp.1) + (1)
- $f \restriction^{\Sigma,\sigma} = f \restriction^{\Sigma,\sigma}$ (3) - (hyp.2) + (2)

□

Lemma 7 (Confined One-Step Transition). *Given a monitored configuration $\langle\langle \mu, f, E[\bar{e}]\rangle, \langle \Gamma, \Sigma, o, \zeta\rangle\rangle$ such that $level(o) \not\sqsubseteq \sigma$ (hyp.1):*

$$\langle\langle \mu, f, E[\bar{e}]\rangle, \langle \Gamma, \Sigma, o, \zeta\rangle\rangle \rightarrow \langle\langle \mu', f', E'[\bar{e}']\rangle, \langle \Gamma', \Sigma', o', \zeta'\rangle\rangle$$

It holds that:

$$\langle\langle \mu, f, E[\bar{e}]\rangle, \langle \Gamma, \Sigma, o, \zeta\rangle\rangle \sim_\sigma \langle\langle \mu', f', E'[\bar{e}']\rangle, \langle \Gamma', \Sigma', o', \zeta'\rangle\rangle$$

Proof. Denoting by (hyp.2) the second hypothesis of the lemma, we conclude that:

- $\mu, \Gamma \sim_\sigma \mu', \Gamma'$ and $f, \Sigma \sim_\sigma f', \Sigma'$ (1) - (hyp.1,2) + *Confinement*
- $E' \restriction^{o',\sigma} = E \restriction^{o,\sigma}$. There are two cases to consider. Either $o' = o$ or $o' \neq o$. Suppose that $o' = o$ (hyp.3) and $o' = o'' :: \sigma'$ for some level σ' and list o'' (hyp.4). It follows that:
  - $E \restriction^{o,\sigma} = \mathsf{flush}(E) \restriction^{o'',\sigma}$ (2.1) - (hyp.1,3,4)
  - $\mathsf{flush}(E) = \mathsf{flush}(E')$ (2.2) - (hyp.2,3)
  - $E' \restriction^{o,\sigma} = \mathsf{flush}(E') \restriction^{o'',\sigma}$ (2.3) - (hyp.1,3,4)
  - $E \restriction^{o,\sigma} = E' \restriction^{o',\sigma}$ (2.4) - (hyp.3) + (2.1-2.3)

  Suppose that $o' \neq o$ (hyp.3) and $o = o'' :: \sigma'$ for some level σ' and list o'' (hyp.4):
  - $E \restriction^{o,\sigma} = \mathsf{flush}(E) \restriction^{o'',\sigma}$ (2.5) - (hyp.1,3,4)
  - $\mathsf{flush}(E) = E'$ and $o' = o''$ (2.6) - (hyp.2,3)
  - $E \restriction^{o,\sigma} = E' \restriction^{o'',\sigma}$ (2.7) - (2.5, 2.6)

  Let n be $|\mathsf{pvalues}(\bar{e})|$, we conclude that:

- $\forall_{0 \leq i < n}\ \lfloor\zeta\rfloor_n(i) \not\sqsubseteq \sigma$ where . (3) - (hyp.3) + *High Redexes*
- $\zeta' = \zeta'' \oplus \zeta'''$, $\zeta = \zeta'' \oplus \lfloor\zeta\rfloor_n$, and $\forall_{0 \leq i < k}\ \zeta'''(i) \not\sqsubseteq \sigma$, where $k = |\zeta'''|$ (4) - (hyp.1,2) + *Confinement*
- $\zeta \sim_\sigma \zeta'$ (5) - (3,4) + *High Suffix Replacement*

□

A.7 Noninterference

In the following, we make use of a new transition relation $\rightarrow^{\mathbf{1},\sigma}$ between configurations that is defined as follows: $cfgm_0 \rightarrow^{\mathbf{1},\sigma} cfgm_1$ *if and only if* there is a configuration $cfgm'_0$ such that: **(1)** $cfgm_0 \rightarrow^* cfgm'_0$, **(2)** $cfgm'_0 \rightarrow cfgm_0$, **(3)** all the steps in **(1)** are performed in invisible contexts, and **(4)** the step **(2)** is performed in a visible context. Observe that since the execution of every program is assumed to start with the empty control stack, all programs perform at least one transition of $\rightarrow^{\mathbf{1},L}$. In the following, we write $cfgm \rightarrow^{\mathbf{n},\sigma} cfgm'$ if there are $n-1$ configurations $cfgm_1, \cdots, cfgm_{n-1}$ such that: $cfgm_1 \rightarrow^{\mathbf{1},\sigma} cfgm_2 \rightarrow^{\mathbf{1},\sigma} \cdots \rightarrow^{\mathbf{1},\sigma} cfgm_{n-1} \rightarrow^{\mathbf{1},\sigma} cfgm'$. Intuitively, $cfgm \rightarrow^{\mathbf{n},\sigma} cfgm'$ if $cfgm$ evaluates to $cfgm'$ in n *low* steps. Finally, we write $cfgm_0 \rightarrow^*_\sigma cfgm'$ if either $cfgm' = cfgm_0$ or there is a finite number n (possibly equal to 0) of configurations $cfgm_1, \cdots, cfgm_n$ such that: $cfgm_0 \rightarrow cfgm_1 \rightarrow \cdots \rightarrow cfgm_n \rightarrow cfgm'$ and for every $0 \leq i \leq n$ $level(o_i) \not\sqsubseteq \sigma$, where o_i is the control context of $cfgm_i$.

Lemma 8 (Low-Value Generating One-Step Transition). *Given two configurations* $\langle\langle \mu_0, f_0, E_0[\bar{e}_0]\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle$ *and* $\langle\langle \mu_1, f_1, E_1[\bar{e}_1]\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle$ *such that:*

- $\bar{e}_0 \equiv \bar{e}_1$ *(hyp.1)*
- $\langle\langle \mu_0, f_0, E_0[\bar{e}_0]\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle \sim_\sigma \langle\langle \mu_1, f_1, E_1[\bar{e}_1]\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle$ *(hyp.2)*
- $\langle\langle \mu_0, f_0, E_0[\bar{e}_0]\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle \rightarrow \langle\langle \mu'_0, f'_0, E_0[\underline{v}_0]\rangle, \langle \Gamma'_0, \Sigma'_0, o'_0, \zeta'_0\rangle\rangle$ *(hyp.3)*
- $\langle\langle \mu_1, f_1, E_1[\bar{e}_1]\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle \rightarrow \langle\langle \mu'_1, f'_1, E_1[\underline{v}_1]\rangle, \langle \Gamma'_1, \Sigma'_1, o'_1, \zeta'_1\rangle\rangle$ *(hyp.4)*
- $level(o_0) \sqcup level(o_1) \sqsubseteq \sigma$ *(hyp.5)*

Then: $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$, $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ *and if either* $o'_0.\mathsf{last} \sqsubseteq \sigma$ *or* $o'_1.\mathsf{last} \sqsubseteq \sigma$, *then:* $o'_0.\mathsf{last} = o'_1.\mathsf{last}$ *and* $\underline{v}_0 = \underline{v}_1$.

Proof. We proceed by case analysis on the semantic transitions that yield parsed values.
[Identifier] $redex_0 = x$ for some variable x (hyp.6). We conclude that:

- $\bar{e}_1 = x$ (1) - (hyp.1) + (hyp.6)
- $\mu_0 = \mu'_0$, $\Gamma_0 = \Gamma'_0$, $f_0 = f'_0$, and $\Sigma_0 = \Sigma'_0$ (2) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu'_1$, $\Gamma_1 = \Gamma'_1$, $f_1 = f'_1$, and $\Sigma_1 = \Sigma'_1$ (3) - (hyp.4) + (2)
- $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$ and $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ **(4)** - (hyp.2) + (2) + (3)
- $o'_0.\mathsf{last} = \Gamma_0(x)$, $o'_1.\mathsf{last} = \Gamma_1(x)$, $\underline{v}_0 = \mu_0(x)$, and $\underline{v}_1 = \mu_1(x)$ (5) - (hyp.3) + (hyp.4) + (hyp.6) + (1)
- $\Gamma_0(x) \sqcap \Gamma_1(x) \sqsubseteq \sigma \Rightarrow \mu_0(x) = \mu_1(x) \wedge \Gamma_0(x) = \Gamma_1(x) \sqsubseteq \sigma$ (6) - (hyp.2)
- $o'_0.\mathsf{last} \sqcap o'_1.\mathsf{last} \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge o'_0.\mathsf{last} = o'_1.\mathsf{last} \sqsubseteq \sigma$ **(7)** - (5) + (6)

[Assignment] $\bar{e}_0 = x = \underline{v}_0$ for some variable x and parsed value $\underline{v}_0$ (hyp.6). Letting $\zeta_0 = \zeta''_0 :: \sigma_0$ and $\zeta_1 = \zeta''_1 :: \sigma_1$, we conclude that:

- $\bar{e}_1 = x = \underline{v}_1$ (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $f_0 = f'_0$, and $\Sigma_0 = \Sigma'_0$, $f_1 = f'_1$, and $\Sigma_1 = \Sigma'_1$ **(3)** - (hyp.3) + (hyp.4) + (hyp.6) + (1)

- $\mu_0' = \mu_0\,[x \mapsto \underline{v}_0]$, $\Gamma_0' = \Gamma_0\,[x \mapsto \sigma_0]$, $\mu_1' = \mu_1\,[x \mapsto \underline{v}_1]$, and $\Gamma_1' = \Gamma_1\,[x \mapsto \sigma_1]$ (4) - (hyp.3) + (hyp.4) + (hyp.6) + (1)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ **(5)** - (hyp.2) + (2) + (4)
- $o_0'.\mathsf{last} = \sigma_0$, $o_1'.\mathsf{last} = \sigma_1$ (6) - (hyp.3) + (hyp.4) + (hyp.6) + (1)
- $o_0'.\mathsf{last} \sqcap o_1'.\mathsf{last} \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge o_0'.\mathsf{last} = o_1'.\mathsf{last} \sqsubseteq \sigma$ **(7)** - (2) + (6)

[End] $\bar{e}_0 = \mathsf{end}(\underline{v}_0)$ for some value $\underline{v}_0$ (hyp.6). Letting $\zeta_0 = \zeta_0'' :: \sigma_0$ and $\zeta_1 = \zeta_1'' :: \sigma_1$, we conclude that:

- $\bar{e}_1 = \mathsf{end}(\underline{v}_1)$ (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu_0'$, $\Gamma_0 = \Gamma_0'$, $f_0 = f_0'$, and $\Sigma_0 = \Sigma_0'$ (3) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu_1'$, $\Gamma_1 = \Gamma_1'$, $f_1 = f_1'$, and $\Sigma_1 = \Sigma_1'$ (4) - (hyp.4) + (1)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ and $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(5)** - (hyp.2) + (3) + (4)
- $o_0'.\mathsf{last} = \sigma_0$ and $o_1'.\mathsf{last} = \sigma_1$ (6) - (hyp.3) + (hyp.4) + (hyp.6) + (1)
- $o_0'.\mathsf{last} \sqcap o_1'.\mathsf{last} \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge o_0'.\mathsf{last} = o_1'.\mathsf{last} \sqsubseteq \sigma$ **(7)** - (2) + (6)

[Literal Value] $\bar{e}_0 = v$ for some literal value v (hyp.6). We conclude that:

- $\bar{e}_1 = v$ (1) - (hyp.1) + (hyp.6)
- $\mu_0 = \mu_0'$, $\Gamma_0 = \Gamma_0'$, $f_0 = f_0'$, $\Sigma_0 = \Sigma_0'$, and $\underline{v}_0 = \underline{v}$ (2) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu_1'$, $\Gamma_1 = \Gamma_1'$, $f_1 = f_1'$, and $\Sigma_1 = \Sigma_1'$, and $\underline{v}_1 = \underline{v}$ (3) - (hyp.4) + (1)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$, $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$, and $\underline{v}_0 = \underline{v}_1$ **(4)** - (hyp.2) + (2) + (3)
- $o_0'.\mathsf{last} = level(o_0)$ and $o_1'.\mathsf{last} = level(o_1)$ (5) - (hyp.3) + (hyp.4) + (hyp.6) + (1)
- $o_0'.\mathsf{last} \sqcap o_1'.\mathsf{last} \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge o_0'.\mathsf{last} = o_1'.\mathsf{last} \sqsubseteq \sigma$ **(7)** - (hyp.5) + (4) + (5)

[Loop False] $\bar{e}_0 = \mathsf{while}^{e_0}(\underline{v}_0)\{e_1\}$ for some expressions e_0 and e_1 and parsed value $\underline{v}_0 \in V_F$ (hyp.6). Letting $\zeta_0 = \zeta_0'' :: \sigma_0$ and $\zeta_1 = \zeta_1'' :: \sigma_1$, we conclude that:

- $\bar{e}_0 = \mathsf{while}^{e_0}(\underline{v}_1)\{e_1\}$ and $\underline{v}_1 \in V_F$ (1) - (hyp.1) + (hyp.4) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu_0'$, $\Gamma_0 = \Gamma_0'$, $f_0 = f_0'$, and $\Sigma_0 = \Sigma_0'$ (3) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu_1'$, $\Gamma_1 = \Gamma_1'$, $f_1 = f_1'$, and $\Sigma_1 = \Sigma_1'$ (4) - (hyp.4) + (1)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ and $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(5)** - (hyp.2) + (3) + (4)
- $o_0'.\mathsf{last} = \sigma_0$ and $o_1'.\mathsf{last} = \sigma_1$ (6) - (hyp.3) + (hyp.4) + (hyp.6) + (1)
- $o_0'.\mathsf{last} \sqcap o_1'.\mathsf{last} \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge o_0'.\mathsf{last} \sqcup o_1'.\mathsf{last} \sqsubseteq \sigma$ **(7)** - (2) + (6)

[Move Upward] $\bar{e}_0 = \mathsf{move}_\uparrow(r_0)$ for some node reference r_0 (hyp.6). Letting $\zeta_0 = \zeta_0'' :: \sigma_0$ and $\zeta_1 = \zeta_1'' :: \sigma_1$, we conclude that:

- $\bar{e}_1 = \mathsf{move}_\uparrow(r_1)$ for some node reference r_1 (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow r_0 = r_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu_0'$, $\Gamma_0 = \Gamma_0'$, $f_0 = f_0'$, $\Sigma_0 = \Sigma_0'$, and $\underline{v}_0 = f_0(r_0).\mathsf{parent}$ (3) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu_1'$, $\Gamma_1 = \Gamma_1'$, $f_1 = f_1'$, and $\Sigma_1 = \Sigma_1'$, and $\underline{v}_1 = f_1(r_1).\mathsf{parent}$ (4) - (hyp.4) + (1)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ and $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(5)** - (hyp.2) + (3) + (4)
- $o_0'.\mathsf{last} = \Sigma(r_0).\mathsf{pos} \sqcup \sigma_0$, $o_1'.\mathsf{last} = \Sigma(r_1).\mathsf{pos} \sqcup \sigma_1$ (6) - (hyp.3) + (hyp.4) + (hyp.6) + (1)

Suppose that $o'_0.\mathsf{last} \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\Sigma_0(r_0).\mathsf{pos} \sqcup \sigma_0 \sqsubseteq \sigma$ (7) - (hyp.7) + (6)
- $\sigma_1 = \sigma_0 \sqsubseteq \sigma$ and $r_0 = r_1$ (8) - (2) + (7)
- $f_0(r_0).\mathsf{parent} = f_1(r_1).\mathsf{parent}$ and $\Sigma_0(r_0) = \Sigma_1(r_1) \sqsubseteq \sigma$ (9) - (hyp.2) + (7) + (8)
- $\underline{v}_0 = \underline{v}_1$ and $o'_0.\mathsf{last} = o'_1.\mathsf{last} \sqsubseteq \sigma$ **(10)** - (3) + (4) + (6) + (9)

[Move Downward] $\bar{e}_0 = \mathsf{move}_{\downarrow}(r_0, i)$ for some node reference r_0 and integer i (hyp.6). Letting $\zeta_0 = \zeta''_0 :: \sigma_0 :: \sigma'_0$ and $\zeta_1 = \zeta''_1 :: \sigma_1 :: \sigma'_1$, we conclude that:

- $\bar{e}_1 = \mathsf{move}_{\downarrow}(r_1, j)$ for some node reference r_l and integer j (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow r_0 = r_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\sigma'_0 \sqcap \sigma'_1 \sqsubseteq \sigma \Rightarrow i = j \wedge \sigma'_0 \sqcup \sigma'_1 \sqsubseteq \sigma$ (3) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu'_0$, $\Gamma_0 = \Gamma'_0$, $f_0 = f'_0$, $\Sigma_0 = \Sigma'_0$, and $\underline{v}_0 = f_0(r_0).\mathsf{children}(i)$ (4) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu'_1$, $\Gamma_1 = \Gamma'_1$, $f_1 = f'_1$, and $\Sigma_1 = \Sigma'_1$, and $\underline{v}_1 = f_1(r_1).\mathsf{children}(j)$ (5) - (hyp.4) + (1)
- $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$ and $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ **(6)** - (hyp.2) + (4) + (5)
- $o'_0.\mathsf{last} = \Sigma(r_0).\mathsf{pos} \sqcup \sigma_0 \sqcup \sigma'_0$, $o'_1.\mathsf{last} = \Sigma(r_1).\mathsf{pos} \sqcup \sigma_1 \sqcup \sigma'_1$ (7) - (hyp.3) + (hyp.4) + (hyp.6) + (1)

Suppose that $o'_0.\mathsf{last} \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\Sigma(r_0).\mathsf{pos} \sqcup \sigma_0 \sqcup \sigma'_0 \sqsubseteq \sigma$ (8) - (hyp.7) + (7)
- $\sigma_1 = \sigma_0 \sqsubseteq \sigma$ and $\sigma'_0 = \sigma'_1 \sqsubseteq \sigma$, $r_0 = r_1$, and $i = j$ (9) - (2) + (8)
- $f_0(r_0).\mathsf{children}(i) = f_1(r_1).\mathsf{children}(j)$ and $\Sigma_0(r_0).\mathsf{pos} = \Sigma_1(r_1).\mathsf{pos} \sqsubseteq \sigma$ (10) - (hyp.2) + (8) + (9)
- $\underline{v}_0 = \underline{v}_1$ and $o'_0.\mathsf{last} = o'_1.\mathsf{last} \sqsubseteq \sigma$ **(11)** - (4) + (5) + (7) + (10)

[Length] $\bar{e}_0 = \mathsf{len}(r_0)$ for some node reference r_0 (hyp.6). Letting $\zeta_0 = \zeta''_0 :: \sigma_0$ and $\zeta_1 = \zeta''_1 :: \sigma_1$, we conclude that:

- $\bar{e}_1 = \mathsf{len}(r_1)$ for some node reference r_l (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow r_0 = r_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu'_0$, $\Gamma_0 = \Gamma'_0$, $f_0 = f'_0$, $\Sigma_0 = \Sigma'_0$, and $\underline{v}_0 = |f_0(r_0).\mathsf{children}|$ (3) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu'_1$, $\Gamma_1 = \Gamma'_1$, $f_1 = f'_1$, and $\Sigma_1 = \Sigma'_1$, and $\underline{v}_1 = |f_1(r_1).\mathsf{children}|$ (4) - (hyp.4) + (1)
- $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$ and $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ **(5)** - (hyp.2) + (3) + (4)
- $o'_0.\mathsf{last} = \Sigma(r_0).\mathsf{struct} \sqcup \sigma_0$, $o'_1.\mathsf{last} = \Sigma(r_1).\mathsf{struct} \sqcup \sigma_1$ (6) - (hyp.3) + (hyp.4) + (hyp.6) + (1)

Suppose that $o'_0.\mathsf{last} \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\Sigma(r_0).\mathsf{struct} \sqcup \sigma_0 \sqsubseteq \sigma$ (7) - (hyp.7) + (6)
- $\sigma_1 = \sigma_0 \sqsubseteq \sigma$, $r_0 = r_1$ (8) - (2) + (7)
- $|f_0(r_0).\mathsf{children}| = |f_1(r_1).\mathsf{children}|$ and $\Sigma_1(r_1).\mathsf{struct} = \Sigma_0(r_0).\mathsf{struct} \sqsubseteq \sigma$ (9) - (hyp.2) + (7) + (8)
- $\underline{v}_0 = \underline{v}_1$ and $o'_0.\mathsf{last} = o'_1.\mathsf{last} \sqsubseteq \sigma$ **(10)** - (3) + (4) + (6) + (9)

[Value] $\bar{e}_0 = \mathsf{value}(r_0)$ for some node reference r_0 (hyp.6). Letting $\zeta_0 = \zeta''_0 :: \sigma_0$ and $\zeta_1 = \zeta''_1 :: \sigma_1$, we conclude that:

- $\bar{e}_1 = \mathsf{value}(r_1)$ for some node reference r_l (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow r_0 = r_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu_0'$, $\Gamma_0 = \Gamma_0'$, $f_0 = f_0'$, $\Sigma_0 = \Sigma_0'$, and $\underline{v}_0 = f_0(r_0).\mathsf{value}$ (3) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu_1'$, $\Gamma_1 = \Gamma_1'$, $f_1 = f_1'$, and $\Sigma_1 = \Sigma_1'$, and $\underline{v}_1 = f_1(r_1).\mathsf{value}$ (4) - (hyp.4) + (1)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ and $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(5)** - (hyp.2) + (3) + (4)
- $o_0'.\mathsf{last} = \Sigma(r_0).\mathsf{value} \sqcup \sigma_0$, $o_1'.\mathsf{last} = \Sigma(r_1).\mathsf{value} \sqcup \sigma_1$ (6) - (hyp.3) + (hyp.4) + (hyp.6) + (1)

Suppose that $o_0'.\mathsf{last} \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\Sigma(r_0).\mathsf{value} \sqcup \sigma_0 \sqsubseteq \sigma$ (7) - (hyp.7) + (6)
- $\sigma_1 = \sigma_0 \sqsubseteq \sigma$, $r_0 = r_1$ (8) - (2) + (7)
- $f_0(r_0).\mathsf{value} = f_1(r_1).\mathsf{value}$ and $\Sigma_1(r_1).\mathsf{value} = \Sigma_0(r_0).\mathsf{value} \sqsubseteq \sigma$ (9) - (hyp.2) + (7) + (8)
- $\underline{v}_0 = \underline{v}_1$ and $o_0'.\mathsf{last} = o_1'.\mathsf{last} \sqsubseteq \sigma$ **(10)** - (3) + (4) + (6) + (9)

[New] $\bar{e}_0 = \mathsf{new}^{\sigma',\sigma'',\sigma'''}(m_0)$ for a parsed string m_0 and three security levels σ', σ'', and σ''' (hyp.6). Letting $\zeta_0 = \zeta_0'' :: \sigma_0$ and $\zeta_1 = \zeta_1'' :: \sigma_1$, we conclude that:

- $\bar{e}_1 = \mathsf{new}^{\sigma',\sigma'',\sigma'''}(m_1)$ for some parsed string m_1 (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow r_0 = r_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu_0'$, $\Gamma_0 = \Gamma_0'$, $f_0' = f_0\,[r_0 \mapsto \langle m_0, null, null, \epsilon\rangle]$, $r_0 = fresh(f_0, \sigma')$, $\underline{v}_0 = r_0$, and $\Sigma_0' = \Sigma_0\,[r_0 \mapsto \langle \sigma_0 \sqcup \sigma', \sigma_0 \sqcup \sigma', \sigma_0 \sqcup \sigma'', \sigma_0 \sqcup \sigma'''\rangle]$ (3) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu_1'$, $\Gamma_1 = \Gamma_1'$, $f_1' = f_1\,[r_1 \mapsto \langle m_1, null, null, \epsilon\rangle]$, $r_1 = fresh(f_1, \sigma')$, $\underline{v}_1 = r_1$, and $\Sigma_1' = \Sigma_1\,[r_1 \mapsto \langle \sigma_1 \sqcup \sigma', \sigma_1 \sqcup \sigma', \sigma_1 \sqcup \sigma'', \sigma_1 \sqcup \sigma'''\rangle]$ (4) - (hyp.4) + (1)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ **(5)** - (hyp.2) + (3) + (4)
- $o_0'.\mathsf{last} = \sigma_0 \sqcup \sigma'$, $o_1'.\mathsf{last} = \sigma_1 \sqcup \sigma'$ (6) - (hyp.3) + (hyp.4) + (hyp.6) + (1)

We have to prove that: $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$. Suppose that: $\sigma_0 \sqcup \sigma' \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\sigma_1 = \sigma_0 \sqsubseteq \sigma$ and $m_0 = m_1$ (7) - (hyp.7) + (2)
- $r_0 = r_1$ (8) - (hyp.2) + (hyp.7) + (3) + (4) + *Fresh Node Creation*
- $f_0'(r_0).\mathsf{tag} = f_1'(r_1).\mathsf{tag}$, $f_0'(r_0).\mathsf{value} = f_1'(r_1).\mathsf{value}$, $f_0'(r_0).\mathsf{children} = f_1'(r_1).\mathsf{children}$ (9) - (3) + (4)
- $\Sigma_0'(r_0).\mathsf{node} = \Sigma_1'(r_1).\mathsf{node}$, $\Sigma_0'(r_0).\mathsf{pos} = \Sigma_1'(r_1).\mathsf{pos}$, $\Sigma_0'(r_0).\mathsf{value} = \Sigma_1'(r_1).\mathsf{value}$, and $\Sigma_0'(r_0).\mathsf{struct} = \Sigma_1'(r_1).\mathsf{struct}$ (10) - (3) + (4) + (7)
- $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ (11) - (hyp.2) + (3) + (4) + (8)-(10)

Suppose that: $\sigma_0 \sqcup \sigma' \not\sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\sigma_1 \sqcup \sigma' \not\sqsubseteq \sigma$ (12) - (hyp.7) + (2)
- $f_0', \Sigma_0' \restriction^\sigma = f_0 \restriction^{\Sigma_0,\sigma}$ and $f_1' \restriction^{\Sigma_1',\sigma} = f_1 \restriction^{\Sigma_1,\sigma}$ (13) - (hyp.7) + (3) + (4) + (12)
- $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ (14) - (hyp.2) + (3) + (4)

Suppose that $o_0'.\mathsf{last} \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\sigma_0 \sqcup \sigma' \sqsubseteq \sigma$ (15) - (hyp.7) + (6)
- $\sigma_1 = \sigma_0 \sqsubseteq \sigma$, $r_0 = r_1$ (16) - (2) + (7)
- $\underline{v}_0 = \underline{v}_1$ and $o_0'.\mathsf{last} = o_1'.\mathsf{last} \sqsubseteq \sigma$ **(17)** - (hyp.7) + (15) + (16)

[Store] $\bar{e}_0 = \mathsf{store}(r_0, \underline{v}_0)$ for a reference r_0 and a parsed value $\underline{v}_0$ (hyp.6). Letting $\zeta_0 = \zeta_0'' :: \sigma_0 :: \sigma_0'$ and $\zeta_1 = \zeta_1'' :: \sigma_1 :: \sigma_1'$, we conclude that:

- $\bar{e}_1 = \mathsf{store}(r_1, \underline{v}_1)$ for a reference r_1 and a parsed value $\underline{v}_1$ (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow r_0 = r_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\sigma_0' \sqcap \sigma_1' \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge \sigma_0' = \sigma_1' \sqsubseteq \sigma$ (3) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu_0'$, $\Gamma_0 = \Gamma_0'$, $f_0' = f_0[r_0 \mapsto \langle f_0(r_0).\mathsf{tag}, \underline{v}_0, f_0(r_0).\mathsf{parent}, f_0(r_0).\mathsf{children}\rangle]$, $\Sigma_0' = \Sigma_0[r_0 \mapsto \langle \Sigma_0(r_0).\mathsf{node}, \sigma_0', \Sigma(r_0).\mathsf{pos}, \Sigma(r_0).\mathsf{struct}\rangle]$, and $\sigma_0 \sqsubseteq \Sigma_0(r_0).\mathsf{value}$ (4) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu_1'$, $\Gamma_1 = \Gamma_1'$, $f_1' = f_1[r_1 \mapsto \langle f_1(r_1).\mathsf{tag}, \underline{v}_1, f_1(r_1).\mathsf{parent}, f_1(r_1).\mathsf{children}\rangle]$, $\Sigma_1' = \Sigma_1[r_1 \mapsto \langle \Sigma_1(r_1).\mathsf{node}, \sigma_1', \Sigma(r_1).\mathsf{pos}, \Sigma(r_1).\mathsf{struct}\rangle]$, and $\sigma_1 \sqsubseteq \Sigma_1(r_1).\mathsf{value}$ (5) - (hyp.4) + (hyp.6)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ **(6)** - (hyp.2) + (4) + (5)
- $o_0'.\mathsf{last} = \sigma_0'$, $o_1'.\mathsf{last} = \sigma_1'$ (7) - (hyp.3) + (hyp.4) + (hyp.6) + (1)
- $o_0'.\mathsf{last} \sqcap o_1'.\mathsf{last} \sqsubseteq \sigma \Rightarrow \underline{v}_0 = \underline{v}_1 \wedge o_0'.\mathsf{last} \sqcup o_1'.\mathsf{last} \sqsubseteq \sigma$ **(8)** - (3) + (7)

We have to prove that: $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$. We consider three distinct cases: **(1)** $\sigma_0 \not\sqsubseteq \sigma$, **(2)** $\sigma_0 \sqsubseteq \sigma \ \wedge \ \sigma_0' \sqcup \Sigma_0(r_0).\mathsf{node} \not\sqsubseteq \sigma$, and **(3)** $\sigma_0 \sqcup \sigma_0' \sqcup \Sigma_0(r_0).\mathsf{node} \sqsubseteq \sigma$. Suppose that: $\sigma_0 \not\sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\sigma_1 \not\sqsubseteq \sigma$ (9) - (hyp.7) + (2)
- $f_0' \restriction^{\Sigma_0', \sigma} = f_0 \restriction^{\Sigma_0, \sigma}$ (10) - (hyp.3) + (hyp.7) + *Strong Confinement of Store Redex*
- $f_1' \restriction^{\Sigma_1', \sigma} = f_1 \restriction^{\Sigma_1, \sigma}$ (11) - (hyp.4) + (9) + *Strong Confinement of Store Redex*
- $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(12)** - (hyp.2) + (10) + (11)

Suppose $\sigma_0 \sqsubseteq \sigma \ \wedge \ \sigma_0' \sqcup \Sigma_0(r_0).\mathsf{node} \not\sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\sigma_1 = \sigma_0 \sqsubseteq \sigma$ and $r_0 = r_1$ (13) - (hyp.7) + (2)
- $\sigma_1' \sqcup \Sigma_1(r_1).\mathsf{node} \not\sqsubseteq \sigma$ (14) - (hyp.2) + (hyp.7) + (3) + (13)
- $f_0' \restriction^{\Sigma_0', \sigma} = f_0' \restriction^{\Sigma_0', \sigma} \setminus \{(r_0, f_0(r_0).\mathsf{value}, \Sigma_0(r_0).\mathsf{value})\}$ (15) - (hyp.7) + (4)
- $f_1' \restriction^{\Sigma_1', \sigma} = f_1' \restriction^{\Sigma_1', \sigma} \setminus \{(r_1, f_1(r_1).\mathsf{value}, \Sigma_1(r_1).\mathsf{value})\}$ (16) - (5) + (14)
- $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(17)** - (hyp.2) + (15) + (16)

Suppose $\sigma_0 \sqcup \sigma_0' \sqcup \Sigma_0(r_0).\mathsf{node} \sqsubseteq \sigma$ (hyp.7). We conclude that: We conclude that:

- $\sigma_1 = \sigma_0 \sqsubseteq \sigma$ and $r_0 = r_1$ (18) - (hyp.7) + (2)
- $\sigma_1' = \sigma_0' \sqsubseteq \sigma$ and $\underline{v}_0 = \underline{v}_1$ (19) - (hyp.7) + (3)
- $\Sigma_0(r_0).\mathsf{node} = \Sigma_1(r_1).\mathsf{node} \sqsubseteq \sigma$ (20) - (hyp.2) + (hyp.7) + (18)
- $f_0' \restriction^{\Sigma_0', \sigma} = f_0' \restriction^{\Sigma_0', \sigma} \setminus \{(r_0, f_0(r_0).\mathsf{value}, \Sigma_0(r_0).\mathsf{value})\} \cup \{(r_0, \underline{v}_0, \Sigma_0(r_0).\mathsf{node} \sqcup \sigma_0 \sqcup \sigma_0')\}$ (21) - (hyp.7) + (4)
- $f_1' \restriction^{\Sigma_1', \sigma} = f_1' \restriction^{\Sigma_1', \sigma} \setminus \{(r_1, f_1(r_1).\mathsf{value}, \Sigma_1(r_1).\mathsf{value})\} \cup \{(r_1, \underline{v}_1, \Sigma_1(r_1).\mathsf{node} \sqcup \sigma_1 \sqcup \sigma_1')\}$ (22) - (5) + (18)-(20)
- $(r_0, \underline{v}_0, \Sigma_0(r_0).\mathsf{node} \sqcup \sigma_0 \sqcup \sigma_0') = (r_1, \underline{v}_1, \Sigma_1(r_1).\mathsf{node} \sqcup \sigma_1 \sqcup \sigma_1')$ (23) - (18)-(19)
- $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(24)** - (hyp.2) + (21)-(23)

[Remove] $\bar{e}_0 = \mathsf{remove}(r_0, i)$ for a reference r_0 and a parsed integer i (hyp.6). Letting:

- $\zeta_0 = \zeta_0'' :: \sigma_0 :: \sigma_0'$,
- $\zeta_1 = \zeta_1'' :: \sigma_1 :: \sigma_1'$,

- $n_0 = f_0(r_0)$,
- $r'_0 = n_0.\mathsf{children}(i)$,
- $n''_0 = \langle n_0.\mathsf{tag}, n_0.\mathsf{value}, n_0.\mathsf{parent}, Shift_L(n_0.\mathsf{children}, i)\rangle$,
- $n'''_0 = \langle n'_0.\mathsf{tag}, n'_0.\mathsf{value}, null, n'_0.\mathsf{children}\rangle$,
- $n_1 = f_1(r_1)$,
- $r'_1 = n_1.\mathsf{children}(j)$,
- $n''_1 = \langle n_1.\mathsf{tag}, n_1.\mathsf{value}, n_1.\mathsf{parent}, Shift_L(n_1.\mathsf{children}, j)\rangle$,
- $n'''_1 = \langle n'_1.\mathsf{tag}, n'_1.\mathsf{value}, null, n'_1.\mathsf{children}\rangle$

We conclude that:

- $\bar{e}_1 = \mathsf{remove}(r_1, j)$ for a reference r_1 and a parsed integer j (1) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow r_0 = r_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\sigma'_0 \sqcap \sigma'_1 \sqsubseteq \sigma \Rightarrow i = j \wedge \sigma'_0 = \sigma'_1 \sqsubseteq \sigma$ (3) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu'_0$, $\Gamma_0 = \Gamma'_0$, $f'_0 = f_0\,[r_0 \mapsto n''_0, r'_0 \mapsto n'''_0]$, $\underline{v}_0 = r'_0$, $\Sigma'_0 = \Sigma_0$, and $\sigma_0 \sqcup \sigma'_0 \sqsubseteq \Sigma_0(r_0).\mathsf{struct} \sqcap \Sigma_0(r'_0).\mathsf{pos}$ (4) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu'_1$, $\Gamma_1 = \Gamma'_1$, $f'_1 = f_1\,[r_1 \mapsto n''_1, r'_1 \mapsto n'''_1]$, $\underline{v}_1 = r'_1$, $\Sigma'_1 = \Sigma_1$, and $\sigma_1 \sqcup \sigma'_1 \sqsubseteq \Sigma_1(r_1).\mathsf{struct} \sqcap \Sigma_1(r'_1).\mathsf{pos}$ (5) - (hyp.4) + (1)
- $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$ **(6)** - (hyp.2) + (4) + (5)
- $o'_0.\mathsf{last} = \Sigma_0(r'_0).\mathsf{pos}$, $o'_1.\mathsf{last} = \Sigma_1(r'_1).\mathsf{pos}$ (7) - (hyp.3) + (hyp.4) + (hyp.6) + (1)

  Suppose $\Sigma_0(r_0).\mathsf{struct} \sqcup \Sigma_0(r'_0).\mathsf{pos} \not\sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\Sigma_1(r_1).\mathsf{struct} \sqcup \Sigma_1(r'_1).\mathsf{pos} \not\sqsubseteq \sigma$ (8)

  Suppose that $\Sigma_1(r_1).\mathsf{struct} \sqcup \Sigma_1(r'_1).\mathsf{pos} \sqsubseteq \sigma$ (hyp.8). We conclude that:
  - $\sigma_1 \sqcup \sigma'_1 \sqsubseteq \sigma$ (8.1) - (hyp.8) + (5)
  - $r_0 = r_1$ and $i = j$ (8.2) - (2) + (3) + (8.1)
  - $\Sigma_1(r_1).\mathsf{struct} = \Sigma_0(r_0).\mathsf{struct}$, $r'_1 = r'_0$, and $\Sigma(r'_0).\mathsf{pos} = \Sigma(r'_1).\mathsf{pos}$ (8.3) - (hyp.2) + (hyp.8) + (8.2)
  - $\Sigma_0(r_0).\mathsf{struct} \sqcup \Sigma_0(r'_0).\mathsf{pos} \sqsubseteq \sigma$ (8.4) - (hyp.8) + (8.3)
  - *Contradiction* (8.5) - (hyp.7) + (8.4)
- $f_0, \Sigma_0 \sim_\sigma f'_0, \Sigma'_0$ (9) - (hyp.3) + (hyp.7) + *Strong Confinement of* remove
- $f_1, \Sigma_1 \sim_\sigma f'_1, \Sigma'_1$ (10) - (hyp.4) + (8) + *Strong Confinement of* remove
- $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ **(11)** - (hyp.2) + (9) + (10)
- $o'_0.\mathsf{last} \sqcap o'_1.\mathsf{last} \not\sqsubseteq \sigma$ **(12)** - (hyp.7) + (7) + (8)

  Suppose $\Sigma_0(r_0).\mathsf{struct} \sqcup \Sigma_0(r'_0).\mathsf{pos} \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\sigma_0 \sqcup \sigma'_0 \sqsubseteq \sigma$ (13) - (hyp.7) + (4)
- $r_0 = r_1$ and $i = j$ (14) - (2) + (3) + (13)
- $r'_0 = r'_1$, $\Sigma_0(r_0).\mathsf{struct} = \Sigma_1(r_1).\mathsf{struct} \sqsubseteq \sigma$, and $\Sigma_0(r'_0).\mathsf{pos} = \Sigma_1(r'_1).\mathsf{pos} \sqsubseteq \sigma$ (15) - (hyp.2) + (14)
- $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ **(16)** - (hyp.2) + (4) + (5) + (15)
- $o'_0.\mathsf{last} = o'_1.\mathsf{last} \sqsubseteq \sigma$ and $\underline{v}_0 = \underline{v}_1$ **(17)** - (4) + (5) + (7) + (15)

[INSERT] $\bar{e}_0 = \mathsf{insert}(r_0, r'_0, i)$ for two references r_0 and a parsed integer i (hyp.6). Using (hyp.1) and (hyp.6), we conclude that $\bar{e}_1 = \mathsf{insert}(r_1, r'_1, j)$, for two references r_1 and r'_1 and an integer j. Letting:

- $\zeta_0 = \zeta_0'' :: \sigma_0 :: \sigma_0' :: \sigma_0''$, $\zeta_1 = \zeta_1'' :: \sigma_1 :: \sigma_1' :: \sigma_1''$,
- $n_0 = f_0(r_0)$, $n_0' = f_0(r_0')$,
- $n_0'' = \langle n_0.\mathsf{tag}, n_0.\mathsf{value}, n_0.\mathsf{parent}, Shift_R(n_0.\mathsf{children}, i, r_0')\rangle$,
- $n_0''' = \langle n_0'.\mathsf{tag}, n_0'.\mathsf{value}, r_0, n_0'.\mathsf{children}\rangle$,
- $n_1 = f_1(r_1)$, $n_1' = f_1(r_1')$,
- $n_1'' = \langle n_1.\mathsf{tag}, n_1.\mathsf{value}, n_1.\mathsf{parent}, Shift_R(n_1.\mathsf{children}, j, r_1')\rangle$,
- $n_1''' = \langle n_1'.\mathsf{tag}, n_1'.\mathsf{value}, r_1, n_1'.\mathsf{children}\rangle$

We conclude that:

- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow r_0 = r_1 \wedge \sigma_0 = \sigma_1 \sqsubseteq \sigma$ (1) - (hyp.2) + (hyp.6) + (1)
- $\sigma_0' \sqcap \sigma_1' \sqsubseteq \sigma \Rightarrow r_0' = r_1' \wedge \sigma_0' = \sigma_1' \sqsubseteq \sigma$ (2) - (hyp.2) + (hyp.6) + (1)
- $\sigma_0'' \sqcap \sigma_1'' \sqsubseteq \sigma \Rightarrow i = j \wedge \sigma_0'' = \sigma_1'' \sqsubseteq \sigma$ (3) - (hyp.2) + (hyp.6) + (1)
- $\mu_0 = \mu_0'$, $\Gamma_0 = \Gamma_0'$, $f_0' = f_0\,[r_0 \mapsto n_0'', r_0' \mapsto n_0''']$, $\underline{v}_0 = r_0'$, $\Sigma_0' = \Sigma_0$, and $\sigma_0 \sqcup \sigma_0' \sqcup \sigma_0'' \sqsubseteq \Sigma_0(r_0).\mathsf{struct} \sqcap \Sigma_0(r_0').\mathsf{pos}$ (4) - (hyp.3) + (hyp.6)
- $\mu_1 = \mu_1'$, $\Gamma_1 = \Gamma_1'$, $f_1' = f_1\,[r_1 \mapsto n_1'', r_1' \mapsto n_1''']$, $\underline{v}_1 = r_1'$, $\Sigma_1' = \Sigma_1$, and $\sigma_1 \sqcup \sigma_1' \sqcup \sigma_1'' \sqsubseteq \Sigma_1(r_1).\mathsf{struct} \sqcap \Sigma_1(r_1').\mathsf{pos}$ (5) - (hyp.4) + (1)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ **(6)** - (hyp.2) + (4) + (5)
- $o_0'.\mathsf{last} = \Sigma_0(r_0').\mathsf{pos}$, $o_1'.\mathsf{last} = \Sigma_1(r_1').\mathsf{pos}$ (7) - (hyp.3) + (hyp.4) + (hyp.6) + (1)

  Suppose $\Sigma_0(r_0).\mathsf{struct} \sqcup \Sigma_0(r_0').\mathsf{pos} \not\sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\Sigma_1(r_1).\mathsf{struct} \sqcup \Sigma_1(r_1').\mathsf{pos} \not\sqsubseteq \sigma$ (8)

  Suppose that $\Sigma_1(r_1).\mathsf{struct} \sqcup \Sigma_1(r_1').\mathsf{pos} \sqsubseteq \sigma$ (hyp.8). We conclude that:
  - $\sigma_1 \sqcup \sigma_1' \sqcup \sigma_1'' \sqsubseteq \sigma$ (8.1) - (hyp.8) + (5)
  - $r_0 = r_1$, $r_0' = r_1'$, and $i = j$ (8.2) - (1)-(3) + (8.1)
  - $\Sigma_1(r_1).\mathsf{struct} = \Sigma_0(r_0).\mathsf{struct}$ and $\Sigma(r_0').\mathsf{pos} = \Sigma(r_1').\mathsf{pos}$ (8.3) - (hyp.2) + (hyp.8) + (8.2)
  - $\Sigma_0(r_0).\mathsf{struct} \sqcup \Sigma_0(r_0').\mathsf{pos} \sqsubseteq \sigma$ (8.4) - (hyp.8) + (8.3)
  - *Contradiction* (8.5) - (hyp.7) + (8.4)
- $f_0, \Sigma_0 \sim_\sigma f_0', \Sigma_0'$ (9) - (hyp.3) + (hyp.7) + *Strong Confinement of* insert
- $f_1, \Sigma_1 \sim_\sigma f_1', \Sigma_1'$ (10) - (hyp.4) + (8) + *Strong Confinement of* insert
- $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(11)** - (hyp.2) + (9) + (10)
- $o_0'.\mathsf{last} \sqcap o_1'.\mathsf{last} \not\sqsubseteq \sigma$ **(12)** - (hyp.7) + (7) + (8)

  Suppose $\Sigma_0(r_0).\mathsf{struct} \sqcup \Sigma_0(r_0').\mathsf{pos} \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\sigma_0 \sqcup \sigma_0' \sqcup \sigma_0'' \sqsubseteq \sigma$ (13) - (hyp.7) + (4)
- $r_0 = r_1$, $r_0' = r_1'$, and $i = j$ (14) - (1)-(3) + (13)
- $\Sigma_0(r_0).\mathsf{struct} = \Sigma_1(r_1).\mathsf{struct} \sqsubseteq \sigma$ and $\Sigma_0(r_0').\mathsf{pos} = \Sigma_1(r_1').\mathsf{pos} \sqsubseteq \sigma$ (15) - (hyp.2) + (14)
- $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(16)** - (hyp.2) + (4) + (5) + (15)
- $o_0'.\mathsf{last} = o_1'.\mathsf{last} \sqsubseteq \sigma$ and $\underline{v}_0 = \underline{v}_1$ **(17)** - (4) + (5) + (7) + (15)

□

Lemma 9 (Low-Expression Generating One-Step Transition). *Given two confs* $\langle\langle \mu_0, f_0, E_0[\bar{e}_0]\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle$ *and* $\langle\langle \mu_1, f_1, E_1[\bar{e}_1]\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle$ *such that:*

- $\bar{e}_0 \equiv \bar{e}_1$ *(hyp.1)*
- $\langle\langle \mu_0, f_0, E_0[\bar{e}_0]\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle \sim_\sigma \langle\langle \mu_1, f_1, E_1[\bar{e}_1]\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle$ *(hyp.2)*
- $\langle\langle \mu_0, f_0, E_0[\bar{e}_0]\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle \to \langle\langle \mu'_0, f'_0, E_0[e_0]\rangle, \langle \Gamma'_0, \Sigma'_0, o'_0, \zeta'_0\rangle\rangle$ *(hyp.3)*
- $\langle\langle \mu_1, f_1, E_1[\bar{e}_1]\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle \to \langle\langle \mu'_1, f'_1, E_1[e_1]\rangle, \langle \Gamma'_1, \Sigma'_1, o'_1, \zeta'_1\rangle\rangle$ *(hyp.4)*
- $level(o_0) \sqcup level(o_1) \sqsubseteq \sigma$ *(hyp.5)*

where e_0 and e_1 are not runtime value, it holds that: $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$, $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$, $level(o'_0) \sqcup level(o'_1) \sqsubseteq \sigma \Rightarrow e_0 = e_1$.

Proof. We proceed by case analysis on the trasitions whose evaluation yield expressions that are not parsed values. These transitions are: [Loop - True], [Conditional], [Loop], and [Sequence].

[Sequence] $\bar{e}_0 = \underline{v}_0; e_0$ (hyp.6). Letting $\zeta_0 = \zeta''_0 :: \sigma_0$ and $\zeta_1 = \zeta''_1 :: \sigma_1$. We conclude that:

- $f_0 = f'_0$, $\mu_0 = \mu'_0$, $\zeta'_0 = \zeta''_0$, and $o'_0 = o_0$ (1) - (hyp.3) + (hyp.6)
- $\bar{e}_1 = \underline{v}_1; e_1$, for some runtime value $\underline{v}_1$, and $e_0 = e_1$ **(2)** - (hyp.1) + (hyp.6)
- $f_1 = f'_1$, $\mu_1 = \mu'_1$, $\zeta'_1 = \zeta''_1$, and $o'_1 = o_1$ (3) - (hyp.4) + (2)
- $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$ and $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ **(4)** - (hyp.2) + (1) + (3)

[Loop] $\bar{e}_0 = \mathsf{while}(e'_0)\{e''_0\}$ (hyp.6). We conclude that:

- $e_0 = \mathsf{while}^{e'_0}(e'_0)\{e''_0\}$, $f_0 = f'_0$, $\mu_0 = \mu'_0$, $\zeta'_0 = \zeta''_0$, and $o'_0 = o_0$ (1) - (hyp.3) + (hyp.6)
- $\bar{e}_1 = \mathsf{while}^{e'_0}(e'_0)\{e''_0\}$, **(2)** - (hyp.1) + (hyp.6)
- $e_1 = \mathsf{while}^{e'_0}(e'_0)\{e''_0\}$, $f_1 = f'_1$, $\mu_1 = \mu'_1$, $\zeta'_1 = \zeta''_1$, and $o'_1 = o_1$ (3) - (hyp.4) + (2)
- $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$ and $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ **(4)** - (hyp.2) + (1) + (3)

[Loop - True] $\bar{e}_0 = \mathsf{while}^{e'_0}(\underline{v}_0)\{e''_0\}$ (hyp.6). Letting $\zeta_0 = \zeta''_0 :: \sigma_0$ and $\zeta_1 = \zeta''_1 :: \sigma_1$. We conclude that:

- $e_0 = \mathsf{end}(e''_0); \mathsf{while}(e'_0)\{e''_0\}$, $\underline{v}_0 \notin V_F$, $f_0 = f'_0$, $\mu_0 = \mu'_0$, $\zeta'_0 = \zeta''_0$, and $o'_0 = o_0 :: \sigma_0$ (1) - (hyp.3) + (hyp.6)
- $\bar{e}_1 = \mathsf{while}^{e'_1}(\underline{v}_1)\{e''_1\}$, $e'_1 = e'_0$, and $e''_1 = e''_0$ (2) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow \sigma_0 \sqcup \sigma_1 \sqsubseteq \sigma \ \wedge \ \underline{v}_0 = \underline{v}_1$ (3) - (hyp.2)

Suppose that $level(o'_0) \sqcup level(o'_1) \sqsubseteq \sigma$ (hyp.7). We conclude that:

- $\sigma_0 \sqsubseteq \sigma$ (4) - (hyp.7)
- $\sigma_1 \sqsubseteq \sigma$ and $\underline{v}_0 = \underline{v}_1$ (5) - (3) + (4)
- $e_1 = \mathsf{end}(e''_1); \mathsf{while}(e'_1)\{e''_1\}$, $\underline{v}_1 \notin V_F$, $f_1 = f'_1$, $\mu_1 = \mu'_1$, $\zeta'_1 = \zeta''_1$, and $o'_1 = o_1 :: \sigma_1$ (6) - (hyp.4) + (1) + (5)
- $e_0 = e_1$ **(7)** - (2) + (6)
- $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$ and $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$ **(8)** - (hyp.2) + (1) + (6)

[Conditional] $\bar{e}_0 = \mathsf{if}(\underline{v}_0)\{e'_0\}\ \mathsf{else}\ \{e''_0\}$ (hyp.6). Letting $\zeta_0 = \zeta''_0 :: \sigma_0$ and $\zeta_1 = \zeta''_1 :: \sigma_1$. We assume, without loss of generality that $\underline{v}_0 \in V_F$ (hyp.7). We conclude that:

- $e_0 = \mathsf{end}(e_0'')$, $f_0 = f_0'$, $\mu_0 = \mu_0'$, $\zeta_0' = \zeta_0''$, and $o_0' = o_0 :: \sigma_0$ (1) - (hyp.3) + (hyp.6) + (hyp.7)
- $\bar{e}_1 = \mathsf{if}(\underline{v}_1)\{e_1'\}\ \mathsf{else}\ \{e_1''\}$, $e_1' = e_0'$, and $e_1'' = e_0''$ (2) - (hyp.1) + (hyp.6)
- $\sigma_0 \sqcap \sigma_1 \sqsubseteq \sigma \Rightarrow \sigma_0 \sqcup \sigma_1 \sqsubseteq \sigma \ \wedge\ \underline{v}_0 = \underline{v}_1$ (3) - (hyp.2)

Suppose that $level(o_0') \sqcup level(o_1') \sqsubseteq \sigma$ (hyp.8). We conclude that:

- $\sigma_0 \sqsubseteq \sigma$ (4) - (hyp.7)
- $\sigma_1 \sqsubseteq \sigma$ and $\underline{v}_0 = \underline{v}_1$ (5) - (3) + (4)
- $e_1 = \mathsf{end}(e_1'')$, $f_1 = f_1'$, $\mu_1 = \mu_1'$, $\zeta_1' = \zeta_1''$, and $o_1' = o_1 :: \sigma_1$ (6) - (hyp.4) + (1) + (5)
- $e_0 = e_1$ **(7)** - (2) + (6)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ and $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$ **(8)** - (hyp.2) + (1) + (6)

□

Lemma 10 (Low One-Step Transition). *Given two monitored configurations $\langle\langle \mu_0, f_0, e_0\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle$ and $\langle\langle \mu_1, f_1, e_1\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle$ such that:*

- $\langle\langle \mu_0, f_0, e_0\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle \sim_\sigma \langle\langle \mu_1, f_1, e_1\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle$ *(hyp.1)*
- $\langle\langle \mu_0, f_0, e_0\rangle, \langle \Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle \rightarrow \langle\langle \mu_0', f_0', e_0'\rangle, \langle \Gamma_0', \Sigma_0', o_0', \zeta_0'\rangle\rangle$ *(hyp.2)*
- $\langle\langle \mu_1, f_1, e_1\rangle, \langle \Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle \rightarrow \langle\langle \mu_1', f_1', e_1'\rangle, \langle \Gamma_1', \Sigma_1', o_1', \zeta_1'\rangle\rangle$ *(hyp.3)*

and $level(o_0) \sqcap level(o_1) \sqsubseteq \sigma$ (hyp.4). It holds that: $\langle\langle \mu_0', f_0', e_0'\rangle, \langle \Gamma_0', \Sigma_0', o_0', \zeta_0'\rangle\rangle \sim_\sigma \langle\langle \mu_1', f_1', e_1'\rangle, \langle \Gamma_1', \Sigma_1', o_1', \zeta_1'\rangle\rangle$

Proof. In the following, we assume, without loss of generality, that $level(o_0) \sqsubseteq \sigma$ (hyp.5). Letting $e_0 = E_0[\bar{e}_0]$ and $e_1 = E_1[\bar{e}_1]$, we conclude that:

- $level(o_1) \sqsubseteq \sigma$ (1) - (hyp.1) + (hyp.5)
- $E_0, \lceil \zeta_0 \rceil_{|E_0|} \approx_\sigma E_1, \lceil \zeta_1 \rceil_{|E_1|}$ and $\bar{e}_0, \lfloor \zeta_0 \rfloor_{|\bar{e}_0|} \approx_\sigma \bar{e}_1, \lfloor \zeta_1 \rfloor_{|E_1|}$ (2) - (hyp.1) + (hyp.4)
- $\bar{e}_0 \equiv \bar{e}_1$, $\mathsf{pvalues}(\bar{e}_0), \lfloor \zeta_0 \rfloor_{|\bar{e}_0|} \sim_\sigma \mathsf{pvalues}(\bar{e}_1), \lfloor \zeta_1 \rfloor_{|\bar{e}_1|}$ (3) - (2)
- $\mu_0, \Gamma_0 \sim_\sigma \mu_1, \Gamma_1$ and $f_0, \Sigma_0 \sim_\sigma f_1, \Sigma_1$ (4) - (hyp.1)
- There are two expressions e_0'' and e_1'' s.t. $e_0' = E_0[e_0'']$ and $e_1' = E_1[e_1'']$ (5) - (hyp.2) + (hyp.3) + *Preservation of Contexts*

We consider two distinct cases. Either the evaluation of $\bar{e}_0$ yields another redex or it yields a runtime value.

[Evaluation yields a runtime value] Suppose that e_0'' is a runtime value (hyp.6). Let $e_0'' = \underline{v}_0$, $\sigma_0 = \zeta_0'.\mathsf{last}$ and $\sigma_1 = \zeta_1'.\mathsf{last}$, we conclude that:

- e_1'' is a runtime value that we will denote by $\underline{v}_1$ (6) - (hyp.1) + (hyp.6)
- $\zeta_0' = \lceil \zeta_0 \rceil_{|E_0|} :: \sigma_0$ and $\zeta_1' = \lceil \zeta_1 \rceil_{|E_1|} :: \sigma_1$ (7) - (hyp.2) + (hyp.3)
- $\mu_0', \Gamma_0' \sim_\sigma \mu_1', \Gamma_1'$ and $f_0', \Sigma_0' \sim_\sigma f_1', \Sigma_1'$, $o_0' \restriction^\sigma = o_1' \restriction^\sigma$, and $\sigma_0 \sqcap \sigma_1 \Rightarrow \sigma_0 \sqcup \sigma_1 \sqsubseteq \sigma \ \wedge\ \underline{v}_0 = \underline{v}_1$ (8) - (hyp.2) + (hyp.3) + (3) + (4) + Lemma 8
- $\langle\langle \mu_0', f_0', e_0'\rangle, \langle \Gamma_0', \Sigma_0', o_0', \zeta_0'\rangle\rangle \sim_\sigma \langle\langle \mu_1', f_1', e_1'\rangle, \langle \Gamma_1', \Sigma_1', o_1', \zeta_1'\rangle\rangle$ **(9)**

  Suppose that $E_0 = []$ (hyp.7), we conclude that:
  - $E_1 = []$ (9.1) - (hyp.7) + (2)
  - $\langle\langle \mu_0', f_0', e_0'\rangle, \langle \Gamma_0', \Sigma_0', o_0', \zeta_0'\rangle\rangle \sim_\sigma \langle\langle \mu_1', f_1', e_1'\rangle, \langle \Gamma_1', \Sigma_1', o_1', \zeta_1'\rangle\rangle$ **(9.2)** - (hyp.7) + (8) + (9.1)

  Suppose that $E_0 \neq []$ (hyp.7), we conclude that:

- $E_1 \neq []$ (9.1) - (hyp.7) + (2)
- There is a context E'_0 and a redex $\bar{e}'_0$ such that: $E_0[\underline{v}_0] = E'_0[\bar{e}'_0] = e'_0$ (9.2) - (hyp.7)
- There is a context E'_1 and a redex $\bar{e}'_1$ such that: $E_1[\underline{v}_1] = E'_1[\bar{e}'_1] = e'_1$ (9.3) - (9.1)
- $E'_0, \lceil\zeta'_0\rceil_{|E'_0|} \approx_\sigma E'_1, \lceil\zeta'_1\rceil_{|E'_1|}$ and $\bar{e}'_0, \lfloor\zeta'_0\rfloor_{|\bar{e}'_0|} \approx_\sigma \bar{e}'_1, \lfloor\zeta'_1\rfloor_{|E'_1|}$ (9.4) - (2) + (8) + (9.2) + (9.3) + *Low-Equal Context Composition*
- $\langle\langle\mu'_0, f'_0, e'_0\rangle, \langle\Gamma'_0, \Sigma'_0, o'_0, \zeta'_0\rangle\rangle \sim_\sigma \langle\langle\mu'_1, f'_1, e'_1\rangle, \langle\Gamma'_1, \Sigma'_1, o'_1, \zeta'_1\rangle\rangle$ **(9.5)** - (8) + (9.4)

[Evaluation does NOT yield a runtime value] Suppose that e''_0 is not a runtime value (hyp.6). In this case, we conclude that:

- e''_1 is not a runtime value (10) - (hyp.1) + (hyp.6)
- $\mathsf{pvalues}(e''_1) = \mathsf{pvalues}(e''_0) = \epsilon$ (11) - (hyp.2) + (hyp.3) + (hyp.6) + (10)
- There is a context E'_0 and a redex $\bar{e}'_0$ such that: $E_0[e''_0] = E'_0[\bar{e}'_0] = e'_0$ (12) - (hyp.6)
- There is a context E'_1 and a redex $\bar{e}'_1$ such that: $E_1[e''_1] = E'_1[\bar{e}'_1] = e'_1$ (13) - (10)
- $\mu'_0, \Gamma'_0 \sim_\sigma \mu'_1, \Gamma'_1$ and $f'_0, \Sigma'_0 \sim_\sigma f'_1, \Sigma'_1$, $o'_0 \restriction^\sigma = o'_1 \restriction^\sigma$, and $level(o'_0) \sqcap level(o'_1) \sqsubseteq \sigma \Rightarrow e''_0 = e''_1$. (14) - (hyp.2) + (hyp.3) + (3) + (4) + Lemma 9

Suppose that $level(o'_0) \sqcap level(o'_1) \sqsubseteq \sigma$ (hyp.7). We then conclude that:

- $e''_0 = e''_1$ (15) - (hyp.7) + (14)
- $E'_0, \lceil\zeta'_0\rceil_{|E'_0|} \approx_\sigma E'_1, \lceil\zeta'_1\rceil_{|E'_1|}$ and $\bar{e}'_0, \lfloor\zeta'_0\rfloor_{|\bar{e}'_0|} \approx_\sigma \bar{e}'_1, \lfloor\zeta'_1\rfloor_{|E'_1|}$ (16) - (2) + (12) + (13) + (15) + *Low-Equal Context Composition*
- $\langle\langle\mu'_0, f'_0, e'_0\rangle, \langle\Gamma'_0, \Sigma'_0, o'_0, \zeta'_0\rangle\rangle \sim_\sigma \langle\langle\mu'_1, f'_1, e'_1\rangle, \langle\Gamma'_1, \Sigma'_1, o'_1, \zeta'_1\rangle\rangle$ **(17)** - (14) + (16)

Suppose that $level(o'_0) \sqcap level(o'_1) \not\sqsubseteq \sigma$ (hyp.7). We then conclude that:

- $E'_0 \restriction^\sigma = E_0$ and $E'_1 \restriction^\sigma = E_1$ (18) - (hyp.7) + (14)
- $\langle\langle\mu'_0, f'_0, e'_0\rangle, \langle\Gamma'_0, \Sigma'_0, o'_0, \zeta'_0\rangle\rangle \sim_\sigma \langle\langle\mu'_1, f'_1, e'_1\rangle, \langle\Gamma'_1, \Sigma'_1, o'_1, \zeta'_1\rangle\rangle$ **(19)** - (14) + (18)

□

Lemma 11 (Lockstep Noninterference). *Given four configurations $cfgm_0$, $cfgm'_0$, $cfgm_1$, and $cfgm'_1$ and a security level σ such that: $cfgm_0 \sim_\sigma cfgm_1$ (hyp.1), $cfgm_0 \rightarrow^{\mathbf{1},\sigma} cfgm'_0$ (hyp.2), $cfgm_1 \rightarrow^{\mathbf{1},\sigma} cfgm'_1$ (hyp.3), it holds that $cfgm'_0 \sim_\sigma cfgm'_1$.*

Proof. In the following, let $cfgm_0$ be $\langle\langle\mu_0, f_0, E_0[\bar{e}_0]\rangle, \langle\Gamma_0, \Sigma_0, o_0, \zeta_0\rangle\rangle$ and $cfgm_1$ be $\langle\langle\mu_1, f_1, E_1[\bar{e}_1]\rangle, \langle\Gamma_1, \Sigma_1, o_1, \zeta_1\rangle\rangle$. We consider two distinct cases. Either the initial configurations correspond to a *high* context – $level(o_0) \sqsubseteq \sigma$ – or to a *low* context – $level(o_1) \sqsubseteq \sigma$.

[High Context.] Suppose $level(o_0) \not\sqsubseteq \sigma$ (hyp.4). Letting $E'_0 = \hat{E}_0 \restriction^{o_0,\sigma}$ and $\hat{E}_1 = E_1 \restriction^{o_1,\sigma}$, we conclude that:

- $level(o_1) \not\sqsubseteq \sigma$ (1) - (hyp.1) + (hyp.4)
- $\hat{E}_0, \lceil\zeta_0\rceil_{|\hat{E}_0|} \approx_\sigma \hat{E}_1, \lceil\zeta_1\rceil_{|\hat{E}_1|}$ and $o_0 \restriction^\sigma = o_1 \restriction^\sigma$ (2) - (hyp.1)

- $E_0 = \hat{E}_0[\hat{E}'_0]$ for a given context $\hat{E}'_0 \neq []$ (3) - (hyp.4)
- $E_1 = \hat{E}_0[\hat{E}'_1]$ for a given context $\hat{E}'_1 \neq []$ (4) - (1)
- There is a configuration $cfgm''_0 = \langle\langle \mu''_0, f''_0, \hat{E}_0[\underline{v}''_0]\rangle, \langle \Gamma''_0, \Sigma''_0, o''_0, \zeta''_0\rangle\rangle$ such that $cfgm_0 \rightarrow^* cfgm''_0$ and all the transitions in this derivation are executed in *high* contexts and $cfgm''_0 \rightarrow cfgm'_0$ (in a *low* context) (5) - (hyp.2)
- There is a configuration $cfgm''_1 = \langle\langle \mu''_1, f''_1, \hat{E}_1[\underline{v}''_1]\rangle, \langle \Gamma''_1, \Sigma''_1, o''_1, \zeta''_1\rangle\rangle$ such that $cfgm_1 \rightarrow^* cfgm''_1$ and all the transitions in this derivation are executed in *high* contexts and $cfgm''_1 \rightarrow cfgm'_1$ (in a *low* context) (6) - (hyp.3)
- $\mu_0 \restriction^{\sigma,\Gamma_0} = \mu''_0 \restriction^{\sigma,\Gamma''_0}$, $f_0 \restriction^{\Sigma_0,\sigma} = f''_0 \restriction^{\Sigma''_0,\sigma}$, $\zeta''_0 = \lceil \zeta_0 \rceil_{|\hat{E}_0|} :: \zeta''_0.\mathsf{last}$, $\zeta''_0.\mathsf{last} \not\sqsubseteq \sigma$, and $o''_0 = o_0 \restriction^{\sigma}$ (7) - (5) + Confined Transitions (Lemma 7)
- $\mu_1 \restriction^{\sigma,\Gamma_1} = \mu''_1 \restriction^{\sigma,\Gamma''_1}$, $f_1 \restriction^{\Sigma_1,\sigma} = f''_1 \restriction^{\Sigma''_1,\sigma}$, $\zeta''_1 = \lceil \zeta_1 \rceil_{|\hat{E}_1|} :: \zeta''_0.\mathsf{last}$ and $\zeta''_1.\mathsf{last} \not\sqsubseteq \sigma$, and $o''_1 = o_1 \restriction^{\sigma}$ (8) - (6) + Confined Transitions (Lemma 7)
- $\mu''_0 \restriction^{\sigma,\Gamma''_0} = \mu''_1 \restriction^{\sigma,\Gamma''_1}$, $f''_0 \restriction^{\Sigma''_0,\sigma} = f''_1 \restriction^{\Sigma''_1,\sigma}$, and $o''_0 \restriction^{\sigma} = o''_0 = o''_1 = o''_1 \restriction^{\sigma}$ (9) - (7) + (8)
- $\hat{E}_0 = \hat{E}_1 \neq []$ (10) - (hyp.2) + (hyp.3)
  Remark: If $\hat{E}_0 = \hat{E}_1 = []$, then no low-transition was possible from configurations $cfgm_0$ and $cfgm_1$ which contradict Hypotheses (hyp.2) and (hyp.3).
- There are two redexes $\bar{e}''_0$ and $\bar{e}''_1$ and two contexts E''_0 and E''_1 such that: $\hat{E}_0[\underline{v}''_0] = E''_0[\bar{e}''_0]$ and $\hat{E}_1[\underline{v}'_1] = E''_1[\bar{e}''_1]$ (11) - (10)
- $\zeta''_0.\mathsf{last} \sqcap \zeta''_1.\mathsf{last} \sqsubseteq \sigma \Rightarrow \underline{v}'_0 = \underline{v}'_1 \ \wedge \ \zeta''_0.\mathsf{last} \sqcup \zeta''_1.\mathsf{last} \sqsubseteq \sigma$ (12) - (7) + (8)
- $E''_0, \lceil \zeta''_0 \rceil_{|E''_0|} \approx_\sigma E''_1, \lceil \zeta''_1 \rceil_{|E''_1|}$ and $\bar{e}''_0, \lfloor \zeta''_0 \rfloor_{|\bar{e}''_0|} \sim_\sigma \bar{e}''_1, \lfloor \zeta''_1 \rfloor_{|\bar{e}''_1|}$
  (13) - (2) + (7) + (8) + (11) + (12) + *Low-Equality Preserving Context Composition*
- $cfgm''_0 \sim_\sigma cfgm''_1$ (14) - (9) + (13)
- $cfgm'_0 \sim_\sigma cfgm'_1$ **(15)** - (5) + (6) + (14) + + Lemma 10

[Low Context.] Suppose $level(o_0) \sqsubseteq \sigma$ (hyp.4). We conclude that:

- $level(o_1) \not\sqsubseteq \sigma$ (1) - (hyp.1) + (hyp.4)
- $cfgm_0 \rightarrow cfgm'_0$ and $cfgm_1 \rightarrow cfgm'_1$ (2) - (hyp.2)-(hyp.4) + (1)
- $cfgm'_0 \sim_\sigma cfgm'_1$ **(3)** - (hyp.1) + (hyp.4) + (1) + (2) + Lemma 10

□

Theorem 1 (Noninterference). *Given four configurations $cfgm_0$, $cfgm'_0$, $cfgm_1$, and $cfgm'_1$ and a security level σ such that: $cfgm_0 \sim_\sigma cfgm_1$ (hyp.1), $cfgm_0 \rightarrow^* cfgm'_0$ (hyp.2), and $cfgm_1 \rightarrow^* cfgm'_1$ (hyp.3), it holds that: $cfgm'_0 \sim_\sigma cfgm'_1$.*

Proof. We conclude that there are two integers n_0 and n_1 (which we assume, without loss of generality that are such that $n_0 \leq n_1$) and two configurations $cfgm''_0$ and $cfgm''_1$ such that:

- $cfgm_0 \rightarrow^{\mathbf{n_0},\sigma} cfgm''_0$, $cfgm_1 \rightarrow^{\mathbf{n_1},\sigma} cfgm''_1$, $cfgm''_0 \rightarrow^*_\sigma cfgm'_0$, and $cfgm''_1 \rightarrow^*_\sigma cfgm'_1$ (1) - (hyp.2) + (hyp.3)
- $n_0 = n_1$ (2)
  Suppose, without loss of generality that $n_0 < n_1$ (hyp.4), we conclude that there is a monitored configuration $cfgm'''_1$ and an integer n'_1 (with $n'_1 > 0$) such that:
  - $cfgm_1 \rightarrow^{\mathbf{n_0},\sigma} cfgm'''_1$, $cfgm'''_1 \rightarrow^{\mathbf{n'_1},\sigma} cfgm''_1$, and $cfgm''_0 \sim_\sigma cfgm'''_1$ (2.1) - (hyp.2)-(hyp.4)
  - $cfgm''_0 \sim_\sigma cfgm'''_1$ (2.2) - (hyp.1) + (1) + (2.1) + Lemma 11

- $E_0'' \restriction^\sigma = []$, where E_0'' is the evaluation context of $cfgm_0''$ (2.3) - (1)
- $E_1''' \restriction^\sigma \neq []$, where E_1''' is the evaluation context of $cfgm_1'''$ (2.4) - (2.1)
- $cfgm_0'' \sim_\sigma cfgm_1'''$ (2.5) - (2.3) + (2.4)
- *Contradiction* (2.2) + (2.3)

– $cfgm_0'' \sim_\sigma cfgm_1''$ (3) - (hyp.1) + (1) + (2) + Lemma 11
– $cfgm_0'' \sim_\sigma cfgm_0'$ (4) - (1) + Lemma 7
– $cfgm_1'' \sim_\sigma cfgm_1'$ (5) - (1) + Lemma 7
– $cfgm_0' \sim_\sigma cfgm_1'$ (6) - (3)-(5)

□

B Proofs of Section 4

Definitions 10 and 11 strengthen the low-equality for sequences introduced in the previous section. Definition 10 requires that the two sequences coincide in their low prefix, while Definition 11 require that they entirely coincide.

Definition 10 (Asymmetric Low-Equality for Sequences). *Two lists of values ω and ω' respectively labeled by two lists of security levels ζ and ζ' are said to be asymmetrically low-equal w.r.t. a security level σ, written $\omega, \zeta \simeq_\sigma \omega', \zeta'$ if the following hold there is an integer i such that:* **(1)** $\forall_{0 \leq j < i}\ \zeta(i) = \zeta'(i) \sqsubseteq \sigma \wedge \omega(i) = \omega'(i)$, **(2)** $\forall_{i \leq j < |\zeta|}\ \zeta(i) \not\sqsubseteq \sigma$, *and* **(3)** $\forall_{i \leq j < |\zeta'|}\ \zeta'(i) \not\sqsubseteq \sigma$. *Furthermore, for all security levels σ, it holds that $\epsilon, \epsilon \simeq_\sigma \epsilon, \epsilon$.*

Definition 11 (Strong Low-Equality for Sequences). *Two lists of values ω and ω' respectively labeled by two lists of security levels ζ and ζ' are said to be strongly low-equal w.r.t. a security level σ, written $\omega, \zeta \approx_\sigma \omega', \zeta'$ if:* **(1)** $|\omega| = |\omega'|$ *and* **(2)** $\forall_{0 \leq i < |\zeta|}\ \zeta(i) = \zeta'(i) \sqsubseteq \sigma \ \wedge\ \omega(i) = \omega'(i)$.

The formalization of the *search predicate* is given in Figure 7, while Figure 8 modifies the *well-labeling* predicate for it to compute additional information used in the proofs. Concretely, it computes a function φ_t, that we call *live record* that maps every pair (m, σ), consisting of a tag name and a security level to the last node in the tree in document order with tag m whose position level is $\sqsubseteq \sigma$.

In the following, given a function g and a list of nodes ω, we use $g(\omega)$ to denote the list ω' obtained by applying g to every element of ω. Formally, ω' is such that: $|\omega| = |\omega'|$ and for all $0 \leq i < |\omega|$: $\omega'(i) = g(\omega)$. We use $\Sigma.\mathsf{pos}$ to denote the function that maps each node reference to the corresponding position level. Formally, $\Sigma.\mathsf{pos}(r) = \Sigma(r).\mathsf{pos}$. Moreover, given a list of security level ζ and a security level σ, we use $\sigma \sqsubseteq \zeta$ as an abbreviation for $\sigma \sqsubseteq \sqcap\{\zeta(i) \mid 0 \leq i < |\zeta|\}$ and $\zeta \sqsubseteq \sigma$ as an abbreviation for $\sqcup\{\zeta(i) \mid 0 \leq i < |\zeta|\} \sqsubseteq \sigma$.

Lemma 12 (Monotonocity of the search relation). *Given a forest f labeled by Σ, a node reference r, a function ϕ_t, and a tag name m such that $\mathcal{WL}_{f,\Sigma} \vdash^r \phi_t \rightsquigarrow \phi'_t$ (hyp.1) and $f \vdash r \rightsquigarrow_m \omega$, for a given function ϕ'_t and list of references ω (hyp.2), it holds that $\Sigma.\mathsf{pos}(\omega)$ is monotonically increasing and $\phi_t(m) \sqsubseteq \Sigma.\mathsf{pos}(\omega) \sqsubseteq \phi'_t(m) \sqsubseteq \sigma_m$.*

$$\frac{|f(r).\mathsf{children}| = 0 \qquad f(r).\mathsf{tag} \neq m}{f \vdash r \rightsquigarrow_m \epsilon}$$ Node Not Found - Orphan Node

$$\frac{\omega = f(r).\mathsf{children} \qquad |\omega| = n \qquad f(r).\mathsf{tag} \neq m}{f \vdash r \rightsquigarrow_m \oplus\{\omega_i \mid 0 \leq i < n \ \wedge \ f \vdash \omega(i) \rightsquigarrow_m \omega_i\}}$$ Node Not Found - Non-Orphan Node

$$\frac{|f(r).\mathsf{children}| = 0 \qquad f(r).\mathsf{tag} = m}{f \vdash r \rightsquigarrow_m r :: \epsilon}$$ Node Found - Orphan Node

$$\frac{\omega = f(r).\mathsf{children} \qquad |\omega| = n \qquad f(r).\mathsf{tag} = m}{f \vdash r \rightsquigarrow_m r :: \oplus\{\omega_i \mid 0 \leq i < n \ \wedge \ f \vdash \omega(i) \rightsquigarrow_m \omega_i\}}$$ Node Found - Non-Orphan Node

Fig. 7. Search Predicate

$$\frac{\begin{array}{cc} f(r).\mathsf{tag} = m & |f(r).\mathsf{children}| = 0 \\ \sigma = \Sigma(r).\mathsf{pos} & \phi_\natural(m) \sqsubseteq \sigma \sqsubseteq \sigma_m \\ \phi'_\natural = \phi_\natural\,[m \mapsto \sigma] & \varphi'_\natural = \varphi_\natural\,[(m,\sigma) \mapsto r] \end{array}}{\mathcal{WL}_{f,\Sigma} \vdash^r \phi_\natural, \varphi_\natural \rightsquigarrow \phi'_\natural, \varphi'_\natural}$$ Orphan Node

$$\frac{\begin{array}{cc} f(r).\mathsf{tag} = m & \sigma = \Sigma(r).\mathsf{pos} \\ \phi_\natural(m) \sqsubseteq \sigma \sqsubseteq \sigma_m & |f(r).\mathsf{children}| = n > 0 \\ \phi^0_\natural = \phi_\natural\,[m \mapsto \sigma] & \varphi^0_\natural = \varphi_\natural\,[(m,\sigma) \mapsto r] \\ \multicolumn{2}{c}{\forall_{0 \leq i < n}\ \Sigma(r).\mathsf{pos} \sqsubseteq \Sigma(f(r).\mathsf{children}(i)).\mathsf{pos}} \\ \multicolumn{2}{c}{\forall_{0 \leq i < n}\ \mathcal{WL}_{f,\Sigma} \vdash^{f(r).\mathsf{children}(i)} \phi^i_\natural, \varphi^i_\natural \rightsquigarrow \phi^{i+1}_\natural, \varphi^{i+1}_\natural} \end{array}}{\mathcal{WL}_{f,\Sigma} \vdash^r \phi_\natural, \varphi_\natural \rightsquigarrow \phi^n_\natural, \varphi^n_\natural}$$ Non-Orphan Node

Fig. 8. Well-Labeling Predicate for Live Primitives

Proof. The proof proceeds by induction on the structure of the derivation of $f \vdash r \rightsquigarrow_m \omega$. There are two base cases to consider [Node Not Found - Orphan Node] and [Node Found - Orphan Node]. The inductive cases are [Node Not Found - Non-Orphan Node] and [Node Found - Non-Orphan Node]. Since the inductive case are analogous, we only consider the case [Node Found - Non-Orphan Node] that is the most complex.

[Node Not Found - Orphan Node] In this case: $|f(r).\mathsf{children}| = 0$ and $f(r).\mathsf{tag} \neq m$ (hyp.3). We conclude that:

- $\phi'_\natural = \phi_\natural$ and $\omega = \epsilon$ **(1)** - (hyp.1)-(hyp.3)

[Node Found - Orphan Node] In this case: $|f(r).\mathsf{children}| = 0$, $f(r).\mathsf{tag} = m$, (hyp.3). Letting $\sigma = \Sigma(r).\mathsf{pos}$, we conclude that:

- $\phi_\natural(m) \sqsubseteq \sigma \sqsubseteq \sigma_m$, $\phi'_\natural = \phi_\natural\,[m \mapsto \sigma]$, and $\omega = r :: \epsilon$ (1) - (hyp.1)-(hyp.3)
- $\phi_\natural(m) \sqsubseteq \Sigma(\omega(0)).\mathsf{pos} = \phi'_\natural(m) \sqsubseteq \sigma_m$ **(2)** - (1)

[Node Found - Non-Orphan Node] In this case: $|f(r).\mathsf{children}| = n$, $n \neq 0$, $f(r).\mathsf{tag} = m$, (hyp.3). Letting $\sigma = \Sigma(r).\mathsf{pos}$ and $\omega' = f(r).\mathsf{children}$, we conclude that:

- $\omega = r :: \oplus\{\omega_i \mid 0 \leq i < n \ \wedge \ f \vdash \omega(i) \rightsquigarrow_m \omega_i\}$ (1) - (hyp.1) + (hyp.3)
- $\phi_\natural(m) \sqsubseteq \sigma \sqsubseteq \sigma_m$ (2) - (hyp.2) + (hyp.3)

– $\phi_t(m) \sqsubseteq \Sigma(r).\mathsf{pos} = \phi_t^0(m) \sqsubseteq \sigma_m$, where $\phi_t^0 = \phi_t\,[m \mapsto \sigma]$ (3) - (hyp.2) + (hyp.3)
– $\forall_{0\leq i<n}\ \Sigma(r).\mathsf{pos} \sqsubseteq \Sigma(f(r).\mathsf{children}(i)).\mathsf{pos}$ (4) - (hyp.2) + (hyp.3)
– $\forall_{0\leq i<n}\ \mathcal{WL}_{f,\Sigma} \vdash^{f(r).\mathsf{children}(i)} \phi_t^i \rightsquigarrow \phi_t^{i+1}$ and $\phi'_t = \phi_t^n$ (5) - (hyp.2) + (hyp.3)
– For all $0 \leq i < n$, $\Sigma.\mathsf{pos}(\omega_i)$ is monotonically increasing and $\phi_t^i(m) \sqsubseteq \Sigma.\mathsf{pos}(\omega_i) \sqsubseteq \phi_t^{i+1}(m) \sqsubseteq \sigma_m$ (6) - (1) + (5) + **ih**
– The list ω is monotonically increasing and $\phi_t(m) \sqsubseteq \Sigma.\mathsf{pos}(\omega) \sqsubseteq \phi'_t(m) \sqsubseteq \sigma_m$ **(7)** - (3) + (6)

□

We define the *low-projection* at level σ of a live record φ_t, written $\varphi_t \restriction^\sigma$ as the live record φ'_t defined as follows:

$$\varphi'_t(m,\sigma') = \begin{cases} \varphi_t(m,\sigma') \text{ if } \sigma' \sqsubseteq \sigma \\ \textit{undefined} \text{ otherwise} \end{cases}$$

Lemma 13 (High-Positioned Tree). *Given a forest f labeled by Σ, a node reference r, two functions ϕ_t and φ_t, and a tag name m such that $\mathcal{WL}_{f,\Sigma} \vdash^r \phi_t, \varphi_t \rightsquigarrow \phi'_t, \varphi'_t$ (hyp.1) and $\Sigma(r).\mathsf{pos} \not\sqsubseteq \sigma$ (hyp.2), for some functions ϕ'_t and φ'_t, it holds that: $\varphi_t \restriction^\sigma = \varphi'_t \restriction^\sigma$.*

Proof. We proceed by induction on the derivation of (hyp.1). The base case is [Orphan Node] and the inductive case is [Non-Orphan Node].

[Orphan Node] In this case: $|f(r).\mathsf{children}| = 0$ (hyp.3). Letting $m = f(r).\mathsf{tag}$ and $\sigma' = \Sigma(r).\mathsf{pos}$, we conclude that:

– $\varphi'_t = \varphi_t\,[(m,\sigma') \mapsto r]$ (1) - (hyp.1) + (hyp.3)
– $\varphi'_t \restriction^\sigma = \varphi_t \restriction^\sigma$ **(2)** - (hyp.2) + (1)

[Non-Orphan Node] In this case: $|f(r).\mathsf{children}| = n$ for $n > 0$ (hyp.3). Letting $m = f(r).\mathsf{tag}$, $\sigma' = \Sigma(r).\mathsf{pos}$, $\phi_t^0 = \phi_t\,[m \mapsto \sigma]$, and $\varphi_t^0 = \varphi_t\,[(m,\sigma) \mapsto r]$, we conclude that:

– $\forall_{0\leq i<n}\ \Sigma(r).\mathsf{pos} \sqsubseteq \Sigma(f(r).\mathsf{children}(i)).\mathsf{pos}$ (1) - (hyp.1) + (hyp.3)
– $\forall_{0\leq i<n}\ \mathcal{WL}_{f,\Sigma} \vdash^{f(r).\mathsf{children}(i)} \phi_t^i, \varphi_t^i \rightsquigarrow \phi_t^{i+1}, \varphi_t^{i+1}$ and $\varphi'_t = \varphi_t^n$ (2) - (hyp.1) + (hyp.3)
– $\varphi_t^0 \restriction^\sigma = \varphi_t \restriction^\sigma$ (3) - *definition*
– $\forall_{0\leq i<n}\ \Sigma(f(r).\mathsf{children}(i)).\mathsf{pos} \not\sqsubseteq \sigma$ (4) - (hyp.2) + (1)
– $\forall_{0\leq i<n}\ \varphi_t^i \restriction^\sigma = \varphi_t^{i+1} \restriction^\sigma$ (5) - (2) + (4) + **ih**
– $\varphi_t^0 \restriction^\sigma = \varphi_t^n \restriction^\sigma = \varphi'_t \restriction^\sigma$ (6) - (2) + (5)
– $\varphi_t \restriction^\sigma = \varphi'_t \restriction^\sigma$ **(7)** - (3) + (6)

□

Lemma 14 (Live Records of Well-labeled Low-Equal Trees). *Given two forests f and $\hat{f}$ respectively well-labeled by Σ and $\hat{\Sigma}$, two live functions ϕ_t and $\hat{\phi}_t$, two live records φ_t and $\hat{\varphi}_t$, a node reference r, and a security level σ such that: $\mathcal{WL}_{f,\Sigma} \vdash^r \phi_t, \varphi_t \rightsquigarrow \phi'_t, \varphi'_t$ (hyp.1), $\mathcal{WL}_{\hat{f},\hat{\Sigma}} \vdash^r \hat{\phi}_t, \hat{\varphi}_t \rightsquigarrow \hat{\phi}'_t, \hat{\varphi}'_t$ (hyp.2), $f, \Sigma \sim_\sigma \hat{f}, \hat{\Sigma}$ (hyp.3), and $\varphi_t \restriction^\sigma = \hat{\varphi}_t \restriction^\sigma$ (hyp.4), it holds that: $\varphi'_t \restriction^\sigma = \hat{\varphi}'_t \restriction^\sigma$.*

Proof. Suppose that $\Sigma(r).\mathsf{pos} \not\sqsubseteq \sigma$ (hyp.5). We conclude that:

- $\varphi'_t \restriction^\sigma = \varphi_t \restriction^\sigma$ (1) - (hyp.1) + (hyp.5) + *High Positioned Tree*
- $\hat{\Sigma}(r).\mathsf{pos} \not\sqsubseteq \sigma$ (2) - (hyp.3) + (hyp.5)
- $\hat{\varphi}'_t \restriction^\sigma = \hat{\varphi}_t \restriction^\sigma$ (3) - (hyp.2) + (2) + *High Positioned Tree*
- $\varphi'_t \restriction^\sigma = \hat{\varphi}'_t \restriction^\sigma$ **(4)** - (hyp.4) + (1) + (3)

In the rest of the proof we suppose that $\Sigma(r).\mathsf{pos} = \hat{\Sigma}(r).\mathsf{pos} \sqsubseteq \sigma$ (hyp.5) and we proceed by induction on the derivation of (hyp.1). The base case is [Orphan Node] and the inductive case is [Non-Orphan Node].

[Orphan Node] In this case: $|f(r).\mathsf{children}| = 0$ (hyp.6). Letting $m = f(r).\mathsf{tag}$ and $\sigma' = \Sigma(r).\mathsf{pos} = \hat{\Sigma}(r).\mathsf{pos}$, $\hat{m} = \hat{f}(r).\mathsf{tag}$, and $\hat{\varphi}^0_t = \hat{\varphi}_t\,[(\hat{m}, \sigma') \mapsto r]$, we conclude that:

- $\varphi'_t = \varphi_t\,[(m, \sigma') \mapsto r]$ (1) - (hyp.1) + (hyp.6)
- $\Sigma(r).\mathsf{node} = \hat{\Sigma}(r).\mathsf{node} \sqsubseteq \sigma$ (2) - (hyp.4) + (hyp.5)
- $m = \hat{m}$ (3) - (hyp.3) + (2)
- $\varphi'_t \restriction^\sigma = \hat{\varphi}^0_t \restriction^\sigma$ (4) - (hyp.4) + (hyp.5) + (1) + (3)

If $|\hat{f}(r).\mathsf{children}| = 0$, then $\hat{\varphi}'_t = \hat{\varphi}^0_t$ and the result follows immediately by (4). Hence, suppose that: $|\hat{f}(r).\mathsf{children}| = n > 0$ (hyp.7). We conclude that:

- $\forall_{0 \le i < n}\ \mathcal{WL}_{\hat{f},\hat{\Sigma}} \vdash^{\hat{f}(r).\mathsf{children}(i)} \hat{\phi}^i_t, \hat{\varphi}^i_t \rightsquigarrow \hat{\phi}^{i+1}_t, \hat{\varphi}^{i+1}_t$ and $\hat{\varphi}'_t = \varphi^n_t$ (5) - (hyp.2) + (hyp.7)
- $\forall_{0 \le i < n}\ \hat{\Sigma}(\hat{f}(r).\mathsf{children}(i)) \not\sqsubseteq \sigma$ (6) - (hyp.3) + (hyp.6) + (hyp.7)
- $\forall_{0 \le i < n}\ \hat{\varphi}^i_t \restriction^\sigma = \hat{\varphi}^{i+1}_t \restriction^\sigma$ (7) - (5) + (6) + *High-Positioned Tree*
- $\hat{\varphi}^0_t \restriction^\sigma = \hat{\varphi}^n_t \restriction^\sigma = \hat{\varphi}'_t \restriction^\sigma$ (8) - (5) + (7)
- $\varphi'_t \restriction^\sigma = \hat{\varphi}'_t \restriction^\sigma$ **(9)** - (4) + (8)

[Non-Orphan Node] In this case: $|f(r).\mathsf{children}| = n > 0$ (hyp.6). Since the case in which $|\hat{f}(r).\mathsf{children}| = 0$ is symmetric to the previous case. We shall assume that: $|\hat{f}(r).\mathsf{children}| = \hat{n} > 0$ (hyp.7). Letting $m = f(r).\mathsf{tag}$ and $\sigma' = \Sigma(r).\mathsf{pos} = \hat{\Sigma}(r).\mathsf{pos}$, $\hat{m} = \hat{f}(r).\mathsf{tag}$, $\varphi^0_t = \varphi_t\,[(m, \sigma') \mapsto r]$, $\hat{\varphi}^0_t = \hat{\varphi}_t\,[(\hat{m}, \sigma') \mapsto r]$, we conclude that:

- $\Sigma(r).\mathsf{node} = \hat{\Sigma}(r).\mathsf{node} \sqsubseteq \sigma$ (1) - (hyp.3) + (hyp.5)
- $m = \hat{m}$ (2) - (hyp.3) + (1)
- $\forall_{0 \le i < n}\ \mathcal{WL}_{f,\Sigma} \vdash^{f(r).\mathsf{children}(i)} \phi^i_t, \varphi^i_t \rightsquigarrow \phi^{i+1}_t, \varphi^{i+1}_t$ and $\varphi'_t = \varphi^n_t$ (3) - (hyp.1) + (hyp.6)
- $\forall_{0 \le i < \hat{n}}\ \mathcal{WL}_{\hat{f},\hat{\Sigma}} \vdash^{\hat{f}(r).\mathsf{children}(i)} \hat{\phi}^i_t, \hat{\varphi}^i_t \rightsquigarrow \hat{\phi}^{i+1}_t, \hat{\varphi}^{i+1}_t$ and $\hat{\varphi}'_t = \varphi^{\hat{n}}_t$ (4) - (hyp.2) + (hyp.7)
- $\varphi^0_t \restriction^\sigma = \hat{\varphi}^0_t \restriction^\sigma$ (5) - (hyp.4) + (1) + (2)

Since the position levels of the children of $f(r)$ and $\hat{f}(r)$ are in increasing order, we conclude form (hyp.3) that there is an unique integer j such that:

- $\forall_{0 \le i < j}\ \Sigma(f(r).\mathsf{children}(i)).\mathsf{pos} \sqsubseteq \sigma$ (6) - (hyp.3)
- $\forall_{j \le i < |f(r).\mathsf{children}|}\ \Sigma(f(r).\mathsf{children}(i)).\mathsf{pos} \not\sqsubseteq \sigma$ (7) - (hyp.3)

- $\forall_{0 \leq i < j}\ \hat{\Sigma}(\hat{f}(r).\mathsf{children}(i)).\mathsf{pos} \sqsubseteq \sigma$ (8) - (hyp.3)
- $\forall_{j \leq i < |\hat{f}(r).\mathsf{children}|}\ \hat{\Sigma}(\hat{f}(r).\mathsf{children}(i)).\mathsf{pos} \not\sqsubseteq \sigma$ (9) - (hyp.3)
- $\varphi'^{j}_{\ell}\restriction^{\sigma} = \varphi'^{n}_{\ell}\restriction^{\sigma} = \varphi'_{\ell}\restriction^{\sigma}$ (10) - (3) + (7)
- $\hat{\varphi}'^{j}_{\ell}\restriction^{\sigma} = \hat{\varphi}'^{n}_{\ell}\restriction^{\sigma} = \hat{\varphi}'_{\ell}\restriction^{\sigma}$ (11) - (4) + (9)
- $\forall_{0 \leq i < j}\ f(r).\mathsf{children}(i) = \hat{f}(r).\mathsf{children}(i)$ (12) - (hyp.3)

We now prove by induction on j that $\varphi'^{j}_{\ell}\restriction^{\sigma} = \hat{\varphi}'^{j}_{\ell}\restriction^{\sigma}$. If $j = 0$, then the result immediately holds by (5). Suppose that $j = k + 1$:

- $\varphi'^{k}_{\ell}\restriction^{\sigma} = \hat{\varphi}'^{k}_{\ell}\restriction^{\sigma}$ (13) - **inner ih**
- $\varphi'^{k+1}_{\ell}\restriction^{\sigma} = \hat{\varphi}'^{k+1}_{\ell}\restriction^{\sigma}$ (14) - (hyp.3) + (3) + (4) + (12) + (13) + **outer ih**

□

Lemma 15 (Live Record Invariance - 1). *Given a forest f labeled by Σ, a live function ϕ_ℓ, a live record φ_ℓ, a node reference r, a tag name m, and two security levels σ and σ' such that: $\mathcal{WL}_{f,\Sigma} \vdash^{r} \phi_\ell, \varphi_\ell \rightsquigarrow \phi'_\ell, \varphi'_\ell$ (hyp.1), $(m, \sigma) \in dom(\varphi_\ell)$ (hyp.2), and $\sigma \not\sqsubseteq \sigma'$ (hyp.3), it holds that: $\varphi_\ell(m, \sigma') = \varphi'_\ell(m, \sigma')$.*

Proof. If $(m, \sigma) \in dom(\varphi_\ell)$, then in order for the subtree rooted in r to be well-labeled by Σ (which it is), all the nodes with tag m that it includes must have a position level higher than or equal to σ. Therefore, we conclude that it does not include any node with tag m whose position level is $\not\sqsupseteq \sigma$, from which the result follows. □

Lemma 16 (Live Record Invariance - 2). *Given a forest f labeled by Σ, a live function ϕ_ℓ, a live record φ_ℓ, a node reference r, a tag name m, and a security level σ such that: $\mathcal{WL}_{f,\Sigma} \vdash^{r} \phi_\ell, \varphi_\ell \rightsquigarrow \phi'_\ell, \varphi'_\ell$ (hyp.1), $f \vdash r \rightsquigarrow_m \omega$ (hyp.2), and $\varphi_\ell(m, \sigma) = \varphi'_\ell(m, \sigma)$ (hyp.3), it holds that $\forall_{0 \leq i < |\omega|}\ \Sigma(\omega(i)).\mathsf{pos} \not\sqsubseteq \sigma$.*

Proof. The proof proceeds by induction on the structure of the derivation of $f \vdash r \rightsquigarrow_m \omega$. There are two base cases to consider [Node Not Found - Orphan Node] and [Node Found - Orphan Node]. The inductive cases are [Node Not Found - Non-Orphan Node] and [Node Found - Non-Orphan Node]. Since the inductive case are analogous, we only consider the case [Node Found - Non-Orphan Node] that is the most complex.

[Node Not Found - Orphan Node] In this case: $|f(r).\mathsf{children}| = 0$. Hence the result holds vacuously.

[Node Found - Orphan Node] In this case: $|f(r).\mathsf{children}| = 0$ and $f(r).\mathsf{tag} = m$ (hyp.4). Letting $\sigma' = \Sigma(r).\mathsf{pos}$, we conclude that:

- $\varphi'_\ell = \varphi_\ell\ [(m, \sigma') \mapsto r]$ (1) - (hyp.1) + (hyp.4)
- $\omega = \sigma' :: \epsilon$ (2) - (hyp.2) + (hyp.4)
- $\sigma' \neq \sigma$ (3) - (hyp.3) + (1)
- $\sigma' \not\sqsubseteq \sigma$ **(4)**

  Suppose that: $\sigma' \sqsubseteq \sigma$ (hyp.4). We conclude that:

- $\sigma' \sqsubset \sigma$ (4.1) - (hyp.4) + (3)
- $\sigma \not\sqsubseteq \sigma'$ (4.2) - (4.1)
- $\varphi_\natural(m, \sigma') = \varphi'_\natural(m, \sigma')$ (4.3) - (4.2) + *Live Record Invariance - 1*
- *Contradiction* (4.4) - (1) + (4.3)

[Node Found - Non-Orphan Node] In this case: $|f(r).\mathsf{children}| = n > 0$, and $f(r).\mathsf{tag} = m$ (hyp.4). Letting $\sigma' = \Sigma(r).\mathsf{pos}$ and $\omega' = f(r).\mathsf{children}$, we conclude that:

- $\omega' = r :: \oplus\{\omega_i \mid 0 \leq i < n \ \wedge \ f \vdash \omega(i) \rightsquigarrow_m \omega_i\}$ (1) - (hyp.2) + (hyp.4)
- $\varphi^0_\natural = \varphi_\natural\ [(m, \sigma') \mapsto r]$ (2) - (hyp.1) + (hyp.4)
- $\sigma' \neq \sigma$ (3) - (hyp.3) + (2)
- $\sigma' \not\sqsubseteq \sigma$ (4) - (hyp.4) + (2) + (3)
- $\forall_{0 \leq i < n}\ \mathcal{WL}_{f,\Sigma} \vdash^{f(r).\mathsf{children}(i)} \phi^i_\natural, \varphi^i_\natural \rightsquigarrow \phi^{i+1}_\natural, \varphi^{i+1}_\natural$ and $\varphi'_\natural = \varphi^n_\natural$ (5) - (hyp.1) + (hyp.4)
- $\forall_{0 \leq i < n}\ \varphi^i_\natural(m, \sigma) = \varphi^{i+1}_\natural(m, \sigma)$ (6) - (hyp.1) + (hyp.3) + (hyp.4)
- $\forall_{0 \leq i < n}\ \forall_{0 \leq j < |\omega_i|}\ \Sigma(\omega_i(j)).\mathsf{pos} \not\sqsubseteq \sigma$ (7) - (1) + (5) + (6) + **ih**
- $\forall_{0 \leq i < |\omega|}\ \Sigma(\omega(i)).\mathsf{pos} \not\sqsubseteq \sigma$ **(8)** - (1) + (7)

□

Lemma 17 (Low-Equal DOM Searches). *Given two forests f and $\hat{f}$ respectively well-labeled by Σ and $\hat{\Sigma}$, two live functions $\phi_\natural$ and $\hat{\phi}_\natural$, two live records $\varphi_\natural$ and $\hat{\varphi}_\natural$, a node reference r, and a security level σ such that: $\mathcal{WL}_{f,\Sigma} \vdash^r \phi_\natural, \varphi_\natural \rightsquigarrow \phi'_\natural, \varphi'_\natural$ (hyp.1), $\mathcal{WL}_{\hat{f},\hat{\Sigma}} \vdash^r \hat{\phi}_\natural, \hat{\varphi}_\natural \rightsquigarrow \hat{\phi}'_\natural, \hat{\varphi}'_\natural$ (hyp.2), $f \vdash r \rightsquigarrow_m \omega$ (hyp.3), $\hat{f} \vdash r \rightsquigarrow_m \hat{\omega}$ (hyp.4), $f, \Sigma \sim_\sigma \hat{f}, \hat{\Sigma}$ (hyp.5), and $\varphi_\natural \restriction^\sigma = \hat{\varphi}_\natural \restriction^\sigma$ (hyp.6), it holds that: $\omega, \Sigma.\mathsf{pos}(\omega) \simeq_\sigma \hat{\omega}, \hat{\Sigma}.\mathsf{pos}(\hat{\omega})$.*

Proof. Suppose that $\Sigma(r).\mathsf{pos} \not\sqsubseteq \sigma$ (hyp.7), we conclude that:

- $\hat{\Sigma}(r).\mathsf{pos} \not\sqsubseteq \sigma$ (1) - (hyp.5) + (hyp.7)
- $\forall_{0 \leq i < |\omega|}\ \Sigma(\omega(i)).\mathsf{pos} \not\sqsubseteq \sigma$ (2) - (hyp.1) + (hyp.3) + (hyp.7) + *Monotonocity of the Search Relation*
- $\forall_{0 \leq i < |\hat{\omega}|}\ \hat{\Sigma}(\hat{\omega}(i)).\mathsf{pos} \not\sqsubseteq \sigma$ (3) - (hyp.2) + (hyp.4) + (1) + *Monotonocity of the Search Relation*
- $\omega, \Sigma.\mathsf{pos}(\omega) \simeq_\sigma \hat{\omega}, \hat{\Sigma}.\mathsf{pos}(\hat{\omega})$ **(4)** - (2) + (3)

In the rest of the proof we assume that $\Sigma(r).\mathsf{pos} \sqcup \hat{\Sigma}(r).\mathsf{pos} \sqsubseteq \sigma$ (hyp.7) and we proceed by induction on the structure of the derivation of $f \vdash r \rightsquigarrow_m \omega$. There are two base cases to consider [Node Not Found - Orphan Node] and [Node Found - Orphan Node]. The inductive cases are [Node Not Found - Non-Orphan Node] and [Node Found - Non-Orphan Node]. Since both the base cases and the inductive cases are analogous, we only consider the cases [Node Not Found - Orphan Node] and [Node Found - Non-Orphan Node].

[Node Not Found - Orphan Node] In this case: $|f(r).\mathsf{children}| = 0$ and $f(r).\mathsf{tag} \neq m$ (hyp.8). Letting $\hat{\omega}_i$ be: $\hat{f} \vdash \hat{f}(r).\mathsf{children}(i) \rightsquigarrow_m \hat{\omega}_i$, for $0 \leq i < |\hat{f}(r).\mathsf{children}|$, we conclude that:

- $\omega = \epsilon$ (1) - (hyp.3) + (hyp.8)
- $\hat{f}(r).\mathsf{tag} \neq m$ (2) - (hyp.5) + (hyp.7) + (hyp.8)
- $\forall_{0 \leq i < |\hat{f}(r).\mathsf{children}|}\ \hat{\Sigma}(\hat{f}(r).\mathsf{children}(i)).\mathsf{pos} \not\sqsubseteq \sigma$ (3) - (hyp.5) + (hyp.7)
- For all $0 \leq i < |\hat{f}(r).\mathsf{children}|$ and for all $0 \leq j < |\hat{\omega}_i|$: $\hat{\Sigma}(\hat{\omega}_i(j)) \not\sqsubseteq \sigma$ (4) - (3) + *Monotonocity of Search Predicate*
- $\omega, \Sigma.\mathsf{pos}(\omega) \simeq_\sigma \hat{\omega}, \hat{\Sigma}.\mathsf{pos}(\hat{\omega})$ **(5)** - (4)

[Node Found - Non-Orphan Node] In this case: $|f(r).\mathsf{children}| = n > 0$ and $f(r).\mathsf{tag} = m$ (hyp.8). Without loss of generality, let us assume that $|\hat{f}(r).\mathsf{children}| = \hat{n} > 0$ (hyp.9). We conclude that:

- $\omega = r :: \oplus\{\omega_i \mid 0 \leq i < n\ \wedge\ f \vdash f(r).\mathsf{children}(i) \rightsquigarrow_m \omega_i\}$ (1) - (hyp.3) + (hyp.8)
- $\hat{\omega} = r :: \oplus\{\hat{\omega}_i \mid 0 \leq i < n\ \wedge\ \hat{f} \vdash \hat{f}(r).\mathsf{children}(i) \rightsquigarrow_m \hat{\omega}_i\}$ (2) - (hyp.4) + (hyp.9)
- $\forall_{0 \leq i < n}\ \mathcal{WL}_{f,\Sigma} \vdash^{f(r).\mathsf{children}(i)} \phi_t^i, \varphi_t^i \rightsquigarrow \phi_t^{i+1}, \varphi_t^{i+1}$ and $\phi'_t = \phi_t^n$ (3) - (hyp.1) + (hyp.8)
- $\forall_{0 \leq i < \hat{n}}\ \mathcal{WL}_{\hat{f},\hat{\Sigma}} \vdash^{\hat{f}(r).\mathsf{children}(i)} \hat{\phi}_t^i, \hat{\varphi}_t^i \rightsquigarrow \hat{\phi}_t^{i+1}, \hat{\varphi}_t^{i+1}$ and $\hat{\phi}'_t = \hat{\phi}_t^{\hat{n}}$ (4) - (hyp.2) + (hyp.9)

Let i be the largest integer such that $\phi_t^{i-1}(m) \sqsubseteq \sigma$ and $\phi_t^i(m) \not\sqsubseteq \sigma$ and let j be the largest integer such that $\hat{\phi}_t^{j-1}(m) \sqsubseteq \sigma$ and $\hat{\phi}_t^j(m) \not\sqsubseteq \sigma$. We have to prove that:

1. Prove that i and j coincide.
2. Prove that for every integer $0 \leq l < i = j$, it holds that:

$$r :: \omega_0 \oplus \cdots \oplus \omega_l, \Sigma(r).\mathsf{pos} :: \Sigma.\mathsf{pos}(\omega_0) \oplus \cdots \oplus \Sigma.\mathsf{pos}(\omega_l) \approx_\sigma$$
$$r :: \hat{\omega}_0 \oplus \cdots \oplus \hat{\omega}_l, \hat{\Sigma}(r).\mathsf{pos} :: \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_0) \oplus \cdots \oplus \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_l)$$

3. Prove that:

$$r :: \omega_0 \oplus \cdots \oplus \omega_i, \Sigma(r).\mathsf{pos} :: \Sigma.\mathsf{pos}(\omega_0) \oplus \cdots \oplus \Sigma.\mathsf{pos}(\omega_i) \simeq_\sigma$$
$$r :: \hat{\omega}_0 \oplus \cdots \oplus \hat{\omega}_i, \hat{\Sigma}(r).\mathsf{pos} :: \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_0) \oplus \cdots \oplus \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_i)$$

4. Prove that: $\sqcap\{\sqcap\Sigma.\mathsf{pos}(\omega_l) \mid i < l < |f(r).\mathsf{children}|\} \not\sqsubseteq \sigma$
5. Prove that: $\sqcap\{\sqcap\hat{\Sigma}.\mathsf{pos}(\hat{\omega}_l) \mid i < l < |\hat{f}(r).\mathsf{children}|\} \not\sqsubseteq \sigma$

Proof of 1. Suppose that $\phi_t^{i-1}(m) \sqsubseteq \sigma$ and $\phi_t^i(m) \not\sqsubseteq \sigma$ and let j be the largest integer such that $\hat{\phi}_t^{j-1}(m) \sqsubseteq \sigma$ and $\hat{\phi}_t^j(m) \not\sqsubseteq \sigma$ (hyp.10). We conclude that:

- $\varphi_t^{i-1} \restriction^\sigma = \hat{\varphi}_t^{i-1} \restriction^\sigma$ and $\varphi_t^i \restriction^\sigma = \hat{\varphi}_t^i \restriction^\sigma$ (5) - (hyp.1) + (hyp.2) + (hyp.5) + (hyp.6) + Lemma 14
- $\hat{\phi}_t^{i-1}(m) \sqsubseteq \sigma$ (6) - (hyp.10) + (5)
- $\hat{\phi}_t^i(m) \not\sqsubseteq \sigma$ (7) - (hyp.10) + (5)
- $j = i$ (8) - (6) + (7)

Proof of 2. We proceed by induction on l.

Base case: $l = 0$.

- $\omega_0, \Sigma.\mathsf{pos}(\omega_0) \simeq_\sigma \hat{\omega}_0, \Sigma.\mathsf{pos}(\omega_0)$ (9) - (hyp.5) + (hyp.6) + (1)-(4) + **outer ih**

– $\omega_0, \Sigma.\mathsf{pos}(\omega_0) \approx_\sigma \hat{\omega}_0, \Sigma.\mathsf{pos}(\omega_0)$ (10) - (hyp.10) + (9)

Inductive case: $l = l' + 1$.

– $r :: \omega_0 \oplus \cdots \oplus \omega'_l, \Sigma(r).\mathsf{pos} :: \Sigma.\mathsf{pos}(\omega_0) \oplus \cdots \oplus \Sigma.\mathsf{pos}(\omega'_l) \approx_\sigma$
$r :: \hat{\omega}_0 \oplus \cdots \oplus \hat{\omega}'_l, \hat{\Sigma}(r).\mathsf{pos} :: \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_0) \oplus \cdots \oplus \hat{\Sigma}.\mathsf{pos}(\hat{\omega}'_l)$ (11) - **inner ih**
– $\omega_l, \Sigma.\mathsf{pos}(\omega_l) \simeq_\sigma \hat{\omega}_l, \Sigma.\mathsf{pos}(\omega_l)$ (12) - (hyp.5) + (hyp.6) + (1)-(4) + **outer ih**
– $\omega_l, \Sigma.\mathsf{pos}(\omega_l) \approx_\sigma \hat{\omega}_l, \Sigma.\mathsf{pos}(\omega_l)$ (13) - (hyp.10) + (9)
– $r :: \omega_0 \oplus \cdots \oplus \omega_l, \Sigma(r).\mathsf{pos} :: \Sigma.\mathsf{pos}(\omega_0) \oplus \cdots \oplus \Sigma.\mathsf{pos}(\omega_l) \approx_\sigma$
$r :: \hat{\omega}_0 \oplus \cdots \oplus \hat{\omega}_l, \hat{\Sigma}(r).\mathsf{pos} :: \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_0) \oplus \cdots \oplus \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_l)$ (14) - (11) + (13)

Proof of 3.

– $\omega_i, \Sigma.\mathsf{pos}(\omega_i) \simeq_\sigma \hat{\omega}_i, \Sigma.\mathsf{pos}(\omega_i)$ (15) - (hyp.5) + (hyp.6) + (1)-(4) + **ih**
– $r :: \omega_0 \oplus \cdots \oplus \omega_i, \Sigma(r).\mathsf{pos} :: \Sigma.\mathsf{pos}(\omega_0) \oplus \cdots \oplus \Sigma.\mathsf{pos}(\omega_i) \simeq_\sigma$
$r :: \hat{\omega}_0 \oplus \cdots \oplus \hat{\omega}_i, \hat{\Sigma}(r).\mathsf{pos} :: \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_0) \oplus \cdots \oplus \hat{\Sigma}.\mathsf{pos}(\hat{\omega}_i)$ (16) - (14) + (15)

Proof of 4.

– $\forall_{i<l<|f(r).\mathsf{children}|}\ \varphi^l_t(m,\sigma) = \varphi^{l+1}_t(m,\sigma)$ (17) - (hyp.1) + (hyp.10)
– $\forall_{i<l<|f(r).\mathsf{children}|}\ \forall_{0\leq k<|\omega_l|}\ \Sigma(\omega_l(k)).\mathsf{pos} \not\sqsubseteq \sigma$ (18) - (hyp.1) + (17) + Lemma 16

Proof of 5.

– $\forall_{i<l<|\hat{f}(r).\mathsf{children}|}\ \hat{\varphi}^l_t(m,\sigma) = \hat{\varphi}^{l+1}_t(m,\sigma)$ (19) - (hyp.2) + (hyp.10) + (8)
– $\forall_{i<l<|\hat{f}(r).\mathsf{children}|}\ \forall_{0\leq k<|\hat{\omega}_l|}\ \hat{\Sigma}(\hat{\omega}_l(k)).\mathsf{pos} \not\sqsubseteq \sigma$ (20) - (hyp.2) + (19) + Lemma 16

□

Theorem 2 (Low-Equality Strengthening). *Given two forests f_0 and f_1 respectively labeled by Σ_0 and Σ_1 and a security level σ such that $\mathcal{WL}(f_0, \Sigma_0)$ (hyp.1) and $\mathcal{WL}(f_1, \Sigma_1)$ (hyp.2) and $f_0, \Sigma_0 \sim_\sigma f_1, \Sigma_1$ (hyp.3), it holds that: $f_0, \Sigma_0 \sim^\natural_\sigma f_1, \Sigma_1$.*

Proof. In order to prove the result, we have to prove that if $(r, m, i, r') \in f_0 \restriction^{\Sigma_0,\sigma}_\natural$, then $(r, m, i, r') \in f_1 \restriction^{\Sigma_1,\sigma}_\natural$ and that if $(r, m, n) \in f_0 \restriction^{\Sigma_0,\sigma}_\natural$, then $(r, m, n) \in f_1 \restriction^{\Sigma_1,\sigma}_\natural$.

Assume that: $(r, m, i, r') \in f_0 \restriction^{\Sigma_0,\sigma}_\natural$ (hyp.4). We conclude that:

– $f_0 \vdash r \rightsquigarrow_m \omega_0$, $\omega_0(i) = r'$, and $\Sigma_0(r').\mathsf{pos} \sqsubseteq \sigma$ (1) - (hyp.4)
– $\Sigma_0(r).\mathsf{pos} \sqsubseteq \sigma$ (2) - (hyp.1) + (1)
– $\Sigma_0(r).\mathsf{node} \sqsubseteq \sigma$ (3) - (2)
– $r \in dom(f_1)$, $\Sigma_1(r).\mathsf{node} \sqsubseteq \sigma$, and $\Sigma_1(r).\mathsf{pos} \sqsubseteq \sigma$ (4) - (hyp.3) + (2)

If we let ω_1 be the list of nodes verifying $f_1 \vdash r \rightsquigarrow_m \omega_1$ ((hyp.5)), we conclude that:

– $\omega_0, \Sigma_0.\mathsf{pos}(\omega_0) \simeq_\sigma \omega_1, \Sigma_1.\mathsf{pos}(\omega_1)$ (5) - (hyp.1)-(hyp.5) + Lemma 17
– $\omega_1(i) = r'$ and $\Sigma_1(r').\mathsf{pos} \sqsubseteq \sigma$ (6) - (1) + (5)
– $(r, m, i, r') \in f_1 \restriction^{\Sigma_1,\sigma}_\natural$ (7) - (hyp.5) + (6)

Assume that: $(r, m, n) \in f_0 \restriction^{\Sigma_0,\sigma}_\natural$ (hyp.4). We conclude that:

– $f_0 \vdash r \rightsquigarrow_m \omega_0$, $|\omega_0| = n$, and $\sigma_m \sqcup \Sigma(r).\mathsf{node} \sqsubseteq \sigma$ (1) - (hyp.4)
– $r \in dom(f_1)$ and $\Sigma_1(r).\mathsf{node} \sqsubseteq \sigma$ (2) - (hyp.3) + (1)

If we let ω_1 be the list of nodes verifying $f_1 \vdash r \rightsquigarrow_m \omega_1$ ((hyp.5)), we conclude that:

– $\omega_0, \Sigma_0.\mathsf{pos}(\omega_0) \simeq_\sigma \omega_1, \Sigma_1.\mathsf{pos}(\omega_1)$ (3) - (hyp.1)-(hyp.5) + Lemma 17
– $\sqcup\Sigma_0.\mathsf{pos}(\omega_0) \sqsubseteq \sigma_m$ (4) - (hyp.1) + (hyp.4)
– $\sqcup\Sigma_1.\mathsf{pos}(\omega_1) \sqsubseteq \sigma_m$ (5) - (hyp.2) + (hyp.5)
– $|\omega_0| = |\omega_1|$ (6) - (3)-(5)
– $(r, m, n) \in f_1 \restriction_{\nmid}^{\Sigma_1,\sigma}$ **(7)** - (hyp.5) + (6)

□

C From DOM to Core DOM and Back

This appendix presents a translation of some of the most used constructs in the DOM API to Core DOM. The translation makes use of a "macro" - $\mathsf{index}(n)$ that corresponds to:

$$
\begin{array}{l}
p = \mathsf{move}_{\uparrow}(n);\\
\mathit{found} = \mathsf{false};\\
\mathsf{while}((i < \mathsf{len}(p))\ \&\&\ !\mathit{found})\{\\
\quad \mathsf{if}(\mathsf{move}_{\downarrow}(p, i) == n)\{\\
\quad\quad \mathit{found} = \mathsf{true}\\
\quad \}\ \mathsf{else}\ \{i = i + 1\}\\
\};\\
\mathsf{if}(\mathit{found})\{i\}\ \mathsf{else}\ \{\mathit{null}\}
\end{array}
$$

where *found*, i and p are supposed not to overlap with the variables of the original program. The translation is given in Tables 1 and 2. Finally, Table 3 presents a translation from Core DOM to DOM that clearly shows that all constructs of Core DOM can be easily mapped to DOM constructs.

Comments on the impact of the choice of language on the enforcement mechanism. The DOM specification states that the children of a node constitute a collection of type `NodeList`. Every `NodeList` implements a method `item(index)` that "returns the indexth item in the collection" or `null` if the "index is greater than or equal to the number of nodes [it contains]" [11]. Core DOM allows the programmer to move directly from a node to its i^{th} child (like established in the DOM API), as well as to insert/remove a node in/from the i^{th} position of the list of children of another node. This fact requires the enforcement mechanism to explicitly ensure that the position levels of sibling nodes are monotonically increasing. If we assume that every implementation of the DOM API forces a `NodeList` to be traversed from left to right, this problem automatically goes away due to standard label propagation. However, the specification makes no such restriction on the implementation of `NodeLists`.

DOM API	*Core DOM*
`n.nextSibling`	$p = \mathsf{move}_{\uparrow}(n)$ $i = \mathsf{index}(n)$ $\mathsf{if}(p \;\&\&\; i < (\mathsf{len}(p) - 1))\{$ $\quad \mathsf{move}_{\downarrow}(p, i + 1)$ $\}\ \mathsf{else}\ \{null\}$
`n.previousSibling`	$p = \mathsf{move}_{\uparrow}(n)$ $i = \mathsf{index}(n)$ $\mathsf{if}(p \;\&\&\; i > 0)\{$ $\quad \mathsf{move}_{\downarrow}(p, i - 1)$ $\}\ \mathsf{else}\ \{null\}$
`n.childNodes.length`	$\mathsf{len}(n)$
`n.childNodes[i]`	$\mathsf{if}(\mathsf{len}(n) > i)\{$ $\quad \mathsf{move}_{\downarrow}(n, i)$ $\}\ \mathsf{else}\ \{null\}$
`n.parentNode`	$\mathsf{move}_{\uparrow}(n)$
`n.firstChild`	$\mathsf{if}(\mathsf{len}(n) \geq 0)\{$ $\quad \mathsf{move}_{\downarrow}(n, 0)$ $\}\ \mathsf{else}\ \{null\}$
`n.lastChild`	$\mathsf{if}(\mathsf{len}(n) \geq 0)\{$ $\quad \mathsf{move}_{\downarrow}(n, (\mathsf{len}(n) - 1))$ $\}\ \mathsf{else}\ \{null\}$

Table 1. From DOM to Core DOM - Navigating Between Nodes

DOM API	*Core DOM*
`document.createElement(tag)`	$\mathsf{new}(tag)$
`n0.appendChild(n1)`	$\mathsf{insert}(n_0, n_1, \mathsf{len}(n_0))$
`n0.insertBefore(n1, n2)`	$\mathsf{if}(p1 = \mathsf{move}_{\uparrow}(n1))\{$ $\quad \mathsf{remove}(p1, n1, \mathsf{index}(n1))$ $\}$ else $\{null\}$; $\mathsf{if}(n0 == \mathsf{move}_{\uparrow}(n2))\{$ $\quad \mathsf{insert}(n0, n1, \mathsf{index}(n2))$ $\}$ else $\{null\}$
`n0.removeChild(n1)`	$\mathsf{if}(n0 == \mathsf{move}_{\uparrow}(n1))\{$ $\quad \mathsf{remove}(n0, \mathsf{index}(n1))$ $\}$ else $\{null\}$
`n0.replaceChild(n1, n2)`	$\mathsf{if}(p1 = \mathsf{move}_{\uparrow}(n1))\{$ $\quad \mathsf{remove}(p1, n1, \mathsf{index}(n1))$ $\}$ else $\{null\}$; $\mathsf{if}(n0 == \mathsf{move}_{\uparrow}(n2))\{$ $\quad \mathsf{insert}(n0, n1, \mathsf{index}(n2))$; $\quad \mathsf{remove}(n0, \mathsf{index}(n1) + 1)$ $\}$ else $\{null\}$;

Table 2. From DOM to Core DOM - Creation and Positioning of DOM Nodes

Core DOM	*DOM API*
$\mathsf{new}(tag)$	`document.createElement(tag)`
$\mathsf{move}_{\uparrow}(n)$	`n.parentNode`
$\mathsf{move}_{\downarrow}(n, i)$	`n.childNodes[i]`
$\mathsf{len}(n)$	`n.childNodes.length`
$\mathsf{insert}(n0, n1, i)$	`n0.insertBefore(n1, n0.childNodes[i])`
$\mathsf{remove}(n0, i)$	`n0.removeChild(n0.childNodes[i])`
$\mathsf{value}(n0)$	`n0.nodeValue`
$\mathsf{store}(n0, v)$	`n0.nodeValue = v`

Table 3. From Core DOM to DOM