Commutativity Analysis in XML Update Languages

Giorgio Ghelli[1], Kristoffer Rose[2], and Jérôme Siméon[2]

[1] Università di Pisa, Dipartimento di Informatica
Via Buonarroti 2, I-56127 Pisa, Italy
ghelli@di.unipi.it
[2] IBM T.J. Watson Research Center
P.O.Box 704, Yorktown Heights, NY 10598, U.S.A.
krisrose and simeon@us.ibm.com

Abstract. A common approach to XML updates is to extend XQuery with update operations. This approach results in very expressive languages which are convenient for users but are difficult to reason about. Deciding whether two expressions can commute has numerous applications from view maintenance to rewriting-based optimizations. Unfortunately, commutativity is undecidable in most recent XML update languages. In this paper, we propose a conservative analysis for an expressive XML update language that can be used to determine whether two expressions commute. The approach relies on a form of path analysis that computes upper bounds for the nodes that are accessed or modified in a given update expression. Our main result is a commutativity theorem that can be used to identify commuting expressions.

1 Introduction

Most of the proposed XML updates languages [7, 15, 19, 1, 12] extend a full-fledged query language such as XQuery [5] with update primitives. To simplify specification and reasoning, some of the first proposals [7, 15, 1] have opted for a so-called *snapshot semantics*, which delays update application until the end of the query. However, this leads to counter-intuitive results for some queries, and limits the expressiveness in a way that is not always acceptable for applications. For that reason, more recent proposals [12, 6] give the ability to apply updates in the course of query evaluation. Such languages typically rely on a semantics with a strict evaluation order. For example, consider the following query, which first inserts a set of elements, then accesses those elements using a path expression.

```
for $x in $doc/country return insert {<new/>} into {$x},
count($doc/country/new)
```

Such an example cannot be written in a language based on a snapshot semantics, as the `count` would always return zero. However, it can be written in the XQuery! [12] or the XQueryP [6] proposals, which both rely on an explicit left-to-right evaluation order. Still, such a semantics severely restricts the optimizer's ability for rewritings, unless the optimizer is able to decide that some pairs of expressions commute.

Deciding commutativity, or more generally whether an update and a query *interfere*, has numerous applications, including optimizations based on algebraic rewritings, detecting when an update needs to be propagated through a view (usually specified as a query), deciding whether sub-expressions of a given query can be executed in parallel, etc. Unfortunately, commutativity is undecidable for XQuery extended with updates. In this paper, we propose a conservative approach to detect whether two query/update expressions interfere, i.e., whether they can be safely commuted or not. Our technique relies on an extension of the path analysis proposed in [17] that infers upper bounds for the nodes accessed and modified by a given expression. Such upper bounds are specified as simple path expressions for which disjointness is decidable [3, 18].

Our commutativity analysis serves a similar purpose to independence checking in the relational context [10, 16]. To the best of our knowledge, our work is the first to study such issues in the XML context, where languages are typically much more expressive. A simpler form of static analysis is proposed in [1, 2], suggesting that similar techniques can be used to optimize languages with a snapshot semantics. Finally, commutativity of tree operations is used in transactional models [9, 14], but relies on run-time information while our purpose is static detection.

Problem and examples. In the rest of the paper, we focus on a simple XQuery extension with insertion and deletion operations. The syntax and semantics of that language is essentially that of [12], with updates applied immediately. This language is powerful enough to exhibit the main problems related to commutativity analysis, yet simple enough to allow a complete formal treatment within the space available for this paper. Here are some sample queries and updates in that language.

Q1
```
count($doc/country/new)
```

Q2
```
$doc/country[population > 20]
```

Q3
```
for $x in $doc//country
return ($x//name)
```

Q4
```
for $x in $doc/country
return $x/new/../very_new
```

U1
```
delete {$doc/wines/california}
```

U2
```
for $x in $doc/country return
  insert {<new/>} into {$x}
```

U3
```
for $x in
  $doc/country[population < 24]
return
  delete {$x/city}
```

Some of those examples obviously commute, for instance **U1** deletes nodes that are unrelated to the nodes accessed by **Q1** or **Q2**. This can be inferred easily by looking at the paths in the query used to access the corresponding nodes. On the contrary, **U2** does not commute with **Q1** since the query accesses nodes being inserted. Deciding whether the set of nodes accessed or modified are disjoint quickly becomes hard for any non-trivial update language. For instance, deciding whether **U3** and **Q2** interfere requires some analysis of the predicates, which can be arbitrarily complex in XQuery.

Approach. We rely on a form of abstract interpretation that approximates the set of nodes processed by a given expression. The analysis must satisfy the following properties. Firstly, since we are looking to check *disjointness*, we must infer an upper bound for the corresponding nodes. Secondly, the analysis must be precise enough to be useful in practical applications. Finally, the result of the analysis must make disjointness decidable. In the context of XML updates, *paths* are a natural choice for the approximation of the nodes being accessed or updated, and they satisfy the precision and decidability requirements.

Contributions. The path analysis itself is a relatively intuitive extension of [17] to handle update operations. However, coming up with a sound analysis turns out to be a hard problem for a number of reasons. First of all, we use paths to denote sets of accessed nodes, but the forthcoming updates will change the nodes denoted by the paths that are being accumulated. We need a way to associate a meaning to a path that is *stable* in the face of a changing data model instance. To address that issue, we introduce a store-based formalization of the XML data model and a notion of store history that allows us to talk about the effect of each single update and to solve the stability issue. Another challenge is to find a precise definition of which nodes are actually used or updated by a query. For instance, one may argue that **U3** only modifies nodes reached by the path *country/city*. However, one would then miss the fact that **U3** interferes with **Q3** because the *city* nodes may have a *country* or a *name* descendant, which is made unreachable by the deletion. In our analysis, this is kept into account by actually inserting into the updated paths of **U3** all the descendants of the deleted expression *country/city*, as detailed in the table below.

U3	**Q3**
accessed paths:	accessed paths:
`$doc/country`	`$doc//country`
`$doc/country/population`	`$doc//country//name`
`$doc/country/city`	
updated paths:	updated paths:
`$doc/country/city/descendant-or-self::*`	

Q4 is interesting as well. If the returned expression *\$x/new/../very_new* were just associated to the path *country/new/../very_new*, the interference with **U2** would not be observed, since the path *country/new/d.-o.-s.*::$*$ updated by **U2** refers to a disjoint set of nodes. Hence, the analysis must also consider the nodes traversed by the evaluation of *\$x/new/../very_new*, which correspond to the path *country*$|$*country/new*$|$*country/new/..*, whose second component intersects with *country/new/d.-o.-s.*::$*$.

The main contributions of the paper are:

– We propose a form of static analysis that infers paths to the nodes that are *accessed* and *modified* by an expression in that language;
– We present a formal definition of when such an analysis is sound, based on a notion of *store history equivalence*; this formal definition provides a guide for the definition of the inference rules;
– We show the soundness of the proposed path analysis;
– We prove a commutativity theorem, that provides a sufficient condition for the commutativity of two expressions, based on the given path analysis.

Organization. The rest of the paper is organized as follows. Section 2 presents the XML data model and the notion of store history. Section 3 reviews the update language syntax and semantics. Section 4 presents the path analysis and the main soundness theorem. Section 5 presents the commutativity theorem. Section 6 reviews related work, and Section 7 concludes the paper. For space reasons, proofs for the analysis soundness and for the commutativity theorem are provided separately in [13].

2 A Store for Updates

We define here the notions of *store* and *store history*, which are used to represent the effect of XML updating expressions. Our store is a simplification of the XQuery Data Model [11] to the parts that are most relevant to our path analysis.

2.1 The Store

We assume the existence of disjoint infinite sets of *node ids*, $\mathcal{N}$, the *node kinds*, $\mathcal{K} = \{\texttt{element}, \texttt{text}\}$, *names*, $\mathcal{Q}$, and possible *textual content*, $\mathcal{T}$. A node *location* is used to identify where a document or an XML fragment originates from; it is either a URI or a unique code-location identifier: *loc* ::= *uri* | *code-loc*.

A *uri* typically corresponds to the URI associated to a document and a *code-loc* is used to identify document fragments generated during query evaluation by an element constructor. Now we are ready to define our basic notion of store.

Definition 1 (Store). *A store* σ *is a quadruple* (N,E,R,F) *where* $N \subset \mathcal{N}$ *contains the set of nodes in the document,* $E \subset N \times N$ *contains the set of edges,* $R\colon N \to loc$ *is a partial function mapping some nodes to their location, and the node description* $F = (\texttt{kind}_F, \texttt{name}_F, \texttt{content}_F)$ *is a triple of partial functions where* $\texttt{kind}_F\colon N \to \mathcal{K}$ *maps each node to its kind,* $\texttt{name}_F\colon N \to \mathcal{Q}$ *maps nodes to their name (if any), and* $\texttt{content}_F\colon N \to \mathcal{T}$ *maps nodes to their text content (if any).*

We use N_σ*,* E_σ*,* R_σ*,* F_σ *to denote the* N,E,R,F *component of* σ*. When* $(m,n) \in E$*, we say that m is a parent of n and n is a child of m. A "root" is a node that has no parent.*

Finally a store must be "well-formed": (1) all nodes mapped by R must be root nodes, (2) every non-root node must be the child node of exactly one parent node, (3) the transitive closure E^+ *of E must be irreflexive (4) element nodes must have a name and no content; and (5) text nodes must have no name and no children but do have content.*

In what follows, every store operation preserves store well-formedness.

2.2 Accessing and updating the store

We assume the standard definitions for the usual accessors (parent, children, descendants, ancestors, name, text-content...), and focus on operations that modify the store (insert,delete, and node creation).[3] We define a notion of *atomic update record*, which captures the dynamic information necessary for each update, notably allowing the update to be re-executed on a store, using the *apply* operation defined below.

Definition 2 (Atomic update records). *Atomic update records are terms with the following syntax, where E is a set of pairs of nodes, and* $\bar{n}$ *and* $\bar{m}$ *are ordered sequences of nodes. In the* `create` *case, F is such that* $(\bar{n},(),(),F)$ *would be a well-formed store.*

$$\texttt{create}(\bar{n},F) \mid \texttt{R-insert}(n,loc) \mid \texttt{insert}(E) \mid \texttt{delete}(\bar{n})$$

Definition 3 (Atomic update application).

The operation apply(σ,u) *returns a new store as detailed below, but fails when the listed preconditions do not hold.*

– *apply*$(\sigma,\texttt{create}(\bar{n},F'))$ *adds* $\bar{n}$ *to N and extends F with* F'*.*
  Preconditions: $\bar{n}$ *disjoint from N.* $(\bar{n},(),(),F')$ *is a well-formed store.*
– *apply*$(\sigma,\texttt{R-insert}(n,loc))$ *extends R with* $n \to loc$*.*
  Preconditions: n is a root node and $R(n_c) = \bot$*.*

[3] Note that replace is trivial to add to the framework.

– *apply*$(\sigma, \texttt{insert}(E'))$ *extends* E *with* E'.
  Preconditions: for each $(n_p, n_c) \in E'$, n_c *has no parent in* $E \cup E' \setminus \{(n_p, n_c)\}$, *and* $R(n_c) = \perp$. *The transitive closure of* $E \cup E'$ *is irreflexive.*
– *apply*$(\sigma, \texttt{delete}(\bar{n}))$ *deletes each edge* $(n_p, n_c) \in E$ *where* $n_c \in \bar{n}$.
  Preconditions: $\bar{n} \subseteq N$.

Definition 4 (Composite updates). *A composite update,* Δ*, is an ordered sequence of atomic updates:* $\Delta \equiv (u_1, \ldots, u_n)$. *apply*$(\sigma, \Delta)$ *denotes the result of applying* $u_1 \ldots u_n$ *on store* σ*, in this order.*

We use *created*(Δ) to denote the set of nodes created by Δ. A composite update Δ *respects creation time* iff, however we split it as Δ_1, Δ_2, no node in *created*(Δ_2) appears in Δ_1. Hereafter we will always assume that we only work with such Δ's.

Finally, we need a notion of *updated*(Δ_1) that enjoys the following property, where $S \# T$ means that S and T are disjoint.

Property 1. If Δ_1, Δ_2 and Δ_2, Δ_1 both respect creation time, then

$$\mathit{updated}(\Delta_1) \# \mathit{updated}(\Delta_2) \;\Rightarrow\; \text{apply}(\sigma, (\Delta_1, \Delta_2)) = \text{apply}(\sigma, (\Delta_2, \Delta_1))$$

The following notion satisfies Property 1.

Definition 5 (Update target). *The* update target *of each update operation is defined as*

$$\begin{array}{ll}
\mathit{updated}(\texttt{create}(\bar{n}, F)) & =_{def} \{\} \\
\mathit{updated}(\texttt{R-insert}(n, loc)) & =_{def} \{\} \\
\mathit{updated}(\texttt{insert}(E)) & =_{def} \{n_c \mid (n_p, n_c) \in E\} \\
\mathit{updated}(\texttt{delete}(\bar{n})) & =_{def} \bar{n}
\end{array}$$

Intuitively, provided that creation time is respected, the only two operations that do not commute are $\texttt{insert}(n_p, n_c)$ and $\texttt{delete}(n_c)$. Any other two operations either do not interfere at all or they fail in whichever order are applied, as happens for any conflicting `R-insert`-`R-insert`, `R-insert`-`insert`, or `insert`-`insert` pair.

2.3 Store History

Finally, we introduce a notion of store history, as a pair $(\sigma, (u_1, \ldots, u_n))$. In our semantics each expression, instead of modifying its input store, extends the input history with new updates. With this tool we will be able, for example, to discuss commutativity of two expressions $Expr_1, Expr_2$ by analysing the histories $(\sigma, (\Delta_1, \Delta_2))$ and $(\sigma, (\Delta'_2, \Delta'_1))$ produced by their evaluations in different orders, and by proving that, under some conditions, $\Delta_1 = \Delta'_1$ and $\Delta_2 = \Delta'_2$.

Definition 6 (Store history). *A store history* $\eta = (\sigma_\eta, \Delta_\eta)$ *is a pair formed by a store and a composite update.*

A store history (σ, Δ) can be mapped to a plain store either by apply(σ, Δ) or by applying *no-delete*(Δ) only, which is the Δ without any deletion. The accessors are extended to store histories using the convention that, for any function defined on stores,

$f(\eta) =_{\text{def}} f(\text{apply}(\eta))$. The second mapping ($\text{mrg}((\sigma,\Delta))$) will be crucial to capture the degree of approximation that store dynamicity imposes over our static analysis.

$$\begin{aligned}\text{apply}((\sigma,\Delta)) &=_{\text{def}} \text{apply}(\sigma,\Delta)\\ \text{mrg}((\sigma,\Delta)) &=_{\text{def}} \text{apply}(\sigma, \textit{no-delete}(\Delta))\end{aligned}$$

By abuse of notation we shall (1) implicitly interpret σ as $(\sigma,())$; (2) extend accessors to store histories using the convention that, for any function defined on stores, $f(\eta) =_{\text{def}} f(\text{apply}(\eta))$; (3) when $\eta = (\sigma,\Delta)$ then write $\eta,\Delta' =_{\text{def}} (\sigma,(\Delta,\Delta'))$. We define history difference $\eta \setminus \eta'$ as follows: $(\sigma,(\Delta,\Delta')) \setminus (\sigma,\Delta) =_{\text{def}} \Delta'$.

Definition 7 (Well-formed History). *A history η is well-formed if mrg(η) is defined (which implies that apply$((\sigma,\Delta))$ is defined).*

3 Update language

The language we consider is a cut-down version of XQuery! [12] characterized by the fact that the evaluation order is fixed and each update operation is applied immediately. It is not difficult to extend our analysis to languages with snapshot semantics, but the machinery becomes heavier, while we are trying here to present the simplest incarnation of our approach. The language has the following syntax; we will use the usual abbreviations for the parent (**p**/..), child (**p**/*name*), and descendant (**p**//*name*) axes. We assume that *code-loc* (See Section 2) is generated beforehand by the compiler.

$$\begin{aligned}
\textit{Expr} ::=\ & \$x \mid \textit{Expr}/\textit{axis}::\textit{ntest} \mid \textit{Expr},\textit{Expr} \mid \textit{Expr} = \textit{Expr}\\
& \mid \texttt{let}\ \$x\ \texttt{:=}\ \textit{Expr}\ \texttt{return}\ \textit{Expr} \mid \texttt{for}\ \$x\ \texttt{in}\ \textit{Expr}\ \texttt{return}\ \textit{Expr}\\
& \mid \texttt{if (}\textit{Expr}\texttt{) then}\ \textit{Expr}\ \texttt{else}\ \textit{Expr} \mid \texttt{delete \{}\textit{Expr}\texttt{\}}\\
& \mid \texttt{insert \{}\textit{Expr}_1\texttt{\} into \{}\textit{Expr}\texttt{\}} \mid \texttt{element}_{\textit{code-loc}}\texttt{\{}\textit{Expr}\texttt{\}\{}\textit{Expr}\texttt{\}}\\
\textit{axis} ::=\ & \textit{child} \mid \textit{descendant} \mid \textit{parent} \mid \textit{ancestor}\\
\textit{ntest} ::=\ & \textit{text()} \mid \textit{node()} \mid \textit{name} \mid *
\end{aligned}$$

The main semantic judgement "$\textit{dEnv} \vdash \eta_0; \textit{Expr} \Rightarrow \eta_1; \bar{n}$" specifies that the evaluation of an expression *Expr*, with respect to a store history η_0 and to a dynamic environment *dEnv* that associates a value to each variable free in *Expr*, produces a value $\bar{n}$ and extends η_0 to $\eta_1 = \eta_0,\Delta$. A value is just a node sequence $\bar{n}$; textual content may be accessed by a function f, but we otherwise ignore atomic values, since they are ignored by path analysis. In an implementation, we would not manipulate the history η_0 but the store apply(η_0), since the value of every expression only depends on that. However, store histories allow us to isolate the store effect of each single expression, both in our definition of soundness and in our proof of commutativity.

As an example, we present here the rule for insert expressions; the complete semantics can be found in [13]. Let $\bar{n}_d$ be the descendants-or-self of the nodes in $\bar{n}$. Insert-into uses *prepare-deep-copy* to identify a fresh node $m_i \in \bar{m}_d$ for each node in $\bar{n}_d$, while E_{copy} and F_{copy} reproduce for $E_{\text{apply}(\eta_2)}$ and $F_{\text{apply}(\eta_2)}$ for $\bar{m}_d$, and $\bar{m}$ is the subset of $\bar{m}_d$ that corresponds to $\bar{n}$. Hence, $\texttt{create}(\bar{m}_d, F_{\text{copy}}), \texttt{insert}(E_{\text{copy}})$ copy $\bar{n}$ and their descendants, while $\texttt{insert}(\{n\} \times \bar{m})$ links the copies of $\bar{n}$ to n. Notice how the rule only depends on apply(η_2), not on the internal structure of η_2.

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr_1 \Rightarrow \eta_1; \bar{n} \\ dEnv \vdash \eta_1; Expr_2 \Rightarrow \eta_2; n \\ (\bar{m}, \bar{m}_d, E_{\text{copy}}, F_{\text{copy}}) = \textit{prepare-deep-copy}(\text{apply}(\eta_2), \bar{n}) \\ \eta_3 = \eta_2, \texttt{create}(\bar{m}_d, F_{\text{copy}}), \texttt{insert}(E_{\text{copy}}), \texttt{insert}(\{n\} \times \bar{m}) \end{array}}{dEnv \vdash \eta_0; \texttt{insert \{}Expr_1\texttt{\} into \{}Expr_2\texttt{\}} \Rightarrow \eta_3; ()}$$

It is easy to prove that, whenever $dEnv \vdash \eta_0; Expr \Rightarrow \eta_1; \bar{n}$ holds and η_0 is well formed, then η_1 is well-formed as well.

4 Path analysis

In this section, we introduce the path analysis judgment and the inference rules that compute it.

4.1 Paths and prefixes

We now define the notion of paths that is used in our static analysis. Observe that the paths used by the analysis are not the same as the paths in the target language. For example, they are rooted in a different way, and the steps need not coincide: if we added order to the store, we could add a following-sibling step to the language, but approximate it with *parent::∗/child::* in the analysis.

Definition 8 (Static paths). Static paths*, or simply* paths*, are defined as follows.*

$$\mathbf{p} ::= () \mid loc \mid \mathbf{p}_0|\mathbf{p}_1 \mid \mathbf{p}/axis::ntest$$

Note that paths are always rooted at a given location. In addition, the particular fragment chosen here is such that important operations, notably intersection, can be checked using known algorithms [3, 18].

Definition 9 (Path Semantics). *For a path* $\mathbf{p}$ *and store* σ, $[\![\mathbf{p}]\!]_\sigma$ *denotes the set of nodes selected from the store by the path with the standard semantics [20] except that order is ignored, and* R_σ *is used to interpret the locations loc. The following concepts are derived from the standard semantics:*

Inclusion. *A path* $\mathbf{p}_1$ *is included in* $\mathbf{p}_2$*, denoted* $\mathbf{p}_1 \subseteq \mathbf{p}_2$*, iff* $\forall\sigma\colon [\![\mathbf{p}_1]\!]_\sigma \subseteq [\![\mathbf{p}_2]\!]_\sigma$.

Disjointness. *Two paths* $\mathbf{p}_1, \mathbf{p}_2$ *are disjoint, denoted* $\mathbf{p}_1 \# \mathbf{p}_2$*, iff* $\forall\sigma\colon [\![\mathbf{p}_1]\!]_\sigma \cap [\![\mathbf{p}_2]\!]_\sigma = \emptyset$.

Prefixes. *For each path* $\mathbf{a}$ *we define* $pref(\mathbf{a})$ *as follows.*

$\mathbf{a}$	loc	$\mathbf{p}/axis::ntest$	$\mathbf{p}\|\mathbf{q}$
$pref(\mathbf{a})$	$\{loc\}$	$\{\mathbf{p}/axis::ntest\} \cup pref(\mathbf{p})$	$\{\mathbf{p}\|\mathbf{q}\} \cup pref(\mathbf{p}) \cup pref(\mathbf{q})$

Prefix Closure. *For a path* $\mathbf{a}$ *we write* $prefclosed(\mathbf{a})$ *iff* $\forall\mathbf{p}\colon \mathbf{p} \in pref(\mathbf{a}) \Rightarrow \mathbf{p} \subseteq \mathbf{a}$.

The *prefixes* of a path are all its initial subpaths, and a path is prefix-closed when it includes all of its prefixes. For example, the paths $/a//b \,|\, /a \,|\, /a//b/c$ and $/\!* \,|\, /a/b$ are both prefix-closed (the latter because $/a \subseteq /\!*$).

4.2 The meaning of the analysis

Definition 10 (Path analysis). *Given an expression Expr and a path environment* **pEnv** *which is a mapping from variables to paths, our path-analysis judgment*

$$\mathbf{pEnv} \vdash \mathit{Expr} \Rightarrow \mathbf{r};\ \langle \mathbf{a}, \mathbf{u} \rangle$$

associates three paths to the expression: **r** *is an upper approximation of the nodes that are returned by the evaluation of Expr,* **a** *of those that are accessed, and* **u** *of those that are updated.*

There are many reasonable ways to interpret which nodes are "returned" and "accessed" by an expression. For example, a path $\$x//a$ only returns the $\$x$ descendants with an a name but, in a naive implementation, may access every descendant of $\$x$. Deciding what is "updated" is even trickier. This definition should be as natural as possible, should allow for an easy computation of a static approximation and, above all, should satisfy the following property: if what is accessed by Expr_1 is disjoint from what is accessed or updated by Expr_2, and vice-versa, then the two expressions commute.

In the following paragraphs we present our interpretation, which will guide the definition of the inference rules and is one of the basic technical contributions of this work.

The meaning of **r** seems the easiest to describe: an analysis is sound if $\mathbf{pEnv} \vdash \mathit{Expr} \Rightarrow \mathbf{r};\ \langle \mathbf{a}, \mathbf{u} \rangle$ and $\mathit{dEnv} \vdash \eta_0; \mathit{Expr} \Rightarrow \eta_1; \bar{n}$ imply that $\bar{n} \subseteq [\![\mathbf{r}]\!]_{\mathrm{apply}(\eta_1)}$. Unfortunately, this is simplistic. Consider the following example:

```
let $x := doc('u1')/a return let $y := $x return (delete($y), $x/b)
```

Our rules bind a path $\mathrm{u1}/a$ to $\$x$, and finally deduce a returned path $\mathrm{u1}/a/b$ for the expression above. However, after *delete($y)*, the value of $\$x/b$ is not in $[\![\mathbf{p}]\!]_{\mathrm{apply}(\eta)}$ anymore; the best we can say it is that it is still in $[\![\mathbf{p}]\!]_{\mathrm{mrg}(\eta)}$. This is just an instance of a general "stability" problem: we infer something about a specific store history, but we need the same property to hold for the store in some future. We solve this problem by accepting that our analysis only satisfies $\bar{n} \subseteq [\![\mathbf{r}]\!]_{\mathrm{mrg}(\eta_1)}$, which is weaker than $\bar{n} \subseteq [\![\mathbf{r}]\!]_{\mathrm{apply}(\eta_1)}$ but is stable; we also generalize the notion to environments.

Definition 11 (Approximation). *A path* **p** *approximates a value* $\bar{n}$ *in the store history* η*, denoted* $\mathbf{p} \supseteq_\eta \bar{n}$*, iff* $\bar{n} \subseteq [\![\mathbf{p}]\!]_{\mathit{mrg}(\eta)}$.

A path environment **pEnv** *approximates a dynamic environment dEnv in a store history* η*, denoted* $\mathbf{pEnv} \supseteq_\eta \mathit{dEnv}$*, iff*

$$(\$x \mapsto \bar{n}) \in \mathit{dEnv} \ \Rightarrow\ \exists \mathbf{b}.\ (\$x \mapsto \mathbf{b}) \in \mathbf{pEnv} \ \mathit{and}\ \mathbf{b} \supseteq_\eta \bar{n}$$

Thanks to this "merge" interpretation, a path denotes all nodes that are reached by that path, or were reached by the path in some past version of the current history. This approximation is quite harmless, because the merge interpretation of a history is still a well-formed store, where every node has just one parent and one name, hence the usual algorithms can be applied to decide path disjointness.

The approach would break if we had, for example, the possibility of moving a node from one parent to another. Formally, $\mathrm{mrg}(\eta)$ may now contain nodes with two parents.

In practice, one could not deduce, for example, that $(a/d)\#(b/c/d)$, because $\$x/a/d$ and $\$x/b/c/d$, if evaluated at different times, may actually return the same node, because its parent was moved from $\$x/a$ to $\$x/b/c$ in the meanwhile. Similarly, if nodes could be renamed, then node names would become useless in the process of checking path disjointness.

The commutativity theorem in Section 5 is based on the following idea: assume that $Expr_1$ transforms η_0 into (η_0,Δ) and only modifies nodes reachable through a path $\mathbf{u}$, while $Expr_2$ only depends on nodes reachable through $\mathbf{a}$, such that $\mathbf{u}\#\mathbf{a}$. Because $Expr_1$ only modifies nodes in $\mathbf{u}$, the histories η_0 and (η_0,Δ) are "the same" with respect to $\mathbf{a}$, hence we may evaluate $Expr_2$ either before or after $Expr_1$.

This is formalized by defining a notion of history equivalence wrt a path $\eta \sim_{\mathbf{p}} \eta'$, and by proving that the inferred $\mathbf{a}$ and $\mathbf{u}$ and the evaluation relation are related by the following soundness properties.

Parallel evolution from a-equivalent stores, first version:
$\eta'_0 \sim_{\mathbf{a}} \eta_0$ and $dEnv \vdash \eta_0; Expr \Rightarrow (\eta_0,\Delta); \overline{n}$
imply $dEnv \vdash \eta'_0; Expr \Rightarrow (\eta'_0,\Delta); \overline{n}$, i.e. the same $\overline{n}$ and Δ are produced.

Immutability out of u, first version:
$\forall \mathbf{c}\colon \mathbf{c}\#\mathbf{u}$ and $dEnv \vdash \eta_0; Expr \Rightarrow (\eta_0,\Delta); \overline{n}$
imply $\eta_0 \sim_{\mathbf{c}} (\eta_0,\Delta)$.

To define the right notion of path equivalence, consider the Comma rule

$$\frac{\begin{array}{c}\mathbf{pEnv} \vdash Expr_1 \Rightarrow \mathbf{r}_1;\ \langle \mathbf{a}_1, \mathbf{u}_1\rangle \\ \mathbf{pEnv} \vdash Expr_2 \Rightarrow \mathbf{r}_2;\ \langle \mathbf{a}_2, \mathbf{u}_2\rangle\end{array}}{\mathbf{pEnv} \vdash Expr_1, Expr_2 \Rightarrow \mathbf{r}_1|\mathbf{r}_2;\ \langle \mathbf{a}_1|\mathbf{a}_2, \mathbf{u}_1|\mathbf{u}_2\rangle} \quad (\text{COMMA})$$

The rule says that if $\eta'_0 \sim_{\mathbf{a}_1|\mathbf{a}_2} \eta_0$ then the evaluation of $Expr_1, Expr_2$ gives the same result in both η_0 and η'_0. Our equivalence over $\mathbf{p}$ will be defined as "$\forall \mathbf{p}' \in \text{pref}(\mathbf{p}). P(\mathbf{p}')$", so that $\eta'_0 \sim_{\mathbf{a}_1|\mathbf{a}_2} \eta_0$ implies $\eta'_0 \sim_{\mathbf{a}_1} \eta_0$ and $\eta'_0 \sim_{\mathbf{a}_2} \eta_0$. Hence, by induction, if we start the evaluation of $Expr_1, Expr_2$ from $\eta_0 \sim_{\mathbf{a}_1|\mathbf{a}_2} \eta'_0$, then $Expr_2$ will be evaluated against (η_0,Δ) and (η'_0,Δ), but we have still to prove that $\eta_0 \sim_{\mathbf{a}_2} \eta'_0$ implies $(\eta_0,\Delta) \sim_{\mathbf{a}_2} (\eta'_0,\Delta)$. This is another instance of the "stability" problem. In this case, the simplest solution is the adoption of the following notion of path equivalence: two histories η_1 and η_2 are equivalent modulo a path $\mathbf{p}$, denoted $\eta_1 \sim_{\mathbf{p}} \eta_2$, iff:

$$\forall \mathbf{p}' \in \text{pref}(\mathbf{p}).\ \forall \Delta.\ \ [\![\mathbf{p}']\!]_{\text{apply}(\eta_1,\Delta)} = [\![\mathbf{p}']\!]_{\text{apply}(\eta_2,\Delta)}$$

The quantification on Δ makes this notion "stable" with respect to store evolution, which is extremely useful for our proofs, but the equality above actually implies that:

$$\forall \Delta.\ (wf(\eta_1,\Delta) \Rightarrow wf(\eta_2,\Delta)) \wedge (\forall \Delta.\ wf(\eta_2,\Delta) \Rightarrow wf(\eta_1,\Delta))$$

This is too strong, because, whenever two stores differ in one node, the Δ that creates the node can only be added to the store that is missing it. Similarly, it they differ in one edge, the Δ that inserts the edge can only be added to the store that is missing it. Hence, only identical stores can be extended with exactly the same set of Δ's.

So, we have to weaken the requirement. We first restrict the quantification to updates that only create nodes that are fresh in both stores. Moreover, we do not require that $wf(\eta_1,\Delta) \Rightarrow wf(\eta_2,\Delta)$, but only that, for every n of interest, a subset of Δ' of Δ exists which can be used to extend η_1 and η_2 so to have n in both. The resulting notion of equivalence is preserved by every update in the language whose path does not intersect pref($\mathbf{p}$); this notion is strong enough for our purposes ($\Delta' \subseteq \Delta$ denotes the inclusion of the inserted edges).

Definition 12 (Store equivalence modulo a path). *Two histories* σ_1 *and* σ_2 *are equivalent modulo a path* $\mathbf{p}$*, denoted* $\sigma_1 \sim_{\mathbf{p}} \sigma_2$*, iff:*

$$\begin{aligned}
&\forall \mathbf{p}' \in \mathit{pref}(\mathbf{p}).\ \forall\Delta.\ \mathit{created}(\Delta)\#(N_{\sigma_1} \cup N_{\sigma_2}) \ \wedge\ n \in [\![\mathbf{p}']\!]_{\mathit{apply}(\sigma_1,\Delta)} \\
&\qquad\qquad \Rightarrow\ \exists\Delta' \subseteq \Delta.\ n \in [\![\mathbf{p}']\!]_{\mathit{apply}(\sigma_1,\Delta')} \ \wedge\ n \in [\![\mathbf{p}']\!]_{\mathit{apply}(\sigma_2,\Delta')} \\
&\forall \mathbf{p}' \in \mathit{pref}(\mathbf{p}).\ \forall\Delta.\ \mathit{created}(\Delta)\#(N_{\sigma_1} \cup N_{\sigma_2}) \ \wedge\ n \in [\![\mathbf{p}']\!]_{\mathit{apply}(\sigma_2,\Delta)} \\
&\qquad\qquad \Rightarrow\ \exists\Delta' \subseteq \Delta.\ n \in [\![\mathbf{p}']\!]_{\mathit{apply}(\sigma_1,\Delta')} \ \wedge\ n \in [\![\mathbf{p}']\!]_{\mathit{apply}(\sigma_2,\Delta')}
\end{aligned}$$

Definition 13 (Store history equivalence modulo a path).

$$\eta_1 \sim_{\mathbf{p}} \eta_2 \ \Leftrightarrow_{def}\ \mathit{apply}(\eta_1) \sim_{\mathbf{p}} \mathit{apply}(\eta_2)$$

Since $[\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_1,\Delta)}$ is monotone wrt Δ, the above definition implies that:

$$\eta_1 \sim_{\mathbf{p}} \eta_2 \ \Rightarrow\ (\forall\Delta.\ wf(\eta_1,\Delta) \ \wedge\ wf(\eta_2,\Delta) \ \Rightarrow\ [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_1,\Delta)} = [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\Delta)})$$

We are now ready for the formal definition of soundness.

Definition 14 (Soundness). *The static analysis* $\mathbf{pEnv} \vdash \mathit{Expr} \Rightarrow \mathbf{r};\ \langle \mathbf{a},\mathbf{u} \rangle$ *is* sound *for the semantic evaluation* $\mathit{dEnv} \vdash \eta_0;\mathit{Expr} \Rightarrow \eta_1;\overline{n}$ *iff for any well-formed* η_0*,* η_1*,* dEnv*,* $\mathbf{pEnv}$*,* Expr*,* $\overline{n}$*,* $\mathbf{r}$*,* $\mathbf{a}$*,* $\mathbf{u}$*, such that:*

$$\begin{aligned}
&\mathbf{pEnv} \vdash \mathit{Expr} \Rightarrow \mathbf{r};\ \langle \mathbf{a},\mathbf{u} \rangle \\
&\mathit{dEnv} \vdash \eta_0;\mathit{Expr} \Rightarrow (\eta_0,\Delta);\overline{n} \\
&\mathbf{pEnv} \supseteq_{\eta_0} \mathit{dEnv}
\end{aligned}$$

the following properties hold.

Approximation by r: $\mathbf{r}$ *is an approximation of the result:* $\mathbf{r} \supseteq_{\eta_1} \overline{n}$

Parallel evolution from a-equivalent stores: *For any alternative initial store history* η_0'*, if* $\eta_0' \sim_{\mathbf{a}} \eta_0$ *and* $N_{\eta_0'}\#\mathit{created}(\Delta)$*, then* $\mathit{dEnv} \vdash \eta_0';\mathit{Expr} \Rightarrow (\eta_0',\Delta);\overline{n}$

Immutability out of u: (1) $\mathbf{u} \supseteq_{\eta_1} \mathit{updated}(\Delta)$
(2) $\forall \mathit{prefclosed}(\mathbf{c}):\ \mathbf{c}\#\mathbf{u} \ \Rightarrow\ \eta_0 \sim_{\mathbf{c}} (\eta_0,\Delta)$.

In the *Parallel evolution* property, the condition $N_{\eta_0'}\#\mathit{created}(\Delta)$ is needed because, if η_0' did already contain some of the nodes that are added by Δ, then it would be impossible to extend η_0' with Δ. This condition is not restrictive, and is needed because we identify nodes in different stores by the fact that they have the same identity. We could relate different store using a node morphism, rather that node identity, but that would make the proofs much heavier.

Immutability has two halves. The first, $\mathbf{u} \supseteq_{\eta_1} \mathit{updated}(\Delta)$, confines the set of edges that are updated to those that are in $\mathbf{u}$, and is important to prove that two updates commute if $\mathbf{u}_1\#\mathbf{u}_2$. The second half specifies that, for every $\mathbf{c}\#\mathbf{u}$, the store after the update is $\mathbf{c}$-equivalent to the store before. Together with *Parallel evolution*, it essentially says that after *Expr* is evaluated, the value returned by any expression Expr_1 that only accesses $\mathbf{c}$ is the same value returned by Expr_1 before *Expr* was evaluated, and is important to prove that an update and a query commute if $\mathbf{a}_1\#\mathbf{u}_2$. The path $\mathbf{c}$ must be prefix-closed for this property to hold. For example, according to our rules, $delete(/a/b)$ updates a path $\mathbf{u} = /a/b/dos::*$. It is disjoint from $\mathbf{c} = /a/b/..$, but still the value of $/a/b/..$ changes after $delete(/a/b)$. This apparent unsoundness arises because $\mathbf{c}$ is not prefix-closed. If we consider the prefix-closure $\mathbf{a} = /a|/a/b|/a/b/..$ of $/a/b/..$, we notice that $\mathbf{a}$ is *not* disjoint from $\mathbf{u}$.

4.3 Path analysis rules

We present the rules in two groups: selection and update rules.

Selection rules. These rules regard the querying fragment of our language. We extend the rules from [17] for the proper handling of updated paths.

The (Comma) rule has been presented above.

The (Var) rule specifies that variable access does not access the store. One may wonder whether $\mathbf{r}$ should not be regarded as "accessed" by the evaluation of $\$x$. The doubt is easily solved by referring to the definition of soundness: the value of $\$x$ is the same in two stores η_0 and η_0' independently of any equivalence among them, hence the accessed path should be empty. This rule also implicitly specifies that variable access commutes with any other expression. For example, *\$x,delete(\$x)* is equivalent to *delete(\$x),\$x*.

$$\frac{(\$x \mapsto \mathbf{r}) \in \mathbf{pEnv}}{\mathbf{pEnv} \vdash \$x \Rightarrow \mathbf{r};\ \langle (), () \rangle} \qquad \text{(VAR)}$$

The (Step) rule specifies that a step accesses the prefix closure of $\mathbf{r}$. Technically, the rule would still be sound if we only put $\mathbf{r}|(\mathbf{r}/\mathit{axis}::\mathit{ntest})$ in the accessed set. However, the commutativity theorem relies on the fact that, for any expression, its inferred accessed path is prefix-closed, for the reasons discussed at the end of the previous section, and the addition of the prefix closure of $\mathbf{r}$ does not seem to seriously affect the analysis precision.

$$\frac{\mathbf{pEnv} \vdash \mathit{Expr} \Rightarrow \mathbf{r};\ \langle \mathbf{a}, \mathbf{u} \rangle}{\mathbf{pEnv} \vdash \mathit{Expr}/\mathit{axis}::\mathit{ntest} \Rightarrow \mathbf{r}/\mathit{axis}::\mathit{ntest};\ \langle \mathrm{pref}(\mathbf{r}/\mathit{axis}::\mathit{ntest})|\mathbf{a}, \mathbf{u} \rangle} \qquad \text{(STEP)}$$

Iteration binds the variable and analyses the body once. Observe that the analysis ignores the order and multiplicity of nodes.

$$\frac{\begin{array}{c}\mathbf{pEnv} \vdash \mathit{Expr}_1 \Rightarrow \mathbf{r}_1;\, \langle \mathbf{a}_1, \mathbf{u}_1 \rangle \\ (\mathbf{pEnv} + \$x \mapsto \mathbf{r}_1) \vdash \mathit{Expr}_2 \Rightarrow \mathbf{r}_2;\, \langle \mathbf{a}_2, \mathbf{u}_2 \rangle\end{array}}{\begin{array}{c}\mathbf{pEnv} \vdash \texttt{for } \$x \texttt{ in } \mathit{Expr}_1 \texttt{ return } \mathit{Expr}_2 \\ \Rightarrow \mathbf{r}_2;\, \langle \mathbf{a}_1 | \mathbf{a}_2, \mathbf{u}_1 | \mathbf{u}_2 \rangle\end{array}} \quad (\textsc{For})$$

Element construction returns the unique constructor location, but there is no need to regard that location as accessed.

$$\frac{\begin{array}{c}\mathbf{pEnv} \vdash \mathit{Expr}_1 \Rightarrow \mathbf{r}_1;\, \langle \mathbf{a}_1, \mathbf{u}_1 \rangle \\ \mathbf{pEnv} \vdash \mathit{Expr}_2 \Rightarrow \mathbf{r}_2;\, \langle \mathbf{a}_2, \mathbf{u}_2 \rangle\end{array}}{\begin{array}{c}\mathbf{pEnv} \vdash \texttt{element}_{\mathit{code\text{-}loc}} \{\mathit{Expr}_1\}\{\mathit{Expr}_2\} \\ \Rightarrow \mathit{code\text{-}loc};\, \langle \mathbf{a}_1 | \mathbf{a}_2, \mathbf{u}_1 | \mathbf{u}_2 \rangle\end{array}} \quad (\textsc{Elt})$$

Local bindings just returns the result of evaluating the body, but the accesses and side effects of both subexpressions are both considered.

$$\frac{\begin{array}{c}\mathbf{pEnv} \vdash \mathit{Expr}_1 \Rightarrow \mathbf{r}_1;\, \langle \mathbf{a}_1, \mathbf{u}_1 \rangle \\ (\mathbf{pEnv} + \$x \mapsto \mathbf{r}_1) \vdash \mathit{Expr}_2 \Rightarrow \mathbf{r}_2;\, \langle \mathbf{a}_2, \mathbf{u}_2 \rangle\end{array}}{\mathbf{pEnv} \vdash \texttt{let } \$x \texttt{ := } \mathit{Expr}_1 \texttt{ return } \mathit{Expr}_2 \Rightarrow \mathbf{r}_2;\, \langle \mathbf{a}_1 | \mathbf{a}_2, \mathbf{u}_1 | \mathbf{u}_2 \rangle} \quad (\textsc{Let})$$

The conditional approximates the paths by merging the results of both branches.

$$\frac{\begin{array}{c}\mathbf{pEnv} \vdash \mathit{Expr} \Rightarrow \mathbf{r}_0;\, \langle \mathbf{a}_1, \mathbf{u}_1 \rangle \\ \mathbf{pEnv} \vdash \mathit{Expr}_1 \Rightarrow \mathbf{r}_1;\, \langle \mathbf{a}_2, \mathbf{u}_2 \rangle \\ \mathbf{pEnv} \vdash \mathit{Expr}_2 \Rightarrow \mathbf{r}_2;\, \langle \mathbf{a}_3, \mathbf{u}_3 \rangle\end{array}}{\begin{array}{c}\mathbf{pEnv} \vdash \texttt{if } (\mathit{Expr}) \texttt{ then } \mathit{Expr}_1 \texttt{ else } \mathit{Expr}_2 \\ \Rightarrow \mathbf{r}_1 | \mathbf{r}_2;\, \langle \mathbf{a}_1 | \mathbf{a}_2 | \mathbf{a}_3, \mathbf{u}_1 | \mathbf{u}_2 | \mathbf{u}_3 \rangle\end{array}} \quad (\textsc{If})$$

Equality returns nothing but accumulate accesses and side effects.

$$\frac{\begin{array}{c}\mathbf{pEnv} \vdash \mathit{Expr}_1 \Rightarrow \mathbf{r}_1;\, \langle \mathbf{a}_1, \mathbf{u}_1 \rangle \\ \mathbf{pEnv} \vdash \mathit{Expr}_2 \Rightarrow \mathbf{r}_2;\, \langle \mathbf{a}_2, \mathbf{u}_2 \rangle\end{array}}{\mathbf{pEnv} \vdash \mathit{Expr}_1 = \mathit{Expr}_2 \Rightarrow ();\, \langle \mathbf{a}_1 | \mathbf{a}_2, \mathbf{u}_1 | \mathbf{u}_2 \rangle} \quad (\textsc{Eq})$$

Update rules. The second set of rules deals with update expressions.

The first rule is the one for delete. The "updated path" **u** is extended with all the descendants of **r** because **u** approximates those paths whose semantics may change after the expression is evaluated, and the semantics of each path in $\mathbf{r}/\mathit{dos}::*$ is affected by the deletion. Assume, for example, that $(\$x \mapsto \mathit{loc}) \in \mathbf{pEnv}$, $(\$x \mapsto n) \in \mathit{dEnv}$, and n is the root of a tree of the form $\langle a \rangle \langle b \rangle \langle c/ \rangle \langle b/ \rangle \langle a/ \rangle$. The evaluation of `delete` $\{\$x/b\}$ would change the semantics of $\$x//c$, although this path does not explicitly traverse loc/b. This is correctly dealt with, since the presence of $\mathit{loc}/b/\mathit{dos}::*$ in **u** means: every path that is not disjoint from $\mathit{loc}/b/\mathit{dos}::*$ may be affected by this operation, and, by Definition 9, $\mathit{loc}//c$ is *not* disjoint from $\mathit{loc}/b/\mathit{dos}::*$.

Observe that `delete` $\{\$x/b\}$ also affects expressions that do not end below $\$x/b$, such as "$\$x/b/..$". This is not a problem either, since the accessed path **a** computed for the expression $\$x/b/..$ is actually $loc|(loc/b)|(loc/b/..)$, and the second component is not disjoint from $loc/b/dos::*$.

$$\frac{\mathbf{pEnv} \vdash Expr \Rightarrow \mathbf{r};\ \langle \mathbf{a}, \mathbf{u} \rangle}{\mathbf{pEnv} \vdash \texttt{delete}\ \{Expr\} \Rightarrow ();\ \langle \mathbf{a}, \mathbf{u}|(\mathbf{r}/dos::*)\rangle} \qquad (\text{DELETE})$$

Similarly, `insert {`$Expr_1$`} into {`$Expr_2$`}` may modify every path that ends with descendants of $Expr_2$. Moreover, it depends on all the descendants of $Expr_1$, since it copies all of them.

$$\frac{\begin{array}{c}\mathbf{pEnv} \vdash Expr_1 \Rightarrow \mathbf{r}_1;\ \langle \mathbf{a}_1, \mathbf{u}_1 \rangle \\ \mathbf{pEnv} \vdash Expr_2 \Rightarrow \mathbf{r}_2;\ \langle \mathbf{a}_2, \mathbf{u}_2 \rangle\end{array}}{\begin{array}{c}\mathbf{pEnv} \vdash \texttt{insert}\ \{Expr_1\}\ \texttt{into}\ \{Expr_2\} \\ \Rightarrow ();\ \langle \mathbf{a}_1|\mathbf{a}_2|(\mathbf{r}_1/dos::*), \mathbf{u}_1|\mathbf{u}_2|(\mathbf{r}_2//*)\rangle\end{array}} \qquad (\text{INSERTCHILD})$$

4.4 Soundness Theorem

Theorem 1 (Soundness of the analysis). *The static analysis rules presented in Section 4.3 are sound.*

Soundness is proved by induction, showing that the soundness properties are preserved by each rule. A detailed presentation of the soundness proof for the most important rules can be found in Appendix B.

5 Commutativity Theorem

Our analysis is meant as a tool to prove for specific expressions whether they can be evaluated on a given store in any order or, put differently, whether they *commute*.

Definition 15 (Commutativity). *We shall use* $[\![Expr]\!]^{dEnv}_{\eta}$ *as a shorthand for the pair* $(apply(\eta'), bag\text{-}of(\overline{n}))$ *such that* $dEnv \vdash \eta; Expr \Rightarrow \eta'; \overline{n}$*, and where* $bag\text{-}of(\overline{n})$ *forgets the order of the nodes in* $\overline{n}$*.*

Two expressions $Expr_1$ *and* $Expr_2$ commute *in* **pEnv***, written* $Expr_1 \overset{\mathbf{pEnv}}{\longleftrightarrow} Expr_2$*, iff, for all* η *and* $dEnv$ *such that* $\mathbf{pEnv} \supseteq_{\eta} dEnv$*, the following equality holds:*

$$[\![Expr_1, Expr_2]\!]^{dEnv}_{\eta} = [\![Expr_2, Expr_1]\!]^{dEnv}_{\eta}$$

Hence, $Expr_1 \overset{\mathbf{pEnv}}{\longleftrightarrow} Expr_2$ means that the order of evaluation of $Expr_1$ and $Expr_2$ only affects the order of the result.

Theorem 2 (Commutativity). *Consider two expressions and their analyses in* **pEnv***:*

$$\mathbf{pEnv} \vdash Expr_1 \Rightarrow \mathbf{r}_1;\ \langle \mathbf{a}_1, \mathbf{u}_1 \rangle$$
$$\mathbf{pEnv} \vdash Expr_2 \Rightarrow \mathbf{r}_2;\ \langle \mathbf{a}_2, \mathbf{u}_2 \rangle$$

If the updates and accesses obtained by the analysis are independent then the expressions commute, in any environment that respects **pEnv***:*

$$\mathbf{u}_1 \# \mathbf{a}_2, \mathbf{a}_1 \# \mathbf{u}_2, \mathbf{u}_1 \# \mathbf{u}_2 \Rightarrow Expr_1 \overset{\mathbf{pEnv}}{\longleftrightarrow} Expr_2$$

Commutativity is our main result. The proof can be found in Appendix C. It follows the pattern sketched in Section 4, after Definition 11. The proof is far easier than the proof of soundness, and is essentially independent on the actual definition of the equivalence relation. It only relies on soundness plus the following five properties, where only *Stability* is non-trivial.

$$\mathbf{p} \supseteq_{\eta_0} \overline{n} \;\Rightarrow\; \mathbf{p} \supseteq_{\eta_0,\Delta} \overline{n} \qquad \text{(Stability)}$$

$$\text{for each } \mathbf{p},\ \sim_{\mathbf{p}} \text{ is an equivalence relation} \qquad \text{(Equivalence)}$$

$$\mathbf{p}\#(\mathbf{q}_0|\mathbf{q}_1) \;\Leftrightarrow\; \mathbf{p}\#\mathbf{q}_0 \wedge \mathbf{p}\#\mathbf{q}_1 \qquad (|\#)$$

$$\eta_0 \sim_{(\mathbf{q}_0|\mathbf{q}_1)} \eta_1 \;\Rightarrow\; \eta_0 \sim_{\mathbf{q}_0} \eta_1 \qquad (|\sim)$$

$$\mathbf{q}_0 \subseteq \mathbf{q}_0|\mathbf{q}_1 \qquad (|\subseteq)$$

6 Related work

Numerous update languages have been proposed in the last few years [7, 15, 19, 1, 12]. Some of the most recent proposals [12, 6] are very expressive, as they provide the ability to observe the effect of updates during query evaluation. Although [6] limits the locations where updates occur, this has little impact on our static analysis which also works for a language where updates can occur anywhere in the query such as [12]. Very little work has been done so far on optimization or static analysis for such XML update languages, a significant exception being the work by Benedikt et al [1, 2]. However, they focus on analysis techniques for a language based on snapshot semantics, while we consider a much more expressive language. A notion of path analysis was proposed in [17], which we extend here by considering side effects.

Independence between updates and queries has been studied in the relational context [10, 16]. The problem becomes more difficult in the XML context because of the expressivity of existing XML query languages. In the relational case, the focus has been on trying to identify fragments of datalog for which the problem is decidable, usually by reducing the problem to deciding reachability. Instead, we propose a conservative approach using a technique based on paths analysis which works for arbitrary XML updates and queries. Finally, commutativity properties for tree operations are important in the context of transactions for tree models [9, 14], but these papers rely on dynamic knowledge while we are interested in static commutativity properties, hence the technical tools involved are quite different.

7 Conclusion

In this paper, we have proposed a conservative approach to detect whether two expressions commute in an expressive XML update language with strict evaluation order and immediate update application. The approach relies on a form of path analysis which computes an upper bound for the nodes accessed or updated in an expression. As there is a growing need to extend XML languages with imperative features [6, 12, 8], we believe the kind of analysis we propose here will be essential for the long-term development of those languages. We are currently exploring the use of our commutativity analysis for the purpose of algebraic optimization of XML update languages.

References

1. Michael Benedikt, Angela Bonifati, Sergio Flesca, and Avinash Vyas. Adding updates to XQuery: Semantics, optimization, and static analysis. In *XIME-P'05*, 2005.
2. Michael Benedikt, Angela Bonifati, Sergio Flesca, and Avinash Vyas. Verification of tree updates for optimization. In *CAV*, pages 379–393, 2005.
3. Michael Benedikt, Wenfei Fan, and Gabriel M. Kuper. Structural properties of xpath fragments. *Theor. Comput. Sci.*, 336(1):3–31, 2005.
4. A. Berglund, S. Boag, D. Chamberlin, M. F. Fernández, M. Kay, J. Robie, and J. Siméon. XML path language (XPath) 2.0. W3C candidate recommendation, World Wide Web Consortium, June 2006. http://www.w3.org/TR/xpath/.
5. S. Boag, D. Chamberlin, M. F. Fernandez, D. Florescu, J. Robie, and J. Siméon. XQuery 1.0: An XML query language. W3C candidate recommendation, World Wide Web Consortium, June 2006. http://www.w3.org/TR/xquery/.
6. Mike Carey, Don Chamberlin, Daniela Florescu, and Jonathan Robie. Programming with XQuery. Draft submitted for publication, April 2006.
7. Don Chamberlin, Daniela Florescu, and Jonathan Robie. XQuery update facility. W3C Working Draft, May 2006.
8. Ezra Cooper, Sam Lindley, Philip Wadler, and Jeremy Yallop. Links: Web programming without tiers, June 2006. Unpublished Manuscript.
9. Stijn Dekeyser, Jan Hidders, and Jan Paredaens. A transaction model for xml databases. *World Wide Web*, 7(1):29–57, 2004.
10. Charles Elkan. Independence of logic database queries and updates. In *PODS*, pages 154–160, 1990.
11. M. Fernández, A. Malhotra, J. Marsh, M. Nagy, and N. Walsh. XQuery 1.0 and XPath 2.0 data model. W3C candidate recommendation, World Wide Web Consortium, June 2006. http://www.w3.org/TR/xpath-datamodel/.
12. Giorgio Ghelli, Christopher Ré, and Jérôme Siméon. XQuery!: An XML query language with side effects. In *DataX Workshop*, Lecture Notes in Computer Science, Munich, Germany, March 2006.
13. Giorgio Ghelli, Kristoffer Rose, and Jérôme Siméon. Commutativity analysis in XML update languages, 2006.
`http://www.di.unipi.it/˜ghelli/papers/UpdateAnalysis.pdf`.
14. Vladimir Lanin and Dennis Shasha. A symmetric concurrent b-tree algorithm. In *FJCC*, pages 380–389, 1986.
15. Patrick Lehti. Design and implementation of a data manipulation processor for an XML query processor, Technical University of Darmstadt, Germany, Diplomarbeit, 2001.
16. Alon Y. Levy and Yehoshua Sagiv. Queries independent of updates. In *19th International Conference on Very Large Data Bases, August 24-27, 1993, Dublin, Ireland, Proceedings*, pages 171–181. Morgan Kaufmann, 1993.
17. Amélie Marian and Jérôme Simeon. Projecting XML documents. In *Proceedings of International Conference on Very Large Databases (VLDB)*, pages 213–224, Berlin, Germany, September 2003.
18. Gerome Miklau and Dan Suciu. Containment and equivalence for a fragment of xpath. *J. ACM*, 51(1):2–45, 2004.
19. I. Tatarinov, Z. Ives, A. Halevy, and D. Weld. Updating XML. In *SIGMOD*, 2001.
20. Philip Wadler. Two semantics of xpath. Discussion note for W3C XSLT Working Group, 1999. http://homepages.inf.ed.ac.uk/wadler/papers/xpath-semantics/xpath-semantics.pdf.

A Language Semantics

A.1 Accessors

For convenience, we define some of the usual accessors, as follows. The definitions are kept informal. Hereafter, we write $E(m,n)$, or mEn, to signify that $(m,n) \in E$.

$$
\begin{aligned}
\texttt{nodekind}(\sigma,n) &=_{\text{def}} \texttt{kind}_F(n) \\
\texttt{children}(\sigma,n) &=_{\text{def}} \{\, n' \mid E(n,n') \,\} \\
\texttt{descendant}(\sigma,n) &=_{\text{def}} \texttt{children}(\sigma,n) \\
&\quad \cup \{\, n'' \mid n' \in \texttt{children}(\sigma,n), n'' \in \texttt{descendant}(\sigma,n') \,\} \\
\texttt{parent}(\sigma,n) &=_{\text{def}} \{\, n' \mid E(n',n) \,\} \\
\texttt{ancestor}(\sigma,n) &=_{\text{def}} \texttt{parent}(\sigma,n) \\
&\quad \cup \{\, n'' \mid n' \in \texttt{parent}(\sigma,n), n'' \in \texttt{ancestor}(\sigma,n') \,\}
\end{aligned}
$$

A.2 Semantics of Paths

To interpret paths we first define a function that interprets each step as a set of pairs.

$$
\begin{aligned}
[\![\texttt{child}::\mathbf{t}]\!]_\sigma &= \{\, (n_1,n_2) \mid n_2 \in \texttt{children}(\sigma,n_1) \ \wedge\ \mathit{NodeTest}(\mathbf{t},n_2) \,\} \\
[\![\texttt{descendant}::\mathbf{t}]\!]_\sigma &= \{\, (n_1,n_2) \mid n_2 \in \texttt{descendant}(\sigma,n_1) \ \wedge\ \mathit{NodeTest}(\mathbf{t},n_2) \,\} \\
[\![\texttt{parent}::\mathbf{t}]\!]_\sigma &= \{\, (n_1,n_2) \mid n_2 \in \texttt{parent}(\sigma,n_1) \ \wedge\ \mathit{NodeTest}(\mathbf{t},n_2) \,\} \\
[\![\texttt{ancestor}::\mathbf{t}]\!]_\sigma &= \{\, (n_1,n_2) \mid n_2 \in \texttt{ancestor}(\sigma,n_1) \ \wedge\ \mathit{NodeTest}(\mathbf{t},n_2) \,\}
\end{aligned}
$$

with the auxiliary

$$
\begin{aligned}
\mathit{NodeTest}(\mathit{QName},n) &\ \Leftrightarrow\ \texttt{name}_F(\sigma,n) = \mathit{QName} \\
\mathit{NodeTest}(\texttt{*},n) &\ \Leftrightarrow\ \exists \mathit{QName}\colon \texttt{name}_F(\sigma,n) = \mathit{QName} \\
\mathit{NodeTest}(\texttt{text()},n) &\ \Leftrightarrow\ \texttt{kind}_F(\sigma,n) = \texttt{text} \\
\mathit{NodeTest}(\texttt{node()},n) &\ \text{is always true}
\end{aligned}
$$

Let $\sigma = (N,E,R,F)$ be a store and $\mathbf{p}$ a path. Path interpretation $[\![\mathbf{p}]\!]_\sigma$ is defined as follows. The result is unordered, for simplicity, and because order is not tracked by the analysis we study in this paper.

$$
\begin{aligned}
[\![()]\!]_\sigma &= \emptyset \\
[\![\mathit{loc}]\!]_\sigma &= \{\, n \mid R(n) = \mathit{loc} \,\} \\
[\![\mathbf{p}|\mathbf{q}]\!]_\sigma &= [\![\mathbf{p}]\!]_\sigma \cup [\![\mathbf{q}]\!]_\sigma \\
[\![\mathbf{p}/\mathit{Step}]\!]_\sigma &= \{\, n_2 \mid n_1 \in [\![\mathbf{p}]\!]_\sigma \ \wedge\ (n_1,n_2) \in [\![\mathit{Step}]\!]_\sigma \,\}
\end{aligned}
$$

A.3 Semantics of Updates

The metavariables n, m, range over node ids, $\bar{n}$ and $\bar{m}$ range over node id sequences, and *name* ranges over qnames. The metavariables constrain rule applicability. This means that, if a judgment in the premise uses n in the result position, as in:

$$dEnv \vdash \eta_0; Expr \Rightarrow \eta_1; n,$$

the judgment can only be applied if *Expr* evaluates to a value which is a node.

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr \Rightarrow \eta_1; \bar{n} \\ \eta_2 = \eta_1, \texttt{delete}(\bar{n}) \end{array}}{dEnv \vdash \eta_0; \texttt{delete } \{Expr\} \Rightarrow \eta_2; ()} \quad (\textsc{Delete})$$

`insert` copies all the descendants of the first argument, and links the copies as new children of the second argument. Let $\bar{n}_d$ be the descendants-or-self of the nodes in $\bar{n}$. Insert-into uses *prepare-deep-copy* to identify a fresh node $m_i \in \bar{m}_d$ for each node in $\bar{n}_d$, while E_{copy} and F_{copy} reproduce for $E_{\text{apply}(\eta_2)}$ and $F_{\text{apply}(\eta_2)}$ for $\bar{m}_d$, and $\bar{m}$ is the subset of $\bar{m}_d$ that corresponds to $\bar{n}$. Hence, $\texttt{create}(\bar{m}_d, F_{\text{copy}}), \texttt{insert}(E_{\text{copy}})$ copy $\bar{n}$ and their descendants, while $\texttt{insert}(\{n\} \times \bar{m})$ links the copies of $\bar{n}$ to n. Notice how the rule only depends on apply(η_2), not on the internal structure of η_2.

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr_1 \Rightarrow \eta_1; \bar{n} \\ dEnv \vdash \eta_1; Expr_2 \Rightarrow \eta_2; n \\ (\bar{m}, \bar{m}_d, E_{\text{copy}}, F_{\text{copy}}) = \textit{prepare-deep-copy}(\text{apply}(\eta_2), \bar{n}) \\ \eta_3 = \eta_2,\ \texttt{create}(\bar{m}_d, F_{\text{copy}}), \texttt{insert}(E_{\text{copy}}), \texttt{insert}(\{n\} \times \bar{m}) \end{array}}{dEnv \vdash \eta_0; \texttt{insert } \{Expr_1\} \texttt{ into } \{Expr_2\} \Rightarrow \eta_3; ()} \quad (\textsc{Insert})$$

Element creation copies all the descendants of the second argument, and links the copy as new children of a fresh node whose name is given by the first argument. The fresh node is linked to *code-loc*, only for the purposes of our analysis. The function *fresh*(N) returns a new node fresh for N.

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr_1 \Rightarrow \eta_1; name \\ dEnv \vdash \eta_1; Expr_2 \Rightarrow \eta_2; \bar{n} \\ (\bar{m}, \bar{m}_d, E_{\text{copy}}, F_{\text{copy}}) = \textit{prepare-deep-copy}(\text{apply}(\eta_2), \bar{n}) \\ m = \textit{fresh}(N_{\text{apply}(ES_2)} \cup \bar{m}_d) \\ \begin{array}{ll} \eta_3 = \eta_2, & \texttt{create}(\bar{m}_d, F_{\text{copy}}), \\ & \texttt{create}(m, (m \mapsto \texttt{element}, m \mapsto name, ())), \\ & \texttt{R-insert}(m, \textit{code-loc}), \texttt{insert}(E_{\text{copy}}), \texttt{insert}(\{n\} \times \bar{m}) \end{array} \end{array}}{dEnv \vdash \eta_0; \texttt{element}_{\textit{code-loc}}\{Expr_1\}\{Expr_2\} \Rightarrow \eta_3; m} \quad (\textsc{Elt})$$

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr \Rightarrow \eta_1; \bar{n} \\ \bar{n} = \{\, n' \mid \exists n \in \bar{n}.\ (n, n') \in [\![Step]\!]_{\text{apply}(\eta_1)} \,\} \end{array}}{dEnv \vdash \eta_0; Expr/Step \Rightarrow \eta_1; \bar{n}} \quad (\textsc{Step})$$

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr_1 \Rightarrow \eta_1; \bar{n}_1 \\ dEnv \vdash \eta_1; Expr_2 \Rightarrow \eta_2; \bar{n}_2 \end{array}}{dEnv \vdash \eta_0; Expr_1, Expr_2 \Rightarrow \eta_2; \bar{n}_1, \bar{n}_2} \quad \text{(COMMA)}$$

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr_1 \Rightarrow \eta_1; \bar{n}_1 \\ (dEnv + \$x \mapsto \bar{n}_1) \vdash \eta_1; Expr_2 \Rightarrow \eta_2; \bar{n}_2 \end{array}}{dEnv \vdash \eta_0; \texttt{let \$}x\ \texttt{:=}\ Expr_1\ \texttt{return}\ Expr_2 \Rightarrow \eta_2; \bar{n}_2} \quad \text{(LET)}$$

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr_1 \Rightarrow \eta_1; item_1, \ldots, item_m \\ for\ i\ in\ 1 \ldots m:\ (dEnv + \$x \mapsto item_i) \vdash \eta_i; Expr_2 \Rightarrow \eta_{i+1}; \bar{n}_i \end{array}}{dEnv \vdash \eta_0; \texttt{for \$}x\ \texttt{in}\ Expr_1\ \texttt{return}\ Expr_2 \Rightarrow \eta_{m+1}; \bar{n}_1, \ldots, \bar{n}_n} \quad \text{(FOR)}$$

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr \Rightarrow \eta_1; \texttt{true} \\ dEnv \vdash \eta_1; Expr_1 \Rightarrow \eta_2; \bar{n} \end{array}}{dEnv \vdash \eta_0; \texttt{if (}Expr\texttt{) then}\ Expr_1\ \texttt{else}\ Expr_2 \Rightarrow \eta_2; \bar{n}} \quad \text{(IFT)}$$

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr \Rightarrow \eta_1; \texttt{false} \\ dEnv \vdash \eta_1; Expr_2 \Rightarrow \eta_2; \bar{n} \end{array}}{dEnv \vdash \eta_0; \texttt{if (}Expr\texttt{) then}\ Expr_1\ \texttt{else}\ Expr_2 \Rightarrow \eta_2; \bar{n}} \quad \text{(IFF)}$$

$$\frac{\begin{array}{c} dEnv \vdash \eta_0; Expr_1 \Rightarrow \eta_1; \bar{n}_1 \\ dEnv \vdash \eta_1; Expr_2 \Rightarrow \eta_2; \bar{n}_2 \\ b = \texttt{equal}(\bar{n}_1, \bar{n}_2) \end{array}}{dEnv \vdash \eta_0; Expr_1 = Expr_2 \Rightarrow \eta_2; b} \quad \text{(EQ)}$$

B Soundness proof

B.1 Some Lemmas

Lemma 1.

$$\begin{array}{l} \Delta' \subseteq \Delta \Rightarrow wf(\eta, \Delta) \Rightarrow wf(\eta, \Delta') \\ \Delta' \subseteq \Delta \Rightarrow wf(\eta, \Delta) \Rightarrow [\![\mathbf{p}]\!]_{apply(\eta,\Delta')} \subseteq [\![\mathbf{p}]\!]_{apply(\eta,\Delta)} \end{array}$$

Lemma 2 (Store history equivalence modulo a path). *The following is an alternative characterization of equivalence*

$$\begin{array}{l} \forall \mathbf{p}' \in pref(\mathbf{p}).\ \forall \Delta.\ wf(\eta_1, \Delta) \wedge wf(\eta_2, \Delta) \Rightarrow [\![\mathbf{p}']\!]_{apply(\eta_1,\Delta)} = [\![\mathbf{p}']\!]_{apply(\eta_2,\Delta)} \\ \forall \mathbf{p}' \in pref(\mathbf{p}).\ \forall \Delta.\ created(\Delta)\#(N_{\eta_1} \cup N_{\eta_2}) \wedge wf(\eta_1, \Delta) \\ \qquad\qquad \wedge\ n \in [\![\mathbf{p}']\!]_{apply(\eta_1,\Delta)} \Rightarrow \exists \Delta' \subseteq \Delta.\ wf(\eta_2, \Delta') \wedge n \in [\![\mathbf{p}']\!]_{apply(\eta_1,\Delta')} \\ \forall \mathbf{p}' \in pref(\mathbf{p}).\ \forall \Delta.\ created(\Delta)\#(N_{\eta_1} \cup N_{\eta_2}) \wedge wf(\eta_2, \Delta) \\ \qquad\qquad \wedge\ n \in [\![\mathbf{p}']\!]_{apply(\eta_2,\Delta)} \Rightarrow \exists \Delta' \subseteq \Delta.\ wf(\eta_1, \Delta') \wedge n \in [\![\mathbf{p}']\!]_{apply(\eta_2,\Delta')} \end{array}$$

We use R^{-1} and R^* to denote the inverse and the Kleene star or a binary relation.

Property 2. Either $[\![step]\!]_\sigma \subseteq E_\sigma^*$ (downward steps) or $[\![step]\!]_\sigma \subseteq (E_\sigma^{-1})^*$ (upward steps).

Proposition 1.

$$(pref() \sim) \;\; \mathbf{p} \in pref(\mathbf{q}) \wedge \eta_1 \sim_{\mathbf{q}} \eta_2 \;\Rightarrow\; \eta_1 \sim_{\mathbf{p}} \eta_2$$

Lemma 3.

$$\begin{array}{lll} \mathbf{p}|\mathbf{p}' \in pref(\mathbf{q}) & \Rightarrow & \mathbf{p} \in pref(\mathbf{q}) \wedge \mathbf{p}' \in pref(\mathbf{q}) \\ \mathbf{p}/Step \in pref(\mathbf{q}) & \Rightarrow & \mathbf{p} \in pref(\mathbf{q}) \end{array}$$

Proof. First part: by induction on $\mathbf{q}$. If $\mathbf{q}$ is *loc*, the result is immediate. If $\mathbf{q} = \mathbf{q}'/StepExpr$, then $\mathbf{p}|\mathbf{p}' \in \text{pref}(\mathbf{q}')$, hence, by induction, $\mathbf{p} \in \text{pref}(\mathbf{q}')$ and $\mathbf{p}' \in \text{pref}(\mathbf{q}')$ and the result follows. If $\mathbf{q} = \mathbf{q}'|\mathbf{q}''$, then either $\mathbf{q} = \mathbf{p}|\mathbf{p}'$, or not. In the first case, the thesis follows because $\mathbf{p} \in \text{pref}(\mathbf{p})$ and $\mathbf{p}' \in \text{pref}(\mathbf{p}')$. Otherwise, $\mathbf{p}|\mathbf{p}' \in \text{pref}(\mathbf{q}')$ or $\mathbf{p}|\mathbf{p}' \in \text{pref}(\mathbf{q}'')$. W.l.o.g., assume the first, then, by induction, $\mathbf{p} \in \text{pref}(\mathbf{q}')$ and $\mathbf{p}' \in \text{pref}(\mathbf{q}')$, and the result follows.

Second part: analogous.

B.2 Delete rule

The rule deduces:

$$\mathbf{pEnv} \vdash \texttt{delete } \{Expr\} \Rightarrow (); \langle \mathbf{a}, \mathbf{u}|(\mathbf{r}/dos::*)\rangle$$

from:

$$(0) \qquad \mathbf{pEnv} \vdash Expr \Rightarrow \mathbf{r}; \langle \mathbf{a}, \mathbf{u}\rangle$$

We have to prove that the following assumptions:

$$\begin{array}{l} (1)\; dEnv \vdash \eta_0; \texttt{delete } \{Expr\} \Rightarrow \eta_2; () \\ (2)\; \mathbf{pEnv} \supseteq_{\eta_0} dEnv \end{array}$$

imply the following facts:

Approximation:
$() \supseteq_{\eta_2} ()$

Immutability:
$\text{prefclosed}(\mathbf{c}) \wedge \mathbf{c}\#(\mathbf{u}|(\mathbf{r}/dos::*)) \Rightarrow \eta_0 \sim_{\mathbf{c}} \eta_2$
$(\mathbf{u}|(\mathbf{r}/dos::*)) \supseteq_{\eta_2} updated(\eta_2 \setminus \eta_0)$

Parallel Evolution:
$\eta_0' \sim_{\mathbf{a}} \eta_0 \wedge N_0'\#(N_1 \setminus N_0)$
$\Rightarrow \exists \eta_2' \,(\, dEnv \vdash \eta_0'; \texttt{delete } \{Expr\} \Rightarrow \eta_2'; ()$
$\wedge\, \eta_2 \setminus \eta_0 = \eta_2' \setminus \eta_0' \,)$

By the inversion property of the dynamic semantics, (1) implies:

$$\begin{array}{l} (3)\; dEnv \vdash \eta_0; Expr \Rightarrow \eta_1; \overline{n} \\ (4)\; \eta_2 = \eta_1, \texttt{delete}(\overline{n}) \end{array}$$

By induction, (0), (3), and (2) imply the following properties:

Approximation – induction:
$\mathbf{r} \supseteq_{\eta_1} \overline{n}$

Immutability – induction:
$\mathbf{c}\#\mathbf{u} \;\Rightarrow\; \eta_0 \sim_{\mathbf{c}} \eta_1$
$\mathbf{u} \supseteq_{\eta_1} \mathit{updated}(\eta_1 \setminus \eta_0)$

Parallel Evolution – induction:
$\eta'_0 \sim_{\mathbf{a}} \eta_0 \;\wedge\; N'_0\#(N_1 \setminus N_0)$
$\Rightarrow\; \exists\eta'_1\; (\; dEnv \vdash \eta'_0; Expr \Rightarrow \eta'_1; \overline{n}$
$\wedge\; \eta'_1 \setminus \eta'_0 = \eta_1 \setminus \eta_0 \;\;)$

Now we can prove the three properties. Approximation is trivial. Immutability and parallel evolution are less trivial.

Immutability. (1) prefclosed($\mathbf{c}$) $\wedge$ $\mathbf{c}\#(\mathbf{r}/\mathit{dos}::*)$ $\Rightarrow$ $\eta_1 \sim_{\mathbf{c}} \eta_2$
(2) $(\mathbf{r}/\mathit{dos}::*) \supseteq_{\eta_2} \mathit{updated}(\eta_2 \setminus \eta_1)$

To prove (2), observe that $\eta_2 \setminus \eta_1 = \mathtt{delete}(\overline{n})$, hence $\mathit{updated}(\eta_2 \setminus \eta_1) = \overline{n}$, by approximation - induction $\mathbf{r} \supseteq_{\eta_1} \overline{n}$, by stability $\mathbf{r} \supseteq_{\eta_2} \overline{n}$, and by the semantics of $(\mathbf{p}/\mathit{dos}::*)$, $(\mathbf{r}/\mathit{dos}::*) \supseteq_{\eta_2} \overline{n}$. The thesis $(\mathbf{u}|(\mathbf{r}/\mathit{dos}::*)) \supseteq_{\eta_2} \mathit{updated}(\eta_2 \setminus \eta_0)$ follows by this property plus the inductione hypothesis $\mathbf{u} \supseteq_{\eta_1} \mathit{updated}(\eta_1 \setminus \eta_0)$, transformed into $\mathbf{u} \supseteq_{\eta_2} \mathit{updated}(\eta_1 \setminus \eta_0)$ by stability.
We now prove the following fact, from which $[\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_0,\Delta)} = [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_0,\mathtt{delete}(\overline{n}),\Delta)}$ immediately follows, since the opposite inclusion is trivial.

$$\forall \mathbf{p} \in \mathrm{pref}(\mathbf{c}).\; \forall\Delta.\; m \in [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_0,\Delta)} \;\Rightarrow\; m \in [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_0,\mathtt{delete}(\overline{n}),\Delta)}$$

We reason by induction on the size of $\mathbf{p}$ and by cases on its shape. Observe that, while $\mathbf{c}$ is prefix-closed, $\mathbf{p}$ is not, in general.

$[\![\mathit{loc}]\!]_{\mathrm{apply}(\eta_0,\Delta)} = [\![\mathit{loc}]\!]_{\mathrm{apply}(\eta_0,\mathtt{delete}(\overline{n}),\Delta)}$: this holds because $\mathtt{delete}(\overline{n})$ has no effect on the semantics of *loc*.

$[\![\mathbf{p}'|\mathbf{p}'']\!]_{\mathrm{apply}(\eta_0,\Delta)} = [\![\mathbf{p}'|\mathbf{p}'']\!]_{\mathrm{apply}(\eta_0,\mathtt{delete}(\overline{n}),\Delta)}$: follows since, by Lemma 3, induction guarantees the same property for $\mathbf{p}'$ and $\mathbf{p}''$.

The only diffcult case in $\mathbf{p} = \mathbf{q}/\mathit{step}$. Assume $m \in [\![\mathbf{q}/\mathit{step}]\!]_{\mathrm{apply}(\eta_0,\Delta)}$.
Then, $\exists m' \in [\![\mathbf{q}]\!]_{\mathrm{apply}(\eta_0,\Delta)}$ and (3) $(m',m) \in [\![\mathit{step}]\!]_{\mathrm{apply}(\eta_0,\Delta)}$.
By lemma 3, $\mathbf{q}/\mathit{step} \in \mathrm{pref}(\mathbf{c})$ implies that $\mathbf{q} \in \mathrm{pref}(\mathbf{c})$.
Hence, by induction $m' \in [\![\mathbf{q}]\!]_{\mathrm{apply}(\eta_0,\mathtt{delete}(\overline{n}),\Delta)}$
We only have to prove that $(m',m) \in [\![\mathit{step}]\!]_{\mathrm{apply}(\eta_0,\mathtt{delete}(\overline{n}),\Delta)}$.
Assume for a contradiction that (4) $(m',m) \notin [\![\mathit{step}]\!]_{\mathrm{apply}(\eta_0,\mathtt{delete}(\overline{n}),\Delta)}$.
By prefclosed($\mathbf{c}$), $\mathbf{q}/\mathit{step} \in \mathrm{pref}(\mathbf{c})$ implies that $\mathbf{q}/\mathit{step} \subseteq \mathbf{c}$, hence $m \in [\![\mathbf{c}]\!]_{\mathrm{apply}(\eta_0,\Delta)}$.
By Lemma 3, $\mathbf{q} \in \mathrm{pref}(\mathbf{c})$, hence $\mathbf{q} \subseteq \mathbf{c}$, hence $m' \in [\![\mathbf{c}]\!]_{\mathrm{apply}(\eta_0,\Delta)}$.
Since we only have upward and downward steps, (3) and (4) together imply that
$\exists n \in \overline{n}$ such that either (i) mE^+nE^*m' or (ii) $m'E^+nE^*m$, where $E = E_{\mathrm{apply}(\eta_0,\Delta)}$.
In either case, an element m or m' of $[\![\mathbf{c}]\!]_{\mathrm{apply}(\eta_0,\Delta)}$ is a descendant (or self) of n
in $\mathrm{apply}(\eta_0,\Delta)$.

Hence, an element of $[\![\mathbf{c}]\!]_{\mathrm{mrg}(\eta_0,\Delta)}$ is a descendant of n in $\mathrm{mrg}(\eta_0,\Delta)$.
By approximation, we know that $n \in [\![\mathbf{r}]\!]_{\mathrm{mrg}(\eta_0)}$.
By stability, $n \in [\![\mathbf{r}]\!]_{\mathrm{mrg}(\eta_0,\Delta)}$.
Hence, every descendant of n in $\mathrm{mrg}(\eta_0,\Delta)$ belongs to $[\![\mathbf{r}/dos::*]\!]_{\mathrm{mrg}(\eta_0,\Delta)}$.
Now, the presence of a $\mathrm{mrg}(\eta_0,\Delta)$-descendant of n in $[\![\mathbf{c}]\!]_{\mathrm{mrg}(\eta_0,\Delta)}$
contraddicts the assumption $\mathbf{c}\#(\mathbf{r}/dos::*)$.

We have now to prove that $\forall\mathbf{p} \in \mathrm{pref}(\mathbf{c})$:

(3) $\forall\Delta.\ n \in [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\Delta)} \wedge (\textit{node-created}(\Delta))\#N_{\mathrm{apply}(\eta_2,\mathtt{delete}(\overline{n}))}$
$\Rightarrow \exists\Delta' \subseteq \Delta.\ wf(\eta_2,\mathtt{delete}(\overline{n}),\Delta') \wedge n \in [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\Delta')}$

(4) $\forall\Delta.\ n \in [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\mathtt{delete}(\overline{n}),\Delta)} \wedge (\textit{node-created}(\Delta))\#N_{\mathrm{apply}(\eta_2)}$
$\Rightarrow \exists\Delta' \subseteq \Delta.\ wf(\eta_2,\Delta') \wedge n \in [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\mathtt{delete}(\overline{n}),\Delta')}$

(3) is trivial: take $\Delta' = \Delta$: the addition of a `delete` creates no conflict. In the (4) case, let E' be the set of pairs (n_p,n_c) such that $(n_p,n_c) \in \mathrm{apply}(\eta_2,\Delta)$ and $n_c \in \overline{n}$, and let Δ' be Δ where each $\mathtt{insert}E$ has been substituted by $\mathtt{insert}E\setminus E'$. Then, $wf(\eta_2,\mathtt{delete}\overline{n},\Delta)$ implies $wf(\eta_2,\Delta')$, and $\mathrm{apply}(\eta_2,\Delta) = \mathrm{apply}(\eta_2,\mathtt{delete}(\overline{n}),\Delta')$, hence $n \in [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\Delta')}$. The thesis $n \in [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\Delta')}$ follows by $[\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\Delta')} = [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta_2,\mathtt{delete}\overline{n},\Delta')}$, which we proved before.

This proves that (1) $\mathrm{prefclosed}(\mathbf{c}) \wedge \mathbf{c}\#(\mathbf{r}/dos::*) \Rightarrow \eta_1 \sim_{\mathbf{c}} \eta_2$. The thesis follows by induction: assume $\mathbf{c}\#(\mathbf{u}|(\mathbf{r}/dos::*))$. This implies $\mathbf{c}\#\mathbf{u}$ and $\mathbf{c}\#(\mathbf{r}/dos::*)$, hence $\eta_0 \sim_{\mathbf{c}} \eta_1$ follows by induction and $\eta_1 \sim_{\mathbf{c}} \eta_2$ follows by (1), hence $\eta_0 \sim_{\mathbf{c}} \eta_2$ follows by transitivity.

Parallel Evolution. We choose any η_1' among those implied by the inductive property, and define $\eta_2' = \eta_1',\mathtt{delete}(\overline{n})$. We must prove $\mathit{dEnv} \vdash \eta_0';\mathtt{delete}\ \{\mathit{Expr}\} \Rightarrow \eta_2';()$ and $\eta_2 \setminus \eta_0 = \eta_2' \setminus \eta_0'$. The first holds by construction. For the second, $(\eta_2 \setminus \eta_0)$= $((\eta_1 \setminus \eta_0),\mathtt{delete}(\overline{n}))$= $((\eta_1' \setminus \eta_0'),\mathtt{delete}(\overline{n}))$= $(\eta_2' \setminus \eta_0')$.

B.3 Insert rule

The rule deduces:

$$\mathbf{pEnv} \vdash \mathtt{insert}\ \{\mathit{Expr}_1\}\ \mathtt{into}\ \{\mathit{Expr}_2\}$$
$$\Rightarrow ();\ \langle \mathbf{a}_1|\mathbf{a}_2|(\mathbf{r}_1/dos::*),\mathbf{u}_1|\mathbf{u}_2|(\mathbf{r}_2//*)\rangle$$

from:

$$(0) \qquad \mathbf{pEnv} \vdash \mathit{Expr}_1 \Rightarrow \mathbf{r}_1;\ \langle \mathbf{a}_1,\mathbf{u}_1\rangle$$
$$(1) \qquad \mathbf{pEnv} \vdash \mathit{Expr}_2 \Rightarrow \mathbf{r}_2;\ \langle \mathbf{a}_2,\mathbf{u}_2\rangle$$

We have to prove that the following assumptions:

(2) $\mathit{dEnv} \vdash \eta_0;\mathtt{insert}\ \{\mathit{Expr}_1\}\ \mathtt{into}\ \{\mathit{Expr}_2\} \Rightarrow \eta_3;()$
(3) $\mathbf{pEnv} \supseteq_{\eta_0} \mathit{dEnv}$

imply the following facts:

Approximation:
$() \supseteq_{\eta_3} ()$

Immutability:
$\mathrm{prefclosed}(\mathbf{c}) \wedge \mathbf{c}\#(\mathbf{u}_1|\mathbf{u}_2|(\mathbf{r}_2//*)) \Rightarrow \eta_0 \sim_{\mathbf{c}} \eta_3$
$(\mathbf{u}_1|\mathbf{u}_2|(\mathbf{r}_2//*)) \supseteq_{\eta_3} \mathit{updated}(\eta_3 \setminus \eta_0)$

Parallel Evolution:
$\eta'_0 \sim_{\mathbf{a}} \eta_0 \wedge N'_0\#(N_1 \setminus N_0)$
$\Rightarrow \exists \eta'_3 \; (\mathit{dEnv} \vdash \eta'_0; \texttt{insert } \{\mathit{Expr}_1\} \texttt{ into } \{\mathit{Expr}_2\} \Rightarrow \eta'_3; ()$
$\wedge \eta_3 \setminus \eta_0 = \eta'_3 \setminus \eta'_0 \;)$

By the inversion property of the dynamic semantics, (2) implies what follows (we identify here $\texttt{insert}(E), \texttt{insert}(E')$ with $\texttt{insert}(E \cup E')$).

$$
\begin{array}{l}
(4)\ \mathit{dEnv} \vdash \eta_0; \mathit{Expr}_1 \Rightarrow \eta_1; \bar{n} \\
(5)\ \mathit{dEnv} \vdash \eta_1; \mathit{Expr}_2 \Rightarrow \eta_2; n \\
(6)\ \eta_3 = \eta_2, \texttt{create}(\bar{m}_d, F'), \texttt{insert}(E' \cup (\{n\} \times \bar{m}))
\end{array}
$$

By induction, (0), (4), (5), and (3) imply the following properties:

Approximation – induction:
$\mathbf{r}_1 \supseteq_{\eta_1} \bar{n}$
$\mathbf{r}_2 \supseteq_{\eta_2} n$

Immutability – induction:
$\mathbf{c}\#\mathbf{u}_1 \Rightarrow \eta_0 \sim_{\mathbf{c}} \eta_1$
$\mathbf{c}\#\mathbf{u}_2 \Rightarrow \eta_1 \sim_{\mathbf{c}} \eta_2$
$\mathbf{u}_1 \supseteq_{\eta_1} \mathit{updated}(\eta_1 \setminus \eta_0)$
$\mathbf{u}_2 \supseteq_{\eta_2} \mathit{updated}(\eta_2 \setminus \eta_1)$

Parallel Evolution – induction:
$\eta'_0 \sim_{\mathbf{a}_1} \eta_0 \wedge N'_0\#(N_1 \setminus N_0)$
$\Rightarrow \exists \eta'_1 \; (\mathit{dEnv} \vdash \eta'_0; \mathit{Expr}_1 \Rightarrow \eta'_1; \bar{n} \wedge \eta'_1 \setminus \eta'_0 = \eta_1 \setminus \eta_0 \;)$
$\eta'_1 \sim_{\mathbf{a}_2} \eta_1 \wedge N'_1\#(N_2 \setminus N_1)$
$\Rightarrow \exists \eta'_2 \; (\mathit{dEnv} \vdash \eta'_1; \mathit{Expr}_2 \Rightarrow \eta'_2; n \wedge \eta'_2 \setminus \eta'_1 = \eta_2 \setminus \eta_1 \;)$

Now we can prove the three properties. Approximation is trivial. Immutability and parallel evolution are less trivial.

Immutability We first prove the following property:

(1) $\forall \mathbf{c}, \mathbf{p} \in \mathrm{pref}(\mathbf{c}), \mathbf{r}, \eta, n_p, \bar{m}_d\#N_\eta, \bar{m} \subseteq \bar{m}_d, E' \subseteq (\bar{m}_d \times \mathit{nodes}()), \Delta.$
$\mathit{wf}(\eta, \texttt{create}(\bar{m}_d, F'), \texttt{insert}(E' \cup (\{n_p\} \times \bar{m})), \Delta)$
$\wedge\, \mathit{wf}(\eta, \mathit{Delta}) \wedge \mathbf{r} \supseteq_\eta n_p \wedge \mathrm{prefclosed}(\mathbf{c}) \wedge \mathbf{c}\#(\mathbf{r}//*)$
$\Rightarrow [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta,\Delta)} = [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta,\texttt{create}(\bar{m}_d,F'),\texttt{insert}(E' \cup (\{n_p\} \times \bar{m})),\Delta)}$

Hereafter we abbreviate $\texttt{create}(\bar{m}_d, F'), \texttt{insert}(E' \cup (\{n_p\} \times \bar{m})), \Delta$ with $\texttt{cr}, \texttt{ins}, \Delta$. We prove the following inclusion, since the opposite is trivial:

$$[\![\mathbf{p}]\!]_{\mathrm{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)} \subseteq [\![\mathbf{p}]\!]_{\mathrm{apply}(\eta,\Delta)}$$

We reason by induction on the size of **p** and by cases on its shape. Observe that we do not assume that **p** is prefix-closed.

$[\![loc]\!]_{\text{apply}(\eta,\Delta)} = [\![loc]\!]_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$: this holds because $\texttt{create}(\bar{m}_d, F')$, $\texttt{insert}(E' \cup (\{n_p\} \times \bar{m}))$ has no effect on the semantics of *loc*.

$[\![\mathbf{p}'|\mathbf{p}'']\!]_{\text{apply}(\eta,\Delta)} = [\![\mathbf{p}'|\mathbf{p}'']\!]_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$: follows by induction from the same property for $\mathbf{p}'$ and $\mathbf{p}''$, which belong to pref($\mathbf{c}$) by Lemma 3.

The difficult case is $\mathbf{p} = \mathbf{q}/step$. Assume $m \in [\![\mathbf{q}/step]\!]_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$.
Then, $\exists m' \in [\![\mathbf{q}]\!]_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$ and $(m', m) \in [\![step]\!]_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$.
By lemma 3, $\mathbf{q}/step \in \text{pref}(\mathbf{c})$ implies that $\mathbf{q} \in \text{pref}(\mathbf{c})$.
Hence, by induction (3) $m' \in [\![\mathbf{q}]\!]_{\text{apply}(\eta,\Delta)}$. We only have to prove that $(m', m) \in [\![step]\!]_{\text{apply}(\eta,\Delta)}$.
If $[\![step]\!]_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$ connects m' to m without traversing an edge added by $\texttt{insert}(E' \cup (\{n_p\} \times \bar{m}))$, then the thesis is obvious. We hence assume that (4) $[\![step]\!]_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$ connects m' to m by traversing an edge added by $\texttt{insert}(E' \cup (\{n_p\} \times \bar{m}))$, and we prove that (4) is impossible. Property (4) implies that *step* is a downward step, since, by (3), m' has no ancestor among the freshly added nodes.
Since m' is not fresh but a fresh node appears in the parent-child chain that connects m' to m, then a pair (o, o') with $o \in N_\eta$ and $o' \notin N_\eta$ must be in that chain. Such pairs in $E_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$ have the shape (n_p, m_i), hence we have $m'E^*n_pEm_iE^*m$, where $E = E_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)}$. By hypothesis $\mathbf{r} \supseteq_\eta n_p$ and by stability $\mathbf{r} \supseteq_{\eta,\texttt{cr},\texttt{ins},\Delta} n_p$, hence m is in $[\![\mathbf{r}//*]\!]_{\text{mrg}(\eta,\texttt{cr},\texttt{ins},\Delta)}$.
This contradicts the hypothesis $\mathbf{c}\#(\mathbf{r}//*)$ since m is in $[\![\mathbf{q}/step]\!]_{\text{apply}(\eta,\texttt{cr},\texttt{ins},\Delta)} \subseteq [\![\mathbf{q}/step]\!]_{\text{mrg}(\eta,\texttt{cr},\texttt{ins},\Delta)}$, and prefix closure of $\mathbf{c}$ implies $[\![\mathbf{q}/step]\!]_{\text{mrg}(\eta,\texttt{cr},\texttt{ins},\Delta)} \subseteq [\![\mathbf{c}]\!]_{\text{mrg}(\eta,\texttt{cr},\texttt{ins},\Delta)}$. This concludes the proof of (1).

We have now to prove that:

(5) $\forall\Delta.\ n \in [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\Delta)} \ \wedge\ (\textit{node-created}(\Delta))\#N_{\text{apply}(\eta_2,\texttt{cr},\texttt{ins})}$
$\quad \Rightarrow\ \exists\Delta' \subseteq \Delta.\ \textit{wf}(\eta_2,\texttt{cr},\texttt{ins},\Delta') \ \wedge\ n \in [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\Delta')}$

(6) $\forall\Delta.\ n \in [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\texttt{cr},\texttt{ins},\Delta)} \ \wedge\ (\textit{node-created}(\Delta))\#N_{\text{apply}(\eta_2)}$
$\quad \Rightarrow\ \exists\Delta' \subseteq \Delta.\ \textit{wf}(\eta_2,\Delta') \ \wedge\ n \in [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\texttt{cr},\texttt{ins},\Delta')}$

(5) is trivial: take $\Delta' = \Delta$. No `insert`-`insert` conflicts may appear between `cr,ins` and Δ, since all the children of all the edges added by `cr,ins` have been created by `cr,ins` itself, hence do not appear in Δ. In the (6) case, let us split Δ into Δ_i, Δ_r, Δ_d and Δ', where the first three contain the `insert`, `R-insert`, and `delete` operations that use a node created by `cr,ins`. This ensures $\textit{wf}(\eta_2,\Delta')$, but we have to prove that $n \in [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\texttt{cr},\texttt{ins},\Delta')}$. We observe that every node created by `cr,ins` has a parent, hence no Δ_r is empty, and every insert in Δ_i has the fresh node in the parent position, hence:
$n \in [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\texttt{create}(\bar{m}_d,F'),\texttt{insert}(E'\cup(\{n_p\}\times\bar{m})),\Delta_i,\Delta_d,\Delta')}$
$\Rightarrow\ n \in [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\texttt{create}(\bar{m}_d,F'),\texttt{insert}(E'\cup(\{n_p\}\times\bar{m})),\Delta_i,\Delta')}$
(by (1)) $\Rightarrow\ [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\Delta')} \ \Rightarrow\ [\![\mathbf{p}]\!]_{\text{apply}(\eta_2,\texttt{cr},\texttt{ins},\Delta')}$.
This ends the proof that (2) prefclosed($\mathbf{c}$) $\wedge$ $\mathbf{c}\#(\mathbf{r}/dos::*)$ $\Rightarrow$ $\eta_2 \sim_{\mathbf{c}} \eta_3$. The thesis follows by induction: assume $\mathbf{c}\#(\mathbf{u}_1|\mathbf{u}_2|(\mathbf{r}/dos::*))$. This implies $\mathbf{c}\#\mathbf{u}_1$ and $\mathbf{c}\#\mathbf{u}_2$ and $\mathbf{c}\#(\mathbf{r}/dos::*)$, hence $\eta_0 \sim_{\mathbf{c}} \eta_1$ and $\eta_1 \sim_{\mathbf{c}} \eta_2$ follow by induction and $\eta_2 \sim_{\mathbf{c}} \eta_3$ follows by (2), hence $\eta_0 \sim_{\mathbf{c}} \eta_3$ follows by transitivity.

(3) $(\mathbf{r}_2//*) \supseteq_{\eta_3} \mathit{updated}(\eta_3 \setminus \eta_2)$

To prove (3), observe that $\eta_3 \setminus \eta_2 = \mathtt{create}(\overline{m}_d, F'), \mathtt{insert}(E' \cup (\{n\} \times \overline{m}))$, where $E' \subseteq (\overline{m}_d \times \overline{m}_d)$ and $\overline{m} \subseteq \overline{m}_d$, hence $\mathit{updated}(\eta_3 \setminus \eta_2) \subseteq \overline{m}_d$, by approximation - induction $\mathbf{r}_2 \supseteq_{\eta_2} n$, by stability $\mathbf{r}_2 \supseteq_{\eta_3} n$, and by the semantics of $(\mathbf{p}/\mathit{dos}::*)$, $(\mathbf{r}_2//*) \supseteq_{\eta_3} \overline{m}_d$, since eah node in $\overline{m}_d$ is a descendant of n in η_3. The thesis $(\mathbf{u}_1|\mathbf{u}_2|(\mathbf{r}_2//*)) \supseteq_{\eta_3} \mathit{updated}(\eta_3 \setminus \eta_0)$ follows by this property plus the induction hypothesis $\mathbf{u}_1 \supseteq_{\eta_1} \mathit{updated}(\eta_1 \setminus \eta_0)$, $\mathbf{u}_2 \supseteq_{\eta_2} \mathit{updated}(\eta_2 \setminus \eta_1)$, combined and transformed into $\mathbf{u}_1|\mathbf{u}_2 \supseteq_{\eta_3} \mathit{updated}(\eta_2 \setminus \eta_0)$ by stability.

B.4 Step rule

$$\frac{\mathbf{pEnv} \vdash \mathit{Expr} \Rightarrow \mathbf{r};\ \langle \mathbf{a}, \mathbf{u} \rangle}{\mathbf{pEnv} \vdash \mathit{Expr}/\mathit{Step} \Rightarrow \mathbf{r}/\mathit{Step};\ \langle \mathrm{pref}(\mathbf{r}/\mathit{Step})|\mathbf{a}, \mathbf{u} \rangle} \qquad (\textsc{Step})$$

The rule deduces:

$$\mathbf{pEnv} \vdash \mathit{Expr}/\mathit{Step} \Rightarrow \mathbf{r}/\mathit{Step};\ \langle \mathrm{pref}(\mathbf{r}/\mathit{Step})|\mathbf{a}, \mathbf{u} \rangle$$

from:

$$(0) \qquad \mathbf{pEnv} \vdash \mathit{Expr} \Rightarrow \mathbf{r};\ \langle \mathbf{a}, \mathbf{u} \rangle$$

We have to prove that the following assumptions:

$$(1)\ \mathit{dEnv} \vdash \eta_0; \mathit{Expr}/\mathit{Step} \Rightarrow \eta_1; \overline{n}$$
$$(2)\ \mathbf{pEnv} \supseteq_{\eta_0} \mathit{dEnv}$$

imply the following facts:
Approximation:
$\mathbf{r}/\mathit{Step} \supseteq_{\eta_1} \overline{n}$
Immutability:
$\mathrm{prefclosed}(\mathbf{c}) \wedge \mathbf{c}\#\mathbf{u} \Rightarrow \eta_0 \sim_{\mathbf{c}} \eta_1$
$\mathbf{u} \supseteq_{\eta_1} \mathit{updated}(\eta_1 \setminus \eta_0)$
Parallel Evolution:
$\eta_0' \sim_{\mathrm{pref}(\mathbf{r}/\mathit{Step})|\mathbf{a}} \eta_0 \ \wedge\ N_0' \# (N_1 \setminus N_0)$
$\Rightarrow\ \exists \eta_1'\ (\ \mathit{dEnv} \vdash \eta_0'; \mathit{Expr}/\mathit{Step} \Rightarrow \eta_1'; \overline{n}$
$\wedge\ \eta_1 \setminus \eta_0 = \eta_1' \setminus \eta_0'\ )$

By the inversion property of the dynamic semantics, (1) implies:

$$(3)\ \mathit{dEnv} \vdash \eta_0; \mathit{Expr} \Rightarrow \eta_1; \overline{n}_1$$
$$(4)\ \overline{n} = \{\, n' \mid \exists n \in \overline{n}_1.\ (n, n') \in [\![\mathit{Step}]\!]_{\mathrm{apply}(\eta_1)} \,\}$$

By induction, (0), (3), and (2) imply the following properties:

Approximation – induction:
$\mathbf{r} \supseteq_{\eta_1} \overline{n}_1$

Immutability – induction:
$\mathbf{c}\#\mathbf{u} \;\Rightarrow\; \eta_0 \sim_{\mathbf{c}} \eta_1$
$\mathbf{u} \supseteq_{\eta_1} \mathit{updated}(\eta_1 \setminus \eta_0)$

Parallel Evolution – induction:
$\eta_0' \sim_{\mathbf{a}} \eta_0 \;\wedge\; N_0' \# (N_1 \setminus N_0)$
$\Rightarrow\; \exists \eta_1' \;(\; dEnv \vdash \eta_0'; Expr \Rightarrow \eta_1'; \bar{n}_1$
$\wedge\, \eta_1' \setminus \eta_0' = \eta_1 \setminus \eta_0 \;)$

Now we can prove the three properties. Immutability is trivial. Approximation and parallel evolution are less trivial.

Parallel Evolution. We first introduce some notation. We use here a new atomic update record `R-delete`(n) whose effect is opposite to `R-insert`, in the same way as `delete` is opposite to `insert`. We could do without, but proofs would become very heavy.

Definition 16.
$$[\![Step]\!]^n_\sigma =_{def} \{\, n' \mid (n, n') \in [\![Step]\!]_{\sigma'} \,\}$$

Definition 17 (*deepcopy*$_{\sigma,\sigma'}(n)$, *refresh*$_{\sigma,\sigma'}(n)$).
deepcopy$_{\sigma,\sigma'}(n)$ *is the following composite update:*
$$\texttt{create}(\bar{m}_d, F_{copy}), \texttt{insert}(E_{copy})$$
where
$$(\bar{m}, \bar{m}_d, E_{copy}, F_{copy}) = \textit{prepare-deep-copy}(\textit{apply}(\eta_2), \bar{n})$$
refresh$_{\sigma,\sigma'}(n)$ *is defined by cases.*

– *If n has a parent n_p in σ, then refresh$_{\sigma,\sigma'}(n)$ is the following composite update:*
$$\texttt{delete}(n), \textit{deepcopy}_{\sigma,\sigma'}(n), \texttt{insert}(n_p, \textit{map}(n))$$
– *If n is a root that is mapped by R, then refresh$_{\sigma,\sigma'}(n)$ is:*
$$\texttt{R-delete}(n), \textit{deepcopy}_{\sigma,\sigma'}(n), \texttt{R-insert}(\textit{map}(n), \textit{loc}(n)).$$
– *Otherwise, refresh$_{\sigma,\sigma'}(n)$ is:*
$$\textit{deepcopy}_{\sigma,\sigma'}(n)$$

Lemma 4. *For any n, η, η', such that $wf(\eta)$ and $wf(\eta')$:*
$wf(\eta, \textit{deepcopy}_{\eta,\eta'}(n))$, $wf(\eta, \textit{deepcopy}_{\eta',\eta}(n))$,
$wf(\eta, \textit{refresh}_{\eta,\eta'}(n))$, $wf(\eta, \textit{refresh}_{\eta',\eta}(n))$.

Observe that, after a store σ goes through a *refresh*$_{\sigma,\sigma'}(n)$, every path expression retains the same semantics, but all and only the descendants-or-self m of n are substituted by $\textit{map}(m)$; if we extend *map* with the identity on all the nodes where it is undefined, we have:
$$[\![\mathbf{r}]\!]_{\mathrm{apply}((\sigma, \textit{refresh}_{\sigma,\sigma'}(n)))} = \textit{map}([\![\mathbf{r}]\!]_\sigma)$$

Refresh gives us an easy way to prove that every node that is reached by a path $\mathbf{p}$ in a store has the same ascendants in any other $\mathbf{p}$-similar store, (fact (c) below), and other similar properties of the equivalence.

Lemma 5.

$$mE^*_\sigma n \;\Rightarrow\; n \notin \llbracket \mathbf{r} \rrbracket_{apply((\sigma, refresh_{\sigma,\sigma'}(m), refresh_{\sigma',\sigma}(m)))} \tag{a}$$

$$n \in \llbracket \mathbf{r} \rrbracket_\sigma \wedge n \notin \llbracket \mathbf{r} \rrbracket_{apply((\sigma, refresh_{\sigma,\sigma'}(m), refresh_{\sigma',\sigma}(m)))} \;\Rightarrow\; mE^*_\sigma n \tag{b}$$

$$\sigma \sim_{\mathbf{p}} \sigma' \wedge (m,n) \in E^*_\sigma \wedge n \in \llbracket \mathbf{p} \rrbracket_\sigma \;\Rightarrow\; (m,n) \in E^*_{\sigma'} \tag{c}$$

$$\begin{aligned} &wf(\sigma,\Delta) \wedge wf(\sigma',\Delta) \wedge \Delta = \textit{no-delete}(\Delta) \\ &\wedge \sigma \sim_{\mathbf{p}|\mathbf{q}} \sigma' \wedge (m,n) \in E^*_\sigma \wedge m \in \llbracket \mathbf{p} \rrbracket_{apply(\sigma,\Delta)} \wedge n \in \llbracket \mathbf{q} \rrbracket_{apply(\sigma,\Delta)} \\ &\Rightarrow\; (m,n) \in E^*_{\sigma'} \end{aligned} \tag{d}$$

$$\sigma \sim_{\mathbf{p}|\mathbf{q}} \sigma' \wedge m \in \llbracket \mathbf{p} \rrbracket_\sigma \wedge n \in \llbracket \mathbf{q} \rrbracket_\sigma \wedge (m,n) \in E_\sigma \wedge (m',n) \in E_{\sigma'} \;\Rightarrow\; m = m' \tag{e}$$

Proof. The statement of (a) and (b) is strange, since (a) and (b) would already hold in the simpler case $\llbracket \mathbf{r} \rrbracket_{\mathrm{apply}((\sigma, refresh_{\sigma,\sigma'}(m)))}$. The second component $refresh_{\sigma',\sigma}(m)$ is needed when (a) and (b) are used to prove (c).
(a): by construction, $refresh_{\sigma,\sigma'}(m)$ makes m and all of its descendants unreachable.
(b): any path to n in σ has a corresponding path in $\mathrm{apply}((\sigma, refresh_{\sigma,\sigma'}(m), refresh_{\sigma',\sigma}(m)))$, and that path ends in n, unless n was a descendant (or self) of m, in which case the path exists but ends in the fresh copy of n.
(c): By (a) and $(m,n) \in E^*_\sigma$: $n \notin \llbracket \mathbf{p} \rrbracket_{\mathrm{apply}((\sigma, refresh_{\sigma,\sigma'}(m), refresh_{\sigma',\sigma}(m)))}$
By $\sigma \sim_{\mathbf{p}} \sigma'$ and $n \in \llbracket \mathbf{p} \rrbracket_\sigma$: $n \in \llbracket \mathbf{p} \rrbracket_{\sigma'}$ and $n \notin \llbracket \mathbf{p} \rrbracket_{\mathrm{apply}((\sigma', refresh_{\sigma,\sigma'}(m), refresh_{\sigma',\sigma}(m)))}$
By commutativity of $refresh_{\sigma,\sigma'}(m)$ and $refresh_{\sigma',\sigma}(m)$:

$n \in \llbracket \mathbf{p} \rrbracket_{\sigma'}$ and $n \notin \llbracket \mathbf{p} \rrbracket_{\mathrm{apply}((\sigma', refresh_{\sigma',\sigma}(m), refresh_{\sigma,\sigma'}(m)))}$

By (b): $(m,n) \in E^*_{\sigma'}$
(d): By $(m,n) \in E^*_\sigma$: $(m,n) \in E^*_{\mathrm{apply}(\sigma,\Delta)}$
By (c) and $n \in \llbracket \mathbf{q} \rrbracket_{\mathrm{apply}(\sigma,\Delta)}$: $(m,n) \in E^*_{\mathrm{apply}(\sigma',\Delta)}$
Assume $(m,n) \notin E^*_{\sigma'}$, for a contradiction; then, $\exists (o_p, o_c) \in E_{\mathrm{apply}(\sigma',\Delta)}$ such that $(m, o_c) \in E^+_{\mathrm{apply}(\sigma',\Delta)}$ and $(o_c, n) \in E^*_{\mathrm{apply}(\sigma',\Delta)}$ and o_c has no father in E^*_σ
By (c) and $(o_c, n) \in E^*_{\mathrm{apply}(\sigma',\Delta)}$: $(o_c, n) \in E^*_{\mathrm{apply}(\sigma,\Delta)}$
By $(m,n) \in E^*_\sigma$, hence $(m,n) \in E^*_{\mathrm{apply}(\sigma,\Delta)}$ but the $m - n$ chain does not go through o_c: $(o_c, m) \in E^*_{\mathrm{apply}(\sigma,\Delta)}$
By (c) and $m \in \llbracket \mathbf{p} \rrbracket_{\mathrm{apply}(\sigma,\Delta)}$: $(o_c, m) \in E^*_{\mathrm{apply}(\sigma',\Delta)}$
Hence we have $(m, o_c) \in E^+_{\mathrm{apply}(\sigma',\Delta)}$ and $(o_c, m) \in E^*_{\mathrm{apply}(\sigma',\Delta)}$ which is a contradiction
(e): By (c), $\sigma \sim_{\mathbf{p}|\mathbf{q}} \sigma'$, $(m,n) \in E_\sigma$ and $n \in \llbracket \mathbf{q} \rrbracket_\sigma$: $mE^*_{\sigma'} n$.
By $m \neq n$: $mE^+_{\sigma'} n$; by $(m',n) \in E_{\sigma'}$: $mE^*_{\sigma'} m'$ (1)
By (c), $\sigma \sim_{\mathbf{p}|\mathbf{q}} \sigma'$, $(m',n) \in E_{\sigma'}$ and $n \in \llbracket \mathbf{q} \rrbracket_\sigma$: $m'E^*_\sigma n$
By $m' \neq n$: $m'E^+_\sigma n$; by $(m,n) \in E_\sigma$: $m'E^*_\sigma m$
By (c), $\sigma \sim_{\mathbf{p}|\mathbf{q}} \sigma'$, $m'E^*_\sigma m$, and $m \in \llbracket \mathbf{p} \rrbracket_\sigma$: $m'E^*_{\sigma'} m$
By $mE^*_{\sigma'} m'$ (1) and $m'E^*_{\sigma'} m$: $m = m'$.

The kernel of the parallel evolution proof is in the following lemma that says that, if two stores are equivalent on $\mathbf{r}/Step$, then, from each single node reached by $\mathbf{r}$, the step *Step* reaches the same set of nodes in the two stores.

Lemma 6.

$$\begin{array}{l} \sigma \sim_{\mathbf{r}/Step} \sigma' \ \wedge\ n \in [\![\mathbf{r}]\!]_{apply(\sigma,\Delta)} \\ \wedge\, \Delta = \mathtt{insert}(E_1),\ldots,\mathtt{insert}(E_n) \\ \Rightarrow\ [\![Step]\!]^n_\sigma = [\![Step]\!]^n_{\sigma'} \end{array}$$

Proof. $\sigma \sim_{\mathbf{r}/Step} \sigma'$ (1) implies (2) $\sigma \sim_{\mathbf{r}} \sigma'$. Consider any $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta)}$. We reason by cases on the axis. In each case, for each m in $[\![Step]\!]^n_\sigma$, it immediately satisfies *ntest* in $F_{\sigma'}$, but we have to prove that $E_{\sigma'}$ relates m and n as required by the axis. By (2) $\exists \Delta' \subseteq \Delta$ such that $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta')}$ and $wf(\sigma',\Delta')$. Throughout the proof we use the fact that, since $\Delta = \mathtt{insert}(E_1),\ldots,\mathtt{insert}(E_n)$, for both σ and σ' we have $[\![\mathbf{p}]\!]_{\sigma''} \subseteq [\![\mathbf{p}]\!]_{\mathrm{apply}(\sigma'',\Delta')}$. We use $E_{\Delta'}$ for the set of edges added by Δ'.

child :: *ntest*, which we abbreviate as *ntest*: We have $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta')}$ and want to prove that $(n,m) \in E_\sigma \ \Rightarrow\ (n,m) \in E_{\sigma'}$.

From $(n,m) \in E_\sigma$ we obtain $(n,m) \in E_{\mathrm{apply}(\sigma,\Delta')}$ (and $(n,m) \notin E_{\Delta'}$) hence $m \in [\![\mathbf{r}/ntest]\!]_{\mathrm{apply}(\sigma,\Delta')}$, hence $m \in [\![\mathbf{r}/ntest]\!]_{\mathrm{apply}(\sigma',\Delta')}$, hence $\exists n' \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma',\Delta')}$ such that $(n',m) \in E_{\mathrm{apply}(\sigma',\Delta')}$.
By $wf(\sigma',\Delta')$, we have that $\mathrm{apply}(\sigma,\Delta') \sim_{\mathbf{r}|(\mathbf{r}/ntest)} \mathrm{apply}(\sigma',\Delta')$, hence we can apply Lemma 5(e) to $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta')}$, $m \in [\![\mathbf{r}/ntest]\!]_{\mathrm{apply}(\sigma,\Delta')}$, $(n,m) \in E_{\mathrm{apply}(\sigma,\Delta')}$, $(n',m) \in E_{\mathrm{apply}(\sigma',\Delta')}$ hence deducing $n = n'$, hence $(n,m) \in E_{\mathrm{apply}(\sigma',\Delta')}$. From $(n,m) \notin E_{\Delta'}$, we obtain $(n,m) \in E_{\sigma'}$.

parent :: *ntest*: We have $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta')}$ and want to prove that $(m,n) \in E_\sigma \ \Rightarrow\ (m,n) \in E_{\sigma'}$.

$(m,n) \in E_\sigma \ \Rightarrow\ (m,n) \in E_{\mathrm{apply}(\sigma,\Delta')}$ and $(m,n) \notin E_{\Delta'}$. By $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta')}$ we have $m \in [\![\mathbf{r}/parent :: ntest]\!]_{\mathrm{apply}(\sigma,\Delta')}$. By Lemma 5(d), $(m,n) \in E_\sigma$, $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta')}$, $m \in [\![\mathbf{r}/parent :: ntest]\!]_{\mathrm{apply}(\sigma,\Delta')}$, imply $(m,n) \in E^+_{\sigma'}$, hence $\exists m'.\ (m',n) \in E_{\sigma'}$.
$(m,n) \in E_{\sigma'} \ \Rightarrow\ (m,n) \in E_{\mathrm{apply}(\sigma',\Delta')}$, hence, by Lemma 5(e), $m = m'$, hence $(m,n) \in E_{\sigma'}$.

descendant :: *ntest*: We have $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta')}$ and want to prove that $(n,m) \in E^+_\sigma \ \Rightarrow\ (n,m) \in E^+_{\sigma'}$.
$(n,m) \in E^+_\sigma \ \Rightarrow\ (n,m) \in E^+_{\mathrm{apply}(\sigma,\Delta')}$ hence $m \in [\![\mathbf{r}//ntest]\!]_{\mathrm{apply}(\sigma,\Delta')}$.
From Lemma 5(d) we deduce $(n,m) \in E^+_{\sigma'}$.

ancestor :: *ntest*: We have $n \in [\![\mathbf{r}]\!]_{\mathrm{apply}(\sigma,\Delta')}$ and want to prove that $(m,n) \in E^+_\sigma \ \Rightarrow\ (m,n) \in E^+_{\sigma'}$.
$(m,n) \in E^+_\sigma \ \Rightarrow\ (m,n) \in E^+_{\mathrm{apply}(\sigma,\Delta')}$ hence $m \in [\![\mathbf{r}/ancestor :: ntest]\!]_{\mathrm{apply}(\sigma,\Delta')}$. From Lemma 5(d) we deduce $(m,n) \in E^+_{\sigma'}$.

We can now prove parallel evolution. We want to prove:
$\eta'_0 \sim_{\mathrm{pref}(\mathbf{r}/Step)|\mathbf{a}} \eta_0 \ \Rightarrow\ dEnv \vdash \eta'_0; Expr/Step \Rightarrow \eta'_1; \bar{n}$
where
$\bar{n} = \{\, n' \mid \exists n \in \bar{n}_1.\ n' \in [\![Step]\!]^n_{\mathrm{apply}(\eta'_1)} \,\}$.
By induction we have:

$\mathbf{r} \supseteq_{\eta_1} \bar{n}_1$

$\eta'_0 \sim_{\mathbf{a}} \eta_0 \ \wedge\ N'_0 \# (N_1 \setminus N_0)$

$\Rightarrow\ \exists\eta'_1\ (\ dEnv \vdash \eta'_0; Expr \Rightarrow \eta'_1; \bar{n}_1\ \wedge\ \eta'_1 \setminus \eta'_0 = \eta_1 \setminus \eta_0\ )$

By induction, $\eta'_1 \setminus \eta'_0 = \eta_1 \setminus \eta_0$. Hence, we only have to prove $\{n' \mid \exists n \in \bar{n}_1.\ n' \in [\![Step]\!]^n_\sigma\} = \{n' \mid \exists n \in \bar{n}_1.\ n' \in [\![Step]\!]^n_{\sigma'}\}$.
The equivalence $\eta'_0 \sim_{\mathrm{pref}(\mathbf{r}/Step)|\mathbf{a}} \eta_0$ implies $\eta'_0 \sim_{\mathbf{r}|(\mathbf{r}/Step)} \eta_0$ hence $(\eta'_0, \eta'_1 \setminus \eta'_0) \sim_{\mathbf{r}|(\mathbf{r}/Step)} (\eta_0, \eta'_1 \setminus \eta'_0)$ hence, by $\eta'_1 \setminus \eta'_0 = \eta_1 \setminus \eta_0$, $\eta'_1 \sim_{\mathbf{r}|(\mathbf{r}/Step)} \eta_1$. Let $E^d_{\eta_1}$ be the set of edges deleted by all the `delete` in η_1. Then $\mathrm{mrg}(\eta_1) = \mathrm{apply}(\mathrm{apply}(\eta_1), \texttt{insert}(E^d_{\eta_1}))$, hence, by Lemma 6, for each $n \in \mathrm{mrg}(\eta_1)$ we have $[\![Step]\!]^n_{\mathrm{apply}(\eta_1)} = [\![Step]\!]^n_{\mathrm{apply}(\eta'_1)}$, hence:

$$\bar{n}_1 \subseteq [\![\mathbf{r}]\!]_{\mathrm{mrg}(\eta_1)} \ \Rightarrow\ \bigcup_{n\in\bar{n}_1} [\![Step]\!]^n_{\mathrm{apply}(\eta_1)} = \bigcup_{n\in\bar{n}_1} [\![Step]\!]^n_{\mathrm{apply}(\eta'_1)}$$

C Commutativity proof

Lemma 7 (Prefix closure of a). pEnv $\vdash Expr \Rightarrow \mathbf{r};\ \langle \mathbf{a}, \mathbf{u}\rangle\ \Rightarrow\ prefclosed(\mathbf{a})$

Theorem

Let
(h1-a) $dEnv \vdash \eta; Expr_1 \Rightarrow \eta_1; \bar{n}_1$
(h1-b) $\mathbf{pEnv} \vdash Expr_1 \Rightarrow \mathbf{r}_1;\ \langle \mathbf{a}_1, \mathbf{u}_1\rangle$
(h1-c) $\mathbf{pEnv} \supseteq_\eta dEnv$
(h2-a) $dEnv \vdash \eta_1; Expr_2 \Rightarrow \eta_{12}; \bar{n}_2$
(h2-b) $\mathbf{pEnv} \vdash Expr_2 \Rightarrow \mathbf{r}_2;\ \langle \mathbf{a}_2, \mathbf{u}_2\rangle$
hence $dEnv \vdash \eta; Expr_1, Expr_2 \Rightarrow \eta_{12}; \bar{n}_2, \bar{n}_2 \ \wedge\ \mathbf{pEnv} \vdash Expr_1, Expr_2 \Rightarrow \mathbf{r}_1|\mathbf{r}_2;\ \langle \mathbf{a}_1|\mathbf{a}_2, \mathbf{u}_1|\mathbf{u}_2\rangle$
If
(h3) $\mathbf{u}_1 \# \mathbf{a}_2, \mathbf{a}_1 \# \mathbf{u}_2, \mathbf{u}_1 \# \mathbf{u}_2$,
(h4) $\mathrm{apply}(\eta') = \mathrm{apply}(\eta)$ and $\mathrm{mrg}(\eta') = \mathrm{mrg}(\eta)$,
then exists η'_{21}, such that:
(t1) $dEnv \vdash \eta'; Expr_2, Expr_1 \Rightarrow \eta'_{21}; \bar{n}_2, \bar{n}_1$
(t2) $\mathrm{apply}(\eta_{12}) = \mathrm{apply}(\eta'_{21})$ and $\mathrm{mrg}(\eta_{12}) = \mathrm{mrg}(\eta'_{21})$.

Throughout this section we use N_i for the set of nodes of store history η_i and N'_i for the set of nodes of store history η'_i.

Proof We will prove that there exist η'_2, η'_{21}, such that:
$dEnv \vdash \eta'; Expr_2 \Rightarrow \eta'_2; \bar{n}_2$
$dEnv \vdash \eta'_2; Expr_1 \Rightarrow \eta'_{21}; \bar{n}_1$
hence
$dEnv \vdash \eta'; Expr_2, Expr_1 \Rightarrow \eta'_{21}; \bar{n}_2, \bar{n}_1$
and such that $\mathrm{mrg}(\eta_{12}) = \mathrm{mrg}(\eta'_{21})$.

First observe that, by Lemma 7, both $\mathbf{a}_1$ and $\mathbf{a}_2$ are prefix-closed. We will use this fact whenever we apply immutability.

We will use (h4) to transfer implicitly most facts about η to η', because (h4) implies that: $\forall \mathbf{p}, \eta''\ \eta \sim_\mathbf{p} \eta'' \ \Leftrightarrow\ \eta' \sim_\mathbf{p} \eta''$;

$N = N'$;
pEnv $\supseteq_{\eta'}$ *dEnv*
We also observe that, by stability, (h1-c) implies:
(h2-c) **pEnv** $\supseteq_{\eta_1}$ *dEnv*

By $\mathbf{u}_1\#\mathbf{a}_2$, (h1-abc) and immutability we have that
(h1-imm-a) $\eta \sim_{\mathbf{a}_2} \eta_1$
(h1-imm-b) $\mathbf{u}_1 \supseteq_{\eta_1} \mathit{updated}(\eta_1 \setminus \eta)$
hence:
(h1-imm-b') $\mathbf{u}_1 \supseteq_{\eta_{12}} \mathit{updated}(\eta_1 \setminus \eta)$
Similarly, by $\mathbf{u}_2\#\mathbf{a}_1$, (h2-abc), and immutability we have that
(h2-imm-a) $\eta_1 \sim_{\mathbf{a}_1} \eta_{12}$
(h2-imm-b) $\mathbf{u}_2 \supseteq_{\eta_{12}} \mathit{updated}(\eta_{12} \setminus \eta_1)$
By (h1-imm-b'), (h2-imm-b), and $\mathbf{u}_1\#\mathbf{u}_2$
(tgt-disj) $(\eta_1 \setminus \eta)\#(\eta_{12} \setminus \eta_1)$

By (h1-imm-a), i.e. $\eta \sim_{\mathbf{a}_2} \eta_1$, (h2-abc), $(N_{12} \setminus N_1)\#N$, and parallel evolution, we have:
$\exists \eta'_2$.
(h2-p-ev-a) $\mathit{dEnv} \vdash \eta'; \mathit{Expr}_2 \Rightarrow \eta'_2; \overline{n}_2$
(h2-p-ev-b) $\eta'_2 \setminus \eta' = \eta_{12} \setminus \eta_1$
(h2-p-ev-b) implies:
(h2-p-ev-c) $N'_2 \setminus N' = N_{12} \setminus N_1$.

Now, we can apply immutability to (h2-p-ev-a), (h2-b), (h1-c) and $\mathbf{a}_1\#\mathbf{u}_2$, and obtain:
(h2-imm-2) $\eta' \sim_{\mathbf{a}_1} \eta'_2$

By stability, $\mathrm{mrg}(\eta') = \mathrm{mrg}(\eta)$ and (h1-c) imply:
(sta-1) **pEnv** $\supseteq_{\eta'_2}$ *dEnv*
From $(N_1 \setminus N)\#(N_{12} \setminus N_1)$, $(N'_2 \setminus N') = (N_{12} \setminus N_1)$ we derive $(N_1 \setminus N)\#(N'_2 \setminus N')$, hence
(disj) $(N_1 \setminus N)\#N'_2$.

Property (h2-imm-2) implies $\eta'_2 \sim_{\mathbf{a}_1} \eta$; and thanks to (h1-b), (sta-1), (disj), we can apply parallel evolution in order to transfer the (h1-a) reduction (η to η_1) into a reduction from η'_2 to a η'_{21}, and obtain:
$\exists \eta'_{21}$.
(h1-p-ev-a) $\mathit{dEnv} \vdash \eta'_2; \mathit{Expr}_1 \Rightarrow \eta'_{21}; \overline{n}_1$
(h1-p-ev-b) $\eta'_{21} \setminus \eta'_2 = \eta_1 \setminus \eta$.

Now, we can prove the thesis.

(t1): follows from (h2-p-ev-a) and (h1-p-ev-a)

(t2): Recall (h2-p-ev-b) and (h1-p-ev-b):
$\eta'_2 \setminus \eta' = \eta_{12} \setminus \eta_1, \quad \eta'_{21} \setminus \eta'_2 = \eta_1 \setminus \eta$
Hence, if we let $\Delta_1 = \eta_1 \setminus \eta$ and $\Delta_2 = \eta_{12} \setminus \eta_1$:

$\eta'_{21} = (\sigma', (\Delta', \Delta_2, \Delta_1)), \quad \eta_{12} = (\sigma, (\Delta, \Delta_1, \Delta_2))$
Hence:
$\mathrm{mrg}(\eta'_{21}) = \mathrm{apply}(\mathrm{apply}(\mathrm{mrg}(\eta'), \Delta_2), \Delta_1)$
By (tgt-disj) and by property 1:
$= \mathrm{apply}(\mathrm{apply}(\mathrm{mrg}(\eta'), \Delta_1), \Delta_2) = \mathrm{apply}(\mathrm{apply}(\mathrm{mrg}(\eta), \Delta_1), \Delta_2) = \mathrm{mrg}(\eta_{12})$.

It is worth noticing that the hypothesis $\mathbf{u}_1 \# \mathbf{a}_2$ and $\mathbf{a}_1 \# \mathbf{u}_2$ have been used to prove that, by commuting $Expr_1$ with $Expr_2$ we transform $(\sigma, (\Delta, \Delta_1, \Delta_2))$ into $(\sigma', (\Delta', \Delta'_2, \Delta'_1))$ where Δ_i is identical to Δ'_i. The further hypothesis $\mathbf{u}_1 \# \mathbf{u}_2$ is only needed to exchange the order of Δ_1 and Δ_2.