# Extracting Dataflow Communication from Object-Oriented Code

**Radu Vanciu** **Marwan Abi-Antoun**

Posted: Oct. 15, 2011; Last updated: July 11, 2012

Department of Computer Science
Wayne State University
Detroit, MI 48202

**Abstract**

Object graphs help developers understand the runtime structure of an object-oriented system, in terms of objects and their runtime relations (points-to, call, or dataflow, depending on the intent of the diagram). Ideally, an object graph is sound and shows all possible objects and the relations between them. The object graph should also be hierarchical to scale and convey architectural abstraction. Achieving soundness requires a static analysis, but architectural hierarchy is not available in code written in general-purpose programming languages. To achieve hierarchy in a statically extracted object graph, we leverage ownership types in the code. We then abstractly interpret the annotated program and extract a global, sound, hierarchical object graph with dataflow communication edges that show the flow of objects due to field reads, field writes, and method invocations. We formalize the static analysis using a constraint-based specification and prove that the object graph is sound.

**Keywords:** hierarchical object graphs, dataflow communication, ownership domains

# Document History

| Date | Version | Description |
| --- | --- | --- |
| Oct. 15, 2011 | 1.0 | Initial posting |
| Feb. 15, 2012 | 1.1 | Added to discussion of recursion (Section 4.2) |
| | | Fixed Df-New |
| | | Included a detailed abstract interpretation of QuadTree |
| Mar. 9, 2012 | 1.2 | Simplified static rules |
| | | Removed $O_{id}$ from `OObject` definition |
| | | Distinguished import and export edges in `OEdge` definition |
| May 11, 2012 | 1.3 | fixed IRC-Context and adapted the proof accordingly |
| | | in QuadTree example, use default constructor instead of `ctor` |
| July 11, 2012 | 1.4 | Use $O_{world}$ instead of $O_{root}$ to start the analysis |
| | | use $O_{world}$ in QuadTree |
| | | fixed *init* in transfer functions |

# Contents

# List of Figures

# 1 Introduction

During software evolution, reverse-engineered diagrams of the code structure and of the runtime structure help developers to understand the system in order to modify it. Diagrams of the code structure are supported by many tools. Diagrams of the runtime structure, however, are more challenging and less mature.

One challenge with diagrams of the runtime structure is soundness, i.e., showing all possible objects and all possible relations between them. Achieving soundness requires static analysis since, by definition, dynamic analysis shows partial diagrams from a finite number of executions. Another challenge is to create a graph that scales and supports program understanding. A flat object graph, with its profusion of objects, does not meet this challenge. One solution is to use hierarchy, which provides both high-level and detailed understanding.

Architectural hierarchy is not observable in legacy object-oriented code, so we follow a previous approach [2] and use ownership types in the code, specifically, the Ownership Domains type system [4]. To support legacy code, we define annotations that implement the type system, using available language support for annotations. Developers use the annotations and specify, within the code, their design intent in the form of strict encapsulation, logical containment and architectural tiers. These annotations enable a static analysis to extract a sound, global, hierarchical Ownership Object Graph (OOG) [2]. An OOG provides architectural abstraction by ownership hierarchy and by types, where architecturally significant objects appear near the top of the hierarchy and data structures are further down.

In related work, we evaluated in a controlled experiment if OOGs, as diagrams of the runtime structure, help developers with program comprehension during coding activities, and thus complement widely-used class diagrams [7, 6]. We found that developers who used OOGs succeeded on code modification tasks, took less time, or explored less irrelevant code compared to developers who used only class diagrams or who just explored the code. In our previous experiment, developers wondered why the OOG did not show some relations between objects. The OOG showed only points-to edges due to field references that capture persistent relations between objects. In addition to points-to edges, developers need usage edges that capture more transient relations between objects [12]. In this paper, we add to the OOG usage edges that make visually obvious the flow of objects in the program, and that we refer to as dataflow communication.

For instance, in object-oriented code that implements the Observer design pattern, understanding “what” gets notified during a change notification is crucial for understanding the system. “What” does not usually mean a class, “what” means a particular instance. Indeed, with many design patterns, developers need to understand the various instances in the system, and object graphs give insights into instances better than class diagrams. To understand what instances point to what other instances, points-to edges are useful. To understand not just “what” gets notified but also “what kind” of notification the subject of the notification sends to its observers, usage edges may be useful.

**Contributions.** In this paper, we propose a static analysis to extract a hierarchical object graph with usage edges showing dataflow communication. Our contributions are:

- We formalize the analysis using a constraint-based specification, showing the static and dynamic semantics;
- We prove the soundness of the extracted object graph;
- We evaluate our analysis on an extended example; we compare an OOG with dataflow edges to a diagram of the runtime structure with dataflow communication drawn by an expert, and to an OOG with points-to edges.

**Outline.** The rest of this report is organized as follows. In Section 2, we describe the challenges of designing a static analysis that extracts a runtime structure. In Section 3, we define dataflow communication. In Section 4, we formalize our analysis, and prove its soundness. We introduce a small example, and describe the analysis on a worked example in Section 6. We discuss related work in Section 7 and conclude.

## 2 Challenges of Static Analysis

We first discuss the challenges of extracting object graphs statically. At runtime, the structure of an object-oriented program can be represented as a Runtime Object Graph (ROG), where nodes represent objects, i.e., instances of classes, and edges represent relations between objects, such as one object calling another object's methods. A sound static analysis extracts an object graph that approximates all possible ROGs, for any program execution. We represent the extracted object graph as an OGraph, where nodes are OObjects and edges are OEdges (Fig. 4). An OObject is a canonical object that represents multiple runtime objects. Similarly, an OEdge is a canonical edge that represents runtime dataflow communication between the corresponding runtime objects. An OGraph is an approximation because multiple runtime edges could have the same representative, or an OGraph might have some representatives that do not come from any real runtime edge. The OGraph is unsound if one runtime object or one runtime edge would have two representatives in the OGraph.

**Object soundness.** The OGraph must show a unique representative for each runtime object. While one OObject can represent multiple runtime objects, the same runtime object cannot map to two separate OObjects. It would be misleading to have one runtime entity appear as two components on an architectural diagram. Then one could assign the two components different values for a key trustLevel property and potentially invalidate the analysis results. In particular, object soundness handles aliasing by enforcing the unique representatives invariant. For two variables that may alias and refer to the same runtime object, the analysis must create a single OObject.

**Edge soundness.** If we were able to observe the ROGs for all possible executions, and there is a runtime dataflow edge between two runtime objects, the OGraph must show an OEdge between the representatives of these objects.

**Summarization.** An ROG can have an unbounded number of runtime objects. For example, in the presence of recursive types, the ROG might have an unbounded depth. The OGraph must be a finite representation of all ROGs and must have a finite depth. The static analysis must stop creating new nodes in the OGraph at some level, and instead use already created nodes. A common heuristic is for the analysis to stop when it gets to a node of the same type as a node it previously created.

**Hierarchy.** A global OGraph must show architecturally significant OObjects near the top of the hierarchy and OObjects representing implementation details further down.

```
class Main{
  A a;  C c;
  void main(){
    main = new Main();
    main.run();
  }
  void run(){
    a = new A(c);
    //no dataflow communication
    a.m1(); //method call
  }
}
```

```
class A{
  B b; C c; D d; E e;
  A(C c){
   //no dataflow communication
   //field initialization
    this.c = c;
  }
  void m1(){
  //method call (a -B-> d)
    d.setB(b);
  }
  B m2(){
  //method call (d -B-> a)
    return d.getB();
  }
  C m3(){
  //field read (b -C-> a)
    return b.c;
  }
  void m4(){
  //field write (a -C-> b)
    b.c = c;
  }
  D m5(){
  //method call(a -B-> e, a -C-> e, e -D-> a)
    return e.me(b,c);
  }
}
```

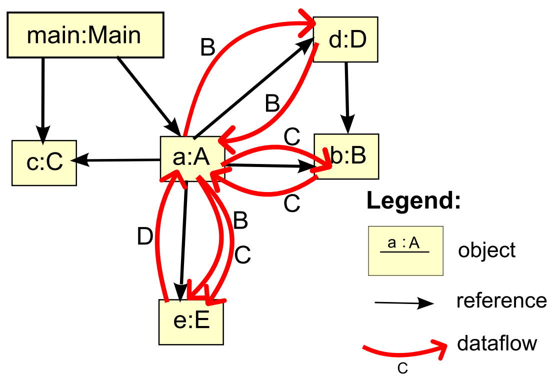



**Figure 1:** Example of export and import dataflow communication.

**Precision.** The analysis must not merge objects excessively. For example, an OGraph that represents all the runtime objects with one OObject is sound but imprecise. Ideally, an OGraph must have no more OEdges than soundness requires. Like any sound static analysis, however, an OGraph may have false positives and show OObjects or OEdges that do not correspond to runtime objects or runtime relations, due to infeasible paths in the program.

**Support for legacy code.** To reverse engineer an OGraph from legacy code, an analysis should not require writing the program in a specific language, such as ArchJava [5] or reengineering legacy code, which is hard [3]. Instead, the analysis should take advantage of available language support for annotations.

## 3 Dataflow Communication

**Definition of dataflow communication:** *Let `a` and `b` be two objects. Dataflow communication exists from `a` to `b` if `a` reads or writes to `b`'s fields or calls `b`'s methods.* In object-oriented code, field writes, field reads, or method invocations lead to dataflow communication. Since the flow can be bidirectional, we distinguish between *import* and *export* dataflow.

**Import dataflow communication:** *An import dataflow communication exists from the source object `b:B` to the destination object `a:A` if `a` receives data from `b`.* That is, there is a method `ma` of $A$ such that `ma` refers to `b.f` or uses the result returned by a method `mb` of `B`.

**Export dataflow communication:** *An export dataflow communication exists from the source object `a:A` to the destination object `b:B` if one of `b`'s field `f` may be modified when one of `a`'s methods is invoked.* That is, there is a method `ma` of `a` such that `ma` contains the field write `b.f = c` or `b.mb(c)`, where `c` is a field of `A`, an argument of `ma`, an object instantiated by `ma`, or an object returned by another method invoked by `ma`. In this paper, when the kind of the edge is clear, we refer to import and export dataflow communication edges simply as import and export edges. To understand the above definitions, consider the example in Figure 1, which has the code for the classes `Main` and `A`, and the corresponding flat object graph. For brevity consider that all the variables are correctly initialized, we do not include the code for the classes `B..E`. In the object graph, the nodes corresponds to objects, and there are two types of edges. Straight arrows means that an object refer another object, while curved arrows correspond to dataflow communications between objects. The curve arrows are labeled with the type of the data communicated between objects.

Dataflow communication exists due to the statements of the methods of `A`, `m1()` to `m5()`. Import dataflow communication exist from `b` to `a` and from `d` to `a` due to the field read and method invocation expressions of `m3()` and `m2()`, respectively. Also, export dataflow communication exist from `a` to `b` and from `a` to `d` due to the field write and method invocation expressions of `m4()` and `m1()`, respectively. Due to only one method invocation expression in `m5()`, two export dataflow communication exist from `a` to `e`, and due to the same expression, an import dataflow communication exists from `e` to `a`.

On the other hand, in the last statement of `run()`, the invocation of `m1()` does not correspond to any import or export dataflow communication, since the method has no arguments, and it returns `void`. Also, there is no dataflow communication from `main` to `a` even though the constructor of `A` has an argument. Dataflow communication definitions ignore object allocation because we consider creation and usage of objects as separate relations, and we distinguish between field initialization in a constructor and field write. That is why, there is no dataflow communication between `main` and `a` and between `a` and `c`.

# 4 Formalization

## 4.1 Abstract Syntax

We formally describe our static analysis using Featherweight Domain Java (FDJ), which models a core of the Java language with ownership domain annotations [4]. To keep the language simple and easier to reason about, FDJ uses Featherweight Java, which ignores Java language constructs such as interfaces and static code.

We adopt the FDJ abstract syntax (Fig. 3) but with the following changes. We exclude cast expressions and domain links, which are part of FDJ, but not crucial to our discussion. We also include a field write expression $e.f = e'$, which can lead to dataflow communication. (Fig. 2)

In FDJ, $C$ ranges over class names; $T$ ranges over types; $f$ ranges over field names; $v$ ranges over values; $d$ ranges over domain names; $e$ ranges over expressions; $x$ ranges over variable names; $n$ ranges over values and variable names; $S$ ranges over stores; $\ell$ and $\theta$ ranges over locations in a store; $\theta$ represents the value of `this`; a store $S$ maps locations $\ell$ to their contents; the set of variables includes the distinguished variable `this` of type $T_{this}$ used to refer to the receiver of a method; the result of the computation is a location $\ell$, which is sometimes referred to as a value $v$; $S[\ell]$ denotes the store entry of $\ell$; $S[\ell, i]$ denotes the value of $i^{th}$ field of $S[\ell]$; $S[\ell \mapsto C\texttt{<}\overline{\ell'.d}\texttt{>}(\overline{v})]$ denotes adding an entry for location $\ell$ to $S$; $\alpha$ and $\beta$ range over formal domain parameters; $m$ ranges over method names; $p$ ranges over formal domain parameters, actual domains, or the special domain `SHARED`; the

$$\frac{\Gamma, \Sigma, \theta \vdash e : T_0 \qquad fields(T_0) = \overline{T}\ \overline{f} \qquad \Gamma, \Sigma, \theta \vdash e' : T \qquad T <: T_i}{\Gamma, \Sigma, \theta \vdash e.f_i = e' : T} \text{[T-WRITE]}$$

$$\frac{S[\ell] = C\texttt{<}\overline{p}\texttt{>}(\overline{v}) \qquad fields(C\texttt{<}\overline{p}\texttt{>}) = \overline{T}\ \overline{f} \qquad S' = S[\ell \mapsto C\texttt{<}\overline{p}\texttt{>}([v/v_i]\overline{v})]}{\ell.f_i = v; S \rightsquigarrow v; S'} \text{[R-WRITE]}$$

$$\frac{\theta \vdash e_0; S \to e_0'; S'}{\theta \vdash e_0.f_i = e_1; S \to e_0'.f_i = e_1; S'} \text{[RC-WRITE-RCV]}$$

$$\frac{\theta \vdash e_1; S \to e_1'; S'}{\theta \vdash v.f_i = e_1; S \to v.f_i = e_1'; S'} \text{[RC-WRITE-ARG]}$$

**Figure 2:** Field write semantics.

$$
\begin{array}{rcl}
CT & ::= & \overline{cdef} \\
cdef & ::= & \texttt{class}\ C\texttt{<}\overline{\alpha}, \overline{\beta}\texttt{>}\ \texttt{extends}\ C'\texttt{<}\overline{\alpha}\texttt{>} \\
 & & \{\ \overline{dom};\ \ \overline{T}\ \overline{f};\ \ C(\overline{T'}\ \overline{f'}, \overline{T}\ \overline{f}) \\
 & & \{\texttt{super}(\overline{f'}); \texttt{this}.\overline{f} = \overline{f};\}\ \ \overline{md}\ \} \\
dom & ::= & [\texttt{public}]\ \texttt{domain}\ d; \\
md & ::= & T_R\ m(\overline{T}\ \overline{x})\ \ T_{this}\ \{\texttt{return}\ e_R;\} \\
e & ::= & x\ \mid \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(\overline{e})\ \mid e.f\ \mid e.f = e' \\
 & & \mid e.m(\overline{e})\ \mid \ell\ \mid \ell \triangleright e \\
n & ::= & x \mid v \\
p & ::= & \alpha \mid n.d \mid \texttt{SHARED} \\
T & ::= & C\texttt{<}\overline{p}\texttt{>} \\
v, \ell, \theta & \in & locations \\
S & ::= & \ell \to C\texttt{<}\overline{\ell'.d}\texttt{>}(\overline{v}) \\
\Sigma & ::= & \ell \to T \\
\Gamma & ::= & x \to T
\end{array}
$$

**Figure 3:** Simplified FDJ abstract syntax [4].

expression form $\ell \triangleright e$ represents a method body $e$ executing with a receiver $\ell$; an overbar denotes a sequence; the fixed class table $CT$ maps classes to their definitions; a program is a tuple ($CT$, $e$) of a class table and an expression; $\Gamma$ is the typing context; and $\Sigma$ is the store typing.

### 4.2 Data Type Declarations

Our analysis produces a hierarchical object graph (OGraph), which has nodes representing objects (OObjects) and domains (ODomains), and edges (OEdges) representing dataflow commu-

$$
\begin{array}{lll}
G \in \mathsf{OGraph} & ::= & \langle\ \textbf{Objects} = DO,\ \textbf{DomainMap} = DD, \textbf{Edges} = DE\ \rangle \\
D \in \mathsf{ODomain} & ::= & \langle\ \textbf{Id} = D_{id},\ \textbf{Domain} = C{::}d\ \rangle \\
O \in \mathsf{OObject} & ::= & \langle\ \textbf{Type} = C{<}\overline{D}{>}\ \rangle \\
E \in \mathsf{OEdge} & ::= & \langle\ \textbf{From} = O_{src},\ \textbf{To} = O_{dst}, \textbf{Class} = C, \textbf{Flag} = Imp\ | Exp\ \rangle \\
DD & ::= & \emptyset\ \mid\ DD \cup \{\ (O, C{::}d) \mapsto D\ \} \\
DO & ::= & \emptyset\ \mid\ DO \cup \{\ O\ \} \\
DE & ::= & \emptyset\ \mid\ DE \cup \{\ E\ \} \\
\Upsilon & ::= & \emptyset\ \mid\ \Upsilon \cup \{\ C{<}\overline{D}{>}\ \} \\
H & ::= & \emptyset\ \mid\ H \cup \{\ \ell \mapsto O\ \} \\
K & ::= & \emptyset\ \mid\ K \cup \{\ \ell.d \mapsto D\ \} \\
L_I & ::= & \emptyset\ \mid\ L_I \cup \{\ (\ell_{src}, \ell_{dst}) \mapsto \{E\}\} \\
L_E & ::= & \emptyset\ \mid\ L_E \cup \{\ (\ell_{src}, \ell_{dst}) \mapsto \{E\}\}
\end{array}
$$

**Figure 4:** Data type declarations for the OGraph.

nication (Fig. 4). The OGraph is a triplet $G = \langle DO, DD, DE\rangle$, where $DO$ is a set of OObjects, $DD$ maps a pair $(O, C{::}d)$ to an ODomain $D$, and $DE$ is a set of dataflow edges. Each $E$ in $DE$ is a directed edge from a source $O_{src}$ to a destination $O_{dst}$. The label $C$ is the class of the communicated object. The flag states whether the OEdge represents an import or an export dataflow communication. Multiple edges with different labels might exists between two OObjects.

Our analysis distinguishes between different instances of the same class $C$ that are in different domains, even if created at the same `new` expression in the program. In addition, the analysis treats an instance of class $C$ with actual parameters $\overline{p}$ differently from another instance that has actual parameters $\overline{p'}$. Hence, the data type of an OObject uses $C{<}\overline{D}{>}$. We follow the FDJ convention and consider an OObject's owning ODomain as the first element $D_1$ of $\overline{D}$. Our analysis relies on the precision about aliasing that Ownership Domains offer, and avoids merging object excessively. The Ownership Domains type system guarantees that two objects in different domains cannot alias. Our analysis only merges two objects of the same class if all their domains are the same. The context $\Upsilon$ records the combination of class and domain parameters $C{<}\overline{D}{>}$ analyzed, to avoid non-termination of the analysis.

In addition to the OEdges that have source and destination OObjects, the OGraph has ownership edges. The OGraph representation is well-formed with respect to the ownership relations declared in the code using the annotations. The data type declarations of the OGraph captures this hierarchy using the $DD$ map without defining directly a set of actual domains and a set of ownership edges. An ownership edge states that an OObject $O = \langle C\texttt{<}\overline{D}\texttt{>}\rangle$ is a child of $D_1$, or that $O$ owns a domain $D$. Given a mapping $\{(O, C'::d) \mapsto D\}$ in $DD$, $D$ is a child of $O$. Since domains are inherited across classes [4], the class $C$ of $O$ can be a subclass of $C'$ where $d$ is declared.

Although a domain $d$ is declared by a class $C$, each runtime instance of type $C$ gets its own runtime domain $\ell.d$. For example, if there are two distinct object locations $\ell$ and $\ell'$ of class $C$, then $\ell.d$ and $\ell'.d$ are distinct. Since an ODomain represents a runtime domain $\ell_i.d_i$, one domain declaration $d$ in the code can create multiple ODomains $D_i$ in the OGraph and the fresh identifier $D_{id}$ ensures that multiple ODomains can be created for the same domain declaration $C::d$. Since no class declares the SHARED domain, we qualify it as ::SHARED.

During initialization, the analysis creates a global ODomain $D_{\texttt{SHARED}}$, the root of the OGraph. A developer picks a root class, $C_{root}$, and the analysis creates $O_{root}$ in $D_{\texttt{SHARED}}$. The analysis also requires an initial context. We use a dummy OObject $O_{world}$, which does not correspond to an actual runtime object. Next, the analysis changes the context from $O_{world}$ to $O_{root}$, and continues recursively with all the expressions in the methods of $C_{root}$.

**Instrumentation.** The maps $H$, $K$, $L_I$, and $L_E$ are part of the instrumented dynamic semantics (Fig. 4). $H$ maps a location $\ell$ to the corresponding OObject, and $K$ maps a runtime domain $\ell.d$ to an ODomain. The multi-valued maps $L_I$ and $L_E$ map a pair of locations ($\ell_{src}$, $\ell_{dst}$) to a set of OEdges $\{E\}$. We use two maps for edges because a pair ($H[\ell_1]$, $H[\ell_2]$) can be associated with an import edge from $H[\ell_1]$ to $H[\ell_2]$, or with an export edge from $H[\ell_1]$ to $H[\ell_2]$.

**Notation.** For a map $M$, a key $k$, and a value $v$, we use $M[k]$ to denote the lookup of $k$, and $M' = M[k \mapsto v]$ for adding an entry for $k$ to $M$. For a multi-valued map $M$, we use the notation $M' = M[k \mapsto_{\cup} \{v\}]$ for adding an entry for $k$ to $M$. If the map already has an entry for $k$, the resulting value is the union of the existing value set and $\{v\}$.

**Static Semantics.** We formalize our static analysis using a constraint-based specification, as a set of inference rules, then prove that the OGraph is sound, i.e., it has all the required OObjects, ODomains, and OEdges.

In this context, soundness means that we can build a map between a ROG and an OGraph. Soundness consists of object soundness and edge soundness. With object soundness, every runtime object maps to a unique representative OObject in the OGraph. With object soundness, every runtime edge maps to a unique representative OEdge in the OGraph. To build the maps, we instrument the FDJ dynamic semantics. We map every newly created runtime object to an OObject. Also, for every field read, field write, or a method invocation, we map the corresponding runtime edge to an OEdge.

In FDJ, a program is a tuple $(CT, e)$ that consists of a class table $CT$, which maps classes to their definitions, and an expression $e$. Our analysis starts with a root expression $e_{root}$, that explicitly instantiates the root class $C_{root}$. The analysis result is the least solution $G = \langle DO, DD, DE \rangle$ of the following constraint system:

$$\emptyset, \emptyset, DO, DD, DE \vdash (CT, e_{root})$$

The analysis starts by creating the OObject $O_{world}$ and its owning ODomain $D_{\texttt{SHARED}}$, which constitutes the root of the OGraph,

$$D_{\texttt{SHARED}} = \langle D_0, ::\texttt{SHARED} \rangle \qquad\qquad O_{world} = \langle C_{dummy}\!<.>\rangle$$

then abstractly interprets $e_{root}$ in the context of $O_{world}$:

$$\emptyset, \emptyset, DO, DD, DE \vdash_{O_{world}} e_{root}$$

The judgement form for expressions is as follows:

$$\Gamma, \Upsilon, DO, DD, DE \vdash_{O,H} e$$

The $O$ subscript on the turnstile captures the context-sensitivity, and represents the context object that the analysis uses to abstractly interpret $e$. The $H$ subscript is a map used by the dynamic semantics and the store typing rule in the static semantics (not shown). For readability, we omit $H$ when not in use. $CT(C)$ and $CT(\texttt{Object})$ represent a lookup of a class $C$ and the class `Object` in the class table, and is an implicit clause in all the static rules. (We list these clauses once at the top of Fig. 5 to avoid repetition.)

In Df-New, the analysis interprets a `new` object allocation in the context of $O$. The analysis first ensures that $DO$ contains an OObject $O_C$ for the newly allocated object. Then, Df-New ensures that $DD$ has a representative ODomain $D_i$ for each domain parameter $p_i$ passed to the constructor of the class $C$. Based on the binding of each formal domain parameter $\alpha_i$ to actual $p_i$, $DD$ maps each $\alpha_i$ to a corresponding $D_i$ in the context of $O_C$ $((O_C, \alpha_i) \mapsto D_i)$ (Fig. 5).

Then, Df-New uses the auxiliary judgement Aux-Dom to ensure that $DD$ has an ODomain corresponding to each domain that $C$ locally declares $((O_C, C{::}d_j) \mapsto D_j)$. Aux-Dom recursively includes inherited domains from base classes as well. Aux-Obj1, the base case of the recursion, deals with the class `Object`, for which Aux-Obj1 does nothing, because `Object` has no fields, domains, or methods in FDJ.

Df-New then obtains each expression $e_R$ in each method $m$ of $C$, and recursively processes $e_R$ in the context of the new OObject $O_C$. To avoid infinite recursion, before Df-New analyzes $e_R$, it checks if the combination of the class $C$ and actual domains $\overline{D}$ have been previously analyzed by looking for this combination in $\Upsilon$. If this combination does not exist, Df-New extends $\Upsilon$ with the current combination. As a side note, $\Upsilon$ tracks previously analyzed OObjects only at the call stack level. It does not do so globally across the program because similar combinations of the same class and domain parameters can occur in different contexts, and must be analyzed separately. Finally, Df-New analyzes each argument of the constructor. Since our analysis distinguishes between a field initialization in a constructor and a field write, Df-New does not require dataflow edges in $DE$.

Df-Lookup defines the auxiliary judgement *lookup* that returns the set of the OObjects $O_k$ in $DO$ such that the class of $O_k$ is $C'$ or one of its subclasses. It also ensures that each domain $D_i$ of $O_k$ corresponds to $D'_i$, a domain associated with $O$ in $DD$. The second condition increases the precision of our analysis, because *lookup* returns only a subset of all the objects of class $C'$ or

$$CT(C) = \texttt{class } C\texttt{<}\overline{\alpha},\overline{\beta}\texttt{> extends } C'\texttt{<}\overline{\alpha}\texttt{>} \; \{ \; \overline{T} \; \overline{f}; \; \overline{dom}; \; \ldots; \; \overline{md}; \; \}$$

$$CT(\texttt{Object}) = \texttt{class Object<}\alpha_o\texttt{>} \;\; \{ \;\; \}$$

$$\frac{\begin{array}{c} \forall i \in 1..|\overline{p}| \qquad D_i = DD[(O, p_i)] \qquad params(C) = \overline{\alpha} \\ O_C = \langle \; C\texttt{<}\overline{D}\texttt{>} \; \rangle \qquad \{O_C\} \subseteq DO \qquad \alpha_i \in \overline{\alpha} \\ \{(O_C, \alpha_i) \mapsto D_i\} \subseteq DD \qquad \{(O_C, p_i) \mapsto D_i\} \subseteq DD \\ DO, DD, DE \vdash_O ddomains(C, O_C) \\ \forall m \in \overline{md} \; mbody(m, C\texttt{<}\overline{p}\texttt{>}) = (\overline{x} : \overline{T}, \; e_R) \\ C\texttt{<}\overline{D}\texttt{>} \notin \Upsilon \Longrightarrow \{\overline{x} : \overline{T}, \; \texttt{this} : C\texttt{<}\overline{p}\texttt{>}\}, \Upsilon \cup \{C\texttt{<}\overline{D}\texttt{>}\}, DO, DD, DE \vdash_{O_C} e_R \\ \Gamma, \Upsilon, DO, DD, DE \vdash_O \overline{e} \end{array}}{\Gamma, \Upsilon, DO, DD, DE \vdash_O \texttt{new } C\texttt{<}\overline{p}\texttt{>}(\overline{e})} \text{[DF-NEW]}$$

$$\frac{\begin{array}{c} \forall (\texttt{domain } d_j) \in \overline{dom} \qquad D_j = \langle D_{id_j}, \; C{::}d_j \rangle \qquad \{(O_C, C{::}d_j) \mapsto D_j\} \subseteq DD \\ DO, DD, DE \vdash_O ddomains(C', O_C) \end{array}}{DO, DD, DE \vdash_O ddomains(C, O_C)} \text{[AUX-DOM]}$$

$$\frac{}{DO, DD, DE \vdash_O ddomains(\texttt{Object}, O_C)} \text{[AUX-OBJ1]} \qquad \frac{\begin{array}{c} O_k \in DO \qquad O_k = \langle C\texttt{<}\overline{D}\texttt{>} \; \rangle \qquad C <: C' \\ \forall i \in 1..|\overline{p'}| \qquad D'_i = DD[(O, p'_i)] \qquad D'_i = D_i \end{array}}{DO, DD, DE \vdash_O lookup \; (C'\texttt{<}\overline{p'}\texttt{>}) = \{O_k\}_{k \in 1..sz}} \text{[DF-LOOKUP]}$$

$$\frac{\begin{array}{c} e_0 : C\texttt{<}\overline{p}\texttt{>} \qquad (T_k \; f_k) \in fields(C\texttt{<}\overline{p}\texttt{>}) \\ DO, DD, DE \vdash_O import(C\texttt{<}\overline{p}\texttt{>}, T_k) \\ \Gamma, \Upsilon, DO, DD, DE \vdash_O e_0 \end{array}}{\Gamma, \Upsilon, DO, DD, DE \vdash_O e_0.f_k} \text{[DF-READ]} \qquad \frac{\begin{array}{c} e_0 : C\texttt{<}\overline{p}\texttt{>} \qquad (T_k \; f_k) \in fields(C\texttt{<}\overline{p}\texttt{>}) \\ e_1 : C_1\texttt{<}\overline{p''}\texttt{>} \qquad C_1\texttt{<}\overline{p''}\texttt{>} <: T_k \\ DO, DD, DE \vdash_O export(C\texttt{<}\overline{p}\texttt{>}, C_1\texttt{<}\overline{p''}\texttt{>}) \\ \Gamma, \Upsilon, DO, DD, DE \vdash_O e_0 \qquad \Gamma, \Upsilon, DO, DD, DE \vdash_O e_1 \end{array}}{\Gamma, \Upsilon, DO, DD, DE \vdash_O e_0.f_k = e_1} \text{[DF-WRITE]}$$

$$\frac{\begin{array}{c} DO, DD, DE \vdash_O lookup \; (T_{src}) = \{O_i\}_{i \in 1..sz} \\ DO, DD, DE \vdash_{O_i} lookup \; (T_{label}) = \{O_j\}_{j \in 1..sz'} \\ \forall i \in 1..sz \; \forall j \in 1..sz' \; O_j = \langle C_j\texttt{<}\overline{D}\texttt{>}\rangle \; \{\langle O_i, O, C_j, Imp\rangle\} \subseteq DE \end{array}}{DO, DD, DE \vdash_O import \; (T_{src}, T_{label})} \text{[AUX-IMPORT]}$$

$$\frac{\begin{array}{c} DO, DD, DE \vdash_O lookup \; (T_{dst}) = \{O_i\}_{i \in 1..sz} \\ DO, DD, DE \vdash_O lookup \; (T_{label}) = \{O_j\}_{j \in 1..sz'} \\ \forall i \in 1..sz \; \forall j \in 1..sz' \; O_j = \langle C_j\texttt{<}\overline{D}\texttt{>}\rangle \; \{\langle O, O_i, C_j, Exp\rangle\} \subseteq DE \end{array}}{DO, DD, DE \vdash_O export \; (T_{dst}, T_{label})} \text{[AUX-EXPORT]}$$

$$\frac{\begin{array}{c} e_0 : C\texttt{<}\overline{p}\texttt{>} \qquad mtype(m, C\texttt{<}\overline{p}\texttt{>}) = \overline{T} \to T_R \\ DO, DD, DE \vdash_O import(C\texttt{<}\overline{p}\texttt{>}, T_R) \\ \forall k \in 1..|\overline{e}| \; e_k : T'_k \qquad T'_k <: T_k \qquad T_k \in \overline{T} \qquad DO, DD, DE \vdash_O export(C\texttt{<}\overline{p}\texttt{>}, T'_k) \\ \Gamma, \Upsilon, DO, DD, DE \vdash_O e_0 \qquad \Gamma, \Upsilon, DO, DD, DE \vdash_O \overline{e} \end{array}}{\Gamma, \Upsilon, DO, DD, DE \vdash_O e_0.m(\overline{e})} \text{[DF-INVK]}$$

**Figure 5:** Static semantics. Additional rules (DF-VAR, DF-LOC, DF-CONTEXT, DF-SIGMA) are in [24].

its subclasses in $DO$. From this subset, our analysis picks the source or destination OObjects, and finds the class representing the label of an OEdge.

The auxiliary judgements Aux-Import and Aux-Export ensure import and export edges between the context OObject $O$ and the OObjects $O_i$, where $O_i$ is the result of *lookup* $(T_{src})$, and *lookup* $(T_{dst})$, respectively. The direction of the edge is from $O_i$ to the context $O$ for Aux-Import, and from the context $O$ to $O_i$ for Aux-Export. To identify an edge's label, Aux-Export calls *lookup* in the context of $O$, while Aux-Import calls the second *lookup* in the context of $O_i$. As a result, there could be multiple edges with different labels between the same two OObjects, depending on what *lookup* returns.

Df-Read and Df-Write abstractly interpret field read and field write expressions, respectively, and use Aux-Import and Aux-Export. Both auxiliary judgements take the type $e_0$ as the first argument, and pass it to *lookup* to set the source and destination OObjects. For the label, Df-Read uses the type of the field $f_k$, while Df-Write uses the type of the right-hand side expression $e_1$. The labels are the classes of these types or one of their subclasses.

Df-Invk abstractly interprets method invocation expressions. First, it ensures the existence of an import edge from the receiver of the method to the context OObject $O$. The label of the import edge is the class of the return type, or one of its subclasses. Next, for each argument $e_k$, Df-Invk ensures the existence of an export edge from $O$ to the receiver of the method. The label of each export edge is the class of the argument or one of its subclasses. The rule ensures export edges only for a method invocation with at least one argument. Finally, the rule evaluates recursively the expressions $e_0$ and $\overline{e}$.

Df-Var, and Df-Loc, and the rest of the rules complete our formalization and make the induction go through (Fig. 6). Df-Context analyzes expressions of the form $\ell \triangleright e$. The context for analyzing $e$ changes from $O$ to $O_C$, where $O_C$ is the result of looking up the receiver $\ell$ in $H$. Finally, the induction requires an augmented store typing rule, Df-Sigma, to ensures that the method bodies have been analyzed for all the locations $\ell$ in the store, and that every $\ell$ has a corresponding OObject in $DO$. To denote all the objects in the store, we use the $CT$ subscript instead of $O$.

**Dynamic Semantics.** To complete the formalization, we instrumented the dynamic semantics (Fig. 7). The instrumentation extends the dynamic semantics of FDJ [4] (the common parts are

$$\frac{}{\Gamma, \Upsilon, DO, DD, DE \vdash_O x}\text{[Df-Var]} \qquad \frac{}{\Gamma, \Upsilon, DO, DD, DE \vdash_O \ell}\text{[Df-Loc]}$$

$$\frac{O_C = H[\ell] \qquad \Gamma, \Upsilon, DO, DD, DE \vdash_{O_C} e}{\Gamma, \Upsilon, DO, DD, DE \vdash_{O,H} \ell \rhd e}\text{[Df-Context]}$$

$$\frac{\begin{array}{c}\forall \ell \in dom(S), \Sigma[\ell] = C\texttt{<}\overline{p}\texttt{>} \qquad H[\ell] = O = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO \\ \forall m.\ mbody(m, C\texttt{<}\overline{p}\texttt{>}) = (\overline{x} : \overline{T},\ e_R) \qquad \{\overline{x} : \overline{T},\ \texttt{this} : C\texttt{<}\overline{p}\texttt{>}\}, \emptyset, DO, DD, DE \vdash_O e_R\end{array}}{DO, DD, DE \vdash_{CT,H} \Sigma}\text{[Df-Sigma]}$$

**Figure 6:** Static semantics (continued).

highlighted), but is safe since discarding it produces exactly the FDJ dynamic semantics. The instrumented evaluation rule is of the following form:

$$\theta \vdash e; S; H; K; L_I; L_E \rightsquigarrow_G e'; S'; H'; K'; L'_I; L'_E$$

where $G = \langle DO, DD, DE\rangle$ is the statically computed object graph, and $\rightsquigarrow_G$ means that the expression $e$ evaluates to $e'$ in the context of $\theta$, the value of `this`. The dynamic semantics keep $G$ unchanged, but change the store $S$ and the maps $H$, $K$, $L_I$, and $L_E$.

IR-New adds a new location $\ell$ to the store $S$, where $\ell$ maps to an object of type $C$ with the specified ownership domain parameters, and the fields set to the values $\overline{v}$ passed to the constructor. The rule extends $H$ by mapping $\ell$ and the OObject $O_C$ from $DO$. The rule requires that each actual domains $p_i$ passed during instantiation corresponds to an actual domain $D_i$ of $O_C$. Next, the rule extends $K$ such that for all the domains $C{::}d_j$, the pair $(O_C,\ C{::}d_j)$ has a corresponding $D_j$ in $DD$.

IR-Read and IR-Write ensure that an OEdge $E$ exists between the context OObject $O$ and the receiver $O_\ell$. They use $\theta$ and $\ell$ to lookup these OObjects in $H$. They also ensure that the edge label $C_v$ is a subclass of the field class $C_i$. Finally, the rules extend the maps $L_I$ and $L_E$, respectively, by adding $E$ to the set of edges associated with $(\ell,\ \theta)$ in $L_I$, and $(\theta,\ \ell)$ in $L_E$.

IR-Invk ensures that an import OEdge $E'$ exists from the receiver $O_\ell$ to the context $O$, having as the edge's label a subclass of the return class $C_R$. IR-Invk also ensures that an export OEdge $E_k$ exist from $O$ to $O_\ell$ for every parameter, having as edge label a subclass of the method's parameter

$$\frac{\begin{array}{c}\boxed{\ell \notin dom(S) \qquad S' = S[\ell \mapsto C<\overline{p}>(\overline{v})]} \\ G = \langle DO, DD, DE \rangle \\ \overline{p} = \overline{\ell'.d} \qquad \forall i \in 1..|\overline{\ell'.d}|\ D_i = K[\ell'_i.d_i] \\ O_C = \langle C<\overline{D}> \rangle \qquad O_C \in DO \qquad H' = H[\ell \mapsto O_C] \\ \forall(\texttt{domain}\ d_j) \in domains(C<\overline{p}>) \qquad D_j = DD[(O_C, C{::}d_j)] \qquad K' = K[\ell.d_j \mapsto D_j]\end{array}}{\theta \vdash \boxed{\texttt{new}\ C<\overline{p}>(\overline{v}); S}; H; K; L_I; L_E \rightsquigarrow_G \boxed{\ell; S'}; H'; K'; L_I; L_E}\,[\text{IR-New}]$$

$$\frac{\begin{array}{c}\boxed{S[\ell] = C<\overline{p}>(\overline{v}) \qquad fields(C<\overline{p}>) = \overline{T}\ \overline{f}} \\ O = H[\theta] \qquad O_\ell = H[\ell] \qquad T_i = C_i<\overline{p'}> \qquad T_i \in \overline{T} \\ E = \langle O_\ell, O, C_v, Imp \rangle \in DE \qquad C_v <: C_i \qquad L'_I = L_I[(\ell, \theta) \mapsto_\cup \{E\}]\end{array}}{\theta \vdash \boxed{\ell.f_i; S}; H; K; L_I; L_E \rightsquigarrow_G \boxed{v_i; S}; H; K; L'_I; L_E}\,[\text{IR-Read}]$$

$$\frac{\begin{array}{c}\boxed{S[\ell] = C<\overline{p}>(\overline{v}) \qquad fields(C<\overline{p}>) = \overline{T}\ \overline{f}} \\ \boxed{S' = S[\ell \mapsto C<\overline{p}>([v/v_i]\overline{v})]} \\ O = H[\theta] \qquad O_\ell = H[\ell] \qquad T_i = C_i<\overline{p'}> \qquad T_i \in \overline{T} \\ E = \langle O, O_\ell, C_v, Exp \rangle \in DE \qquad C_v <: C_i \qquad L'_E = L_E[(\theta, \ell) \mapsto_\cup \{E\}]\end{array}}{\theta \vdash \boxed{\ell.f_i = v; S}; H; K; L_I; L_E \rightsquigarrow_G \boxed{v; S'}; H; K; L_I; L'_E}\,[\text{IR-Write}]$$

$$\frac{\begin{array}{c}\boxed{S[\ell] = C<\overline{p}>(\overline{v}) \qquad mbody(m, C<\overline{p}>) = (\overline{x}, e_R)} \\ O = H[\theta] \qquad O_\ell = H[\ell] \qquad mtype(m, C<\overline{p}>) = \overline{T} \to T_R \qquad T_R = C_R<\overline{p'}> \\ E' = \langle O_\ell, O, C'_R, Imp \rangle \in DE \qquad C'_R <: C_R \qquad L'_I = L_I[(\ell, \theta) \mapsto_\cup \{E'\}] \\ \forall k \in 1..|\overline{T}|\ T_k = C_k<\overline{p''}> \qquad E_k = \langle O, O_\ell, C'_k, Exp \rangle \in DE \qquad C'_k <: C_k \\ L'_E = L_E[(\theta, \ell) \mapsto_\cup \{E_k\}]\end{array}}{\theta \vdash \boxed{\ell.m(\overline{v}); S}; H; K; L_I; L_E \rightsquigarrow_G \boxed{\ell \triangleright [\overline{v}/\overline{x}, \ell/\texttt{this}]e_R; S}; H; K; L'_I; L'_E}\,[\text{IR-Invk}]$$

$$\frac{}{\theta \vdash \boxed{\ell \triangleright v; S}; H; K; L_I; L_E \rightsquigarrow_G \boxed{v;\ S}; H; K; L_I; L_E}\,[\text{IR-Context}]$$

**Figure 7:** Instrumented dynamic semantics (core rules).

class $C_k$. The rule uses $\theta$ and $\ell$ to lookup $O$ and $O_\ell$ in $H$ . It extends both $L_I$ and $L_E$ by adding $E'$ to the set of import edges between the locations $\ell$ and $\theta$ in $L_I$, and by adding each $E_k$ to the set of export edges between the locations $\theta$ and $\ell$ in $L_E$.

When the method expression reduces to a value $v$, IR-Context propagates $v$ outside of its method context. This rule does not affect the execution of the program.

Finally, the dynamic semantics include standard congruence rules. The congruence rules are similar to those in FDJ [4] (Fig. 8). In addition, there are two congruence rules for field-write:

$$\frac{\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G e'_i; S'; H'; K'; L'_I; L'_E}{\begin{array}{c}\theta \vdash \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e_i, e_{i+1..n}); S; H; K; L_I; L_E \rightsquigarrow_G \\ \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e'_i, e_{i+1..n}); S'; H'; K'; L'_I; L'_E\end{array}}\text{[IRC-New]}$$

$$\frac{\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e'_0; S'; H'; K'; L'_I; L'_E}{\begin{array}{c}\theta \vdash e_0.f_i; S; H; K; L_I; L_E \rightsquigarrow_G \\ e'_0.f_i; S'; H'; K'; L'_I; L'_E\end{array}}\text{[IRC-Read]}$$

$$\frac{\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e'_0; S'; H'; K'; L'_I; L'_E}{\begin{array}{c}\theta \vdash e_0.f_i = e_1; S; H; K; L_I; L_E \rightsquigarrow_G \\ e'_0.f_i = e_1; S'; H'; K'; L'_I; L'_E\end{array}}\text{[IRC-Write-Rcv]}$$

$$\frac{\theta \vdash e_1; S; H; K; L_I; L_E \rightsquigarrow_G e'_1; S'; H'; K'; L'_I; L'_E}{\begin{array}{c}\theta \vdash v.f_i = e_1; S; H; K; L_I; L_E \rightsquigarrow_G \\ v.f_i = e'_1; S'; H'; K'; L'_I; L'_E\end{array}}\text{[IRC-Write-Arg]}$$

$$\frac{\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e'_0; S'; H'; K'; L'_I; L'_E}{\begin{array}{c}\theta \vdash e_0.m(\overline{e}); S; H; K; L_I; L_E \rightsquigarrow_G \\ e'_0.m(\overline{e}); S'; H'; K'; L'_I; L'_E\end{array}}\text{[IRC-RecvInvk]}$$

$$\frac{\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G e'_i; S'; H'; K'; L'_I; L'_E}{\begin{array}{c}\theta \vdash v.m(v_{1..i-1}, e_i, e_{i+1..n}); S; H; K; L_I; L_E \rightsquigarrow_G \\ v.m(v_{1..i-1}, e'_i, e_{i+1..n}); S'; H'; K'; L'_I; L'_E\end{array}}\text{[IRC-ArgInvk]}$$

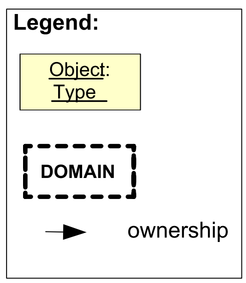
$$\frac{\ell \vdash e; S; H; K; L_I; L_E \rightsquigarrow_G e'; S'; H'; K'; L'_I; L'_E}{\theta \vdash \ell \triangleright e; S; H; K; L_I; L_E \rightsquigarrow_G \ell \triangleright e'; S'; H'; K'; L'_I; L'_E}\text{[IRC-Context]}$$

**Figure 8:** Instrumented dynamic semantics (congruence rules).

IRC-Write-Rcv and IRC-Write-Arg. IRC-Write-Rcv states that the receiver expression $e_0$ reduces to $e'_0$, while IRC-Write-Arg states that the right-hand side expression $e_1$ reduces to $e'_1$.

**Recursive Types.** The analysis must handle recursive types which would otherwise lead to an unbounded number of nodes in the OGraph. To get a finite OGraph and ensure that the analysis terminates, the analysis could stop expanding an OGraph after a certain depth. Truncating the recursion at an arbitrary depth may omit objects or edges beyond the cutoff depth, which would be unsound. Instead, to preserve soundness, the analysis creates a cycle in the OGraph when it encounters a domain declaration $d$ in class $C$ ($C$::$d$), already analyzed in the context of $O_C$. According to DF-NEW, a domain declaration may be analyzed multiple times using different contexts, which result in multiple ODomains for the same domain declaration. In the presence of a recursive type, the pair $(O_C, C$::$d)$ is the same for multiple passes of the analysis. On the first pass, the analysis adds $C{<}\overline{D}{>}$ of $O_C$ in $\Upsilon$ and performs a lookup in $DD$. If the pair is not found, it creates a new ODomain and a new entry for the pair in $DD$. On the second pass, the analysis encounters the same pair and reuses the existing ODomain. So the analysis creates a cycle in the OGraph, and the reused ODomain appears as the child of two OObjects. This justifies an ODomain not having a unique owning OObject (Fig. 4). On the next pass, the analysis encounters the same $C{<}\overline{D}{>}$ in $\Upsilon$ and does not recurse any further.

```
Main<SHARED> main = new Main<SHARED>();
class Main<OWNER> {
  domain OWNED;
  QuadTree<this.OWNED> aQT;
  Main() {
    this.aQT = new QuadTree<this.OWNED>();
  }
}
class QuadTree<M> {
  domain OWNED;
  QuadTree<OWNED> nwQT;
  QuadTree() {
    this.nwQT = new QuadTree<this.OWNED>();
  }
}
```



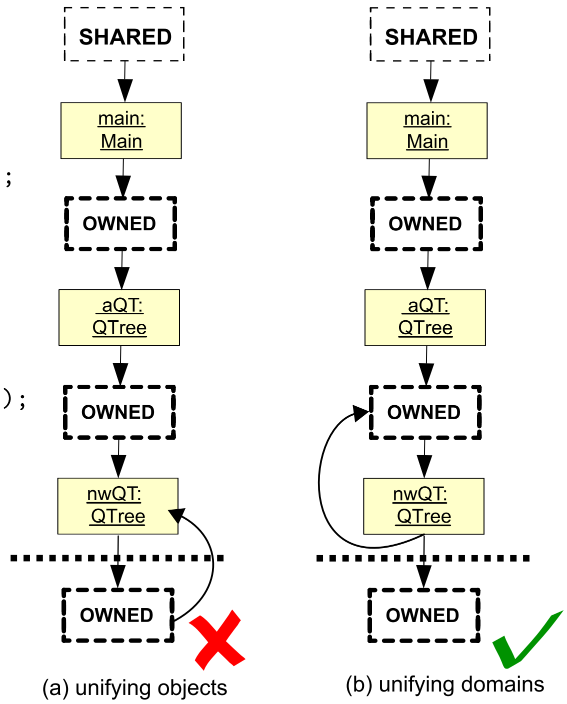




**Figure 9:** Handling recursive types, revised from [1, Figure 2.22].

```
Oworld dummy context
{(Oworld, SHARED)↦ D_SHARED} ⊆ DD
ϒ = { }

//Analyzing (line 1) in the context of Oworld:
```

$$\frac{}{\emptyset; \emptyset; DO, DD, DE \vdash_{O_{world}} \texttt{new Main} < \texttt{SHARED} >)()}$$

```
CT(Main) = class Main<OWNER> {
  domain OWNED;
  QuadTree<this.OWNED> aQT;
  Main() { this.aQT = new QuadTree<this.OWNED>(); }
}
 In Df-New:
O == Oworld
this == θ0
DO == [Oworld]
DD == [(Oworld, SHARED)↦ SHARED; ]
DE == []
C == Main
i == 1
αi == Main::OWNER
pi == ::SHARED
Di == DD[(Oworld, ::SHARED)] == SHARED
OC == Main<SHARED>
{ Main<SHARED> } ⊆ DO
{ (Main<SHARED>, Main::OWNER )↦ SHARED,
(Main<SHARED>, ::SHARED )↦ SHARED } ⊆ DD

// In Aux-Dom:
DD == [(Oworld, ::SHARED)↦ SHARED;
(Main<SHARED>, Main::OWNER )↦ SHARED;
(Main<SHARED>, ::SHARED )↦ SHARED; ]
dom == [domain OWNED]
j == 1
C::Dj == Main::OWNED
OC == Main<SHARED>
Dj == ODomain(main.OWNED, Main::OWNED)
{ (Main<SHARED>, Main::OWNED) ↦ main.OWNED } ⊆ DD
```

**Figure 10:** Applying DF-NEW on the QuadTree example. First pass: the analysis creates the OObject for `main` (line 1) and the ODomain `main.OWNED`.

```
//Back in Df-New, analyze recursively constructor body as if it were a method:
Υ = { Main<SHARED> }
// In context O, where O = O_C above, i.e., Main<SHARED>, analyze:
```

$$\frac{}{\Gamma; \Upsilon; DO; DD; DE \vdash_O \texttt{new QuadTree<this.OWNED>}()}$$

```
CT(QuadTree) = class QuadTree<M> {
  domain OWNED;
  QuadTree<OWNED> nwQT;
  QuadTree() {
    this.nwQT = new QuadTree<this.OWNED>();
  }
}
// In Df-New:
O == Main<SHARED>
this == main
C == QuadTree
DO == [O_world; Main<SHARED>]
DD == [(O_world, ::SHARED)↦ SHARED;
(Main<SHARED>, Main::OWNER) ↦ SHARED;
(Main<SHARED>, ::SHARED )↦ SHARED;
(Main<SHARED>, Main::OWNED) ↦ main.OWNED; ]
i == 1
p_i == Main::OWNED
α_i == QuadTree::M
D_i == DD[(Main<SHARED>, this.OWNED)] = main.OWNED
O_C == QuadTree<main.OWNED>
{ QuadTree<main.OWNED>} ⊆ DO
{ (QuadTree<main.OWNED>, QuadTree::M)↦ main.OWNED,
(QuadTree<main.OWNED>, Main::OWNED)↦ main.OWNED
} ⊆ DD
// In Aux-Dom:
DD == [(O_world, ::SHARED)↦ SHARED;
(Main<SHARED>, Main::OWNER) ↦ SHARED;
(Main<SHARED>, ::SHARED )↦ SHARED;
(Main<SHARED>, Main::OWNED) ↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::M)↦ main.OWNED;
(QuadTree<main.OWNED>, Main::OWNED)↦ main.OWNED; ]
dom == [domain OWNED]
j == 1
C::D_j == QuadTree::OWNED
O_C == QuadTree<main.OWNED>
D_j == ODomain(main.OWNED.aQT.OWNED, QuadTree::OWNED)
{(QuadTree<main.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQT.OWNED }⊆ DD
```

**Figure 11:** Applying DF-NEW on the QuadTree example. Second pass: the analysis creates the OObject for aQT (line 6) and the ODomain main.OWNED.aQT.OWNED.

```
//Back in Df-New, analyze recursively constructor body as if it were a method:
ϒ = { Main<SHARED>, QuadTree<main.OWNED> }
// In context O, where O = O_C above, i.e., QuadTree<main.OWNED>, analyze:
```

$$\Gamma;\Upsilon;DO;DD;DE \vdash_O \texttt{new QuadTree<this.OWNED>()}$$

```
CT(QuadTree) = class QuadTree<M> {
  domain OWNED;
  QuadTree<OWNED> nwQT;
  QuadTree() {
    this.nwQT = new QuadTree<this.OWNED>();
  }
}
// In Df-New:
O == QuadTree<main.OWNED>
this == aQT
DO == [O_world; Main<SHARED>; QuadTree<main.OWNED>]
DD == [(O_world, ::SHARED)↦ SHARED;
(Main<SHARED>, Main::OWNER) ↦ SHARED;
(Main<SHARED>, ::SHARED )↦ SHARED;
(Main<SHARED>, Main::OWNED) ↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::M)↦ main.OWNED;
(QuadTree<main.OWNED>, Main::OWNED)↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQT.OWNED; ]
C == QuadTree
i == 1
p_i == QuadTree::OWNED
α_i == QuadTree::M
D_i == DD[ (QuadTree<main.OWNED>, QuadTree::OWNED)]= main.OWNED.aQT.OWNED
O_C == QuadTree<main.OWNED.aQT.OWNED>
{ QuadTree<main.OWNED.aQT.OWNED> } ⊆ DO
{ (QuadTree<main.OWNED.aQT.OWNED>, QuadTree::M)↦ main.OWNED.aQt.OWNED,
(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQt.OWNED } ⊆ DD
// In Aux-Dom:
DD == [(O_world, ::SHARED)↦ SHARED;
(Main<SHARED>, Main::OWNER) ↦ SHARED;
(Main<SHARED>, ::SHARED )↦ SHARED;
(Main<SHARED>, Main::OWNED) ↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::M)↦ main.OWNED;
(QuadTree<main.OWNED>, Main::OWNED)↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQT.OWNED;
(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::M)↦ main.OWNED.aQt.OWNED;
(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQt.OWNED; ]
dom == [domain OWNED] j == 1
C::D_j == QuadTree::OWNED
O_C == QuadTree<main.OWNED.aQT.OWNED>
D_j == ODomain(main.OWNED.aQT.OWNED, QuadTree::OWNED) //reuse
{ (QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED) ↦ main.OWNED.aQt.OWNED } ⊆ DD
```

**Figure 12:** Applying Df-New on the QuadTree example. Third pass: the analysis creates the OObject for `nwQT` (line 13), and reuses the ODomain `main.OWNED.aQT.OWNED`

```
//Back in Df-New, analyze recursively constructor body as if it were a method:
Υ = { Main<SHARED>, QuadTree<main.OWNED>, QuadTree<main.OWNED.aQT.OWNED> }
// In context O, where O = O_C above, i.e., QuadTree<main.OWNED.aQT.OWNED>, analyze:
```

$$\Gamma; \Upsilon; DO; DD; DE \vdash_O \texttt{new QuadTree<this.OWNED>}()$$

```
// In Df-New:
O == QuadTree<main.OWNED.aQT.OWNED>
this == nwQT
DO == [O_world; Main<SHARED>; QuadTree<main.OWNED>; QuadTree<main.OWNED.aQT.OWNED>]
DD == [(O_world, ::SHARED)↦ SHARED;
(Main<SHARED>, Main::OWNER) ↦ SHARED;
(Main<SHARED>, ::SHARED )↦ SHARED;
(Main<SHARED>, Main::OWNED) ↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::M)↦ main.OWNED;
(QuadTree<main.OWNED>, Main::OWNED)↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQT.OWNED;
(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::M)↦ main.OWNED.aQt.OWNED;
(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQt.OWNED; ]
C == QuadTree
i == 1
p_i == QuadTree::OWNED
α_i == QuadTree::M
D_i == DD[ (QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED)]= main.OWNED.aQT.OWNED
O_C == QuadTree<main.OWNED.aQT.OWNED> // Reuse
{ QuadTree<main.OWNED.aQT.OWNED > } ⊆ DO
{ (QuadTree<main.OWNED.aQT.OWNED >, QuadTree::M)↦ main.OWNED.aQT.OWNED,
(QuadTree<main.OWNED.aQT.OWNED >, QuadTree::OWNED)↦ main.OWNED.aQT.OWNED} ⊆ DD
// In Aux-Dom:
DD == [(O_world, ::SHARED)↦ SHARED;
(Main<SHARED>, Main::OWNER) ↦ SHARED;
(Main<SHARED>, ::SHARED )↦ SHARED;
(Main<SHARED>, Main::OWNED) ↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::M)↦ main.OWNED;
(QuadTree<main.OWNED>, Main::OWNED)↦ main.OWNED;
(QuadTree<main.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQT.OWNED;
(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::M)↦ main.OWNED.aQt.OWNED;
(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED)↦ main.OWNED.aQt.OWNED; ]
dom == [domain OWNED]
j == 1
C::D_j == QuadTree::OWNED
D_j == ODomain(main.OWNED.aQT.OWNED.nwQT.OWNED, QuadTree::OWNED)
{ (QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED) ↦ QuadTree<main.OWNED.aQT.OWNED>} ⊆ DD
//Back in Df-New:
Υ = { Main<SHARED>, QuadTree<main.OWNED>, QuadTree<main.OWNED.aQT.OWNED> }
QuadTree<main.OWNED.aQT.OWNED> ∈ Υ //STOP.
```

**Figure 13:** Applying Df-New on the QuadTree example. Forth pass: the analysis terminates when `QuadTree<main.OWNED.aQT.OWNED>` is found in $\Upsilon$

```
Main<SHARED> main = new Main<SHARED>();
OObject(main, SHARED, Main)
analyze(main, [Main::OWNER↦SHARED])
this↦main
Main::OWNER↦SHARED
class Main<OWNER> {
  domain OWNED;
  ODomain(main.OWNED, Main::OWNED)
  OObject(main.OWNED.aQT, main.OWNED, QuadTree)
  QuadTree<OWNED> aQT;
  Main() {
    this.aQT = new QuadTree<OWNED>();
  analyze(main.OWNED.aQT, [QuadTree::M↦Main::OWNED])
  }
}
this↦main.OWNED.aQT
[QuadTree::M↦Main::OWNED]
class QuadTree<M> {
  domain OWNED;
  ODomain(main.OWNED.aQT.OWNED, QuadTree::OWNED)
  OObject(main.OWNED.aQT.OWNED.nwQT, main.OWNED.aQT.OWNED, QuadTree)
  QuadTree<OWNED> nwQT;
  QuadTree() {
    nwQT = new QuadTree<OWNED>();
  analyze(main.OWNED.aQT.OWNED.nwQT, [QuadTree::M↦QuadTree::OWNED])
  }
}
this ↦ main.OWNED.aQT.OWNED.nwQT
[QuadTree::M ↦ QuadTree::OWNED]
class QuadTree<M> {
  domain OWNED;
  ODomain(main.OWNED.aQT.OWNED, QuadTree::OWNED)
  OObject(main.OWNED.aQT.OWNED.nwQT, main.OWNED.aQT.OWNED, QuadTree)
  QuadTree<OWNED> nwQT;
  QuadTree() {
    nwQT = new QuadTree<OWNED>();
  analyze(main.OWNED.aQT.OWNED.nwQT, [QuadTree::M ↦ QuadTree::OWNED])
  }
}
```

**Figure 14:** Worked example with recursive types, revised from [1, Figure 2.24].

As an example, consider a class `QuadTree`, which declares a field `nwQT` of type `QuadTree` in its `OWNED` private domain (Fig. 9). The analysis does four passes over Df-New and Aux-Dom. In the first two passes, the analysis creates two new OObject instances while interpreting the `new` expressions (Fig 9 line 1 and line 6) and two new ODomain instances while interpreting the domain declarations (Fig 9 line 3 and line 10). The details of each pass are in Fig. 10 and Fig. 11. In each pass, the context $O$ changes to $O_C$ while analyzing the body of the default constructor. The default constructor consists of a sequence of field initializations. We consider that all the field writes that occur in the body of a constructor are field initializations. This is similar to Java, where final fields can be initialized in a constructor, but not later.

In the third pass, the analysis creates a new OObject `QuadTree<main.OWNED.aQT.OWNED`, but while interpreting the domain declaration `QuadTree::OWNED`, the analysis reuses the existing ODomain `main.OWNED.aQT.OWNED` created during the second pass. Two constraints are ensuring this reuse. First, in the constraint $(O_C, p_i) \mapsto D_i \subseteq DD$ of Df-New $O_C$ is `QuadTree<main.OWNED.aQT.OWNED>` and $p_i$ is the domain `QuadTree::OWNED`. Consequently, the analysis ensures that the pair `(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED)` maps to `main.OWNED.aQT.OWNED` in $DD$. Second, while ensuring the constraint $(O_C, C :: d_j) \mapsto D_j \subseteq DD$ of Aux-Dom, the analysis encounters again the pair `(QuadTree<main.OWNED.aQT.OWNED>, QuadTree::OWNED)`. This justifies why, the analysis reuses the `main.OWNED.aQT.OWNED` ODomain instead of creating a new one (Fig 12). By detecting the same ODomain, the analysis can make the OObject `QuadTree<main.OWNED.aQT.OWNED>` to be both the parent and the child of an ODomain, thus creating a cycle.

In the forth pass, the analysis reuses the existing OObject `QuadTree<main.OWNED.aQT.OWNED>` as $O_C$ to ensure that $\{O_C\} \in DO$ and, similarly to pass 3, the analysis reuses the existing ODomain `main.OWNED.aQT.OWNED`. Next, since $O_C == O$ and the condition $C{<}\overline{D}{>} \notin \Upsilon$ is unsatisfied, the analysis terminates (Fig. 13).

### 4.3 Soundness

An OGraph is a *sound* approximation of a ROG, represented by a well-typed store $S$, if the OGraph relates to the ROG as follows:

**Object soundness.** There is a map $H$ that maps each object $\ell$ in $S$ to exactly one representative OObject in the OGraph. Similarly, there is a map $K$ such that each runtime domain $\ell.d$ has exactly one representative ODomain in the OGraph.

**Edge soundness.** If there is a dataflow communication from an object $\ell_1$ to $\ell_2$ in a ROG, with their representatives OObjects $O_1$ and $O_2$ in the OGraph, then there are two maps $L_I$ and $L_E$ that map the pair $(\ell_1, \ell_2)$ to a set of OEdges in the OGraph that represent the dataflow communication between $O_1$ and $O_2$.

To relate the dynamic and the static semantics of the analysis, we define an approximation relation (DF-APPROX) between a runtime state $(S,H,K,L_I,L_E)$ and an analysis result $(DO, DD, DE)$. It ensures that the runtime objects, runtime domains and runtime edges are consistent with their representatives in the statically extracted OGraph.

**Approximation Relation (Df-Approx).**

$$\forall\ \Sigma \vdash S,\quad (S, H, K, L_I, L_E) \sim (DO, DD, DE)$$

$$\iff$$

$$\forall \ell \in dom(S), \Sigma[\ell] = C\texttt{<}\overline{\ell'.d}\texttt{>}$$

$$\implies$$

$$H[\ell] = O_C = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$$

$$and\ \forall \ell'_j.d_j \in \overline{\ell'.d}\ K[\ell'_j.d_j] = D_j = \langle D_{id_j}, d_j\rangle \in rng(DD)$$

$$and\ \forall d_i \in domains(C\texttt{<}\overline{\ell'.d}\texttt{>})$$

$$K[\ell.d_i] = D_i = \langle D_{id_i}, d_i\rangle\ \{(O_C, C{::}d_i) \mapsto D_i\} \in DD$$

$$and\ \forall \ell_{src} \in dom(H),\ fields(\Sigma[\ell_{src}]) = \overline{T_{src}}\ \overline{f}$$

$$\forall m.\ mtype(m, \Sigma[\ell_{src}]) = \overline{T} \to T_R$$

$$\forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$$

$$E'_k \in L_I[(\ell_{src}, \ell)]\ E'_k = \langle H[\ell_{src}], H[\ell], C'_k, Imp\rangle \in DE\ C'_k <: C_k$$

$$and\ \forall \ell_{dst} \in dom(H),\ fields(\Sigma[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f}$$

$$\forall m.\ mtype(m, \Sigma[\ell_{dst}]) = \overline{T} \to T_R$$

$$\forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$$

$$E_k \in L_E[(\ell, \ell_{dst})]\ E_k = \langle H[\ell], H[\ell_{dst}], C'_k, Exp\rangle \in DE\ C'_k <: C_k$$

Df-Approx states that given a well-typed store $S$ of a program and an OGraph $\langle DO, DD, DE\rangle$ of the same program, there are maps $H$, $K$, $L_I$, and $L_E$, such that $H$ maps each runtime object $\ell$ in the store to a unique OObject $O_C$ from $DO$, $K$ maps each runtime domain $\ell.d_i$ in the store to a unique ODomain $D_i$, and $L_I$ and $L_E$ map each pair of runtime objects ($\ell_{src}$, $\ell$) and ($\ell$, $\ell_{dst}$) to OEdges from $DE$. Df-Approx ensures the consistency of these mappings with the ownership relation, and with the dataflow communication.

The last two conditions relate runtime dataflow communication back to field reads, field writes, and method invocations that produce the corresponding import and export edges in $DE$. $L_I$ maps a runtime dataflow communication from a runtime object $\ell_{src}$ to another runtime object $\ell$ back to an import $\mathsf{OEdge}$ $E'_k$ from $DE$. By our definition of import dataflow communication, $E'_k$ exists in $DE$ due to a field read or a method invocation expression that has $\ell_{src}$ as its receiver. The condition also ensures that the edge's label is a subclass of $C_k$, the class of a field of $\ell_{src}$'s class, or the return class of a method of $\ell_{src}$'s class.

Similarly, $L_E$ maps a runtime dataflow communication from a runtime object $\ell$ to another runtime object $\ell_{dst}$ back to an export $\mathsf{OEdge}$ $E_k$ from $DE$. By our definition of export dataflow communication, $E_k$ exists in $DE$ due to a field write or a method invocation expression that has $\ell_{dst}$ as its receiver. The condition also ensures that the edge's label is a subclass of $C_k$, the class of a field of $\ell_{dst}$'s class, or the class of a parameter on a method of $\ell_{dst}$'s class.

**Theorem: Dataflow Object Graph Soundness.**

$$
\begin{aligned}
&\textit{If } G = \langle DO, DD, DE \rangle \\
&\quad DO, DD, DE \vdash (CT, e_{root}) \\
&\quad \forall e,\ \theta_0 \vdash e; \emptyset, \emptyset, \emptyset, \emptyset, \emptyset \rightsquigarrow^*_G e; S; H; K; L_I; L_E \\
&\quad \Sigma \vdash S \\
&\textit{then } DO, DD, DE \vdash_{CT,H} \Sigma \\
&\quad (S, H, K, L_I, L_E) \sim (DO, DD, DE)
\end{aligned}
$$

where $\rightsquigarrow^*_G$ relation is the reflexive and transitive closure of $\rightsquigarrow_G$ relation, and $\theta_0$ is the location of the first object instantiated by $e_{root}$. To prove the Object Graph Soundness theorem, we prove the Dataflow Preservation and Dataflow Progress theorems, which extend the standard FDJ Preservation and Progress. The common parts are highlighted.

**Theorem: Dataflow Preservation (Subject reduction).**

$$
\begin{array}{l}
\textit{If } \boxed{\emptyset, \Sigma, \theta \vdash e : T} \\
\quad \boxed{\Sigma \vdash S} \\
\quad DO, DD, DE \vdash_{CT,H} \Sigma \\
\quad \emptyset, \emptyset, DO, DD, DE \vdash_O e \\
\quad (S, H, K, L_I, L_E) \sim (DO, DD, DE) \\
\quad \theta \vdash \boxed{\text{e; S}}; H; K; L_I; L_E \rightsquigarrow_G \boxed{\text{e'; S'}}; H'; K'; L_I'; L_E' \\
\textit{then } \boxed{\textit{there exists } \Sigma' \supseteq \Sigma \textit{ and } T' <: T \textit{ such that}} \\
\quad \boxed{\emptyset, \Sigma', \theta \vdash e' : T' \textit{ and } \Sigma' \vdash S'} \\
\quad (S', H', K', L_I', L_E') \sim (DO, DD, DE) \\
\quad \emptyset, \emptyset, DO, DD, DE \vdash_O e' \\
\quad \textit{and } DO, DD, DE \vdash_{CT,H} \Sigma'
\end{array}
$$

**Theorem: Dataflow Progress.**

$$
\begin{array}{l}
\textit{If } \boxed{\emptyset, \Sigma, \theta \vdash e : T} \\
\quad \boxed{\Sigma \vdash S} \\
\quad DO, DD, DE \vdash_{CT,H} \Sigma \\
\quad \emptyset, \emptyset, DO, DD, DE \vdash_O e \\
\quad (S, H, K, L_I, L_E) \sim (DO, DD, DE) \\
\textit{then either } \boxed{\textit{e is a value}} \\
\quad \textit{or else } \theta \vdash \boxed{\text{e}; S}; H; K; L_I; L_E \rightsquigarrow_G \boxed{\text{e}'; S'}; H'; K'; L_I'; L_E'
\end{array}
$$

### 4.4 Theorem: Dataflow Preservation (Subject reduction)

$$
\begin{array}{l}
If \\
\quad \boxed{\emptyset, \Sigma, \theta \vdash e : T} \\
\quad \boxed{\Sigma \vdash S} \\
\quad DO, DD, DE \vdash_{CT,H} \Sigma \\
\quad \emptyset, \emptyset, DO, DD, DE \vdash_O e \\
\quad (S, H, K, L_I, L_E) \sim (DO, DD, DE) \\
\quad \theta \vdash \boxed{e; S}; H; K; L_I; L_E \rightsquigarrow_G \boxed{e'; S'}; H'; K'; L'_I; L'_E \\
then \\
\quad \boxed{there\ exists\ \Sigma' \supseteq \Sigma\ and\ T' <: T\ such\ that\ \emptyset, \Sigma', \theta \vdash e' : T'\ and\ \Sigma' \vdash S'} \\
\quad (S', H', K', L'_I, L'_E) \sim (DO, DD, DE) \\
\quad \emptyset, \emptyset, DO, DD, DE \vdash_O e' \\
\quad and\ DO, DD, DE \vdash_{CT,H} \Sigma'
\end{array}
$$

The Dataflow Preservation theorem extends the FDJ Type Preservation theorem (the common parts are highlighted). Those parts are proved by induction over the derivation of the FDJ evaluation relation : $e; S \rightsquigarrow e'; S'$.

**Proof:** We prove preservation by induction on the instrumented evaluation relation

$$\theta \vdash e; S; H; K; L_I; L_E \rightsquigarrow_G e'; S'; H'; K'; L'_I; L'_E$$

The most interesting cases are Ir-New, Ir-Read (page 33), Ir-Write (page 34), and Ir-Invk (page 35).

**Case Ir-New:** e $=$ `new` $C\texttt{<}\overline{\ell'.d}\texttt{>}(\overline{v})$, and $e' = \ell$.

To Show:

(1) $(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$

(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$

(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e; S; H; K; L_I; L_E \rightsquigarrow_G e'; S'; H'; K'; L'_I; L'_E$ By assumption

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ By assumption

$\forall \ell \in dom(S),\ \Sigma(\ell) = C\texttt{<}\overline{\ell'.d}\texttt{>}$ Since $\Sigma \vdash S$

$H[\theta] = O = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ By Df-Approx

$\forall \theta'_j.d_j \in \overline{\theta'.d}\ K[\theta'_j.d_j] = D_j = \langle D_{id_j}, d_j\rangle \in rng(DD)$ By Df-Approx

$\forall d_i \in domains(C\texttt{<}\overline{\theta'.d}\texttt{>})\ K[\theta.d_i] = D_i = \langle D_{id_i}, d_i\rangle$

$\quad \{(O, d_i) \mapsto D_i\} \in DD$ By Df-Approx

$\forall \ell_{src} \in dom(H),\ fields(\Sigma[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{src}]) = \overline{T} \rightarrow T_R$

$\quad\quad \forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E'_k \in L_I[(\ell_{src}, \theta)] = \langle H[\ell_{src}], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By Df-Approx

$\forall \ell_{dst} \in dom(H),\ fields(\Sigma[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{dst}]) = \overline{T} \rightarrow T_R$

$\quad\quad \forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E_k \in L_E[(\theta, \ell_{dst})] = \langle H[\theta], H[\ell_{dst}], C'_k, Exp\rangle \in DE \quad C'_k <: C_k$ By Df-Approx

$O_C = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ By sub-derivation of Ir-New

$S' = S[\ell \mapsto C\texttt{<}\overline{p}\texttt{>}(\overline{v})]$ By sub-derivation of Ir-New

$H' = H[\ell \mapsto O_C]$ By sub-derivation of Ir-New

$\overline{p} = \overline{\ell'.d}\ \forall i \in 1..|\overline{\ell'.d}|\ D_i = K[\ell'_i.d_i]$ By sub-derivation of Ir-New

$\forall(\texttt{domain}\ d_j) \in domains(C\texttt{<}\overline{p}\texttt{>}) \quad D_j = DD[(O_C, d_j)]$

$K' = K[\ell.d_j \mapsto D_j]$ By sub-derivation of Ir-New

$L'_I = L_I \quad L'_E = L_E$ By sub-derivation of Ir-New

$\exists \Sigma' \supseteq \Sigma\ \ and\ T' <: T\ s.t.\ \emptyset, \Sigma', \theta \vdash e' : T'\ and\ \Sigma' \vdash S'$ By FDJ Type Preservation

$\Sigma'[\ell] = C_\ell\texttt{<}\overline{\ell'.d}\texttt{>}$ By $\Sigma' \vdash S'$

$(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$ By Df-Approx

This proves (1).

$\emptyset, \emptyset, DO, DD, DE \vdash_O e'$ By Df-Loc, since $e' = \ell$

This proves (2).

$DO, DD, DE \vdash_{CT,H} \Sigma$ By assumption

$\forall \ell \in dom(S), \Sigma[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}$ By sub-derivation of Df-Sigma

$H[\ell] = O_\ell = \langle C_\ell\texttt{<}\overline{D_\ell}\texttt{>}\rangle \in DO$ By sub-derivation of Df-Sigma

$\forall m.\ mbody(m, C_\ell\texttt{<}\overline{p}\texttt{>}) = (\overline{x} : \overline{T},\ e_R)$ By sub-derivation of Df-Sigma

$\{\overline{x} : \overline{T},\ \texttt{this} : C_\ell\texttt{<}\overline{p}\texttt{>}\}, \emptyset, DO, DD, DE \vdash_{O_\ell} e_R$ By sub-derivation of Df-Sigma

$O_C = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ By sub-derivation of Ir-New

$S' = S[\ell \mapsto C\texttt{<}\overline{p}\texttt{>}(\overline{v})]$ By sub-derivation of Ir-New

$H' = H[\ell \mapsto O_C]$ By sub-derivation of Ir-New

$\emptyset, \emptyset, DO, DD, DE \vdash_O e$ By assumption with $e, \Upsilon$ below

$e = \texttt{new}\ C\texttt{<}\overline{\ell'.d}\texttt{>}(\overline{v}),$ and $\Upsilon = \emptyset$

$\forall m.\ mbody(m, C\texttt{<}\overline{p}\texttt{>}) = (\overline{x} : \overline{T},\ e_R)$ By sub-derivation of Df-New

$C\texttt{<}\overline{D}\texttt{>} \notin \Upsilon \implies$

$\{\overline{x} : \overline{T}, \mathtt{this} : C\texttt{<}\overline{p}\texttt{>}\}, \Upsilon \cup \{C\texttt{<}\overline{D}\texttt{>}\}, DO, DD, DE \vdash_{O_C} e_R$ By sub-derivation of Df-New

$\{\overline{x} : \overline{T}, \mathtt{this} : C\texttt{<}\overline{p}\texttt{>}\}, \emptyset, DO, DD, DE \vdash_{O_C} e_R$ By Df-Strengthening Lemma

$\forall \ell \in dom(S'), \Sigma'[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}$

$H'[\ell] = O_\ell = \langle C_\ell\texttt{<}\overline{D_\ell}\texttt{>}\rangle \in DO$

$\forall m.\ mbody(m, C_\ell\texttt{<}\overline{p}\texttt{>}) = (\overline{x} : \overline{T},\ e_R)$

$\{\overline{x} : \overline{T},\ \mathtt{this} : C_\ell\texttt{<}\overline{p}\texttt{>}\}, \emptyset, DO, DD, DE \vdash_{O_\ell} e_R$ By above

$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By Df-Sigma with above $H'$ and $\Sigma'$

This proves (3).

**Case Ir-Read:** e $= \ell.f_i$, and $e' = v_i$.

To Show:

(1) $(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$

(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$

(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e; S; H; K; L_I; L_E \rightsquigarrow_G e'; S'; H'; K'; L'_I; L'_E$ By assumption

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ By assumption

$\forall \ell \in dom(S),\ \Sigma(\ell) = C\texttt{<}\overline{\ell'.d}\texttt{>}$ Since $\Sigma \vdash S$

$H[\theta] = O = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ By Df-Approx

$\forall \theta'_j.d_j \in \overline{\theta'.d}\ K[\theta'_j.d_j] = D_j = \langle D_{id_j}, d_j\rangle \in rng(DD)$ By Df-Approx

$\forall d_i \in domains(C\texttt{<}\overline{\theta'.d}\texttt{>})\ K[\theta.d_i] = D_i = \langle D_{id_i}, d_i\rangle$

$\{(O, d_i) \mapsto D_i\} \in DD$ By Df-Approx

$\forall \ell_{src} \in dom(H),\ fields(\Sigma[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$

$\forall m.\ mtype(m, \Sigma[\ell_{src}]) = \overline{T} \to T_R$

$\forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$E'_k \in L_I[(\ell_{src}, \theta)] = \langle H[\ell_{src}], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By Df-Approx

$\forall \ell_{dst} \in dom(H),\ fields(\Sigma[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$

$\forall m.\ mtype(m, \Sigma[\ell_{dst}]) = \overline{T} \to T_R$

$\forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$E_k \in L_E[(\theta, \ell_{dst})] = \langle H[\theta], H[\ell_{dst}], C'_k, Exp\rangle \in DE\ C'_k <: C_k$ By Df-Approx

$S' = S, H' = H, K' = K, L'_E = L_E$ By sub-derivation of Ir-Read

$S[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}(\overline{v}) \quad fields(C_\ell\texttt{<}\overline{p}\texttt{>}) = \overline{T'}\ \overline{f}$ By sub-derivation of Ir-Read

$O = H[\theta] \quad O_\ell = H[\ell] \quad T'_i = C_i\texttt{<}\overline{p'}\texttt{>}$ By sub-derivation of Ir-Read

$E' = \langle O_\ell, O, C_v, Imp\rangle \in DE \quad C_v <: C_i$ By sub-derivation of Ir-Read

$L'_I = L_I[(\ell,\theta) \mapsto_\cup \{E'\}]$ By sub-derivation of Ir-Read

$\forall \ell_{src} \in dom(H'),\ fields(\Sigma'[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma'[\ell_{src}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E'_k \in L'_I[(\ell_{src},\theta)] = \langle H'[\ell_{src}], H'[\theta], C'_k, Imp\rangle \in DE\ C'_k <: C_k$ By above, since $\Sigma' = \Sigma$

$(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$ By Df-Approx

This proves (1).

$\emptyset, \emptyset, DO, DD, DE \vdash_O e'$ By Df-Loc, since $e' = v_i$

This proves (2).

$DO, DD, DE \vdash_{CT,H} \Sigma$ By assumption

$S' = S, H' = H$ By sub-derivation of Ir-Read

$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By Df-Sigma with the above $H'$ and $\Sigma' = \Sigma$

This proves (3).

**Case Ir-Write:** $\text{e} = \ell.f_i = v$, and $e' = v$

To Show:

(1) $(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$

(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$

(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e; S; H; K; L_I; L_E \leadsto_G e'; S'; H'; K'; L'_I; L'_E$ By assumption

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ By assumption

$\forall \ell \in dom(S),\ \Sigma(\ell) = C\texttt{<}\overline{\ell'.d}\texttt{>}$ Since $\Sigma \vdash S$

$H[\theta] = O = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ By Df-Approx

$\forall \theta'_j.d_j \in \overline{\theta'.d}\ K[\theta'_j.d_j] = D_j = \langle D_{id_j}, d_j\rangle \in rng(DD)$ By Df-Approx

$\forall d_i \in domains(C\texttt{<}\overline{\theta'.d}\texttt{>})\ K[\theta.d_i] = D_i = \langle D_{id_i}, d_i\rangle$

$\quad \{(O, d_i) \mapsto D_i\} \in DD$ By Df-Approx

$\forall \ell_{src} \in dom(H),\ fields(\Sigma[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{src}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E'_k \in L_I[(\ell_{src},\theta)] = \langle H[\ell_{src}], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By Df-Approx

$\forall \ell_{dst} \in dom(H),\ fields(\Sigma[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{dst}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E_k \in L_E[(\theta, \ell_{dst})] = \langle H[\theta], H[\ell_{dst}], C'_k, Exp\rangle \in DE\ C'_k <: C_k$ By Df-Approx

$H' = H, K' = K, L'_I = L_I$ By sub-derivation of Ir-Write

$S[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}(\overline{v}) \quad fields(C_\ell\texttt{<}\overline{p}\texttt{>}) = \overline{T'}\ \overline{f}$ By sub-derivation of Ir-Write

$S' = S[\ell \mapsto C_\ell\texttt{<}\overline{p}\texttt{>}([v/v_i]\overline{v})]$ By sub-derivation of Ir-Write

$O = H[\theta] \quad O_\ell = H[\ell] \quad T'_i = C_i\texttt{<}\overline{p'}\texttt{>}$ By sub-derivation of Ir-Write

$E = \langle O, O_\ell, C_v, Exp\rangle \in DE \quad C_v <: C_i$ By sub-derivation of Ir-Write

$L'_E = L_E[(\theta, \ell) \mapsto_\cup \{E\}]$ By sub-derivation of Ir-Write

$\exists \Sigma' \supseteq \Sigma\ \ and\ T' <: T\ s.t.\ \emptyset, \Sigma', \theta \vdash e' : T'\ and\ \Sigma' \vdash S'$ By FDJ Type Preservation

$\Sigma'[\ell] = C\texttt{<}\overline{\ell'.d}\texttt{>}$ $\Sigma' \vdash S'$

$\forall \ell_{dst} \in dom(H'),\ fields(\Sigma'[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma'[\ell_{dst}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E_k \in L'_E[(\theta, \ell_{dst})] = \langle H'[\theta], H'[\ell_{dst}], C'_k, Exp\rangle \in DE\ C'_k <: C_k$ By above

$(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$ By Df-Approx

This proves (1).

$\emptyset, \emptyset, DO, DD, DE \vdash_O e'$ By Df-Loc, since $e' = v_i$

This proves (2).

$DO, DD, DE \vdash_{CT,H} \Sigma$ By assumption

$\forall \ell \in dom(S), \Sigma[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}$

$\quad H[\ell] = O_\ell = \langle C_\ell\texttt{<}\overline{D_\ell}\texttt{>}\rangle \in DO$

$\quad \forall m.\ mbody(m, C_\ell\texttt{<}\overline{p}\texttt{>}) = (\overline{x} : \overline{T},\ e_R)$

$\quad\quad \{\overline{x} : \overline{T},\ \texttt{this} : C_\ell\texttt{<}\overline{p}\texttt{>}\}, \emptyset, DO, DD, DE \vdash_{O_\ell} e_R$ By sub-derivation of Df-Sigma

$H' = H$ By sub-derivation of Ir-Write

$S[\ell] = C\texttt{<}\overline{p}\texttt{>}(\overline{v}) \quad fields(C\texttt{<}\overline{p}\texttt{>}) = \overline{T}\ \overline{f}$ By sub-derivation of Ir-Write

$S' = S[\ell \mapsto C\texttt{<}\overline{p}\texttt{>}([v/v_i]\overline{v})]$ By sub-derivation of Ir-Write

$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By Df-Sigma with the above $H'$ and $\Sigma' = \Sigma$

This proves (3).

**Case Ir-Invk:** e $= \ell.m(\overline{v})$, and $e' = \ell \triangleright [\overline{v}/\overline{x}, \ell/\texttt{this}]e_R$

To Show:

(1) $(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$

(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$

(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

| | |
|---|---|
| $\theta \vdash e; S; H; K; L_I; L_E \rightsquigarrow_G e'; S'; H'; K'; L'_I; L'_E$ | By assumption |
| $(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ | By assumption |
| $\forall \ell \in dom(S),\ \Sigma(\ell) = C{<}\overline{\ell'.d}{>}$ | Since $\Sigma \vdash S$ |
| $H[\theta] = O = \langle C{<}\overline{D}{>}\rangle \in DO$ | By Df-Approx |
| $\forall \theta'_j.d_j \in \overline{\theta'.d}\ K[\theta'_j.d_j] = D_j = \langle D_{id_j}, d_j\rangle \in rng(DD)$ | By Df-Approx |
| $\forall d_i \in domains(C{<}\overline{\theta'.d}{>})\ K[\theta.d_i] = D_i = \langle D_{id_i}, d_i\rangle$ | |
| $\quad \{(O, d_i) \mapsto D_i\} \in DD$ | By Df-Approx |
| $\forall \ell_{src} \in dom(H),\ fields(\Sigma[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$ | |
| $\quad \forall m.\ mtype(m, \Sigma[\ell_{src}]) = \overline{T} \rightarrow T_R$ | |
| $\quad\quad \forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k{<}\overline{p}{>}$ | |
| $\quad\quad\quad E'_k \in L_I[(\ell_{src}, \theta)] = \langle H[\ell_{src}], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ | By Df-Approx |
| $\forall \ell_{dst} \in dom(H),\ fields(\Sigma[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$ | |
| $\quad \forall m.\ mtype(m, \Sigma[\ell_{dst}]) = \overline{T} \rightarrow T_R$ | |
| $\quad\quad \forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k{<}\overline{p}{>}$ | |
| $\quad\quad\quad E_k \in L_E[(\theta, \ell_{dst})] = \langle H[\theta], H[\ell_{dst}], C'_k, Exp\rangle \in DE\ C'_k <: C_k$ | By Df-Approx |
| $S' = S \quad H' = H \quad K' = K$ | By sub-derivation of Ir-Invk |
| $S[\ell] = C_\ell{<}\overline{p}{>}(\overline{v}) \quad mbody(m, C_\ell{<}\overline{p}{>}) = (\overline{x}, e_R)$ | By sub-derivation of Ir-Invk |
| $H[\theta] = O \quad H[\ell] = O_\ell$ | By sub-derivation of Ir-Invk |
| $mtype(m, C_\ell{<}\overline{p}{>}) = \overline{T} \rightarrow T_R \quad T_R = C_R{<}\overline{p'}{>}$ | By sub-derivation of Ir-Invk |
| $E' = \langle O_\ell, O, C'_R, Imp\rangle \in DE \quad C'_R <: C_R$ | By sub-derivation of Ir-Invk |
| $L'_I = L_I[(\ell, \theta) \mapsto_\cup \{E'\}]$ | By sub-derivation of Ir-Invk |
| $\forall i \in 1..\lvert\overline{T}\rvert\ T_i = C_i{<}\overline{p''}{>} \quad E_i = \langle O, O_\ell, C'_i, Exp\rangle \in DE \quad C'_i <: C_i$ | By sub-derivation of Ir-Invk |
| $L'_E = L_E[(\theta, \ell) \mapsto_\cup \{E_i\}]$ | By sub-derivation of Ir-Invk |
| $\exists \Sigma' \supseteq \Sigma\ \ and\ T' <: T\ \ s.t.\ \emptyset, \Sigma', \theta \vdash e' : T'\ \ and\ \Sigma' \vdash S'$ | By FDJ Type Preservation |
| $\Sigma'[\ell] = C_\ell{<}\overline{\ell'.d}{>}$ | $\Sigma' \vdash S'$ |

$\forall \ell_{src} \in dom(H'),\ fields(\Sigma'[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma'[\ell_{src}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E'_k \in L'_I[(\ell_{src}, \theta)] = \langle H'[\ell_{src}], H'[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By above

$\forall \ell_{dst} \in dom(H'),\ fields(\Sigma'[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma'[\ell_{dst}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E_k \in L'_E[(\theta, \ell_{dst})] = \langle H'[\theta], H'[\ell_{dst}], C'_k, Exp\rangle \in DE \quad C'_k <: C_k$ By above

$(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$ By Df-Approx

This proves (1).

| | |
|---|---|
| $\emptyset, \emptyset, DO, DD, DE \vdash_O e$ | By assumption |
| $e = \ell.m(\overline{v}) \quad e_0 = \ell \quad \overline{e} = \overline{v}$ | By assumption |
| $e' = \ell \triangleright [\overline{v}/\overline{x}, \ell/\texttt{this}]e_R$ | By assumption |
| $\emptyset, \Sigma, \theta \vdash e : T$ | By assumption |
| $\exists \Sigma' \supseteq \Sigma \ \ and\ T' <: T\ s.t.\ \emptyset, \Sigma', \theta \vdash e' : T'\ and\ \Sigma' \vdash S'$ | By FDJ Type Preservation |
| $\quad e_0 : T_0 \quad T_0 = C_\ell\texttt{<}\overline{p}\texttt{>}$ | By sub-derivation of Df-Invk |
| $mtype(m, C_\ell\texttt{<}\overline{p}\texttt{>}) = \overline{T} \to T_R$ | By sub-derivation of Df-Invk |
| $\emptyset, \emptyset, DO, DD, DE \vdash_O e_0$ | By sub-derivation of Df-Invk |
| $\emptyset, \emptyset, DO, DD, DE \vdash_O \overline{e}$ | By sub-derivation of Df-Invk |
| $\{\overline{x} : \overline{T}, \texttt{this} : C_\ell\texttt{<}\alpha, \overline{\beta}\texttt{>}\}, \Sigma, \theta \vdash e_R : T_R \quad T_R <: T$ | By FDJ *Meth*OK: |
| $S[\ell] = C_\ell\texttt{<}d, \overline{d'}\texttt{>}(\overline{v})$ | By sub-derivation of Ir-Invk |
| $mbody(m, C_\ell\texttt{<}d, \overline{d'}\texttt{>}) = (\overline{x}, e_R)$ | By sub-derivation of Ir-Invk |
| $\Sigma[\ell] = C_\ell\texttt{<}d, \overline{d'}\texttt{>} = T_0$ | Since $e_0 = \ell$, by T-Store |
| $e_0 : C_\ell\texttt{<}d, \overline{d'}\texttt{>}$ | Since $e_0 = \ell$, by T-Store |
| $mtype(m, C_\ell\texttt{<}d, \overline{d'}\texttt{>}) = \overline{T} \to T_R$ | Since $e_0 = \ell$, by T-Store |
| $\overline{v} : \overline{T_a}$ | By inversion |
| $\overline{T_a} <: [\overline{v}/\overline{x}, \ell/\texttt{this}]\overline{T}$ | For some $\overline{T_a}$ and $\overline{T}$ |
| there are some $D\texttt{<}\overline{d}\texttt{>}$ and $T'_R$ so that: | By Method Lemma |
| $T'_R <: T_R$ and $C_\ell\texttt{<}d, \overline{d'}\texttt{>} <: D\texttt{<}\overline{d}\texttt{>}$ | By Method Lemma |
| so that $\{\overline{x} : \overline{T}, \texttt{this} : D\texttt{<}\overline{d}\texttt{>}\}, \Sigma, \theta \vdash e_R : T'_R$ | By Method Lemma |
| there exists $T_S, T_S <: T'_R$ s. t. $[\overline{v}/\overline{x}, \ell/\texttt{this}]e_R : T_S$ | Since term substitution preserves typing |
| $T_S <: T'_R$ and $T'_R <: T_R$ | By above |
| $T_S <: T_R$ | By transitivity of <: |
| Take $T = T' = T_R$ in FDJ Preservation | |

$\{\overline{x} : \overline{T}, \texttt{this} : C_\ell\texttt{<}d, \overline{d'}\texttt{>}\}, \emptyset, DO, DD, DE \vdash_{O_C} e_R$ By Df-Sigma

$O_C = H[\ell]$ By Df-Sigma

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell$ By Df-Loc

$\emptyset, \emptyset, DO, DD, DE \vdash_{O_C} [\overline{v}/\overline{x}, \ell/\texttt{this}]e_R$ By Df-Substitution Lemma

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell \triangleright [\overline{v}/\overline{x}, \ell/\texttt{this}]e_R$ By Df-Context

This proves (2).

$DO, DD, DE \vdash_{CT,H} \Sigma$ By assumption

$S' = S, H' = H$ By sub-derivation of Ir-Invk

$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By Df-Sigma with the above $H'$ and $\Sigma' = \Sigma$

This proves (3).

**Case Ir-Context:** e $= \ell \triangleright v$, and $e' = v$

To Show:

(1) $(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$

(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$

(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ By assumption

$S' = S, H' = H, K' = K, L'_I = L_I, L'_E = L_E$ By sub-derivation of Ir-Context

This proves (1).

$\emptyset, \emptyset, DO, DD, DE \vdash_O e'$ By Df-Loc, since $e' = v$

This proves (2).

$DO, DD, DE \vdash_{CT,H} \Sigma$ By assumption

$S' = S, H' = H$ By sub-derivation of Ir-Context

$DO, DD, DE \vdash_{CT,H'} \Sigma'$ Take $\Sigma' = \Sigma$

This proves (3).

**Case Irc-New:** e $= \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e_i, e_{i+1..n})$, and $e' = \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e'_i, e_{i+1..n})$.

To Show:

(1) $(S', H', K', L'_I, L'_E) \sim (DO, DD, DE)$

(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$

(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G e_i'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-New
$(S', H', K', L_I', L_E') \sim (DO, DD, DE)$ By induction hypothesis
This proves (1).

$\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G e_i'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-New
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_i'$ By induction hypothesis
$\emptyset, \emptyset, DO, DD, DE \vdash_O \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e_i', e_{i+1..n})$ By Df-New
This proves (2).

$\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G e_i'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-New
$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By induction hypothesis, take $\Sigma' = \Sigma$
This proves (3).

**Case Irc-Read:** e $= e_0.f_k$, and $e' = e_0'.f_k$.
To Show:
(1) $(S', H', K', L_I', L_E') \sim (DO, DD, DE)$
(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$
(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Read
$(S', H', K', L_I', L_E') \sim (DO, DD, DE)$ By induction hypothesis
This proves (1).

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Read
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_0'$ By induction hypothesis
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_0'.f_k$ By Df-Read
This proves (2).

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Read
$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By induction hypothesis, take $\Sigma' = \Sigma$
This proves (3).

**Case Irc-Write-Rcv:** e $= (e_0.f_k = e_1)$, and $e' = (e_0'.f_k = e_1)$.
To Show:
(1) $(S', H', K', L_I', L_E') \sim (DO, DD, DE)$
(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$
(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Write-Rcv
$(S', H', K', L_I', L_E') \sim (DO, DD, DE)$ By induction hypothesis
This proves (1).

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Write-Rcv
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_0'$ By induction hypothesis
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_1$ By Df-Write
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_0'.f_k = e_1$ By Df-Write
This proves (2).

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Write-Rcv
$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By induction hypothesis, take $\Sigma' = \Sigma$
This proves (3).

**Case Irc-Write-Arg:** e $= (v.f_k = e_1)$, and $e' = (v.f_k = e_1')$.
To Show:
(1) $(S', H', K', L_I', L_E') \sim (DO, DD, DE)$
(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$
(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e_1; S; H; K; L_I; L_E \rightsquigarrow_G e_1'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Write-Arg
$(S', H', K', L_I', L_E') \sim (DO, DD, DE)$ By induction hypothesis
This proves (1).

$\theta \vdash e_1; S; H; K; L_I; L_E \rightsquigarrow_G e_1'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Write-Arg
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_1'$ By induction hypothesis
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_0'.f_k = e_1'$ By Df-Write
This proves (2).

$\theta \vdash e_1; S; H; K; L_I; L_E \rightsquigarrow_G e_1'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-Write-Arg
$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By induction hypothesis, take $\Sigma' = \Sigma$
This proves (3).

**Case Irc-Recvinvk:** e $= e_0.m(\overline{e})$, and $e' = e_0'.m(\overline{e})$.
To Show:
(1) $(S', H', K', L_I', L_E') \sim (DO, DD, DE)$
(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$

(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-RecvInvk
$(S', H', K', L_I', L_E') \sim (DO, DD, DE)$ By induction hypothesis
This proves (1).

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-RecvInvk
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_0'$ By induction hypothesis
$\emptyset, \emptyset, DO, DD, DE \vdash_O \overline{e}$ By Df-Invk
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_0'.m(\overline{e})$ By Df-Invk
This proves (2).

$\theta \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-RecvInvk
$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By induction hypothesis, take $\Sigma' = \Sigma$
This proves (3).

**Case Irc-Arcinvk:** e $= v.m(v_{1..i-1}, e_i, e_{i+1..n})$,and $e' = v.m(v_{1..i-1}, e_i', e_{i+1..n})$.
To Show:
(1) $(S', H', K', L_I', L_E') \sim (DO, DD, DE)$
(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$
(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G e_i'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-ArgInvk
$(S', H', K', L_I', L_E') \sim (DO, DD, DE)$ By induction hypothesis
This proves (1).

$\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G e_i'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-ArgInvk
$\emptyset, \emptyset, DO, DD, DE \vdash_O e_i'$ By induction hypothesis
$\emptyset, \emptyset, DO, DD, DE \vdash_O v.m(v_{1..i-1}, e_i', e_{i+1..n})$ By Df-Invk
This proves (2).

$\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G e_i'; S'; H'; K'; L_I'; L_E'$ By sub-derivation of Irc-ArgInvk
$DO, DD, DE \vdash_{CT,H'} \Sigma'$ By induction hypothesis, take $\Sigma' = \Sigma$
This proves (3).

**Case Irc-Context:** e $= \ell \triangleright e_0$, and $e' = \ell \triangleright e_0'$.
To Show:
(1) $(S', H', K', L_I', L_E') \sim (DO, DD, DE)$

(2) $\emptyset, \emptyset, DO, DD, DE \vdash_O e'$
(3) $DO, DD, DE \vdash_{CT,H'} \Sigma'$

$\ell \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ — By sub-derivation of Irc-Context
$(S', H', K', L_I', L_E') \sim (DO, DD, DE)$ — By induction hypothesis
This proves (1).

$\ell \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ — By sub-derivation of Irc-Context
$O_\ell = H[\ell]$ — By induction hypothesis
$\emptyset, \emptyset, DO, DD, DE \vdash_{O_\ell} e_0'$ — By induction hypothesis
$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell \triangleright e_0'$ — By Df-Context
This proves (2).

$\ell \vdash e_0; S; H; K; L_I; L_E \rightsquigarrow_G e_0'; S'; H'; K'; L_I'; L_E'$ — By sub-derivation of Irc-Context
$DO, DD, DE \vdash_{CT,H'} \Sigma'$ — By induction hypothesis, take $\Sigma' = \Sigma$
This proves (3).

$\blacksquare$

## 4.5 Theorem: Dataflow Progress

$$
\begin{array}{l}
If \\
\quad \boxed{\emptyset, \Sigma, \theta \vdash e : T} \\
\quad \boxed{\Sigma \vdash S} \\
\quad DO, DD, DE \vdash_{CT,H} \Sigma \\
\quad \emptyset, \emptyset, DO, DD, DE \vdash_O e \\
\quad (S, H, K, L_I, L_E) \sim (DO, DD, DE) \\
then \\
\quad either \ \boxed{e\ is\ a\ value} \\
\quad or\ else\ \theta \vdash \boxed{e; S}; H; K; L_I; L_E \rightsquigarrow_G \boxed{e'; S'}; H'; K'; L'_I; L'_E
\end{array}
$$

**Proof:** We prove progress by derivation of $\emptyset, \emptyset, DO, DD, DE \vdash_O e$, with a case analysis on the last typing rule used. The most interesting cases are Df-New, Df-Read (page 44), Df-Write (page 46), and Df-Invk (page 48).

**Case DF-NEW** : e = $new\ C$<$\overline{p}$>($\overline{e}$).

**Subcase $\overline{e} = \overline{v}$** that is $e = new\ C$<$\overline{p}$>($\overline{v}$). Take $e' = \ell$, then Ir-New can apply.

To show:
(1) $\forall i \in |\overline{\ell'.d}| \quad D_i = K[\ell'_i.d_i]$
(2) $O_C = \langle C<\overline{D}> \rangle \quad O_C \in DO$
(3) $\forall d_j \in domains(C<\overline{\ell'.d}>) \quad D_j = DD[(O_C, d_j)]$

| | |
|---|---|
| $(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ | By assumption |
| $\forall \ell \in dom(S), \Sigma[\ell] = C<\overline{\ell'.d}>$ | $\Sigma \vdash S$ |
| $H[\ell] = O_C = \langle C<\overline{D}> \rangle \in DO$ | By Df-Approx |
| $\forall \ell'_j.d_j \in \overline{\ell'.d} \quad K[\ell'_j.d_j] = D_j = \langle D_{id_j}, d_j \rangle \in rng(DD)$ | By Df-Approx |
| $\forall d_i \in domains(C<\overline{\ell'.d}>)\ K[\ell.d_i] = D_i = \langle D_{id_i}, d_i \rangle$ | |
| $\{(O_C, d_i) \mapsto D_{\ell i}\} \in DD$ | By Df-Approx |

This proves (1).

$CT(C) = \texttt{class}\ C\texttt{<}\overline{\alpha},\overline{\beta}\texttt{>}\ \texttt{extends}\ C'\texttt{<}\overline{\alpha}\texttt{>}\ \ldots\ \{\ \overline{T}\ \overline{f};\ \overline{dom};\ \ldots;\ \overline{md};\ \}$

| | |
|---|---|
| $\emptyset, \emptyset, DO, DD, DE \vdash_O e$ | By assumption |
| $\forall i \in 1..\lvert\overline{p}\rvert \quad D_i = DD[(O, p_i)]$ | By sub-derivation of Df-New |
| $params(C) = \overline{\alpha}$ | By sub-derivation of Df-New |
| $O_C = \langle\ C\texttt{<}\overline{D}\texttt{>}\ \rangle \quad \{O_C\} \subseteq DO$ | By sub-derivation of Df-New |
| This proves (2). | |
| $\{(O_C, \alpha_i) \mapsto D_i\} \subseteq DD$ | By sub-derivation of Df-New |
| $\{(O_C, p_i) \mapsto D_i\} \subseteq DD$ | By sub-derivation of Df-New |
| $DO, DD, DE \vdash_O ddomains(C, O_C)$ | By sub-derivation of Df-New |
| This proves (3). | By Df-Domains Lemma |

**Subcase** $e = new\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e_i, e_{i+1..n})$ . Then Irc-New can apply.

| | |
|---|---|
| $\Gamma, \Upsilon, DO, DD, DE \vdash_O e_i$ | By sub-derivation of Df-New |
| $\theta \vdash e_i; S; H; K; L_I; L_E \rightsquigarrow_G S'; H'; K'; L'_I; L'_E$ | By induction hypothesis |
| $\theta \vdash \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e_i, e_{i+1..n})S; H; K; L_I; L_E \rightsquigarrow_G$ | |
| $\quad \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e'_i, e_{i+1..n}); S'; H'; K'; L'_I; L'_E$ | By Irc-New |
| This proves (2). | |
| $\{(O_C, \alpha_i) \mapsto D_i\} \subseteq DD$ | By sub-derivation of Df-New |
| $\{(O_C, p_i) \mapsto D_i\} \subseteq DD$ | By sub-derivation of Df-New |
| $DO, DD, DE \vdash_O ddomains(C, O_C)$ | By sub-derivation of Df-New |
| Take $e' = \texttt{new}\ C\texttt{<}\overline{p}\texttt{>}(v_{1..i-1}, e'_i, e_{i+1..n})$ | By Df-Domains Lemma |

**Case DF-VAR** : $e = x$.
Not applicable since variable is not a closed term.

**Case DF-LOC** : $e = \ell$.
e is a value.

**Case DF-READ** : e $= e_0.f_i$. There are two subcases to consider depending on whether the receiver $e_0$ is a value.

**Subcase $e_0 = \ell$.** Then $e = \ell.f_i$
To show:
(1) $O = H[\theta]$
(2) $O_\ell = H[\ell]$
(3) $E = \langle O_\ell, O, C_v, Imp\rangle \in DE \quad C_v <: C_i$

$DO, DD, DE \vdash_{CT,H} \Sigma$ By assumption

$\forall \ell' \in dom(S), \Sigma[\ell'] = C'\texttt{<}\overline{p}\texttt{>}$ By sub-derivation of Df-Sigma

$H[\ell'] = O' = \langle C'\texttt{<}\overline{D'}\texttt{>}\rangle \in DO$ By sub-derivation of Df-Sigma

$H[\theta] = O = \langle O_{\theta id}, C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ Since $\theta \in dom(S)$

$H[\ell] = O_\ell = \langle O_{\ell id}, C_\ell\texttt{<}\overline{D_\ell}\texttt{>}\rangle \in DO$ Since $\ell \in dom(S)$

this proves (1), and (2).

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ By assumption

$\forall \ell \in dom(S),\ \Sigma(\ell) = C\texttt{<}\overline{\ell'.d}\texttt{>}$ Since $\Sigma \vdash S$

$H[\theta] = O = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ By Df-Approx

$\forall \theta'_j.d_j \in \overline{\theta'.d}\ K[\theta'_j.d_j] = D_j = \langle D_{id_j}, d_j\rangle \in rng(DD)$ By Df-Approx

$\forall d_i \in domains(C\texttt{<}\overline{\theta'.d}\texttt{>})\ K[\theta.d_i] = D_i = \langle D_{id_i}, d_i\rangle$

$\quad \{(O, d_i) \mapsto D_i\} \in DD$ By Df-Approx

$\forall \ell_{src} \in dom(H),\ fields(\Sigma[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{src}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E'_k \in L_I[(\ell_{src}, \theta)] = \langle H[\ell_{src}], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By Df-Approx

$\forall \ell_{dst} \in dom(H),\ fields(\Sigma[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{dst}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E_k \in L_E[(\theta, \ell_{dst})] = \langle H[\theta], H[\ell_{dst}], C'_k, Exp\rangle \in DE\ C'_k <: C_k$ By Df-Approx

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell.f_i$ By assumption

$fields(\Sigma[\ell]) = \overline{T'}\ \overline{f}$ By FDJ T-Store

Since $e_0 = \ell \in dom(H)$

$\ell : \Sigma[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}\ (T'_i\ f_i) \in fields(C_\ell\texttt{<}\overline{p}\texttt{>})\ T'_i = C_i\texttt{<}\overline{p'}\texttt{>}$ By sub-derivation of Df-Read

$DO, DD, DE \vdash_O import(\Sigma[\ell], T'_i)$ By sub-derivation of Df-Read

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell$ By sub-derivation of Df-Read

Take $\ell_{src} = \ell$.

$\ell : \Sigma[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}\ (T'_i\ f_i) \in fields(C_\ell\texttt{<}\overline{p}\texttt{>})\ T'_i = C_i\texttt{<}\overline{p'}\texttt{>}$ By above sub-derivation

$\forall m.\ mtype(m, \Sigma[\ell]) = \overline{T} \rightarrow T_R$

$\forall T_k \in \{\overline{T'}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p''}\texttt{>}$

$\langle H[\ell], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By above DF-APPROX

Take $T_k = T'_i \in \overline{T'}, C_i = C_k$, and $C_v = C'_k$, this proves (3).

**Subcase $e_0 = e'_0.f_i$.** That is, $e_0$ is not a value

From IRC-READ:

$\theta \vdash e'_0; S; H; K; L_I; L_E \rightsquigarrow_G e''_0; S'; H'; K'; L'_I; L'_E$ By induction hypothesis

$\theta \vdash e'_0.f_i; S; H; K; L_I; L_E \rightsquigarrow_G e''_0.f_i; S'; H'; K'; L'_I; L'_E$ By IRC-READ

Take $e' = e''_0.f_i$.

**Case DF-WRITE** : e = $(e_0.f_i = e_1)$. There are three subcases to consider depending on whether the receiver $e_0$, and $e_1$ are values.

**Subcase $e_0 = \ell$, and $e_1 = v$.** Then $e = (\ell.f_i = v)$

To show:

(1) $O = H[\theta]$

(2) $O_\ell = H[\ell]$

(3) $E = \langle O, O_\ell, C_v, Exp\rangle \in DE \quad C_v <: C_i$

$DO, DD, DE \vdash_{CT,H} \Sigma$ By assumption

$\forall \ell' \in dom(S), \Sigma[\ell'] = C'\texttt{<}\overline{p}\texttt{>}$ By sub-derivation of DF-SIGMA

$H[\ell'] = O' = \langle C'\texttt{<}\overline{D'}\texttt{>}\rangle \in DO$ By sub-derivation of DF-SIGMA

$H[\theta] = O = \langle O_{\theta id}, C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ Since $\theta \in dom(S)$

$H[\ell] = O_\ell = \langle O_{\ell id}, C_\ell\texttt{<}\overline{D_\ell}\texttt{>}\rangle \in DO$ Since $\ell \in dom(S)$

this proves (1), and (2).

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ By assumption

$\forall \ell \in dom(S),\ \Sigma(\ell) = C\texttt{<}\overline{\ell'.d}\texttt{>}$ Since $\Sigma \vdash S$

$H[\theta] = O = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ By DF-APPROX

$\forall \theta'_j.d_j \in \overline{\theta'.d}\ K[\theta'_j.d_j] = D_j = \langle D_{id_j}, d_j\rangle \in rng(DD)$ By DF-APPROX

$\forall d_i \in domains(C\texttt{<}\overline{\theta'.d}\texttt{>})\ K[\theta.d_i] = D_i = \langle D_{id_i}, d_i\rangle$

$\quad \{(O, d_i) \mapsto D_i\} \in DD$ By DF-APPROX

$\forall \ell_{src} \in dom(H),\ fields(\Sigma[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{src}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E'_k \in L_I[(\ell_{src}, \theta)] = \langle H[\ell_{src}], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By DF-APPROX

$\forall \ell_{dst} \in dom(H),\ fields(\Sigma[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{dst}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E_k \in L_E[(\theta, \ell_{dst})] = \langle H[\theta], H[\ell_{dst}], C'_k, Exp\rangle \in DE\ C'_k <: C_k$ By DF-APPROX

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell.f_i = v$ By assumption:

Since $e_0 = \ell \in dom(H) \quad e_1 = v$:

$\ell : \Sigma[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}\ (T'_i\ f_i) \in fields(C_\ell\texttt{<}\overline{p}\texttt{>}) = \overline{T'}\ \overline{f}\ T'_i = C_i\texttt{<}\overline{p'}\texttt{>}$ By sub-derivation of DF-WRITE

$v : \Sigma[v] = C_v\texttt{<}\overline{p''}\texttt{>} \quad \Sigma[v] <: T'_i$ By sub-derivation of DF-WRITE

$DO, DD, DE \vdash_O export(\Sigma[\ell], \Sigma[v])$ By sub-derivation of DF-WRITE

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell$ By sub-derivation of DF-WRITE

$\emptyset, \emptyset, DO, DD, DE \vdash_O v$ By sub-derivation of DF-WRITE

Take $\ell_{dst} = \ell$.

$\ell : \Sigma[\ell] = C_\ell\texttt{<}\overline{p}\texttt{>}\ (T'_i\ f_i) \in fields(C_\ell\texttt{<}\overline{p}\texttt{>}) = \overline{T'}\ \overline{f}\ T'_i = C_i\texttt{<}\overline{p'}\texttt{>}$ By the sub-derivation above

$\forall m.\ mtype(m, \Sigma[\ell]) = \overline{T} \to T_R$

$\quad \forall T_k \in \{\overline{T'}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p'''}\texttt{>}$

$\quad\quad \langle H[\theta], H[\ell], C'_k, Exp\rangle \in DE \quad C'_k <: C_k$ By above DF-APPROX

Take $T_k = T'_i \in \overline{T'}, C_i = C_k$, and $C_v = C'_k$, this proves (3).

**Subcase $e_0 = e'_0$.** Then $e = (e'_0.f_i = e_1)$

From IRC-WRITE-RCV:

$\theta \vdash e'_0; S; H; K; L_I; L_E \leadsto_G e''_0; S'; H'; K'; L'_I; L'_E$ By induction hypothesis

$\theta \vdash e'_0.f_i = e_1; S; H; K; L_I; L_E \leadsto_G e''_0.f_i = e_1; S'; H'; K'; L'_I; L'_E$ By IRC-WRITE-RCV

Take $e' = (e''_0.f_i = e_1)$.

**Subcase $e_0 = v$, and $e_1 = e'_1$.** Then $e = (v.f_i = e'_1)$

From IRC-WRITE-ARG:

$\Gamma, \Upsilon, DO, DD, DE \vdash_O e_1$ By sub-derivation of DF-WRITE

$\theta \vdash e_1; S; H; K; L_I; L_E \leadsto_G e'_1; S'; H'; K'; L'_I; L'_E$ By induction hypothesis

$\theta \vdash v.f_i = e_1; S; H; K; L_I; L_E \leadsto_G v.f_i = e'_1; S'; H'; K'; L'_I; L'_E$ By IRC-WRITE-ARG

Take $e' = (v.f_i = e'_1)$.

**Case DF-INVK** : e $= e_0.m(\overline{e})$. There are three subcases to consider, depending on whether the receiver $e_0$, or the arguments $\overline{e}$ are values.

**Subcase $e_0 = \ell$, and** $\overline{e} = \overline{v}$ that is $e = \ell.m(\overline{v})$

To show:

(1) $O = H[\theta]$

(2) $O_\ell = H[\ell]$

(3) $mtype(m, C_\ell\texttt{<}\overline{p}\texttt{>}) = \overline{T} \to T_R$ $T_R = C_R\texttt{<}\overline{p'}\texttt{>}$

$E' = \langle O_\ell, O, C'_R, Imp\rangle \in DE$ $C'_R <: C_R$

(4) $\forall i \in 1..|\overline{T}|$ $T_i = C_i\texttt{<}\overline{p''}\texttt{>}$ $E_i = \langle O, O_\ell, C'_i, Exp\rangle \in DE$ $C'_i <: C_i$

$DO, DD, DE \vdash_{CT,H} \Sigma$ By assumption

$\forall \ell' \in dom(S), \Sigma[\ell'] = C'\texttt{<}\overline{p}\texttt{>}$ By sub-derivation of DF-SIGMA

$H[\ell'] = O' = \langle C'\texttt{<}\overline{D'}\texttt{>}\rangle \in DO$ By sub-derivation of DF-SIGMA

$H[\theta] = O = \langle O_{\theta id}, C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ Since $\theta \in dom(S)$

$H[\ell] = O_\ell = \langle O_{\ell id}, C_\ell\texttt{<}\overline{D_\ell}\texttt{>}\rangle \in DO$ Since $\ell \in dom(S)$

this proves (1), and (2).

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$ By assumption

$\forall \ell \in dom(S),\ \Sigma(\ell) = C\texttt{<}\overline{\ell'.d}\texttt{>}$ Since $\Sigma \vdash S$

$H[\theta] = O = \langle C\texttt{<}\overline{D}\texttt{>}\rangle \in DO$ By DF-APPROX

$\forall \theta'_j.d_j \in \overline{\theta'.d}\ K[\theta'_j.d_j] = D_j = \langle D_{id_j}, d_j\rangle \in rng(DD)$ By DF-APPROX

$\forall d_i \in domains(C\texttt{<}\overline{\theta'.d}\texttt{>})\ K[\theta.d_i] = D_i = \langle D_{id_i}, d_i\rangle$

$\quad \{(O, d_i) \mapsto D_i\} \in DD$ By DF-APPROX

$\forall \ell_{src} \in dom(H),\ fields(\Sigma[\ell_{src}]) = \overline{T_{src}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{src}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{src}}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E'_k \in L_I[(\ell_{src}, \theta)] = \langle H[\ell_{src}], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By DF-APPROX

$\forall \ell_{dst} \in dom(H),\ fields(\Sigma[\ell_{dst}]) = \overline{T_{dst}}\ \overline{f},$

$\quad \forall m.\ mtype(m, \Sigma[\ell_{dst}]) = \overline{T} \to T_R$

$\quad\quad \forall T_k \in \{\overline{T_{dst}}\} \cup \{\overline{T}\} \quad T_k = C_k\texttt{<}\overline{p}\texttt{>}$

$\quad\quad\quad E_k \in L_E[(\theta, \ell_{dst})] = \langle H[\theta], H[\ell_{dst}], C'_k, Exp\rangle \in DE\ C'_k <: C_k$ By DF-APPROX

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell.m(\overline{v})$ By assumption

$\ell : \Sigma[\ell] = C_\ell\texttt{<}\overline{\ell'.d}\texttt{>}$ By sub-derivation of DF-INVK

$mtype(m, C_\ell\texttt{<}\overline{\ell'.d}\texttt{>}) = \overline{T} \to T_R \quad T_R = C_R\texttt{<}\overline{p'}\texttt{>}$ By sub-derivation of DF-INVK

$DO, DD, DE \vdash_O import(\Sigma[\ell], T_R)$ By sub-derivation of DF-INVK

$\forall i \in 1..|\overline{v}|\ v_i : \Sigma[v_i]\ \Sigma[v_i] <: T_i\ DO, DD, DE \vdash_O export(\Sigma[\ell], \Sigma[v_i])$ By sub-derivation of DF-INVK

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ell$ By sub-derivation of DF-INVK

$\emptyset, \emptyset, DO, DD, DE \vdash_O \overline{v}$ By sub-derivation of DF-INVK

Take $\ell_{src} = \ell$.

$mtype(m, \Sigma[\ell]) = \overline{T} \to T_R \quad T_R = C_R\texttt{<}\overline{p'}\texttt{>}$ By above sub-derivation

$fields(\Sigma[\ell]) = \overline{T'}\ \overline{f}$ By FDJ T-Store

$\forall T_k \in \{\overline{T'}\} \cup \{T_R\} \quad T_k = C_k\texttt{<}\overline{p'''}\texttt{>}$

$\quad \langle H[\ell], H[\theta], C'_k, Imp\rangle \in DE \quad C'_k <: C_k$ By above DF-APPROX

Take $T_k = T_R, C_R = C_k$ and $C'_R = C'_k$, this proves (3).

Take $\ell_{dst} = \ell$.

$mtype(m, \Sigma[\ell]) = \overline{T} \to T_R \quad T_i = C_i\textless\overline{p''}\textgreater$ By above sub-derivation

$fields(\Sigma[\ell]) = \overline{T'}\ \overline{f}$ By FDJ T-Store

$\forall T_k \in \{\overline{T'}\} \cup \{\overline{T}\} \quad T_k = C_k\textless\overline{p'''}\textgreater$

$\langle H[\theta], H[\ell], C'_k, Exp\rangle \in DE \quad C'_k <: C_k$ By above DF-APPROX

Take $\forall i \in 1..\overline{T}$. $T_k = T_i \in \overline{T}, C_i = C_k$ and $C'_i = C'_k$. This proves (4).

**Subcase** $e_0 = e'_0$ that is $e = e'_0.m(\overline{e})$.
From IRC-RecvInvk

$\theta \vdash e'_0; S; H; K; L_I; L_E \leadsto_G e''_0; S'; H'; K'; L'_I; L'_E$ By induction hypothesis

$\theta \vdash e'_0.m(\overline{e}); S; H; K; L_I; L_E \leadsto_G e''_0.m(\overline{e}); S'; H'; K'; L'_I; L'_E$ By IRC-RecvInvk

Take $e' = e''_0.m(\overline{e})$.

**Subcase** $e_0 = v$ that is $e = v.m(v_{1..i-1}, e_i, e_{i+1..n})$.
From IRC-ArgInvk:

$\Gamma, \Upsilon, DO, DD, DE \vdash_O e_i$ By sub-derivation of Df-Invk

$\theta \vdash e_i; S; H; K; L_I; L_E \leadsto_G e'_i; S'; H'; K'; L'_I; L'_E$ By induction hypothesis

$\theta \vdash v.m(v_{1..i-1}, e_i, e_{i+1..n}); S; H; K; L_I; L_E \leadsto_G$
$v.m(v_{1..i-1}, e'_i, e_{i+1..n}); S'; H'; K'; L'_I; L'_E$ By IRC-ArgInvk

Take $e' = v.m(v_{1..i-1}, e'_i, e_{i+1..n})$.

**Case DF-CONTEXT** : e $= \ell \triangleright e_0$. there are two subcases to consider, depending on whether $e_0$ is a value

**Subcase** $e_0$ **is a value** that is $e = \ell \triangleright v$.
From IR-CONTEXT:
Then IR-CONTEXT can apply. Take $e' = v$.

**Subcase** $e_0$ **is not a value** that is $e = \ell \triangleright e'_0$.
From IRC-CONTEXT:

$\ell \vdash e_0; S; H; K; L_I; L_E \leadsto_G e'_0; S'; H'; K'; L'_I; L'_E$ By induction hypothesis

$\theta \vdash \ell \triangleright e_0; S; H; K; L_I; L_E \leadsto_G \ell \triangleright e'_0; S'; H'; K'; L'_I; L'_E$ By IRC-CONTEXT

Take $e' = \ell \triangleright e'_0$.

■

$$\frac{}{\theta \vdash e; S; H; K; L_I; L_E \rightsquigarrow^*_G e; S; H; K; L_I; L_E}\text{[Df-Reflex]}$$

$$\frac{\begin{array}{c}\theta \vdash e; S; H; K; L_I; L_E \rightsquigarrow^*_G e''; S''; H''; K''; L''_I; L''_E \\ \theta \vdash e''; S''; H''; K''; L''_I; L''_E \rightsquigarrow_G e'; S'; H'; K'; L'_I; L'_E\end{array}}{\theta \vdash e; S; H; K; L_I; L_E \rightsquigarrow^*_G e'; S'; H'; K'; L'_I; L'_E}\text{[Df-Trans]}$$

**Figure 15:** Reflexive, transitive closure of the instrumented evaluation relation

## 4.6 Theorem: Object Graph Soundness

*If*

$G = \langle DO, DD, DE \rangle$

$DO, DD, DE \vdash (CT, e_{root})$

$\forall e,\ \theta_0 \vdash e; \emptyset, \emptyset, \emptyset, \emptyset, \emptyset \rightsquigarrow^*_G e; S; H; K; L_I; L_E$

$\Sigma \vdash S$

*then*

$DO, DD, DE \vdash_{CT,H} \Sigma$

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$

where $\rightsquigarrow^*_G$ relation is the reflexive and transitive closure of $\rightsquigarrow_G$ relation (Fig. 15). $\theta_0$ is the location of the first object instantiated by $e_{root}$.

To prove the Object Graph Soundness theorem, we need to show:

(1) $DO, DD, DE \vdash_{CT,H} \Sigma$

(2) $(S, H, K, L_I, L_E) \sim (DO, DD, DE)$

**Proof:** The proof is by induction on the $\rightsquigarrow^*_G$ relation. There are two cases to consider: [1]

**Case Df-Reflex** :

Since $S = \emptyset$ :

$(S, H, K, L_I, L_E) \sim G$

Immediately, from Df-Sigma store constraint with $S = \emptyset$:

$DO, DD, DE \vdash_{CT,H} \Sigma$

**Case Df-Trans** :

By assumption:

$\theta_0 \vdash e; \emptyset; \emptyset; \emptyset; \emptyset; \emptyset \rightsquigarrow^*_G e; S; H; K; L_I; L_E$

Since $S = \emptyset$ :

$(\emptyset, \emptyset, \emptyset, \emptyset, \emptyset) \sim G$

By inversion of Df-Trans:

[1] The soundness proof follows similar steps to the one of points-to analysis [1].

$\theta_0 \vdash e; \emptyset; \emptyset; \emptyset; \emptyset; \emptyset \leadsto^*_G e'; S'; H'; K'; L'_I; L'_E$
By induction hypothesis:
$(S'; H'; K'; L'_I; L'_E) \sim G$
By inversion of DF-TRANS:
$\theta_0 \vdash e'; S'; H'; K'; L'_I; L'_E \leadsto_G e; S; H; K; L_I; L_E$
By preservation:
$(S; H; K; L_I; L_E) \sim G$

By assumption:
$\theta_0 \vdash e; \emptyset; \emptyset; \emptyset; \emptyset; \emptyset \leadsto^*_G e; S; H; K; L_I; L_E$
Since $S = \emptyset$ :
$(\emptyset, \emptyset, \emptyset, \emptyset, \emptyset) \sim G$
By inversion of DF-TRANS:
$\theta_0 \vdash e; \emptyset; \emptyset; \emptyset; \emptyset; \emptyset \leadsto^*_G e'; S'; H'; K'; L'_I; L'_E$
By induction hypothesis:
$DO, DD, DE \vdash_{CT,H'} \Sigma'$
By inversion of DF-TRANS:
$\theta_0 \vdash e'; S'; H'; K'; L'_I; L'_E \leadsto_G e; S; H; K; L_I; L_E$
By preservation:
$DO, DD, DE \vdash_{CT,H} \Sigma$

■

### 4.6.1 Lemmas

To prove the Progress and Preservation theorems, we use the following lemmas. We intended to use the first four lemmas, (i.e. the import and export lemmas) in the Progress theorem proof. However, we complete the Progress proof without their use. We keep them for backward compatibility with the previous version of this report.

**Df-Substitution Lemma**.
*If*
$\Gamma \cup \{\overline{x} : \overline{T_f}\}, \Sigma, \theta \vdash e : T$
$\Gamma \cup \{\overline{x} : \overline{T_f}\}, \Upsilon, DO, DD, DE \vdash_O e$
$\Gamma, \Sigma, \theta \vdash \overline{v} : \overline{T_a}$ where $\overline{T_a} <: [\overline{v}/\overline{x}]\overline{T_f}$
*then*
$\Gamma, \Sigma, \theta \vdash [\overline{v}/\overline{x}]e : T'$ *for some* $T' <: [\overline{v}/\overline{x}]T$
$\Gamma, \Upsilon, DO, DD, DE \vdash_O [\overline{v}/\overline{x}]e$
**Proof:** By induction on the $\Gamma, \Upsilon, DO, DD, DE \vdash_O e$ relation. ■

**Df-Weakening Lemma**.
*If*
$\Gamma, \Upsilon, DO, DD, DE \vdash_O e$
*then*
$\Gamma, \Upsilon \cup \{C\langle\overline{D}\rangle\}, DO, DD, DE, \vdash_O e$

**Proof:** By induction on the $\Gamma, \Upsilon, DO, DD, DE \vdash_O e$ relation. ■

**Df-Strengthening Lemma**.

*If*

$\Gamma, \emptyset, DO, DD, DE \vdash_O \texttt{new}\ C{<}\overline{p}{>}(v)$

$\forall i \in 1..|\overline{p}| \quad D_i = DD[(O, p_i)]$

$\Gamma, \Upsilon \cup \{C{<}\overline{D}{>}\}, DO, DD, DE, \vdash_{O'} e'$

*then*

$\Gamma, \Upsilon, DO, DD, DE, \vdash_O e$

**Proof:** By induction on the $\Gamma, \Upsilon, DO, DD, DE \vdash_O e$ relation. ■

**Df-Domains Lemma**.

*If*

$\emptyset, \Sigma, \theta \vdash e : T$

$\Sigma \vdash S$

$DO, DD, DE \vdash_{CT,H} \Sigma$

$\emptyset, \emptyset, DO, DD, DE \vdash_O \ \mathit{new}\ C{<}\overline{p}{>}(\overline{v})$

$(S, H, K, L_I, L_E) \sim (DO, DD, DE)$

$DO, DD, DE \vdash_O \mathit{ddomains}(C, O_C)$

$\forall i \in 1..|\overline{p}| \quad D_i = DD[(O, p_i)]$

$O_C = \langle C{<}\overline{D}{>}\rangle \quad \{O_C\} \subseteq DO$

*then*

$\forall d_j \in \mathit{domains}(C{<}\overline{p}{>}) \quad D_j = DD[(O_C, d_j)]$

**Proof:** By induction on the $DO, DD, DE \vdash_O \mathit{ddomains}(C, O_C)$ relation. ■

**Differences with earlier versions of this work.** Our formalization refines the one in Rawshdeh's thesis [20]. Our analysis does not consider creational edges, it focuses on usage edges only. We completed the formalization of the static and dynamic semantics, and proved progress, preservation, and soundness. We defined the approximation relation, and used the additional maps $L_I$ and $L_E$ to track import and export edges.

**Differences with points-to analysis.** Our formalization is similar to the one for the points-to analysis [1, Section 3.2 and 3.3]. The two analyses create the same object-domain hierarchy, but the analysis in this paper shows additional edges that are missing from an OOG with points-to edges. The key differences in the formalization deal with generating the dataflow edges and the soundness proof. The previous work made a simplistic assumption about dataflow edges, namely that they can be approximated by reverting points-to edges, but the assumption turned out to be imprecise.

# 5 Addressed Challenges

We discuss how our analysis addressed each challenge in Section 2.

**Object soundness.** The OGraph shows a unique representative for each runtime object. We built the map $H$ from runtime object to an OObject, and proved that each runtime object $\ell$ has a unique representative OObject (Section 4.6). We detailed the steps of building the map in the Ir-New inference rule of dynamic semantics (Fig. 7).

**Aliasing.** Ownership domains ensures the aliasing invariant: two objects in different domains cannot alias. The analysis create separate OObjects for different parent ODomain. Although the code may show only one domain declaration `domain d` followed by a `new` expression `new`$C$<$d, ...$>, the analysis creates distinct ODomains depending on the context `OObject` $O$ in which the domain declaration is analyzed. For two variables of the same type, that may refer to the same runtime object, the analysis shows a unique representative $C{<}\overline{D}{>}$ in $DO$. The condition $O_C = \langle C{<}\overline{D}{>}\rangle \quad \{O_C\} \subseteq DO$ in Df-New ensures this.

**Edge soundness.** If there is a runtime dataflow communication between two runtime objects, the OGraph must show an OEdge between the representatives of these objects. We built the maps $L_I$ and $L_E$ that map each pair of runtime objects ($\ell_1$, $\ell_2$) to an OEdge between the representative of $\ell_1$ and $\ell_2$ in the map $H$, and we provided the soundness proof (Section 4.6). We detailed the steps of building the maps in the Ir-Read, Ir-Write, Ir-Invk inference rules of dynamic semantics(Fig. 7).

**Summarization.** In the presence of recursive types, the analysis stops creating new ODomains when the a domain declaration is analyzed using the same context. The analysis reuses an existing ODomain and creates a cycle with respect to ownership edges in the OGraph, which ensures a finite representation and a finite depth for the ROG (Fig. 5[Df-New, Aux-Dom]). In an extended example, we show the detailed steps of the analysis while analyzing a QuadTree recursive type (Section 4.2).

**Hierarchy.** The extracted OGraph contains a hierarchical organization of objects given by the ownership edges. A OObject has domains, which contain other objects to form its substructure, and so on. The OGraph provides abstraction by ownership hierarchy when it shows architecturally significant objects near the top of the hierarchy, and instances of data structures further down.

**Precision.** To avoid excessive merging of objects, the analysis relies on the aliasing precision provided by ownership domains. We map runtime objects in distinct runtime domains are mapped to distinct OObjects. The analysis also uses ownership domains to increase the precision of dataflow communication edges. While extracting OEdges, the analysis relies on Df-Lookup. For a variable of type $C'<\overline{p}>$, Df-Lookup returns only a subset of all the objects of class $C'$ or its subclasses in $DO$. The analysis uses these results to determine the source and destination OObjects, and the class representing the edge label (Fig. 5[Df-Lookup]).

## 5.1 Analysis Invariants

- The analysis might create multiple ODomains for a single domain declaration $C::d$. As an exception, for top-level domain declarations, the analysis creates a single ODomain.
- The analysis might create multiple OObjects for a single expression `new`.
- The analysis might create a single OObject for multiple `new` expressions in the code, when the same class is instantiated multiple times. The `new` expressions might be scattered over multiple methods in different classes.
- For one field expression the analysis might create multiple import edges, depending on the result of *lookup* on the type of the receiver.
- The analysis does not create an export dataflow communication edge for a method invocation expression when the method has no arguments.
- The analysis does not create an import dataflow communication edge for a method invocation expression when the method returns `void`.
- In the presence of recursive types, the analysis reuses ODomains and creates a cycle in the ownership structure of the OGraph.

# 6 Evaluation

## 6.1 Notation.

We use the following notation: `obj.DOM` refers to either a public or a private domain `DOM` inside object `obj`. We effectively treat a domain as a field of an object, e.g., `main.DOC`; `obj1.DOM.obj2` refers to the object `obj2` inside the domain `DOM` of `obj1`, e.g., `main.DOC.model`; $C$::$d$ refers to a domain $d$ qualified by the class $C$ that declares it. The first domain parameter corresponds to the owning domain, and we call it `OWNER`. We use capital letters for domain names to distinguish them from other program identifiers.

The analysis calls the *analyze* method for every expression $e$, with the bindings $p_i \mapsto D_i$, and the context $O$:

$$analyze(e, [..., p_i \mapsto D_i, ...], O)$$

When it encounters inheritance, *analyze* recursively analyzes the base class of the current class (in that case, we do not show the parameter $e$).

A boxed statement represents the analysis step performed while analyzing the preceding statement. When a boxed statement precedes a class declaration, it includes the mapping of formal domain parameters to actual domains, and the context OObject $O$. Consecutive boxed statements correspond to consecutive analysis steps.

For example, when the analysis encounters a method invocation expression, it calls *lookup* multiple times to find the type of the receiver expression, the type of method arguments, and the return type. Next, it creates dataflow edges, and continues in the body of $m$. For brevity, we include only the most interesting *lookup* calls.

## 6.2 Worked Example.

Our analysis starts with the developer selecting the root type, in this case, the `Main` class (Fig. 16). The analysis creates the OObject (O0) for the `main` object allocation. Then, it analyzes `Main` in the context of `main`. Before analyzing `Main`, the analysis maps all formal domain parameters, if any, to their corresponding ODomains in the OGraph. In this case, the analysis maps

```
Main<SHARED> main = new Main();
OObject(main, Main<SHARED>)  (O0)
analyze ( new Main<OWNER>(), [Main::OWNER ↦ SHARED], O ↦ main )

[Main::OWNER↦ ::SHARED], O↦ main
class Main<OWNER> {
  public domain DOC, VIEW;
  ODomain(main.DOC, Main::DOC)  (D1)
  ODomain(main.VIEW, Main::VIEW)  (D2)

  BarChart<VIEW, DOC> barChart = new BarChart();
  OObject(main.VIEW.barChart, BarChart<main.VIEW, main.DOC>)  (O1)
  analyze(new BarChart<OWNER, M>(), [BarChart::OWNER ↦ main.VIEW, BarChart::M ↦ main.DOC], O ↦
  main.VIEW.barChart)
  // continue to Fig. 17

  PieChart<VIEW, DOC> pieChart = new PieChart();
  OObject(main.VIEW.pieChart, PieChart<main.VIEW, main.DOC>)  (O2)
  analyze(new PieChart<OWNER, M>(), [PieChart::OWNER ↦ main.VIEW, PieChart::M ↦ main.DOC], O ↦
  main.VIEW.pieChart)
  // The analysis is similar to barChart, omitted for brevity

  Model<DOC, VIEW> model = new Model();
  OObject(main.DOC.model, Model<main.DOC, main.VIEW>)  (O3)
  analyze(new Model<OWNER, V>(), [Model::OWNER ↦ main.DOC, Model::V ↦ main.VIEW],O ↦
  main.DOC.model)
   // continue to Fig. 18
    ...
```

**Figure 16:** Abstractly interpreting the program, starting with the root class `Main`.

`MAIN::OWNER` to the global domain `::SHARED`. The analysis also tracks the context OObject $O$.

The analysis continues inside `Main` and finds that the first statement is a domain declaration. In response, it creates two ODomains: `DOC` and `VIEW`. Next, for the object allocation statement of the `barChart` object, the analysis creates an OObject (O1), and proceeds to analyze the class `BarChart`, mapping $O$ to `main.VIEW.barChart`. It also maps the domain parameter `BarChart::OWNER` to `main.VIEW`, and `BarChart::M` to `main.DOC`.

Next, the analysis covers `BarChart` and its base class `BaseChart` in the context of the OObject `barChart` (Fig. 17). The analysis proceeds into the base class `BaseChart` mapping `BaseChart::OWNER` to `main.VIEW`, and `BaseChart::M` to `main.DOC` while the context $O$ re-

```
[BarChart::OWNER ↦ main.VIEW, BarChart::M ↦ main.DOC], O ↦ main.VIEW.barChart
class BarChart<OWNER, M> extends BaseChart<OWNER, M> {
  analyze([BaseChart::OWNER ↦ main.VIEW, BaseChart::M ↦ main.DOC], O ↦ main.VIEW.barChart)

  public void update(Msg<DATA> msg) {...}
}

[BaseChart::OWNER ↦ main.VIEW, BaseChart::M ↦ main.DOC], O ↦ main.VIEW.barChart
class BaseChart<OWNER, M> extends Listener<OWNER> {
  domain OWNED;
  ODomain(main.VIEW.barChart.OWNED, BaseChart::OWNED)  (D3)

  public domain DATA;
  ODomain(main.VIEW.barChart.DATA, BaseChart::DATA)  (D4)

  List<OWNED, Listener<M>> listeners = new List();
  OObject(main.VIEW.barChart.OWNED.listeners, List<main.VIEW.barChart.OWNED,
  Listener<main.DOC>)  (O4)
  analyze(new List<OWNER, ELTS>(), [List::OWNER ↦ main.VIEW.barChart.OWNED, List::ELTS
  ↦ main.DOC], O ↦ main.VIEW.barChart.OWNED.listeners)
  ...
}

[List::OWNER ↦ main.VIEW.barChart.OWNED, List::ELTS ↦ main.DOC], O
↦main.VIEW.barChart.OWNED.listeners
T = Listener  //generic type
class List<OWNER, T<ELTS>> {
  T<ELTS> value; // ELTS is a domain parameter for list elements
  ...
}
```

**Figure 17:** Abstractly interpreting the program (continued): `BarChart`, `BaseChart` and `List`.

mains unchanged. Inside `BaseChart`, the analysis encounters two domain declarations: `domain OWNED` and `public domain DATA`. As a result, it creates a private and a public ODomains for `barChart`. Next statement is an instantiation of the class `List`, the analysis creates the OObject `main.VIEW.barChart.OWNED.listeners` (O4) inside the `barChart.OWNED` domain. Since `List` has no domain declarations or `new` statements, the analysis backtracks to `BaseChart`, and then further on to `Main`.

The analysis of class `PieChart`, its base class `BaseChart`, and its `List` is similar to `BarChart`, so we omitted it for brevity.

Back in `Main` (Fig. 16), the analysis creates the OObject `main.DOC.model` (O3) corresponding to

```
[ Model::OWNER ↦ main.DOC, Model::V ↦ main.VIEW], O ↦ main.DOC.model
class Model<OWNER, V> extends Listener<OWNER> {
  domain OWNED;
  ODomain(main.DOC.model.OWNED, Model::OWNED)  (D9)

  public domain DATA;
  ODomain(main.DOC.model.DATA, Model::DATA)  (D10)

  List<OWNED, Listener<V>> listeners = new List();
  OObject(main.DOC.model.OWNED.listeners, List<main.DOC.model.OWNED,
  Listener<main.VIEW>>)  (O6)
  analyze(new List<OWNER, ELTS>(), [List::ELTS ↦ main.VIEW, List::OWNER ↦
  main.DOC.model.OWNED], O ↦ main.DOC.model.OWNED.listeners)
  ...
} [List::OWNER ↦ main.DOC.model.OWNED, List::ELTS ↦ main.VIEW], O
  ↦main.DOC.model.OWNED.listeners
T = Listener  //generic type
class List<OWNER, T<ELTS>> {

  T<ELTS> value; // ELTS is a domain parameter for list elements
  ...
}
```

**Figure 18:** Abstractly interpreting the program (continued): `Model` and `List`.

the instantiation of the class `Model` inside the ODomain `DOC`. Then it proceeds to analyze `Model` in the context of `main.DOC.model` (Fig. 18). The analysis maps the domain parameter `Model::OWNER` to `main.DOC`, and `Model::V` to `main.VIEW`. Similar to `BaseChart` the analysis creates a private and a public ODomain `OWNED` and `DATA`, and an OObject `main.DOC.model.OWNED.listeners`. Note that the analysis distinguishes between the `listeners` object owned by `model`, and the one owned by `barChart` although they are both instances of `List`.

Next, the analysis encounters the method invocation `main.run()` (Fig. 19). In this case, $O$ correspond to `main`. Inside `run()`, the analysis encounters `model.addListener(barChart)`, and it changes the context to `main.DOC.model`. This method invocation introduces an export edge (E1) from `main` to `model` because `main` exports an object of type `BarChart` to `model` as the argument of `addListener(Listener)`. For edge label, the analysis calls *lookup* and finds one OObject of type `BarChart<main.VIEW, main.DOC>`, `main.VIEW.barChart`.

Inside `addListener(Listener)` of `Model`, the analysis encounters `listeners.add(l)`.

```
main.run();
analyze(main.run(), [Main::OWNER ↦ SHARED], O ↦ main)

public class Main<OWNER> {
  ...
  public void run() {

    model.addListener(barChart);
    analyze(model.addListener(barChart), [Model::OWNER ↦ main.DOC, Model::V ↦
    main.VIEW], O ↦ main.DOC.model
    OObject(main.DOC.model, Model<main.DOC, main.VIEW>) ∈ lookup(Model<main.DOC,
    main.VIEW>)
    OEdge(main, main.DOC.model, BarChart, Exp)  (E1)
    // continue to Fig. 20

    model.addListener(pieChart);
    // The analysis is similar to model.addListener(barChart)
    // Omitted for brevity
    OEdge(main, main.DOC.model, PieChart, Exp)  (E4)

    barChart.addListener(model);
    analyze(barChart.addListener(model), [BaseChart::OWNER ↦ main.VIEW, BaseChart::M ↦
    main.DOC], O ↦ main.VIEW.barChart)
    OObject(main.VIEW.barchart, BarChart<main.VIEW, main.DOC>) ∈
    lookup(BarChart<main.VIEW, main.DOC>)
    OEdge(main, main.VIEW.barChart, Model, Exp)  (E7)
    // continue to Fig. 21

    pieChart.addListener(model);
    // The analysis is similar to barChart.addListener(model)
    // Omitted for brevity
    OEdge(main, main.VIEW.pieChart, Model, Exp)  (E9)

    model.notifyObservers();
    analyze(model.notifyObservers(), [Model::OWNER ↦ main.DOC, Model::V ↦ main.VIEW], O
    ↦ main.DOC.model)
    // continue to Fig. 22

    barChart.notifyObservers();
    analyze(barChart.notifyObservers(), [BaseChart::OWNER ↦ main.VIEW, BaseChart::M ↦
    main.DOC], O ↦ main.VIEW.barChart)
    // continue to Fig. 23

    pieChart.notifyObservers();
    // The analysis is similar to barChart.notifyObservers()
    // Omitted for brevity
  }
}
```

**Figure 19:** Abstractly interpreting the program, class `Main`.

```
[Model::OWNER ↦ main.DOC, Model::V ↦ main.VIEW], O ↦ main.DOC.model
class Model<OWNER,V> extends Listener<OWNER> {
  ...
  l:BarChart<main.VIEW, main.DOC>
  public void addListener(Listener<V> l) {
    listeners.add(l);
    analyze(listeners.add(l),[List::OWNER ↦ main.DOC.model.OWNED, List::ELTS ↦
    main.VIEW], O ↦ main.DOC.model.OWNED.listeners)
    OObject(main.DOC.model.OWNED.listeners, List<main.DOC.model.OWNED,
    Listener<main.VIEW>>) ∈ lookup(List<main.DOC.model.OWNED, Listener<main.VIEW>>)
    OEdge(main.DOC.model, main.DOC.model.OWNED.listeners, BarChart, Exp) (E2)
  }
} [List::OWNER ↦ main.DOC.model.OWNED, List::ELTS ↦ main.VIEW], O
  ↦main.DOC.model.OWNED.listeners
 T = Listener //generic type
 class List<OWNER, T<ELTS>> {
    T<ELTS> value; // ELTS is a domain parameter for list elements
    public void add(T<ELTS> value) {...}
    ...
}
```

**Figure 20:** Abstractly interpreting the program (continued): `Model` addListener method.

```
[BarChart::OWNER ↦ main.VIEW, BarChart::M ↦ main.DOC], O ↦ main.VIEW.barChart
class BarChart<OWNER, M> extends BaseChart<OWNER, M> {
  analyze([BaseChart::OWNER ↦ main.VIEW, BaseChart::M ↦ main.DOC], O ↦
  main.VIEW.barChart)

  public void update(Msg<DATA> msg) {...}
}

[BaseChart::OWNER ↦ main.VIEW, BaseChart::M ↦ main.DOC], O ↦ main.VIEW.barChart
class BaseChart<OWNER, M> extends Listener<OWNER> {
  ...
  l : Model<main.DOC, main.VIEW>
  public void addListener(Listener<M> l) {
    listeners.value = l; // field write - export dataflow communication
    OObject(main.VIEW.barChart.OWNED.listeners, List<main.VIEW.barChart.OWNED,
    Listener<main.DOC>>) ∈ lookup(List<main.VIEW.barChart.OWNED, Listener<main.DOC>>)
    OEdge(main.VIEW.barChart, main.VIEW.barChart.OWNED.listeners, Model, Exp) (E8)
  }
}
```

**Figure 21:** Abstractly interpreting the program (continued): `BaseChart` addListener method.

```
[Model::OWNER ↦ main.DOC, Model::V ↦ main.VIEW], O ↦ main.DOC.model
class Model<OWNER,V> extends Listener<OWNER> {
  ...
  public void notifyObservers() {
    MsgMtoV<DATA> mTOv = new MsgMtoV();
    OObject(main.DOC.model.DATA.mTOv, MsgMtoV<main.DOC.model.DATA>) (O7)
    analyze(new MsgMtoV<OWNER>(), [MsgMtoV::OWNER ↦ main.DOC.model.DATA], O ↦
    main.DOC.model.DATA.mTOv)

    Listener<V> l = listeners.value; //field read - import dataflow communication
    OObject(main.DOC.model.OWNED.listeners, List<main.DOC.model.OWNED,
    Listener<main.VIEW>>) ∈ lookup(List<main.DOC.model.OWNED, Listener<main.VIEW>>)
    OObject(main.VIEW.barChart, BarChart<main.VIEW, main.DOC>) ∈
    lookup(Listener<main.VIEW>)
    OObject(main.VIEW.pieChart, PieChart<main.VIEW, main.DOC>) ∈
    lookup(Listener<main.VIEW>)
    OEdge(main.DOC.model.OWNED.listeners, main.DOC.model, BarChart, Imp) (E11)
    OEdge(main.DOC.model.OWNED.listeners, main.DOC.model, PieChart, Imp) (E12)

    l.update(mTOv);
    analyze(l.update(vTOm),[BarChart::OWNER ↦ main.VIEW, BarChart::M ↦ main.DOC], O
    ↦ main.VIEW.barChart)
    OObject(main.VIEW.barChart, BarChart<main.VIEW, main.DOC>) ∈
    lookup(Listener<main.VIEW>)
    OEdge(main.DOC.model, main.VIEW.barChart, MsgMtoV, Exp) (E13)

    analyze(l.update(vTOm),[PieChart::OWNER ↦ main.VIEW, PieChart::M ↦ main.DOC], O
    ↦ main.VIEW.pieChart)
    OObject(main.VIEW.pieChart, PieChart<main.VIEW, main.DOC>) ∈
    lookup(Listener<main.VIEW>)
    OEdge(main.DOC.model, main.VIEW.pieChart, MsgMtoV, Exp) (E14)
    }
  }
}
```

**Figure 22:** Abstractly interpreting the program (continued): `Model` notifyObservers method.

A first *lookup* call returns the OObject `listeners` of type `List<main.DOC.model.OWNED, Listener<main.VIEW>>`, i.e., the object of type `List` of the ODomain `model.OWNED`, which is a collection of elements of type `Listener`, and each element of the collection is of the ODomain `main.VIEW` (Fig. 20). A second *lookup* returns the OObject `barChart` and, the analysis adds an OEdge (E2) between `model` and `listeners` labeled using `BarChart`. At this point the analysis

```
[BarChart::OWNER ↦ main.VIEW, BarChart::M ↦ main.DOC], O ↦ main.VIEW.barChart
class BarChart<OWNER, M> extends BaseChart<OWNER, M> {
  analyze([BaseChart::OWNER ↦ main.VIEW, BaseChart::M ↦ main.DOC], O ↦
  main.VIEW.barChart)

  public void update(Msg<DATA> msg) {...}
} [BaseChart::OWNER ↦ main.VIEW, BaseChart::M ↦ main.DOC], O ↦ main.VIEW.barChart
class BaseChart<OWNER, M> extends Listener<OWNER> {
  ...
  public void notifyObservers() {
    MsgVtoM<DATA> vTOm = new MsgVtoM();
    OObject(main.VIEW.barChart.DATA.vTOm, MsgVtoM<main.VIEW.barChart.DATA>) (O8)
    analyze(new MsgVtoM<OWNER>(), [MsgVtoM::OWNER ↦ main.VIEW.barChart.DATA], O ↦
    main.VIEW.barChart.DATA.vTOm)

    Listener<M> l = listeners.getFirst(); //generates import dataflow communication
    analyze(listeners.getFirst(), [List::OWNER ↦ main.VIEW.barChartl.OWNED, List::ELTS
    ↦ main.DOC], O ↦ main.VIEW.barChart.OWNED.listeners)
    OObject(main.VIEW.barChart.OWNED.listeners, List<main.VIEW.barChart.OWNED,
    Listener<main.DOC>>) ∈ lookup(List<main.VIEW.barChart.OWNED, Listener<main.DOC>>)
    OObject(main.DOC.model, Model<main.DOC, main.VIEW>) ∈ lookup(Listener<main.DOC>)
    OEdge(main.VIEW.barChart.OWNED.listeners, main.VIEW.barChart, Model, Imp) (E15)

    l.update(vTOm);
    analyze(l.update(vTOm),[Model::OWNER ↦ main.DOC, Model::V ↦ main.VIEW], O ↦
    main.DOC.model)
    OObject(main.DOC.model, Model<main.DOC, main.VIEW>) ∈ lookup(Listener<main.DOC>)
    OEdge(main.VIEW.barChart, main.DOC.model, MsgVtoM, Exp)  (E16)
  }
}

[List::OWNER ↦ main.VIEW.barChart.OWNED, List::ELTS ↦ main.DOC], O
↦main.VIEW.barChart.OWNED.listeners
 T = Listener  //generic type
 class List<OWNER, T<ELTS>> {
    T<ELTS> value; // ELTS is a domain parameter for list elements
    public T<ELTS> getFirst() {  return value;  }
}
```

**Figure 23:** Abstractly interpreting the program (continued): `BaseChart` notifyObservers method.

backtracks to `Main` (Fig. 19).

Similar to the previous analyzed statement, the analysis of the method invocation `model.addListener(pieChart)` creates two edges labeled `PieChart`: from `main` to `model` (E4), from `model` to `listeners` (E5).

For barChart.addListener(model) and pieChart.addListener(model), the analysis creates two OEdges labeled with Model: from main to barChart (E7), and from main to pieChart (E9). In both cases, the analysis encounters statement listeners.value = l in the addListener method of the class BaseChart. In response to this field write statement, the analysis calls *lookup* with the parameter `List<main.VIEW.barChart.OWNED, Listener<main.DOC>>`, and `List<main.VIEW.pieChart.OWNED, Listener<main.DOC>>`, respectively. The resulting OObjects are the two listeners owned by barChart and pieChart, respectively, and in each case, the analysis creates an OEdge labeled with Model (i.e., the actual type of l): from barChart to listeners (E8), and from pieChart to its owned listeners (E10) (Fig. 21).

Back in run(), the analysis processes three method invocations notifyObservers() with different receivers (Fig. 19). Since the method has no parameters, the analysis does not include additional OEdge from main to the receivers. The analysis continues in the notifyObservers() methods of Model, BarChart, and PieChart.

While analyzing notifyObservers() of Model in the context of model ($O$), the analysis encounter the first statement, a class instantiation, and it creates a new OObject (O7) mTOv in the public domain DATA of model (Fig. 22).

The second statement contains the field read expression listener.value. In response, the analysis calls *lookup* twice. First *lookup* searches for object of type List in model.OWNED, while the second *lookup* searches for objects of type `Listener<main.VIEW>`. For the first call *lookup* returns listeners, while for the later call, *lookup* returns two OObjects: barChart and pieChart. As a result, the analysis creates two OEdges from listeners to model, one labeled with BarChart (E11), and the other labeled with PieChart (E12). Note that if the second *lookup* would not have been performed, the label would be Listener, which can be interpreted as any of the five classes extending Listener: Model, BarChart, PieChart or BaseChart. Therefore, by calling *lookup*, the analysis produces more accurate labels. Another observation is that the field read expression introduces an import edge, and $O$ is the destination of the edge, while in the previous cases $O$ was the source.

The third and last statement contains the method invocation l.update(mTOv). The analysis calls again *lookup* searching for OObjects of type `Listener<main.VIEW>`. The result are the two OObjects `barChart` and `pieChart`. The analysis includes two OEdges labeled as MsgMtoV: from `model` to `barChart` (E13), and from `model` to `pieChart` (E14).

Since the `update` methods are empty, the analysis returns to `Main` and proceeds to `notifyObservers()` with `barChart` as receiver ($O$) (Fig. 23). The method is implemented in the superclass `BaseChart`, and the analysis performs the similar steps as previously discussed with two major differences. First, the second statement is the method invocation `listeners.getFirst()` instead of field read. The `getFirst()` method returns an alias to the `value` field. After a first *lookup* identifies `listeners` as the receiver of `getFirst()`, the analysis calls a second *lookup* searching for OObjects of type `Listener<main.DOC>`, which corresponds to the returned type of `getFirst()`. The result of the second *lookup* is `model`, and its class constitutes the edge label. As for field read, $O$ is the destination of the OEdge from `listeners` to `barChart` (E15). Second, the analysis looks up the OObjects of a subtype of the local variable `l` in the method invocation `l.update(vTOm)`, and it finds only one OObject in the `main.DOC` domain (i.e., `model`). Therefore, it creates the OEdge from `barChart` to `model` labeled with `MsgVtoM` (E16).

The analysis concludes with the method invocation `pieChart.notifyObservers()`, and its corresponding implementation from `BaseChart`. The analysis performs the same steps previously discussed in the context of `pieChart` ($O$).

### 6.3 Graphical notation.

In the visualization of the OOG, we graphically distinguish between objects and domains by using a rectangle-shape to represent an object and a dashed rectangle-shape to represent a domain. We further distinguish between public and private domains using a thin dashed border for a public domain, and a bold dashed border for a private domain. In all cases, we label each rectangle with the name of the object or domain that corresponds to it. We represent the dataflow edges with a red solid arrow, and the ownership edges from domains to objects and vice-versa with a black arrow. We display as a root the `SHARED` domain, which constitutes the root node of the graph. The only object `SHARED` we display is the first object instantiated when the application starts, in

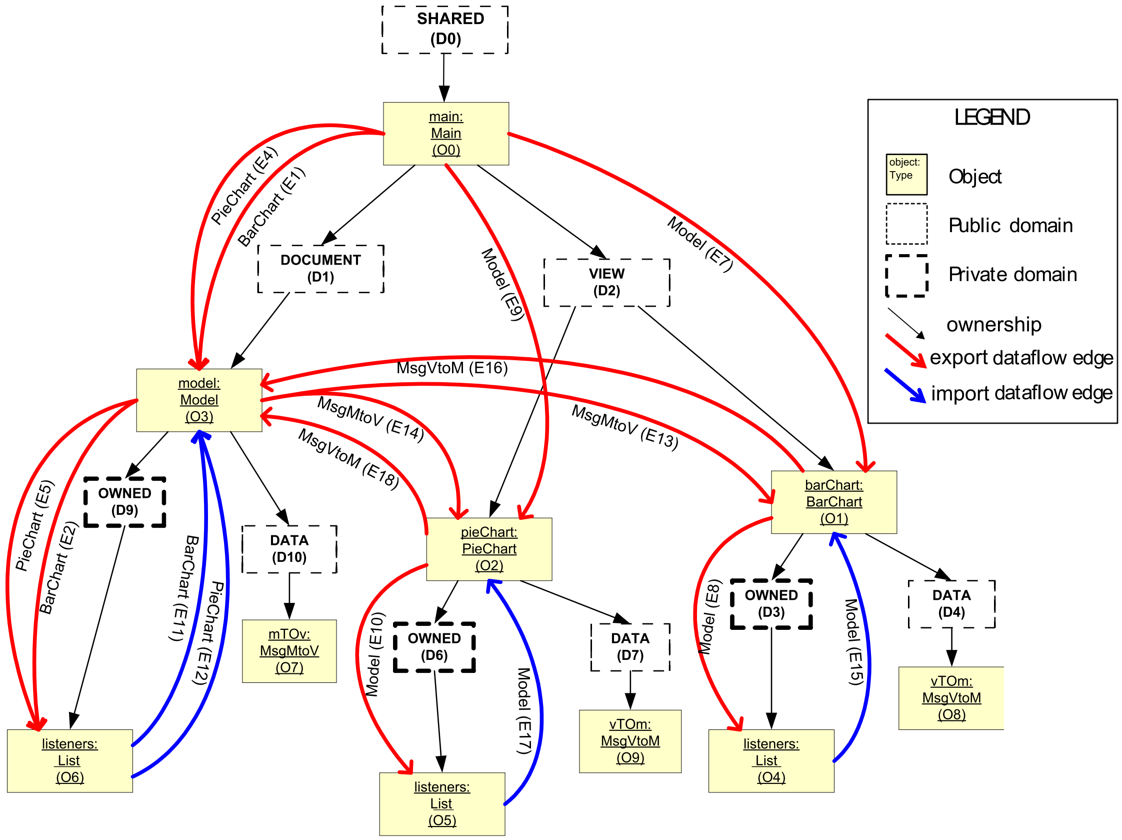



**Figure 24:** OOG extracted for Listeners

our case `main`. On the dataflow edges, we also display the class of the object passed through the dataflow (Fig. 24). Developer can also opt for the hierarchical view (Fig. 25), hide the low level objects, and visualize only the dataflow communication between the high level objects (Fig. 26).

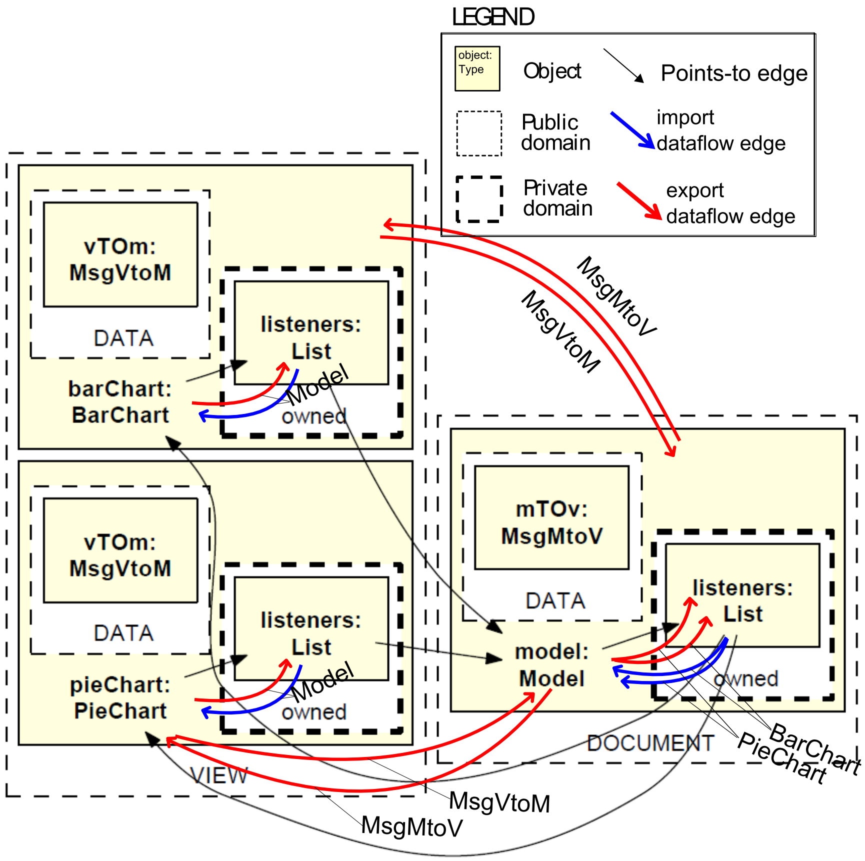



**Figure 25:** Display Graph for Listeners, with both points-to and dataflow edges.

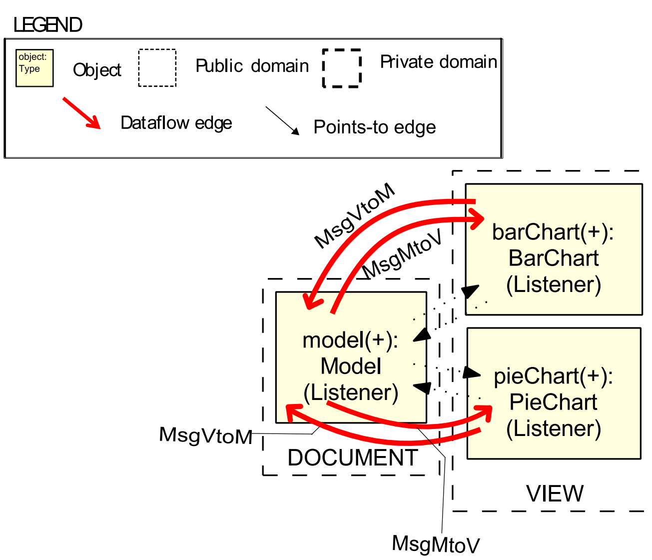



**Figure 26:** Display Graph for Listeners, after collapsing the sub-structures of top-level objects.

# 7 Related Work

Murphy's Reflexion Models (RM) [18] inspired the evaluation style in this paper. In RM, a developer maps source-level entities to components in a high-level model. However, the mechanism of our approach is different since the OOG correspond to a runtime architecture, not a code architecture. Tools that work for code architecture are more mature, but they do not necessarily work for runtime architecture. For example, code architecture does not deal with aliasing. In a class diagram, a class is represented by one box, so an expert cannot reason about communication between difference instances of the same class. Also, in the presence of inheritance, two boxes in a class diagram may correspond to the one instance in an object graph. For example, in CryptoDB one instances of `KeyStore` is part of `keyTool` and stores the encryption keys of the admin. The second instance stores the keys of the users. In case the admin account is compromised, the keys of the users are still safe.

Since our work focuses on extracting usage relationships between objects, we seek how related analyses addressed the challenges we listed in Section 2.

**Dataflow Communication.** Andersen's static analysis extracts dataflow and points-to information from programs written in C [8], and was extended to object-oriented code [15, 23] including Java [21]. These analyses determined the memory locations that may be modified by the execution of a statement. A dataflow edge means that *an object a owns a reference to an object c, and passes it to an object b*, or *an object a owns a reference to an object b, from which it receives a reference to an object c which only b knew before* [21]. However, the results of these analyses are flat graphs [10, 21]. For example, Spiegel builds a type graph which is then unfolded into an object graph. We use the same definition of dataflow edges, but a completely different technology, namely abstract interpretation. Not only is our analysis sound, it is also more precise due to *lookup* which returns instances of a given type in a reachable domain, as opposed to instances of a given type in the whole program. Previous work [25] has shown that hierarchical object graphs can dramatically reduce the number of top-level objects in an OOG, and produce succinct diagrams that convey high-level comprehension of the runtime structure. For architectural risk analysis, half the battle is often extracting a "forest-level view" of the system structure [14, Chap. 5]).

**Sensitivity.** An object graph analysis can be flow, context, or object-sensitive. A flow-sensitive analysis considers the order in which methods are called. A context-sensitive analysis analyzes the methods for different contexts that invoke the method. Object-sensitive analyses for points-to and dataflow edges addressed the aliasing and precision challenges [23, 15]. Such an analysis worked well for on-demand based approaches which refined the references analyzed [22], but might not scale for large number of references. Seeking a tradeoff between soundness and precision, our analysis considers ownership domains as contexts and distinguishes objects of the same type but in different domains. So, our analysis is *domain-sensitive*, and object- and flow-insensitive.

**Dynamic analyses.** Object graphs were extracted by analyzing heap snapshots [16, 17], and execution traces [13]. Lienhard analyzed execution traces and extracted an Object Flow Graph (OFG) in which edges represent objects, and nodes represent code structures: classes, and groups of classes [13]. The OFG analysis addressed the aliasing challenge, and linked objects to field read, field write, and method invocation expressions in the code, the same expressions used by our analysis. Since one class corresponds to one OFG node, an OFG is unable to show the communication between different instances of the same class and is not sound. One advantage of dynamic analysis is that it does not require annotations. However, it can only infer a strict, owner-as-dominator hierarchy, which is limited in representing some design idioms [4]. Ownership Domains also support logical containment (through public domains) and thus are more flexible in expressing arbitrary design intent. In addition, a dynamic analysis requires extensive graph summarization to obtain an abstracted graph [17, 9].

**Annotation-based static analyses.** Lam and Rinard [11] proposed a type system and a static analysis where developer-specified annotations guide the static abstraction of an object model by merging objects based on tokens. Their approach supports a fixed set of statically declared global tokens, and their analysis shows a graph indicating which objects appear in which tokens. Since there is a statically fixed number of tokens, all of which are at the top level, the extracted object model is non-hierarchical, thus with limited scalability. In addition to their object model, Lam and Rinard extract models for “subsystem access”, “call/return interaction”, and “heap interaction”, which are similar to the dataflow information our analysis extracts. From the challenges we listed, they addressed aliasing, and precision supported by tokens. Our approach is different than Lam and Rinard's since it extracts hierarchical object graphs and supports object-oriented language constructs such as inheritance.

# 8 Conclusion

We proposed a static analysis to extract a hierarchical object graph with dataflow communication edges that show usage relations between objects. We formalized the analysis following Ownership Domains and Featherweight Domain Java, and proved its soundness. Ownership Domains improve the precision of our analysis and provide a hierarchical organization of objects. We evaluated our analysis on an extended example and showed that the reverse engineered edges are similar to the edges drawn by an architect who reasons about security and dataflow communication.


# Acknowledgements

The authors thank Suhib Rawshdeh for his contributions to an earlier version of this work.

## References


[1] M. Abi-Antoun. *Static Extraction and Conformance Analysis of Hierarchical Runtime Architectural Structure*. PhD thesis, CMU, 2010.

[2] M. Abi-Antoun and J. Aldrich. Static Extraction and Conformance Analysis of Hierarchical Runtime Architectural Structure using Annotations. In *OOPSLA*, 2009.

[3] M. Abi-Antoun, J. Aldrich, and W. Coelho. A Case Study in Re-engineering to Enforce Architectural Control Flow and Data Sharing. *J. Systems & Software*, 80(2), 2007.

[4] J. Aldrich and C. Chambers. Ownership Domains: Separating Aliasing Policy from Mechanism. In *ECOOP*, 2004.

[5] J. Aldrich, C. Chambers, and D. Notkin. ArchJava: Connecting Software Architecture to Implementation. In *ICSE*, 2002.

[6] N. Ammar. Evaluation of the Usefulness of Diagrams of the Run-Time Structure for Coding Activities. Master's thesis, WSU, 2011.

[7] N. Ammar and M. Abi-Antoun. Evaluation of Global Hierarchical Object Graphs for Coding Activities: a Controlled Experiment, 2012.

[8] L. O. Andersen. *Program Analysis and Specialization for the C Programming Language*. PhD thesis, University of Copenhagen, 1994.

[9] T. Hill, J. Noble, and J. Potter. Scalable Visualizations of Object-Oriented Systems with Ownership Trees. *J. Visual Lang. and Comp.*, 13(3), 2002.

[10] D. Jackson and A. Waingold. Lightweight Extraction of Object Models from Bytecode. *TSE*, 27(2), 2001.

[11] P. Lam and M. Rinard. A Type System and Analysis for the Automatic Extraction and Enforcement of Design Information. In *ECOOP*, 2003.

[12] T. LaToza and B. Myers. Hard-to-answer questions about code. In *PLATEAU*, 2010.

[13] A. Lienhard, S. Ducasse, and T. Grba. Taking an object-centric view on dynamic information with object flow analysis. *COMLAN*, 35, 2009.

[14] G. McGraw. *Software Security: Building Security In*. 2006.

[15] A. Milanova, A. Rountev, and B. G. Ryder. Parameterized Object Sensitivity for Points-To Analysis for Java. *TOSEM*, 14(1), 2005.

[16] N. Mitchell. The Runtime Structure of Object Ownership. In *ECOOP*, 2006.

[17] N. Mitchell, E. Schonberg, and G. Sevitsky. Making Sense of Large Heaps. In *ECOOP*, 2009.

[18] G. Murphy, D. Notkin, and K. Sullivan. Software Reflexion Models: Bridging the Gap between Design and Implementation *TSE*, 27(4), 2001.

[19] PLAID Research Group. The Crystal Static Analysis Framework, 2009. `http://code.google.com/p/crystalsaf`.

[20] S. Rawshdeh and M. Abi-Antoun. A static analysis to extract dataflow edges from object-oriented programs with ownership domain annotations. Technical report, WSU, 2011.

[21] A. Spiegel. *Automatic Distribution of Object-Oriented Programs*. PhD thesis, FU Berlin, 2002.

[22] M. Sridharan, D. Gopan, L. Shan, and R. Bodík. Demand-driven points-to analysis for Java. In *OOPSLA*, 2005.

[23] P. Tonella and A. Potrich. *Reverse Engineering of Object Oriented Code*. Springer-Verlag, 2004.

[24] R. Vanciu and M. Abi-Antoun. Extracting Dataflow Communication from Object-Oriented Code. Technical report, WSU, 2011. `www.cs.wayne.edu/~mabianto/tech_reports/VA11_TR.pdf`.

[25] R. Vanciu and M. Abi-Antoun. Object Graphs with Ownership Domains: an Empirical Study. In *Springer LNCS State-of-the-Art Survey on Aliasing in Object-Oriented Programming*, 2012. to appear.

# APPENDIX

## A Source Code of Listeners Example

```

class Main<OWNER> {

  public domain DOC, VIEW;
  BarChart<VIEW, DOC> barChart = new BarChart();
  PieChart<VIEW, DOC> pieChart = new PieChart();
  Model<DOC, VIEW> model = new Model();

  public void run() {
    model.addListener(barChart);
    model.addListener(pieChart);
    barChart.addListener(model);
    pieChart.addListener(model);

    model.notifyObservers();
    barChart.notifyObservers();
    pieChart.notifyObservers();
  }

  public static void main(String[]<SHARED[SHARED]> args){
    Main<SHARED> main = new Main();
    main.run();
  }
}

class BaseChart<OWNER, M> extends Listener<OWNER> {
  domain OWNED;
  List<OWNED, Listener<M>> listeners = new List();

  public void addListener(Listener<M> l) {
    listeners.value = l;
  }

  public void notifyObservers() {
    MsgVtoM<DATA> vTOm = new MsgVtoM();
    Listener<M> l = listeners.getFirst();
    l.update(vTOm);
  }
}

class BarChart<OWNER, M> extends BaseChart<OWNER, M> {
  public void update(Msg<DATA> msg) {...}
}

class PieChart<OWNER, M> extends BaseChart<OWNER, M> {
  public void update(Msg<DATA> msg) {...}
}
```

$$\frac{p = n.d \qquad \Gamma;\Sigma;\theta \vdash n : C\texttt{<}\overline{p'}\texttt{>} \qquad d \in domains(C\texttt{<}\overline{p'}\texttt{>})}{\Gamma;\Sigma;\theta \vdash qual(p) == C{::}d}\text{[Qual-Var]}$$

$$\frac{\Gamma;\Sigma;\theta \vdash \texttt{this} : C\texttt{<}\overline{p'}\texttt{>} \qquad \alpha \in params(C) \qquad p = \alpha}{\Gamma;\Sigma;\theta \vdash qual(p) = C{::}\alpha}\text{[Qual-Param]}$$

$$\frac{}{\Gamma;\Sigma;\theta \vdash qual(\texttt{SHARED}) = {::}\texttt{SHARED}}\text{[Qual-Shared]}$$

**Figure 27:** Qualify domains rules.

```
//generic type T
class List<OWNER, T<ELTS>> {
  T<ELTS> value; // ELTS is a domain parameter for list elements
  public T<ELTS> getFirst() {  return value;  }
  ...
}

class Model<OWNER, V> extends Listener<OWNER> {
  domain OWNED;
  List<OWNED, Listener<V>> listeners = new List();

  public void addListener(Listener<V> l) {
    listeners.add(l);
  }

  public void notifyObservers() {
    MsgMtoV<DATA> mTOv = new MsgMtoV();
    Listener<V> l = listeners.value;
    l.update(mTOv);
    }
  }

}

abstract class Listener<OWNER> {
  public domain DATA;
  public abstract void update(Msg<DATA> msg);
}
```

# B Auxiliary judgements

Figure 27 shows the definitions we use to qualify a domain $p$ by the class $C$ that declares it. In the context of $\Gamma$, $\Sigma$, and $\theta$, Qual-Var qualifies $n.d$ as $C{::}d$. This judgement also applies to the case when $n$ is `this` and $p = \texttt{this}.d$. Qual-Param qualifies a formal domain parameter $\alpha$ as $C{::}\alpha$, where $C$ is the class of `this`. Since no class declares the `SHARED` domain, Qual-Shared qualifies it as ::`SHARED`. We use these rules implicitly in the static and dynamic semantics to ensure that $(O, C{::}d) \mapsto D$ is in $DD$ and for the lookup operations $D = DD[(O, p)]$.

Figure 28 shows the definitions of many auxiliary judgments used earlier in the semantics. These definitions are the auxiliary judgments from ownership domains [4]. The Aux-Public rule checks whether a domain is public. The next few rules define the *domains*, and *fields* functions

$$CT(C) = \texttt{class}\ C\texttt{<}\overline{\alpha}, \overline{\beta}\texttt{>}\ \texttt{extends}\ C'\texttt{<}\overline{\alpha}\texttt{>}\ \texttt{assumes}\ \overline{\gamma} \rightarrow \overline{\delta}\ \{\ \overline{D};\ \overline{L};\ \overline{F};\ K\ \overline{M};\ \}$$

$$\frac{(\texttt{public domain}\ d) \in \overline{D}}{public(d)}\ \textit{Aux-Public}$$

$$\frac{\overline{D} = \overline{\texttt{public}_{opt}\ \texttt{domain}\ d_C} \qquad domains(C'\texttt{<}\overline{p}\texttt{>}) = \overline{d'}}{domains(C\texttt{<}\overline{p}, \overline{p'}\texttt{>}) = \overline{this.d_C}, \overline{d'}}\ \textit{Aux-Domains}$$

$$\frac{}{domains(\texttt{Object<}\overline{\alpha_0}\texttt{>}) = \emptyset}\ \textit{Aux-Domains-Obj}$$

$$\frac{\texttt{class}\ C\texttt{<}\overline{\alpha}\texttt{>}}{params(C) = \overline{\alpha}}\ \textit{Aux-Params}$$

$$\frac{\overline{F} = \overline{T}\ \overline{f} \qquad fields(C'\texttt{<}\overline{p}\texttt{>}) = \overline{T'}\ \overline{f'}}{fields(C\texttt{<}\overline{p}, \overline{p'}\texttt{>}) = ([\overline{p}/\overline{\alpha}, \overline{p'}/\overline{\beta}]\ \overline{T}\ \overline{f}), \overline{T'}\ \overline{f'}}\ \textit{Aux-Fields}$$

$$\frac{}{fields(\texttt{Object<}\overline{\alpha_0}\texttt{>}) = \emptyset}\ \textit{Aux-Fields-Obj}$$

$$\frac{}{owner(C\texttt{<}\overline{p}\texttt{>}) = p_1}\ \textit{Aux-Owner}$$

$$\frac{(T_R\ m(\overline{T}\ \overline{x})\ \{\ \texttt{return}\ e;\ \}) \in \overline{M}}{mtype(m, C\texttt{<}\overline{p}\texttt{>}) = [\overline{p}/\overline{\alpha}]\ \overline{T} \rightarrow T_R}\ \textit{Aux-MType1}$$

$$\frac{m\ is\ not\ defined\ in\ \overline{M}}{mtype(m, C\texttt{<}\overline{p}, \overline{p'}\texttt{>}) = mtype(m, C'\texttt{<}\overline{p}\texttt{>})}\ \textit{Aux-MType2}$$

$$\frac{(T_R\ m(\overline{T}\ \overline{x})\ \{\ \texttt{return}\ e;\ \}) \in \overline{M}}{mbody(m, C\texttt{<}\overline{p}\texttt{>}) = [\overline{p}/\overline{\alpha}]\ (\overline{x},\ e)}\ \textit{Aux-MBody1}$$

$$\frac{m\ is\ not\ defined\ in\ \overline{M}}{mbody(m, C\texttt{<}\overline{p}, \overline{p'}\texttt{>}) = mbody(m, C'\texttt{<}\overline{p}\texttt{>})}\ \textit{Aux-MBody2}$$

$$\frac{(mtype(m, C\texttt{<}\overline{p}\texttt{>}) = \overline{T'} \rightarrow T') \implies (\overline{T} = \overline{T'} \wedge T = T')}{override(m, C\texttt{<}\overline{p}\texttt{>}, \overline{T} \rightarrow T)}\ \textit{Aux-Override}$$

**Figure 28:** Auxiliary Judgments. Source: [4].

by looking up the declarations in the class and adding them to the declarations in the base classes. The *owner* function just returns the first domain parameter (which represents the owning domain in our formal system).

The *mtype* function looks up the type of a method in the class; if the method is not present, it looks in the superclass instead. The *mbody* function looks up the body of a method in a similar way. Finally, the *override* function verifies that if a superclass defines method $m$, it has the same type as the definition of $m$ in a subclass.

# C Transfer Functions

We formalize the analysis using transfer functions, to show how to implement these rules in a dataflow analysis framework such as Crystal [19].

Transfer functions generate the OGraph by abstractly interpreting the program (Fig. 30). Each function takes as input some program text, an input lattice, and produce an output lattice. In our case, the lattice is the OGraph, together with some context information.

| | |
|---|---|
| Context | $\Gamma = \emptyset$ |
| | $\Upsilon = \emptyset$ |
| *init* | $D_{\texttt{SHARED}} = \langle D_s, ::\texttt{SHARED} \rangle \quad O_{world} = \langle C_{dummy}< . > \rangle$ |
| | $G = \langle \{O_{world}\}, \{(O_{world}, ::\texttt{SHARED}) \mapsto D_{\texttt{SHARED}}\}, \emptyset \rangle$ |
| | $[\![\texttt{new } C_{root}<\texttt{SHARED}>()]\!] \ O_{world} \ G$ |
| $[\![\texttt{new } C<\overline{p}>(\overline{e})]\!] \ O \ G$ | $G' : \langle DO', DD', DE' \rangle$ |
| | $CT(C) = \texttt{class } C<\overline{\alpha}, \overline{\beta}> \texttt{ extends } C'<\overline{\alpha}> \{ \ \overline{T} \ \overline{f}; \ \overline{dom}; \ \ldots; \}$ |
| | $D_i = DD[(O, p_i)], i \in 1..n, n = \lvert\overline{p}\rvert$ |
| | $O_C = \langle \ C<\overline{D}> \rangle$ |
| | $DO' = DO \cup \{O_C\}$ |
| | $DD' = DD \cup \{(O_C, \alpha_i) \mapsto D_i, (O_C, p_i) \mapsto D_i)\}$ |
| | $(\texttt{domain } d_j) \in domains(C<\overline{p}>) \qquad [\![\texttt{domain } d_j]\!] \ C \ O_C \ G'$ |
| | $DE' = DE$ |
| | *if* $C<\overline{D}> \notin \Upsilon$ *then* |
| | $\quad \Upsilon' = \Upsilon \cup \{C<\overline{D}>\}$ |
| | $\quad \forall m \in \overline{md} \ mbody(m, C<\overline{p}>) = (\overline{x}, e_R)$ |
| | $\qquad \Gamma' = \Gamma \cup \{\overline{x} : \overline{T}, \ \texttt{this} : C<\overline{p}>\}$ |
| | $\qquad [\![e_R]\!] \ O_C \ G'$ |
| | $\forall e_k \in \overline{e} \ [\![e_k]\!] \ O \ G'$ |
| $[\![\texttt{domain } d_j]\!] \ C \ O_C \ G$ | $G' : \langle DO', DD', DE' \rangle$ |
| | *if* $DD'[(O_C, C::d_j)] == \emptyset$ *and* $d_j \in \overline{dom}$ *then* |
| | $\quad D_j = \langle D_{id_j}, C::d_j \ \rangle$ |
| | $\quad DD' = DD \cup \{(O_C, d_j) \mapsto D_j\}$ |
| | *else if* $d_j \in \overline{dom}$ *then* |
| | $\quad D_j = DD'[(O_C, C::d_j)]$ |
| | $\quad DD' = DD \cup \{(O_C, d_j) \mapsto D_j\}$ |
| | *else* |
| | $[\![\texttt{domain } d_j]\!] \ C' \ O_C \ G'$ |

**Figure 29:** Transfer functions $[\![.]\!]$ for the construction of the OGraph. They transform $G : \langle DO, DD, DE \rangle$ to $G' : \langle DO', DD', DE' \rangle$. Initialization and `new` expressions.

| | |
|---|---|
| $[\![e_0.f_k]\!]\ O\ G$ | $G' : \langle DO', DD', DE' \rangle$<br>$DO = DO'$<br>$DD = DD'$<br>$e_0 : C<\overline{p}>$<br>$(C_k<\overline{p'}>\ f_k) = fields(C<\overline{p}>)[k]$<br>$\{O_i \in DO \mid O_i = C_i<\overline{D}>, i = 1..sz\} = lookup(O, C<\overline{p}>)$<br>$\{O_j \in DO \mid O_j = C_j<\overline{D'}>, j = 1..sz'\} = lookup(O_i, C_k<\overline{p'}>)$<br>$DE' = DE \cup \bigsqcup_{i=1..sz,j=1..sz'} \{\langle O_i, O, C_j, imp \rangle\}$<br>$[\![e_0]\!]\ O\ G'$ |
| $[\![e_0.f_k := e_1]\!]\ O\ G$ | $G' : \langle DO', DD', DE' \rangle$<br>$DO = DO'$<br>$DD = DD'$<br>$e_0 : C<\overline{p}>$<br>$(C_k<\overline{p'}>\ f_k) = fields(C<\overline{p}>)[k]$<br>$e_1 : C_1<\overline{p''}>\ C_1<\overline{p''}> <: C_k<\overline{p'}>$<br>$\{O_i \in DO \mid O_i = C_i<\overline{D}>, i = 1..sz\} = lookup(O, C<\overline{p}>)$<br>$\{O_j \in DO \mid O_j = C_j<\overline{D'}>, j = 1..sz'\} = lookup(O, C_1<\overline{p''}>)$<br>$DE' = DE \cup \bigsqcup_{i=1..sz,j=1..sz'} \{\langle O, O_i, C_j, exp \rangle\}$<br>$[\![e_0]\!]\ O\ G'$<br>$[\![e_1]\!]\ O\ G'$ |
| $[\![e.m(\overline{e})]\!]\ O\ G$ | $G' : \langle DO', DD', DE' \rangle$<br>$DO = DO'$<br>$DD = DD'$<br>$e_0 : C<\overline{p}>$<br>$mtype(m, C<\overline{p}>) = \overline{T} \rightarrow T_R$<br>$\{O_i \in DO \mid O_i = C_i<\overline{D}>, i = 1..sz\} = lookup(O, C<\overline{p}>)$<br>$\{O_j \in DO \mid O_j = \langle C_j<\overline{D'}> \rangle, j = 1..sz'\} = lookup(O_i, T_R)$<br>$DE' = DE \cup \bigsqcup_{i=1..sz,j=1..sz'} \{\langle O_i, O, C_j, imp \rangle\}$<br>$\forall e_k \in \overline{e}\ e_k : T'_k\ T'_k <: T_k$<br>$\quad \{O_{j'} \in DO \mid O_{j'} = \langle C_{j'}<\overline{D''}> \rangle, j' = 1..sz''\} = lookup(O, T'_k)$<br>$\quad DE' = DE' \cup \bigsqcup_{i=1..sz,j'=1..sz''} \{\langle O, O_i, C_{j'}, exp \rangle\}$<br>$[\![e_0]\!]\ O\ G'$<br>$\forall e_k \in \overline{e}\ [\![e_k]\!]\ O\ G'$ |
| | $lookup(O, C'<\overline{p'}>) = \{O_k \in DO \mid O_k = \langle C<\overline{D}> \rangle, C <: C',\ \forall i \in 1..\lvert\overline{p'}\rvert\ D_i = DD[(O, p'_i)]\}$ |

**Figure 30:** Transfer functions $[\![.]\!]$ for the construction of the OGraph. They transform $G : \langle DO, DD, DE \rangle$ to $G' : \langle DO', DD', DE' \rangle$. Field read, field write and method invocation expressions.