7-10-2012

Trust, but verify: Optimistic Effect Analysis for Reusable Code

Yuheng Long
Iowa State University, csgzlong@iastate.edu

Hridesh Rajan
Iowa State University

Follow this and additional works at: http://lib.dr.iastate.edu/cs_techreports

Part of the Programming Languages and Compilers Commons, and the Software Engineering Commons

Recommended Citation
http://lib.dr.iastate.edu/cs_techreports/212

This Article is brought to you for free and open access by the Computer Science at Iowa State University Digital Repository. It has been accepted for inclusion in Computer Science Technical Reports by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.
Abstract: This is the Technical Report version of the 2013 POPL submission by the same title. It includes the POPL version verbatim, followed by an appendix containing omitted contents and proofs.

Keywords: type-and-effect, open effects, optimistic concurrency

CR Categories:
D.1.3 [Concurrent Programming] Parallel programming
D.1.5 [Programming Techniques] Object-Oriented Programming
D.2.2 [Design Tools and Techniques] Modules and interfaces, Object-oriented design methods
D.2.3 [Coding Tools and Techniques] Object-Oriented Programming
D.2.4 [Software/Program Verification] Validation
D.2.10 [Software Engineering] Design
D.3.1 [ Formal Definitions and Theory] Semantics, Syntax
D.3.1 [Language Classifications] Concurrent, distributed, and parallel languages, Object-oriented languages
D.3.3 [Programming Languages] Concurrent programming structures, Language Constructs and Features - Control structures
D.3.4 [Processors] Compilers

Copyright (c) 2012, Yuheng Long, and Hridesh Rajan.

Department of Computer Science
226 Atanasoff Hall
Iowa State University
Ames, Iowa 50011-1041, USA
# Contents

1 Introduction 1
   1.1 The Problems and Their Importance 1
   1.2 Contributions to the State-of-the-Art: Open Effects 2

2 Optimistic Effect Analysis for Reusable Code 3
   2.1 Using Open Effects in Sorting Algorithms 3
   2.2 Using Open Effects in Search Algorithms 4
   2.3 Using Open Effects with Map-Reduce Framework 4

3 A Concurrent Object-oriented Calculus 5

4 Type and Static Effect Computation 5
   4.1 Notations and Conventions 5
   4.2 Type-and-Effect Rules for Method Declaration 5
   4.3 Open Effects of Polymorphic Method calls 6
   4.4 Type-and-effects for Field Related Expressions 6

5 Dynamic Semantics with Open Effects 6
   5.1 Notations and Conventions 6
   5.2 Dynamic Effect Management in OO Expressions 7
   5.3 Safe Optimistic Concurrency using Open Effect 8
   5.4 Key Properties of OpenEffectJ 8
   5.5 Open References 9

6 Adding Open Effects to OpenJDK 9
   6.1 Effect Storage and Maintenance 10
   6.2 Performance Evaluation 10

7 Comparative Analysis with Related Work 10
   7.1 Overview of Closely Related Ideas 10
   7.2 Criteria and Analysis Results 11
   7.3 Scope and Applicability of Open Effects 11

8 Conclusion and Future Work 11

References 12

A Type-and-effect System: Omitted Details 13
   A.1 Type-and-Effect Rules for Declarations 13
   A.2 Type-and-Effect Rules for Expressions 13

B Dynamic Semantics: Omitted Details 13

C Proof of Key Properties 14
   C.1 Preliminary Definitions 14
   C.2 Effect Preservation 15
   C.3 Deterministic Semantics 17
   C.4 Type Soundness 18
Abstract
We present an optimistic effect system for enabling safe concurrency in modern object-oriented languages with an open world assumption. New to our effect system is the notion of open effects. An open effect is a placeholder effect. It is produced by method calls when the dynamic type of the receiver object is unknown. An open effect is assumed to be blank (i.e., noninterfering effect) statically but verified to be truly so when the dynamic type of the receiver is known. An open effect-based analysis has several benefits. It is modular and so it allows analysis of partial programs and libraries. It is more precise than a comparable static analysis. It also has a small annotation overhead, and does not require specification on super type methods to restrict overriding in subclasses. We have formalized our analysis and proven that it is sound and that it enables deterministic semantics. We have also extended the OpenJDK Java compiler with support for open effects and tested its effectiveness on several reusable library classes where it shows only about 0.13-7.65% overhead and good speedup.

Categories and Subject Descriptors D.3.1 [Programming Languages]: Formal Definitions and Theory—Semantics

General Terms Languages, Theory, Verification

Keywords type-and-effect, open effects, optimistic concurrency

1. Introduction
Both static [2, 5, 6, 8, 11, 17, 32, 34, 42] and dynamic [7, 16, 18, 39] analyses have been proposed to help programmers write correct concurrent software. In essence, these techniques compute sets of computational effects [20, 29, 41] of concurrent tasks to determine whether these tasks interfere with each other and thus could lead to unexpected program behavior.

1.1 The Problems and Their Importance
For soundness, such static analysis for an object-oriented (OO) language must conservatively handle features such as dynamic dispatch [17], pp. 222]. Consider a method call, if the exact runtime type of the call’s receiver is not known statically, then a static analysis has two options. First option is to compute the sets of effects, e.g., {reads field f}, produced by all overriding implementations of that method and take the set of potential effects of that call to be the union of these sets. The second option is to require specifying a method’s implementation in the supertype and use that specification to compute an upper bound on the potential effects produced by all overriding implementations of that method.

To illustrate consider the class ArrayList in Figure 1 inspired from its namesake in the Java Development Kit (JDK). This class provides an operation applyall that iterates over each element in the list and calls method run with argument c of type Command as the receiver object. Two separate applications, PROGRAM and PROGRAM’ (among others) use this ArrayList class. Each application provides separate and distinct implementation of the command interface. PROGRAM computes a prefix sum, which, as implemented, is not a commutative operation [35]. PROGRAM’ computes a 32-bit hash of array elements, which is an independent operation for each element in the array list.

Now consider a concurrent implementation of the method applyall in ArrayList. If the effect of each iteration of run on line 8 does not interfere with any other iteration, then this method may be safely parallelized. Unfortunately, computing the set of effects produced by all implementations of method run may not be feasible. In fact, many such overriding implementations, such as those in PROGRAM and PROGRAM’ may not even be available during compilation of the library class ArrayList.

The second option is to ask programmers to annotate the method run such that the effect annotations provide an upper bound on the potential effects produced by all overriding implementations of run. Computing such upper bound is difficult primarily due to the variety of, and often unanticipated, usage of library classes such as ArrayList. Even if we are able to anticipate all such usage and compute an upper bound, such a bound may be overly conservative. For example, based on the code of the method run in PROGRAM, one may conclude that parallelization of the applyall method would be unsafe. Whereas, in reality there may be several subclasses of Command, such as class Hash in PROGRAM’, for which applyall method can be safely parallelized.

Dynamic analyses can help; however, they provide incomplete, post-deployment detection of concurrency-related defects, whereas we seek preventative detection and defect avoidance [25], pp. 6:2]. For example, we would like to avoid unsafe parallelization of applyall in PROGRAM instead of detecting an unsafe trace. Also, majority of current proposals for sound, software-based dynamic analysis cause a major slowdown in programs (see Table 1), e.g., STM-based solutions are reported to have 2X overhead [40]. Goldilocks that requires a custom virtual machine (VM) is reported to have 2X overhead [16] and even higher for production VM [18]. Most of this overhead is due to conflict detection and state buffering (for roll back) mechanisms.

To summarize, OO languages e.g., Java, C#, allow separate compilation and testing of libraries and frameworks that is not supported by static, whole program analyses; asking a developer to annotate methods with effects such that these annotations give an upper bound on effects of all overriding methods could be challenging; and purely dynamic analysis could be expensive [18].
1.2 Contributions to the State-of-the-Art: Open Effects

A promising idea is for the programmer to optimistically assert that method calls, with certain special references as receivers, will produce concurrency-safe effects, and the compiler to trust the programmer statically and generate parallel code, but also emit code to verify programmer’s assertion at runtime. We present a new optimistic effect analysis that takes this idea and blends static effect analysis with dynamic effect verification, producing an analysis that has many of the advantages of both static and dynamic analyses, but suffers from none of the limitations described above.

Our effect system has two kinds of effects: open and concrete effects. An open effect is produced by a method call, whose receiver’s dynamic type is unknown, but its static type is qualified with an annotation @open. An open effect is assumed to be blank (i.e., noninterfering) statically, but it is filled in at runtime. Concrete effects include reads and writes to memory regions [41].

Like static analyses, we compute effects at compile-time. However, unlike static approaches that make conservative approximations when the exact dynamic type is unavailable, we use placeholder open effects. Like dynamic approaches, a parallelization technique based on our analysis may treat each parallelization operation as noninterfering prior to forking off parallel tasks.

To illustrate, imagine that the programmer optimistically marked the argument c’s type in the class ArrayList as open as on line 4 in Figure 2. The static part of our analysis would then trust the programmer by taking the effect of a method call on this reference as an open effect, i.e. an effect that could be extended at runtime but is blank statically. So the effect of method call c.run(..) on line 5 would be taken as an open effect, because the dynamic type of c is unknown. Thus, the effect of an iteration of the for loop on line 6 would be reading the ith element of the array elements and an open effect. An open effect is treated as a blank effect statically, so an iteration of this for loop would be treated (trustingly) as parallel since it is independent of other iterations.

The dynamic part of our analysis fills in, or concretizes, open effects when references marked with @open annotations, such as c, are assigned. Then, if the concretized (previously open) effects of the method call c.run(..) do not interfere, the for loop on line 7 could be run in parallel, else it must be run sequentially.

Figure 2. ArrayList with an Open Parameter. Thus, method applyall has open effects. Applications remain the same.

On a different day, the developer of PROGRAM imports the class ArrayList. At runtime, PROGRAM creates an instance al of ArrayList, and passes an instance p of class Prefix on line 11 in Figure 3 as argument c. This assignment to the argument c concretizes the effect of an iteration of the for loop, because the effect of this for loop contains an open effect (method call effect on an unknown reference c). Note that the receiver object c is now an alias of the instance p of class Prefix. So, the extended effect (the original effect union with the concrete effect of the method run of the class Prefix) of the loop iteration is now reading and writing to the field sum of instance Prefix and writing to different slot of an array. As a result, iterations of the for loop now has a loop carried dependence (on the field sum, line 15 in Figure 1). Thus, the for loop on line 16 is run sequentially when method applyall is called on line 17 in PROGRAM in Figure 3.

On yet another day, developer of PROGRAM imports the ArrayList class. PROGRAM also instantiates ArrayList, but passes an instance of class Hash in Figure 1 as argument c,
which concretizes the effects of method call c.run(. . .) on line 6. These concrete effects are writing to different slot of an array. The effect of an iteration of the for loop is similarly enlarged. As a result, iterations of the loop are still independent. Thus, the same for loop on line 5 is run in parallel in PROGRAM’.

Thus, our optimistic effect analysis can help expose safe concurrency in this case whereas purely static analysis, analyzing only this library and its dependencies, would conservatively label the for loop on line 5 as a sequential loop. Alternatively, such static analysis could also ask users for effect annotations that will specify an upper bound on effects for all subclasses of the Command class [6][34]. A benefit of such analysis would be that it will not incur any dynamic overhead, whereas a drawback is that writing effect annotations by hand, when only partial code is available, can be difficult. Our analysis also has following benefits.

• It is modular and so it allows analysis of libraries and frameworks, which is important for software reuse and maintenance. Here “modular” means that the analysis can be done using only the code in question and the interface of the static types used in the code. For example, static analysis of ArrayList relies only on code for ArrayList and the interface of the Command classes, but not necessarily on its implementation. This would be essential for analyzing ArrayList without requiring PROGRAM or PROGRAM’ to also be present. This benefit of OpenEffectJ is critical for libraries, which are analyzed and compiled once, but reused often. Previous work show that most concurrency is exposed via libraries [6][23].

• It does not require annotating methods in a supertype to specify upper bounds on the effect of all subclasses, e.g. the run method in type Command (Figure 2 line 10).

• Parallelization based on our effect analysis will never require rollback, rather an operation is attempted in parallel if and only if the open effect assertions hold.

• For our use cases, it had a small annotation overhead, e.g. one annotation was needed in the ArrayList.

• User annotations cannot break soundness, in the worst case they can create extra overhead (and only when effects are unknown statically).

• It is more precise than a comparable static analysis, but would have some runtime overhead. Our evaluation shows that these overheads are negligible. For example, OpenEffectJ was able to distinguish between effects of the method call run in PROGRAM (with Prefix class) and PROGRAM’ (with Hash class) designed by two different programmers at two different times. This allows the for loop in the ArrayList class to be optimistically parallelized. Main benefits of this parallelization are reaped by PROGRAM’, where the implementation of run method is safe to parallelize. However, PROGRAM also does not suffer significantly because OpenEffectJ preemptively detects conflicts and does not require rollbacks.

These benefits make an open effects-based analysis an interesting point in the design space between a fully static and a fully dynamic effect analysis. Since the annotation @open is explicit, programmers can control the optimism in the analysis and thus the overhead of its dynamic part.

In summary, main contributions of this work are:

• a language design with open effects that facilitates important patterns of optimistic and deterministic parallelism in object-oriented programs in Section 3 and examples in Section 2

• a static semantics with open effects in Section 4. The novelty lies in the integration of the open effects with standard effects;

• a dynamic semantics with open effect concretization and open effect-based concurrency decisions in Section 5

• a prototype compiler based on the OpenJDK Compiler in Section 6 that shows only about 0.13-7.65% overhead;

• a rigorous proof that OpenEffectJ ensures determinism – thus, users are guaranteed to avoid many complex concurrency issues in Section 5.4. The soundness proof is challenging compared to the static analyses, because the effect of a task could change at runtime, due to the open effects; and

• a comparative analysis with related ideas in Section 7

2. Optimistic Effect Analysis for Reusable Code

We anticipate that OpenEffectJ is useful for exposing safe and optimistic concurrency in libraries and frameworks, which could be extended with possibly concurrency-unsafe code by clients, e.g. the ArrayList class in Section 1. Here, we present further assessment on several representative algorithms.

2.1 Using Open Effects in Sorting Algorithms

We now study an implementation of merge sort. The code below is adapted from the package java.util. It uses a divide-and-conquer technique on line 16 and line 17 and combines it with an insertion sort as a base case for small arrays on lines 6-14.

To allow clients of this library to extend sorting by implementing application-specific comparisons, this library is designed to use an abstract class Comparator.

```java
public class Arrays {
  final Object[] mergeSort(@open Comparator c,
                           Object[] src, int low, int high) {
    int size = high - low;
    Object[] dest = new Object[size];
    if (size < THRESHOLD) { // Use insertion sort
      System.arraycopy(src, low, dest, 0, size);
      for (int i=0; i<size; i++) {
        for (int j=i; j>0 && c.compare(src[j-1], src[j])>0; j--)
          this.swap(dest, j-1, j);
      }
      return dest;
    }
    int mid = (low + high) / 2;
    Object[] d1 = this.mergeSort(c, src, low, mid);
    Object[] d2 = this.mergeSort(c, src, mid, high);
    /* The details of merge omitted. */
    return;
  }
}
```

The method mergeSort in the library uses an instance of the class Comparator on line 10 to compare two objects in the array.

It is almost a universal belief that the comparators are pure methods and thus this parallelization can be done safely. However, programmers may or may not subscribe to this belief. For example, in OpenJDK itself, the class RuleBasedCollator (RBC) in package java.text is a Comparator, but the method compare has side effects. So the parallelization of merge sort may have heap conflicts if an instance of this class is used as a Comparator and would result in incorrect output. We can annotate the class Comparator to require that method compare be pure; however, such annotation could make it unnecessarily difficult to implement certain comparators, e.g. RBC.

However, most comparators are side effect free. Thus, it would be nice to parallelize merge sort for these cases. We can do so in...
2.2 Using Open Effects in Search Algorithms

Next, we study a representative search algorithm, depth-first search (DFS). DFS is typically formulated as a graph traversal as in the listing below [23]. For extensibility and reuse, this library is designed to use abstract implementation of classes Node and Goal. A client of this library would extend the class Node on line 17 to create an application-specific node and extend the class Goal on line 19 to implement application-specific search objectives.

```
1  class DFS {
2     final boolean dfs(@open Goal goal, Node curr) {  
3         if (mark.contains(curr)) return false;
4         else mark.add(curr);
5         boolean found = false;
6         if (goal.satisfied(curr)) {  
7             rs.add(curr);
8             found = true;
9             for(int i=0; i<curr.children.length; i++)
10             found |= this.dfs(goal, curr.children[i]);
11             return found;
12         }
13         HashSet mark = new HashSet();
14         HashSet rs = new HashSet();
15         class Node { Node[] children; }
16         class Goal {
17             boolean satisfied(Node node) { return false; }
18         }
19     }
```

When the input range is small, the base case applies, on lines [10][17] where the map method is applied on each element of the array on line [13]. The results from the Mapper are combined, on line [14] by the Reducer. The algorithm divides the array into non overlapping subarrays and recursively applies compute on these subarrays, on lines [19][20].

This algorithm could be parallelized by executing the compute on the subarrays concurrently, lines [19][20]. Since we may not know about the effect of each subclass of the Mapper and Reducer, we declare them as open fields, lines [21][22] to ensure concurrency safety. The method calls on these fields result in two open effects. The method compute can be safely parallelized when mapper and reducer point to instances of concurrency safe subclasses of Mapper and Reducer, respectively.

**Summary** We applied OpenEffectJ to 4 representative examples, 3 of which are library classes from OpenDK. For each case OpenEffectJ gracefully assists the programmer in parallelization of reusable libraries and/or frameworks. Here the libraries or frameworks could be extended by the clients. Thus, OpenEffectJ opti-mistically provides safe concurrency opportunities. In each case, at most two annotations were needed to safely parallelize the library class under consideration. Finally, in each case OpenEffectJ did not require the entire client code for effect analysis.
3. A Concurrent Object-oriented Calculus

This section introduces OpenEffectJ, an expression language based on Classic Java [19]. The grammar is shown in Figure 4. The grammar include two interim expressions for semantics: loc that represents locations and yield that models concurrency.

prog ::= decl e
decl ::= class c extends d { field; meth }
field ::= [open] f t
meth ::= t m ( arg ) ( e )
t ::= c | void
arg ::= var | null | arg = e ; e ; e
| new c() | e | m( t )
| e | f | e | f
| fork ( e ; e )
loc | yield e
where

Figure 4. The Grammar for OpenEffectJ.

The notation over-bar denotes a finite ordered sequence (π stands for a1...an). The notation [a] means that a is optional. The examples in Section 2 used an extended language with integers and boolean constants and operations, e.g., int is used as a shorthand for Integer, i < j is for i.lt(j), etc. As in Fork/Join framework [26], we desugar for loop to the code below.

fork ( loop (l,h-l/2); loop (h-l/2,h) )

OpenEffectJ provides one construct for expressing parallelism: the fork expression. This expression has the form fork(ε0|ε1). It runs ε0 and ε1 in two concurrent tasks. Concurrent execution of these tasks is dependent upon whether they may conflict. If these tasks do not conflict they are run concurrently, else sequentially. A novelty in OpenEffectJ’s semantics is that this parallelization decision is based upon the information available at the time of the evaluation of a fork expression. Delaying parallelization decision allows the use of useful dynamic information. This is similar to Best et al.’s synchronization via scheduling [5], but differs from static [34] and dynamic analysis [13] (more in Section 7).

A programmer writing parallel code in reusable classes, e.g. the class ArrayList in Figure 2 typically knows that a reference such as c in that class may point to concrete objects of different types at runtime, and if a method is called on such a reference, it may result in different effects. Some of these effects may be concurrency safe while the others may not, which will affect the parallelization decision. In such cases, they can mark the type of these references as open, using the annotation @open (e.g. line 2 in Figure 2).

To focus our attention on the essence of open effects and to make the presentation tractable, we have formalized a subset of OpenEffectJ. In the core language, only fields can be annotated @open, but not other references, e.g., variables and parameters. In Section 5.5 we will discuss how we could extend the formalism to model other @open references. So all the examples presented work out nicely as they are.

4. Type and Static Effect Computation

OpenEffectJ’s type-and-effect system has both a static and a dynamic part. The purpose of the static part is to compute the effects of every method. The statically computed effects include standard read/write effects and bottom effect.

Main novelty of this effect system is the notion of open effects. An open effect is produced as a result of evaluating method call expressions with open fields as receiver object. The format is @open f m p. It contains the name of the open field f, the method m being invoked, and a placeholder for concrete effects p.

The placeholder for concrete effects in an open effect is used by the dynamic part of our type-and-effect system. At runtime, the dynamic part concretizes the open effects by filling in this placeholder with actual effects. These concretization points happen whenever f is set. OpenEffectJ uses these concretized effects to make concurrency decisions, when evaluating the fork expressions.

4.1 Notations and Conventions

As Figure 5 shows, we represent type attributes for expressions as (t,ρ), the type t of an expression and its effects ρ.

θ ::= OK | (t1 × ... × tn → t1) ∈ c “program/decl/body types”
| (t1 → t2) ∈ c “method types”
| (t1,ρ1) ∈ c “expression types”
ρ ::= {εj}j∈N “program effects”
| read f “read effect”
| write f “write effect”
| open m p “open effect”
| ⊥ “bottom effect”
Π ::= {varj → tij}j∈N “type environments”

Figure 5. Type and effect attributes.

The notation t′<:t means t′ is a subtype of t. It is the standard reflexive-transitive closure of the declared subclass relationship [19]. We will use the notation ρ0 ⊑ ρ1 to mean that effects ρ0 and ρ1 do not interfere and ρ0 ⊑ ρ1 to mean that they do interfere.

We state the type checking rules using a fixed class table (list of declarations CT [19]). The typing rules for expressions use a type environment Π, which is a finite partial mapping from variable names var to a type t. Each method in the class table (CT) contains its effect ρ, computed by OpenEffectJ’s static type-and-effect system, in its signature.

The rules for top-level declarations are fairly standard. The typings and effects rules for OO expressions that do not produce effects are also standard. These include object creation, variable reference and declaration, null reference and sequence (Section 4.1 contains the rules for programs, classes and the standard OO rules).

4.2 Type-and-Effect Rules for Method Declaration

The (METHOD) rule says that a method m type checks in class c, in which m is declared, if the body has type u and latent effect ρ.

(T-METHOD) override(m,c,(t1 × ... × tn → t1))
∀i ∈ {1,...,n}, isClass(ti) isType(t1)
| var1 : t1,...,varn : tn, this : : e : e′(u,ρ)
| u <: t
| t m t1 var1,...,tn varn ( e ) (t1 × ... × tn → t ) in c

2 We simplify the presentation by avoiding tracking object instances in read/write effects. In the implementation, OpenEffectJ tracks object instances and uses a sound intra-procedural aliasing analysis [21] and a purity analysis [30] to improve the precision of the static effect analysis.

//Sugar: for(int i=1; i<h; i++) be
final void loop (int i, int h) {
if(h == 1) be
else fork ( loop (1,h-1/2); loop (h-1/2,h) )
}
4.3 Open Effects of Polymorphic Method calls

The rules for method call are one of the central new rules. The typings and effects for the field access rules (T-GET) and (T-SET) are standard. The auxiliary function typeOFF uses the class table CT to find the type of a field f, the class in which f is declared and the open annotation information, for the input field f.

\[
\text{(T-GET)} \\
\Pi \vdash e : (c, \rho) \quad \text{typeOFF}(f) = (d, \open f \rho) \\
\Pi \vdash e : (t, \rho \cup \{\text{read f}\}) \\
\text{(T-SET)} \\
\Pi \vdash e : (c, \rho) \quad \text{typeOFF}(f) = (c', t') \quad \Pi \vdash e : (t', \rho') \quad t' < t \\
\Pi \vdash e : (t', \rho' \cup \{\text{write f}\}) \\
\]

Using only field to denote read/write effect here is somewhat conservative. However, it helps create an efficient dynamic effect management system, which is crucial.

The (T-SET-OPEN) rule denotes a concretization point, which may change the static precomputed effects of other methods. OpenEffectJ gives it a bottom effect to maintain soundness. In practice, this can be relaxed using an aliasing analysis to determine the set of concrete objects that an open field can point to.

\[
\text{(T-YIELD)} \\
\Pi \vdash e : (t, \rho) \\
\Pi \vdash \text{yield} : (t, \rho) \quad \Pi \vdash \text{fork} : (e', \emptyset, \rho \cup \{\text{void}\}) \\
\]

Concurrency expressions: The (T-YIELD) rule says that a yield expression has the same type and effect as the expression e. The (T-FORK) first type checks its two subexpressions. It has the type void. Its effect is the union of the effects of the subexpressions.

5. Dynamic Semantics with Open Effects

Here we give a small-step operational semantics for OpenEffectJ. To the best of our knowledge, this is the first work to integrate dynamic effect management with an object-oriented semantics, to enable safe, optimistic concurrency.

5.1 Notations and Conventions

The small steps taken in the semantics are defined as transitions from one configuration (Σ in Figure 6) to another. Some rules use an implicit attribute, the class table CT.
domain value. The task queue consists of an expression and the corresponding task dependencies that it waits on. We present the semantics as a set of evaluation contexts which is new. If a field is declared open, assigning a value to it may change the effect of those methods that access it. The function update shown below implements this.

\[
update(\mu, loc, f, v, f') = \mu \quad \text{where} \quad \mu(loc) = \lfloor c.F.E \rfloor
\]

\[
E' = updateEff(\mu, f, v, E) \quad \text{and} \quad E' \neq E
\]

\[
E' = updateEff(\mu, f, v, E) \quad \text{and} \quad reverse(\mu, loc) = \kappa
\]

\[
\mu' = \{ loc \rightarrow \lfloor c.F.E' \rfloor \} \oplus \mu \quad \text{and} \quad fixPoint(\mu', loc, \kappa) = \mu''
\]

The inputs to update are the current store \(\mu\), the object reference \(loc\), the field \(f\), and the R-value \(v\). The output is a modified store. This function first updates the effect (by calling updateEff) of the object pointed to by \(loc\) (by the effect of an object \(o\), we mean the effects of all the methods of \(o\)). If the effects of \(o\) remain unchanged, the algorithm stops. Otherwise, the effect of an object \(o'\), which has some open field pointing to \(o\), should also be changed. Effects are further updated using the function fixPoint until a fixed point is reached.

reverse(\mu, loc) = \bigcup_{i=1}^{n} S_{i} \quad \text{where} \quad \forall i \in \{1..n\} s.t. loc_{i} \in dom(\mu) ::

\[
S_{i} = \{(loc_{i}, f) \mid F(f) = loc \land \mu(loc) = \lfloor c.F.E \rfloor \}
\]

The function reverse, searches the input store \(\mu\) for objects \(loc_{i}\) and field \(f_{i}\) pair that is pointing to the current object \(loc\). In practice, reverse pointers could be used to optimize this update.

updateEff(\mu, f, v, \lfloor m_{i} \rfloor) = \lfloor m_{i} \rfloor'

where \(\forall i \in \{1..n\} \rho_{i} = \{ e_{i} | 1 \leq k \leq p \} \) and \(\rho'_{i} = \{ e'_{i} | 1 \leq k \leq p \} \)

and \(\forall f \in \{1..p\} :: e_{f} \in \rho_{i} : \text{concretize}(\mu, f, v, e_{f}) = e'_{f} \)

Each object contains a map \(E\) of effects. The updateEff function concretizes the effects in \(E\) one by one, by calling concretize.

concretize(\(\mu, f, v, e\)) = match \(e\) with

| @open \(f'\) \(m\) \(\rho\) -> match \(f'\) with

| \(null\) -> @open \(f\) \(m\) \(\emptyset\)

\(\text{and} \quad \rho' = \bigcup_{i=1}^{n} \rho_{i} \quad \text{and} \quad E' = \{ e_{i} | 1 \leq i \leq n \} \)

\(\text{and} \quad \forall i \in \{1..n\} :: \text{cp}(\epsilon_{i}) = \rho_{i} \)

\(\_ \to \epsilon\)

The function concretize changes the concrete effects in the placeholder inside an open effect. Note that when the open field \(f\) is set in the (T-SET) rule, only the open effects that have \(f\) as receiver are concretized, i.e., @open \(f\) \(m\) \(\rho\).

\(\text{cp}(\epsilon) = \text{match} \(\epsilon\) with\)

| @open \(f\) \(m\) \(\rho\) -> \(\rho\)

\(\_ \to \epsilon\)

The function \(\text{cp}\) is used by the function concretize to retrieve the concrete effects, i.e., the effects of the R-value \(v\) are copied to fill the placeholder effects of the open effect of \(loc\) in the (SET) rule.
The (Call) rule is standard. It acquires the method signature via the function findMeth (Section 5.1) that uses dynamic dispatch [19].

\[
\text{(Call)} \quad (c',i,m(\text{var}_1,\ldots,\text{var}_n)(e),\rho) = \text{findMeth}(c,m) \quad [c,\text{E}] \quad e' = \text{loc/this}.\text{var}_1,\ldots,\text{var}_n.e
\]

\[
\langle\langle [E,\text{loc.m}([\text{var}_1,\ldots,\text{var}_n]),\tau] + \psi,\mu \rangle \mapsto [\langle\langle \text{yield e'},\tau \rangle + \psi,\mu \rangle]
\]

To summarize, in OpenEffectJ’s semantics, object creation is augmented to initialize the effect map; and field assignment to open fields updates these effect maps.

5.3 Safe Optimistic Concurrency using Open Effect

We now describe how open effects are used by a fork expression. Recall from Section 4 that OpenEffectJ’s static effect system would advise a parallelizing compiler to parallelize fork(e0; e1) if and only if statically computed effects of e0 and e1 do not interfere.

Interference checks for open effects were deferred to allow optimistic parallelism. This deferred check is included in the dynamic semantics of the fork expression, which checks if the two subexpressions e0 and e1 could run in parallel. To do so, we use the effect judgements in Figure 7 that recursively computes the effects of subexpressions. An effect judgement of the form \( \mu \vdash e : \rho \) means that an expression e has static effect \( \rho \) with respect to a store \( \mu \). In practice, expressions e0 and e1 can be tightly nested within single compiler-generated methods m0 and m1; OpenEffectJ can then retrieve the effects of e0 and e1 from the effect map E of the this object, thus eliminating the need for this dynamic effect computation.

![Figure 7](image_url)

The dynamic rules in Figure 7 are similar to the static rules in Section 5 except for method calls on open fields (E-CALL-OPEN). The open effect now has a concrete part \( \rho \), instead of \( \emptyset \), because we know the concrete object that an open field is pointing to.

After computing the effects, the rules for fork verify that the effects of e0 and e1 do not interfere (written \( \mu_0 = \emptyset,e_1 \)). Read effects do not interfere; read/write and write/write pairs conflict if they access the same field; open effect \( \text{open} f \) conflicts with another effect e if any effect e' in \( \rho \) conflicts with e; bottom effect \( \bot \) conflicts with any effect.

If e0 and e1’s effects do conflict, the (fork-sequential) rule applies; otherwise the (fork-parallel) rule will be used. OpenEffectJ makes its concurrency decision at this point, which allows the usage of more accurate effect information than a pure static analysis. A pure dynamic analysis will optimistically execute the tasks in concurrent.

5.4 Key Properties of OpenEffectJ

The key formal properties of OpenEffectJ are: effect preservation, type preservation, and determinism. The proof of type preservation uses the standard subject reduction argument [19]. It is contained in our report [23], which also contains detailed proof for effect preservation and determinism.

5.4.1 Effect Preservation

The effect preservation property is that the dynamic effect, i.e. heap accesses, of each concurrent task refines the static effect of that task computed when it is forked off. First, we define dynamic effects.

A dynamic effect \( \eta \) of a task id is a read effect \( \text{rd}, \text{loc}, f, i \) or a write effect \( \text{wt}, \text{loc}, f, i \). A dynamic effect \( \eta \) refines a static effect \( \rho \), written \( \eta \prec \rho \), if either \( \eta = \langle \text{rd}, \text{loc}, f, i \rangle \wedge \langle \text{read} f \rangle \in \rho \) or \( \eta = \langle \text{wt}, \text{loc}, f, i \rangle \wedge \langle \text{write} f \rangle \in \rho \).
The dynamic effect of a task $id$ is a dynamic trace $\chi = \eta$, a sequence of dynamic effects.

Informally, effect preservation will hold if the dynamic effects of a task $id$ and dynamic effects of all the child tasks spawned by $id$ together refine the static effects of $id$. Since our dynamic semantics does not maintain the parent-child relationship between tasks nor maintain dynamic effects, we introduce an instrumented semantics $dyn$, which augments dynamic semantics in Section 3 with dynamic effects and an additional parent-child relationship $\gamma$, which is a map $\{id_j \mapsto I\}_{j \in \mathbb{N}}$. Here, $id$ is a task's identity and $I$ is a set of its children tasks' identities.

The function $dyn$ (below), records the dynamic memory footprint for each task [13][44], which helps us understand the relation between the static effects and their corresponding dynamic effects. It is trivial to see that this instrumented semantics retains formal properties of the original dynamic semantics.

![Image of the instrumented semantics](image)

The novelty of OpenEffectJ is that it stores the effects $\rho$ in object records for methods. These methods will be used by the fork expression at runtime. Therefore, two invariants (Definition 5.3), for these method effects $\rho$, are necessary to maintain the effect preservation property. These invariants include: the placeholder effect $\rho_0$ of an open effect $\odot open f m \rho_0$ should be superreflexive $\supseteq$ of the effect $E(m)$ for the method $m$ of the object $f$ is pointing to (Definition 5.4), i.e., $E(m) \subseteq \rho_0$, and the effect $E(m)$ of a method $m$ stored in the object record should be superreflexive of the effect $\rho$ of the body $e$ of $m$ (Definition 5.5). For example, in Figure 3 after the open parameter $\rho$ is bound to the instance $\rho$, on line 17, the open effect, of the for loop of the ArrayList instance $a$, is superreflexive of the effect of the method run of $p$.

**Definition 5.1.** [Well-formed object] An object record $o = \{E.F.E\}$ is a well-formed object in $\mu$, written $\mu \vdash o$, if for all open effect $\odot open f m \rho_0 \in \rho \in \text{ring}(E)$, either $(F(f) = \text{loc}) \land \mu(\text{loc}) = (\{E.F.E\}) \land (E(m) \subseteq \rho_0)$; or $(F(f) = \text{null}) \land (\rho_0 = \emptyset)$.

**Definition 5.2.** [Well-formed location] A location loc is well-formed in $\mu$, written $\mu \vdash loc$, if either $(l = \text{loc}) \land (\forall m \in (\sigma) \exists \text{findMethod}(c,m) = (E,F,E)) \land (\forall (e, \rho) \in \mu \vdash \text{this}(e); \rho$, then $\rho \subseteq \mu(m))$; or $(\exists \mu(\text{loc}) = \text{null})$.

**Definition 5.3.** [Well-formed store] A store $\mu$ is well-formed, written $\mu \vdash \circ$, if $\forall o \in \text{ring}(\mu)$, $\mu \vdash \circ$ and $\text{loc}(\mu) \vdash \text{loc}$. 

**Theorem 5.4.** [Effect preservation] Let the program configuration be $\Sigma = \{e_i, (id_i, I_i)\} \vdash \psi, \mu$. If it transits to another configuration $\Sigma' = \{e_i', (id_i')\} \vdash \psi', \mu'$, the store is well-formed $\mu \vdash \circ$, $\mu' \vdash \circ$, and $(\land) \not\in \rho$, then there is some $p', \chi \vdash (\mu(a) \vdash e' : \rho', \rho' \subseteq \rho; \text{and} (b) (\mu(\Sigma, \chi, Y) = (\Sigma, \chi, Y)) \Rightarrow (\eta \equiv \rho))$

**Proof Sketch:** The essence of Theorem 5.4 is that during program execution, the subsequent expression $e'$ has a subeffect $p' \subseteq \rho$ of the previous expression $e$, with the effect judgment $\mu \vdash e : \rho$ (Figure 4). We prove that the dynamic effect $\eta$ in each step refines the static $\rho$ of the original expression $e$, $\eta \equiv \rho$. Thus with $(a)$, $\eta$ refines the effect $\rho_0$ of the expression $e_0$ when the task was forked off, with the heap $\mu_0$, e.g., $\text{fork}(e_0; e_1)$ and $\mu_0 \vdash e_0 : \rho_0$. Unlike the static approaches, which compute at compile-time, OpenEffectJ computes $\rho_0$ before evaluating the fork expression.

### 5.4.2 Determinism

We prove the determinism of OpenEffectJ programs by showing that the concurrent tasks do not have dynamic effect interference and therefore a well-typed OpenEffectJ program produces the same result given the same input.

To prove that the tasks do not have heap interference, we introduce the accumulated dynamic effects function $dynE$. These effects, produced by a concurrent task $id$ and all its descendants $id' (id' \leq id)$, refine the static effect computed when $id$ is forked off. The function $dynE$ is $\text{dynE}(\Sigma, \chi, Y, n) = \text{dynE}(\Sigma', \chi', Y', n-1)$, if $\Sigma, \chi, Y = (\Sigma', \chi', Y')$ and $\text{dynE}(\Sigma, \chi, Y) = (\Sigma', \chi', Y')$.

A task $id'$ is a descendant of a task $id$, with $Y$, written as $id' \leq Y$, if $id' \in \text{desc}(id, Y)$. Here, $\text{desc}(id, Y) = I \cup \bigcup_{i=0}^{\infty} I_i$, $Y(id) = \{i_0, \ldots, i_{n-1}\}$, and $\forall i \in I, \text{desc}(id, Y) = I_i$.

To reason about the interaction between the two concurrent tasks, we define the newly generated queue $\psi$, which is formed by these two tasks, i.e., we write $\Sigma \rightarrow \psi$, if $\Sigma \rightarrow \psi'$. Let $\Sigma = \{\text{fork}(e', \psi), \psi, \mu\}$, and $\Sigma' = \{e_0, \psi', \psi, \mu\}$. To say that concurrent tasks do not interfere (heap accesses), we define the noninterference relation for dynamic effects $(\eta \equiv \rho)$ as follows: reads effects do not conflict with each other; read-write and write-write pairs do not conflict if the location or the field is different. A set of dynamic effects $\psi = \{\eta_1, \eta_2\}$ do not conflict with another set $\psi' = \{\eta_1', \eta_2'\}$ if $\forall i \in \{1, \ldots, n\}, j \in \{1, \ldots, p\}$ s.t. $\eta_i \equiv \eta_j'$.

**Theorem 5.5.** [Deterministic semantic] Let $\mu \vdash \circ$, $\Sigma \rightarrow \psi, \mu$. For the two tasks $e_1(id, id_1), i_1 \in \psi$ and $e_2(id_2, id_2) \in \psi$, $e_1 : r_1, \mu \vdash e_2 : r_2, \eta_1 \eta_2, \mu \vdash r_1, \mu \vdash r_2$. Then $\forall n \in \mathbb{N}$ s.t. $\text{dynE}(\Sigma, \psi, \mu, n) = (\Sigma, \psi, \mu)$,

$\text{dynESet}(id_1, \chi, Y) \oplus \text{dynESet}(id_2, \chi, Y)$. Here $\eta \equiv \chi$ and $\eta = (\{id_1, id_2\} \rightarrow \text{desc}(id, Y)) = \text{dynESet}(id, \chi, Y)$.

**Proof Sketch:** The essence of the theorem is that for the 2 concurrent tasks $id_1$ and $id_2$ generated by a fork expression, if the store is well-formed $\mu \vdash \circ$, the effect judgments give them effect $\eta_1$ and $\eta_2$ respectively and they do not interfere $\eta_1 \eta_2$, then their dynamic effects $\text{dynESet}(id_1, \psi)$ returns the dynamic traces by the task $id_1$, do not interfere $\text{dynESet}(id_2, \chi, Y)$. The map $Y$ records the children set (Section 5.1) of a task $id$. We need $Y$ because the effect of a child task of $id$ should count as id's effect.

Proving the above soundness theorems are non-trivial compared to static effect approaches [13][44], in which the exact effect of a task is known statically. A technical challenge for proving the soundness of OpenEffectJ is that the effects of the concurrent tasks may change due to the open effect, i.e., the effect concretization.

### 5.5 Open References

As discussed in Section 3 other open references can be allowed. Here, we discuss how we can extend OpenEffectJ to enable open variable and parameter. At compiler-time, OpenEffectJ's type-and-effect system will generate an open effect $\odot open var m \emptyset$ for a method call $\text{var.m}(\ldots)$. At runtime, the concretization of the open effect happens in the fork rule. At runtime, if var is bound to a location loc, the (E-CALL-LOC) rule in Figure 4 takes effect. It transits from the placeholder effect $\odot open var m \emptyset$ to the concrete effect $\rho_0$ (the second item in (E-CALL-LOC)). With this concretized effect, the fork rules become more optimistic and all the examples follow directly from this extension.

### 6. Adding Open Effects to OpenJDK

We have extended the OpenJDK Java compiler to add support for open effects. An overview of the compiler is presented in Figure 8. Apart from modifications to support the $@open$ annotation and the fork expression, parsing remains unchanged. Type checking
(the Attribute and Flow phases in the OpenJDK compiler) are modified to implement new constraints specified in Section 4. This phase is also extended with an effect analysis, which implements the effect system discussed in Section 4 augmented with modular analyses to further improve precision. These include an intra-procedural definite alias analysis [21], purity analysis [36], and modular inter-procedural analysis that detect temporary objects. This phase attributes each AST node with static effects for each method, which is used by tree rewriting phase to generate code for runtime effect manipulation.

6.1 Effect Storage and Maintenance

Application classes are instrumented to contain dynamic effects. Concrete effects are stored as a static member array, to avoid duplication, and open effects are stored as an instance field array.

We noted in Section 5 that if the effects of an object o changes, the effects of an object, o′ which has some open field pointing to o, should also be changed. In the semantics, we implemented this change using the function update. In the implementation, we maintain a reverse pointer from o to o′ for efficiency reasons. This reverse pointer is maintained as a weak reference, which does not prevent o′ from being garbage-collected. It is only needed for classes that have open fields. If a class has no open fields, the effect of all of its method will be concrete effects and will not change.

When an open field f is assigned a value, concrete effects of the methods in the object that contains f may change. In our example in Section 2.3, when the mapper of an instance of class MapReduce changed, concrete effect of method compute will change also.

We generate a method cascade to implement this functionality. The method first checks whether the effect is actually enlarged by this open field assignment, i.e., whether it has reached a fixpoint. If so, the algorithm stops propagating the changes (Section 5). Otherwise, it calls the cascade method of all its reverse pointers.

6.2 Performance Evaluation

We have conducted an initial evaluation of OpenEffectJ's prototype compiler using the library classes described in Section 1 and Section 2. These are array list with hash computation (Hash), array list with slightly heavier computation (Heavy), merge sort algorithm (MergeSort), depth-first search algorithm (Search), and a map-reduce application (MapReduce). All experiments were run on a system with a total of 4 cores (Intel Core2 chips 2.40GHz) running Fedora GNU/Linux. For each of the experiments, an average of the results over ten runs was taken.

The Heavy variant of array list computes the following formula \( Math.sqrt(2 * Math.pow((double)o, 2)) \) for each element o in the list. For both Hash and Heavy variant, array list contained 20 Million elements. The merge sort algorithm sorts a list of 10 Million randomly generated integers. The search algorithm searches for solutions to an n-queens problem, where n is 11. In the map-reduce algorithm, map step computes the formula \( Math.sqrt(2 * Math.pow((double)o, 2)) \) for the element o and reduce step is simply addition. It is applied to 100 Million integers.

The performance results of running these applications are shown in Figure 9. In this table, the columns marked Sequential show the time taken by the single-threaded version of the application. The columns marked Manual show the time taken by (and speedup of) the manually parallelized version, which does not manage effects (and thus could be unsafe). The columns marked OpenEffectJ shows the time taken by (and speedup of) a version of our compiler, which does effect comparison prior to forking off each task. The columns marked OpenEffectJ shows the time taken by (and speedup of) an improved version of our compiler, which does an intra-procedural analysis to determine that effects will not change between one fork and next (and thus first effect check implies the second).

The manual (unsafe) version showed decent to good speedup for all of these applications. The OpenEffectJ and OpenEffectJ version also showed comparable speedup. For the array list, results for both OpenEffectJ and OpenEffectJ are the same. The overhead for this example was also small. For the MergeSort, Search and MapReduce examples, however, the overhead for OpenEffectJ increased significantly. This was because each of these problems use recursive, parallel algorithm. This was precisely where OpenEffectJ shines, because this version compiler is able to eliminate the effect check for the nested fork expressions. Thus, this version outperformed our previous version on all of the recursive cases.

These results show that support for open effects can be provided in an industrial strength compiler such as the OpenJDK compiler at a reasonable cost (single digit overheads). To put these overheads in perspective, a dynamic analysis can sometimes incur 2X overhead [15, Table 1]. More attention to OpenEffectJ’s compiler prototype will help discover simple and more clever optimizations that will help decrease overheads even further.

7. Comparative Analysis with Related Work

We now compare OpenEffectJ with closely related ideas.

7.1 Overview of Closely Related Ideas

Like OpenEffectJ, Synchronization via Scheduling (SVS) [5] conflicts computes between potentially concurrent tasks right before forking them off. SVS supports a C like language. It compares reachable objects graph (OG) of tasks to determine if they may conflict [33]. Compared to SVS, OpenEffectJ supports a full OO language with support for overriding and dynamic dispatch, which makes conflict detection much more challenging [17]. Furthermore, using effects sets instead of reachable OG may be more precise for OO features, e.g., in every example in Section 1 and Section 2 the OG for all the tasks are the same (all of them access the same receiver object of the method call on the open references) and thus overlap with each other; therefore, SVS will recommend sequential execution for all of them, whereas OpenEffectJ allows parallelism.

In type, regions and effect-based approaches [6][8][11][23] programmers specify the footprint (region) of concurrent tasks. By reasoning that two regions are disjoint, programmers conclude that the tasks do not depend on each other. These approaches are pure static, whereas OpenEffectJ uses a hybrid approach. This allows greater optimism in exposing safe parallelization opportunities compared to static approaches that also operate within the same constraints. OpenEffectJ’s analysis is modular and does not require effect annotations in supertypes. Here by modular, we mean that to analyze a piece of code, the analysis requires only the code in question and the interface of static types used in the code.

DPJ framework [6] uses effect parameters [29] and effect constraint to reason about the correctness of the client code. Effect constraint is used to restrict the effect of the user-supplied subclass.
There are two main differences. First, OpenEffectJ requires no annotations on super classes to restrict overriding subclasses, whereas DPJ does. Second, if a subclass does not refine its superclass specifications DPJ signals compilation error, whereas if a subclass has interfering effects, OpenEffectJ runs relevant tasks serially.

There is a large body of work on dynamic analysis for concurrency [2, 16, 18, 19]. In essence, they monitor memory footprints of tasks and signal when conflicts are detected. In contrast, OpenEffectJ detects conflicts just before forking off parallel tasks.

Transactional memory [22, 27, 37, 40] optimistically executes tasks concurrently, but monitors memory accesses. It rolls back side effects when conflicts happen. There are TM-like approaches [4, 15, 43] that provide sequential consistency (DTM) by enforcing a deterministic commit order, instead of rolling back nondeterministically conflicting. In OpenEffectJ, state buffering is required, because conflicts are detected before parallel code.

In concurrent revisions [9, 10] programmers know that tasks conflict on shared objects and annotate these objects. Each task has a local copy of the objects to avoid data races. In OpenEffectJ, however, when a concurrent library class c is developed, the presence/absence of conflicts may be unknown, because c could be extended with concurrency-unsafe code by clients. OpenEffectJ exposes safe, optimistic concurrency for the library.

Gradual Typing [38] and Hybrid Type Checking [25] blend the advantages of static and dynamic type checking, whereas OpenEffectJ blends the advantages of static and dynamic effect analysis. 7.2 Criteria and Analysis Results

The comparison criteria and the results are summarized below:

<table>
<thead>
<tr>
<th>Work</th>
<th>SM</th>
<th>OO</th>
<th>DS</th>
<th>IC</th>
<th>FT</th>
<th>OPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenEffectJ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Hybrid</td>
<td>Fork Point</td>
</tr>
<tr>
<td>DPJ [5, 34]</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Static</td>
<td>Static</td>
</tr>
<tr>
<td>Galois [10]</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Dynamic</td>
<td>Complete</td>
</tr>
<tr>
<td>Ownership [11, 13]</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Fork Point</td>
</tr>
<tr>
<td>Actor [3]</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Static</td>
<td>Static</td>
</tr>
<tr>
<td>TM [22, 27, 37, 40]</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Dynamic</td>
<td>Complete</td>
</tr>
<tr>
<td>FastTrack [18], CP [35]</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Dynamic</td>
<td>Complete</td>
</tr>
<tr>
<td>Goldilocks [16]</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Hybrid</td>
<td>Complete</td>
</tr>
<tr>
<td>Revision [9, 10]</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>

In shared memory (SM) systems, tasks communicate via accessing the shared memory space, while in the distributed memory systems, tasks communicate via messages. X10 is classified as shared memory because places can share heap objects. As the main stream languages (C++, Java and C#) adopt the shared memory and object-oriented (OO) models, it may require more intellectual efforts to use distributed models [31] and/or the non-OO models.

In a programming model with deterministic semantics (DS), a given input will produce the same result. Programmers generally find it easier to reason about deterministic programs. The actor model, due to its asynchronous nature, does not provide deterministic semantics, since the order of the arrival of the messages is arbitrary [31]. Galois targets applications that do not require determinism. Normally, TM has no determinism guarantee due to its nondeterministic commit order, except for deterministic TMs.

By inheritance constraint (IC) we mean that the subclass c must obey certain rule due to the specification on its superclasses, e.g., c has subeffect of its superclasses [6]. It facilitates reasoning, but requires extra efforts developing superclass, especially when subclasses may not be anticipated easily.

The last two columns, deployment time (DT) and optimism level (OPT) show when the systems are activated and how optimistic they are in concurrency. A static approach does reasoning at compile time, has least runtime information and is least optimistic. A hybrid analysis, like OpenEffectJ, uses static information to facilitate the runtime analysis and is more optimistic than a static one. A dynamic approach reasons about correctness completely at runtime and is the most optimistic. The actor model does not do any static/dynamic analysis, and is put in the static category. Goldilocks is hybrid because it could apply static analysis to reduce runtime overhead, which requires whole program analysis.

7.3 Scope and Applicability of Open Effects

Here, we compare OpenEffectJ with static and dynamic approaches for their scope and applicability.

The best scenario for static analyses is when using compile-time knowledge, we could soundly conclude that the tasks either always or never conflict, e.g., if a task c is a consumer of a producer task p, then c should not be executed until p is done; or if two tasks are pure computations. In such cases, a static analysis wins hands down with no runtime overhead. However, if a static analysis makes use of many conservative approximations, because accurate type information is not available, an optimistic approach such as OpenEffectJ or TM should be a more desirable model.

The best scenario for dynamic approaches is when the parallel section has alternate paths, e.g., p1 and p2, some of which p1 have data races, but these are not the hot paths in program. The others p2 have no side effect and are frequently executed. TM will win, because 1) p1 will indeed be executed, and so all the sound models which make decisions before the parallel section must indicate that it is not safe; and 2) p2, is more frequently used.

There are at least two scenarios when OpenEffectJ outperforms the other two. First is when barriers for memory access can be removed when adequate runtime information is acquired before the parallel section, but not enough at compile time. In the second scenario, there are three tasks a, b and c. Task a and b do not conflict, but both conflict with c. The static approach may sequentialize all of them. OpenEffectJ will indicate that c should be run after a and b are done and a and b can be run concurrently. TM will most likely run all of them concurrently and c will be rolled back [3].

8. Conclusion and Future Work

Two reasons severely hinder the safe parallelization of object-oriented libraries: overriding and dynamic dispatch. The developer of a library class, when writing that class, has little knowledge about the behavior and side effects of its clients’ code. The side effects of clients’ code can affect the correctness of the parallelization of the library code. We have developed a new effect system in OpenEffectJ that solves this problem. This effect system employs an optimistic strategy that blends modular static effect analysis with...
dynamic effect verification. It has many benefits. It is modular and so it allows analysis of libraries and frameworks. It does not require annotations on methods in a supertype to specify upper bounds on the effect of all subtypes. It is more precise compared to a static analysis with same properties, but would have some runtime overhead. It is less precise compared to a pure dynamic analysis, but would detect conflicts before they occur. Thus, state buffering for rollbacks is not necessary and overhead is less. In future, it would be sensible to explore a logical extreme, where every reference is implicitly open and a static analysis is used to systematically eliminate open references. Combining effect specifications and open effects would also be interesting.

Acknowledgements

This work was supported in part by the NSF under grants CCF-08-46059, and CCF-11-17937.

References

A. Type-and-effect System: Omitted Details

This section presents type-and-effect rules that were omitted in the main text for brevity.

A.1 Type-and-Effect Rules for Declarations

The rules for top-level declarations are fairly standard. Below, the (T-PROGRAM) rule says that the entire program type checks if all the declarations type check and the expression e has any type t and any effect ρ.

(T-PROGRAM)
\[ \forall decl \in decl \vdash \text{decl} : \text{OK} \quad \vdash e : (t, \rho) \]

The (T-CLASS) rule says that a class declaration type checks if all the following constraints are satisfied. First, all the newly declared fields are not fields of its super class (this is checked by the auxiliary function validF). Next, its super class d is defined in the Class Table (this is checked by the auxiliary function isClass). Finally, all the declared methods type check.

(T-CLASS)
\[ \forall fields \in \text{field} \vdash \text{validF}(fields, d) \]
\[ \text{isClass}(d) \quad \forall \text{meth1} \in \text{meth} \vdash \text{meth1} : (t_1, \rho_1) \text{ in } c \]
\[ \vdash \text{class } c \text{ extends } d \{ \text{field meth} \} : \text{OK} \]

The function validF and isClass check if a field is valid and a class is declared, respectively, which are standard.

\[ \text{validF}(f, \text{Object}) \quad \text{class c extends d \{field meth\} in CT} \]
\[ \text{isClass}(c) \]
\[ \text{isType}(t) \]

A.2 Type-And-Effect Rules for Expressions

The rules for OO expressions are standard, except for the effects in type attributes.

(T-NEW)
\[ \text{isClass}(c) \]
\[ \Pi \vdash \text{var} = t \]
\[ \Pi \vdash \text{null} : (t, \emptyset) \]

(T-VAR)
\[ \Pi \vdash \text{new } c() : (c, \emptyset) \]
\[ \Pi \vdash \text{var} = t \]
\[ \Pi \vdash \text{null} : (t, \emptyset) \]

(T-NULL)
\[ \Pi \vdash \text{isType}(t) \]

(T-DEFINE)
\[ \text{isClass}(c) \]
\[ \Pi \vdash e_1 : (t_1, \rho_1) \]
\[ \Pi \vdash e_2 : (t_2, \rho_2') \]
\[ \Pi \vdash \text{var} + e_1 : e_2 : (t_2, \rho_2' \cup \rho_1) \]
\[ \Pi \vdash e_1 : (t_1, \rho_1) \]
\[ \Pi \vdash e_2 : (t_2, \rho_2') \]

The (T-NEW) rule ensures that the class c being instantiated was declared. This expression has empty effects. The (T-VAR) rule checks that var is in the environment. The (T-NULL) rule says that the null expression could be of any valid type. The declaration expression (T-DEFINE) rule ensures that the initial expression should be a subtype of the type of the new variable. Also, the subsequent expression e2 types check if the type of the variable is placed in the environment. The (T-SEQUENCE) rule states that the sequence expression has same type as the last expression and its effects are the union of the two expressions. The sequence expression type checks if both left and right expressions type check.

B. Dynamic Semantics: Omitted Details

This section presents auxiliary functions that were omitted in Section 5 for brevity. The fields function, used in the (NEW) rule, returns all the fields declared in the class and its super classes (it uses the fieldOf function defined in Section A.2).

\[ \text{fields}(c) = F_s \cup \{ f_1 \ldots f_n \} \]
\[ \text{where } CT(c) = \text{class c extends d \{field meth\} and fields(d) = F_s and } \forall i \in \{1, n\} : \text{fieldOf}(field_i) = (f_i, t_i) \]

The function fixPoint, used in the (SET) rule is shown below. It calls the update function in Section 5.2 until the store µ, or more specifically the effects in the store, does not change. The update is called on all the loci fields pairs that are pointing to the loc, whose effects have been changed. The effects of loci are changed by calling the update function.

\[ \text{fixPoint}(\mu, \text{loc}, \kappa) = \mu_0 \]
\[ \text{where } \kappa = \{ \langle \text{loc}_i, f_i \rangle \mid 1 \leq i \leq n \} \]
\[ \text{and } \text{update}(\mu, \text{loc}_1, f_1, \text{loc}) = \mu_1 \]
\[ \text{and } \forall i \in \{2, n\} : \text{update}(\mu, \text{loc}_{i-1}, f_i, \text{loc}) = \mu_i \]

The function active (below) returns the top most task in ψ that can be run. A task is ready to run if all the tasks in its children set are done (evaluated to a single value v).

\[ \text{active}(e, \tau) + \psi = (e, \tau) + \psi \quad \text{if intersect}(\tau, \psi) = \text{false} \]
\[ \text{active}(e, \tau) + \psi = \text{active}(\psi + (e, \tau)) \quad \text{if intersect}(\tau, \psi) = \text{true} \]

The function intersect, used by the active function, checks whether there is still any task in the dependent (children) set of the current set, i.e., to check either the dependent set is empty or all the tasks in the dependent set are done and thus deleted from the queue ψ.

\[ \text{intersect}((d, \emptyset), \psi) = \text{false} \]
\[ \text{intersect}((d, \{id_1, \ldots, id_n\}), \psi) = \psi \]
\[ \text{where } \forall i \in \{1, n\} : \text{inQueue}(id_i, \psi) = b_i \]

The function inQueue, used by the intersect function, searches whether there is a task id matching the input value n.

\[ \text{inQueue}(n, \bullet) = \text{false} \]
\[ \text{inQueue}(n, \{e, \{n, \{id_1 \mid j \in N\}\} + \psi = \text{true} \]
\[ \text{inQueue}(n, \{e, \{n', \{id_j \mid j \in N\}\} + \psi = \text{inQueue}(n, \psi) \quad \text{if } n \neq n' \]

This function gets the tasks from the task queue ψ and matches the input n with the id of the tasks. If one task matches, the function returns true. Otherwise it continues searching the rest of the tasks in the queue until one of them matches or none of the tasks matches.
C. Proof of Key Properties

We now prove the key properties of OpenEffectJ: Effect and Type Preservation, and Determinism. Some of the definitions, descriptions and proof sketches are also in Section 5.4. We write all these for the sake of clarity.

We have proven the soundness of OpenEffectJ’s type system (Section C.4) contains proof that use the standard subject reduction argument [19]. The Effect preservation property is that the dynamic effect (heap accesses) of each concurrent task id refines the static effect computed when id is forked off. We prove this in Section C.2. We prove the determinism of OpenEffectJ programs by showing that the concurrent tasks do not have dynamic effect interference and therefore a well-typed OpenEffectJ program produces the same result given the same input in Section C.3. Proving effect soundness is non-trivial compared to static effect approaches [13][34], in which the exact effect of a task is known statically. A technical challenge for proving the soundness of OpenEffectJ is that the effects of the concurrent tasks may change due to the open effect, i.e., the effect concretization.

C.1 Preliminary Definitions

We now give some preliminary definitions used in the proofs for OpenEffectJ’s properties. A standard approach to show determinism, for multi-tasking systems, is to prove that the heap accesses of the tasks do not interfere [34]. To record the heap accessed for each task, we define dynamic trace d, which contains a sequence of dynamic effects (heap accesses) by the tasks. Later we will show that the dynamic effects of each task id refines the static effect ρ computed when id is forked off, s.t. if the static effects do not interfere, the dynamic effects will not interfere [13][34] (Section C.2).

Definition C.1. Dynamic Trace A dynamic trace d consists of a sequence of dynamic effects d (η), where η can be a read effect rd, loc, f, id) or write effect wt, loc, f, id).

Next, we will introduce a relationship Y. It records the children tasks of a task id. The relationship Y will be used to prove that the dynamic traces produced by a child task refine the static effect of its parent task id.

Definition C.2. Relationship A relationship Y for tasks is a map {id → Y} id∈T. Here id is a task’s identity and Y is a set of its children tasks’ identities.

The function dyn, defined in Figure 10, records the dynamic memory footprint for each task. With it, we can prove that the dynamic effects of each task id refines the static effect ρ computed when it is forked off.

Figure 10. Dynamic Effect function dyn.

Here, we define what it means by dynamic effects refine the static effects, s.t. the non-interference of the static effects implies the non-interference of the dynamic effects.

Definition C.3. Static effect inclusion An effect ε is included in an effect set ρ = {ε} 1≤i≤n, where (1) ε ∈ ρ, written ε ∈ ρ, if either: ∃ ε i. s.t. ε = ε i; or ∃ ε i. s.t. (ε i = open f m ρ i and ρ i = {ε j} 1≤j≤n i) ∧ (ε = ε f).

This definition says that an effect ε is included in an effect set ρ if it is one of the elements in ρ; or there is an open effect @open f m ρ i in ρ and ε is an element of ρ i.

Definition C.4. Dynamic effect refines static effect A dynamic effect η refines a static effect ρ, where (1) η ∈ ρ, written η ⊑ ρ, if either η = rd, loc, f, id) ∧ (read f) ∈ ρ; or η = wt, loc, f, id) ∧ (write f) ∈ ρ.

Definition C.5. Static effect refinement An effect set ρ i refines another effect set ρ if ρ i ⊑ ρ ∧ (∀(l) ⊏ ρ).

During the evaluation of concurrent tasks, the store keeps changing, and we want to ensure that the same expression has the same static effect in the presence of task interleaving (Theorem C.7). To do so, we define effect equivalent stores (Definition C.8) and prove that these stores give the same effects for a same expression.

Definition C.6. Effect equivalent stores Two stores µ and µ' are effect equivalent, written µ ≡ µ', if both conditions hold: dom(µ) ⊆ dom(µ'); and ∀loc if µ(loc) = c.f.E.E, then µ'(loc) = c.f.E.E', for some E'.

This definition says that two stores are effect equivalent if they have the same effects for all common locations.

Except for the method call expression, proving that an expression has static effects that are refined by their subsequent expression is standard [13][34]. The novelty is that effects for method calls are new in this work and OpenEffectJ needs to maintain proper effects for methods (Definition C.7) and Definition C.8). To prove that a method call on open field has static effects that are refined by their subsequent expression, we introduce well-formed object.

Definition C.7. Well-formed object An object record o = c.f.E.E is a well-formed object in µ, written µ ⊢ o, if for all open effect @open f m ρ 0 ⊈ ρ ∈ rng(E), either (F(f) = loc) ∧ (µ(loc) = c.f'.E'.E') ∧ (E'(m) ⊆ ρ 0); or (F(f) = null) ∧ (ρ 0 = {}).

This definition says that an object record is well-formed, if all of its open effect (@open f m ρ) is supereffect (2) of the effect of the method m of the object the field f is pointing to.

To prove that a method call on a location loc have static effects that are refined by their subsequent expression, we introduce well-formed location (Definition C.8).

Definition C.8. Well-formed location A location loc is well-formed in µ, written µ ⊢ loc, if either µ(loc) = c.f.E.E, ∀m ∈ dom(E) s.t. findMeth(m) = (c', t, m(F var)(e), ρ) ∧ µ(loc) = c.f.E'E, then µ(loc) = null.

A location loc is well-formed in a store µ, if the effect, of each method m of the object loc is pointing to, is supereffect (2) of the effect given by the effect judgment of the body e of the method m.

Finally, to prove the effect preservation theorem (Theorem C.10), we need to prove an invariant of any OpenEffectJ program, i.e., the store is well-formed (Definition C.9). With a well-formed store, it is ready to show that the effect of a method call has expression that is refined by its subsequent expression.

Definition C.9. Well-formed store A store µ is well-formed, written µ ⊢ o, if ∀o ∈ rng(µ) s.t. µ ⊢ o and ∀loc ∈ dom(µ) s.t. µ(loc).
The definition says that the store is well-formed, if all the locations and object records are well-formed.

C.2 Effect Preservation

In this section, we prove OpenEffect’s effect preservation property. This involves three invariants during the evaluation of the concurrent tasks. First, the effect $\rho$ produced by an expression $e$ is refined by the effect $\rho'$, by its subsequence expression $e'$ ($\rho' \subseteq \rho$); and second, the dynamic effect $\eta$, produced by the reduction, if any, refines $\rho$ ($\eta \subsetneq \rho$); finally, the store remains effect equivalent ($\mu \equiv \mu'$).

**THEOREM C.10.** [Effect preservation] Let the program configuration $\Sigma = \langle \langle e, (id, I) + \psi, \mu \rangle \rangle$. If it transits to another configuration $\Sigma' = \langle \langle e', (id, I') + \psi', \mu' \rangle \rangle$, the store is well-formed $\mu \vdash o$, $\mu \vdash e : \rho$ and $\eta \subseteq \rho$, then there is some $\rho'$, $\chi s.t.$

(a) $\mu \equiv \mu'$

(b) $\mu \vdash e' : \rho'$, and $\rho' \subseteq \rho$

(c) $\text{dyn}(\Sigma, \chi, Y) = (\Sigma', \chi + \eta, \chi') \Rightarrow (\eta \subsetneq \rho)$

**Proof:** The proof is by cases on the reduction step applied. We first state two useful lemmas.

C.2.1 Replacement with Subeffect

The following lemma says that two effect equivalent stores give the same effect $\rho$ to the same expression $e$. Because we will prove that during the concurrent execution of the tasks, all the stores are effect equivalent $\mu \equiv \mu'$. Therefore, it suffices to prove that the effect of the subsequence expression $e'$ refines the effect of the expression $e$, given by effect equivalent stores.

**LEMMA C.11.** [Stationary effect] Let $e$ be an expression, $\mu$ and $\mu'$ two stores s.t. $\mu \equiv \mu'$. If $\mu \vdash e : \rho$ and $(\perp) \not\subseteq \rho$, then $\mu' \vdash e : \rho$.

**Proof:** Proof is by induction on the structure of the expression $e$. We prove it by case by case on the rule used to generate the effect $\rho$. In each case we show that $\mu \vdash e : \rho$ implies that $\mu' \vdash e : \rho$, and thus the claim holds by the induction hypothesis (IH). The base cases include (NEW), (NULL), (LOC), and (VAR). These cases are obvious: $\rho' = \rho = \emptyset$. The remaining cases cover the induction step. The IH is that the claim of the lemma holds for all sub-derivations of the derivation being considered. The case for (SET-OPEN) and (CALL) hold because in these cases $\perp \subseteq \rho$.

The cases for (DEFINE), (SEQUENCE), (GET), (SET), (YIELD), and (FORK) follow directly from the induction hypothesis. We show the case for (FORK) and other cases are similar.

**FORK** The last type derivation step is:

$$
\mu \vdash e_0 : \rho_0 \quad \mu \vdash e_1 : \rho_1 \\
\mu' \vdash e_0 : \rho'_0 \quad \mu' \vdash e_1 : \rho'_1
$$

By the IH, $\rho'_0 \subseteq \rho_0$ and $\rho'_1 \subseteq \rho_1$. Therefore $\rho' = \rho'_0 \cup \rho'_1 = \rho_0 \cup \rho_1 = \rho$, and the claim holds.

**CALL-OPEN** Here $e = \text{loc}.f.m(e_1, \ldots, e_n)$. The last type derivation step has the following form:

$$
\begin{align*}
\mu(\text{loc}) &= [c.F.E] \\
\mu' (\text{loc}) &= [c.F'.E'] \\
\mu \vdash \text{loc}.f.m : \rho_0 \\
\mu' \vdash \text{loc}.f.m : \rho'_0
\end{align*}
$$

Clearly, $\rho_0 = \rho'_0 = \{\text{read } f\}$. Since $\mu \equiv \mu'$, the effect maps $E$ are the same. By the IH, $\forall i \in \{1..n\} \vdash \rho_i' = \rho_i$. Thus $\rho' = \{\text{open } f \in \rho'\} \cup \bigcup_{i=0}^{n} \rho_i'$. Therefore, the claim holds.

**CALL-LOC** Here $e = \text{loc}.m(e_1, \ldots, e_n)$. The last type derivation step has the following form:

$$
\begin{align*}
\mu(\text{loc}) &= [c.F.E] \\
\mu' (\text{loc}) &= [c.F'.E'] \\
\mu \vdash \text{loc}.m : \rho_0 \\
\mu' \vdash \text{loc}.m : \rho'_0
\end{align*}
$$

Since $\mu \equiv \mu'$, the effect maps $E$ are the same and $\rho_0 = \rho'_0$. By the induction hypothesis, $\forall i \in \{1..n\} \vdash \rho_i' = \rho_i$. Thus $\rho' = \bigcup_{i=0}^{n} \rho_i' = \rho$, and the claim holds.

Thus, for all possible derivations of $\mu \vdash e : \rho$ and $\mu' \vdash e' : \rho'$, we see that $\rho' = \rho$.

**Proof:** The following lemma says that given two effect equivalent stores, and the same evaluation context, if the effect of the subsequence expression $e'$ refines the original expression $e$, then the effect of the entire subexpression $\mu' \vdash [e'] : \rho'$ refines the entire original expression $\mu' \vdash [e] : \rho'$. With this lemma, it suffices to show that the effect of the subsequence expression $e'$ refines the original expression $e$.

**LEMMA C.12.** [Replacement with subeffect] If $\mu \vdash 0$, $\Sigma \rightarrow \Sigma' = \langle \langle \mu, \psi, \xi \rangle \rangle$, $\xi = \langle \xi', \psi', \mu' \rangle$, $\mu \vdash [e] : \rho$, $\mu' \vdash [e'] : \rho'$, $\mu' \vdash [e'] : \rho' \supseteq \rho$, and $\xi$ holds, the claim holds.

By the definition of field lookup, $\text{typeOfF}(f) = (c, i)$. Thus, by (E-SET), $\mu' \vdash [e'] : \rho_1 \cup \rho_2 \cup \{\text{write } f\}$.

**Case \(v_0.f = -\)** The last step for $\mu' \vdash [e']$ should be (E-SET):

$$
\mu' \vdash [e'] : \rho' \quad \mu' \vdash [e] : \rho \quad \{\text{write } f\}
$$

So $\mu' \vdash [e'] : \rho_1 \cup \{\text{write } f\}$.

**Case \(-m(e_1, \ldots, e_n)\)** The last step in the effect derivation for $\mu' \vdash [e]$ should be (E-CALL-OPEN): $e = \text{loc}.f$.

$$
\begin{align*}
\mu(\text{loc}) &= [c.F.E] \\
\mu' (\text{loc}) &= [c.F'.E'] \\
\mu \vdash \text{loc}.f.m \cup \{\text{open } f \in \rho'\} \\
\mu' \vdash \text{loc}.f.m \cup \{\text{open } f \in \rho'\}
\end{align*}
$$

By (GET), $e' = \text{loc}'$.

$$
\begin{align*}
\mu(\text{loc}') &= [c.F.E'] \\
\mu' (\text{loc}') &= [c.F'.E'] \\
\mu \vdash \text{loc}.' : \rho' \\
\mu' \vdash \text{loc}.' : \rho'
\end{align*}
$$

Because $\mu \equiv \mu'$, by Definition C.9 and Definition C.7, we have $\rho'_0 \subseteq \rho'_1$, $\forall i \in \{1..n\} \epsilon_i$. Does not change, thus $\rho'_1 = \rho'_0$. Therefore, the claim holds.
Refines the one before the substitution.

\[ \mu \vdash \{ c, E \} \]

\( \mu(E) = \mu(p)^n \) \quad \( \forall i \in \{p + 1, n\} : \mu(e_i) = \rho_i^n \)

\( \mu \vdash E \colon \rho_0 \cup \rho^n \cup \bigcup_{i=p+1}^n \rho_i \)

By (E-CALL-LOC), \( \mu \vdash E_2[e'] : \rho_1 \cup \rho^n \cup \bigcup_{i=p+1}^n \rho_i \).

Using the lemmas

To prove Theorem 1.2.1 in each reduction case, let \( e = \{ \mu_0 \} = \mu_0 \vdash e_1 \vdash \nu_1 \) and \( \mu_0 \vdash e_1 : \rho_1 \). Given that (a) \( \mu \equiv \mu_0 \), by Lemma 1.1, and Lemma 1.11, we divide the cases into 3 categories: in the first category, some variables (var) will be replaced by actual values (v), in Section 1.2.2.2, the cases, in the second category, access the store, in Section 1.2.2.3, and the other cases are listed below.

Here all the rules leave no dynamic trace, and (c) holds. All the cases, other than the New Object, do not change the store, i.e., \( \mu' = \mu \), therefore \( \mu \equiv \mu' \) and (a) holds.

New Object:

Here \( e = \{ new \ c \} \), \( e' = \{ \text{yield loc} \} \), where \( \text{loc} \notin \text{dom} \mu \), \( \mu' = \{ \text{loc} \} \vdash \text{null} \colon \{ f \in \text{fields}(c) : \{ m \mapsto \rho \in \text{meth}(c) \} \} \vdash \mu \). Because this rule does not change any object, \( \mu \equiv \mu' \). Also new \( c \) : \( \emptyset \) and \( \mu' \vdash \text{yield loc} \vdash \emptyset \), and (b) holds.

Yield:

Here \( e = \{ \text{yield e}_1 \} \), \( e' = \{ e_1 \} \). Notice that \( id \) remains unchanged in the statement of the theorem, i.e., the reduction step does not switch control to other task. Therefore \( \mu' = \mu, \mu \equiv \mu' \) and the claim holds.

Fork Sequential:

Here \( e = \{ \text{fork}(e_0', e_1') \} \), \( e' = \{ \text{yield e}_2' \} \) and \( e_0' = e_0, e_1' = \text{null} \). Let \( \mu \vdash e_0' : \rho_0 \vdash \rho_1 \). By (FORK), \( \mu \vdash e_0' : \rho_0 \vdash e_1' : \rho_1 \). Therefore, \( \mu' \vdash e_0', e_1' : \rho_0 \vdash \rho_1 \). (b) holds.

(b) holds.

Fork Parallel:

Here \( e = \{ \text{fork}(e_0', e_1') \} \), \( e' = \{ \text{yield null} \} \). Since \( \mu \vdash \text{null} : \emptyset \), (b) holds.

C.2.2 Substituting Variables with Values

Here all the rules leave no dynamic trace, and (c) holds. Neither do they change the store, i.e., \( \mu = \mu' \) and \( \mu \equiv \mu' \), thus (b) holds. We state a lemma for substituting the variables \( \var{v} \) for the actual values \( v \), which indicates that the static effect \( \rho' \) after the substitution refines the one before the substitution \( \rho \). This lemma is useful for method calls and definitions, where parameters and local variables, respectively, will be substituted by values.

**Lemma C.13.** (Substitution effect) If \( \mu \vdash e : \rho \), then there is some \( \rho' \), such that \( \mu \vdash [v_1/\var{v_1}, \ldots, v_n/\var{v_n}] e : \rho' \), for all values \( v_i \) and free variables \( \var{v_i} \), and \( \rho' \subseteq \rho \).

**Proof.** To simplify the notations, let \( [\var{v}] = [v_1/\var{v_1}, \ldots, v_n/\var{v_n}] \).

We prove it by structural induction on the derivation of \( \mu \vdash e : \rho \) and by cases, based on the last step in that derivation. The base cases include (E-NEW), (E-NULL), (E-LOC), and (E-VAR). The first three of these cases are obvious: \( e \) has no variables, \( \rho' = \emptyset \). In the (E-VAR) case, \( \mu \vdash v : \emptyset \) and \( \mu \vdash v \} = \emptyset \). Thus, it holds.

The remaining cases cover the induction step. The induction hypothesis (IH) is that the claim of the lemma holds for all subderivations of the derivation being considered.

The cases for (E-GET), (E-DEFINE), (E-YIELD), and (E-SEQ) follow directly from the induction hypothesis.

The case for (E-SET-OPEN) and (E-CALL) hold because in these cases \( \bot \subseteq \rho \). \( \bot \) is the maximum, any effect \( \rho' \subseteq \bot \).

(E-CALL-OPEN) Here \( e = \{ loc.f.m(e_1), \ldots, e_n \} \). The last effect derivation step has the following form:

\[ \mu \vdash \{ loc.f.m \} : \rho_0 \vdash \bigcup_{i=0}^n \rho_i \]

Let \( e_i' = [\var{v}] e_i \) for \( i \in \{1, n\} \). \( [\var{v}] e_i = \text{loc.f.m}(\var{v}) \). We show that \( \mu \vdash \var{v} : \rho_0 \vdash \bigcup_{i=0}^n \rho_i \).

(E-CALL-LOC) Here \( e = \{ loc.m \} \). The last step is:

\[ \mu \vdash \{ loc.m(e_1) \} : \rho_0 \vdash \bigcup_{i=0}^n \rho_i \]

Let \( e_i' = [\var{v}] e_i \) for \( i \in \{1, n\} \). \( [\var{v}] e_i = \text{loc.f.m}(\var{v}) \). We show that \( \mu \vdash \var{v} : \rho_0 \vdash \bigcup_{i=0}^n \rho_i \).

(E-SET) Here \( e = e_0.f = e_1 \). The last derivation step is:

\[ \mu \vdash e_0 : \rho_0 \cup \rho \vdash e_1 : \rho_1 \]

Using the lemma

We now present the case for method call and local declaration.

**Method Call:** Here \( e = \{ loc.m(\var{v}) \} \), \( (u', \text{loc.m}(\var{v}) \{ e_2 \}) : \rho_0 \) = findMethod(u,m), \( e'_1 = \text{yield e}_1 \), \( e_1 = \text{loc/this e}_2 \).

Let \( \mu \vdash \text{loc.m}(\var{v}) : \rho_0 \), i.e., \( E(m) = \rho_0 \). Let \( e_3 = \{ \text{this e}_2 \} : \rho_3 \vdash \rho_1 \) and \( \mu \vdash e_1 : \rho_1 \). By Lemma C.13, \( \rho_1 \subseteq \rho_0 \). By \( \mu \vdash \text{null} : \emptyset \), Definition C.8 and Definition C.9, \( \rho_1 \subseteq \rho_0 \), thus \( \rho_0 \).

Local Declaration:

Here \( e = \{ \text{var} = v \} \). \( e' \) = \( [\var{v}] e_1 \). Let \( \mu \vdash e_1 : \rho_0 \). By (E-DEFINE), \( \mu \vdash \text{var} : v_1 \vdash e_1 : \rho_0 \). \( \mu \vdash [\var{v}] e_1 : \rho_1 \), for some \( \rho_1 \subseteq \rho_0 \), by Lemma C.13.

C.2.3 Fields Access

In this subsection, we first state a lemma for the effect relationship between an expression and its subexpression. The following lemma says that the effect \( \rho \) of subexpression \( e \) is a subset \( \subseteq \) of the effect \( \rho' \) of its entire expression \( E[e] \).

**Lemma C.14.** (Subexpression effect containment) If \( \mu \vdash e : \rho \) and \( \mu \vdash E[e] : \rho' \), then \( \rho \subseteq \rho' \).

Proof: By the effect rule for each expression, the effect of any direct subexpression is a subset of the entire expression.
Using the lemma: We now prove cases for field accesses.

Field Get: Here $e = \exists[\text{loc}, f, v]$, $e' = \exists[\text{yield}, v]$, where $\mu(\text{loc}) = [u.F.E]$, $F(f) = v$, $\mu' = \mu$ and $\mu \cong \mu'$. Because $\mu \cong \text{loc}, f$: $\{\text{read}, f\}$, and $\mu' \gtrdot \text{yield}, v \vdash \emptyset$, (b) holds. Finally, $\eta = (\text{rd}, \text{loc}, f, i)$, and $\eta \cong \{\text{read}, f\} \subseteq \rho$, by Lemma C.14.

Field Set: Here $e = \exists[\text{loc}, f = v], e' = \exists[\text{yield}, v], \mu' = \mu \oplus (\text{loc} \mapsto \alpha)$, and $\alpha = [u.F(\exists(f \mapsto v))].E$, where $\mu(\text{loc}) = [u.F.E]$ and typeQF$(f) = (c,t)$ for some $t$. The field is an open field, and by the function update, it does not update any effect, and $\mu \cong \mu'$. To see $\mu \cong \exists[v]; \rho' \subseteq \rho$, we have $\mu \cong \text{loc}, f = v; \{\text{write}, f\}$, and $\mu' \vdash v : \emptyset$, thus $\rho' \subseteq \rho$. Finally, $\eta = (\text{wt}, \text{loc}, f, i)$, and $\eta \cong \{\text{write}, f\}$, by Lemma C.14.

Field Set Open: Here $e = \exists[\text{loc}, f = v], e' = \exists[\text{yield}, v]$, where $\mu_0 = \mu \oplus (\text{loc} \mapsto c([F(\exists(f \mapsto v))].E))$, and $\mu' = \text{update}(\mu_0, \text{loc}, f, v)$. Impossible, since $\emptyset \notin \rho$. |  

C.3 Deterministic Semantics
The goal of this section is to show that the tasks generated by a fork expression do not interfere (Theorem C.25) and therefore OpenEffectI provides deterministic results. First we show that the expressions, in later configurations of a task, refine the expressions in earlier configurations [34]. We define multistep reduction (Definition C.15), which relates the later configurations with earlier configurations. To reason about the interaction between the two concurrent tasks, we define the newly generated queue, in Definition C.17, which is formed by these two tasks. To prove that the tasks do not have heap interference, we introduce the accumulated dynamic effect in Definition C.16 (accumulated heap effects) and show that these accumulated effects, produced by a concurrent task id and all its descendants (Definition C.18), refine the static effect computed when id is forked off.

Definition C.15. [Multiple reduction steps] We write $\Sigma \vdash_{\text{S}} \Sigma'$ if $\Sigma \vdash_{\text{S}} \Sigma'$, and $\Sigma \vdash_{\text{S}} \Sigma' \vdash_{\text{S}} \Sigma''$ if $(\Sigma \vdash_{\text{S}} \Sigma' \vdash_{\text{S}} \Sigma'' \vdash_{\text{S}} \Sigma'') \wedge (\Sigma' \vdash_{\text{S}} \Sigma'').$ We write $\Sigma \vdash_{\text{S}} \Sigma'$ if $\exists n \geq 0 \Sigma_n \vdash \Sigma'$.  

Definition C.16. [Multi step effect] The multi step effect function dynE is: $\text{dynE}(\Sigma, \chi, Y, n) = \text{dynE}(\Sigma', \chi', Y', n-1), \text{if dyn}(\Sigma, \chi, Y) = (\Sigma', \chi', Y', 0) = \text{dynE}(\Sigma, \chi, Y)$. Here, the function dyn produces the dynamic effect and the relationship $\chi$ for an one step transition from a configuration to another. The function dynE accumulates the dynamic effects and the relationship for n transition steps.

Definition C.17. [Queue for parallel fork] We said that $\psi'$ is a queue for parallel fork tasks and we write $\Sigma \vdash_{\text{S}} \psi'$, if $\Sigma \vdash_{\text{S}} \Sigma'$, $\Sigma = (\exists[\text{fork} (e,e')], \psi, \psi, \mu)$, and $\Sigma' = (\exists[\text{fork} (e,e')], \psi + \psi, \psi, \mu)$. The queue $\psi'$ for parallel fork contains the two concurrent tasks generated by the fork expression.

To say that concurrent tasks do not interfere (heap accesses), we define the noninterference relation for dynamic effects $(\eta\eta')$ as follows: the noninterference relation is symmetric; reads effects do not conflict with each other; read-write and write-write pairs do not conflict if the location or the field is different. A set of dynamic effects $\varphi = \{\eta_1, \eta_2\}$ do not conflict with another set $\varphi' = \{\eta_1', \eta_2'\}$ of $\varphi \setminus \eta_1 \setminus \eta_1'$ or $\varphi \setminus \eta_2 \setminus \eta_2'$.

Definition C.18. [Descendant] A task id' is a descendant of a task id, with $\chi'$, written as $id' \preceq id$ if $id' \in \text{desc}(id, Y)$. Here, $\text{desc}(id, Y) = \{id_{\chi_1}, \ldots, id_{\chi_n}\}$, and $\text{desc}(id, Y) = \{id_{\chi_1}, \ldots, id_{\chi_n}\}$, and $\forall id_{\chi} \in \text{desc}(id, Y), Y(id) = L$. The descendant is a recursive relationship. The descendant of a task id includes the children tasks id' of id and all the descendant of id'.
We will prove it by induction on $n$. The base case $n = 0$. Note that

$\Sigma = \langle E', \Psi \rangle \cup (\psi, \mu)$ and when the fork expression is being evaluated, the queue is empty ($\bullet$). According to the (Yield) rule, the next configuration must schedule a task $id_1$ in $\psi$, by the active function, i.e., $\Sigma_0 = \langle \langle E'_1, \langle (i_1, j_1) \rangle \rangle \rangle \cup (\psi, \mu)$ and $\langle E'_1, \langle (i_1, j_1) \rangle \rangle \rangle \rangle \cup (\psi, \mu)$. As stated, for $id_1$ and $id_2, \rho_1 \rho_2, \tau_1 \tau_2$, thus (a) holds. We have $\mu \vdash \circ$, by Theorem C.10 (b) holds, (c) holds, because this is the first time the task id$_1$ makes progress, i.e., $\beta \Sigma, \tau \cdot \Sigma \Rightarrow \Sigma$.

For the induction step, we have $\forall j \cdot s.t. 0 \leq j \leq i$ all the conditions of the lemma are true, and it suffices to prove that when $j = i + 1$, the lemma is true.

Let $\Sigma_j = \langle \langle E[i], \langle (i, j) \rangle \rangle \rangle \cup (\psi, \mu) \rangle$ and $\Sigma_{j + 1} = \langle \langle E[i], \langle (i, j + 1) \rangle \rangle \rangle \cup (\psi, \mu, \mu_{j + 1} \vdash \circ) \rangle$ and $\Sigma_{j + 2} = \langle \langle E[i], \langle (i, j + 2) \rangle \rangle \rangle \cup (\psi, \mu_{j + 1}, \mu_{j + 1}) \vdash \circ \rangle$. By Lemma C.20 $\mu_{j + 1} \vdash \circ$.

1. if $id_1 = id_2$, by Theorem C.10 (a) holds;

2. $id_1 \neq id_2$, then $\mu_{j + 1} \vdash \circ$ for some $e'$ for $\mu_{j + 1} \vdash \circ$.

For (b), if $id_1 = id_2$, then by Theorem C.10 it holds; otherwise, $\mu_{j + 1} \vdash \circ$ for some $e'$. By (Yield) rule, $\mu_{j + 2} \vdash \circ$. By IH, (1) if $\exists k \cdot s.t. \Sigma_k \Rightarrow \Sigma_{k + 1}$, then $\rho_{j + 1} \vdash \circ$.

For all steps $n \leq N$, we see that $\eta \vdash \circ$, and for each local reduction $\Sigma \Rightarrow \Sigma'$, $\rho \vdash \circ$. By Lemma C.22 the effect of a child task refines the corresponding fork expression of its parent task. Thus, dyn.Eset(id$_1, X, Y$) dyn.Eset(id$_2, X, Y$), if $\rho \vdash \circ$.

Theorem C.25. (Deterministic semantic) Let $\mu \vdash \circ$, $\Sigma \Rightarrow \Sigma'$, and $\Sigma \Rightarrow \Psi$ and $\Sigma \Rightarrow \Psi$. For the two tasks $\langle (i, j, \mu) \rangle \Rightarrow \langle (i, j, \mu) \rangle \Rightarrow \langle (i, j, \mu) \rangle \Rightarrow \Psi, \mu \vdash \circ$. By IH, $\mu \vdash \circ$.

Proof: Note that the difference between this theorem and Theorem C.24 is that $\psi$ may or may not be $\bullet$. Observe that there exists $\Sigma_{\psi} = \langle \langle E, \langle (i, j, \mu) \rangle \rangle \rangle \Rightarrow \psi \Rightarrow (\psi, \mu)$. Without loss of generality, assume that the task $id_1$ finishes before $id_2$. Let $N$ be the smallest integer such that both tasks $id_1$ and $id_2$ are done, i.e., $\Sigma_N = \langle (i, j, \mu) \rangle \Rightarrow (\psi, \mu) \Rightarrow \Sigma_N \Rightarrow \Psi$. By Lemma C.24 $\forall 0 \leq k \leq N$ if $\Sigma_k \Rightarrow \Sigma_{k + 1}$, then $\mu_k \vdash \circ$. Observe that all the conditions of Lemma C.24 are still correct in this theorem and the claim holds.

C.4 Type Soundness

In this section, we prove the standard type preservation property. Type rules omitted in Section 3 are in Figure C.4. To prove the type preservation, we extend the type environment, which maps variables and locations to types.

Before proving the type preservation theorem, we define the consistency between a type environment and a store [19], which is standard. One difference between concurrent tasks application and serial application is context switching. We will show in the type preservation theorem that after the control comes back to the current task, the remaining expression has the same type before yielding control. This is mainly proven by Lemma C.31 i.e., each task in the reduction do not change the type of locations in the type environment and the type environment keeps extending (Definition C.27 i.e. $\Pi \subset \Pi'$). Also, we need to ensure that during the evaluation, all the tasks have proper types, i.e., all the tasks in the queue $\psi$ are well-typed (Definition C.28 and Definition C.29). Finally, we state the standard lemmas [14, 19] (Lemma C.30 Lemma C.31 Lemma C.32 and Lemma C.33).

Definition C.26. [Environment-store consistency] A store $\mu$ is consistent with a type environment $\Pi$, written $\mu \rhd \Pi$ if all of the following hold:

1. $\forall s.t. \mu(\pi) = t, \exists c$.
2. $\exists c$.
3. $\exists c$.
4. $\exists c$.
5. $\exists c$.

Definition C.27. [Environment enlargement] Let $\Pi$ and $\Pi'$ be two type environments. We write $\Pi \lhd \Pi'$ if $\exists \Pi \subseteq \Pi'$ and $\forall c \in \Pi$. If $\Pi(\pi) \rhd \Pi'$, then $\Pi(\pi) \rhd \Pi'$.

This definition says that an environment $\Pi'$ enlarges another environment $\Pi$, if the domain of $\Pi'$ is a subset of $\Pi'$ and, they give the same type for the common location. This definition will be used to show that during the evaluation of any OpenEffectU program, we can use an ever increasing type environment to type check the expressions.

Definition C.28. [Well-typed queue] A queue $\psi$ is well-typed in $\Pi$, written $\Pi \rhd \psi$, if $\forall (e, \tau) \in \psi, \Pi \vdash e : (\tau, \rho)$ for some type $\tau$ and effect $\rho$.

A queue is well-typed, if the expression in each task in the queue has proper type. This definition will be used to prove that after the control go back to the original expression, due to thread interleaving, it has the same type given the update-to-date type environment.

Definition C.29. [Well-typed configuration] A configuration $\Pi \rhd \psi$ is well-typed in $\Pi$, written $\Pi \rhd \psi$, if $\Pi \vdash \psi$ and $\psi \rhd \Pi$.
Lemma C.30. [Substitution] If $\bar{\Pi} \vdash e : (t, p)$ and $\forall i \in \{1..n\}$, $\Pi \vdash v_i : (s_i, 0 \ldots 0) \therefore s_i : t_i$ then $\Pi \vdash [\bar{v}/\bar{e}] r : (s, p')$ for some $s < s'$ and some $p'$.

Proof: To simplify the notations, let $\bar{\Pi} = \Pi \vdash [\bar{v}/\bar{e}] r$. We prove it by structural induction on the derivation of $\Pi \vdash e : (t, p)$ and by cases, based on the last step in that derivation. The base cases include (T-NEW), (T-NULL), (T-LOC), and (T-VAR). The first three of these cases are obvious: $e$ has no variables, $s = t$. In the (T-VAR) case, $e = v$, and there are two subcases. If $v \notin \{\bar{v}_1, \ldots, \bar{v}_n\}$, then $\Pi \vdash (\bar{v}/\bar{e}) = t$ and the claim holds. Otherwise, suppose $v = \bar{v}_k$. Then $\Pi \vdash [\bar{v}/\bar{e}] = v_k$ and, by the assumptions of the lemma, $\Pi \vdash [\bar{v}/\bar{e}] : (s_k, 0)$ and $s_k < s_k = t$.

The remaining cases cover the induction step. The induction hypothesis (IH) is that the claim of the lemma holds for all subderivations of the derivation being considered.

The cases for (T-YIELD), (T-DEFINE), and (T-SEQ) follow directly from the induction hypothesis. (T-FORK) holds because its type is void before and after the substitution.

(T-CALL-OPEN) Here $e = \text{this.f.m} (\vec{c})$. The last type derivation step has the following form:

\[
\begin{array}{l}
\Pi \vdash e'_0 : \text{this.f} \\
\Pi \vdash \text{findMeth}(c_0, 0) = (c_1, t, m (u_1 \ldots, u_n, \bar{\rho}_n)) (e_{n+1}, \rho_2) \\
(\forall i \in \{1..n\} : \Pi' \vdash e'_i : (u'_i, \rho_i) \land u'_i < u_i)
\end{array}
\]

Let $e'_i = \Pi' \vdash [\bar{v}/\bar{e}] r_i : (i, \{\bar{f}/\bar{m} \emptyset \cup \bigcup \rho_i\})$. We show that $\Pi \vdash [\bar{v}/\bar{e}] r : (t, p')$. By IH, $\Pi \vdash e'_0 : (c_0, \rho_0)$, where $c_0 < c_0$. If findMeth$(c_0, 0) = (c_1, t, m (\bar{\tau}/\bar{\rho})(e_{n+1}, \rho_2))$ and findMeth$(c_2, m) = (c_3, t_2, m (\bar{\tau}/\bar{\rho})(e_{n+1}, \rho_2))$, then $\Pi \vdash \text{findMeth}(c_2, m) : (t, \rho)$. Also, by IH, $\forall i \in \{1..n\} : \Pi \vdash e'_i : (u'_i, \rho_i)$ and $u'_i < u_i$. Finally, $\forall i \in \{1..n\} : u'_i < u_i$, by transitivity, the claim holds.

(T-CALL) Here $e = e_0 \cdot m(\vec{c})$. The last type derivation step has the following form:

\[
\begin{array}{l}
\Pi \vdash e_0 : \text{this.f} \\
\Pi \vdash \text{typeOf}(f) = (d, \text{open} c_0) \\
\Pi \vdash \text{findMeth}(c_0, m) = (c_1, t, m (u_1 \ldots, u_n, \bar{\rho}_n)) (e_{n+1}, \rho_0) \\
(\forall i \in \{1..n\} : \Pi' \vdash e'_i : (u'_i, \rho_i) \land u'_i < u_i)
\end{array}
\]

Let $e'_i = \Pi' \vdash [\bar{v}/\bar{e}] r_i : (i, \{\bar{f}/\bar{m} \emptyset \cup \bigcup \rho_i\})$. We show that $\Pi \vdash [\bar{v}/\bar{e}] r : (t, p')$. By IH, $\Pi \vdash e'_0 : (c_0, \rho_0)$, where $u'_0 < u_0$. By the definitions of findMeth and override, if findMeth$(u_0, m) = (c_1, t, m (\bar{\tau}/\bar{\rho})(e_{n+1}, \rho_0))$, and findMeth$(u_0, m) = (c_2, t_2, m (\bar{\tau}/\bar{\rho})(e_{n+1}, \rho_0)))$, then $t_2 < t$. Also, by IH, $\forall i \in \{1..n\} : \Pi \vdash e'_i : (u'_i, \rho_i)$ and $u'_i < u_i$. Finally, $\forall i \in \{1..n\} : u'_i < u_i$, by transitivity, the claim holds.

(T-CALL-OPEN) Here $e = \text{loc}.f.m(\vec{c})$. The last type derivation step has the following form:

\[
\begin{array}{l}
\Pi \vdash e_0 : \text{this.f} \\
\Pi \vdash \text{typeOf}(f) = (d, \text{open} c_0) \\
\Pi \vdash \text{findMeth}(c_0, m) = (c_1, t, m (u_1 \ldots, u_n, \bar{\rho}_n)) (e_{n+1}, \rho_0) \\
(\forall i \in \{1..n\} : \Pi' \vdash e'_i : (u'_i, \rho_i) \land u'_i < u_i)
\end{array}
\]

Let $e'_i = \Pi' \vdash [\bar{v}/\bar{e}] r_i : (\{\bar{f}/\bar{m} \emptyset \cup \bigcup \rho_i\})$. We show that $\Pi \vdash [\bar{v}/\bar{e}] r : (t, p')$. By IH, $\Pi \vdash e'_0 : (c_0, \rho_0)$, where $u'_0 < u_0$. By the definitions of findMeth and override, if findMeth$(u_0, m) = (c_1, t, m (\bar{\tau}/\bar{\rho})(e_{n+1}, \rho_0))$, and findMeth$(u_0, m) = (c_2, t_2, m (\bar{\tau}/\bar{\rho})(e_{n+1}, \rho_0))$, then $t_2 < t$. Also, by IH, $\forall i \in \{1..n\} : \Pi \vdash e'_i : (u'_i, \rho_i)$ and $u'_i < u_i$. Finally, $\forall i \in \{1..n\} : u'_i < u_i$, by transitivity, the claim holds.

(T-GET) Here $e = e'.f$. The last derivation step is:

\[
\begin{array}{l}
\Pi \vdash e' : (c, p') \\
\Pi \vdash \text{typeOf}(f) = (d, t) \\
\Pi \vdash t < : (t, \rho_0 \cup \{\text{read } f\})
\end{array}
\]

Now $\Pi' \vdash [\bar{v}/\bar{e}] r : (\{\bar{f}/\bar{m} \emptyset \cup \bigcup \rho_i\})$. By IH, $\Pi \vdash e'.f : (\{\bar{f}/\bar{m} \emptyset \cup \{\text{read } f\}\})$. The claim holds.

(T-GET-OPEN) Here $e = \text{this}.f$. The last step is:

\[
\begin{array}{l}
\Pi' \vdash (\text{this.f}) : c \\
\Pi \vdash \text{typeOf}(f) = (d, \text{open} t) \\
\Pi \vdash t < : (t, \rho_0 \cup \{\text{read } f\})
\end{array}
\]

There are two subcases: 1) if this $\notin \{\bar{v}_1, \ldots, \bar{v}_n\}$, then $\Pi \vdash e = \Pi \vdash e$ and the claim holds. Otherwise, suppose this $= \bar{v}_k$. Then $\Pi' \vdash [\bar{v}/\bar{e}] r = v_k.f$ and, by (T-GET-OPEN-LOC), $\Pi' \vdash [\bar{v}/\bar{e}] r : (t, \{\text{read } f\})$.

(T-GET-OPEN-LOC) Here $e = \text{loc}.f$. This expression has no free variable, the claim holds.

(T-SET) Here $e = e'.f = e_2$. The last derivation step is:

\[
\begin{array}{l}
\Pi' \vdash e'_1 : (c, p_1) \\
\Pi \vdash \text{typeOf}(f) = (d, u) \\
\Pi \vdash t < : (t, \rho_0 \cup \{\text{write } f\})
\end{array}
\]

Now $\Pi' \vdash [\bar{v}/\bar{e}] r : (\{\bar{f}/\bar{m} \emptyset \cup \bigcup \rho_i\})$. By IH, $\Pi \vdash e'_1 : (\{\bar{f}/\bar{m} \emptyset \cup \{\text{write } f\}\})$. The last step is:

Thus, for all possible derivations of $\Pi' \vdash e : (t, p)$ we see that $\Pi \vdash [\bar{v}/\bar{e}] r : (t, \rho_0)$.

Lemma C.31. [Environment extension] If $\Pi \vdash e : (t, p)$ and $a \notin \text{dom(}\Pi))$, then $\Pi, a : t' \vdash e : (t, p)$.

Proof: Observe that the effect does not depend on the typing environment and it suffices to prove the typing relationship. The proof is by structural induction on the derivation of $\Pi \vdash e : (t, p)$. The base cases are (T-NEW), (T-NULL), (T-LOC), and (T-VAR). In (T-NEW)
and (T-NULL), the type environment does not appear in the hypotheses of the judgment, so the claim holds. For the (T-VAR) case, e = var and \( \Pi(var) = t \). But \( a \notin \text{dom}(\Pi) \), so var \( \neq a \). Therefore, \( (\Pi, a : t') (var) = t' \) and the claim holds for this case. The (T-LOC) case is similar. The remaining rules cover the induction step. By the induction hypothesis, changing the type environment to \( (\Pi, a : t') \) does not change the types and effects assigned by any hypotheses of each rule. Therefore, the types and effects assigned by each rule are also unchanged and the claim holds.

**LEMMA C.32. (Replacement)** If \( \Sigma = (\{E[e], (id, I)\} + \psi, \mu) \), \( \Sigma' = (\{E'[e'], (id, I')\} + \psi', \mu') \), \( E \rightarrow \Sigma', \Pi \vdash E'[e'] : (t, \rho) \), \( \Pi\vdash e' : (t', \rho') \) and \( \Pi\vdash e' : (t', \rho'_0) \), then \( \Pi\vdash E'[e'] : (t, \rho_0) \), for some \( \rho_0 \).

**Proof:** Proof is by induction on the size of the evaluation context. Since the \( E \) refers to the number of recursive applications of the syntactic rules necessary to create \( E \). In the base case, \( E \) is size zero, \( E = - \), and \( t' = u' < u = t \). For the induction step we divide the evaluation context into two parts such that \( E[e_1] = E_1 [E_2[e_2]] \), and \( E_2 \) has size one. The induction hypothesis (IH) is that the lemma holds for all evaluation contexts, which is smaller than the one \( E_1 \) considered in the induction step. We prove it case by case on the rule used to generate \( E_2 \). In each case we show that \( \Pi \vdash E_2[e] : (s, \rho) \) implies that \( \Pi \vdash E_2[e'] : (s, \rho') \), for some \( \rho' \), and thus the claim holds by IH.

The cases for \( \text{loc}_0 \rightarrow f = - \), \( - \rightarrow e_2 \), and \( (e, \var) \rightarrow = e_2 \) follow directly from the induction hypothesis.

**Case \( \rightarrow m(\bar{a}) \)** The last step for \( E_2[e] \) could be
\[
\Pi\vdash e : (u, \rho_0) \quad \forall i \in \{1, n\} : \Pi\vdash e_i : (t'_i, \rho'_i) \therefore \Pi\vdash E_2[e] : (t, \rho'_0) \]

Here \( \text{findMeth}(u, m) = (c_2, t, m (T\\text{Var}) (\{e'_n\} + \rho''_n)) \), by the definitions of \( \text{override} \) and \( \text{findMeth} \), where \( E_2 < c_1 \), so (T-CALL) gives \( \Pi\vdash E_2[e] : (t, \rho') \); or
\[
\Pi\vdash E_2[e'] : (t', \rho') \quad \Pi\vdash e' : (\{\text{open} f m \theta\} \cup \rho' \cup \bigcup_{i=1}^n \rho''_i) \]

It must be the case that \( e' = \text{loc}_f \). From the statement of the lemma, we have \( \Pi\vdash \text{loc}_f : (t', \rho'_0) \). Also the results of \( \text{typeOf} \) and \( \text{findMeth} \) does not change, therefore, by (T-CALL-OPEN-LOC), the type of the expression is \( t \).

**Case \( \rightarrow \text{loc}_f \)** The last step for \( E_2[e] \) could be
\[
\Pi\vdash e : (u, \rho_0) \quad \forall i \in \{1, n\} : \Pi\vdash e_i : (t'_i, \rho'_i) \therefore \Pi\vdash E_2[e] : (t, \rho'_0) \]

Here \( \text{findMeth}(u, m) = (c_2, t, m (T\\text{Var}) (\{e'_n\} + \rho''_n)) \), by the definitions of \( \text{override} \) and \( \text{findMeth} \), where \( E_2 < c_1 \), so (T-CALL) gives \( \Pi\vdash E_2[e] : (t, \rho') \); or
\[
\Pi\vdash E_2[e'] : (t', \rho') \quad \Pi\vdash e' : (\{\text{open} f m \theta\} \cup \rho' \cup \bigcup_{i=1}^n \rho''_i) \]

It must be the case that \( e' = \text{loc}_f \). From the statement of the lemma, we have \( \Pi\vdash \text{loc}_f : (t', \rho'_0) \). Also the results of \( \text{findMeth} \) does not change, therefore, by (T-CALL), the type of the expression is \( t \).

**Case \( \rightarrow f \)** The last step for \( E_2[e] \) could be
\[
\Pi\vdash e : (c, \rho_0) \quad \text{typeOf}(f) = (d, t) \quad c < : d \quad \Pi\vdash E_2[e] : (t, \rho_0 \cup \{\text{read } f\}) \]

The result of \( \text{typeOf} \) does not change. Thus, by (T-OPEN-LOC), \( \Pi\vdash E_2[e] : (t, \rho_0) \); or
\[
\Pi\vdash E_2[e] : (t, \rho_0) \quad \Pi\vdash e : (u, \rho_0) \quad \Pi\vdash e' : (u', \rho_1) \text{ and } u' < : u \quad \text{then } \Pi\vdash E_2[e'] : (t', \rho'_0) \text{ where } t' < : t. \]

**LEMMA C.33. (Replacement with subtyping)** If \( \Sigma = (\{E[e], (id, I)\} + \psi, \mu) \), \( \Sigma' = (\{E'[e'], (id, I')\} + \psi', \mu') \), \( E \rightarrow \Sigma', \Pi \vdash E'[e'] : (t, \rho) \), \( \Pi\vdash e' : (u', \rho_1) \) and \( u' < : u \), then \( \Pi\vdash E_2[e'] : (t, \rho'_0) \).

**Proof:** Proof is by induction on the size of the evaluation context. Since the \( E \) refers to the number of recursive applications of the syntactic rules necessary to create \( E \). In the base case, \( E \) has size zero, \( E = - \), and \( t' = u' < : u = t \). For the induction step we divide the evaluation context into two parts such that \( E[e_1] = E_1 [E_2[e_2]] \), and \( E_2 \) has size one. The induction hypothesis (IH) is that the lemma holds for all evaluation contexts, which is smaller than the one \( E_1 \) considered in the induction step. We prove it case by case on the rule used to generate \( E_2 \). In each case we show that \( \Pi\vdash E_2[e] : (s, \rho) \) implies that \( \Pi\vdash E_2[e'] : (s', \rho') \), for some \( s' < : s \), and the claim holds by IH. The cases for \( \text{loc}_0 \rightarrow f = - \), \( - \rightarrow e_2 \), and \( (e, \var) \rightarrow = e_2 \) follow directly from IH.

4Formulation of the proof is similar to Clifton's work [14] and Flatt's work [19]
\[ e = \text{this}, f \quad \text{typeOff}(f) = (d, \emptyset) \]
\[ (c_1, t, m (\forall v) \{ e_{n+1}, \rho_1 \}) = \text{findMeth}(t', m) \quad \forall i \in \{1..n\} :: \Pi \vdash e_i : (t'_i, \rho'_i) \quad t'_i < t_i \]
\[ \Pi \vdash E_2[e] : (t, \{ \}) \]

We have \( \text{findMeth}(t', m) = (c_2, t, m (\forall v) \{ e_{n+1}, \rho_1 \}) \), by the definitions of \textit{override} and \textit{findMeth}, \( c_2 < c_1 \), so (T-CALL) gives 
\[ \Pi \vdash E_2[e] : (t, \{ \}) \]

\[ e = \text{loc}, f \quad \text{typeOff}(f) = (d, \emptyset) \]
\[ (c_1, t, m (\forall v) \{ e_{n+1}, \rho_1 \}) = \text{findMeth}(t', m) \quad \forall i \in \{1..n\} :: \Pi \vdash e_i : (t'_i, \rho'_i) \quad t'_i < t_i \]
\[ \Pi \vdash E_2[e] : (t, \{ \}) \]

It must be the case that \( e' = \text{loc}.f \). From the statement of the lemma, we have \( \Pi \vdash \text{loc}.f : (u', \rho_1) \), where \( u' < u \). By the definitions of \textit{override} and \textit{findMeth}, \( \text{findMeth}(u', m) = (c_2, t, m (\forall v) \{ e_{n+1}, \rho_1 \}) \).

The result of \textit{typeOff} does not change, so the type of the expression is \( t \), by (T-CALL-OPEN-LOC):

\[ e = \text{loc}, f \quad \text{typeOff}(f) = (d, \emptyset) \]
\[ (c_1, t, m (\forall v) \{ e_{n+1}, \rho_1 \}) = \text{findMeth}(t', m) \quad \forall i \in \{1..n\} :: \Pi \vdash e_i : (t'_i, \rho'_i) \quad t'_i < t_i \]
\[ \Pi \vdash E_2[e] : (t, \{ \}) \]

It must be the case that \( e' = \text{loc}' \). From the statement of the lemma, we have \( \Pi \vdash \text{loc}'.f : (u', \rho_0) \), where \( u' < u \). By the definitions of \textit{override} and \textit{findMeth}, \( \text{findMeth}(u', m) = (c_2, t, m (\forall v) \{ e_{n+1}, \rho_1 \}) \).

Therefore, by (T-CALL), the type of the expression is \( t \).

\[ \text{Case } m(\pi) \quad \text{The last step for } E_2[e] \text{ could be} \]
\[ \Pi \vdash e : (t', \rho') \quad \text{typeOff}(f) = (d, \emptyset) \quad t'' < t \]
\[ \Pi \vdash E_2[e] : (t, \{ \}) \]

Now \( u' < u < t' \), so by (T-CALL), \( \Pi \vdash E_2[e'] : (t, \{ \}) \).

\[ \text{Case } f = e_2 \quad \text{The last step for } E_2[e] \text{ could be} \]
\[ \Pi \vdash e : (u, \rho_0) \quad \text{typeOff}(f) = (d, t) \quad u < d \]
\[ \Pi \vdash E_2[e] : (t, \{ \}) \]

Now \( u' < u < d \). The result of \textit{typeOff} does not change. Thus, by (T-SET), \( \Pi \vdash E_2[e'] : (t, \{ \rho' \}) \), or (T-SET-OPEN):

\[ e = \text{this}, f \quad \text{typeOff}(f) = (d, \emptyset) \]
\[ u < d \]
\[ \Pi \vdash e : (t, \{ \rho' \}) \]

The only possibility is that \( e' = \text{loc}, \) for some \( \text{loc} \). By the statement of this lemma \( \Pi \vdash e' : (u', \rho_1) \), where \( u' < u < d \). Thus by (T-SET-OPEN-LOC), the type is \( t \).

\[ \text{Case } f \quad \text{The last step for } E_2[e] \text{ could be} \]
\[ \Pi \vdash e : (c, \rho_1) \quad \text{typeOff}(f) = (d, t) \quad c < d \]
\[ \Pi \vdash E_2[e] : (t, \{ \}) \]

The result of \textit{typeOff} does not change. Thus, by (T-GET), \( \Pi \vdash E_2[e'] : (t', \rho_0) \), or (T-GET-OPEN):

\[ e = \text{this}, f \quad \text{typeOff}(f) = (d, \emptyset) \quad \Pi \vdash E_2[e] : (t, \{ \}) \]

Here \( e' \) must be \textit{loc}, for some \( \text{loc} \). By the statement \( \Pi \vdash \text{loc} : \{ e', \rho_0 \}, \) and \( c' < c \). The result of \textit{typeOff} does not change. Thus, by (T-GET-OPEN-LOC), \( \Pi \vdash E_2[e'] : (t, \{ \}) \).

THEOREM C.34. [Type preservation] \( \Pi \vdash \Sigma \), where \( \Sigma = \langle \{e,(\text{id}, I)\} + \psi, \mu \rangle \), \( \Sigma \vdash \langle \{e,(\text{id}, I)\} + \psi, \mu \rangle \), and \( \Pi \vdash e : (t, \rho) \), then there is some \( \Pi' \) and \( \rho' \) such that

(a) \( \mu' \approx \Pi' \) and \( \Pi' \vdash \psi' \), i.e. \( \Pi' \vdash \Sigma' \);
(b) \( \Pi' \vdash \Pi' \); and
(c) \( \Pi' \vdash e' : (t', \rho') \) and \( t' < t \).

Proof: The proof is by cases on the reduction step applied. We prove the first seven cases where the reduction takes only one task local step. Then, we prove the case for yielding controls to other tasks. For all the base cases (except for the \textit{fork}-parallel rule), the queue \( \psi \) does not change, so by Lemma C.33 (Environment extension) and Definition C.32 if \( \Pi \vdash \psi \), then \( \Pi \vdash \psi' \).

\[ \text{New Object} \quad \text{Here } e = \text{new } c [] \] and \( e' = \text{yield } \nu \text{ loc} \), where \( \text{loc} \not\in dom(\mu) \) and \( \mu' = \{ \text{loc} : \{e, f = \text{null} \} \} \).

Let \( \Pi' = \{ \text{loc} : \} \). We now show that \( \Pi' \not\approx \Pi \not\approx \Pi' \).

We now show that \( \Pi \vdash E[\text{yield } \nu] : (t', \rho') \) for some \( t', \rho' \). We have \( \Pi \vdash E[\text{loc}, f] : (t, \rho') \). The last step in this derivation must be (T-GET) or (T-GET-OPEN-LOC). By the first hypothesis of (T-GET), (T-GET-OPEN-LOC) and by (T-LOC), and by \( \Pi \vdash \mu, \) we have \( \Pi(\text{loc}) = u \). By the second hypothesis of (T-GET), \textit{typeOff}(f) = (c, s). By the second hypothesis of (T-GET-OPEN-LOC), \textit{typeOff}(f) = (c, \emptyset, s). Also by \( \Pi \vdash \mu, \) if \( (\mu(\nu) = u', F', E') \), then \( \Pi(\nu) = u' \) and \( u' < s < \omega \); otherwise \( \mu(\nu) = \text{null} \). In both cases, the type of \( \nu \) is subtype of \( s \), by Lemma C.33 (Replacement with subtyping), \( \Pi \vdash E[\text{yield } \nu] : (t', \rho') \).

\[ \text{Field Get} \quad \text{Here } e = \text{loc}, f = \text{yield } \nu, \] \( \text{loc} = \mu \not\in \{ \text{loc} : \} \).

\[ \Pi \vdash E[\text{loc}, f = \text{yield } \nu, \mu'] = \{ \text{loc} : \{e, f = \text{null} \} \} \] and \( \mu' = \{ \text{loc} : \{e, f = \text{null} \} \} \). Let \( \Pi' = \{ \text{loc} : \} \). We now show that \( \Pi' \not\approx \Pi' \).

For part (1) \( \Pi'(\text{loc}) = \) and \( \mu'(\text{loc}) = \{e, f = \text{null} \} \).

For part (2) \( \mu'(\text{loc}) = \{e, f = \text{null} \} \).

2012/7/21
well-typed. For part 1(c), \( \text{rng}(F \uplus (f \mapsto v)) \subseteq \text{rng}(F) \cup \{v\} \). Now since \( \text{loc}.f = v \) is well-typed, then \( v \in \text{dom}(\Pi) \) or \( v = \text{null} \). In the former case, by \( \Pi \models \mu \), then \( v \in \text{dom}(\mu) \). \( v \in \text{dom}(\mu) \) implies \( v \in \text{dom}(\mu') \). In either case \( \text{rng}(F) \cup \{v\} \subseteq \text{dom}(\mu') \cup \{\text{null}\} \). Part (1d) holds for all \( f \in \text{dom}(F) \), \( f = v \). Part (1d) holds vacuously for \( f = \text{null} \). Otherwise, \( (F \uplus (f \mapsto v))(f) = v \), and by (T-SET) or (T-SET-OPEN-LOC) and (T-LOC), \( \Pi(v) = \text{null} \), where fields(\( u \)) = (\( c, s' \)) and \( u < c \). Parts 2 holds since \( \text{dom}(\mu') = \text{dom}(\mu) \).

To see \( \Pi \vdash e' : (t, \rho) \), let \( \Pi \vdash \text{loc}.f = v : (s, \rho_0) \). By (T-SET) or (T-SET-OPEN-LOC), \( \Pi \vdash v : (s, \emptyset) \) and Lemma C.32 (Replacement), \( \Pi \vdash \text{yield } v : (t, \rho_1) \).

**Method Call** Here \( e = \text{E}[\text{loc}.m(\mu')], e' = \text{E}[\text{yield } e_1], \mu(\text{loc}) = [u.F.E]((\text{findMeth}(u,m) = (u',i,m[\text{var}])(e_2), \rho_0), \mu' = \mu \) and \( e_1 = \text{[this;}v, \text{var}]e_2 \). Let \( \Pi' = \Pi \). Clearly \( \Pi' \models \mu' \), and \( \Pi \vdash \Pi' \).

We now show that \( \Pi \vdash e' : (t', \rho') \) for some \( t' < t \) and some \( \rho' \). \( \Pi \vdash e : (t, \rho) \) implies that \( \text{loc}.m(\mu) \) and all its subterms are well-typed in \( \Pi \). By part 1(a) of \( \Pi \models \mu \), \( \Pi \vdash \text{loc}.(u, \emptyset) \). By the definition of findMeth, \( u < u' \). Let \( \Pi \vdash v : (u_0, \emptyset) \) \( \forall i \in \{1..n\} \) and let \( \Pi \vdash \text{loc}.m(\mu)(t_0, \rho_0) \). This last judgment must be \( (\text{T-CALL}) \), with \( (u_1, \mu_1, m[\text{var}])(e_2), \rho_0) = \text{findMeth}(u,m), \forall i \in \{1..n\} \) \( : u_i < t_i \). By the definition of the function findMeth, rules \( (\text{T-METHOD}) \) and \( \text{override}, (\text{VAR}: t, \text{this}: u') \vdash e_2 : (u_m, \rho_1) \), and \( u_m < t_m \).

By Lemma C.31 (Environment extension) (and appropriate alpha conversion of free variables in \( e_2 \)), \( \Pi \vdash \text{[this};v, \text{var}]e_2 : (u_m, \rho_1) \).

By Lemma C.30 (Substitution), \( \Pi \vdash \text{loc}.m(\mu')(\text{this};v, \text{var}]e_2 : (u_0', \rho_0) \), for some \( u_0' < u_0 \). Finally, Lemma C.33 (Replacement with subtyping) gives \( \Pi \vdash e' : (t', \rho') \) for some \( t' < t \).

**Local Declaration** In this case \( e = \text{E}[t \text{var} = v; e_1], e' = \text{E}[\text{yield } e_1] \), where \( e_1 = [v \text{var}]e_1 \) and \( \mu' = \mu \). Let \( \Pi = \Pi' \). Obviously \( \Pi' = \Pi' \), and \( \Pi \vdash \Pi' \). We show \( \Pi \vdash \text{yield } e_1 : (t', \rho') \) for some \( t' < t \). \( \Pi \vdash e : (t, \rho) \) implies that \( t \text{var} = v; e_1 \) and all its subterms are well typed in \( \Pi' \), let \( \Pi \vdash t \text{var} = v; e_1 : (s, \rho_0) \). By (T-DEFINE), \( \Pi \vdash v : (s, \rho_0) \).

By Lemma C.30 (Substitution), \( \Pi \vdash [v \text{var}]e_1 : (s', \rho_1) \), for some \( s' < s \). Finally, Lemma C.33 (Replacement with subtyping) gives \( \Pi \vdash e' : (t', \rho') \) for some \( t' < t \).

**Fork-Sequential** Here \( e = \text{E}[\text{fork}(e_2; e_3)], e' = \text{E}[\text{yield } e_0], \mu' = \mu \) and \( e_0 = e_2, e_3 = \text{null} \). Let \( \Pi = \Pi' \). Clearly \( \Pi' = \Pi' \), and \( \Pi \vdash \Pi' \).

We now show that \( \Pi \vdash e' : (t', \rho') \) for some \( t' < t \) and some \( \rho' \). By (T-FORK), \( \Pi \vdash \text{fork}(e_2; e_3) : (\text{void}, \rho_0) \). Because the expression is well type, \( e_2 \) and \( e_3 \) are well-typed. We know \( \Pi \vdash \text{null} : (\text{void}, \emptyset) \). By (T-SEQ), \( \Pi \vdash (\text{yield } e_0) : (u, \rho_1) \), for any valid type \( u \) and some \( \rho_1 \). Since the type of \( \text{null} \) is subtype of any type, Lemma C.33 (Replacement with subtyping) gives \( \Pi \vdash e' : (t', \rho') \) for some \( t' < t \).

Next, we show that \( \Pi \vdash \psi \). Because the expression is well type, \( e_2 \) and \( e_3 \) are well-typed.

**Yield** In this case, \( e = \text{E}[\text{yield } e_1], e' = \text{E}[e_1] \). There are two cases: (a) there is no reduction step happens for other tasks during this reduction; (b) there are reduction steps happen for other tasks during this reduction.

In the first case, \( \psi = \psi \) and \( \mu' = \mu \). Let \( \Pi = \Pi' \), then \( \Pi' = \Pi' \), \( \Pi \vdash \psi \), and \( \Pi \vdash \psi \). Let \( \Pi \vdash (\text{yield } e_1) : (t_0, \rho_0) \), then \( \Pi \vdash e_1 : (t_0, \rho_0) \), thus by Lemma C.32 (Replacement), \( \Pi \vdash e' : (t, \rho) \).