Modular Reasoning in the Presence of Event Subtyping

Mehdi Bagherzadeh$^{\alpha}$ Robert Dyer$^{\beta}$ Rex D. Fernando$^{\gamma}$ José Sánchez$^{\theta}$ Hridesh Rajan$^{\alpha}$

$^{\alpha}$Iowa State University, USA $^{\beta}$Bowling Green State University, USA $^{\gamma}$University of Wisconsin, USA $^{\theta}$University of Central Florida, USA

$^{\alpha}${mbagherz,hridesh}@iastate.edu $^{\beta}$rdyer@bgsu.edu $^{\gamma}$rex@cs.wisc.edu $^{\theta}$sanchez@eecs.ucf.edu

Abstract

Separating crosscutting concerns while preserving modular reasoning is challenging. Type-based interfaces (event types) separate modularized crosscutting concerns (observers) and traditional object-oriented concerns (subjects). Event types paired with event specifications were shown to be effective in enabling modular reasoning about subjects and observers. Similar to class subtyping, organizing event types into subtyping hierarchies is beneficial. However, unrelated behaviors of observers and their arbitrary execution orders could cause unique, somewhat counterintuitive, reasoning challenges in the presence of event subtyping. These challenges threaten both tractability of reasoning and reuse of event types. This work makes three contributions. First, we pose and explain these challenges. Second, we propose an event-based calculus to show how these challenges can be overcome. Finally, we present modular reasoning rules of our technique and show its applicability to other event-based techniques.

Categories and Subject Descriptors D.2.4 [*Software/Program Verification*]: Programming by contract, Assertion checkers; F.3.1 [*Specifying and Verifying and Reasoning about Programs*]: Assertions, Invariants, Pre- and post-conditions, Specification techniques

General Terms Design, Languages, Verification

Keywords Event subtyping, event type inheritance, modular reasoning, event specification refinement, translucid contracts

1. Introduction

Separation of crosscutting concerns has generated significant interest over the past decade or so [1–19]. An interesting challenge in separation of crosscutting concerns is to preserve modular reasoning and its underlying modular type checking. Recently some consensus has been formed that a notion of explicit interfaces between modularized crosscutting concerns and traditional object-oriented (OO) concerns enables modular type checking [10–15, 18–20], modular reasoning [2, 5–14] and design stability [21–23].

Previous work, such as join point types (JPT) [19], join point interfaces (JPI) [18] and Ptolemy's typed events [24], just to name a few, propose a type-based formulation of these interfaces to enable modular type checking. These type-based interfaces could be thought of as *event types* which are announced, implicitly or explicitly, by traditional OO concerns, or *subjects*, where modularized crosscutting concerns, or *observers*, register for the events and run upon their announcement [25, 26]. Announcement of an event type could cause *zero or more* of its observers to run in a chain where observers can invoke each other. This event announcement and handling model for separation of concerns has been popularized by AspectJ [1] and is different from models in which the subject is responsible for invoking all of its observers, as in Java's event model and the Observer pattern.

Similar to OO subtyping, where a class can subtype another class, an event type can subtype another event type. *Event subtyping* enables structuring of event types and allows for code reuse [18, 19, 24]. Code reuse allows *an observer of an event to run upon announcement of any of its subevents*, i.e. observer reuse, and makes the data attributes of the event accessible in its subevents, i.e. event inheritance. Modular type checking of subjects and observers in the presence of event subtyping has been explored [18, 19, 24].

Modular reasoning about subjects and observers, unlike their modular type checking, is focused on understanding their behaviors [5, 27], control effects [7, 9, 28], data effects [2, 29] and exception flows [8]. In modular reasoning, a system is understood one module at a time and in isolation using only its implementation and the interfaces, not implementations, of other modules it references [12, 13]. Previous work, such as crosscutting programming interfaces (XPI) [5], crosscutting programming interfaces with design rules (XPIDR) [28] and translucid contracts [7–9], enables modular reasoning about subjects and observers using *event specifications*, however, they do not support event subtyping.

Modular reasoning about behaviors of subjects and observers, using event specifications of event types that can subtype each other, where announcement of an event allows not only observers of the event but also observers of *all* of its superevents, with possibly *unrelated behaviors*, run in an *arbitrary order*, faces the following unique challenges:

- *Problem ❶ – Combinatorial reasoning*: unrelated behaviors of observers may require a factorial number of combinations of execution orders of observers of the event and observers of all of its superevents, up to $n!$ for n observers, to be considered in reasoning about the subject, which makes reasoning intractable;
- *Problem ❷ – Behavior invariance*: arbitrary execution orders of observers may force observers of the event and observers of all of its superevents to satisfy the same behavior, which prevents reuse of event types, their specifications and observers.

In this work, we solve problem *(1)* by imposing a novel *refining relation* among specifications of an event and its superevents, such that for each event in a subtyping hierarchy its greybox specification [30] refines both behaviors and control effects of the greybox specification of its superevent. Our refining relation is the inverse of the classical refining for blackbox specifications [31] and extends it to greybox specifications with control effect specifications. We solve problem *(2)* by imposing a *non-decreasing rela-*

MODULARITY'15, March 16–19, 2015, Fort Collins, CO, USA
Copyright 2015 ACM 978-1-4503-3249-1/15/03...$15.00
http://dx.doi.org/10.1145/2724525.2724569

tion on execution orders of observers of an event and observers of its superevents, such that for each event in a subtyping hierarchy observers of an event run before observers of its superevents. With the refining and non-decreasing relations combined, subjects and observers of an event could be understood modularly and in a tractable manner using only the specification of their event, independent of observers of the event, observers of its superevents and their execution orders, while allowing reuse. This is only sound when we impose a *conformance relation* on subjects and observers of an event such that each subject and observer of the event respects behaviors and control effects of their event specifications.

We illustrate problems *(1)–(2)* in the event-based language Ptolemy [24] by adding greybox event specifications to it, and propose our solution in the context of a new language design called *Ptolemy*$_{\mathbb{S}}$. The language *Ptolemy*$_{\mathbb{S}}$ has built-in support for the refining, non-decreasing and conformance relations that together enable modular reasoning about behaviors and control effects of subjects and observers. Our proposed solution could be applied to other event-based systems especially those with event announcement and handling models similar to AspectJ [1], including join point types [19] and join point interfaces [18].

Contributions We make the following contributions:

- identification and illustration of problems *(1)–(2)* of modular reasoning about subjects and observers, in the presence of event subtyping (Section 2);
- the refining relation for greybox event specifications, the non-decreasing relation for execution orders of observers and the conformance relation for behaviors and control effects of subjects and observers of an event hierarchy, to solve problems *(1)–(2)* and enable modular reasoning (Sections 3 and 4);
- *Ptolemy*$_{\mathbb{S}}$'s Hoare logic [32] for modular reasoning (Section 4);
- *Ptolemy*$_{\mathbb{S}}$, a language design and its sound semantics with support for the refining, non-decreasing and conformance relations;
- applicability of *Ptolemy*$_{\mathbb{S}}$'s reasoning to AspectJ-like event-based systems including join point types [19] (Section 5) and understanding control effects and interference (Section 6).

Implementation of *Ptolemy*$_{\mathbb{S}}$'s compiler is publicly available at *http://sf.net/p/ptolemyj/code/HEAD/tree/pyc/branches/event-inheritance/*. Section 7 discusses the implementation and limitations of our approach. Section 8 presents related work and Section 9 discusses future work and concludes.

Appendix Sections A and B discuss *Ptolemy*$_{\mathbb{S}}$'s static and dynamic semantics. Proofs for soundness of *Ptolemy*$_{\mathbb{S}}$'s Hoare logic and type system along with other details not included in this paper can be found in our technical report [33].

2. Problems

In this section we illustrate problems *(1)–(2)*, discussed in Section 1, using the event-based language Ptolemy [24].

As an example of modular reasoning about the behavior of a subject, consider *static* verification of the JML-like assertion Φ on line 8 of Figure 1. The assertion says that *the expression* `e` *and its state remain the same after announcement and handling of the event type* `AndEv`*, on lines 4–7*, where `AndEv` is a subevent of `BinEv` and `ExpEv`, in the event subtyping hierarchy of Figure 2. The assertion assumes that `e`, `e.left`, and `e.right` are not null. The method `equals` checks for equality of two objects and their states, e.g. two expressions of type `AndExp` are equal, if their object references, `parent`s and their `left` and `right` children are equal. The expression ***old*** refers to values of variables at the beginning of method

```
1  /* subject */
2  class ASTVisitor {
3   void visit(AndExp e) {
4    announce AndEv(e, e.left, e.right) {
5     e.left.accept(this);
6     e.right.accept(this);
7    }
8    assert e.equals(old(e)); Φ
9   }
10  void visit(TrueExp e) { announce TrueEv(e) {} } ..
11 }
```

Figure 1. Static verification of Φ in subject `ASTVisitor`.

```
12 /* event types */
13 void event ExpEv                 { Exp node; }
14 void event BinEv  extends ExpEv {
15  BinExp node; Exp left, right;
16 }
17 void event AndEv  extends BinEv { AndExp node; }
18 void event UnEv   extends ExpEv { UnExp node; }
19 void event TrueEv extends UnEv  { TrueExp node; }
20 /* data types */
21 class Exp {
22  Exp parent;
23  void accept(ASTVisitor v) { v.visit(this); }
24 }
25 class BinExp extends Exp    { Exp left, right; .. }
26 class AndExp extends BinExp { .. }
27 class UnExp  extends Exp    { .. }
28 class TruExp extends UnExp  { .. }
```

Figure 2. Event `AndEv` and its superevents `BinEv` and `ExpEv`.

`visit`, on line 3. To better understand the problems of modular reasoning, we first provide a short background on Ptolemy.

2.1 Ptolemy in a Nutshell

Ptolemy [24] is an extension of Java for separation of crosscutting concerns [15]. It has a unified model like Eos [16, 34–37] with support for event types, event subtyping and explicit announcement and handling of events. In Ptolemy, a subject announces an event and observers register for the event and run upon its announcement. Announcement of an event causes observers of the event and observers of its superevents to run in a chain according to their *dynamic registration order*, where observers can invoke each other.

Written in Ptolemy, Figures 1, 2 and 3 together show a simple expression language with a tracer, type checker and evaluator for boolean expressions such as `AndExp`, `OrExp` and numerical expressions. We focus on the code for boolean expressions, but the complete code can be found elsewhere[1]. A parser generates abstract syntax trees (AST) for expressions of the language and provides a visitor to visit these abstract syntax trees.

The subject `ASTVisitor`, in Figure 1, uses ***announce*** expressions to announce event types for each node type in the AST of an expression, upon its visit. For example, it announces the event type `AndEv` for visiting `AndExp`, on lines 4–7, with its event body on lines 5–6. Observers `Tracer`, `Checker` and `Evaluator`, in Figure 3, show interest in events and register to run upon their announcement. For example, `Evaluator` shows interest in `AndEv` using a ***when – do*** binding declaration, on line 59, and registers for it using a ***register*** expression, on line 53. `Evaluator` runs the observer handler method[2] `evalAndExp`, on lines 54–58, upon announcement of `AndEv`. The handler pops up values of the left and right children of

[1] *http://sf.net/p/ptolemyj/code/HEAD/tree/pyc/branches/event-inheritance/examples/100-Polymorphic-Expressions*

[2] Phrases 'observer' and 'observer handler method' are used interchangably.

the visited AndExp node from a value stack, conjoins them together to evaluate the value of the conjunct expression and pushes the result back to the stack. For a binary boolean expression, Checker ensures that its children are boolean expressions by popping and casting their boolean values from a type stack. Types Type and Value and their subtypes, e.g. Bool and BoolVal, denote types and values of boolean and numerical expressions.

```
29 /* observers */
30 class Tracer {
31  Tracer() { register(this); }
32  void printExp(ExpEv next) {
33   next.invoke();
34   logVisitEnd(next.node()); }
35  when ExpEv do printExp;
36 }
37 class Checker{
38  Stack<Type> typeStack = ..
39  Checker() { register(this); }
40  void checkBinExp (BinEv next) {
41   next.invoke();
42   Bool t1 = (Bool) typeStack.pop();
43   Bool t2 = (Bool) typeStack.pop();
44   typeStack.push(new Bool()); }
45  when BinEv do checkBinExp;
46  void checkUnExp(UnEv next) {
47   next.invoke();
48   typeStack.push(new Bool()); }
49  when UnEv do checkUnExp;
50 }
51 class Evaluator {
52  Stack<Value> valStack = ..
53  Evaluator() { register(this); }
54  void evalAndExp (AndEv next) {
55   next.invoke();
56   BoolVal b1 = (BoolVal) valStack.pop();
57   BoolVal b2 = (BoolVal) valStack.pop();
58   valStack.push(new BoolVal(b1.val && b2.val)); }
59  when AndEv do evalAndExp;
60  void evalTrueExp (TrueEv next) {
61   next.invoke();
62   valStack.push(new BoolVal(true)); }
63  when TrueEv do evalTrueExp; ..
64 }
```

Figure 3. Observers Tracer, Checker and Evaluator.

Announcement of AndEv, on lines 4–7, could cause the observer Evaluator of the event and observers Checker and Tracer of its superevents BinEv and ExpEv to run in a chain, if they are registered. An observer of an event is bound to the event through a binding declaration. For example, Evaluator is an observer of AndEv because of its binding declaration whereas Checker is not, though it may run upon announcement of AndEv. Observers are put in a chain of observers as they register for an event with the event body as the last observer. For example, the event body for AndEv is the last observer of the event in the chain. The chain of observers is stored inside an event closure represented by a variable ***next*** and the chain is passed to each observer handler method. For example, the chain is passed to evalAndExp on line 54. An observer of an event can invoke the next observer in the chain using an ***invoke*** expression which is similar to AspectJ's ***proceed***. Dynamic registration of observers allows observers to register in any arbitrary order which in turn means that an observer of an event can invoke another observer of the same event, an observer of any of its superevents or any of its subevents. For example, the observer Evaluator for the event AndEv can invoke, on line 55, another observer of AndEv or any of its superevents or subevents.

Event types must be declared before they are announced by subjects or handled by observers. An event declaration names a superevent in its ***extends*** clause and a set of context variables in its body. Context variables are shared data between subjects and observers of an event. An event inherits contexts of its superevents via event inheritance, can redeclare contexts of its superevents via depth subtyping or add to them via width subtyping. For example, the declaration of AndEv extends BinEv as its superevent, inherits its context variables left and right and redeclares its context node. The declaration of BinEv, on lines 14–16, adds contexts left and right, using width subtyping, to node that it inherits from its superevent ExpEv. Contexts left and right serve illustration purposes only, otherwise they could be projected from node. Values of context variables of an event are set upon its announcement and stored in its event closure. For example, the contexts node, left and right of AndEv are set with values e, e.left and e.right upon announcement of AndEv, on line 4.

2.1.1 Event Type Specifications

To verify Φ in Figure 1, the behavior of the announce expression for AndEv, on lines 4–7, must be understood, which in turn is dependent on behaviors of observers of AndEv and observers of its superevents, running upon its announcement. For such understanding to be modular, only the implementation of the subject ASTVisitor, on lines 2–11, and interfaces of modules it references, including the event types AndEv and its superevents BinEv and ExpEv, are available. However, neither ASTVisitor nor AndEv, BinEv or ExpEv say anything about the behaviors of their observers, which in turn makes modular verification of Φ difficult.

Previous work [7–9] proposes translucid contracts as event type specifications to specify behaviors and control effects of subjects and observers of an event and enables their modular reasoning in the *absence* of event subtyping. We add translucid contracts to Ptolemy's event types and illustrate how unrelated event specifications of events in a subtyping hierarchy and arbitrary execution of their observers could cause problems *(1)–(2)* in modular reasoning about subjects and observers in the *presence* of event subtyping.

In its original form [7], a translucid contract of an event is a greybox specification [30] that specifies behaviors and control effects of individual observers of the event, with *no relation* to behaviors and control effects of its superevents or subevents. Figure 4 shows translucid contracts of a few event types of Figure 2. The translucid contract of AndEv, on lines 20–26, specifies behavior and control effects of the observer Evaluator of AndEv and especially its observer handler method evalAndExp. The behavior of evalAndExp is specified using the precondition ***requires***, on line 20, and the postcondition ***ensures***, on line 26, which says that the execution of the observer starts in a state in which the context node, left and right are not null, i.e. $left != \textbf{null}$ && $right != \textbf{null}$ && $node\ != \textbf{null}$, and if the execution terminates it terminates in a state in which the node is the same as before the start of the execution of the observer, i.e. $node.equals(\textbf{old}\ (node))$.

Control effects of evalAndExp are specified by the ***assumes*** block, on lines 21–25, that limits its implementation structure. The assumes block is a combination of program and specification expressions. The program expression $\textbf{next}.\textbf{invoke}()$, on line 22, specifies and exposes control effects of interest, e.g. occurrence of the invoke expression in the implementation of evalAndExp, and the specification expression ***requires*** $\textbf{next}.node().left! = \textbf{null}$ && $\textbf{next}.node().right! = \textbf{null}$ ***ensures*** $\textbf{next}.node().parent == \textbf{old}\ (\textbf{next}.node().parent)$, on lines 23–24, hides the rest of the implementation of evalAndExp, allowing it to vary as long as it respects the specification. The assumes block of AndEv says that an observer evalAndExp of AndEv must invoke the next observer in the chain of observers, line 22, and then can do anything as long as it does not modify the parent field of the context variable node, on lines 23–24. The expression $\textbf{next}.node()$ in the contract retrieves the context node from the event closure ***next*** for AndEv and the expression ***old*** refers to values of variables before event announcement.

```
1  void event ExpEv { ..
2   requires node != null
3   assumes {
4    next.invoke();
5    requires true
6    ensures next.node().parent==old(next.node().parent);
7   }
8   ensures node.equals(old(node))
9  }
10 void event BinEv extends ExpEv { ..
11  requires left != null && right != null && node != null
12  assumes {
13   next.invoke();
14   requires
        next.node().left!=null&&next.node().right!=null
15   ensures next.node().parent==old(next.node().parent);
16  }
17 ensures true
18 }
19 void event AndEv extends BinEv { ..
20  requires left != null && right != null && node != null
21  assumes {
22   next.invoke();
23   requires
        next.node().left!=null&&next.node().right!=null
24   ensures next.node().parent==old(next.node().parent);
25  }
26  ensures node.equals(old(node))
27 }
```

Figure 4. Unrelated contracts of subtyping events.

Through the specification of behaviors of observers of an event, the translucid contract of an event also specifies the behavior of an invoke expression in the implementation of an observer of the event. This is true because in the absence of event subtyping the invoke expression causes the invocation of the next observer of the same event. For example, the contract of `AndEv` specifies the behavior of the invoke expression in the implementation of the observer handler method `evalAndExp` to have the precondition $left! = \textbf{\textit{null}}$ && $right! = \textbf{\textit{null}}$ && $node! = \textbf{\textit{null}}$ and the postcondition $node.equals(\textbf{\textit{old}}\ (node))$. The precondition of the invoke expression must hold right before its invocation and its postcondition must hold right after it.

2.2 Combinatorial Reasoning, Problem (1)

Various execution orders of observers of an event and observers of its superevents could yield different behaviors, especially if there is no relation between behaviors of observers of the event and its superevents and no known order on their execution. Combinatorial reasoning forces all such variations of execution orders to be considered in reasoning about a subject of an event, which makes the reasoning intractable [26].

To illustrate, reconsider static verification of Φ for announcement of `AndEv`, on lines 4–7 of Figure 1, with an observer instance `evaluator` registered to handle `AndEv` and an observer instance `checker` registered to handle `BinEv`. Translucid contracts of `AndEv` and `BinEv` in Figure 4 specify the behaviors of `evaluator` and `checker`, respectively. Announcement of `AndEv` could cause the observers `evaluator` and `checker` to run in two alternative execution orders χ_1: `evaluator` $\rightharpoonup$ `checker` or χ_2: `checker` $\rightharpoonup$ `evaluator`, depending on their dynamic registration order. In χ_1, `evaluator` runs first, where it invokes `checker` using its invoke expression, on line 55 of Figure 3, and the opposite happens in χ_2. Body of `AndEv` runs as the last observer in χ_1 and χ_2 (not shown).

For χ_1, the assertion Φ could be verified using the contract of `AndEv` for `evaluator`, on lines 20–26 of Figure 4, using its postcondition $node.equals(\textbf{\textit{old}}\ (node))$, on line 26. Recall that the precondition and postcondition of `AndEv` are the precondition and postcondition of its observer `evaluator`. To verify Φ, the postcondition of `AndEv` is copied right after the announce expression, using the copy rule [38], and its context variables `node`, `left` and `right` are replaced respectively with parameters `e`, `e.left` and `e.right` of the announce expression [7]. This allows use of the postcondition of the contract of `AndEv` in the scope of the method `visit`. Replacing the context variables in the postcondition of `AndEv` produces the predicate $e.equals(\textbf{\textit{old}}\ (e))$, which is exactly the assertion Φ that we wanted to prove.

In χ_1, the assertion Φ could be verified using the postcondition of the translucid contract of `AndEv` alone. An example of a more subtle interplay of behaviors of `evaluator` and `checker` is a scenario in which translucid contracts of `AndEv` and `BinEv` look like ***requires true assumes*** $\{$ ***establishes true***; $\textbf{\textit{next}}.\textbf{\textit{invoke}}();\}$ ***ensures true*** and ***requires true assumes*** $\{$***establishes*** $node.equals\ (\textbf{\textit{old}}\ (node))$; $\textbf{\textit{next}}.\textbf{\textit{invoke}}();\}$ ***ensures true***, respectively. The specification expression ***establishes*** q is a sugar for ***requires true ensures*** q. With these contracts, neither the postcondition of `AndEv` nor `BinEv` alone are enough to verify Φ, but their interplay results in a postcondition that implies and consequently verifies Φ.

In contrast, Φ cannot be statically verified for χ_2 because neither the postcondition ***true*** of the contract of `BinEv`, on line 17 of Figure 4, nor the interplay of behaviors of observers `evaluator` and `checker` in χ_2 provides the guarantees required by Φ.

As illustrated, in reasoning about a subject of an event, various execution orders of its observers and observers of its superevents must be considered. Generally for n observers of events in a subtyping hierarchy there can be up to $n!$ possible execution orders [8, 26] which in turn makes the reasoning intractable. Also, dependency of the reasoning on execution orders of observers *threatens the modularity* of the reasoning. This is because any changes in execution orders of observers could invalidate any previous reasoning. For example, the already verified assertion Φ for the execution order χ_1 is invalidated by changing the execution order to χ_2.

2.3 Behavior Invariance, Problem (2)

In reasoning about an observer of an event, arbitrary execution orders of observers of the event and observers of its superevents in a chain could force observers of the event and observers of all of its superevents in a subtyping hierarchy to satisfy the same behavior. This could prevent reuse of event types, their specifications [39] and their observers [18, 19].

To illustrate, consider reasoning about the behavior of the invoke expression in the observer `evaluator`, in Figure 3 line 55, with an observer instance `evaluator` registered to handle `AndEv` and observer instance `tracer` registered to handle its transitive superevent `ExpEv`. Translucid contracts of `AndEv` and `ExpEv` in Figure 4 specify behaviors of `evaluator` and `tracer`, respectively. Upon announcement of `AndEv`, observers `evaluator` and `tracer` could run in two alternative execution orders χ_1: `evaluator` $\rightharpoonup$ `tracer` or χ_2: `tracer` $\rightharpoonup$ `evaluator`.

Recall that the translucid contract of an event also specifies behaviors of invoke expressions in implementations of its observers. In other words, the contract of `AndEv` specifies the behavior of the invoke expression in its observer `evaluator`, on line 55. That is, the precondition $left! = \textbf{\textit{null}}$ && $right! = \textbf{\textit{null}}$ && $node! = \textbf{\textit{null}}$ of `AndEv` must hold right before the invoke expression in `evaluator` and the postcondition $node.equals(\textbf{\textit{old}}\ (node))$ must hold right after the invoke expression.

In χ_1, for the invoke expression of `evaluator` to invoke `tracer`, its precondition must imply the precondition $node! = \textbf{\textit{null}}$ of `tracer` and the postcondition $node.equals(\textbf{\textit{old}}\ (node))$ of `tracer` must imply the postcondition of the invoke expression in `evaluator`. In other words, χ_1 requires $\omega_1 : \mathscr{P}(\texttt{AndEv}) \Rightarrow \mathscr{P}(\texttt{ExpEv}) \wedge \mathscr{Q}(\texttt{ExpEv}) \Rightarrow \mathscr{Q}(\texttt{AndEv})$ to hold for `evaluator` to invoke `tracer`. Auxiliary functions $\mathscr{P}$ and $\mathscr{Q}$ return the precondition and postcondition of an event type, respectively. In contrast, χ_2 requires $\omega_2 : \mathscr{P}(\texttt{ExpEv}) \Rightarrow \mathscr{P}(\texttt{AndEv}) \wedge \mathscr{Q}(\texttt{AndEv}) \Rightarrow \mathscr{Q}(\texttt{ExpEv})$ to hold for `tracer` to invoke `evaluator`. To allow both execution orders χ_1 and χ_2, both conditions ω_1 and ω_2 must hold which in turn requires preconditions and postconditions of `AndEv` and `ExpEv` and consequently preconditions and postconditions of their observers `evaluator` and `tracer` to be the same, i.e. invariant.

3. Solution

To solve combinatorial reasoning and behavior invariance problems we propose to *(1)* relate behaviors of observers of an event and its superevent by a refining relation among greybox event specifications in an event subtyping hierarchy and to *(2)* limit arbitrary execution order of observers by a non-decreasing relation on execution orders of observers. This proposal constitutes a new language design called *Ptolemy*$_{\mathbb{S}}$ with support for these relations. Figure 5 shows an overview of these relations in *Ptolemy*$_{\mathbb{S}}$.

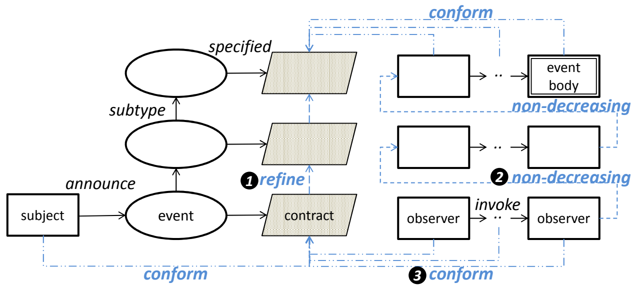

Figure 5. Refining, non-decreasing and conformance relations.

In Figure 5, for an event subtyping hierarchy, the refining relation guarantees that the specification (contract) of an event refines the specification of its superevent and the non-decreasing relation guarantees that upon announcement of an event by a subject, an observer of the event runs before an observer of its superevent. The conformance relation guarantees that each subject and observer of an event conform to and respect their event specification.

Detailed formalization of *Ptolemy*$_{\mathbb{S}}$'s sound static and dynamic semantics can be found in Sections A and B.

3.1 *Ptolemy*$_{\mathbb{S}}$'s Syntax

Figure 6 shows the expression-based core syntax of *Ptolemy*$_{\mathbb{S}}$ with focus on event types, event subtyping and event specifications. Hereafter, *term** means a sequence of zero or more terms and [*term*] means zero or one term.

A *Ptolemy*$_{\mathbb{S}}$ program is a set of declarations followed by an expression, which is like a call to the main method in Java. There are two kinds of declarations: class and event type declarations. A class can extend another class and it may have zero or more fields, methods and binding declarations.

Similarly, an event type declaration can extend (subtype) another event type and has a return type, a set of context variable declarations and an optional translucid contract. The return type of an event specifies the return type of its observers. An interesting property of return types of subtyping events is that, because of the non-decreasing relation, the return type of an event is a supertype of the return type of the event it extends, see Section B. An event type declaration inherits context variables of the event types it extends and can declare more through width subtyping. It can also redeclare the context variables of the event types it extends through depth subtyping [24], as long as the type of the redeclaring context is a subtype of the type of the redeclared context. Figure 2 illustrates the declaration of the event type `AndEv`, on line 17.

```
prog ::= decl* e
decl ::= class c extends d { form* meth* binding* }
       | c event ev extends ev′ { form* [contract] }
meth ::= t m (form*) { e }
binding ::= when ev do m
e, se ::= var | null | new c() | cast c e | if (e) {e} else {e}
       | e.m(e*) | e.f | e.f = e | form = e ; e
       | announce ev (e*) { e } | e.invoke()
       | register(e) | unregister(e)
       | refining spec { e } | spec | either {e} or {e}
p, q ::= var | p.f | p == p | p < p | ! p | p && p | old(p)
contract ::= requires p [assumes { se }] ensures q
spec ::= requires p ensures q
t ::= c | thunk ev
form ::= t var
```

$c,\ d$	$\in \mathscr{C} \cup \{\textbf{\textit{Object}}\}$	set of class names
$ev,\ ev'$	$\in \mathscr{E} \cup \{\textbf{\textit{Event}}\}$	set of event names
f	$\in \mathscr{F}$	set of field names
var	$\in \mathscr{V} \cup \{\textbf{\textit{this}}, \textbf{\textit{next}}\}$	set of variable names

Figure 6. *Ptolemy*$_{\mathbb{S}}$'s core syntax, based on [7, 15, 24].

3.2 Refining Relation of Event Specifications

Ptolemy$_{\mathbb{S}}$ relates behaviors and control effects of observers of events in a subtyping hierarchy by relating their greybox event specifications through a refinement relation $\trianglelefteq$. In the refining relation, the specification of an event refines the specification of its superevent, for both behaviors and control effects. *Ptolemy*$_{\mathbb{S}}$'s refinement among greybox event specifications is the inverse of classical behavioral subtyping for blackbox method specifications [31], however, blackbox specifications do not specify control effects.

In *Ptolemy*$_{\mathbb{S}}$, a translucid contract [7, 8] of an event is a greybox specification that, *in relation* to its superevents, specifies behaviors and control effects of individual observers of the event and their invoke expressions. A translucid contract of an event specifies behaviors using the precondition ***requires*** and the postcondition ***ensures***. The behavior ***requires*** *p* ***ensures*** *q* says that if the execution of an observer of the event starts in state σ satisfying p, written as $\sigma \models p$, and it terminates normally, it terminates in a state σ' that satisfies q, i.e. $\sigma' \models q$.

A translucid contract specifies control effects of its individual observers using its ***assumes*** block. An assumes block is a combination of program and specification expressions. A program expression exposes control effects of interest, e.g. invoke expressions, in the implementation of an observer whereas a specification expression *spec* hides the rest of its implementation allowing it to vary as long it respects its specification. The contract of an event only names the context variables of the event and must expose invoke expressions in the implementation of its observers. Figure 4 illustrates the translucid contract of `AndEv`, on lines 20–26, with its precondition, on line 20, postcondition, on line 26, program expression, on line 22 and specification expression, on lines 23–24. *Ptolemy*$_{\mathbb{S}}$ relates translucid contracts of an event and its superevents through the refining relation $\trianglelefteq$.

DEFINITION 3.1. ***(refining translucid contracts)****. For event types ev and ev', where ev is a subevent of ev', written as $ev \lll: ev'$*[3]*, and their respective translucid contracts $\mathscr{G} = ($ **requires** p **assumes** $\{se\}$ **ensures** $q)$ and $\mathscr{G}' = ($ **requires** p' **assumes** $\{se'\}$ **ensures** $q')$, $\mathscr{G}'$ is refined by $\mathscr{G}$, written as $\mathscr{G}' \trianglelefteq \mathscr{G}$, if and only if:*

(i). ***requires*** p' ***ensures*** q' $\trianglelefteq$ ***requires*** p ***ensures*** q
(ii). $se' \trianglelefteq se$

Figure 7 defines the refinement relation $\trianglelefteq$ for Ptolemy$_{\mathbb{S}}$ expressions.

[3] The class subtyping relation $\preccurlyeq$ is different from *Ptolemy*$_{\mathbb{S}}$'s event subtyping relation $\lll:$, as discussed in Section B.

Event specification refinement relation: $\boxed{\Gamma \vdash se' \trianglelefteq se}$

(R-SPEC)

$$\frac{spec = \textbf{\textit{requires}}\ p\ \textbf{\textit{ensures}}\ q \qquad spec' = \textbf{\textit{requires}}\ p'\ \textbf{\textit{ensures}}\ q' \qquad p \Rightarrow p' \qquad q' \Rightarrow q}{\Gamma \vdash spec' \trianglelefteq spec}$$

(R-INVOKE)

$$\frac{\Gamma \vdash se' \trianglelefteq se}{\Gamma \vdash se'.\textbf{\textit{invoke}}() \trianglelefteq se.\textbf{\textit{invoke}}()}$$

(R-VAR)

$$\frac{textualMatch(var', var)}{\Gamma \vdash var' \trianglelefteq var}$$

(R-DEFINE)

$$\frac{\Gamma \vdash se_1' \trianglelefteq se_1 \qquad \Gamma, t : var \vdash se_2' \trianglelefteq se_2}{\Gamma \vdash t\ var = se_1'; se_2' \trianglelefteq t\ var = se_1; se_2}$$

(R-IF)

$$\frac{\Gamma \vdash sp' \trianglelefteq sp \qquad \Gamma \vdash se_1' \trianglelefteq se_1 \qquad \Gamma \vdash se_2' \trianglelefteq se_2}{\Gamma \vdash \textbf{\textit{if}}(sp')\{se_1'\}\ \textbf{\textit{else}}\{se_2'\} \trianglelefteq \textbf{\textit{if}}(sp)\{se_1\}\ \textbf{\textit{else}}\{se_2\}}$$

Figure 7. Select rules for the refining relation $\trianglelefteq$.

In Definition 3.1, for a translucid contract of an event to refine the contract of its superevent, *(i)* its behavior must refine the behavior of the contract of the superevent and *(ii)* its assumes block must refine the assumes block of the translucid contract of its superevent.

In Figure 7, the rule (R-SPEC) shows the refinement of the behavior $spec' = \textbf{\textit{requires}}\ p'\ \textbf{\textit{ensures}}\ q'$ by the behavior $spec = \textbf{\textit{requires}}\ p\ \textbf{\textit{ensures}}\ q$. For the behavior *spec* to refine $spec'$, its precondition p must imply the precondition p', i.e. $p \Rightarrow p'$, and the opposite must be true for their postconditions, i.e. $q' \Rightarrow q$. That is the subevent can *strengthen* the precondition of its superevent and *weaken* its postcondition which is the inverse of classical refinement in class subtyping [31] where a subclass weakens the precondition of its superclass and strengthens its postcondition. Such inverse relation of behaviors is necessary in *Ptolemy*$_{\mathbb{S}}$ to allow an observer of a superevent to run upon announcement of its subevents. Also unlike *Ptolemy*$_{\mathbb{S}}$'s refining, the classical refining is for blackbox contracts and does not directly apply to greybox translucid contracts [30] and especially their assumes block [40] with control effect specifications.

The assumes block *se* of the translucid contract of an event refines the assumes block se' of the contract of its superevent, i.e. $se' \trianglelefteq se$, if: *(a)* each specification expression in *se* refines its *corresponding* specification expression in se' and *(b)* each program expression in *se* refines its corresponding program expression in *se*. The rule (R-SPEC) for refinement of behaviors also applies for refinement of specification expressions since they similarly are behavior specifications with a precondition and postcondition [40]. A specification expression in a subevent can strengthen the precondition of its corresponding specification expression in its superevent and weaken its postcondition. For a program expression to refine another program expression, they must textually match. The rule (R-VAR) checks for textual matching of variable names using the auxiliary function *textualMatch*. For other program expressions, such as invoke and conditional, their refinement boils down to the refinement of their subexpressions, as in rules (R-INVOKE), (R-DEFINE) and (R-IF).

To illustrate, the translucid contract of `AndEv`, on lines 20–26 in Figure 4, refines the contract of `ExpEv`, on lines 2–8. This is because *(i)* the precondition $left != \textbf{\textit{null}}\ \&\&\ right != \textbf{\textit{null}}\ \&\&\ node != \textbf{\textit{null}}$ of `AndEv` implies the precondition $node != \textbf{\textit{null}}$ of `ExpEv` and the postcondition $node.equals(\textbf{\textit{old}}\ (node))$ of `ExpEv` implies the same postcondition of `AndEv`, and thus using the rule (R-SPEC) the behavior of `AndEv` refines the behavior of `ExpEv`; *(ii)* the program expression $\textbf{\textit{next}}.\textbf{\textit{invoke}}()$ of `AndEv`, on line 22, refines its corresponding program expression of `ExpEv`, on line 4, using (R-INVOKE) and (R-VAR), and specification expression $\textbf{\textit{requires}}\ \textbf{\textit{next}}.node().left == \textbf{\textit{old}}\ (\textbf{\textit{next}}.node().left)\ \&\&\ \textbf{\textit{next}}.node().right == \textbf{\textit{old}}\ (\textbf{\textit{next}}.node().right)\ \textbf{\textit{ensures}}\ \textbf{\textit{next}}.node().parent == \textbf{\textit{old}}\ (\textbf{\textit{next}}.node().parent)$ of `AndEv`, on lines 23–24, refines its corresponding specification expression $\textbf{\textit{requires}}\ \textbf{\textit{true}}\ \textbf{\textit{ensures}}\ \textbf{\textit{next}}.node().parent == \textbf{\textit{old}}\ (\textbf{\textit{next}}.node().parent)$ in `ExpEv`, on lines 5–6, using (R-SPEC).

However, the translucid contract of `AndEv` does not refine the contract of `BinEv`, on lines 11–17, because the postcondition ***true*** of `BinEv` does not imply the postcondition of `AndEv`. Changing the postcondition of `BinEv` to $\textbf{\textit{next}}.node().parent == \textbf{\textit{old}}\ (\textbf{\textit{next}}.node().parent)$ makes the contract of `BinEv` refine the contract of `ExpEv`.

Textual matching of program expressions is a simpler alternative to complex higher order logic or trace verification techniques with its tradeoffs [40]. Textual matching works because *Ptolemy*$_{\mathbb{S}}$'s semantics enforces depth subtyping, ensuring that a redeclaring context variable in an event is a subtype of the redeclared context in its superevents and a ***next*** variable in the contract of an event is a subtype of the next variable in the contract of its superevent.

The refining relation $\trianglelefteq$ defines the refinement for corresponding program and specification expressions. That is, only *structurally similar* contracts may refine each other. Two translucid contracts are structurally similar if for each specification (program) expression in the assumes block of one, a possibly different specification (program) expression exists in the assumes block of the other at the same location. *Ptolemy*$_{\mathbb{S}}$'s structural similarity for the refining relation allows definition of *Ptolemy*$_{\mathbb{S}}$'s event specification inheritance, see our technical report [33], such that it statically guarantees the refining relation by combining translucid contracts of an event and its superevents in a subtyping hierarchy.

3.3 Non-Decreasing Relation of Observers' Execution

Ptolemy$_{\mathbb{S}}$ limits the arbitrary execution order of observers of an event and its superevents by enforcing a non-decreasing relation on execution orders of observers. In the non-decreasing order , an observer of an event runs before an observer of its superevent. *Ptolemy*$_{\mathbb{S}}$'s semantics for ***announce***, ***invoke***, ***register*** and ***unregister*** expressions and the relation of return types of events in an event hierarchy guarantee the non-decreasing order.

In *Ptolemy*$_{\mathbb{S}}$, a subject announces an event *ev* using the announce expression $\textbf{\textit{announce}}\ ev(e*)\{e'\}$. The announce expression evaluates parameters $e*$ to values $v*$, creates an event closure for the event *ev* and binds values $v*$ to context variables of *ev* in the closure. The announce expression also creates, in the event closure, a chain containing registered observers of *ev* and observers of *all its superevents* and runs the first observer in the chain. To construct the chain, the announce expression adds observers of the event *ev* to an empty chain followed by adding observers of the direct superevent of *ev* and recursively continues until it reaches the root event ***Event***[4]. The event body e' is added to the end of the chain.

By construction, the announce expression ensures that an observer of an event shows up before an observer of its superevent in the chain, which basically is the non-decreasing order of observers. Observers of the same event in the chain *maintain* among themselves the same order as their dynamic registration order, i.e. an observer registered earlier shows up in the chain before the ones registered later. This makes *Ptolemy*$_{\mathbb{S}}$ backward compatible with its earlier versions [7, 8, 15] that do not support event subtyping. The expression ***next*** is a placeholder for an event closure and the type ***thunk*** *ev* is the type of the event closure of an event *ev*.

[4] ***Event*** is not accessible to programmers and does not have observers, as a simple design choice, to not allow programmers to affect behaviors of events of a system by defining a specification for ***Event***.

After construction of the chain and running the first observer in the chain, by the announce expression, observers in the chain can invoke each other using an invoke expression $e.\textbf{\textit{invoke}}()$. The invoke expression evaluates e to an event closure containing the chain of observers and runs the next observer in the chain, which is according to the non-decreasing order. For observers to run in the non-decreasing order, the return type of an observer of an event must be a supertype of the return type of the observers of its superevent. *Ptolemy*$_{\mathbb{S}}$'s static semantics, in Section B, guarantees this by ensuring that the return type of an event is a supertype of the return type of its superevent.

Upon announcement of an event, only registered observers of the event and its superevents run. In *Ptolemy*$_{\mathbb{S}}$, observers show interest in events through binding declarations and register to handle the events. A binding declaration ***when*** *ev* ***do*** *m* in an observer says to run the observer handler method *m* when an event of type *ev* is announced. The expression $\textbf{\textit{register}}(e)$ evaluates e to an object and adds it to the list of observers $A[ev]$ for each event type *ev* that is named in binding declarations of the observer, and $\textbf{\textit{unregister}}(e)$ removes the object e from the list of observers of those events. The announce expression for an event *ev* recursively concatenates the list of observers $A[ev]$ of the event *ev* and the list of observers of its superevents to construct the chain of observers.

3.4 Refining + Non-decreasing Relations

Any of refining or non-decreasing relations alone cannot solve both combinatorial reasoning and behavior invariance problems. With the refining relation alone, because of the arbitrary execution order of observers, still up to $n!$ possible execution orders of n observers of the event and observers of its superevents should be considered in reasoning, which threatens its tractability; changes in execution orders of observers of the event or observers of its superevents can still invalidate any previous reasoning, which threatens modularity of reasoning; and observers of events in a subtyping hierarchy still could be forced to satisfy the same behavior, which threatens reuse. A trivial refining relation in which events of a hierarchy satisfy the same behavior enables modular reasoning, however, it is undesirable as it prevents reuse of event types, their specifications [39] and observers [18, 19].

With the non-decreasing relation alone, because of unrelated behaviors of observers, observers of events in a subtyping hierarchy may still be forced to satisfy the same behavior and any changes in behaviors of superevents of an event could invalidate any previous reasoning about subjects and observers of the event.

Interestingly, reversing both refining and non-decreasing relations still allows modular reasoning. To reverse these relations, the translucid contract of a superevent refines the contract of its subevent and an observer of a superevent runs before any observer of its subevent. We chose the current design, as it seemed more natural, to us, for observers of an already announced event to run before observers of its superevents.

4. Modular Reasoning

This section formalizes *Ptolemy*$_{\mathbb{S}}$'s Hoare logic for modular reasoning, its conformance relation for subjects and observers and soundness of its reasoning technique.

Ptolemy$_{\mathbb{S}}$'s refining and non-decreasing relations enable its modular reasoning about subjects and observers of an event, as shown in Figure 8. The main idea is to use the translucid contract of an event as a sound approximation of the behaviors of its observers and observers of its superevents to reason about:

(1) a subject of the event, especially its ***announce*** expression, independent of its observers and observers of its superevents and their execution orders; and

(2) an observer of the event, especially its ***invoke*** expressions, independent of its subjects as well as observers it may invoke and their execution orders.

reasoning judgement: $\boxed{\Gamma \vdash \{p\}\ e\ \{q\}}$

(V-ANNOUNCE)
$$\frac{\begin{array}{c}(c\ \textbf{\textit{event}}\ ev\ \textbf{\textit{extends}}\ ev'\{(t\ var)^*\ contract\}) \in CT\\ contract = \textbf{\textit{requires}}\ p\ \textbf{\textit{assumes}}\ \{se\}\ \textbf{\textit{ensures}}\ q\\ topContract(ev) = \textbf{\textit{requires}}\ p'\ \textbf{\textit{assumes}}\ \{se'\}\ \textbf{\textit{ensures}}\ q'\\ \Gamma \vdash \{p'[e^*/var^*]\}\ e'\ \{q'[e^*/var^*]\}\end{array}}{\Gamma \vdash \{p[e^*/var^*]\}\ \textbf{\textit{announce}}\, ev(e^*)\ \{e'\}\ \{q[e^*/var^*]\}}$$

(V-INVOKE)
$$\frac{\begin{array}{c}\textbf{\textit{thunk}}\ ev = \Gamma(\textbf{\textit{next}})\\ (c\ \textbf{\textit{event}}\ ev\ \textbf{\textit{extends}}\ ev'\{form^*\ contract\}) \in CT\\ contract = \textbf{\textit{requires}}\ p\ \textbf{\textit{assumes}}\ \{se\}\ \textbf{\textit{ensures}}\ q\end{array}}{\Gamma \vdash \{p\}\ \textbf{\textit{next}}.\textbf{\textit{invoke}}()\ \{q\}}$$

(V-REFINING)
$$\frac{\Gamma \vdash \{p\}\ e\ \{q\}}{\Gamma \vdash \{p\}\ (\textbf{\textit{refining}}\ \ \textbf{\textit{requires}}\ p\ \textbf{\textit{ensures}}\ q\ \{\ e\ \})\ \{q\}}$$

(V-SPEC)
$$\Gamma \vdash \{p\}\ \textbf{\textit{requires}}\ p\ \textbf{\textit{ensures}}\ q\ \{q\}$$

(V-CONSEQ)
$$\frac{p \Rightarrow p' \qquad q' \Rightarrow q \qquad \{p'\}\ e\ \{q'\}}{\Gamma \vdash \{p\}\ e\ \{q\}}$$

Figure 8. Select reasoning rules in *Ptolemy*$_{\mathbb{S}}$'s Hoare [32] logic, inspired by [9, 40].

Figure 8 shows *Ptolemy*$_{\mathbb{S}}$'s Hoare logic [32] for modular reasoning about behaviors of subjects and observers. *Ptolemy*$_{\mathbb{S}}$'s reasoning rules use a reasoning judgement of the form $\Gamma \vdash \{p\}\ e\ \{q\}$ that says the Hoare triple $\{p\}\ e\ \{q\}$ is provable using the variable typing environment Γ, which maps variables to their types. The judgement $\Gamma \vdash \{p\}\ e\ \{q\}$ is valid, written as $\Gamma \models \{p\}\ e\ \{q\}$, if for every state σ that agrees with type environment Γ, if p is true in σ, i.e. $\sigma \models p$, and if the execution of e terminates in a state σ', then $\sigma' \models q$. This definition of validity is for partial correctness where termination is not guaranteed. *Ptolemy*$_{\mathbb{S}}$'s reasoning rules use a fixed class table *CT*, which is a set of the program's class and event type declarations. The notation $ep[e^*/var^*]$ denotes replacing variables var^* with e^* in the expression ep. *Ptolemy*$_{\mathbb{S}}$'s rules for reasoning about standard object-oriented expressions remain the same as in previous work [32, 40–42] and are omitted.

In Figure 8, the rule (V-ANNOUNCE) reasons about the behavior of an announce expression in a subject. The rule says that the behavior of an announce expression announcing an event *ev* is the behavior ***requires*** *p* ***ensures*** *q* of the translucid *contract* of the event *ev*. To use the precondition *p* of the contract and its postcondition *q* in the scope of the announce expression, their context variables var^* are replaced by arguments e^* of the announce expression [38]. The rule (V-ANNOUNCE) does not require and is independent of any knowledge of individual observers of *ev* or observers of its superevents, their implementations or execution orders which in turn makes it modular and tractable.

To illustrate (V-ANNOUNCE), reconsider verification of the assertion Φ for the announce expression of `AndEv`, on lines 4–7 of Figure 1. Using the translucid contract of `AndEv`, on lines 20–26, the conclusion of (V-ANNOUNCE) replaces parameters `e`, `e.left` and `e.right` of the announce expression for context variables of `node`, `left` and `right` of `AndEv` in the precondition and postcondition of the contract of `AndEv` and yields the Hoare triple:

$$\begin{array}{l}\Gamma \vdash \{e.left! = \textbf{\textit{null}}\ \&\&\ e.right! = \textbf{\textit{null}}\ \&\&\ e! = \textbf{\textit{null}}\}\\ \qquad \textbf{\textit{announce}}\ AndEv(e,\ e.left,\ e.right)\\ \qquad\quad \{e.left.accept(\textbf{\textit{this}});\ e.right.accept(\textbf{\textit{this}});\}\\ \qquad \{e.equals(\textbf{\textit{old}}\ (e))\}\end{array}$$

The above judgement says, if `e`, `e.left` and `e.right` are not null, the expression e and its state remain the same after announcement and handling of `AndEv`, i.e. $e.equals(\textbf{\textit{old}}\ (e))$, which is exactly the assertion Φ we wanted to verify.

The rule (V-INVOKE) reasons about the behavior of an invoke expression, in an observer. The rule says that the behavior of an invoke expression in an observer of the event *ev*, is the behavior of the translucid *contract* of *ev*. The type of the event that the observer handles, i.e. *ev*, is part of the type of the event closure ***next***. The function $\Gamma(\textbf{\textit{next}})$ returns the type of the ***next*** expression in the typing environment Γ. Recall that the event closure next is passed as a parameter to each observer handler method. Again, the rule (V-INVOKE) does not require and is independent of any knowledge about subjects of the event *ev* or observers it may invoke in the chain of observer ***next*** and thus is modular and tractable.

The rule (V-REFINING) says that the behavior of the body e of a refining expression is the behavior of its specification expression ***requires*** p ***ensures*** q. This is true, because the body of the refining expression claims to refine its specification. The rule (V-SPEC) is straightforward [40] and the rule (V-CONSEQ) is standard [32].

4.1 Soundness of Reasoning

In *Ptolemy*$_{\mathbb{S}}$'s the translucid contract of an event is a sound approximation of behaviors of its subjects and observers independent of observers of the event, observers of its superevents and their execution orders. This is sound because of the following:

1. conformance of each observer and subject of an event to the translucid contract of the event; and
2. refining relation among specifications of the event and its superevents; and
3. non-decreasing relation on execution orders of observers of the event and observers of its superevents.

For a greybox translucid contract of an event, *all* subjects and observers of the event must conform to the contract of the event. This is different from a blackbox method specification, e.g. in JML, in which only a single method has to respect a contract [8, 31]. *Ptolemy*$_{\mathbb{S}}$'s semantics, in Sections A and B, guarantees the conformance using a combination of type checking and runtime assertion checking. *Ptolemy*$_{\mathbb{S}}$'s event specification inheritance [33], statically guarantees the refining relation and *Ptolemy*$_{\mathbb{S}}$'s dynamic semantics guarantees the non-decreasing relation. Figure 5 shows the interplay of conformance, refining and non-decreasing relations.

4.1.1 Conforming Observers

DEFINITION 4.1. *(Conforming observer) For an event type ev with a translucid contract* $\mathscr{G} = (\textbf{\textit{requires}}\ p\ \textbf{\textit{assumes}}\ \{se\}\ \textbf{\textit{ensures}}\ q)$*, its observer handler method m with its implementation e is conforming if and only if there exists a typing environment* Γ *such that:*

(i). $\Gamma \models \{p\}\ e\ \{q\}$

(ii). $se \sqsubseteq_s e$

where Figure 9 defines the structural refinement relation $\sqsubseteq_s$ *between the assumes block se and the body e of its observer.*

Definition 4.1 says that for an observer handler method of an event *ev* to be conforming, its implementation e must satisfy the precondition p and postcondition q of the translucid contract of the event, i.e. requirement *(i)*. An expression e satisfies a precondition p and a postcondition q in a typing environment Γ, written as $\Gamma \models \{p\}\ e\ \{q\}$, if and only if for every program state σ that agrees with the type environment Γ, if the precondition p is true in σ, and if the execution of e terminates in a state σ', then q is true in σ'. Currently *Ptolemy*$_{\mathbb{S}}$ uses runtime assertions to check for satisfaction of preconditions and postconditions of a contract by its observers. Static verification techniques could also be used to check for such satisfaction [9]. Figure 10 shows the conforming observer `Evaluator` and its observer handler method `evalAndExp`, on lines 21–32. In `evalAndExp`, assertions on lines 22 and 31 check for preconditions and postconditions of the contract of `AndEv` on lines 2 and 8.

Structural refinement relation: $\boxed{\Gamma \vdash se \sqsubseteq_s e}$

(S-REFINING)
$$\Gamma \vdash spec\ \sqsubseteq_s\ \textbf{\textit{refining}}\ spec\ \{e\}$$

(S-INVOKE)
$$\frac{\Gamma \vdash se \sqsubseteq_s e}{\Gamma \vdash se.\textbf{\textit{invoke}}() \sqsubseteq_s e.\textbf{\textit{invoke}}()}$$

(S-VAR)
$$\frac{textualMatch(var', var)}{\Gamma \vdash var' \sqsubseteq_s var}$$

(S-ANNOUNCE)
$$\frac{\Gamma \vdash se{*} \sqsubseteq_s e{*} \qquad \Gamma \vdash se \sqsubseteq_s e}{\Gamma \vdash \textbf{\textit{announce}}\ ev(se{*})\{se\}\ \sqsubseteq_s\ \textbf{\textit{announce}}\ ev(e{*})\{e\}}$$

(S-EITHEROR)
$$\frac{\Gamma \vdash se_1 \sqsubseteq_s e \vee \Gamma \vdash se_2 \sqsubseteq_s e}{\Gamma \vdash \textbf{\textit{either}}\ \{se_1\}\ \textbf{\textit{or}}\ \{se_2\}\ \sqsubseteq_s\ e}$$

(S-DEFINE)
$$\frac{\Gamma \vdash se_1 \sqsubseteq_s e_1 \qquad \Gamma, var : t \vdash se_2 \sqsubseteq_s e_2}{\Gamma \vdash t\ var = se_1; se_2 \sqsubseteq_s\ t\ var = e_1; e_2}$$

(S-IF)
$$\frac{\Gamma \vdash sp \sqsubseteq_s ep \qquad \Gamma \vdash se_1 \sqsubseteq_s e_1 \qquad \Gamma \vdash se_2 \sqsubseteq_s e_2}{\Gamma \vdash \textbf{\textit{if}}(sp)\{se_1\}\ \textbf{\textit{else}}\{se_2\} \sqsubseteq_s \textbf{\textit{if}}(ep)\{e_1\}\ \textbf{\textit{else}}\{e_2\}}$$

Figure 9. Select rules for structural refinement $\sqsubseteq_s$ [7, 40].

Definition 4.1 also requires the implementation e of a conforming observer to structurally refine the assumes block *se* of its translucid contract, i.e. requirement *(ii)*. The structural refinement $\sqsubseteq_s$ guarantees that an observer of an event, in its implementation has the control effects exposed in its translucid contract [7, 8] using its program expressions. Figure 9 shows select rules for *Ptolemy*$_{\mathbb{S}}$'s structural refinement.

The implementation e of an observer handler method structurally refines the assumes block *se* of its translucid contract if: *(a)* for each specification expression *spec* in *se* there is a corresponding ***refining*** expression in e with the same specification and *(b)* for each program expression in *se*, there is a corresponding textually matching program expression in e. The rule (S-REFINING) checks for structural refinement of a specification expression by a refining expression. (S-VAR) checks for textual matching of variable names using the auxiliary function *textualMatch*. For other program expressions, structural refinement boils down to structural refinement of their subexpressions. The rule (S-EITHEROR) allows an observer to choose between behaviors in its either-branch or its or-branch. Similar to the refining relation, structural refinement requires structural similarity between the implementation of a conforming observer and the assumes block of its contract.

In Figure 10, the assumes block, on lines 3–7, is structurally refined by the implementation of the conforming observer `evalAndExp`, on lines 22–31 (ignoring runtime assertion checks), because the program expression $\textbf{\textit{next.invoke}}()$ on line 4 is structurally refined by the program expression in the implementation on line 23 and the specification expression on lines 5–6 is refined by a refining expression with the same specification on lines 25–29. Structural refinement guarantees that the implementation of `evalAndExp` has a $\textbf{\textit{next.invoke}}()$ expression as its control effect, as specified by the program expression $\textbf{\textit{next.invoke}}()$ in its contract.

A refining expression claims that its body satisfies its specification. *Ptolemy*$_{\mathbb{S}}$ uses runtime assertions to check this claim. In Figure 10, runtime checks on lines 24 and 30 check that the body of the refining expression satisfies its precondition and postcondition on lines 26 and 27.

Though similar, in the structural refinement $\sqsubseteq_s$ the implementation of an observer refines the assumes block of the translucid contract of its event, whereas in the refining relation $\trianglelefteq$ the contract of an event refines the contract of its superevent. A specification expression in a contract is structurally refined by a refining expression in $\sqsubseteq_s$ whereas it is refined by another specification expression in $\trianglelefteq$.

4.1.2 Conforming Subjects

DEFINITION 4.2. *(Conforming subject) For an event type ev with a translucid contract $\mathscr{G} = ($**requires** p **assumes** $\{se\}$ **ensures** $q)$, its subject with an announce expression **announce** $ev(e^*)\{e'\}$ in its implementation, is conforming if and only if:*
$\Gamma \models \{p'\}\ e'\ \{q'\}$ *where* **requires** p' **assumes** $\{se'\}$ **ensures** $q' = topContract(ev)$

The definition says that for a subject of *ev* to be conforming its event body e' must satisfy the precondition p' and postcondition q' of the translucid contract of the event on top of the subtyping hierarchy of *ev*, right before the root event ***Event***. The auxiliary function *topContract* returns the translucid contract of this event. As shown in Figure 5, this is necessary for the non-decreasing relation in which observers of the event and observers of its superevent run before the event body e' in the chain of observers. Figure 10 shows the conforming subject `ASTVisitor`, on lines 10–19. Runtime assertions on lines 13 and 16 check for satisfaction of the precondition and postcondition of the top contract of `AndEv`, i.e. the translucid contract of `ExpEv`, by the event body.

4.1.3 Soundness Theorem

Theorem 4.3 formalizes soundness of *Ptolemy*$_{\mathbb{S}}$'s Hoare logic.

THEOREM 4.3. *(Soundness of Ptolemy$_{\mathbb{S}}$'s Hoare logic) Ptolemy$_{\mathbb{S}}$'s Hoare logic, in Figure 8, is sound for conforming Ptolemy$_{\mathbb{S}}$ programs. In other words, any Hoare triple provable using Ptolemy$_{\mathbb{S}}$'s logic, i.e. $\Gamma \vdash \{p\}\ e\ \{q\}$, is a valid triple, i.e. $\Gamma \models \{p\}\ e\ \{q\}$.*

The proof is based on induction on the number of events in a subtyping hierarchy and the number of their observers and uses conformance, refining and non-decreasing relations. Full proof of the theorem can be found in our technical report [33] .

4.2 Revisiting Reasoning about Announce and Invoke

Ptolemy$_{\mathbb{S}}$'s reasoning rules (V-ANNOUNCE) and (V-INVOKE) are sound because the conformance, refining and non-decreasing relations allow, in any chain of observers, the implementation of an invoked observer to be inlined in place of invoke expressions of its invoking observer *without violating* the precondition and postcondition of the invoking observer. This in turn allows the chain of observers of an event and observers of its superevents, starting from the event body at the end of the chain back to its beginning, to be recursively inlined in an announce expression without violating the precondition and postcondition of the contract of the event.

To illustrate, reconsider reasoning about the behavior of ***announce*** *AndEv*$(e,\ e.left,\ e.right)$, in Figure 1. Upon announcement of `AndEv`, if there are no observers of `AndEv` or observers of its superevents `BinEv` or `ExpEv` in the chain of observers, then the event body $e.left.accept(\textbf{\textit{this}});\ e.right.accept(\textbf{\textit{this}})$ executes. The subject `ASTVisitor` of `AndEv` is conforming and thus the event body satisfies the behavior of the contract of `ExpEv`, which is the top event in the hierarchy of `AndEv`. That is, the event

```
1  void event AndEv extends BinEv { ..
2   requires left != null && right != null && node != null
3   assumes {
4    next.invoke();
5    requires
         next.node().left!=null&&next.node().right!=null
6    ensures next.node().parent==old(next.node().parent);
7   }
8   ensures node.equals(old(node))
9  }
10 class ASTVisitor {
11  void visit(AndExp e) {
12   announce AndEv(e, e.left, e.right) {
13    assert(e != null);
14    e.left.accept(this);
15    e.right.accept(this);
16    assert(node.equals(old(node)));
17   }
18  } ..
19 }
20 class Evaluator { ..
21  void evalAndExp (AndEv next) {
22   assert(next.node().left!=null&&next.node().right!=null
         &&next.node()!=null);
23   next.invoke();
24   assert(next.node().left!=null&&next.node().right!=null);
25   refining
26   requires
         next.node().left!=null&&next.node().right!=null
27   ensures next.node().parent==old(next.node().parent){
28    BoolVal b1 = (BoolVal) valStack.pop();
29   }
30   assert(next.node().parent==old(next.node().parent));
31   assert(next.node().equals(old(next.node())));
32  }
33  when AndEv do evalAndExp; ..
34 }
```

Figure 10. Conforming `Evaluator` and `ASTVisitor`.

body satisfies the precondition $node\ != \textbf{\textit{null}}$ and the postcondition $node.equals(\textbf{\textit{old}}\ (node))$ of `ExpEv` after the context *node* is replaced with parameter *e* of the announce expression:

$$\begin{array}{l}(\text{H-BODY})\\ \Gamma \models \{e\ != \textbf{\textit{null}}\}\\ \qquad e.left.accept(\textbf{\textit{this}});\ e.right.accept(\textbf{\textit{this}});\\ \quad \{e.equals(\textbf{\textit{old}}\ (e))\}\end{array}$$

The refining relation guarantees that the behavior of `AndEv` refines the behavior of `ExpEv`. That is, the precondition of `AndEv` implies the precondition of `ExpEv`, i.e. $left! = \textbf{\textit{null}}\ \&\&\ right! = \textbf{\textit{null}}\ \&\&\ node! = \textbf{\textit{null}} \Rightarrow node\ != \textbf{\textit{null}}$, and the opposite is true for their postconditions, i.e. $node.equals(\textbf{\textit{old}}\ (node)) \Rightarrow node.equals(\textbf{\textit{old}}\ (node))$. Using these implications, the rule (V-CONSEQ) and after replacing the context *node* with *e*, one can conclude that the event body satisfies the behavior of `AndEv`:

$$\begin{array}{l}\Gamma \models \{e.left! = \textbf{\textit{null}}\ \&\&\ e.right! = \ \textbf{\textit{null}}\ \&\&\ e! = \textbf{\textit{null}}\}\\ \qquad e.left.accept(\textbf{\textit{this}});\ e.right.accept(\textbf{\textit{this}});\\ \quad \{e.equals(\textbf{\textit{old}}\ (e))\}\end{array}$$

Since the event body is the only observer that executes upon announcement of `AndEv`, the announce expression can be replaced with the event body:

$$\begin{array}{l}(\text{H-ANNOUNCE-BODY})\\ \Gamma \models \{e.left! = \ \textbf{\textit{null}}\ \&\&\ e.right! = \textbf{\textit{null}}\ \&\&\ e! = \textbf{\textit{null}}\}\\ \qquad \textbf{\textit{announce}}\ AndEv(e,\ e.left,\ e.right)\\ \qquad\quad \{e.left.accept(\textbf{\textit{this}});\ e.right.accept(\textbf{\textit{this}});\}\\ \quad \{e.equals(\textbf{\textit{old}}\ (e))\}\end{array}$$

The judgement (H-ANNOUNCE-BODY) says the announce expression of `AndEv` with event body as its only observer satisfies the behavior of the translucid contract of `AndEv`.

However, the event body may not be the only observer of `AndEv`. Consider observers `evaluator` and `tracer` of event `AndEv` and `ExpEv` and the event body of `AndEv`, shown as $\mathscr{B}$`(AndEv)`, run in a chain χ_1 : `evaluator` $\rightharpoonup$ `tracer` $\rightharpoonup$ $\mathscr{B}$`(AndEv)`. Again, conformance of `ASTVisitor` means that the event body satisfies the behavior of the contract of `ExpEv`, i.e. (H-BODY). Recall that an observer of an event and the invoke expressions in its implementation have the precondition and postcondition of the contract of the event. The precondition of the invoke expression in the implementation of `tracer` implies the precondition of the event body, i.e. $node! = \textbf{null} \Rightarrow node! = \textbf{null}$ and the postcondition of the event body implies the postcondition of the invoke expression, i.e. $node.equals(\textbf{old}\ (node)) \Rightarrow node.equals(\textbf{old}\ (node))$. This in turn allows the event body, in grey, to be inlined in the place of the invoke expression in the implementation of `tracer`, in Figure 3, without violating the precondition and postcondition of `tracer`:

$$
\begin{array}{l}
\text{(H-TRACER)}\\
\Gamma \models \{e\ != \textbf{null}\}\\
\qquad e.left.accept(\textbf{this});\ e.right.accept(\textbf{this});\\
\qquad \textbf{refining requires true}\\
\qquad \textbf{ensures}\ e.parent == \textbf{old}\ (e.parent)\{..\}\\
\quad \{e.equals(\textbf{old}\ (e))\}
\end{array}
$$

Using the refining relation, the precondition of `AndEv` implies the precondition of `ExpEv` and the opposite is true for their postconditions. This means the precondition of the invoke expression in the implementation of `evaluator` implies the precondition of `tracer`, i.e. $left! = \textbf{null}\ \&\&\ right! = \textbf{null}\ \&\&\ node! = \textbf{null} \Rightarrow node\ != \textbf{null}$, and the postcondition of `tracer` implies the postcondition of the invoke expression in `evaluator`, i.e. $node.equals(\textbf{old}\ (node)) \Rightarrow node.equals(\textbf{old}\ (node))$. This allows the implementation of `tracer` in (H-TRACER) to be inlined, in grey, in place of the invoke expression in `evaluator` without violating its precondition and postcondition of `evaluator`:

$$
\begin{array}{l}
\text{(H-EVALUATOR)}\\
\Gamma \models \{e.left! = \textbf{null}\ \&\&\ e.right! = \textbf{null}\ \&\&\ e! = \textbf{null}\}\\
\qquad e.left.accept(\textbf{this});\ e.right.accept(\textbf{this});\\
\qquad \textbf{refining requires true}\\
\qquad \textbf{ensures}\ e.parent == \textbf{old}\ (e.parent)\{..\};\\
\qquad \textbf{refining}\\
\qquad \textbf{requires}\ e.left! = \textbf{null}\ \&\&\ e.right! = \textbf{null}\\
\qquad \textbf{ensures}\ e.parent == \textbf{old}\ (e.parent)\{..\};\\
\quad \{e.equals(\textbf{old}\ (e))\}
\end{array}
$$

Since the announcement of `AndEv` causes the chain χ_1 to run, the inlined chain of observers in (H-EVALUATOR) can be replaced with the announce expression:

$$
\begin{array}{l}
\text{(H-ANNOUNCE-}\chi_1\text{)}\\
\Gamma \models \{e.left! = \textbf{null}\ \&\&\ e.right! = \textbf{null}\ \&\&\ e! = \textbf{null}\}\\
\qquad \textbf{announce}\ AndEv(e,\ e.left,\ e.right)\\
\qquad \{e.left.accept(\textbf{this});\ e.right.accept(\textbf{this});\}\\
\quad \{e.equals(\textbf{old}\ (e))\}
\end{array}
$$

The judgement (H-ANNOUNCE-χ_1) says that the behavior of the announce expression of `AndEv` with the chain of observers χ_1 satisfies the behavior of the contract of `AndEv`.

(H-ANNOUNCE-BODY) and (H-ANNOUNCE-χ_1) say the behavior a chain of observers of `AndEv` and observers of its superevents, can be approximated with the precondition and postcondition of the translucid contract of the `AndEv` which is what the rule (V-ANNOUNCE) in *Ptolemy*$_{\mathbb{S}}$'s reasoning logic says. A similar justification holds for the rule (V-INVOKE).

5. Applicability

Our proposed modular reasoning technique is not exclusive to *Ptolemy*$_{\mathbb{S}}$ and could be adapted to similar AspectJ-like [1] event-based systems such as join point types (JPT) [19] and join point interfaces (JPI) [18]. Application of our reasoning technique to join point interfaces could be found in our technical report [33].

With join point types, a subject (base) exhibits a join point type (event) using an ***exhibits*** statement and aspects (observers) advise the event and handle it using ***advises*** statements. A join point type can extend another join point type, inherit its context variables and add to them through width subtyping. Exhibiting a join point type causes its aspects and aspects of its super join point types to run in a chain where aspects can invoke each other, using ***proceed*** statements. The execution order of aspects is specified using precedence declarations. Join point types do not support depth subtyping, however, this does not affect the applicability of *Ptolemy*$_{\mathbb{S}}$'s reasoning technique to them.

```
1  joinpointtype AndEv extends BinEv {
2  /*@ requires node!=null && left!=null &&right!=null;
3    @ model_program {
4    @  proceed(next);
5    @  requires node.left!=null && node.right!=null;
6    @  ensures node.parent == old(node.parent);
7    @ }
8    @ ensures node.equals(old(node)); */
9  }
10 class ASTVisitor exhibits AndEv,.. {
11  void visit(AndExp e) {
12   exhibits new AndEv(e, e.left, e.right) {
13    e.left.accept(this);
14    e.right.accept(this);
15   }; ..
16  } ..
17 }
18 aspect Evaluator advises AndEv,.. { ..
19  void around(AndEv jp) {
20   proceed(jp);
21   refining
22    requires node.left!=null && node.right!=null;
23    ensures node.parent == old(node.parent){
24    .. //same as before
25   }
26  } ..
27 }
```

Figure 11. Join point type `AndEv` and its translucid contract.

Figure 11 shows parts of the expression language example rewritten using join point types where the subject `ASTVisitor` exhibits a join point instance `AndEv`, on lines 12–15, and the observer `Evaluator` advises the join point, on lines 19–26. `Evaluator` invokes the next observer in the chain of observers using a proceed statement on line 20, which takes as argument a join point instance `jp` of join point type `AndEv`. The join point type `AndEv` is declared on lines 1–9 and extends the join point type `BinEv`.

Figure 11 shows the syntactic adaptation of the translucid contract of the join point type `AndEv`, on lines 2–8, using a JML-like syntax. JML syntax is specifically chosen to minimize required syntactic changes. In a contract of a join point type, a JML model program [40] is similar to an assumes block and a proceed statement is equivalent to an invoke expression [7]. A variable ***next*** in the contract of a join point type is a placeholder for join point instances of that type, which contains values of its contexts.

Although, a translucid contract of a join point type uses JML's syntax, its verification is completely different from JML. This is because a JML contract specifies the behavior and structure of only a single method whereas a translucid contract of a join point type specifies all bases and aspects of the join point type. Consequently, for the conformance relation, for each join point type, all of its bases and aspects must conform to the translucid contract of their join point type, i.e. structurally refine the contract and satisfy its preconditions and postconditions. Type checking rules of join point types could be augmented to check for structural refinement and runtime assertions could be added to bases and aspects to check for their satisfaction of preconditions and postconditions of their contract and their specification expressions. In addition to syntactic adaptations of structural refinement, the rule (S-VAR) should be slightly modified to allow for structural refinement of placeholder variables ***next*** by join point instance variables. Unlike *Ptolemy*$_{\mathbb{S}}$ in which a variable ***next*** is structurally refined by a textually matching variable ***next***, in join point types a variable ***next*** in a contract of a join point type is structurally refined by a join point instance variable in the implementation of an observer if their types are the same. For example, in Figure 11, the variable ***next*** in the translucid contract of `AndEv`, on line 4, is structurally refined by the join point instance variable `jp` in the observer `Evaluator`, on line 20, because they both are of the same type `AndEv`.

Another difference between translucid contracts and JML contracts is that JML requires model programs of a type and its supertype to be the same [40], whereas in translucid contracts the assumes block of an event refines the assumes block of its superevent. Consequently, for the refining relation, *Ptolemy*$_{\mathbb{S}}$'s specification inheritance [33] could be adapted to join point types, mostly through syntactic adaptations, to statically guarantee the refining relation between translucid contracts of a join point type and its super type.

For the non-decreasing relation, precedence declarations of aspects could be statically checked to ensure that an aspect of a join point type runs before aspects of its super join point type or execution of aspects can be reordered dynamically at runtime to guarantee the non-decreasing relation.

A similar technique, with several adaptations, could be applied to join point interfaces due to similarities of event announcement, handling and subtyping models of join point types and join point interfaces [33].

6. Modular Reasoning about Control Effects

Ptolemy$_{\mathbb{S}}$ not only enables modular reasoning about behaviors of observers of an event but also their control effects [7, 28] in the presence of event subtyping. In *Ptolemy*$_{\mathbb{S}}$, similar to Aspect-like [1] languages, observers run in a chain and invoke each other using an ***invoke*** expression. This in turn means an observer of an event can skip the execution of other observers of the event or observers of its superevents, including the event body, by not executing its invoke expression. Understanding the invocations among observers of an event and its superevents in a chain of observers falls under the category of modular reasoning about control effects of observers.

As an example of modular reasoning about control effects of observers consider static verification of the control effect assertion Ψ that says *upon announcement and handling of* `AndEv`*, its event body, on lines 5–6 of Figure 1 will be executed and will not be skipped*[5]. This is important because if the execution of the event body of `AndEv` is skipped, the right and left children of an `AndExp` expression and subtrees recursively rooted in these children are not going to be visited. The execution of the body of `AndEv`, shown as $\mathscr{B}$`(AndEv)`, could be skipped in a chain of observers if any of observers of `AndEv` or observers of its superevents `BinEv` or `ExpEv`, which run before the event body, skip the execution of their invoke expression and break the invocation chain. For example, in chain χ_2: `evaluator` $\rightharpoonup$ `tracer` $\rightharpoonup$ $\mathscr{B}$`(AndEv)`, the execution of $\mathscr{B}$`(AndEv)` is skipped if any or both invoke expressions in the implementations of `evaluator`, on line 55 of Figure 3, or `tracer`, on line 41, goes missing.

[5] *Ptolemy*$_{\mathbb{S}}$' core does not support throwing or handling of exceptions [8].

To reason about the control effects of an announcement of an event, the control effects of all of its observers and observers of its superevents for their various execution orders must be understood, especially regarding the execution of their invoke expressions. Such reasoning is dependent on control effects of individual observers of the event and observers of its superevents and any changes in these control effects can invalidate any previous reasoning, which threatens its modularity.

Ptolemy$_{\mathbb{S}}$'s translucid contracts enable modular reasoning about control effects of observers of an event and observers of its superevents, independent of observers and their execution orders. This is sound because each conforming observer of an event has the same control effects as the translucid contract of the event and *Ptolemy*$_{\mathbb{S}}$'s refining relation ensures that the contract of an event refines the control effects of the contract of its superevent. Control effects are specified by program expressions in translucid contracts.

In *Ptolemy*$_{\mathbb{S}}$, the assertion Ψ could be verified using the translucid contract of `AndEv` and especially its assumes block, on lines 21–25 of Figure 4. The program expression ***next.invoke***(), on line 22, guarantees that each observer of `AndEv` includes the invoke expression in their implementations and the refining relation ensures that each observer of superevents of `AndEv` contain the invoke expression in their implementations too. This means that the invoke expression in the implementation of `evaluator` or `tracer` in χ_2 cannot go missing or otherwise these observers will not be conforming to their translucid contracts. This in turn means that all the observers in the chain χ_2, including the event body at the end of the chain, are invoked and executed.

6.1 Control Interference of Subjects and Observers

Rinard *et al.* [43] classify the control interactions of a subject and observer of an event into four categories: *(i)* augmentation, *(ii)* narrowing, *(iii)* replacement and *(iv)* combination. These categories are concerned about the number of invoke expressions and their executions in an implementation of an observer. An augmentation observer executes its invoke expression exactly once, a narrowing observer executes it at most once, a replacement observer does not execute any invoke expressions and a combination observer executes its invoke expression zero or more times in its implementation.

Ptolemy$_{\mathbb{S}}$'s translucid contracts allow modular reasoning about the control interference category of interactions of subjects and observers of an event, independent of observers of the event and observers of its superevents. To reason about the control interference of subjects and observers of an event, one uses the translucid contract of the event to decide about the the number of times invoke expressions of the translucid contract may execute. An invoke expression surrounded by an if conditional executes at most once, whereas an invoke expression surrounded by a loop may execute zero times or more. Otherwise, an invoke expression executes exactly once. This is sound because the structural refinement of the conformance relation requires each observer of an event to have the same control effects as its translucid contracts, especially regarding the number of invoke expressions in its implementation. Also, the refining relation ensures that the control effects of observers of an event refine the control effects of observers of its superevents.

Augementation interactions and observers To illustrate the augmentation interaction, consider the observer `Evaluator` and subject `ASTVisitor` of the event `AndEv`. Using only the translucid contract of `AndEv`, on lines 20–26 of Figure 4, one can conclude that subjects and observers of `AndEv` have an augmentation interaction, in which `Evaluator` augments the behavior of its subject, i.e. `Evaluator` is an augmentation observer. This is because the assumes block of the contract of `AndEv` contains an invoke expression, on line 22, which is not surrounded by any conditionals or loops. This in turn means that the conforming observer `Evaluator` has only one invoke expression in its implementation which executes exactly once. For observers `Checker` and `Tracer` of superevents `BinEv` and `ExpEv` of `AndEv`, the refining relation ensures that they also have only one invoke expressions in their implementations and thus they are augmentation observers too.

For an event with augmentation interactions and observers, one can conclude that upon announcement of the event all observers of the event and observers of its superevent including the event body execute and no execution is skipped, similar to assertion Ψ.

Replacement interactions and observers To illustrate the replacement interaction, consider the event `AndEv` with its translucid contract in Figure 4, but without its invoke expression. Using this contract one can conclude that subjects and observers of `AndEv` have a replacement interaction, in which `Evaluator` replaces the body of its announce expression in a subject, i.e. `Evaluator` is a replacement observer. To structurally refine its contract, `Evaluator` cannot have any invoke expression in its implementation. The refining relation ensures that superevents `BinEv` and `ExpEv` cannot have invoke expressions in their contracts either and thus observers `Checker` and `Tracer` are replacement observers too.

For an event with replacement observers, one can conclude that upon announcement of the event the first observer of the event or its superevents executes and executions of the rest of the observers including the event body are skipped. This is because none of the observers have an invoke expression in their implementations.

7. Discussion

Implementation To prove the feasibility of our proposed language, we implemented *Ptolemy*$_{\mathbb{S}}$'s compiler on top of Ptolemy's compiler [24], which itself is an extension of the OpenJDK Java compiler. To the previous compiler, we added translucid contracts, static structural refinement, static event specification inheritance, runtime assertion checking of preconditions and postconditions of contracts and their specification expressions and a non-decreasing execution order of observers of an event and its superevents. Compared to Ptolemy's compiler, maintaining separate lists for observers of separate events, rather than a single global list, simplified implementation of event announcement and handling especially with dynamic (un)registration of observers.

Limitation A non-decreasing relation among observers of an event and its superevent(s) limits execution order of observers and could require a programmer to co-design the event subtyping hierarchy of a program and execution order of their observers. Without such a co-design there could be some execution orders of observers that may not be allowed by a specific event subtyping hierarchy. For example, with the event hierarchy in our expression language example, observer `evaluator` always runs before `checker`. Placement of invoke expressions in observers play an important role in the functionality of a system. For example, although `evaluator` runs before `checker`, an expression is not evaluated unless it is first type checked. This is enforced because `evaluator` invokes the handler chain before evaluating an expression.

8. Related Work

Modular type checking Previous work on join point types (JPT) [19], join point interfaces (JPI) [18] and Ptolemy's typed events [24] enables modular type checking of subjects and observers of subtyping event types. EventJava [11] extends Java with events and event correlation in distributed settings and Escala [6] extends Scala with explicitly declared events as members of classes. However, previous works are not concerned with modular reasoning about behaviors and control effects of subjects and observers of events using specification of subtyping event types.

Modular reasoning Previous work on MAO [29], EffectiveAdvice [44], MRI [45] and the work of Khatchadourian *et al.* [27] enables modular reasoning, however, it does not use explicit interfaces among subjects and observers and thus is not concerned about their subtyping. Previous work on crosscutting programming interfaces (XPI) [5], crosscutting programming interfaces with design rules (XPIDR) [28] and open modules [2] enables modular reasoning using explicit interfaces, however, it is not concerned about subtyping of these interfaces. Translucid contracts [7–9, 46] proposes event type specifications to enable modular reasoning, however, it is not concerned with event subtyping.

Modular reasoning about dynamic dispatch Supertype abstraction [47] enables modular reasoning about invocation of a dynamically dispatched method in the presence of class subtyping [47], relying on a refinement relation among blackbox contracts of a supertype and its subtypes [31, 48]. *Ptolemy*$_{\mathbb{S}}$'s refining of event contracts is the inverse of the refinement in supertype abstraction and extends it to greybox contracts with control effects. Refinement in supertype abstraction relies on known links among method invocations and method names, whereas in *Ptolemy*$_{\mathbb{S}}$ there is no link among subjects and observers of an event [8, 26]. Subjects and observers do not know about each other and only know their event. Unlike a method invocation which invokes exactly one method, announcement of an event in *Ptolemy*$_{\mathbb{S}}$ by a subject could invoke zero or more observers of the event and observers of its superevents where all these observers and the subject must conform to their event specifications. The challenge in supertype abstraction is modular reasoning about a method invocation independent of the dynamic types of its receiver, whereas in *Ptolemy*$_{\mathbb{S}}$ the challenge is tractable reasoning about announcement and handling of an event, independent of its observers, observers of its superevents and their execution orders, while allowing reuse of events.

9. Conclusion and Future Work

In this work we identified combinatorial reasoning and behavior invariance as two problems of modular reasoning about subjects and observers in the presence of event subtyping. We proposed a refining relation among greybox event specifications of events in a subtyping hierarchy, a non-decreasing relation on execution orders of their observers and a conformance relation among subjects and observers of an event and their translucid contract to solve these problems in the context of a new language design called *Ptolemy*$_{\mathbb{S}}$. We showed applicability of *Ptolemy*$_{\mathbb{S}}$'s modular reasoning to other AspectJ-like [1] event-based systems such as join point types [19] and its use in modular reasoning about control interference.

Future work includes performing a large experimental study similar to [21–23] to further investigate benefits of *Ptolemy*$_{\mathbb{S}}$'s event model and its modular reasoning. It would also be interesting to examine the interplay between semantics of invoke and execution order of observers. Recent work has explored asynchronous execution of observers [49]. Examining the interplay of concurrency and event inheritance will also be interesting.

Acknowledgements

We thank *Modularity'15* reviewers. Bagherzadeh, Dyer and Rajan were partly supported by the NSF grant CCF-10-17334. Fernando and Rajan were partly supported by the NSF grant CCF-08-46059. Rajan was also partly supported by the NSF grant CCF-11-17937. Sanchez was partly supported by NSF grant CCF-1017334.

References

[1] Kiczales, G., Hilsdale, E., Hugunin, M., Kersten, M., Palm, J., Griswold, W.G.: An overview of AspectJ. In: ECOOP'01

[2] Aldrich, J.: Open Modules: Modular reasoning about advice. In: ECOOP'05

[3] Sullivan, K., Griswold, W.G., Song, Y., Cai, Y., Shonle, M., Tewari, N., Rajan, H.: Information hiding interfaces for aspect-oriented design. In: ESEC/FSE'05

[4] Griswold, W.G., Sullivan, K., Song, Y., Shonle, M., Tewari, N., Cai, Y., Rajan, H.: Modular software design with crosscutting interfaces. IEEE Softw.'06 **23**(1)

[5] Sullivan, K.J., Griswold, W.G., Rajan, H., Song, Y., Cai, Y., Shonle, M., Tewari, N.: Modular aspect-oriented design with XPIs. TOSEM'11 **20**(2)

[6] Gasiunas, V., Satabin, L., Mezini, M., nez, A.N., Noyé, J.: EScala: modular event-driven object interactions in Scala. In: AOSD'11

[7] Bagherzadeh, M., Rajan, H., Leavens, G.T., Mooney, S.: Translucid contracts: Expressive specification and modular verification for aspect-oriented interfaces. In: AOSD'11

[8] Bagherzadeh, M., Rajan, H., Darvish, A.: On exceptions, events and observer chains. In: AOSD'13

[9] Sánchez, J., Leavens, G.: Separating obligations of subjects and handlers for more flexible event type verification. In: SC'13

[10] Hoffman, K., Eugster, P.: Bridging Java and AspectJ through explicit join points. In: PPPJ'07

[11] Eugster, P., Jayaram, K.R.: EventJava: An extension of Java for event correlation. In: ECOOP'09

[12] Clifton, C., Leavens, G.T.: Obliviousness, modular reasoning, and the behavioral subtyping analogy. In: SPLAT'03

[13] Kiczales, G., Mezini, M.: Aspect-oriented programming and modular reasoning. ICSE'05

[14] Clifton, C., Leavens, G.T.: A design discipline and language features for modular reasoning in aspect-oriented programs. Technical Report 05-23, Iowa State University (2005)

[15] Rajan, H., Leavens, G.T.: Ptolemy: A language with quantified, typed events. In: ECOOP'08

[16] Rajan, H., Sullivan, K.J.: Unifying aspect- and object-oriented design. TOSEM'09 **19**(1)

[17] Rajan, H., Leavens, G.T.: Quantified, typed events for improved separation of concerns. Technical Report 07-14, Iowa State University (2007)

[18] Bodden, E., Tanter, E., Inostroza, M.: Joint point interfaces for safe and flexible decoupling of aspects. TOSEM'14 **23**(1)

[19] Steimann, F., Pawlitzki, T., Apel, S., Kästner, C.: Types and modularity for implicit invocation with implicit announcement. TOSEM'10 **20**(1)

[20] Rajan, H., Dyer, R., Hanna, Y.W., Narayanappa, H.: Preserving separation of concerns through compilation. In: SPLAT'06

[21] Dyer, R., Rajan, H., Cai, Y.: An exploratory study of the design impact of language features for aspect-oriented interfaces. In: AOSD'12

[22] Dyer, R., Rajan, H., Cai, Y.: Language features for software evolution and aspect-oriented interfaces: An exploratory study. TAOSD'10 **10**

[23] Dyer, R., Bagherzadeh, M., Rajan, H., Cai, Y.: A preliminary study of quantified, typed events. In: ESCOT'10

[24] Fernando, R., Dyer, R., Rajan, H.: Event type polymorhphism. In: FOAL'12

[25] Xu, J., Rajan, H., Sullivan, K.: Understanding aspects via implicit invocation. In: ASE'04

[26] Dingel, J., Garlan, D., Jha, S., Notkin, D.: Towards a formal treatment of implicit invocation using rely/guarantee reasoning. Formal Asp. Comput.'98 **10**(3)

[27] Khatchadourian, R., Dovland, J., Soundarajan, N.: Enforcing behavioral constraints in evolving aspect-oriented programs. In: FOAL'08

[28] Rebelo, H., Leavens, G.T., Lima, R.M.F., Borba, P., Ribeiro, M.: Modular aspect-oriented design rule enforcement with XPIDRs. In: FOAL'13

[29] Clifton, C., Leavens, G., Noble, J.: MAO: Ownership and effects for more effective reasoning about aspects. In: ECOOP'07

[30] Büchi, M., Weck, W.: The greybox approach: When blackbox specifications hide too much. Technical Report 297, Turku Center for Computer Science (1999)

[31] Leavens, G.T., Naumann, D.A.: Behavioral subtyping, specification inheritance, and modular reasoning. Technical Report CS-TR-13-03, University of Central Florida (2013)

[32] Hoare, C.A.R.: An axiomatic basis for computer programming. Commun. ACM'83 **26**(1)

[33] Bagherzadeh, M., Dyer, R., Fernando, R.D., Sánchez, J., Rajan, H.: Modular reasoning in the presence of event subtyping. Technical Report 14-02b, Iowa State University (2015)

[34] Rajan, H.: Unifying Aspect- and Object-Oriented Program Design. PhD thesis, The University of Virginia (2005)

[35] Rajan, H.: Design pattern implementations in Eos. In: PLoP'07

[36] Rajan, H., Sullivan, K.J.: Classpects: Unifying aspect- and object-oriented language design. In: ICSE'05

[37] Rajan, H., Sullivan, K.: Eos: instance-level aspects for integrated system design. In: ESEC/FSE'03

[38] Morgan, C.: Procedures, parameters, and abstraction: separate concerns. SCP'88 **11**(1)

[39] Dhara, K.K., Leavens, G.T.: Forcing behavioral subtyping through specification inheritance. In: ICSE'97

[40] Shaner, S.M., Leavens, G.T., Naumann, D.A.: Modular verification of higher-order methods with mandatory calls specified by model programs. In: OOPSLA'07

[41] Abadi, M., Leino, K.: A logic of object-oriented programs. In: TAPSOFT'97

[42] Boer, F.: A WP-calculus for OO. In: Foundations of Software Science and Computation Structures'99

[43] Rinard, M., Salcianu, A., Bugrara, S.: A classification system and analysis for aspect-oriented programs. In: FSE'04

[44] Oliveira, B.C.d.S., Schrijvers, T., Cook, W.R.: EffectiveAdvice: Disciplined advice with explicit effects. In: AOSD'10

[45] Oliveira, B.c.d.s., Schrijvers, T., Cook, W.r.: MRI: Modular reasoning about interference in incremental programming. JFP'12 **22**(6)

[46] Bagherzadeh, M., Rajan, H., Leavens, G.T., Mooney, S.: Translucid contracts for aspect-oriented interfaces. In: FOAL'10

[47] Leavens, G.T., Weihl, W.E.: Specification and verification of object-oriented programs using supertype abstraction. Acta Informatica'95

[48] Liskov, B.H., Wing, J.M.: A behavioral notion of subtyping. TOPLAS'94 **16**(6)

[49] Long, Y., Mooney, S.L., Sondag, T., Rajan, H.: Implicit invocation meets safe, implicit concurrency. In: GPCE'10

[50] Wright, A.K., Felleisen, M.: A syntactic approach to type soundness. Information and Computation '94 **115**(1)

A. Dynamic Semantics

In this section, we present a substitution-based small-step operational semantics for *Ptolemy*$_{\mathbb{S}}$ with special focus on announcing and handling of events in an event inheritance hierarchy and the non-decreasing relation on execution order of their observers.

A.1 Dynamic Semantic Objects

Ptolemy$_{\mathbb{S}}$'s operational semantics relies on few additional expressions that are not part of its surface syntax, as shown in Figure 12, including *loc* to represent the locations in the store and ***evalpost*** *e q* to check that the expression *e* satisfies the postcondition *q*. *Ptolemy*$_{\mathbb{S}}$

also uses three exceptions to represent dereferencing null references, i.e. ***NPE***, runtime cast exceptions, i.e. ***CCE***, and violations of translucid contracts, i.e. ***TCE***. In *Ptolemy*$_{\mathbb{S}}$'s core semantics, exceptions are terminal states [15]. Figure 12 also shows the evaluation contexts used in *Ptolemy*$_{\mathbb{S}}$'s dynamic semantics. An evaluation context $\mathbb{E}$ specifies the evaluation order and the position in an expression where the evaluation is happening. *Ptolemy*$_{\mathbb{S}}$ uses a left-most inner-most call-by-value evaluation policy.

Added syntax:
$e ::= loc \mid \textbf{\textit{evalpost}}\ e\ q$
$\quad \mid \textbf{\textit{NPE}} \mid \textbf{\textit{CCE}} \mid \textbf{\textit{TCE}}$
$\quad loc \in \mathscr{L}$, a set of locations

Evaluation contexts:
$\mathbb{E} ::= - \mid \mathbb{E}\,.m(e\ldots) \mid v\,.m(v\ldots\mathbb{E}e\ldots) \mid \mathbb{E}.f \mid \mathbb{E}\,.f\texttt{=}e$
$\quad \mid \texttt{if (}\mathbb{E}\texttt{) \{ } e \texttt{ \} else \{ } e \texttt{ \}} \mid \texttt{cast}\ c\ \mathbb{E} \mid t\ var\texttt{=}\mathbb{E}\texttt{;}\ e$
$\quad \mid \texttt{announce (}v\ldots\mathbb{E}e\ldots\texttt{) \{}e\texttt{\}} \mid \texttt{invoke (}\mathbb{E}\texttt{)}$
$\quad \mid \texttt{register (}\mathbb{E}\texttt{)} \mid \texttt{unregister (}\mathbb{E}\texttt{)}$
$\quad \mid \texttt{refining requires}\ \mathbb{E}\ \texttt{ensures}\ q$

Evaluation relation: $\hookrightarrow: \langle e,S,\Pi,A\rangle \to \langle e',S',\Pi',A'\rangle$

Domains:

$\Sigma ::= \langle e,S,\Pi,A\rangle$	configurations
$S ::= \{loc_k \mapsto sv_k\}$	stores
$v ::= \textbf{\textit{null}} \mid loc$	values
$sv ::= or \mid ec$	storable values
$or ::= [c\,.F]$	object records
$F ::= \{f_k \mapsto v_k\}$	field maps
$\rho ::= \{var \mapsto v_k\}$	environments
$ec ::= \textbf{\textit{eClosure}}(H,e,\rho)$	event closure
$H ::= h + H \mid \bullet$	handler records list
$h ::= \langle loc,m\rangle$	handler record
$A ::= \{ev_k \mapsto O_k\}$	active objects map
$O ::= loc + O \mid \bullet$	active objects list
$\quad k \in \mathscr{K}$, is finite	

Figure 12. Added syntax, evaluation contexts and configuration.

Ptolemy$_{\mathbb{S}}$'s operational semantics transitions from one configuration to another. A configuration Σ, in Figure 12, contains an expression e, store S, store typing Π and a mapping A from events ev to their ordered list of observers O. A store maps locations to storable values sv which themselves are either an object record or or an event closure ec. An object record has a class name c and a map F from fields to their values. An event closure $\textbf{\textit{eClosure}}(H,e,\rho)$ contains an ordered list of observer handlers H, an expression e and an environment ρ for running e. An observer handler method h contains a location loc that points to its observer object and a handler method name m. A value v is either a location loc or ***null***. A store typing is maintained and updated by the dynamic rules only to be used in the soundness proof.

A.2 Dynamic Semantic Rules

Figure 13 shows dynamic semantic of *Ptolemy*$_{\mathbb{S}}$-specific expressions. In *Ptolemy*$_{\mathbb{S}}$, a subject announces an event using an announce expression, observers (un)register for the event using (un)register expressions and invoke each other using invoke expressions.

The rule (ANNOUNCE) says that upon announcement of an event ev an event closure $\textbf{\textit{eClosure}}(H,e,\rho)$ is constructed that contains the list (chain) of observer handler methods of the event and the observer handler methods of its superevent, in H, the event body e and an environment mapping context variables var^* of the event to their values v^*, in ρ. The list H is constructed using the auxiliary function *handlersOf*, in Figure 14. The function *handlersOf* first computes the list of observer handler methods of the event ev, using *hbind*, and concatenates it to the handlers of the superevents ev' until the event ***Event*** is reached. This in turn ensures that the observer handler methods of the event ev appear before the observer handler methods of its superevent ev' in the list of observer handler methods H, according to the non-decreasing relation. The event ***Event*** has no observers since is not part of *Ptolemy*$_{\mathbb{S}}$'s surface syntax and observers can not register for or handle it. The concatenate operator $\oplus$ ignores empty $\bullet$ elements. The function *hbind* binds the observer loc, in the beginning of the $A[ev]$, to observer handler method m, using the auxiliary function *match* and concatenates it to the bindings for the rest of $A[ev]$. After construction, the event closure is mapped to a fresh location loc and the execution of the chain of observer handler methods starts using the invoke expression, i.e. $loc.\textbf{\textit{invoke}}()$.

Evaluation relation: $\boxed{\hookrightarrow: \langle e,S,\Pi,A\rangle \to \langle e',S',\Pi',A'\rangle}$

(ANNOUNCE)
$$\frac{\begin{array}{c}(c\ \textbf{\textit{event}}\ ev\ \textbf{\textit{extends}}\ ev'\{(t\ var)^*\ contract_{ev}\}) \in CT \qquad loc \notin dom(S)\\ H = handlersOf(ev) \qquad \rho = \{var_i \mapsto v_i \mid var_i \in var^* \wedge v_i \in v^*\}\\ S' = S \uplus (loc \mapsto \textbf{\textit{eClosure}}(H,e,\rho)) \qquad \Pi' = \Pi \uplus (loc : \textbf{\textit{thunk}}\ ev)\end{array}}{\langle \mathbb{E}[\textbf{\textit{announce}}\ ev\ (v^*)\ \{e\}],S,\Pi,A\rangle \hookrightarrow \langle \mathbb{E}[loc.\textbf{\textit{invoke}}()],S',\Pi',A\rangle}$$

(INVOKEDONE)
$$\frac{\textbf{\textit{eClosure}}(\bullet,e,\rho) = S(loc)}{\langle \mathbb{E}[loc.\textbf{\textit{invoke}}()],S,\Pi,A\rangle \hookrightarrow \langle \mathbb{E}[e],S,A,\Pi\rangle}$$

(INVOKE)
$$\frac{\begin{array}{c}\textbf{\textit{eClosure}}(\langle loc',m\rangle + H,e,\rho) = S(loc)\\ [c\,.F'] = S(loc') \qquad (c_2,t\ m(t_1\ var_1)\{e'\}) = methodBody(c,m)\\ e'' = [loc_1/var_1, loc'/\textbf{\textit{this}}]e' \qquad loc_1 \notin dom(S)\\ S' = S \uplus (loc_1 \mapsto \textbf{\textit{eClosure}}(H,e,\rho)) \qquad \Pi' = \Pi \uplus (loc_1 : \Pi(loc))\end{array}}{\langle \mathbb{E}[loc.\textbf{\textit{invoke}}()],S,\Pi,A\rangle \hookrightarrow \langle \mathbb{E}[e''],S',\Pi',A\rangle}$$

(REGISTER)
$$\frac{\forall ev \in eventsOf(loc)\ .\ A'[ev] = A[ev] + loc}{\langle \mathbb{E}[\textbf{\textit{register}}(loc)],S,\Pi,A\rangle \hookrightarrow \langle \mathbb{E}[loc],S,\Pi,A'\rangle}$$

(UNREGISTER)
$$\frac{\forall ev \in eventsOf(loc)\ .\ A'[ev] = A[ev] - loc}{\langle \mathbb{E}[\textbf{\textit{unregister}}(loc)],S,\Pi,A\rangle \hookrightarrow \langle \mathbb{E}[loc],S,\Pi,A'\rangle}$$

(REFINING)
$$\frac{n \neq 0}{\langle \mathbb{E}[\textbf{\textit{refining requires}}\ n\ \textbf{\textit{ensures}}\ q\ \{e\}],S,\Pi,A\rangle \hookrightarrow \langle \mathbb{E}[\textbf{\textit{evalpost}}\ e\ q],S,\Pi,A\rangle}$$

(EVALPOST)
$$\frac{n \neq 0}{\langle \mathbb{E}[\textbf{\textit{evalpost}}\ v\ n],S,\Pi,A\rangle \hookrightarrow \langle \mathbb{E}[v],S,\Pi,A\rangle}$$

(ECGET)
$$\frac{\textbf{\textit{eClosure}}(H,e,\rho) = S(loc) \qquad v = \rho(f)}{\langle \mathbb{E}[loc.f],S,\Pi,A\rangle \hookrightarrow \langle \mathbb{E}[v],S,\Pi,A\rangle}$$

Figure 13. Select rules for *Ptolemy*$_{\mathbb{S}}$'s dynamic semantics, based on [15].

(ANNOUNCE) also updates the store typing environment Π with a new mapping from the location loc to the type ***thunk*** ev of the event closure it points to. Recall that thunk types mark event closure types. The operator $\uplus$ is an overriding union operator.

Rules (INVOKEDONE) and (INVOKE) handle the base case and recursive case of observer invocation. The auxiliary function *methodBody* emulates dynamic dispatch at runtime. After the execution of the observer handler method at the beginning of the list H, the event closure is updated to reflect the execution of the observer and the updated event closure is stored at a fresh location

loc_1. (INVOKE) also updates the store typing environment Π with a mapping between location loc_1 of new event closure and its type.

$$handlersOf(\textbf{\textit{Event}}) = \bullet$$

$$\frac{(c\ \textbf{\textit{event}}\ ev\ \textbf{\textit{extends}}\ ev'\{form*\ contract_{ev}\}) \in CT}{handlersOf(ev) = hbind(ev,S,A[ev]) \oplus handlersOf(ev')}$$

$$hbind(ev,S,\bullet) = \bullet$$

$$\frac{[c.F] = S(loc) \qquad B = bindingsOf(c)}{hbind(ev,S,loc+A[ev]) = match(B,ev,S,loc) \oplus hbind(ev,S,A[ev])}$$

$$bindingsOf(\textbf{\textit{Object}}) = \bullet$$

$$\frac{(\textbf{\textit{class}}\ c\ \textbf{\textit{extends}}\ d\ \{form*\ meth*\ binding*\}) \in CT}{bindingsOf(c) = binding* \oplus bindingsOf(d)}$$

$$match(\bullet,ev,S,loc) = \bullet$$

$$match((\textbf{\textit{when}}\ ev\ \textbf{\textit{do}}\ m)+B,ev,S,loc) = (\langle loc,m\rangle + match(B,ev,S,loc))$$

$$\frac{[c.F] = S(loc) \qquad B = bindingsOf(c)}{eventsOf(loc) = registeredFor(loc,B)} \qquad registeredFor(loc,\bullet) = \bullet$$

$$registeredFor(loc,(\textbf{\textit{when}}\ ev\ \textbf{\textit{do}}\ m)+B) = ev \oplus registeredFor(loc,B)$$

Figure 14. Select auxiliary functions for *Ptolemy*$_{\mathbb{S}}$'s dynamic semantics, based on [8, 15].

A refining expression claims that its body satisfies the precondition and postcondition of its specification, which is checked by rules (REFINING) and (EVALPOST). Exceptional cases in rules (X-REFINING) and (X-EVALPOST) represent violation of precondition and postcondition.

(X-REFINING)
$$\frac{n == 0}{\langle \mathbb{E}[\textbf{\textit{refining requires}}\ n\ \textbf{\textit{ensures}}\ q\ \{e\}],S,\Pi,A\rangle \hookrightarrow \langle \textbf{\textit{TCE}},S,\Pi,A\rangle}$$

(X-REGISTER)
$$\langle \mathbb{E}[\textbf{\textit{register}}(\textbf{\textit{null}})],S,\Pi,A\rangle \hookrightarrow \langle \textbf{\textit{NPE}},S,\Pi,A\rangle$$

(X-UNREGISTER)
$$\langle \mathbb{E}[\textbf{\textit{unregister}}(\textbf{\textit{null}})],S,\Pi,A\rangle \hookrightarrow \langle \textbf{\textit{NPE}},S,\Pi,A\rangle$$

(X-EVALPOST)
$$\frac{n == 0}{\langle \mathbb{E}[\textbf{\textit{evalpost}}\ v\ n],S,\Pi,A\rangle \hookrightarrow \langle \textbf{\textit{TCE}},S,\Pi,A\rangle}$$

(X-CAST)
$$\frac{[c\,.\,F] = S(loc) \qquad c \not\preccurlyeq t}{\langle \mathbb{E}[\textbf{\textit{cast}}\ t\ loc],S,\Pi,A\rangle \hookrightarrow \langle \textbf{\textit{CCE}},S,\Pi,A\rangle}$$

Figure 15. *Ptolemy*$_{\mathbb{S}}$'s exceptional dynamic semantics.

Ptolemy$_{\mathbb{S}}$ also supports standard object-oriented expressions for object creation, getting and setting the value of a field, if conditionals, etc. Their semantics can be found in our report [33].

B. Type Checking

In this section, we discuss *Ptolemy*$_{\mathbb{S}}$'s static semantics with the focus on event subtyping, the refining relation among greybox event specifications and the non-decreasing relation.

B.1 Type Attributes

Figure 16 defines the type attributes used in *Ptolemy*$_{\mathbb{S}}$'s typing rules. The type attribute OK shows that a higher level declaration type checks, whereas OK in c shows type checking in the context of a class c. Other type attributes ***var*** t and ***exp*** t show variables and expressions of type t, respectively. Variable and store typing environments Γ and Π, respectively, map variables and locations to their types. The typing judgment $\Gamma,\Pi \vdash e : \theta$ says that in the variable typing environment Γ and the store typing environment Π, the expression e has the type θ. *Ptolemy*$_{\mathbb{S}}$'s type checking rules use a fixed class table CT, which is a set of program's class and event type declarations. Top-level names in a program are distinct and inheritance relations on classes and events types are acyclic.

$\theta ::=$	type attributes
OK	program/top-level decl.
$\mid$ OK in c	method, binding
$\mid$ ***var*** t	var/formal/field
$\mid$ ***exp*** t	expression
$t ::= c \mid$ int $\mid$ bool	types
$\Gamma ::= \{var : t\}$	variable typing environment
$\Pi ::= \{loc : t\}$	store typing environment
$\Gamma,\Pi \vdash e : \theta$	typing judgement

Figure 16. Type attributes, based on [15].

B.2 Static Semantics Rules

Figure 17 shows select typing rules for *Ptolemy*$_{\mathbb{S}}$. The rest of *Ptolemy*$_{\mathbb{S}}$'s typing rules, which are mostly standard object-oriented rules can be found in our technical report [33].

The rule (T-EVENT) type checks the declaration of an event ev. Since ev extends another event ev', the rule ensures that ev is a valid subevent of ev', i.e. $ev \lll: ev'$, and its translucid contract refines the translucid contract of ev', i.e. $contract_{ev'} \trianglelefteq contract_{ev}$. The refinement of the translucid contract of ev' by the contract of ev is statically guaranteed by *Ptolemy*$_{\mathbb{S}}$'s specification inheritance [33]. (T-EVENT) also checks, using the auxiliary function *isClass*, that the return type and types of context variables of ev are valid class types. Figure 18 shows the auxiliary functions used in *Ptolemy*$_{\mathbb{S}}$'s typing rules. The auxiliary function *isClass* simply ensures that its parameter is a class declared in the class table CT.

(T-SUBEVENT) checks that an event ev is a valid subtype of event ev', regarding both width and depth subtyping. Width subtyping allows ev to declare context variables in addition to the context it inherits from its superevent ev', i.e. $contextsOf(ev') \subseteq contextsOf(ev)$. The auxiliary function *contextsOf* returns all the context variables of an event along with their types, including context inherited from all of its superevents. Depth subtyping allows ev to redeclare a context variable of its superevent ev'. To redeclare a context variable var_i of type t'_i, the redeclaring context variable must have the same name var_i and its type t_i must be a subtype of t'_i, i.e. $t_i \preccurlyeq t'_i$. Similar to class subtyping, event subtyping is a reflexive, transitive relation on event types, with a root event type ***Event***.

(T-SUBEVENT) also ensures that the return type of an event ev is a *supertype* of the return type of its superevent ev'. This is necessary for the non-decreasing relation on observers of an event and its superevent, which ensures that an observer of an event runs before an observer of its superevents. The auxiliary function *returnType* returns the return type of an event.

(T-ANNOUNCE) type checks an announce expression. It ensures that the type of a parameter expression e_i is a subtype of its corresponding context variable var_i, i.e. $t'_i \preccurlyeq t_i$. Recall that an event can inherit context variables from its superevents and the announce expression must provide values for all context variables of the event.

(T-ANNOUNCE) also ensures that the type of the event body e' is the same as the return type of the top event in the event inheritance hierarchy. The top event of an event in an inheritance hierarchy is the superevent of the event right before the root event ***Event***. For example, in Figure 2, the event `ExpEv` is the top event for `AndEv`. The auxiliary function *topEvent* returns the top event of an event. The relation between the return type of the event body and the the return type of its top event is necessary for the non-decreasing relation in which the event body runs as the last observer.

(T-EVENT)
$$\frac{\begin{array}{c}(c'\ \textbf{event}\ ev'\ \textbf{extends}\ ev''\ \{(t'\ var')^*\ contract_{ev'}\})\in CT\\ \Gamma,\Pi\vdash contract_{ev'}\trianglelefteq contract_{ev}\\ \vdash ev \ll: ev' \qquad isClass(c)\qquad \forall t_i\in t^*\ .\ isClass(t_i)\end{array}}{\vdash c\ \textbf{event}\ ev\ \textbf{extends}\ ev'\ \{(t\ var)^*\ contract_{ev}\}:\text{OK}}$$

(T-SUBEVENT)
$$\frac{\begin{array}{c}contextsOf(ev')\subseteq contextsOf(ev)\\ (t\ var)^* = contextsOf(ev)\qquad (t'\ var')^* = contextsOf(ev')\\ \forall\ (t_i\ var_i)\in(t\ var)^*,\ (t'_i\ var_i)\in(t'\ var')^*\ .\ t_i\preccurlyeq t'_i\\ returnType(ev')\preccurlyeq returnType(ev)\end{array}}{\vdash ev\ll: ev'}$$

(T-ANNOUNCE)
$$\frac{\begin{array}{c}(t\ var)^* = contextsOf(ev)\\ \forall e_i\in e^*,\ (t_i\ var_i)\in(t\ var)^*\ .\ \Gamma,\Pi\vdash e_i:\textbf{exp}\ t'_i\wedge t'_i\preccurlyeq t_i\\ c''\ \textbf{event}\ ev'\textbf{extends}\ \textbf{Event}\{\} = topEvent(ev)\\ c = returnType(ev)\qquad \Gamma,\Pi\vdash e':\textbf{exp}\ c''\end{array}}{\Gamma,\Pi\vdash\textbf{announce}\ ev\ (e^*)\ \{e'\}:\textbf{exp}\ c}$$

(T-BINDING)
$$\frac{\begin{array}{c}(c\ \textbf{event}\ ev\ \textbf{extends}\ ev'\ \{form^*\ contract_{ev}\})\in CT\\ contract_{ev} = \textbf{requires}\ p\ \textbf{assumes}\ \{se\}\ \textbf{ensures}\ q\\ (c\ m\ (\textbf{thunk}\ ev\ var)\ \{e\}) = methodBody(c',m)\qquad se\trianglelefteq e\end{array}}{\vdash\textbf{when}\ ev\ \textbf{do}\ m:\text{OK in }c'}$$

(T-INVOKE)
$$\frac{\begin{array}{c}c\ \textbf{event}\ ev\ \textbf{extends}\ ev'\ \{form^*\ \ contract_{ev}\}\in CT\\ \Gamma,\Pi\vdash e:\textbf{exp}\ \textbf{thunk}\ ev\end{array}}{\Gamma,\Pi\vdash e.\textbf{invoke}():\textbf{exp}\ c}$$

(T-REGISTER)
$$\frac{\Gamma,\Pi\vdash e:\textbf{exp}\ t}{\Gamma,\Pi\vdash\textbf{register}(e):\textbf{exp}\ t}$$

(T-UNEGISTER)
$$\frac{\Gamma,\Pi\vdash e:\textbf{exp}\ t}{\Gamma,\Pi\vdash\textbf{unregister}(e):\textbf{exp}\ t}$$

(T-EVALPOST)
$$\frac{\Gamma,\Pi\vdash e:\textbf{exp}\ t\qquad \Gamma,\Pi\vdash q:\textbf{exp}\ t_2}{\Gamma,\Pi\vdash\textbf{evalpost}\ e\ q:\textbf{exp}\ t}$$

(T-SPEC)
$$\frac{\Gamma,\Pi\vdash p:\textbf{exp}\ t_1\qquad \Gamma,\Pi\vdash q:\textbf{exp}\ t_2}{\Gamma,\Pi\vdash\textbf{requires}\ p\ \textbf{ensures}\ q\ :\textbf{exp}\ \bot}$$

(T-REFINING)
$$\frac{\begin{array}{c}spec = \textbf{requires}\ p\ \textbf{ensures}\ q\\ \Gamma,\Pi\vdash spec:\textbf{exp}\bot\qquad \Gamma,\Pi\vdash e:\textbf{exp}\ t\end{array}}{\Gamma,\Pi\vdash\textbf{refining}\ spec\ \{e\}:\textbf{exp}\ t}$$

(T-PROGRAM)
$$\frac{\forall decl\in decl^*\ .\ \ \vdash decl:\text{OK}\qquad \vdash e:\textbf{exp}\ t}{\vdash decl^*\ e:\textbf{exp}\ t}$$

(T-CLASS)
$$\frac{\begin{array}{c}\forall meth\in meth^*\ .\ \ \vdash meth:\text{OK in }c\\ \forall binding\in binding^*\ .\ \ \vdash binding:\text{OK in }c\\ isClass(d)\qquad \forall(t\ f)\in form^*\ .\ isClass(t)\wedge f\notin dom(fieldsOf(d))\end{array}}{\vdash\textbf{class}\ c\ \textbf{extends}\ d\ \{form^*\ meth^*\ binding^*\}:\text{OK}}$$

Figure 17. Select typing rules for *Ptolemy*$_{\mathbb{S}}$ [8, 24].

(T-BINDING) type checks a binding declaration. It ensures that the body *e* of the observer handler method *m* refines the assumes block *se* of the translucid contract of its event *ev*, i.e. $se \trianglelefteq e$, as defined in Figure 9. The auxiliary function *methodBody* returns the body of a method of a class defined in the class table *CT*. The rule also ensures that the return type of the observer handler method *m* is *the same* as the the return type of the event.

(T-INVOKE) type checks an invoke expression. The invoke expression invokes the next observer in the chain of observers. The chain of observers is included in the event closure receiver object *e*. The rule ensures that the event closure of an event *ev* is of type ***thunk*** *ev*. A thunk type marks the type of an event closure. The type of an invoke expression is the same as the return type *c* of its event *ev*. This is sound because the non-decreasing relation ensures that observers of an event run before observers of its superevent. Typing rules for register, unregister, specification, refining and evalpost expressions are intuitive.

$$\frac{\begin{array}{c}(c\ \textbf{event}\ ev\ \textbf{extends}\ ev'\ \{(t\ var)^*\ contract_{ev}\})\in CT\\ (t'\ var')^* = contextsOf(ev')\end{array}}{contextsOf(ev) = (t'\ var')^*\ \oplus\ (t\ var)^*}$$

$$contextsOf(\textbf{Event}) = \bullet$$

$$\frac{(c\ \textbf{event}\ ev\ \textbf{extends}\ ev'\ \{form^*\ contract_{ev}\})\in CT}{returnType(ev) = c}$$

$$\frac{(c\ \textbf{event}\ ev\ \textbf{extends}\ ev'\ \{form^*\ contract_{ev}\})\in CT}{isEvent(ev)}$$

$$\frac{\textbf{class}\ c\ \textbf{extends}\ d\{form^*\ meth^*\ binding^*\}\in CT}{isClass(c)}$$

$$\frac{t = \textbf{thunk}\ ev}{isThunkType(t)}\qquad\qquad \frac{isClass(t)\vee isThunkType(t)}{isType(t)}$$

$$\frac{\textbf{class}\ c\ \textbf{extends}\ d\{(t\ var)^*\ meth^*\ binding^*\}\in CT}{fieldsOf(c) = (var:t)^*}$$

$$\frac{\begin{array}{c}\textbf{class}\ c\ \textbf{extends}\ d\{form^*\ meth^*\ binding^*\}\in CT\\ (c''\ m\ (t\ var)^*\ \{e\})\in meth^*\end{array}}{methodBody(c,m) = (c''\ m\ (t\ var)^*\ \{e\})}$$

$$\frac{\begin{array}{c}\textbf{class}\ c\ \textbf{extends}\ d\{form^*\ meth^*\ binding^*\}\in CT\\ (c''\ m\ (t\ var)^*\ \{e\})\notin meth^*\end{array}}{methodBody(c,m) = methodBody(d,m)}$$

Figure 18. Select auxiliary functions for *Ptolemy*$_{\mathbb{S}}$'s typing rules, based on [8, 15].

B.3 Soundness of Type System

THEOREM B.1. *(Soundness of Ptolemy$_{\mathbb{S}}$'s Semantics) Ptolemy$_{\mathbb{S}}$'s semantics is sound regarding its progress and preservation [50].*

The proof follows standard progress and preservation arguments. Full proof of the theorem can be found in our report [33].