Practical Optional Types for Clojure

Ambrose Bonnaire-Sergeant†, Rowan Davies*, Sam Tobin-Hochstadt†

Indiana University†; Omnia Team, Commonwealth Bank of Australia*
{abonnair,samth}@indiana.edu, Rowan.Davies@cba.com.au

Abstract. Typed Clojure is an optional type system for Clojure, a dynamic language in the Lisp family that targets the JVM. Typed Clojure enables Clojure programmers to gain greater confidence in the correctness of their code via static type checking while remaining in the Clojure world, and has acquired significant adoption in the Clojure community. Typed Clojure repurposes Typed Racket's *occurrence typing*, an approach to statically reasoning about predicate tests, and also includes several new type system features to handle existing Clojure idioms.
In this paper, we describe Typed Clojure and present these type system extensions, focusing on three features widely used in Clojure. First, multimethods provide extensible operations, and their Clojure semantics turns out to have a surprising synergy with the underlying occurrence typing framework. Second, Java interoperability is central to Clojure's mission but introduces challenges such as ubiquitous `null`; Typed Clojure handles Java interoperability while ensuring the absence of null-pointer exceptions in typed programs. Third, Clojure programmers idiomatically use immutable dictionaries for data structures; Typed Clojure handles this with multiple forms of heterogeneous dictionary types. We provide a formal model of the Typed Clojure type system incorporating these and other features, with a proof of soundness. Additionally, Typed Clojure is now in use by numerous corporations and developers working with Clojure, and we present a quantitative analysis on the use of type system features in two substantial code bases.

1 Clojure with static typing

The popularity of dynamically-typed languages in software development, combined with a recognition that types often improve programmer productivity, software reliability, and performance, has led to the recent development of a wide variety of optional and gradual type systems aimed at checking existing programs written in existing languages. These include TypeScript [19] and Flow [11] for JavaScript, Hack [10] for PHP, and mypy [15] for Python among the optional systems, and Typed Racket [23], Reticulated Python [25], and GradualTalk [1] among gradually-typed systems.[1]

[1] We use "gradual typing" for systems like Typed Racket with sound interoperation between typed and untyped code; Typed Clojure or TypeScript which don't enforce type invariants we describe as "optionally typed".

```
(ann pname [(U File String) -> (U nil String)])
(defmulti pname class)  ; multimethod dispatching on class of argument
(defmethod pname String [s] (pname (new File s))) ; String case
(defmethod pname File [f] (.getName f)) ; File case, static null check
(pname "STAINS/JELLY") ;=> "JELLY" :- (U nil Str)
```

Fig. 1. A simple Typed Clojure program (delimiters: Java interoperation (green), type annotation (blue), function invocation (black), collection literal (red), other (gray))

One key lesson of these systems, indeed a lesson known to early developers of optional type systems such as StrongTalk, is that type systems for existing languages must be designed to work with the features and idioms of the target language. Often this takes the form of a core language, be it of functions or classes and objects, together with extensions to handle distinctive language features.

We synthesize these lessons to present *Typed Clojure*, an optional type system for Clojure. Clojure is a dynamically typed language in the Lisp family—built on the Java Virtual Machine (JVM)—which has recently gained popularity as an alternative JVM language. It offers the flexibility of a Lisp dialect, including macros, emphasizes a functional style via immutable data structures, and provides interoperability with existing Java code, allowing programmers to use existing Java libraries without leaving Clojure. Since its initial release in 2007, Clojure has been widely adopted for "backend" development in places where its support for parallelism, functional programming, and Lisp-influenced abstraction is desired on the JVM. As a result, there is an extensive base of existing untyped programs whose developers can benefit from Typed Clojure, an experience we discuss in this paper.

Since Clojure is a language in the Lisp family, we apply the lessons of Typed Racket, an existing gradual type system for Racket, to the core of Typed Clojure, consisting of an extended λ-calculus over a variety of base types shared between all Lisp systems. Furthermore, Typed Racket's *occurrence typing* has proved necessary for type checking realistic Clojure programs.

However, Clojure goes beyond Racket in many ways, requiring several new type system features which we detail in this paper. Most significantly, Clojure supports, and Clojure developers use, **multimethods** to structure their code in extensible fashion. Furthermore, since Clojure is an untyped language, dispatch within multimethods is determined by application of dynamic predicates to argument values. Fortunately, the dynamic dispatch used by multimethods has surprising symmetry with the conditional dispatch handled by occurrence typing. Typed Clojure is therefore able to effectively handle complex and highly dynamic dispatch as present in existing Clojure programs.

But multimethods are not the only Clojure feature crucial to type checking existing programs. As a language built on the Java Virtual Machine, Clojure provides flexible and transparent access to existing Java libraries, and **Clojure/Java interoperation** is found in almost every significant Clojure code

base. Typed Clojure therefore builds in an understanding of the Java type system and handles interoperation appropriately. Notably, `null` is a distinct type in Typed Clojure, designed to automatically rule out null-pointer exceptions.

An example of these features is given in Figure 1. Here, the `pname` multimethod dispatches on the `class` of the argument—for `String`s, the first method implementation is called, for `File`s, the second. The `String` method calls a `File` constructor, returning a non-nil `File` instance—the `getName` method on `File` requires a non-nil target, returning a nilable type.

Finally, flexible, high-performance immutable dictionaries are the most common Clojure data structure. Simply treating them as uniformly-typed key-value mappings would be insufficient for existing programs and programming styles. Instead, Typed Clojure provides a flexible **heterogenous map** type, in which specific entries can be specified.

While these features may seem disparate, they are unified in important ways. First, they leverage the type system mechanisms inherited from Typed Racket—multimethods when using dispatch via predicates, Java interoperation for handling `null` tests, and heterogenous maps using union types and reasoning about subcomponents of data. Second, they are crucial features for handling Clojure code in practice. Typed Clojure's use in real Clojure deployments would not be possible without effective handling of these three Clojure features.

Our main contributions are as follows:

1. We motivate and describe Typed Clojure, an optional type system for Clojure that understands existing Clojure idioms.
2. We present a sound formal model for three crucial type system features: multi-methods, Java interoperability, and heterogenous maps.
3. We evaluate the use of Typed Clojure features on existing Typed Clojure code, including both open source and in-house systems.

The remainder of this paper begins with an example-driven presentation of the main type system features in Section 2. We then incrementally present a core calculus for Typed Clojure covering all of these features together in Section 3 and prove type soundness (Section 4). We then present an empirical analysis of significant code bases written in `core.typed`—the full implementation of Typed Clojure—in Section 5. Finally, we discuss related work and conclude.

2 Overview of Typed Clojure

We now begin a tour of the central features of Typed Clojure, beginning with Clojure itself. Our presentation uses the full Typed Clojure system to illustrate key type system ideas,[2] before studying the core features in detail in Section 3.

[2] Full examples: `https://github.com/typedclojure/esop16`

2.1 Clojure

Clojure [13] is a Lisp that runs on the Java Virtual Machine with support for concurrent programming and immutable data structures in a mostly-functional style. Clojure provides easy interoperation with existing Java libraries, with Java values being like any other Clojure value. However, this smooth interoperability comes at the cost of pervasive `null`, which leads to the possibility of null pointer exceptions—a drawback we address in Typed Clojure.

2.2 Typed Clojure

A simple one-argument function `greet` is annotated with `ann` to take and return strings.

```
(ann  greet [Str -> Str])
(defn greet [n] (str "Hello, " n "!"))
(greet "Grace") ;=> "Hello, Grace!" :- Str
```

Providing `nil` (exactly Java's `null`) is a static type error—`nil` is not a string.

```
(greet nil) ; Type Error: Expected Str, given nil
```

Unions To allow `nil`, we use *ad-hoc unions* (`nil` and `false` are logically false).

```
(ann  greet-nil [(U nil Str) -> Str])
(defn greet-nil [n] (str "Hello" (when n (str ", " n)) "!"))
(greet-nil "Donald") ;=> "Hello, Donald!" :- Str
(greet-nil nil)      ;=> "Hello!"         :- Str
```

Typed Clojure prevents well-typed code from dereferencing `nil`.

Flow analysis Occurrence typing [24] models type-based control flow. In `greetings`, a branch ensures `repeat` is never passed `nil`.

```
(ann  greetings [Str (U nil Int) -> Str])
(defn greetings [n i]
  (str "Hello, " (when i (apply str (repeat i "hello, "))) n "!"))
(greetings "Donald" 2)  ;=> "Hello, hello, hello, Donald!" :- Str
(greetings "Grace" nil) ;=> "Hello, Grace!"                :- Str
```

Removing the branch is a static type error—`repeat` cannot be passed `nil`.

```
(ann  greetings-bad [Str (U nil Int) -> Str])
(defn greetings-bad [n i]           ; Expected Int, given (U nil Int)
  (str "Hello, " (apply str (repeat i "hello, ")) n "!"))
```

2.3 Java interoperability

Clojure can interact with Java constructors, methods, and fields. This program calls the `getParent` on a constructed `File` instance, returning a nullable string.

```
(.getParent (new File "a/b"))  ;=> "a" :- (U nil Str)
```

Example 1

Typed Clojure can integrate with the Clojure compiler to avoid expensive reflective calls like `getParent`, however if a specific overload cannot be found based on the surrounding static context, a type error is thrown.

```
(fn [f] (.getParent f)) ; Type Error: Unresolved interop: getParent
```

Function arguments default to `Any`, which is similar to a union of all types. Ascribing a parameter type allows Typed Clojure to find a specific method.

```
(ann parent [(U nil File) -> (U nil Str)])
(defn parent [f] (if f (.getParent f) nil))
```

Example 2

The conditional guards from dereferencing `nil`, and—as before—removing it is a static type error, as typed code could possibly dereference `nil`.

```
(defn parent-bad-in [f :- (U nil File)]
  (.getParent f)) ; Type Error: Cannot call instance method on nil.
```

Typed Clojure rejects programs that assume methods cannot return `nil`.

```
(defn parent-bad-out [f :- File] :- Str
  (.getParent f)) ; Type Error: Expected Str, given (U nil Str).
```

Method targets can never be `nil`. Typed Clojure also prevents passing `nil` as Java method or constructor arguments by default—this restriction can be adjusted per method.

In contrast, JVM invariants guarantee constructors return non-null.[3]

```
(parent (new File s))
```

Example 3

2.4 Multimethods

Multimethods are a kind of extensible function—combining a *dispatch function* with one or more *methods*—widely used to define Clojure operations.

Value-based dispatch This simple multimethod takes a keyword (`Kw`) and says hello in different languages.

```
(ann hi [Kw -> Str]) ; multimethod type
(defmulti hi identity) ; dispatch function `identity`
(defmethod hi :en [_] "hello") ; method for `:en`
(defmethod hi :fr [_] "bonjour") ; method for `:fr`
(defmethod hi :default [_] "um...") ; default method
```

Example 4

[3] `http://docs.oracle.com/javase/specs/jls/se7/html/jls-15.html#jls-15.9.4`

When invoked, the arguments are first supplied to the dispatch function—`identity`—yielding a *dispatch value*. A method is then chosen based on the dispatch value, to which the arguments are then passed to return a value.

```
(map hi [:en :fr :bocce]) ;=> ("hello" "bonjour" "um...")
```

For example, `(hi :en)` evaluates to *"hello"*—it executes the `:en` method because `(= (identity :en) :en)` is true and `(= (identity :en) :fr)` is false.

Dispatching based on literal values enables certain forms of method definition, but this is only part of the story for multimethod dispatch.

Class-based dispatch For class values, multimethods can choose methods based on subclassing relationships. Recall the multimethod from Figure 1. The dispatch function `class` dictates whether the `String` or `File` method is chosen. The multimethod dispatch rules use `isa?`, a hybrid predicate which is both a subclassing check for classes and an equality check for other values.

```
(isa? :en :en)       ;=> true
(isa? String Object) ;=> true
```

The current dispatch value and—in turn—each method's associated dispatch value is supplied to `isa?`. If exactly one method returns true, it is chosen. For example, the call `(pname "STAINS/JELLY")` picks the `String` method because `(isa? String String)` is true, and `(isa? String File)` is not.

2.5 Heterogeneous hash-maps

The most common way to represent compound data in Clojure are immutable hash-maps, typically with keyword keys. Keywords double as functions that look themselves up in a map, or return `nil` if absent.

Example 5

```
(def breakfast {:en "waffles" :fr "croissants"})
(:en breakfast)    ;=> "waffles" :- Str
(:bocce breakfast) ;=> nil       :- nil
```

HMap types describe the most common usages of keyword-keyed maps.

```
breakfast ; :- (HMap :mandatory {:en Str, :fr Str}, :complete? true)
```

This says `:en` and `:fr` are known entries mapped to strings, and the map is fully specified—that is, no other entries exist—by `:complete?` being `true`.

HMap types default to partial specification, with `'{:en Str :fr Str}` abbreviating `(HMap :mandatory {:en Str, :fr Str})`.

Example 6

```
(ann lunch '{:en Str :fr Str})
(def lunch {:en "muffin" :fr "baguette"})
(:bocce lunch) ;=> nil :- Any ; less accurate type
```

HMaps in practice The next example is extracted from a production system at CircleCI, a company with a large production Typed Clojure system (Section 5.2 presents a case study and empirical result from this code base).

Example 7

```
(defalias RawKeyPair ; extra keys disallowed
  (HMap :mandatory {:pub RawKey, :priv RawKey},
        :complete? true))
(defalias EncKeyPair ; extra keys disallowed
  (HMap :mandatory {:pub RawKey, :enc-priv EncKey}, :complete? true))

(ann enc-keypair [RawKeyPair -> EncKeyPair])
(defn enc-keypair [kp]
  (assoc (dissoc kp :priv) :enc-priv (encrypt (:priv kp))))
```

As `EncKeyPair` is fully specified, we remove extra keys like `:priv` via `dissoc`, which returns a new map that is the first argument without the entry named by the second argument. Notice removing `dissoc` causes a type error.

```
(defn enc-keypair-bad [kp] ; Type error: :priv disallowed
  (assoc kp :enc-priv (encrypt (:priv kp))))
```

2.6 HMaps and multimethods, joined at the hip

HMaps and multimethods are the primary ways for representing and dispatching on data respectively, and so are intrinsically linked. As type system designers, we must search for a compositional approach that can anticipate any combination of these features.

Thankfully, occurrence typing, originally designed for reasoning about `if` tests, provides the compositional approach we need. By extending the system with a handful of rules based on HMaps and other functions, we can automatically cover both easy cases and those that compose rules in arbitrary ways.

Futhermore, this approach extends to multimethod dispatch by reusing occurrence typing's approach to conditionals and encoding a small number of rules to handle the `isa?`-based dispatch. In practice, conditional-based control flow typing extends to multimethod dispatch, and vice-versa.

We first demonstrate a very common, simple dispatch style, then move on to deeper structural dispatching where occurrence typing's compositionality shines.

HMaps and unions Partially specified HMap's with a common dispatch key combine naturally with ad-hoc unions. An `Order` is one of three kinds of HMaps.

```
(defalias Order "A meal order, tracking dessert quantities."
  (U '{:Meal ':lunch, :desserts Int} '{:Meal ':dinner :desserts Int}
     '{:Meal ':combo :meal1 Order :meal2 Order}))
```

The `:Meal` entry is common to each HMap, always mapped to a known keyword singleton type. It's natural to dispatch on the `class` of an instance—it's similarly natural to dispatch on a known entry like `:Meal`.

Example 8

```
(ann desserts [Order -> Int])
(defmulti desserts :Meal)  ; dispatch on :Meal entry
(defmethod desserts :lunch [o] (:desserts o))
(defmethod desserts :dinner [o] (:desserts o))
(defmethod desserts :combo [o]
  (+ (desserts (:meal1 o)) (desserts (:meal2 o))))

(desserts {:Meal :combo, :meal1 {:Meal :lunch :desserts 1},
           :meal2 {:Meal :dinner :desserts 2}}) ;=> 3
```

The `:combo` method is verified to only structurally recur on `Order`s. This is achieved because we learn the argument `o` must be of type `'{:Meal :combo}` since `(isa? (:Meal o) :combo)` is true. Combining this with the fact that `o` is an `Order` eliminates possibility of `:lunch` and `:dinner` orders, simplifying `o` to `'{:Meal ':combo :meal1 Order :meal2 Order}` which contains appropriate arguments for both recursive calls.

Nested dispatch A more exotic dispatch mechanism for `desserts` might be on the `class` of the `:desserts` key. If the result is a number, then we know the `:desserts` key is a number, otherwise the input is a `:combo` meal. We have already seen dispatch on `class` and on keywords in isolation—occurrence typing automatically understands control flow that combines its simple building blocks.

The first method has dispatch value `Long`, a subtype of `Int`, and the second method has `nil`, the sentinel value for a failed map lookup. In practice, `:lunch` and `:dinner` meals will dispatch to the `Long` method, but Typed Clojure infers a slightly more general type due to the definition of `:combo` meals.

Example 9

```
(ann desserts' [Order -> Int])
(defmulti desserts'
  (fn [o :- Order] (class (:desserts o))))
(defmethod desserts' Long [o]
;o :- (U '{:Meal (U ':dinner ':lunch), :desserts Int}
;        '{:Meal ':combo, :desserts Int, :meal1 Order, :meal2 Order})
  (:desserts o))
(defmethod desserts' nil [o]
  ; o :- '{:Meal ':combo, :meal1 Order, :meal2 Order}
  (+ (desserts' (:meal1 o)) (desserts' (:meal2 o))))
```

In the `Long` method, Typed Clojure learns that its argument is at least of type `'{:desserts Long}`—since `(isa? (class (:desserts o)) Long)` must be true. Here the `:desserts` entry *must* be present and mapped to a `Long`—even in a `:combo` meal, which does not specify `:desserts` as present or absent.

In the `nil` method, `(isa? (class (:desserts o)) nil)` must be true—which implies `(class (:desserts o))` is `nil`. Since lookups on missing keys return `nil`, either

- `o` has a `:desserts` entry to `nil`, like `desserts nil:desserts nil`, or
- `o` is missing a `:desserts` entry.

We can express this type with the `:absent-keys` HMap option

```
(U '{:desserts nil} (HMap :absent-keys #{:desserts}))
```

This eliminates non-`:combo` meals since their `'{:desserts Int}` type does not agree with this new information (because `:desserts` is neither `nil` or absent).

From multiple to arbitrary dispatch Clojure multimethod dispatch, and Typed Clojure's handling of it, goes even further, supporting dispatch on multiple arguments via vectors. Dispatch on multiple arguments is beyond the scope of this paper, but the same intuition applies—adding support for multiple dispatch admits arbitrary combinations and nestings of it and previous dispatch rules.

3 A Formal Model of λ_{TC}

After demonstrating the core features of Typed Clojure, we link them together in a formal model called λ_{TC}. Building on occurrence typing, we incrementally add each novel feature of Typed Clojure to the formalism, interleaving presentation of syntax, typing rules, operational semantics, and subtyping.

3.1 Core type system

We start with a review of occurrence typing [24], the foundation of λ_{TC}.

Expressions Syntax is given in Figure 2. Expressions e include variables x, values v, applications, abstractions, conditionals, and let expressions. All binding forms introduce fresh variables—a subtle but important point since our type environments are not simply dictionaries. Values include booleans b, nil, class literals C, keywords k, integers n, constants c, and strings s. Lexical closures $[\rho, \lambda x^{\tau}.e]_{\mathsf{c}}$ close value environments ρ—which map bindings to values—over functions.

Types Types σ or τ include the top type $\top$, *untagged* unions ($\bigcup\ \overrightarrow{\tau}$), singletons ($\mathbf{Val}\, l$), and class instances C. We abbreviate the classes **Boolean** to **B**, **Keyword** to **K**, **Nat** to **N**, **String** to **S**, and **File** to **F**. We also abbreviate the types ($\bigcup$) to $\bot$, ($\mathbf{Val}\,\mathsf{nil}$) to **nil**, ($\mathbf{Val}\,\mathsf{true}$) to **true**, and ($\mathbf{Val}\,\mathsf{false}$) to **false**. The difference between the types ($\mathbf{Val}\, C$) and C is subtle. The former is inhabited by class literals like **K** and the result of (class :a)—the latter by *instances* of classes, like a keyword literal :a, an instance of the type **K**. Function types $x{:}\sigma \xrightarrow[o]{\psi|\psi} \tau$ contain *latent* (terminology from [17]) propositions ψ, object o, and return type τ, which may refer to the function argument x. They are instantiated with the actual object of the argument in applications.

$$
\begin{array}{lll}
e & ::= x \mid v \mid (e\ e) \mid \lambda x^{\tau}.e \mid (\text{if } e\ e\ e) \mid (\text{let } [x\ e]\ e) & \text{Expressions} \\
v & ::= l \mid n \mid c \mid s \mid [\rho, \lambda x^{\tau}.e]_{\mathsf{c}} & \text{Values} \\
c & ::= \mathit{class} \mid n? & \text{Constants} \\
\sigma, \tau & ::= \top \mid (\bigcup\ \overrightarrow{\tau}) \mid x{:}\tau \xrightarrow[o]{\psi \mid \psi} \tau \mid (\mathbf{Val}\, l) \mid C & \text{Types} \\
l & ::= k \mid C \mid \mathsf{nil} \mid b & \text{Value types} \\
b & ::= \mathsf{true} \mid \mathsf{false} & \text{Boolean values} \\
\\
\psi & ::= \tau_{\pi(x)} \mid \overline{\tau}_{\pi(x)} \mid \psi \supset \psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid \mathbb{tt} \mid \mathbb{ff} & \text{Propositions} \\
o & ::= \pi(x) \mid \emptyset & \text{Objects} \\
\pi & ::= \overrightarrow{pe} & \text{Paths} \\
pe & ::= \mathbf{class} \mid \mathbf{key}_k & \text{Path elements} \\
\\
\Gamma & ::= \overrightarrow{\psi} & \text{Proposition environments} \\
\rho & ::= \{\overrightarrow{x \mapsto v}\} & \text{Value environments}
\end{array}
$$

Fig. 2. Syntax of Terms, Types, Propositions and Objects

Objects Each expression is associated with a symbolic representation called an *object*. For example, variable m has object m; $(\mathbf{class}\,(:\mathsf{lunch}\ m))$ has object $\mathbf{class}(\mathbf{key}_{:\mathsf{lunch}}(m))$; and 42 has the *empty* object $\emptyset$ since it is unimportant in our system. Figure 2 gives the syntax for objects o—non-empty objects $\pi(x)$ combine of a root variable x and a *path* π, which consists of a possibly-empty sequence of *path elements* (pe) applied right-to-left from the root variable. We use two path elements—**class** and $\mathbf{key}_k$—representing the results of calling *class* and looking up a keyword k, respectively.

Propositions with a logical system In standard type systems, association lists often track the types of variables, like in LC-Let and LC-Local.

$$
\text{LC-Let}\ \frac{\Gamma \vdash e_1 : \sigma \qquad \Gamma, x \mapsto \sigma \vdash e_2 : \tau}{\Gamma \vdash (\text{let } [x\ e_1]\ e_2) : \tau} \qquad \text{LC-Local}\ \frac{\Gamma(x) = \tau}{\Gamma \vdash x : \tau}
$$

Occurrence typing instead pairs *logical formulas*, that can reason about arbitrary non-empty objects, with a *proof system*. The logical statement σ_x says variable x is of type σ.

$$
\text{T0-Let}\ \frac{\Gamma \vdash e_1 : \sigma \qquad \Gamma, \sigma_x \vdash e_2 : \tau}{\Gamma \vdash (\text{let } [x\ e_1]\ e_2) : \tau} \qquad \text{T0-Local}\ \frac{\Gamma \vdash \tau_x}{\Gamma \vdash x : \tau}
$$

In T0-Local, $\Gamma \vdash \tau_x$ appeals to the proof system to solve for τ.

We further extend logical statements to *propositional logic*. Figure 2 describes the syntax for propositions ψ, consisting of positive and negative *type propositions* about non-empty objects—$\tau_{\pi(x)}$ and $\overline{\tau}_{\pi(x)}$ respectively—the latter pronounced "the object $\pi(x)$ is *not* of type τ". The other propositions are standard

$$\textsc{T-Local}\ \frac{\Gamma \vdash \tau_x \quad \sigma = (\cup\ \mathbf{nil}\ \mathbf{false})}{\Gamma \vdash x : \tau\ ;\ \overline{\sigma}_x|\sigma_x\ ;\ x}$$

$$\textsc{T-Abs}\ \frac{\Gamma, \sigma_x \vdash e \Rightarrow e' : \sigma'\ ;\ \psi_+|\psi_-\ ;\ o \quad \tau = x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \sigma'}{\Gamma \vdash \lambda x^\sigma.e \Rightarrow \lambda x^\sigma.e' : \tau\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

$$\textsc{T-If}\ \frac{\begin{array}{c}\Gamma \vdash e_1 \Rightarrow e_1' : \tau_1\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1 \\ \Gamma, \psi_{1+} \vdash e_2 \Rightarrow e_2' : \tau\ ;\ \psi_+|\psi_-\ ;\ o \\ \Gamma, \psi_{1-} \vdash e_3 \Rightarrow e_3' : \tau\ ;\ \psi_+|\psi_-\ ;\ o \\ e' = (\text{if}\ e_1'\ e_2'\ e_3')\end{array}}{\Gamma \vdash (\text{if}\ e_1\ e_2\ e_3) \Rightarrow e' : \tau\ ;\ \psi_+|\psi_-\ ;\ o}$$

$$\textsc{T-Kw}\ \frac{}{\Gamma \vdash k : (\mathbf{Val}\,k)\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset} \qquad \textsc{T-Num}\ \frac{}{\Gamma \vdash n : \mathbf{N}\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

$$\textsc{T-Nil}\ \frac{}{\Gamma \vdash \mathsf{nil} : \mathbf{nil}\ ;\ \mathtt{ff}|\mathtt{tt}\ ;\ \emptyset} \qquad \textsc{T-False}\ \frac{}{\Gamma \vdash \mathsf{false} : \mathbf{false}\ ;\ \mathtt{ff}|\mathtt{tt}\ ;\ \emptyset}$$

$$\textsc{T-Const}\ \frac{}{\Gamma \vdash c : \delta_\tau(c)\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset} \qquad \textsc{T-True}\ \frac{}{\Gamma \vdash \mathsf{true} : \mathbf{true}\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

$$\textsc{T-Str}\ \frac{}{\Gamma \vdash s : \mathbf{S}\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset} \qquad \textsc{T-Class}\ \frac{}{\Gamma \vdash C : (\mathbf{Val}\,C)\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

$$\textsc{T-Let}\ \frac{\begin{array}{c}\Gamma \vdash e_1 \Rightarrow e_1' : \sigma\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1 \qquad \psi' = \overline{(\cup\ \mathbf{nil}\ \mathbf{false})}_x \supset \psi_{1+} \\ \psi'' = (\cup\ \mathbf{nil}\ \mathbf{false})_x \supset \psi_{1-} \qquad \Gamma, \sigma_x, \psi', \psi'' \vdash e_2 \Rightarrow e_2' : \tau\ ;\ \psi_+|\psi_-\ ;\ o\end{array}}{\Gamma \vdash (\text{let}\ [x\ e_1]\ e_2) \Rightarrow (\text{let}\ [x\ e_1']\ e_2') : \tau[o_1/x]\ ;\ \psi_+|\psi_-[o_1/x]\ ;\ o[o_1/x]}$$

$$\textsc{T-App}\ \frac{\Gamma \vdash e \Rightarrow e_1 : x{:}\sigma \xrightarrow[o_f]{\psi_{f+}|\psi_{f-}} \tau\ ;\ \psi_+|\psi_-\ ;\ o \quad \Gamma \vdash e' \Rightarrow e_1' : \sigma\ ;\ \psi'_+|\psi'_-\ ;\ o'}{\Gamma \vdash (e\ e') \Rightarrow (e_1\ e_1') : \tau[o'/x]\ ;\ \psi_{f+}|\psi_{f-}[o'/x]\ ;\ o_f[o'/x]}$$

$$\textsc{T-Subsume}\ \frac{\Gamma \vdash e \Rightarrow e' : \tau\ ;\ \psi_+|\psi_-\ ;\ o \quad \Gamma, \psi_+ \vdash \psi'_+ \quad \Gamma, \psi_- \vdash \psi'_- \quad \vdash \tau <: \tau' \quad \vdash o <: o'}{\Gamma \vdash e \Rightarrow e' : \tau'\ ;\ \psi'_+|\psi'_-\ ;\ o'}$$

Fig. 3. Core typing rules

logical connectives: implications, conjunctions, disjunctions, and the trivial ($\mathtt{tt}$) and impossible ($\mathtt{ff}$) propositions. The full proof system judgement $\Gamma \vdash \psi$ says *proposition environment* Γ proves proposition ψ.

Each expression is associated with two propositions—when expression e_1 is in test position like (if e_1 e_2 e_3), the type system extracts e_1's 'then' and 'else' proposition to check e_2 and e_3 respectively. For example, in (if o e_2 e_3) we learn variable o is true in e_2 via o's 'then' proposition $\overline{(\cup\ \mathbf{nil}\ \mathbf{false})}_o$, and that o is false in e_3 via o's 'else' proposition $(\cup\ \mathbf{nil}\ \mathbf{false})_o$.

To illustrate, recall Example 8. The parameter o is of type **Order**, written $\mathbf{Order}_o$ as a proposition. In the :combo method, we know (:Meal o) is :combo, based on multimethod dispatch rules. This is written $(\mathbf{Val}\,\mathsf{:combo})_{\mathbf{key}_{\mathsf{:Meal}}(o)}$, pronounced "the :Meal path of variable o is of type (**Val** :combo)".

To attain the type of o, we must solve for τ in $\Gamma \vdash \tau_o$, under proposition environment $\Gamma = \mathbf{Order}_o, (\mathbf{Val}\,\mathsf{:combo})_{\mathbf{key}_{\mathsf{:Meal}}(o)}$ which deduces τ to be a :combo meal. The logical system *combines* pieces of type information to deduce more accurate types for lexical bindings—this is explained in Section 3.6.

$$\frac{\exists i.\ \vdash \tau <: \sigma_i}{\vdash \tau <: (\bigcup\ \overrightarrow{\sigma}^i)}\ \text{S-UnionSuper} \qquad \frac{\overrightarrow{\vdash \tau_i <: \sigma}^i}{\vdash (\bigcup\ \overrightarrow{\tau}^i) <: \sigma}\ \text{S-UnionSub} \qquad \vdash x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau <: \mathbf{Fn}\ \text{S-FunMono}$$

$$\vdash C <: \mathbf{Object}\ \text{S-Object} \qquad \vdash (\mathbf{Val}\, C) <: \mathbf{Class}\ \text{S-SClass} \qquad \vdash (\mathbf{Val}\, b) <: \mathbf{B}\ \text{S-SBool}$$

$$\frac{\vdash \sigma' <: \sigma \qquad \vdash \tau <: \tau' \qquad \psi_+ \vdash {\psi'}_+ \qquad \psi_- \vdash {\psi'}_- \qquad \vdash o <: o'}{\vdash x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau <: x{:}\sigma' \xrightarrow[o']{{\psi'}_+|{\psi'}_-} \tau'}\ \text{S-Fun}$$

$$\vdash \tau <: \tau\ \text{S-Refl} \qquad \vdash \tau <: \top\ \text{S-Top} \qquad \vdash (\mathbf{Val}\, k) <: \mathbf{K}\ \text{S-SKw}$$

Fig. 4. Core subtyping rules

$$\frac{\rho \vdash e_1 \Downarrow v_1 \qquad v_1 \neq \mathsf{false} \qquad v_1 \neq \mathsf{nil} \qquad \rho \vdash e_2 \Downarrow v}{\rho \vdash (\mathrm{if}\ e_1\ e_2\ e_3) \Downarrow v}\ \text{B-IfTrue}$$

$$\frac{\rho \vdash e_1 \Downarrow \mathsf{false} \ \text{ or } \ \rho \vdash e_1 \Downarrow \mathsf{nil} \qquad \rho \vdash e_3 \Downarrow v}{\rho \vdash (\mathrm{if}\ e_1\ e_2\ e_3) \Downarrow v}\ \text{B-IfFalse}$$

Fig. 5. Select core semantics

Typing judgment We formalize our system following Tobin-Hochstadt and Felleisen [24]. The typing judgment $\Gamma \vdash e \Rightarrow e' : \tau\ ;\ \psi_+|\psi_-\ ;\ o$ says expression e rewrites to e', which is of type τ in the proposition environment Γ, with 'then' proposition ψ_+, 'else' proposition ψ_- and object o.

We write $\Gamma \vdash e \Rightarrow e' : \tau$ to mean $\Gamma \vdash e \Rightarrow e' : \tau\ ;\ {\psi'}_+|{\psi'}_-\ ;\ o'$ for some ${\psi'}_+$, ${\psi'}_-$ and o', and abbreviate self rewriting judgements $\Gamma \vdash e \Rightarrow e : \tau\ ;\ \psi_+|\psi_-\ ;\ o$ to $\Gamma \vdash e : \tau\ ;\ \psi_+|\psi_-\ ;\ o$.

Typing rules The core typing rules are given as Figure 3. We introduce the interesting rules with the complement number predicate as a running example.

$$\lambda d^{\top}.(\mathrm{if}\ (n?\ d)\ \mathsf{false}\ \mathsf{true}) \tag{1}$$

The lambda rule T-Abs introduces $\sigma_x = \top_d$ to check the body. With $\Gamma = \top_d$, T-If first checks the test $e_1 = (n?\ d)$ via the T-App rule, with three steps.

First, in T-App the operator $e = n?$ is checked with T-Const, which uses δ_τ (Figure 7, dynamic semantics in the supplemental material) to type constants. $n?$ is a predicate over numbers, and *class* returns its argument's class.

Resuming $(n?\ d)$, in T-App the operand $e' = d$ is checked with T-Local as

$$\Gamma \vdash d : \top\ ;\ \overline{(\cup\ \mathbf{nil}\ \mathbf{false})}_d|(\cup\ \mathbf{nil}\ \mathbf{false})_d\ ;\ d \tag{2}$$

which encodes the type, proposition, and object information about variables. The proposition $\overline{(\cup\ \mathbf{nil}\ \mathbf{false})}_d$ says "it is not the case that variable d is of type $(\cup\ \mathbf{nil}\ \mathbf{false})$"; $(\cup\ \mathbf{nil}\ \mathbf{false})_d$ says "d is of type $(\cup\ \mathbf{nil}\ \mathbf{false})$".

Finally, the T-App rule substitutes the operand's object o' for the parameter x in the latent type, propositions, and object. The proposition $\mathbf{N}_{\,d}$ says "d is of type $\mathbf{N}$"; $\overline{\mathbf{N}}_{\,d}$ says "it is not the case that d is of type $\mathbf{N}$". The object d is the symbolic representation of what the expression d evaluates to.

$$\Gamma \vdash (n?\ d) : \mathbf{B}\ ;\ \mathbf{N}_{\,d}|\overline{\mathbf{N}}_{\,d}\ ;\ \emptyset \tag{3}$$

To demonstrate, the 'then' proposition—in T-App $\psi_+[o'/x]$—substitutes the latent 'then' proposition of $\delta_\tau(n?)$ with d, giving $\mathbf{N}_{\,x}[d/x] = \mathbf{N}_{\,d}$.

To check the branches of (if $(n?\ d)$ false true), T-If introduces $\psi_{1+} = \mathbf{N}_{\,d}$ to check $e_2 = \mathsf{false}$, and $\psi_{1-} = \overline{\mathbf{N}}_{\,d}$ to check $e_3 = \mathsf{true}$. The branches are first checked with T-False and T-True respectively, the T-Subsume premises $\Gamma, \psi_+ \vdash \psi'_+$ and $\Gamma, \psi_- \vdash \psi'_-$ allow us to pick compatible propositions for both branches.

$$\Gamma, \mathbf{N}_{\,d} \vdash \mathsf{false} : \mathbf{B}\ ;\ \overline{\mathbf{N}}_{\,d}|\mathbf{N}_{\,d}\ ;\ \emptyset$$
$$\Gamma, \overline{\mathbf{N}}_{\,d} \vdash \mathsf{true} : \mathbf{B}\ ;\ \overline{\mathbf{N}}_{\,d}|\mathbf{N}_{\,d}\ ;\ \emptyset$$

Finally T-Abs assigns a type to the overall function:

$$\vdash \lambda d^{\top}.(\text{if } (n?\ d)\ \mathsf{false}\ \mathsf{true}) : d{:}\top \xrightarrow[\emptyset]{\overline{\mathbf{N}}_{\,d}|\mathbf{N}_{\,d}} \mathbf{B}\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset$$

Subtyping Figure 4 presents subtyping as a reflexive and transitive relation with top type $\top$. Singleton types are instances of their respective classes—boolean singleton types are of type $\mathbf{B}$, class literals are instances of **Class** and keywords are instances of $\mathbf{K}$. Instances of classes C are subtypes of **Object**. Function types are subtypes of **Fn**. All types except for **nil** are subtypes of **Object**, so $\top$ is similar to $(\bigcup$ **nil Object**$)$. Function subtyping is contravariant left of the arrow—latent propositions, object and result type are covariant. Subtyping for untagged unions is standard.

Operational semantics We define the dynamic semantics for λ_{TC} in a big-step style using an environment, following [24]. We include both errors and a *wrong* value, which is provably ruled out by the type system. The main judgment is $\rho \vdash e \Downarrow \alpha$ which states that e evaluates to answer α in environment ρ. We chose to omit the core rules (included in supplemental material) however a notable difference is nil is a false value, which affects the semantics of if (Figure 5).

3.2 Java Interoperability

We present Java interoperability in a restricted setting without class inheritance, overloading or Java Generics. We extend the syntax in Figure 6 with Java field lookups and calls to methods and constructors. To prevent ambiguity between zero-argument methods and fields, we use Clojure's primitive "dot" syntax: field accesses are written $(.\ e\ fld)$ and method calls $(.\ e\ (mth\ \overrightarrow{e}))$.

In Example 1, `(.getParent (new File "a/b"))` translates to

$$(.\ (\text{new}\ \ \mathbf{F}\ \text{“}\mathsf{a/b}\text{”})\ (\text{getParent})) \tag{4}$$

$$
\begin{array}{lll}
e & ::= \ldots \mid (.\ e\ fld) \mid (.\ e\ (mth\ \overrightarrow{e})) \mid (\text{new } C\ \overrightarrow{e}) & \text{Expressions} \\
 & \quad \mid (.\ e\ fld^{C}_{C}) \mid (.\ e\ (mth^{C}_{[[\overrightarrow{C}],C]}\ \overrightarrow{e})) \mid (\text{new}_{[\overrightarrow{C}]}\ C\ \overrightarrow{e}) & \text{Non-reflective Expressions} \\
v & ::= \ldots \mid C\ \{\overrightarrow{fld : v}\} & \text{Values} \\
ce & ::= \{\mathsf{m} \mapsto \{mth \mapsto [[\overrightarrow{C}], C]\}, \mathsf{f} \mapsto \{\overrightarrow{fld \mapsto C}\}, \mathsf{c} \mapsto \{[\overrightarrow{C}]\}\} & \text{Class descriptors} \\
\mathcal{CT} & ::= \{\overrightarrow{C \mapsto ce}\} & \text{Class Table}
\end{array}
$$

$$
\text{T-New}\quad \frac{[\overrightarrow{C_i}] \in \mathcal{CT}[C][\mathsf{c}] \qquad \overrightarrow{\mathsf{JT}_{\mathsf{nil}}(C_i) = \tau_i} \qquad \overrightarrow{\Gamma \vdash e_i \Rightarrow e_i' : \tau_i} \qquad \mathsf{JT}(C) = \tau}{\Gamma \vdash (\text{new } C\overrightarrow{e_i}) \Rightarrow (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i}) : \tau\ ;\ \mathtt{tt} \mid \mathtt{ff}\ ;\ \emptyset}
$$

$$
\text{T-Method}\quad \frac{\Gamma \vdash e \Rightarrow e' : \sigma \qquad \mathsf{TJ}(\sigma) = C_1 \qquad mth \mapsto [[\overrightarrow{C_i}], C_2] \in \mathcal{CT}[C_1][\mathsf{m}] \qquad \overrightarrow{\mathsf{JT}_{\mathsf{nil}}(C_i) = \tau_i} \qquad \overrightarrow{\Gamma \vdash e_i \Rightarrow e_i' : \tau_i} \qquad \mathsf{JT}_{\mathsf{nil}}(C_2) = \tau \qquad \vdash \sigma <: \mathbf{Object}}{\Gamma \vdash (.\ e\ (mth\overrightarrow{e_i})) \Rightarrow (.\ e'\ (mth^{C_1}_{[[\overrightarrow{C_i}],C_2]}\ \overrightarrow{e_i})) : \tau\ ;\ \mathtt{tt} \mid \mathtt{tt}\ ;\ \emptyset}
$$

$$
\text{T-Field}\quad \frac{\Gamma \vdash e \Rightarrow e' : \sigma \quad \vdash \sigma <: \mathbf{Object} \quad \mathsf{TJ}(\sigma) = C_1 \quad fld \mapsto C_2 \in \mathcal{CT}[C_1][\mathsf{f}] \quad \mathsf{JT}_{\mathsf{nil}}(C_2) = \tau}{\Gamma \vdash (.\ e\ fld) \Rightarrow (.\ e'\ fld^{C_1}_{C_2}) : \tau\ ;\ \mathtt{tt} \mid \mathtt{tt}\ ;\ \emptyset}
$$

$$
\begin{array}{llll}
\mathsf{JT}_{\mathsf{nil}}(\mathbf{Void}) = \mathbf{nil} & & \mathsf{JT}(\mathbf{Void}) = \mathbf{nil} & \mathsf{TJ}(\tau) = C \quad \text{if } \vdash \tau <: \mathsf{JT}_{\mathsf{nil}}(C) \\
\mathsf{JT}_{\mathsf{nil}}(C) = (\bigcup\ \mathbf{nil}\ C) & & \mathsf{JT}(C) = C &
\end{array}
$$

$$
\text{B-Field}\quad \frac{\rho \vdash e \Downarrow v \qquad \mathsf{JVM}_{\mathsf{getstatic}}[C_1, v_1, fld, C_2] = v}{\rho \vdash (.\ e\ fld^{C_1}_{C_2}) \Downarrow v} \qquad \text{B-New}\quad \frac{\overrightarrow{\rho \vdash e_i \Downarrow v_i} \qquad \mathsf{JVM}_{\mathsf{new}}[C_1, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = v}{\rho \vdash (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i}) \Downarrow v}
$$

$$
\text{B-Method}\quad \frac{\rho \vdash e_m \Downarrow v_m \qquad \overrightarrow{\rho \vdash e_a \Downarrow v_a} \qquad \mathsf{JVM}_{\mathsf{invokestatic}}[C_1, v_m, mth, [\overrightarrow{C_a}], [\overrightarrow{v_a}], C_2] = v}{\rho \vdash (.\ e_m\ (mth^{C_1}_{[[\overrightarrow{C_a}],C_2]}\ \overrightarrow{e_a})) \Downarrow v}
$$

Fig. 6. Java Interoperability Syntax, Typing and Operational Semantics

$$
\begin{array}{ll}
\delta_\tau(class) = x{:}\top \xrightarrow[\mathbf{class}(x)]{\mathtt{tt} \mid \mathtt{tt}} (\bigcup\ \mathsf{nil}\ \mathbf{Class}) \\
\delta_\tau(n?) = x{:}\top \xrightarrow[\emptyset]{\mathbf{N}_x \mid \overline{\mathbf{N}}_x} \mathbf{B}
\end{array}
$$

Fig. 7. Constant typing

But both the constructor and method are unresolved. We introduce *non-reflective* expressions for specifying exact Java overloads.

$$(. \ (\text{new}_{[\mathbf{S}]} \ \ \mathbf{F} \ \ \text{“a/b”}) \ (\text{getParent}^{\mathbf{F}}_{[[],\mathbf{S}]})) \tag{5}$$

From the left, the one-argument constructor for **F** takes a **S**, and the getParent method of **F** takes zero arguments and returns a **S**.

We now walk through this conversion.

Constructors First we check and convert (new **F** “a/b”) to ($\text{new}_{[\mathbf{S}]}$ **F** “a/b”). The T-New typing rule checks and rewrites constructors. To check (new **F** “a/b”) we first resolve the constructor overload in the class table—there is at most one to simplify presentation. With $C_1 = \mathbf{S}$, we convert to a nilable type the argument with $\tau_1 = (\bigcup \ \mathbf{nil} \ \mathbf{S})$ and type check “a/b” against τ_1. Typed Clojure defaults to allowing non-nilable arguments, but this can be overridden, so we model the more general case. The return Java type **F** is converted to a non-nil Typed Clojure type $\tau = \mathbf{F}$ for the return type, and the propositions say constructors can never be false—constructors can never produce the internal boolean value that Clojure uses for false, or nil. Finally, the constructor rewrites to ($\text{new}_{[\mathbf{S}]}$ **F** “a/b”).

Methods Next we convert (. ($\text{new}_{[\mathbf{S}]}$ **F** “a/b”) (getParent)) to the non-reflective expression (. ($\text{new}_{[\mathbf{S}]}$ **F** “a/b”) ($\text{getParent}^{\mathbf{F}}_{[[],\mathbf{S}]}$)). The T-Method rule for unresolved methods checks (. ($\text{new}_{[\mathbf{S}]}$ **F** “a/b”) (getParent)). We verify the target type $\sigma = \mathbf{F}$ is non-nil by T-New. The overload is chosen from the class table based on $C_1 = \mathbf{F}$—there is at most one. The nilable return type $\tau = (\bigcup \ \mathbf{nil} \ \mathbf{S})$ is given, and the entire expression rewrites to expression 5.

The T-Field rule (Figure 6) is like T-Method, but without arguments.

The evaluation rules B-Field, B-New and B-Method (Figure 6) simply evaluate their arguments and call the relevant JVM operation, which we do not model—Section 4 states our exact assumptions. There are no evaluation rules for reflective Java interoperability, since there are no typing rules that rewrite to reflective calls.

3.3 Multimethod preliminaries: isa?

We now consider the isa? operation, a core part of the multimethod dispatch mechanism. Recalling the examples in Section 2.4, isa? is a subclassing test for classes, but otherwise is an equality test. The T-IsA rule uses IsAProps (Figure 8), a metafunction which produces the propositions for isa? expressions.

To demonstrate the first IsAProps case, the expression (isa? (*class* x) **K**) is true if x is a keyword, otherwise false. When checked with T-IsA, the object of the left subexpression $o = \mathbf{class}(x)$ (which starts with the **class** path element) and the type of the right subexpression $\tau = (\mathbf{Val}\,\mathbf{K})$ (a singleton class type) together trigger the first IsAProps case $\text{IsAProps}(\mathbf{class}(x), (\mathbf{Val}\,\mathbf{K})) = \mathbf{K}_x|\overline{\mathbf{K}}_x$, giving propositions that correspond to our informal description $\psi_+|\psi_- = \mathbf{K}_x|\overline{\mathbf{K}}_x$.

The second IsAProps case captures the simple equality mode for non-class singleton types. For example, the expression (isa? x :en) produces true when x evaluates to :en, otherwise it produces false. Using T-IsA, it has the propositions $\psi_+|\psi_- = \mathsf{IsAProps}(x, (\mathbf{Val}\,\mathsf{:en})) = (\mathbf{Val}\,\mathsf{:en})_x|\overline{(\mathbf{Val}\,\mathsf{:en})}_x$ since $o = x$ and $\tau = (\mathbf{Val}\,\mathsf{:en})$. The side condition on the second IsAProps case ensures we are in equality mode—if x can possibly be a class in (isa? x **Object**), IsAProps uses its conservative default case, since if x is a class literal, subclassing mode could be triggered. Capture-avoiding substitution of objects $[o/x]$ used in this case erases propositions that would otherwise have $\emptyset$ substituted in for their objects—it is defined in the appendix.

The operational behavior of isa? is given by B-IsA (Figure 8). IsA explicitly handles classes in the second case.

3.4 Multimethods

Figure 8 presents *immutable* multimethods without default methods to ease presentation. Figure 9 translates the mutable Example 4 to λ_{TC}.

To check (defmulti $x\!:\!\mathbf{K} \to \mathbf{S}\ \lambda x^{\mathbf{K}}.x$), we note (defmulti $\sigma\ e$) creates a multimethod with *interface type* σ, and dispatch function e of type σ', producing a value of type (**Multi** $\sigma\ \sigma'$). The T-DefMulti typing rule checks the dispatch function, and verifies both the interface and dispatch type's domain agree. Our example checks with $\tau = \mathbf{K}$, interface type $\sigma = x\!:\!\mathbf{K} \to \mathbf{S}$, dispatch function type $\sigma' = x\!:\!\mathbf{K} \xrightarrow[x]{\mathtt{tt}|\mathtt{tt}} \mathbf{K}$, and overall type ($\mathbf{Multi}\, x\!:\!\mathbf{K} \to \mathbf{S}\ x\!:\!\mathbf{K} \xrightarrow[x]{\mathtt{tt}|\mathtt{tt}} \mathbf{K}$).

Next, we show how to check (defmethod hi_0 :en $\lambda x^{\mathbf{K}}.$"hello"). The expression (defmethod $e_m\ e_v\ e_f$) creates a new multimethod that extends multimethod e_m's dispatch table, mapping dispatch value e_v to method e_f. The T-DefMulti typing rule checks e_m is a multimethod with dispatch function type τ_d, then calculates the extra information we know based on the current dispatch value ${\psi''}_+$, which is assumed when checking the method body. Our example checks with e_m being of type ($\mathbf{Multi}\, x\!:\!\mathbf{K} \to \mathbf{S}\ x\!:\!\mathbf{K} \xrightarrow[x]{\mathtt{tt}|\mathtt{tt}} \mathbf{K}$) with $o' = x$ (from below the arrow on the right argument of the previous type) and $\tau_v = (\mathbf{Val}\,\mathsf{:en})$. Then ${\psi''}_+ = (\mathbf{Val}\,\mathsf{:en})_x$ from $\mathsf{IsAProps}(x, (\mathbf{Val}\,\mathsf{:en})) = (\mathbf{Val}\,\mathsf{:en})_x|\overline{(\mathbf{Val}\,\mathsf{:en})}_x$ (see Section 3.3). Since $\tau = \mathbf{K}$, we check the method body with $\mathbf{K}_x, (\mathbf{Val}\,\mathsf{:en})_x \vdash$ "hello" $:\mathbf{S}\ ;\ \mathtt{tt}|\mathtt{tt}\ ;\ \emptyset$. Finally from the interface type τ_m, we know $\psi_+ = \psi_- = \mathtt{tt}$, and $o = \emptyset$, which also agrees with the method body, above. Notice the overall type of a defmethod is the same as its first subexpression e_m.

It is worth noting the lack of special typing rules for overlapping methods—each method is checked independently based on local type information.

Subtyping Multimethods are functions, via S-PMultiFn, which says a multimethod can be upcast to its interface type. Multimethod call sites are then handled by T-App via T-Subsume. Other rules are given in Figure 8.

$$
\begin{array}{llll}
e & ::= \ldots \mid (\text{defmulti } \tau\ e) \mid (\text{defmethod } e\ e\ e) \mid (\text{isa? } e\ e) & \text{Expressions} \\
v & ::= \ldots \mid [v,t]_{\mathsf{m}} & \text{Values} \\
t & ::= \{\overrightarrow{v \mapsto v}\} & \text{Dispatch tables} \\
\sigma,\tau & ::= \ldots \mid (\mathbf{Multi}\,\tau\ \tau) & \text{Types}
\end{array}
$$

T-DefMulti

$$\frac{\sigma = x{:}\tau \xrightarrow[o]{\psi_+|\psi_-} \tau' \qquad \sigma' = x{:}\tau \xrightarrow[o']{\psi'_+|\psi'_-} \tau'' \qquad \Gamma \vdash e \Rightarrow e' : \sigma'}{\Gamma \vdash (\text{defmulti } \sigma\ e) \Rightarrow (\text{defmulti } \sigma\ e') : (\mathbf{Multi}\,\sigma\ \sigma')\ ;\ \mathbb{tt}|\mathbb{ff}\ ;\ \emptyset}$$

T-DefMethod

$$\frac{\begin{array}{c}\tau_m = x{:}\tau \xrightarrow[o]{\psi_+|\psi_-} \sigma \qquad \tau_d = x{:}\tau \xrightarrow[o']{\psi'_+|\psi'_-} \sigma' \qquad \Gamma \vdash e_m \Rightarrow e'_m : (\mathbf{Multi}\,\tau_m\ \tau_d) \\ \Gamma \vdash e_v \Rightarrow e'_v : \tau_v \qquad \mathsf{IsAProps}(o', \tau_v) = \psi''_+|\psi''_- \\ \Gamma, \tau_x, \psi''_+ \vdash e_b \Rightarrow e'_b : \sigma\ ;\ \psi_+|\psi_-\ ;\ o \qquad e' = (\text{defmethod } e'_m\ e'_v\ \lambda x^\tau.e'_b)\end{array}}{\Gamma \vdash (\text{defmethod } e_m\ e_v\ \lambda x^\tau.e_b) \Rightarrow e' : (\mathbf{Multi}\,\tau_m\ \tau_d)\ ;\ \mathbb{tt}|\mathbb{ff}\ ;\ \emptyset}$$

T-IsA

$$\frac{\Gamma \vdash e \Rightarrow e_1 : \sigma\ ;\ \psi'_+|\psi'_-\ ;\ o \qquad \Gamma \vdash e' \Rightarrow e'_1 : \tau \qquad \mathsf{IsAProps}(o,\tau) = \psi_+|\psi_-}{\Gamma \vdash (\text{isa? } e\ e') \Rightarrow (\text{isa? } e_1\ e'_1) : \mathbf{B}\ ;\ \psi_+|\psi_-\ ;\ \emptyset}$$

$$
\begin{array}{ll}
\mathsf{IsAProps}(\mathbf{class}(\pi(x)), (\mathbf{Val}\,C)) & = C_{\pi(x)}|\overline{C}_{\pi(x)} \\
\mathsf{IsAProps}(o, (\mathbf{Val}\,l)) & = ((\mathbf{Val}\,l)_x|\overline{(\mathbf{Val}\,l)}_x)[o/x] \text{ if } l \neq C \\
\mathsf{IsAProps}(o, \tau) & = \mathbb{tt}|\mathbb{tt} \qquad \text{otherwise}
\end{array}
$$

S-PMultiFn

$$\frac{\vdash \sigma_t <: x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau \qquad \vdash \sigma_d <: x{:}\sigma \xrightarrow[o']{\psi'_+|\psi'_-} \tau'}{\vdash (\mathbf{Multi}\,\sigma_t\ \sigma_d) <: x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau}$$

S-PMulti

$$\frac{\vdash \sigma <: \sigma' \qquad \vdash \tau <: \tau'}{\vdash (\mathbf{Multi}\,\sigma\ \tau) <: (\mathbf{Multi}\,\sigma'\ \tau')}$$

S-MultiMono

$$\vdash (\mathbf{Multi}\,x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau\ x{:}\sigma \xrightarrow[o']{\psi'_+|\psi'_-} \tau') <: \mathbf{Multi}$$

B-DefMulti

$$\frac{\rho \vdash e \Downarrow v_d \qquad v = [v_d, \{\}]_{\mathsf{m}}}{\rho \vdash (\text{defmulti } \tau\ e) \Downarrow v}$$

B-DefMethod

$$\frac{\rho \vdash e \Downarrow [v_d, t]_{\mathsf{m}} \qquad \rho \vdash e' \Downarrow v_v \qquad \rho \vdash e_f \Downarrow v_f \qquad v = [v_d, t[v_v \mapsto v_f]]_{\mathsf{m}}}{\rho \vdash (\text{defmethod } e\ e'\ e_f) \Downarrow v}$$

$\mathsf{GM}(t, v_e) = v_f$ if $\overrightarrow{v_{fs}} = \{v_f\}$ where $\overrightarrow{v_{fs}} = \{v_f | v_k \mapsto v_f \in t \text{ and } \mathsf{IsA}(v_e, v_k) = \mathsf{true}\}$
$\mathsf{GM}(t, v_e) = \mathsf{err}$ otherwise

B-IsA

$$\frac{\rho \vdash e_1 \Downarrow v_1 \qquad \rho \vdash e_2 \Downarrow v_2 \qquad \mathsf{IsA}(v_1, v_2) = v}{\rho \vdash (\text{isa? } e_1\ e_2) \Downarrow v}$$

$$
\begin{array}{ll}
\mathsf{IsA}(v, v) & = \mathsf{true} \qquad v \neq C \\
\mathsf{IsA}(C, C') & = \mathsf{true} \vdash C <: C' \\
\mathsf{IsA}(v, v') & = \mathsf{false} \text{ otherwise}
\end{array}
$$

B-BetaMulti

$$\frac{\rho \vdash e \Downarrow [v_d, t]_{\mathsf{m}} \quad \rho \vdash e' \Downarrow v' \quad \rho \vdash (v_d\ v') \Downarrow v_e \quad \mathsf{GM}(t, v_e) = v_f \quad \rho \vdash (v_f\ v') \Downarrow v}{\rho \vdash (e\ e') \Downarrow v}$$

Fig. 8. Multimethod Syntax, Typing and Operational Semantics

$$
\begin{array}{l}
(\text{let } [hi_0 \ (\text{defmulti } x{:}\,\mathbf{K} \xrightarrow[\emptyset]{\mathtt{tt}\,|\,\mathtt{tt}} \mathbf{S} \ \ \lambda x^{\mathbf{K}}.x)] \\
\quad (\text{let } [hi_1 \ (\text{defmethod } hi_0 \ \mathsf{:en} \ \lambda x^{\mathbf{K}}.\text{“}\mathsf{hello}\text{”})] \\
\quad\quad (\text{let } [hi_2 \ (\text{defmethod } hi_1 \ \mathsf{:fr} \ \lambda x^{\mathbf{K}}.\text{“}\mathsf{bonjour}\text{”})] \\
\quad\quad\quad (hi_2 \ \mathsf{:en}))))
\end{array}
$$

Fig. 9. Multimethod example

Semantics Multimethod definition semantics are also given in Figure 8. B-DefMulti creates a multimethod with the given dispatch function and an empty dispatch table. B-DefMethod produces a new multimethod with an extended dispatch table.

The overall dispatch mechanism is summarised by B-BetaMulti. First the dispatch function v_d is applied to the argument v' to obtain the dispatch value v_e. Based on v_e, the GM metafunction (Figure 8) extracts a method v_f from the method table t and applies it to the original argument for the final result.

3.5 Precise Types for Heterogeneous maps

Figure 10 presents heterogeneous map types. The type $(\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})$ contains $\mathcal{M}$, a map of *present* entries (mapping keywords to types), $\mathcal{A}$, a set of keyword keys that are known to be *absent* and tag $\mathcal{E}$ which is either $\mathcal{C}$ (“complete”) if the map is fully specified by $\mathcal{M}$, and $\mathcal{P}$ (“partial”) if there are *unknown* entries. The partially specified map of `lunch` in Example 6 is written $(\mathbf{HMap}^{\mathcal{P}}\{(\mathbf{Val}\,\mathsf{:en})\ \mathbf{S}, (\mathbf{Val}\,\mathsf{:fr})\ \mathbf{S}\}\ \{\})$ (abbreviated **Lu**). The type of the fully specified map `breakfast` in Example 5 elides the absent entries, written $(\mathbf{HMap}^{\mathcal{C}}\{(\mathbf{Val}\,\mathsf{:en})\ \mathbf{S}, (\mathbf{Val}\,\mathsf{:fr})\ \mathbf{S}\})$ (abbreviated **Bf**). To ease presentation, if an HMap has completeness tag $\mathcal{C}$ then $\mathcal{A}$ is elided and implicitly contains all keywords not in the domain of $\mathcal{M}$—dissociating keys is not modelled, so the set of absent entries otherwise never grows. Keys cannot be both present and absent.

The metavariable m ranges over the runtime value of maps $\{\overrightarrow{k \mapsto v}\}$, usually written $\{\overrightarrow{k\ v}\}$. We only provide syntax for the empty map literal, however when convenient we abbreviate non-empty map literals to be a series of assoc operations on the empty map. We restrict lookup and extension to keyword keys.

How to check A mandatory lookup is checked by T-GetHMap.

$$\lambda b^{\mathbf{Bf}}.(\text{get } b\ \mathsf{:en})$$

The result type is $\mathbf{S}$, and the return object is $\mathbf{key}_{\mathsf{:en}}(b)$. The object $\mathbf{key}_k(x)[o/x]$ is a symbolic representation for a keyword lookup of k in o. The substitution for x handles the case where o is empty.

$$\mathbf{key}_k(x)[y/x] = \mathbf{key}_k(y) \qquad \mathbf{key}_k(x)[\emptyset/x] = \emptyset$$

$$
\begin{array}{lll}
e & ::= \ldots \mid (\text{get } e\ e) \mid (\text{assoc } e\ e\ e) & \text{Expressions} \\
v & ::= \ldots \mid \{\} & \text{Values} \\
\tau & ::= \ldots \mid (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}) & \text{Types} \\
\mathcal{M} & ::= \{\overrightarrow{k \mapsto \tau}\} & \text{HMap mandatory entries} \\
\mathcal{A} & ::= \{\overrightarrow{k}\} & \text{HMap absent entries} \\
\mathcal{E} & ::= \mathcal{C} \mid \mathcal{P} & \text{HMap completeness tags}
\end{array}
$$

T-AssocHMap

$$\frac{\Gamma \vdash e \Rightarrow (\text{assoc } e'\ e'_k\ e'_v) : (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}) \quad \Gamma \vdash e_k \Rightarrow e'_k : (\mathbf{Val}\, k) \quad \Gamma \vdash e_v \Rightarrow e'_v : \tau \quad k \notin \mathcal{A}}{\Gamma \vdash (\text{assoc } e\ e_k\ e_v) \Rightarrow (\text{assoc } e'\ e'_k\ e'_v) : (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}[k \mapsto \tau]\ \mathcal{A})\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

T-GetHMap

$$\frac{\Gamma \vdash e \Rightarrow e' : (\bigcup\ \overrightarrow{(\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})}^{i})\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o \quad \Gamma \vdash e_k \Rightarrow e'_k : (\mathbf{Val}\, k) \quad \overrightarrow{\mathcal{M}[k] = \tau}^{i}}{\Gamma \vdash (\text{get } e\ e_k) \Rightarrow (\text{get } e'\ e'_k) : (\bigcup\ \overrightarrow{\tau}^{i})\ ;\ \mathtt{tt}|\mathtt{tt}\ ;\ \mathbf{key}_k(x)[o/x]}$$

T-GetHMapAbsent

$$\frac{\Gamma \vdash e \Rightarrow e' : (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o \qquad \Gamma \vdash e_k \Rightarrow e'_k : (\mathbf{Val}\, k) \qquad k \in \mathcal{A}}{\Gamma \vdash (\text{get } e\ e_k) \Rightarrow (\text{get } e'\ e'_k) : \mathbf{nil}\ ;\ \mathtt{tt}|\mathtt{tt}\ ;\ \mathbf{key}_k(x)[o/x]}$$

T-GetHMapPartialDefault

$$\frac{\begin{array}{c}\Gamma \vdash e \Rightarrow e' : (\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ \mathcal{A})\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o \\ \Gamma \vdash e_k \Rightarrow e'_k : (\mathbf{Val}\, k) \qquad k \notin dom(\mathcal{M}) \qquad k \notin \mathcal{A}\end{array}}{\Gamma \vdash (\text{get } e\ e_k) \Rightarrow (\text{get } e'\ e'_k) : \top\ ;\ \mathtt{tt}|\mathtt{tt}\ ;\ \mathbf{key}_k(x)[o/x]}$$

S-HMapMono

$$\vdash (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}) <: \mathbf{Map}$$

S-HMapP

$$\frac{\forall i.\ \mathcal{M}[k_i] = \sigma_i \text{ and } \vdash \sigma_i <: \tau_i}{\vdash (\mathbf{HMap}^{\mathcal{C}}\ \mathcal{M}\ \mathcal{A}') <: (\mathbf{HMap}^{\mathcal{P}}\ \overrightarrow{\{k \mapsto \tau\}}^{i}\ \mathcal{A})}$$

S-HMap

$$\frac{\forall i.\ \mathcal{M}[k_i] = \sigma_i \text{ and } \vdash \sigma_i <: \tau_i \qquad \mathcal{A}_1 \supseteq \mathcal{A}_2}{\vdash (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}_1) <: (\mathbf{HMap}^{\mathcal{E}}\ \overrightarrow{\{k \mapsto \tau\}}^{i}\ \mathcal{A}_2)}$$

B-Assoc

$$\frac{\begin{array}{c}\rho \vdash e \Downarrow m \qquad \rho \vdash e_k \Downarrow k \\ \rho \vdash e_v \Downarrow v_v\end{array}}{\rho \vdash (\text{assoc } e\ e_k\ e_v) \Downarrow m[k \mapsto v_v]}$$

B-Get

$$\frac{\rho \vdash e \Downarrow m \qquad \rho \vdash e' \Downarrow k \qquad k \in dom(m)}{\rho \vdash (\text{get } e\ e') \Downarrow m[k]}$$

B-GetMissing

$$\frac{\rho \vdash e \Downarrow m \qquad \rho \vdash e' \Downarrow k \qquad k \notin dom(m)}{\rho \vdash (\text{get } e\ e') \Downarrow \mathsf{nil}}$$

Fig. 10. HMap Syntax, Typing and Operational Semantics

$$
\begin{array}{l}
\mathsf{restrict}(\tau, \sigma) = \bot \text{ if } \nexists v.\ \vdash v : \tau\ ;\ \psi\ ;\ o \text{ and } \vdash v : \sigma\ ;\ \psi'\ ;\ o' \\
\mathsf{restrict}(\tau, \sigma) = \tau \text{ if } \vdash \tau <: \sigma \\
\mathsf{restrict}(\tau, \sigma) = \sigma \text{ otherwise}
\end{array}
\qquad
\begin{array}{l}
\mathsf{remove}(\tau, \sigma) = \bot \text{ if } \vdash \tau <: \sigma \\
\mathsf{remove}(\tau, \sigma) = \tau \text{ otherwise}
\end{array}
$$

Fig. 11. Restrict and remove

An absent lookup is checked by T-GetHMapAbsent.

$$\lambda b^{\mathbf{Bf}}.(\text{get } b \text{ :bocce})$$

The result type is **nil**—since **Bf** is fully specified—with return object $\mathbf{key}_{:\mathsf{bocce}}(b)$.

A lookup that is not present or absent is checked by T-GetHMapPartialDefault.

$$\lambda u^{\mathbf{Lu}}.(\text{get } u \text{ :bocce})$$

The result type is $\top$—since **Lu** has an unknown :bocce entry—with return object $\mathbf{key}_{:\mathsf{bocce}}(u)$. Notice propositions are erased once they enter a HMap type.

For presentational reasons, lookups on unions of HMaps are only supported in T-GetHMap and each element of the union must contain the relevant key.

$$\lambda u^{(\bigcup\ \mathbf{Bf}\,\mathbf{Lu})}.(\text{get } u \text{ :en})$$

The result type is **S**, and the return object is $\mathbf{key}_{:\mathsf{en}}(u)$. However, lookups of :bocce on $(\bigcup\ \mathbf{Bf}\,\mathbf{Lu})$ maps are unsupported. This restriction still allows us to check many of the examples in Section 2—in particular we can check Example 8, as :Meal is in common with both HMaps, but cannot check Example 9 because a :combo meal lacks a :desserts entry. Adding a rule to handle Example 9 is otherwise straightforward.

Extending a map with T-AssocHMap preserves its completeness.

$$\lambda b^{\mathbf{Bf}}.(\text{assoc } b \text{ :au “beans”})$$

The result type is $(\mathbf{HMap}^{\mathcal{C}}\{(\mathbf{Val}\,\text{:en})\ \mathbf{S}, (\mathbf{Val}\,\text{:fr})\ \mathbf{S}, (\mathbf{Val}\,\text{:au})\ \mathbf{S}\})$, a complete map. T-AssocHMap also enforces $k \notin \mathcal{A}$ to prevent badly formed types.

Subtyping Subtyping for HMaps designate **Map** as a common supertype for all HMaps. S-HMap says that HMaps are subtypes if they agree on $\mathcal{E}$, agree on mandatory entries with subtyping and at least cover the absent keys of the supertype. Complete maps are subtypes of partial maps as long as they agree on the mandatory entries of the partial map via subtyping (S-HMapP).

The semantics for get and assoc are straightforward.

3.6 Proof system

The occurrence typing proof system uses standard propositional logic, except for where nested information is combined. This is handled by L-Update:

$$\text{L-UPDATE}\ \frac{\Gamma \vdash \tau_{\pi'(x)} \qquad \Gamma \vdash \nu_{\pi(\pi'(x))}}{\Gamma \vdash \mathsf{update}(\tau, \nu, \pi)_{\pi'(x)}}$$

It says under Γ, if object $\pi'(x)$ is of type τ, and an extension $\pi(\pi'(x))$ is of possibly-negative type ν, then update (τ, ν, π) is $\pi'(x)$'s type under Γ.

$$
\begin{array}{ll}
\mathsf{update}((\bigcup\ \overrightarrow{\tau}), \nu, \pi) & = (\bigcup\ \overrightarrow{\mathsf{update}(\tau, \nu, \pi)}) \\
\mathsf{update}(\tau, (\mathbf{Val}\, C), \pi :: \mathbf{class}) & = \mathsf{update}(\tau, C, \pi) \\
\mathsf{update}(\tau, \nu, \pi :: \mathbf{class}) & = \tau \\
\mathsf{update}((\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}), \nu, \pi :: \mathbf{key}_k) & = (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}[k \mapsto \mathsf{update}(\tau, \nu, \pi)]\ \mathcal{A}) \\
 & \quad \text{if } \mathcal{M}[k] = \tau \\
\mathsf{update}((\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}), \nu, \pi :: \mathbf{key}_k) & = \bot \quad \text{if } \vdash \mathbf{nil} \not<: \nu \text{ and } k \in \mathcal{A} \\
\mathsf{update}((\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ \mathcal{A}), \tau, \pi :: \mathbf{key}_k) & = (\cup\ (\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}[k \mapsto \tau]\ \mathcal{A}) \\
 & \qquad (\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ (\mathcal{A} \cup \{k\}))) \\
 & \quad \text{if } \vdash \mathbf{nil} <: \tau,\ k \notin dom(\mathcal{M}) \text{ and } k \notin \mathcal{A} \\
\mathsf{update}((\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ \mathcal{A}), \nu, \pi :: \mathbf{key}_k) & = (\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}[k \mapsto \mathsf{update}(\top, \nu, \pi)]\ \mathcal{A}) \\
 & \quad \text{if } \vdash \mathbf{nil} \not<: \nu,\ k \notin dom(\mathcal{M}) \text{ and } k \notin \mathcal{A} \\
\mathsf{update}(\tau, \nu, \pi :: \mathbf{key}_k) & = \tau \\
\mathsf{update}(\tau, \sigma, \epsilon) & = \mathsf{restrict}(\tau, \sigma) \\
\mathsf{update}(\tau, \overline{\sigma}, \epsilon) & = \mathsf{remove}(\tau, \sigma)
\end{array}
$$

Fig. 12. Type update (the metavariable ν ranges over τ and $\overline{\tau}$ (without variables), $\vdash \mathbf{nil} \not<: \overline{\tau}$ when $\vdash \mathbf{nil} <: \tau$, see Figure 11 for restrict and remove.)

Recall Example 8. Solving $\mathbf{Order}_o, (\mathbf{Val}\,{:}\mathsf{combo})_{\mathbf{key}_{:\mathsf{Meal}}(o)} \vdash \tau_o$ uses L-Update, where $\pi = \epsilon$ and $\pi' = [\mathbf{key}_{:\mathsf{Meal}}]$.

$$\Gamma \vdash \mathsf{update}(\mathbf{Order}, (\mathbf{Val}\,{:}\mathsf{combo}), [\mathbf{key}_{:\mathsf{Meal}}])_o$$

Since **Order** is a union of HMaps, we structurally recur on the first case of update (Figure 12), which preserves π. Each initial recursion hits the first HMap case, since there is some τ such that $\mathcal{M}[k] = \tau$ and $\mathcal{E}$ accepts partial maps $\mathcal{P}$.

To demonstrate, :lunch meals are handled by the first HMap case and update to $(\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}[(\mathbf{Val}\,{:}\mathsf{Meal}) \mapsto \sigma']\ \{\})$ where $\sigma' = \mathsf{update}\ ((\mathbf{Val}\,{:}\mathsf{lunch}), (\mathbf{Val}\,{:}\mathsf{combo}), \epsilon)$ and $\mathcal{M} = \{(\mathbf{Val}\,{:}\mathsf{Meal}) \mapsto (\mathbf{Val}\,{:}\mathsf{lunch}), (\mathbf{Val}\,{:}\mathsf{desserts}) \mapsto \mathbf{N}\}$. σ' updates to $\bot$ via the penultimate update case, because $\mathsf{restrict}\ ((\mathbf{Val}\,{:}\mathsf{lunch}), (\mathbf{Val}\,{:}\mathsf{combo})) = \bot$ by the first restrict case. The same happens to :dinner meals, leaving just the :combo HMap.

In Example 9, $\Gamma \vdash \mathsf{update}(\mathbf{Order}, \mathbf{Long}, [\mathbf{class}, \mathbf{key}_{:\mathsf{desserts}}])_o$ updates the argument in the **Long** method. This recurs twice for each meal to handle the **class** path element.

We describe the other update cases. The first **class** case updates to C if *class* returns $(\mathbf{Val}\,C)$. The second $\mathbf{key}_k$ case detects contradictions in absent keys. The third $\mathbf{key}_k$ case updates unknown entries to be mapped to τ or absent. The fourth $\mathbf{key}_k$ case updates unknown entries to be *present* when they do not overlap with **nil**.

4 Metatheory

We prove type soundness following Tobin-Hochstadt and Felleisen [24]. Our model is extended to include errors err and a *wrong* value, and we prove well-

typed programs do not go wrong; this is therefore a stronger theorem than proved by Tobin-Hochstadt and Felleisen [24]. Errors behave like Java exceptions—they can be thrown and propagate "upwards" in the evaluation rules (err rules are deferred to the appendix).

Rather than modeling Java's dynamic semantics, a task of daunting complexity, we instead make our assumptions about Java explicit. We concede that method and constructor calls may diverge or error, but assume they can never go wrong (other assumptions given in the supplemental material).

Assumption 1 ($\mathsf{JVM}_{\mathsf{new}}$). *If* $\forall i.\ v_i = C_i\ \{\overrightarrow{fld_j : v_j}\}$ *or* $v_i = \mathsf{nil}$ *and* v_i *is consistent with* ρ *then either*

- $\mathsf{JVM}_{\mathsf{new}}[C, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = C\ \{\overrightarrow{fld_k : v_k}\}$ *which is consistent with* ρ*,*
- $\mathsf{JVM}_{\mathsf{new}}[C, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = \mathsf{err}$*, or*
- $\mathsf{JVM}_{\mathsf{new}}[C, [\overrightarrow{C_i}], [\overrightarrow{v_i}]]$ *is undefined.*

For the purposes of our soundness proof, we require that all values are *consistent*. Consistency (defined in the supplemental material) states that the types of closures are well-scoped—they do not claim propositions about variables hidden in their closures.

We can now state our main lemma and soundness theorem. The metavariable α ranges over v, err and *wrong*. Proofs are deferred to the supplemental material.

Lemma 1. *If* $\Gamma \vdash e' \Rightarrow e : \tau\ ;\ \psi_+|\psi_-\ ;\ o$*,* $\rho \models \Gamma$*,* ρ *is consistent, and* $\rho \vdash e \Downarrow \alpha$ *then either*

- $\rho \vdash e \Downarrow v$ *and all of the following hold:*
  1. *either* $o = \emptyset$ *or* $\rho(o) = v$*,*
  2. *either* $\mathsf{TrueVal}(v)$ *and* $\rho \models \psi_+$ *or* $\mathsf{FalseVal}(v)$ *and* $\rho \models \psi_-$*,*
  3. $\vdash v \Rightarrow v : \tau\ ;\ {\psi'}_+|{\psi'}_-\ ;\ o'$ *for some* ${\psi'}_+$*,* ${\psi'}_-$ *and* o'*, and*
  4. v *is consistent with* ρ*, or*
- $\rho \vdash e \Downarrow \mathsf{err}$.

Theorem 1 (Type soundness). *If* $\Gamma \vdash e' \Rightarrow e : \tau\ ;\ \psi_+|\psi_-\ ;\ o$ *and* $\rho \vdash e \Downarrow v$ *then* $\vdash v \Rightarrow v : \tau\ ;\ {\psi'}_+|{\psi'}_-\ ;\ o'$ *for some* ${\psi'}_+$*,* ${\psi'}_-$ *and* o'*.*

5 Experience

Typed Clojure is implemented as `core.typed` [2], which has seen wide usage.

5.1 Implementation

`core.typed` provides preliminary integration with the Clojure compilation pipeline, primarily to resolve Java interoperability.

The `core.typed` implementation extends this paper in several key areas to handle checking real Clojure code, including an implementation of Typed

	feeds2imap	CircleCI
Total number of typed namespaces	11 (825 LOC)	87 (19,000 LOC)
Total number of `def` expressions	93	1834
• checked	52 (56%)	407 (22%)
• unchecked	41 (44%)	1427 (78%)
Total number of Java interactions	32	105
• static methods	5 (16%)	26 (25%)
• instance methods	20 (62%)	36 (34%)
• constructors	6 (19%)	38 (36%)
• static fields	1 (3%)	5 (5%)
Methods overriden to return non-nil	0	35
Methods overriden to accept nil arguments	0	1
Total HMap lookups	27	328
• resolved to mandatory key	20 (74%)	208 (64%)
• resolved to optional key	6 (22%)	70 (21%)
• resolved of absent key	0 (0%)	20 (6%)
• unresolved key	1 (4%)	30 (9%)
Total number of `defalias` expressions	18	95
• contained HMap or union of HMap type	7 (39%)	62 (65%)
Total number of checked `defmulti` expressions	0	11
Total number of checked `defmethod` expressions	0	89

Fig. 13. Typed Clojure Features used in Practice

Racket's variable-arity polymorphism [22], and support for other Clojure idioms like datatypes and protocols. There is no integration with Java Generics, so only Java 1.4-style erased types are "trusted" by `core.typed`. Casts are needed to recover the discarded information, which—for collections—are then tracked via Clojure's universal sequence interface [14].

5.2 Evaluation

Throughout this paper, we have focused on three interrelated type system features: heterogenous maps, Java interoperability, and multimethods. Our hypothesis is that these features are widely used in existing Clojure programs in interconnecting ways, and that handling them as we have done is required to type check realistic Clojure programs.

To evaluate this hypothesis, we analyzed two existing `core.typed` code bases, one from the open-source community, and one from a company that uses `core.typed` in production. For our data gathering, we instrumented the `core.typed` type checker to record how often various features were used (summarized in Figure 13).

feeds2imap feeds2imap[4] is an open source library written in Typed Clojure. It provides an RSS reader using the *javax.mail* framework.

[4] `https://github.com/frenchy64/feeds2imap.clj`

Of 11 typed namespaces containing 825 lines of code, there are 32 Java interactions. The majority are method calls, consisting of 20 (62%) instance methods and 5 (16%) static methods. The rest consists of 1 (3%) static field access, and 6 (19%) constructor calls—there are no instance field accesses.

There are 27 lookup operations on HMap types, of which 20 (74%) resolve to mandatory entries, 6 (22%) to optional entries, and 1 (4%) is an unresolved lookup. No lookups involved fully specified maps.

From 93 `def` expressions in typed code, 52 (56%) are checked, with a rate of 1 Java interaction for 1.6 checked top-level definitions, and 1 HMap lookup to 1.9 checked top-level definitions. That leaves 41 (44%) unchecked vars, mainly due to partially complete porting to Typed Clojure, but in some cases due to unannotated third-party libraries.

No typed multimethods are defined or used. Of 18 total type aliases, 7 (39%) contained one HMap type, and none contained unions of HMaps—on further inspection there was no HMap entry used to dictate control flow, often handled by multimethods. This is unusual in our experience, and is perhaps explained by feeds2imap mainly wrapping existing *javax.mail* functionality.

CircleCI CircleCI [7] provides continuous integration services built with a mixture of open- and closed-source software. Typed Clojure was used at CircleCI in production systems for two years [8], maintaining 87 namespaces and 19,000 lines of code, an experience we summarise in Section 5.3.

The CircleCI code base contains 11 checked multimethods. All 11 dispatch functions are on a HMap key containing a keyword, in a similar style to Example 8. Correspondingly, all 89 methods are associated with a keyword dispatch value. The argument type was in all cases a single HMap type, however, rather than a union type. In our experience from porting other libraries, this is unusual.

Of 328 lookup operations on HMaps, 208 (64%) resolve to mandatory keys, 70 (21%) to optional keys, 20 (6%) to absent keys, and 30 (9%) lookups are unresolved. Of 95 total type aliases defined with `defalias`, 62 (65%) involved one or more HMap types. Out of 105 Java interactions, 26 (25%) are static methods, 36 (34%) are instance methods, 38 (36%) are constructors, and 5 (5%) are static fields. 35 methods are overriden to return non-nil, and 1 method overridden to accept nil—suggesting that `core.typed` disallowing `nil` as a method argument by default is justified.

Of 464 checked top-level definitions (which consists of 57 `defmethod` calls and 407 `def` expressions), 1 HMap lookup occurs per 1.4 top-level definitions, and 1 Java interaction occurs every 4.4 top-level definitions.

From 1834 `def` expressions in typed code, only 407 (22%) were checked. That leaves 1427 (78%) which have unchecked definitions, either by an explicit `:no-check` annotation or `tc-ignore` to suppress type checking, or the `warn-on-unannotated-vars` option, which skips `def` expressions that lack expected types via `ann`. From a brief investigation, reasons include unannotated third-party libraries, work-in-progress conversions to Typed Clojure, unsupported Clojure idioms, and hard-to-check code.

Lessons Based on our empirical survey, HMaps and Java interoperability support are vital features used on average more than once per typed function. Multimethods are less common in our case studies. The CircleCI code base contains only 26 multimethods total in 55,000 lines of mixed untyped-typed Clojure code, a low number in our experience.

5.3 Further challenges

After a 2 year trial, the second case study decided to disabled type checking [9]. They were supportive of the fundamental ideas presented in this paper, but primarily cited issues with the checker implementation in practice and would reconsider type checking if they were resolved. This is also supported by Figure 13, where 78% of `def` expressions are unchecked.

Performance Rechecking files with transitive dependencies is expensive since all dependencies must be rechecked. We conjecture caching type state will significantly improve re-checking performance, though preserving static soundness in the context of arbitrary code reloading is a largely unexplored area.

Library annotations Annotations for external code are rarely available, so a large part of the untyped-typed porting process is reverse engineering libraries.

Unsupported idioms While the current set of features is vital to checking Clojure code, there is still much work to do. For example, common Clojure functions are often too polymorphic for the current implementation or theory to account for. The post-mortem [9] contains more details.

6 Related Work

Multimethods [20] and collaborators present a sequence of systems [4, 5, 20] with statically-typed multimethods and modular type checking. In contrast to Typed Clojure, in these system methods declare the types of arguments that they expect which corresponds to exclusively using `class` as the dispatch function in Typed Clojure. However, Typed Clojure does not attempt to rule out failed dispatches.

Record Types Row polymorphism [26, 3, 12], used in systems such as the OCaml object system, provides many of the features of HMap types, but defined using universally-quantified row variables. HMaps in Typed Clojure are instead designed to be used with subtyping, but nonetheless provide similar expressiveness, including the ability to require presence and absence of certain keys.

Dependent JavaScript [6] can track similar invariants as HMaps with types for JS objects. They must deal with mutable objects, they feature refinement types and strong updates to the heap to track changes to objects.

TeJaS [16], another type system for JavaScript, also supports similar HMaps, with the ability to record the presence and absence of entries, but lacks a compositional flow-checking approach like occurrence typing.

Typed Lua [18] has *table types* which track entries in a mutable Lua table. Typed Lua changes the dynamic semantics of Lua to accommodate mutability:

Typed Lua raises a runtime error for lookups on missing keys—HMaps consider lookups on missing keys normal.

Java Interoperability in Statically Typed Languages Scala [21] has nullable references for compatibility with Java. Programmers must manually check for `null` as in Java to avoid null-pointer exceptions.

Other optional and gradual type systems Several other gradual type systems have been developed for existing dynamically-typed languages. Reticulated Python [25] is an experimental gradually typed system for Python, implemented as a source-to-source translation that inserts dynamic checks at language boundaries and supporting Python's first-class object system. Clojure's nominal classes avoids the need to support first-class object system in Typed Clojure, however HMaps offer an alternative to the structural objects offered by Reticulated. Similarly, Gradualtalk [1] offers gradual typing for Smalltalk, with nominal classes.

Optional types have been adopted in industry, including Hack [10], and Flow [11] and TypeScript [19], two extensions of JavaScript. These systems support limited forms of occurrence typing, and do not include the other features we present.

7 Conclusion

Optional type systems must be designed with close attention to the language that they are intended to work for. We have therefore designed Typed Clojure, an optionally-typed version of Clojure, with a type system that works with a wide variety of distinctive Clojure idioms and features. Although based on the foundation of Typed Racket's occurrence typing approach, Typed Clojure both extends the fundamental control-flow based reasoning as well as applying it to handle seemingly unrelated features such as multi-methods. In addition, Typed Clojure supports crucial features such as heterogeneous maps and Java interoperability while integrating these features into the core type system. Not only are each of these features important in isolation to Clojure and Typed Clojure programmers, but they must fit together smoothly to ensure that existing untyped programs are easy to convert to Typed Clojure.

The result is a sound, expressive, and useful type system which, as implemented in `core.typed` with appropriate extensions, is suitable for typechecking a significant amount of existing Clojure programs. As a result, Typed Clojure is already successful: it is used in the Clojure community among both enthusiasts and professional programmers.

Our empirical analysis of existing Typed Clojure programs bears out our design choices. Multimethods, Java interoperation, and heterogeneous maps are indeed common in both Clojure and Typed Clojure, meaning that our type system must accommodate them. Furthermore, they are commonly used together, and the features of each are mutually reinforcing. Additionally, the choice to make Java's `null` explicit in the type system is validated by the many Typed Clojure programs that specify non-nullable types.

References

1. Allende, E., Callau, O., Fabry, J., Tanter, É., Denker, M.: Gradual typing for Smalltalk. Science of Computer Programming 96, 52–69 (2014)
2. Bonnaire-Sergeant, A., contributors: core.typed, `https://github.com/clojure/core.typed`
3. Cardelli, L., Mitchell, J.C.: Operations on records. In: Mathematical Structures in Computer Science. pp. 3–48 (1991)
4. Chambers, C.: Object-oriented multi-methods in Cecil. In: Proc. ECOOP (1992)
5. Chambers, C., Leavens, G.T.: Typechecking and modules for multi-methods. In: Proc. OOPSLA (1994)
6. Chugh, R., Herman, D., Jhala, R.: Dependent types for JavaScript. In: Proc. OOPSLA (2012)
7. CircleCI: CircleCI, `https://circleci.com`
8. CircleCI: Why we're supporting Typed Clojure, and you should too! (September 2013), `http://blog.circleci.com/supporting-typed-clojure/`
9. CircleCI; O'Morain, M.: Why we're no longer using core.typed (September 2015), `http://blog.circleci.com/why-were-no-longer-using-core-typed/`
10. Facebook: Hack language specification. Tech. rep., Facebook (2014)
11. Facebook: Flow language specification. Tech. rep., Facebook (2015)
12. Harper, R., Pierce, B.: A record calculus based on symmetric concatenation. In: Proc. POPL (1991)
13. Hickey, R.: The Clojure programming language. In: Proc. DLS (2008)
14. Hickey, R.: Clojure sequence Documentation (February 2015), `http://clojure.org/sequences`
15. Lehtosalo, J.: mypy, `http://mypy-lang.org/`
16. Lerner, B.S., Politz, J.G., Guha, A., Krishnamurthi, S.: TeJaS: Retrofitting type systems for JavaScript. In: Proceedings of the 9th Symposium on Dynamic Languages. pp. 1–16. DLS '13, ACM, New York, NY, USA (2013), `http://doi.acm.org/10.1145/2508168.2508170`
17. Lucassen, J.M., Gifford, D.K.: Polymorphic effect systems. In: Proc. POPL (1988)
18. Maidl, A.M., Mascarenhas, F., Ierusalimschy, R.: Typed Lua: An optional type system for Lua. In: Proc. Dyla (2014)
19. Microsoft: Typescript language specification. Tech. Rep. Version 1.4, Microsoft (2014)
20. Millstein, T., Chambers, C.: Modular statically typed multimethods. In: Information and Computation. pp. 279–303. Springer-Verlag (2002)
21. Odersky, M., Cremet, V., Dragos, I., Dubochet, G., Emir, B., McDirmid, S., Micheloud, S., Mihaylov, N., Schinz, M., Stenman, E., Spoon, L., Zenger, M., et al.: An overview of the Scala programming language (second edition). Tech. rep., EPFL Lausanne, Switzerland (2006)
22. Strickland, T.S., Tobin-Hochstadt, S., Felleisen, M.: Practical variable-arity polymorphism. In: Proc. ESOP (2009)
23. Tobin-Hochstadt, S., Felleisen, M.: The design and implementation of Typed Scheme. In: Proc. POPL (2008)
24. Tobin-Hochstadt, S., Felleisen, M.: Logical types for untyped languages. In: Proc. ICFP. ICFP '10 (2010)
25. Vitousek, M.M., Kent, A.M., Siek, J.G., Baker, J.: Design and evaluation of gradual typing for Python. In: Proc. DLS (2014)
26. Wand, M.: Type inference for record concatenation and multiple inheritance (1989)

A Soundness for Typed Clojure

Assumption A.1 ($\mathsf{JVM}_{\mathsf{new}}$)**.** *If* $\forall i.\ v_i = C_i\ \{\overrightarrow{fld_j : v_j}\}$ *or* $v_i = \mathsf{nil}$ *and* v_i *is consistent with* ρ *then either*

- $\mathsf{JVM}_{\mathsf{new}}[C, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = C\ \{\overrightarrow{fld_k : v_k}\}$ *which is consistent with* ρ*,*
- $\mathsf{JVM}_{\mathsf{new}}[C, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = \mathsf{err}$*, or*
- $\mathsf{JVM}_{\mathsf{new}}[C, [\overrightarrow{C_i}], [\overrightarrow{v_i}]]$ *is undefined.*

Assumption A.2 ($\mathsf{JVM}_{\mathsf{getstatic}}$)**.** *If* $v_1 = C_1\ \{fld : v_f, \overrightarrow{fld_l : v_l}\}$*, then either*

- $\mathsf{JVM}_{\mathsf{getstatic}}[C_1, v_1, fld, C_2] = v_f$*, and either*
  - $v_f = C_2\ \{\overrightarrow{fld_m : v_m}\}$ *or*
  - $v_f = \mathsf{nil}$*, or*
- $\mathsf{JVM}_{\mathsf{getstatic}}[C_1, v_1, fld, C_2] = \mathsf{err}$*.*

Assumption A.3 ($\mathsf{JVM}_{\mathsf{invokestatic}}$)**.** *If* $v_1 = C_1\ \{\overrightarrow{fld_l : v_l}\}, \forall i.\ v_i = C_i\ \{\overrightarrow{fld_j : v_j}\}$ *or* $v_i = \mathsf{nil}$ *then either*

- $\mathsf{JVM}_{\mathsf{invokestatic}}[C_1, v_m, mth, [\overrightarrow{C_i}], [\overrightarrow{v_i}], C_2] = v$ *and either*
  - $v = C_2\ \{\overrightarrow{fld_m : v_m}\}$ *or* $v = \mathsf{nil}$*, or*
- $\mathsf{JVM}_{\mathsf{invokestatic}}[C_1, v_m, mth, [\overrightarrow{C_i}], [\overrightarrow{v_i}], C_2] = \mathsf{err}$*, or*
- $\mathsf{JVM}_{\mathsf{invokestatic}}[C_1, v_m, mth, [\overrightarrow{C_i}], [\overrightarrow{v_i}], C_2]$ *is undefined.*

Lemma A.1. *If* ρ *and* ρ' *agree on* $\mathsf{fv}(\psi)$ *and* $\rho \models \psi$ *then* $\rho' \models \psi$*.*

Proof. Since the relevant parts of ρ *and* ρ' *agree, the proof follows trivially.*

Lemma A.2. *If*

- $\psi_1 = \psi_2[o/x]$*,*
- $\rho_2 \models \psi_2$*,*
- $\forall v \in \mathsf{fv}(\psi_2) - x.\ \rho_1(v) = \rho_2(v)$*,*
- *and* $\rho_2(x) = \rho_1(o)$

then $\rho_1 \models \psi_1$*.*

Proof. By induction on the derivation of the model judgement.

Lemma A.3. *If* $\rho \models \Gamma$ *and* $\Gamma \vdash \psi$ *then* $\rho \models \psi$*.*

Proof. By structural induction on $\Gamma \vdash \psi$*.*

Lemma A.4. *If* $\Gamma \vdash \tau_{\pi(x)}$*,* $\rho \models \Gamma$ *and* $\rho(\pi(x)) = v$ *then* $\vdash v : \tau\ ;\ {\psi'}_+ | {\psi'}_-\ ;\ o'$ *for some* ${\psi'}_+$*,* ${\psi'}_-$ *and* o'*.*

Proof. Corollary of lemma A.3.

Lemma A.5 (Paths are independent). *If* $\rho(o) = \rho_1(o')$ *then* $\rho(\pi(o)) = \rho_1(\pi(o'))$

Proof. *By induction on* π.

Lemma A.6 (*class*). *If* $\rho \vdash (\text{class } \rho(\pi(x))) \Downarrow C$ *then* $\rho \models C_{\pi(x)}$.

Proof. *Induction on the definition of* class.

Definition A.1. v *is consistent with* ρ *iff* $\forall\, [\rho_1, \lambda x^{\sigma}.e]_{\mathsf{c}}$ *in* v, *if* $\vdash [\rho_1, \lambda x^{\sigma}.e]_{\mathsf{c}} : \tau \;;\; \mathtt{tt}|\mathtt{ff} \;;\; \emptyset$ *and* $\forall\, o'$ *in* τ, *either* $o' = \emptyset$, *or* $o' = \pi'(x)$, *or* $\rho(o') = \rho_1(o')$.

Definition A.2. ρ *is consistent iff*
$\forall v \in rng(\rho)$, v *is consistent with* ρ.

Definition A.3. $\mathsf{TrueVal}(v)$ *iff* $v \neq \mathsf{false}$ *and* $v \neq \mathsf{nil}$.

Definition A.4. $\mathsf{FalseVal}(v)$ *iff* $v = \mathsf{false}$ *or* $v = \mathsf{nil}$.

Lemma A.7 (isa? has correct propositions). *If*

- $\Gamma \vdash v_1 \Rightarrow v_1 : \tau_1 \;;\; \psi_{1+}|\psi_{1-} \;;\; o_1$,
- $\Gamma \vdash v_2 \Rightarrow v_2 : \tau_2 \;;\; \psi_{2+}|\psi_{2-} \;;\; o_2$,
- $\mathsf{IsA}(v_1, v_2) = v$,
- $\rho \models \Gamma$,
- $\mathsf{IsAProps}(o_1, \tau_2) = \psi'_+|\psi'_-$,
- $\psi'_+ \vdash \psi_+$, *and*
- $\psi'_- \vdash \psi_-$,

then either

- *if* $\mathsf{TrueVal}(v)$ *then* $\rho \models \psi_+$, *or*
- *if* $\mathsf{FalseVal}(v)$ *then* $\rho \models \psi_-$.

Proof. *By cases on the definition of* IsA *and subcases on* IsA.

> ***Subcase 1 (*$\mathsf{IsA}(v_1, v_1) = \mathsf{true}$*, if* $v_1 \neq C$*).***
> $v_1 = v_2$, $v_1 \neq C$, $v_2 \neq C$, $\mathsf{TrueVal}(v)$
> *Since* $\mathsf{TrueVal}(v)$ *we prove* $\rho \models \psi_+$ *by cases on the definition of* IsAProps*:*
>
> > ***Subcase 2 (*$\mathsf{IsAProps}(\textbf{\textit{class}}(\pi(x)), (\mathbf{Val}\, C)) = C_{\pi(x)}|\overline{C}_{\pi(x)}$*).***
> > $o_1 = \textbf{\textit{class}}(\pi(x))$, $\tau_2 = (\mathbf{Val}\, C)$, $C_{\pi(x)} \vdash \psi_+$
> > *Unreachable by inversion on the typing relation, since* $\tau_2 = (\mathbf{Val}\, C)$*, yet* $v_2 \neq C$.
> >
> > ***Subcase 3 (*$\mathsf{IsAProps}(o, (\mathbf{Val}\, l)) = ((\mathbf{Val}\, l)_x|\overline{(\mathbf{Val}\, l)}_x)[o/x]$ *if* $l \neq C$*).***
> > $\tau_2 = (\mathbf{Val}\, l)$, $l \neq C$, $(\mathbf{Val}\, l)_x[o_1/x] \vdash \psi_+$
> > *Since* $\tau_2 = (\mathbf{Val}\, l)$ *where* $l \neq C$, *by inversion on the typing judgement* v_2 *is either* true, false, nil *or* k *by T-True, T-False, T-Nil or T-Kw.*
> > *Since* $v_1 = v_2$ *then* $\tau_1 = \tau_2$, *and since* $\tau_2 = (\mathbf{Val}\, l)$ *then* $\tau_1 = (\mathbf{Val}\, l)$, *so* $\vdash v_1 : (\mathbf{Val}\, l)$
> > *If* $o_1 = \emptyset$ *then* $\psi_+ = \mathtt{tt}$ *and we derive* $\rho \models \mathtt{tt}$ *with M-Top.*
> > *Otherwise* $o_1 = \pi(x)$ *and* $(\mathbf{Val}\, l)_{\pi(x)} \vdash \psi_+$, *and since* $\vdash v_1 : (\mathbf{Val}\, l)$ *then* $\vdash \rho(\pi(x)) : (\mathbf{Val}\, l)$, *which we can use M-Type to derive* $\rho \models (\mathbf{Val}\, l)_{\pi(x)}$.

Subcase 4 *(*$\mathsf{IsAProps}(o, \tau) = \mathtt{tt}|\mathtt{tt}$*).*
$\psi_+ = \mathtt{tt}$
$\rho \models \mathtt{tt}$ *holds by M-Top.*

Subcase 5 *(*$\mathsf{IsA}(C_1, C_2) = \mathsf{true}$*, **if** *$\vdash C_1 <: C_2$*).*
$v_1 = C_1$, $v_2 = C_2$, $\vdash C_1 <: C_2$, $\mathsf{TrueVal}(v)$
Since $\mathsf{TrueVal}(v)$ *we prove* $\rho \models \psi_+$ *by cases on the definition of* IsAProps*:*

Subcase 6 *(*$\mathsf{IsAProps}(\textbf{\textit{class}}(\pi(x)), (\mathbf{Val}\, C)) = C_{\pi(x)}|\overline{C}_{\pi(x)}$*).*
$o_1 = \textbf{\textit{class}}(\pi(x))$, $\tau_2 = (\mathbf{Val}\, C_2)$, $C_{2\pi(x)} \vdash \psi_+$
By inversion on the typing relation, since ***class*** *is the last path element of* o_1 *then* $\rho \vdash (\text{class } \rho(\pi(x))) \Downarrow v_1$.
Since $\rho \vdash (\text{class } \rho(\pi(x))) \Downarrow C_1$*, as* $v_1 = C_1$*, we can derive from lemma A.6* $\rho \models C_{1\pi(x)}$.
By the induction hypothesis we can derive $\Gamma \vdash C_{1\pi(x)}$*, and with the fact* $\vdash C_1 <: C_2$ *we can use L-Sub to conclude* $\Gamma \vdash C_{2\pi(x)}$*, and finally by lemma A.3 we derive* $\rho \models C_{2\pi(x)}$.

Subcase 7 *(*$\mathsf{IsAProps}(o, (\mathbf{Val}\, l)) = ((\mathbf{Val}\, l)_x|\overline{(\mathbf{Val}\, l)}_x)[o/x]$ ***if*** *$l \neq C$*).*
$\tau_2 = (\mathbf{Val}\, l)$, $l \neq C$, $(\mathbf{Val}\, l)_x[o_1/x] \vdash \psi_+$
Unreachable case since $\tau_2 = (\mathbf{Val}\, l)$ *where* $l \neq C$*, but* $v_2 = C_2$.

Subcase 8 *(*$\mathsf{IsAProps}(o, \tau) = \mathtt{tt}|\mathtt{tt}$*).*
$\psi_+ = \mathtt{tt}$
$\rho \models \mathtt{tt}$ *holds by M-Top.*

Subcase 9 *(*$\mathsf{IsA}(v_1, v_2) = \mathsf{false}$*, **otherwise**).*
$v_1 \neq v_2$, $\mathsf{FalseVal}(v)$
Since $\mathsf{FalseVal}(v)$ *we prove* $\rho \models \psi_-$ *by cases on the definition of* IsAProps*:*

Subcase 10 *(*$\mathsf{IsAProps}(\textbf{\textit{class}}(\pi(x)), (\mathbf{Val}\, C)) = C_{\pi(x)}|\overline{C}_{\pi(x)}$*).*
$o_1 = \textbf{\textit{class}}(\pi(x))$, $\tau_2 = (\mathbf{Val}\, C)$, $\overline{C}_{\pi(x)} \vdash \psi_-$
By inversion on the typing relation, since ***class*** *is the last path element of* o_1 *then* $\rho \vdash (\text{class } \rho(\pi(x))) \Downarrow v_1$.
By the definition of class *either* $v_1 = C$ *or* $v_1 = \mathsf{nil}$.
If $v_1 = \mathsf{nil}$*, then we know from the definition of* IsA *that* $\rho(\pi(x)) = \mathsf{nil}$.
Since $\vdash \rho(\pi(x)) : \mathbf{nil}$*, and there is no* v_1 *such that both* $\vdash \rho(\pi(x)) : C$ *and* $\vdash \rho(\pi(x)) : \mathbf{nil}$*, we use M-NotType to derive* $\rho \models \overline{C}_{\pi(x)}$.
Similarly if $v_1 = C_1$*, by the definition of* IsAProps *we know* $\vdash C_1 \not<: C$ *and* $\rho(\pi(x)) = C_1$.
Since $\vdash \rho(\pi(x)) : C_1$*, and there is no* v_1 *such that both* $\vdash v_1 : C$ *and* $\vdash v_1 : C_1$*, we use M-NotType to derive* $\rho \models \overline{C}_{\pi(x)}$.

Subcase 11 *(*$\mathsf{IsAProps}(o, (\mathbf{Val}\, l)) = ((\mathbf{Val}\, l)_x|\overline{(\mathbf{Val}\, l)}_x)[o/x]$ ***if*** *$l \neq C$*).*

$\tau_2 = (\mathbf{Val}\, l)$, $l \neq C$, $\overline{(\mathbf{Val}\, l)}_x[o_1/x] \vdash \psi_-$
Since $\tau_2 = (\mathbf{Val}\, l)$ *where* $l \neq C$*, by inversion on the typing judgement* v_2 *is either* true, false, nil *or* k *by T-True, T-False, T-Nil or T-Kw.*
If $o_1 = \emptyset$ *then* $\psi_- = \mathtt{tt}$ *and we derive* $\rho \models \mathtt{tt}$ *with M-Top.*
Otherwise $o_1 = \pi(x)$ *and* $\overline{(\mathbf{Val}\, l)}_{\pi(x)} \vdash \psi_-$*. Noting that* $v_1 \neq v_2$*, we know* $\vdash \rho(\pi(x)) : \sigma$ *where* $\sigma \neq (\mathbf{Val}\, l)$*, and there is no* v_1 *such that both* $\vdash v_1 : (\mathbf{Val}\, l)$ *and* $\vdash v_1 : \sigma$ *so we can use M-NotType to derive* $\rho \models \overline{(\mathbf{Val}\, l)}_{\pi(x)}$.

Subcase 12 *(*$\mathsf{IsAProps}(o, \tau) = \mathtt{tt}|\mathtt{tt}$*).*
$\psi_- = \mathtt{tt}$
$\rho \models \mathtt{tt}$ *holds by M-Top.*

Lemma A.8. *If* $\Gamma \vdash e' \Rightarrow e : \tau \ ; \ \psi_+|\psi_- \ ; \ o$, $\rho \models \Gamma$, ρ *is consistent, and* $\rho \vdash e \Downarrow \alpha$ *then either*

- $\rho \vdash e \Downarrow v$ *and all of the following hold:*
  1. *either* $o = \emptyset$ *or* $\rho(o) = v$,
  2. *either* $\mathsf{TrueVal}(v)$ *and* $\rho \models \psi_+$ *or* $\mathsf{FalseVal}(v)$ *and* $\rho \models \psi_-$,
  3. $\vdash v \Rightarrow v : \tau \ ; \ {\psi'}_+|{\psi'}_- \ ; \ o'$ *for some* ${\psi'}_+$, ${\psi'}_-$ *and* o', *and*
  4. v *is consistent with* ρ, *or*
- $\rho \vdash e \Downarrow \mathsf{err}$.

Proof. By induction and cases on the derivation of $\rho \vdash e \Downarrow \alpha$, *and subcases on the penultimate rule of the derivation of* $\Gamma \vdash e' \Rightarrow e : \tau \ ; \ \psi_+|\psi_- \ ; \ o$ *followed by T-Subsume as the final rule.*

Case 1 (B-Val).

Subcase 13 (T-True). $v = \mathsf{true}$, $e' = \mathsf{true}$, $e = \mathsf{true}$, $\vdash \mathbf{true} <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$
Proving part 1 is trivial: o *is a superobject of* $\emptyset$, *which can only be* $\emptyset$.
To prove part 2, we note that $v = \mathsf{true}$ *and* $\mathtt{tt} \vdash \psi_+$, *so* $\rho \models \psi_+$ *by M-Top.*
Part 3 holds as e *can only be reduced to itself via B-Val.*
Part 4 holds vacuously.
Subcase 14 (T-HMap). $v = \{\overrightarrow{v_k \mapsto v_v}\}$, $e' = \{\overrightarrow{v_k \mapsto v_v}\}$, $e = \{\overrightarrow{v_k \mapsto v_v}\}$, $\vdash (\mathbf{HMap}^{\mathcal{C}}\ \mathcal{M}) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$, $\overrightarrow{\vdash v_k : (\mathbf{Val}\, k)}$, $\overrightarrow{\vdash v_v : \tau_v}$, $\mathcal{M} = \{\overrightarrow{k \mapsto \tau_v}\}$
Similar to T-True.
Part 4 holds by the induction hypothese on $\overrightarrow{v_k}$ *and* $\overrightarrow{v_v}$.
Subcase 15 (T-Kw). $v = k$, $e' = k$, $e = k$, $\vdash (\mathbf{Val}\, k) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$
Similar to T-True.

Subcase 16 (T-Str). *Similar to T-Kw.*

Subcase 17 (T-False). $v = \mathsf{false}$, $e' = \mathsf{false}$, $e = \mathsf{false}$, $\vdash \mathbf{false} <: \tau$, $\mathtt{ff} \vdash \psi_+$, $\mathtt{tt} \vdash \psi_-$, $\vdash \emptyset <: o$
Proving part 1 is trivial: o *is a superobject of* $\emptyset$, *which must be* $\emptyset$.
To prove part 2, we note that $v = \mathsf{false}$ *and* $\mathtt{tt} \vdash \psi_-$, *so* $\rho \models \psi_-$ *by M-Top.*
Part 3 holds as e *can only be reduced to itself via B-Val.*
Part 4 holds vacuously.
Subcase 18 (T-Class). $v = C$, $e' = C$, $e = C$, $\vdash (\mathbf{Val}\, C) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$
Similar to T-True.

Subcase 19 (T-Instance). $v = C\ \{\overrightarrow{fld_i : v_i}\}$, $e' = C\ \{\overrightarrow{fld : v}\}$, $e = C\ \{\overrightarrow{fld : v}\}$, $\vdash C <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$
Similar to T-True.
Part 4 holds by the induction hypotheses on $\overrightarrow{v_i}$.
Subcase 20 (T-Nil). $v = \mathsf{nil}$, $e' = \mathsf{nil}$, $e = \mathsf{nil}$, $\vdash \mathbf{nil} <: \tau$, $\mathtt{ff} \vdash \psi_+$, $\mathtt{tt} \vdash \psi_-$, $\vdash \emptyset <: o$
Similar to T-False.
Subcase 21 (T-Multi). $v = [v_1, \{\overrightarrow{v_k \mapsto v_v}\}]_{\mathsf{m}}$ $e' = [v_1, \{\overrightarrow{v_k \mapsto v_v}\}]_{\mathsf{m}}$, $\vdash v_1 \Rightarrow v_1 : \tau_1$, $\overrightarrow{\vdash v_k \Rightarrow v_k : \top}$, $\overrightarrow{\vdash v_v \Rightarrow v_v : \sigma}$, $e = [v_1, \{\overrightarrow{v_k \mapsto v_v}\}]_{\mathsf{m}}$, $\vdash (\mathbf{Multi}\, \sigma\ \tau_1) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$
Similar to T-True.
Subcase 22 (T-Const). $e = c$, $\vdash \delta_\tau(c) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$
Parts 1, 2 and 3 hold for the same reasons as T-True.

Case 2 (B-Local). $\rho(x) = v$, $\rho \vdash x \Downarrow v$

Subcase 23 (T-Local). $e' = x$, $e = x$, $\overline{(\cup\ \mathbf{nil}\ \mathbf{false})}_x \vdash \psi_+$, $(\cup\ \mathbf{nil}\ \mathbf{false})_x \vdash \psi_-$, $\vdash x <: o$, $\Gamma \vdash \tau_x$
Part 1 follows from $\rho(o) = v$*, since either* $o = x$ *and* $\rho(x) = v$ *is a premise of B-Local, or* $o = \emptyset$ *which also satisfies the goal.*
Part 2 considers two cases: if $\mathsf{TrueVal}(v)$*, then* $\rho \models \overline{(\cup\ \mathbf{nil}\ \mathbf{false})}_x$ *holds by M-NotType; if* $\mathsf{FalseVal}(v)$*, then* $\rho \models (\cup\ \mathbf{nil}\ \mathbf{false})_x$ *holds by M-Type.*
We prove part 3 by observing $\Gamma \vdash \tau_x$*,* $\rho \models \Gamma$*, and* $\rho(x) = v$ *(by B-Local) which gives us the desired result.*
Part 4 holds vacuously.

Case 3 (B-Do). $\rho \vdash e_1 \Downarrow v_1$, $\rho \vdash e_2 \Downarrow v$

Subcase 24 (T-Do). $e' = (\mathrm{do}\ e_1'\ e_2')$, $\Gamma \vdash e_1' \Rightarrow e_1 : \tau\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$, $\Gamma, \psi_{1+} \vee \psi_{1-} \vdash e' \Rightarrow e : \tau\ ;\ \psi_+|\psi_-\ ;\ o$, $e = (\mathrm{do}\ e_1\ e_2)$
For all parts we note since e_1 *can be either a true or false value then* $\rho \models \Gamma, \psi_{1+} \vee \psi_{1-}$ *by M-Or, which together with* $\Gamma, \psi_{1+} \vee \psi_{1-} \vdash e_2 : \tau\ ;\ \psi_+|\psi_-\ ;\ o$*, and* $\rho \vdash e_2 \Downarrow v$ *allows us to apply the induction hypothesis on* e_2*.*
To prove part 1 we use the induction hypothesis on e_2 *to show either* $o = \emptyset$ *or* $\rho(o) = v$*, since* e *always evaluates to the result of* e_2*.*
For part 2 we use the induction hypothesis on e_2 *to show if* $\mathsf{TrueVal}(v)$ *then* $\rho \models \psi_+$ *or if* $\mathsf{FalseVal}(v)$ *then* $\rho \models \psi_-$*.*
Parts 3 and 4 follow from the induction hypothesis on e_2*.*

Case 4 (BE-Do1). $\rho \vdash e_1 \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
Trivially reduces to an error.

Case 5 (BE-Do2). $\rho \vdash e_1 \Downarrow v_1$, $\rho \vdash e_2 \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
As above.

Case 6 (B-New). $\overrightarrow{\rho \vdash e_i \Downarrow v_i}$, $\mathsf{JVM}_{\mathsf{new}}[C_1, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = v$

Subcase 25 (T-New). $e' = (\text{new } C\overrightarrow{e_i'})$, $[\overrightarrow{C_i}] \in \mathcal{CT}[C][\mathsf{c}]$, $\overrightarrow{\mathsf{JT}_{\mathsf{nil}}(C_i) = \tau_i}$, $\overrightarrow{\Gamma \vdash e_i' \Rightarrow e_i : \tau_i}$, $e = (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i'})$, $\vdash \mathsf{JT}(C) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$

Part 1 follows $o = \emptyset$.

Part 2 requires some explanation. The two false values in Typed Clojure cannot be constructed with new, so the only case is $v \neq \mathsf{false}$ (or nil) where $\psi_+ = \mathtt{tt}$ so $\rho \models \psi_+$. **Void** *also lacks a constructor.*

Part 3 holds as B-New reduces to a non-nilable *instance of C via $\mathsf{JVM}_{\mathsf{new}}$ (by assumption A.1), and τ is a supertype of $\mathsf{JT}\ (C)$.*

Subcase 26 (T-NewStatic). $e' = (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i'})$

Non-reflective constructors cannot be written directly by the user, so we can assume the class information attached to the syntax corresponds to an actual constructor by inversion from T-New.

The rest of this case progresses like T-New.

Case 7 (BE-New1). $\overrightarrow{\rho \vdash e_{i-1} \Downarrow v_{i-1}}$, $\rho \vdash e_i \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$

Trivially reduces to an error.

Case 8 (BE-New2). $\overrightarrow{\rho \vdash e_i \Downarrow v_i}$, $\mathsf{JVM}_{\mathsf{new}}[C_1, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$

As above.

Case 9 (B-Field). $\rho \vdash e_1 \Downarrow C_1\ \{fld : v\}$

Subcase 27 (T-Field). $e' = (.\ e_1'\ fld)$, $\Gamma \vdash e' \Rightarrow e : \sigma$, $\vdash \sigma <: \mathbf{Object}$, $\mathsf{TJ}\ (\sigma) = C_1$, $fld \mapsto C_2 \in \mathcal{CT}[C_1][\mathsf{f}]$, $e = (.\ e_1\ fld_{C_2}^{C_1}) \vdash \mathsf{JT}_{\mathsf{nil}}(C_2) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{tt} \vdash \psi_-$, $\vdash \emptyset <: o$

Part 1 is trivial as o is always $\emptyset$.

Part 2 holds trivially; v can be either a true or false value and both ψ_+ and ψ_- are $\mathtt{tt}$.

Part 3 relies on the semantics of $\mathsf{JVM}_{\mathsf{getstatic}}$ (assumption A.2) in B-Field, which returns a nilable *instance of C_2, and τ is a supertype of $\mathsf{JT}_{\mathsf{nil}}(C_2)$. Notice $\vdash \sigma <: \mathbf{Object}$ is required to guard from dereferencing* nil*, as C_1 erases occurrences of* **nil** *in σ via $\mathsf{TJ}\ (\sigma) = C_1$.*

Subcase 28 (T-FieldStatic). $e' = (.\ e_1\ fld_{C_2}^{C_1})$

Non-reflective field lookups cannot be written directly by the user, so we can assume the class information attached to the syntax corresponds to an actual field by inversion from T-Field.

The rest of this case progresses like T-Field.

Case 10 (BE-Field). $\rho \vdash e_1 \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$

Trivially reduces to an error.

Case 11 (B-Method). $\rho \vdash e_m \Downarrow v_m$, $\overrightarrow{\rho \vdash e_a \Downarrow v_a}$, $\mathsf{JVM}_{\mathsf{invokestatic}}[C_1, v_m, mth, [\overrightarrow{C_a}], [\overrightarrow{v_a}], C_2] = v$

Subcase 29 (T-Method). $\Gamma \vdash e' \Rightarrow e : \sigma$, $\vdash \sigma <: \mathbf{Object}$, $\mathsf{TJ}\ (\sigma) = C_1$, $mth \mapsto [[\overrightarrow{C_i}], C_2] \in \mathcal{CT}[C_1][\mathsf{m}]$, $\overrightarrow{\mathsf{JT}_{\mathsf{nil}}(C_i) = \tau_i}$, $\overrightarrow{\Gamma \vdash e'_i \Rightarrow e_i : \tau_i}$, $e = (.\ e_m\ (mth^{C_1}_{[[\overrightarrow{C_i}], C_2]}\ \overrightarrow{e_a}))$, $\vdash \mathsf{JT}_{\mathsf{nil}}(C_2) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{tt} \vdash \psi_-$, $\vdash \emptyset <: o$
Part 1 is trivial as o is always $\emptyset$.
Part 2 holds trivially, v can be either a true or false value and both ψ_+ and ψ_- are $\mathtt{tt}$.
Part 3 relies on the semantics of $\mathsf{JVM}_{\mathsf{invokestatic}}$ (assumption A.3) in B-Method, which returns a nilable *instance of C_2, and τ is a supertype of $\mathsf{JT}_{\mathsf{nil}}(C_2) = .$ Notice $\vdash \sigma <: \mathbf{Object}$ is required to guard from dereferencing* nil*, as C_1 erases occurrences of* **nil** *in σ via $\mathsf{TJ}\ (\sigma) = C_1$.*
Subcase 30 (T-MethodStatic). $e' = (.\ e_1\ (mth^{C_1}_{[[\overrightarrow{C_i}], C_2]}\ \overrightarrow{e_i}))$
Non-reflective method invocations cannot be written directly by the user, so we can assume the class information attached to the syntax corresponds to an actual method by inversion from T-Method.
The rest of this case progresses like T-Method.

Case 12 (BE-Method1). $\rho \vdash e_m \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
Trivially reduces to an error.

Case 13 (BE-Method2). $\rho \vdash e_m \Downarrow v_m$, $\overrightarrow{\rho \vdash e_{n-1} \Downarrow v_{n-1}}$, $\rho \vdash e_n \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
As above.

Case 14 (BE-Method3). $\rho \vdash e_m \Downarrow v_m$, $\overrightarrow{\rho \vdash e_a \Downarrow v_a}$, $\mathsf{JVM}_{\mathsf{invokestatic}}[C_1, v_m, mth, [\overrightarrow{C_a}], [\overrightarrow{v_a}], C_2] = \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
As above.

Case 15 (B-DefMulti). $v = [v_d, \{\}]_{\mathsf{m}}$, $\rho \vdash e_d \Downarrow v_d$

Subcase 31 (T-DefMulti). $e' = (\text{defmulti}\ \sigma\ e'_d)$, $\sigma = x{:}\tau_1 \xrightarrow[o_1]{\psi_{1+}|\psi_{1-}} \tau_2$, $\tau_d = x{:}\tau_1 \xrightarrow[o_2]{\psi_{2+}|\psi_{2-}} \tau_3$, $\Gamma \vdash e' \Rightarrow e : \sigma'$, $e = (\text{defmulti}\ \sigma\ e_d)$, $\vdash (\mathbf{Multi}\ \sigma\ \tau_d) <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $\vdash \emptyset <: o$
Part 1 and 2 hold for the same reasons as T-True. For part 3 we show $\vdash [v_d, \{\}]_{\mathsf{m}} : (\mathbf{Multi}\ \sigma\ \tau_d)$ by T-Multi, since $\vdash v_d : \tau_d$ by the inductive hypothesis on e_d and $\{\}$ vacuously satisfies the other premises of T-Multi, so we are done.

Case 16 (BE-DefMulti). $\rho \vdash e_d \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
Trivially reduces to an error.

Case 17 (B-DefMethod).

1. $v = [v_d, t']_{\mathsf{m}}$,
2. $\rho \vdash e_m \Downarrow [v_d, t]_{\mathsf{m}}$,
3. $\rho \vdash e_v \Downarrow v_v$,

4. $\rho \vdash e_f \Downarrow v_f$,
5. $t' = t[v_v \mapsto v_f]$

Subcase 32 (T-DefMethod).

6. $e' = (\text{defmethod } e'_m\ e'_v\ e'_f)$,
7. $\tau_m = x{:}\tau_1 \xrightarrow[o_m]{\psi_{m+}|\psi_{m-}} \sigma$,
8. $\tau_d = x{:}\tau_1 \xrightarrow[o_d]{\psi_{d+}|\psi_{d-}} \sigma'$,
9. $\Gamma \vdash e'_m \Rightarrow e_m : (\mathbf{Multi}\,\tau_m\ \tau_d)$
10. $\mathsf{IsAProps}(o_d, \tau_v) = \psi_{i+}|\psi_{i-}$,
11. $\Gamma \vdash e_v \Rightarrow e_v : \tau_v$
12. $\Gamma, \tau_{1x}, \psi_{i+} \vdash e'_f \Rightarrow e_f : \sigma\ ;\ \psi_{m+}|\psi_{m-}\ ;\ o_m$
13. $e = (\text{defmethod } e_m\ e_v\ e_f)$,
14. $e_f = \lambda x^{\tau_1}.e_b$,
15. $\vdash (\mathbf{Multi}\,\tau_m\ \tau_d) <: \tau$,
16. $\mathbb{tt} \vdash \psi_+$,
17. $\mathbb{ff} \vdash \psi_-$,
18. $\vdash \emptyset <: o$

Part 1 and 2 hold for the same reasons as T-True, noting that the propositions and object agree with T-Multi.
For part 3 we show $\vdash [v_d, t[v_v \mapsto v_f]]_{\mathsf{m}} : (\mathbf{Multi}\,\tau_m\ \tau_d)$ *by noting* $\vdash v_d : \tau_d$, $\vdash v_v : \top$ *and* $\vdash v_f : \tau_m$, *and since* t *is in the correct form by the inductive hypothesis on* e_m *we can satisfy all premises of T-Multi, so we are done.*

Case 18 (BE-DefMethod1). $\rho \vdash e_m \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
Trivially reduces to an error.

Case 19 (BE-DefMethod2). $\rho \vdash e_m \Downarrow [v_d, t]_{\mathsf{m}}$, $\rho \vdash e_v \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
Trivially reduces to an error.

Case 20 (BE-DefMethod3). $\rho \vdash e_m \Downarrow [v_d, t]_{\mathsf{m}}$, $\rho \vdash e_v \Downarrow v_v$, $\rho \vdash e_f \Downarrow \mathsf{err}$, $\rho \vdash e \Downarrow \mathsf{err}$
Trivially reduces to an error.

Case 21 (B-BetaClosure).

- $\rho \vdash e \Downarrow v$,
- $\rho \vdash e_1 \Downarrow [\rho_c, \lambda x^{\sigma}.e_b]_{\mathsf{c}}$,
- $\rho \vdash e_2 \Downarrow v_2$,
- $\rho_c[x \mapsto v_2] \vdash e_b \Downarrow v$

Subcase 33 (T-App).

- $e' = (e'_1\ e'_2)$,
- $\Gamma \vdash e'_1 \Rightarrow e_1 : x{:}\sigma \xrightarrow[o_f]{\psi_{f+}|\psi_{f-}} \tau_f\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$,
- $\Gamma \vdash e'_2 \Rightarrow e_2 : \sigma\ ;\ \psi_{2+}|\psi_{2-}\ ;\ o_2$,
- $e = (e_1\ e_2)$,

- $\vdash \tau_f[o_2/x] <: \tau$,
- $\psi_{f+}[o_2/x] \vdash \psi_+$,
- $\psi_{f-}[o_2/x] \vdash \psi_-$,
- $\vdash o_f[o_2/x] <: o$

By inversion on e_1 from T-Clos there is some environment Γ_c such that

- $\rho_c \models \Gamma_c$ *and*
- $\Gamma_c \vdash \lambda x^{\sigma}.e_b : x{:}\sigma \xrightarrow[o_f]{\psi_{f+}|\psi_{f-}} \tau_f \ ; \ \psi_{1+}|\psi_{1-} \ ; \ o_1$,

and also by inversion on e_1 from T-Abs

- $\Gamma_c, \sigma_x \vdash e'_b \Rightarrow e_b : \tau_f \ ; \ \psi_{f+}|\psi_{f-} \ ; \ o_f$.

From

- $\rho_c \models \Gamma_c$,
- $\Gamma \vdash e'_2 \Rightarrow e_2 : \sigma \ ; \ \psi_{2+}|\psi_{2-} \ ; \ o_2$ *and*
- $\rho \vdash e_2 \Downarrow v_2$,

we know (by substitution) $\rho_c[x \mapsto v_2] \models \Gamma_c, \sigma_x$.
We want to prove $\Gamma_c \vdash e'_b[v_2/x] \Rightarrow e_b[v_2/x] : \tau_f[o_2/x] \ ; \ \psi_{f+}|\psi_{f-}[o_2/x] \ ; \ o_f[o_2/x]$,
which can be justified by noting

- $\Gamma_c, \sigma_x \vdash e'_b \Rightarrow e_b : \tau_f$,
- $\Gamma \vdash e'_2 \Rightarrow e_2 : \sigma \ ; \ \psi_{2+}|\psi_{2-} \ ; \ o_2$ *and*
- $\rho \vdash e_2 \Downarrow v_2$.

From the previous fact and $\rho_c \models \Gamma_c$, we know $\rho_c \vdash e_b[v_2/x] \Downarrow v$.
Noting that $\vdash \tau_f[o_2/x] <: \tau$, $\psi_{f+}[o_2/x] \vdash \psi_+$, $\psi_{f-}[o_2/x] \vdash \psi_-$ and $\vdash o_f[o_2/x] <: o$,
we can use

- $\Gamma_c \vdash e'_b[v_2/x] \Rightarrow e_b[v_2/x] : \tau_f[o_2/x] \ ; \ \psi_{f+}|\psi_{f-}[o_2/x] \ ; \ o_f[o_2/x]$,
- $\rho_c \models \Gamma_c$,
- ρ_c *is consistent (via induction hypothesis on e'_1), and*
- $\rho_c \vdash e_b[v_2/x] \Downarrow v$.

to apply the induction hypothesis on $e'_b[v_2/x]$ and satisfy all conditions.

Case 22 (B-Delta). $\rho \vdash e_1 \Downarrow c$, $\rho \vdash e_2 \Downarrow v_2$, $\delta(c, v_2) = v$

Subcase 34 (T-App).

- $e' = (e'_1 \ e'_2)$,
- $\Gamma \vdash e'_1 \Rightarrow e_1 : x{:}\sigma \xrightarrow[o_f]{\psi_{f+}|\psi_{f-}} \tau_f \ ; \ \psi_{1+}|\psi_{1-} \ ; \ o_1$,
- $\Gamma \vdash e'_2 \Rightarrow e_2 : \sigma \ ; \ \psi_{2+}|\psi_{2-} \ ; \ o_2$,
- $e = (e_1 \ e_2)$,
- $\vdash \tau_f[o_2/x] <: \tau$,
- $\psi_{f+}[o_2/x] \vdash \psi_+$,
- $\psi_{f-}[o_2/x] \vdash \psi_-$,
- $\vdash o_f[o_2/x] <: o$

Prove by cases on c.

Subcase 35 ($c =$ class). $\vdash x{:}\top \xrightarrow[\boldsymbol{class}(x)]{\mathbb{tt}|\mathbb{tt}} (\bigcup \ \mathbf{nil} \ \mathbf{Class}) <: x{:}\sigma \xrightarrow[o_f]{\psi_{f+}|\psi_{f-}} \tau_f$

Prove by cases on v_2.

Subcase 36 *($v_2 = C\ \{\overrightarrow{fld_i : v_i}\}$).* $v = C$
To prove part 1, note $\vdash o_f[o_2/x] <: o$, *and* $\vdash \textbf{\textit{class}}(x) <: o_f$. *Then either* $o = \emptyset$ *and we are done, or* $o = \textbf{\textit{class}}(o_2)$ *and by the induction hypothesis on* e_2 *we know* $\rho(o_2) = v_2$ *and by the definition of path translation we know* $\rho(\textbf{\textit{class}}(o_2)) = (\text{class}\ \rho(o_2))$, *which evaluates to* v.
Part 2 is trivial since both propositions can only be $\mathbb{tt}$.
Part 3 holds because $v = C, \vdash (\bigcup\ \textbf{nil}\ \textbf{Class}) <: \tau_f[o_2/x]$ *and* $\vdash \tau_f[o_2/x] <: \tau$, *so* $\vdash v : \tau$ *since* $\vdash C : (\bigcup\ \textbf{nil}\ \textbf{Class})$.
Subcase 37 *($v_2 = C$).* $v = \textbf{Class}$
As above.
Subcase 38 *($v_2 = \mathsf{true}$).* $v = \textbf{B}$
As above.
Subcase 39 *($v_2 = \mathsf{false}$).* $v = \textbf{B}$
As above.
Subcase 40 *($v_2 = [\rho, \lambda x^{\tau}.e]_{\mathsf{c}}$).* $v = \textbf{Fn}$
As above.
Subcase 41 *($v_2 = [v_d, t]_{\mathsf{m}}$).* $v = \textbf{Map}$
As above.
Subcase 42 *($v_2 = \{\overrightarrow{v_1 \mapsto v_2}\}$).* $v = \textbf{K}$
As above.
Subcase 43 *($v_2 = \mathsf{nil}$).* $v = \mathsf{nil}$
Parts 1 and 2 as above. Part 3 holds because $v = \mathsf{nil}$ *and* $\vdash \mathsf{nil} : (\bigcup\ \textbf{nil}\ \textbf{Class})$.

Case 23 (B-BetaMulti).

- $\rho \vdash e_1 \Downarrow [v_d, t]_{\mathsf{m}}$,
- $\rho \vdash e_2 \Downarrow v_2$,
- $\rho \vdash (v_d\ v_2) \Downarrow v_e$,
- $\mathsf{GM}\ (t,\ v_e) = v_g$,
- $\rho \vdash (v_g\ v_2) \Downarrow v$,
- $t = \{\overrightarrow{v_k \mapsto v_v}\}$

Subcase 44 (T-App).

- $e' = (e'_1\ e'_2)$,
- $\Gamma \vdash e'_1 \Rightarrow e_1 : x{:}\sigma \xrightarrow[o_f]{\psi_{f+}|\psi_{f-}} \tau_f\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$,
- $\Gamma \vdash e'_2 \Rightarrow e_2 : \sigma\ ;\ \psi_{2+}|\psi_{2-}\ ;\ o_2$,
- $e = (e_1\ e_2)$,
- $\vdash \tau_f[o_2/x] <: \tau$,
- $\psi_{f+}[o_2/x] \vdash \psi_+$,
- $\psi_{f-}[o_2/x] \vdash \psi_-$,
- $\vdash o_f[o_2/x] <: o$,

By inversion on e_1 *via T-Multi we know*

- $\Gamma \vdash e'_1 \Rightarrow e_1 : (\textbf{Multi}\,\sigma_t\ \sigma_d)\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$,
- $\sigma_t = x{:}\sigma \xrightarrow[o_f]{\psi_{f+}|\psi_{f-}} \tau_f$,

- $\sigma_d = x{:}\sigma \xrightarrow[o_d]{\psi_{d+}|\psi_{d-}} \tau_d$,
- $\vdash v_d : \sigma_d$
- $\overrightarrow{\vdash v_k : \top}$, *and*
- $\overrightarrow{\vdash v_v : \sigma_t}$.

By the inductive hypothesis on $\rho \vdash e_2 \Downarrow v_2$ *we know* $\Gamma \vdash v_2 \Rightarrow v_2 : \sigma \ ; \ \psi_{2+}|\psi_{2-} \ ; \ o_2$.
We then consider applying the evaluated argument to the dispatch function:
$\rho \vdash (v_d \ v_2) \Downarrow v_e$.
Since we can satisfy T-App with

- $\vdash v_d : x{:}\sigma \xrightarrow[o_d]{\psi_{d+}|\psi_{d-}} \tau_d$, *and*
- $\Gamma \vdash v_2 \Rightarrow v_2 : \sigma \ ; \ \psi_{2+}|\psi_{2-} \ ; \ o_2$.

we can then apply the inductive hypothesis to derive $\Gamma \vdash v_e \Rightarrow v_e : \tau_d[o_2/x] \ ; \ \psi_{d+}|\psi_{d-}[o_2/x] \ ; \ o_d[o_2/x]$.
Now we consider how we choose which method to dispatch to.
As $\mathsf{GM}\ (t, \ v_e) = v_g$, *by inversion on* GM *we know there exists exactly one* v_k *such that* $v_k \mapsto v_g \in t$ *and* $\mathsf{IsA}(v_e, v_k) = \mathsf{true}$.
By inversion we know T-DefMethod must have extended t *with the well-typed dispatch value* v_k, *thus* $\vdash v_k : \tau_k$, *and the well-typed method* v_g, *so* $\vdash v_g : \sigma_t$.
We can also prove that given

- $\Gamma \vdash v_e \Rightarrow v_e : \tau_d[o_2/x] \ ; \ \psi_{d+}|\psi_{d-}[o_2/x] \ ; \ o_d[o_2/x]$.
- $\Gamma \vdash v_k : \tau_k$,
- $\mathsf{IsA}(v_e, v_k) = \mathsf{true}$,
- $\rho \models \Gamma$,
- $\mathsf{IsAProps}(o_d[o_2/x], \tau_k) = \psi'_+|\psi'_-$,
- $\psi'_+ \vdash \psi'_+$, *and*
- $\psi'_- \vdash \psi'_-$.

we can apply Lemma A.7 to derive then $\rho \models \psi'_+$.
Now we consider applying the evaluated argument to the chosen method:
$\rho \vdash (v_g \ v_2) \Downarrow v$.
By inversion via B-DefMethod we can assume $v_g = \lambda x^\sigma.e_b$, *ie. that we have chosen a method to dispatch to that is a closure.*
Because $\rho \vdash (v_g \ v_2) \Downarrow v$ *and* $\Gamma \vdash v_2 : \sigma$, *by inversion via B-BetaClosure we know* $v = e_b[v_2/x]$.
With the following premises:

- $\Gamma, \psi'_+ \vdash e'_b[v_2/x] \Rightarrow e_b[v_2/x] : \tau_f[o_2/x] \ ; \ \psi_{f+}|\psi_{f-}[o_2/x] \ ; \ o_f[o_2/x]$,
  - *From* $\Gamma, \sigma_x \vdash e_b \Rightarrow e_b : \tau_f \ ; \ \psi_{f+}|\psi_{f-} \ ; \ o_f$ *via the inductive hypothesis on* $\rho \vdash (\lambda x^\sigma.e_b \ v_2) \Downarrow v$,
  - *then we can derive* $\Gamma \vdash e'_b[v_2/x] \Rightarrow e_b[v_2/x] : \tau_f[o_2/x] \ ; \ \psi_{f+}|\psi_{f-}[o_2/x] \ ; \ o_f[o_2/x]$ *via substitution and the fact that* x *is fresh therefore* $x \notin \mathsf{fv}(\Gamma)$ *so we do not need to substitution for* x *in* Γ.
  - $\rho \models \Gamma, \psi'_+$ *because* $\rho \models \Gamma$ *and* $\rho \models \psi'_+$ *via M-And.*
- $\rho \models \Gamma, \psi'_+$,
  - *From* $\rho \models \Gamma$ *and*
  - $\rho \models \psi'_+$ *via M-And.*
- ρ *is consistent, and*
- $\rho \vdash e_b[v_2/x] \Downarrow v$.

we can apply the inductive hypothesis to satisfy our overall goal for this subcase.

Case 24 (BE-Beta1).
Reduces to an error.

Case 25 (BE-Beta2).
Reduces to an error.

Case 26 (BE-BetaClosure).
Reduces to an error.

Case 27 (BE-BetaMulti1).
Reduces to an error.

Case 28 (BE-BetaMulti2).
Reduces to an error.

Case 29 (BE-Delta).
Reduces to an error.

Case 30 (B-IsA). $\rho \vdash e_1 \Downarrow v_1$, $\rho \vdash e_2 \Downarrow v_2$, $\mathsf{IsA}(v_1, v_2) = v$

Subcase 45 (T-IsA). $e' = (isa?\ e'_1\ e'_2)$, $\Gamma \vdash e'_1 \Rightarrow e_1 : \tau_1\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$, $\Gamma \vdash e'_2 \Rightarrow e_2 : \tau_2\ ;\ \psi_{2+}|\psi_{2-}\ ;\ o_2$, $e = (isa?\ e_1\ e_2)$, $\vdash \mathbf{B} <: \tau$, $\mathsf{IsAProps}(o_1, \tau_2) = \psi'_+|\psi'_-$, $\psi'_+ \vdash \psi_+$, $\psi'_- \vdash \psi_-$, $\vdash \emptyset <: o$
Part 1 holds trivially with $o = \emptyset$.
For part 2, by the induction hypothesis on e_1 *and* e_2 *we know* $\Gamma \vdash v_1 \Rightarrow v_1 : \tau_1\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$ *and* $\Gamma \vdash v_2 \Rightarrow v_2 : \tau_2\ ;\ \psi_{2+}|\psi_{2-}\ ;\ o_2$, *so we can then apply Lemma A.7 to reach our goal.*
Part 3 holds because by the definition of IsA v *can only be* true *or* false, *and since* $\Gamma \vdash \mathsf{true} : \tau$ *and* $\Gamma \vdash \mathsf{false} : \tau$ *we are done.*

Case 31 (BE-IsA1). $\rho \vdash e_1 \Downarrow \mathsf{err}$
Trivially reduces to an error.

Case 32 (BE-IsA2). $\rho \vdash e_1 \Downarrow v_1$, $\rho \vdash e_2 \Downarrow \mathsf{err}$
Trivially reduces to an error.

Case 33 (B-Get). $\rho \vdash e_m \Downarrow v_m$, $v_m = \{\overrightarrow{(v_a\ v_b)}\}$, $\rho \vdash e_k \Downarrow k$, $k \in dom(\{\overrightarrow{(v_a\ v_b)}\})$, $\{\overrightarrow{(v_a\ v_b)}\}[k] = v$

Subcase 46 (T-GetHMap). $e' = (\mathrm{get}\ e'_m\ e'_k)$, $\Gamma \vdash e'_m \Rightarrow e_m : (\bigcup\ \overrightarrow{(\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})})\ ;\ \psi_{m+}|\psi_{m-}\ ;\ o_m$, $\Gamma \vdash e'_k \Rightarrow e_k : (\mathbf{Val}\, k)$, $\overrightarrow{\mathcal{M}[k] = \tau_i}$, $e = (\mathrm{get}\ e_m\ e_k)$, $\vdash (\bigcup\ \overrightarrow{\tau_i}) <: \tau$, $\psi_+ = \mathbb{tt}$, $\psi_- = \mathbb{tt}$, $\vdash \boldsymbol{key}_k(x)[o_m/x] <: o$
To prove part 1 we consider two cases on the form of o_m*:*

- *if* $o_m = \emptyset$ *then* $o = \emptyset$ *by substitution, which gives the desired result;*

- *if* $o_m = \pi_m(x_m)$ *then* $\vdash \textbf{\textit{key}}_k(o_m) <: o$ *by substitution. We note by the definition of path translation* $\rho(\textbf{\textit{key}}_k(o_m)) = (\text{get } \rho(o_m)\ k)$ *and by the induction hypothesis on* e_m $\rho(o_m) = \{\overrightarrow{(v_a\ v_b)}\}$*, which together imply* $\rho(o) = (\text{get } \{\overrightarrow{(v_a\ v_b)}\}\ k)$*. Since this is the same form as B-Get, we can apply the premise* $\{\overrightarrow{(v_a\ v_b)}\}[k] = v$ *to derive* $\rho(o) = v$*.*

Part 2 holds trivially as $\psi_+ = \mathtt{tt}$ *and* $\psi_- = \mathtt{tt}$*.*

To prove part 3 we note that (by the induction hypothesis on e_m*)* $\vdash v_m : (\bigcup\ \overrightarrow{(\textbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})})$*, where* $\overrightarrow{\mathcal{M}[k] = \tau_i}$*, and both* $k \in dom(\{\overrightarrow{(v_a\ v_b)}\})$ *and* $\{\overrightarrow{(v_a\ v_b)}\}[k] = v$ *imply* $\vdash v : (\bigcup\ \overrightarrow{\tau_i})$*.*

Subcase 47 (T-GetHMapAbsent). $e' = (\text{get } e'_m\ e'_k)$, $\Gamma \vdash e'_k \Rightarrow e_k : (\textbf{Val}\, k)$, $\Gamma \vdash e'_m \Rightarrow e_m : (\textbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})$; $\psi_{m+}|\psi_{m-}$; o_m, $k \in \mathcal{A}$, $e = (\text{get } e_m\ e_k)$, $\vdash \textbf{nil} <: \tau$, $\psi_+ = \mathtt{tt}$, $\psi_- = \mathtt{tt}$, $\vdash \textbf{\textit{key}}_k(x)[o_m/x] <: o$

Unreachable subcase because $k \in dom(\{\overrightarrow{(v_a\ v_b)}\})$*, contradicts* $k \in \mathcal{A}$*.*

Subcase 48 (T-GetHMapPartialDefault). $e' = (\text{get } e'_m\ e'_k)$, $\Gamma \vdash e'_k \Rightarrow e_k : (\textbf{Val}\, k)$, $\Gamma \vdash e'_m \Rightarrow e_m : (\textbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ \mathcal{A})$; $\psi_{m+}|\psi_{m-}$; o_m, $k \notin dom(\mathcal{M})$, $k \notin \mathcal{A}$, $e = (\text{get } e_m\ e_k)$, $\tau = \top$, $\psi_+ = \mathtt{tt}$, $\psi_- = \mathtt{tt}$, $\vdash \textbf{\textit{key}}_k(x)[o_m/x] <: o$

Parts 1 and 2 are the same as the B-Get subcase. Part 3 is trivial as $\tau = \top$*.*

Case 34 (B-GetMissing). $v = \mathsf{nil}$, $\rho \vdash e_m \Downarrow \{\overrightarrow{(v_a\ v_b)}\}$, $\rho \vdash e_k \Downarrow k$, $k \notin dom(\{\overrightarrow{(v_a\ v_b)}\})$

Subcase 49 (T-GetHMap). $e' = (\text{get } e'_m\ e'_k)$, $\Gamma \vdash e'_m \Rightarrow e_m : (\bigcup\ \overrightarrow{(\textbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})})$; $\psi_{m+}|\psi_{m-}$; o_m, $\Gamma \vdash e'_k \Rightarrow e_k : (\textbf{Val}\, k)$, $\overrightarrow{\mathcal{M}[k] = \tau_i}$, $e = (\text{get } e_m\ e_k)$, $\vdash (\bigcup\ \overrightarrow{\tau_i}) <: \tau$, $\psi_+ = \mathtt{tt}$, $\psi_- = \mathtt{tt}$, $\vdash \textbf{\textit{key}}_k(x)[o_m/x] <: o$

Unreachable subcase because $k \notin dom(\{\overrightarrow{(v_a\ v_b)}\})$ *contradicts* $\mathcal{M}[k] = \tau$*.*

Subcase 50 (T-GetHMapAbsent). $e' = (\text{get } e'_m\ e'_k)$, $\Gamma \vdash e'_k \Rightarrow e_k : (\textbf{Val}\, k)$, $\Gamma \vdash e'_m \Rightarrow e_m : (\textbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})$; $\psi_{m+}|\psi_{m-}$; o_m, $k \in \mathcal{A}$, $e = (\text{get } e_m\ e_k)$, $\vdash \textbf{nil} <: \tau$, $\psi_+ = \mathtt{tt}$, $\psi_- = \mathtt{tt}$, $\vdash \textbf{\textit{key}}_k(x)[o_m/x] <: o$

To prove part 1 we consider two cases on the form of o_m*:*

- *if* $o_m = \emptyset$ *then* $o = \emptyset$ *by substitution, which gives the desired result;*
- *if* $o_m = \pi_m(x_m)$ *then* $\vdash \textbf{\textit{key}}_k(o_m) <: o$ *by substitution. We note by the definition of path translation* $\rho(\textbf{\textit{key}}_k(o_m)) = (\text{get } \rho(o_m)\ k)$ *and by the induction hypothesis on* e_m $\rho(o_m) = \{\overrightarrow{(v_a\ v_b)}\}$*, which together imply* $\rho(o) = (\text{get } \{\overrightarrow{(v_a\ v_b)}\}\ k)$*. Since this is the same form as B-GetMissing, we can apply the premise* $v = \mathsf{nil}$ *to derive* $\rho(o) = v$*.*

Part 2 holds trivially as $\psi_+ = \mathtt{tt}$ *and* $\psi_- = \mathtt{tt}$*.*

To prove part 3 we note that e_m *has type* $(\textbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})$ *where* $k \in \mathcal{A}$*, and the premises of B-GetMissing* $k \notin dom(\{\overrightarrow{(v_a\ v_b)}\})$ *and* $v = \mathsf{nil}$ *tell us* v *must be of type* τ*.*

Subcase 51 (T-GetHMapPartialDefault). $e' = (\text{get } e'_m\ e'_k)$, $\Gamma \vdash e'_k \Rightarrow e_k : (\textbf{Val}\, k)$, $\Gamma \vdash e'_m \Rightarrow e_m : (\textbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ \mathcal{A})$; $\psi_{m+}|\psi_{m-}$; o_m, $k \notin dom(\mathcal{M})$, $k \notin \mathcal{A}$, $e = (\text{get } e_m\ e_k)$, $\tau = \top$, $\psi_+ = \mathtt{tt}$, $\psi_- = \mathtt{tt}$, $\vdash \textbf{\textit{key}}_k(x)[o_m/x] <: o$

Parts 1 and 2 are the same as the B-GetMissing subcase of T-GetHMapAbsent.

Part 3 is trivial as $\tau = \top$*.*

Case 35 (BE-Get1).
Reduces to an error.

Case 36 (BE-Get2).
Reduces to an error.

Case 37 (B-Assoc). $v = \{\overrightarrow{(v_a\ v_b)}\}[k \mapsto v_v]$, $\rho \vdash e_m \Downarrow \{\overrightarrow{(v_a\ v_b)}\}$, $\rho \vdash e_k \Downarrow k$, $\rho \vdash e_v \Downarrow v_v$

Subcase 52 (T-AssocHMap). $\Gamma \vdash e'_m \Rightarrow e_m : (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})$, $\Gamma \vdash e'_k \Rightarrow e_k : (\mathbf{Val}\, k)$, $\Gamma \vdash e'_v \Rightarrow e_v : \tau$, $k \notin \mathcal{A}$, $e' = (\text{assoc}\ e'_m\ e'_k\ e'_v)$, $e = (\text{assoc}\ e_m\ e_k\ e_v)$, $\vdash (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}[k \mapsto \tau]\ \mathcal{A}) <: \tau$, $\psi_+ = \mathtt{tt}$, $\psi_- = \mathtt{ff}$, $o = \emptyset$
Parts 1 and 2 hold for the same reasons as T-True.

Case 38 (BE-Assoc1).
Reduces to an error.

Case 39 (BE-Assoc2).
Reduces to an error.

Case 40 (BE-Assoc3).
Reduces to an error.

Case 41 (B-IfFalse). $\rho \vdash e_1 \Downarrow \mathsf{false}$ *or* $\rho \vdash e_1 \Downarrow \mathsf{nil}$, $\rho \vdash e_3 \Downarrow v$

Subcase 53 (T-If). $e' = (\text{if}\ e'_1\ e'_2\ e'_3)$, $\Gamma \vdash e'_1 \Rightarrow e_1 : \tau_1\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$, $\Gamma, \psi_{1+} \vdash e'_2 \Rightarrow e_2 : \tau\ ;\ \psi_{2+}|\psi_{2-}\ ;\ o$, $\Gamma, \psi_{1-} \vdash e'_3 \Rightarrow e_3 : \tau\ ;\ \psi_{3+}|\psi_{3-}\ ;\ o$, $e = (\text{if}\ e_1\ e_2\ e_3)$, $\psi_{2+} \vee \psi_{3+} \vdash \psi_+$, $\psi_{2-} \vee \psi_{3-} \vdash \psi_-$
For part 1, either $o = \emptyset$*, or* e *evaluates to the result of* e_3*.*
To prove part 2, we consider two cases:

- *if* $\mathsf{FalseVal}(v)$ *then* e_3 *evaluates to a false value so* $\rho \models \psi_{3-}$*, and thus* $\rho \models \psi_{2-} \vee \psi_{3-}$ *by M-Or,*
- *otherwise* $\mathsf{TrueVal}(v)$*, so* e_3 *evaluates to a true value so* $\rho \models \psi_{3+}$*, and thus* $\rho \models \psi_{2+} \vee \psi_{3+}$ *by M-Or.*

Part 3 is trivial as $\rho \vdash e_3 \Downarrow v$ *and* $\vdash v : \tau$ *by the induction hypothesis on* e_3*.*

Case 42 (B-IfTrue). $\rho \vdash e_1 \Downarrow v_1$, $v_1 \neq \mathsf{false}$, $v_1 \neq \mathsf{nil}$, $\rho \vdash e_2 \Downarrow v$

Subcase 54 (T-If). $e' = (\text{if}\ e'_1\ e'_2\ e'_3)$, $\Gamma \vdash e'_1 \Rightarrow e_1 : \tau_1\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$, $\Gamma, \psi_{1+} \vdash e'_2 \Rightarrow e_2 : \tau\ ;\ \psi_{2+}|\psi_{2-}\ ;\ o$, $\Gamma, \psi_{1-} \vdash e'_3 \Rightarrow e_3 : \tau\ ;\ \psi_{3+}|\psi_{3-}\ ;\ o$, $e = (\text{if}\ e_1\ e_2\ e_3)$, $\psi_{2+} \vee \psi_{3+} \vdash \psi_+$, $\psi_{2-} \vee \psi_{3-} \vdash \psi_-$
For part 1, either $o = \emptyset$*, or* e *evaluates to the result of* e_2*.*
To prove part 2, we consider two cases:

- *if* $\mathsf{FalseVal}(v)$ *then* e_2 *evaluates to a false value so* $\rho \models \psi_{2-}$*, and thus* $\rho \models \psi_{2-} \vee \psi_{3-}$ *by M-Or,*
- *otherwise* $\mathsf{TrueVal}(v)$*, so* e_2 *evaluates to a true value so* $\rho \models \psi_{2+}$*, and thus* $\rho \models \psi_{2+} \vee \psi_{3+}$ *by M-Or.*

Part 3 is trivial as $\rho \vdash e_2 \Downarrow v$ *and* $\vdash v : \tau$ *by the induction hypothesis on* e_2*.*

Case 43 (BE-If).
Reduces to an error.

Case 44 (BE-IfFalse).
Reduces to an error.

Case 45 (BE-IfTrue).
Reduces to an error.

Case 46 (B-Let). $e = (\text{let } [x\ e_1]\ e_2)$, $\rho \vdash e_1 \Downarrow v_1$, $\rho[x \mapsto v_1] \vdash e_2 \Downarrow v$

Subcase 55 (T-Let). $e' = (\text{let } [x\ e_1']\ e_2')$, $\Gamma \vdash e_1' \Rightarrow e_1' : \sigma\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$, $\psi' = \overline{(\cup\ \mathbf{nil}\ \mathbf{false})}_x \supset \psi_{1+}$, $\psi'' = (\cup\ \mathbf{nil}\ \mathbf{false})_x \supset \psi_{1-}$, $\Gamma, \sigma_x, \psi', \psi'' \vdash e_2' \Rightarrow e_2 : \tau\ ;\ \psi_+|\psi_-\ ;\ o$
For all the following cases (with a reminder that x is fresh) we apply the induction hypothesis on e_2. We justify this by noting that occurrences of x inside e_2 have the same type as e_1 and simulate the propositions of e_1 because
- $\Gamma, \sigma_x, \psi', \psi'' \vdash e_2' \Rightarrow e_2 : \tau\ ;\ \psi_+|\psi_-\ ;\ o$,
- $\rho[x \mapsto v_1] \models \Gamma, \sigma_x, \psi', \psi''$,
- $\rho[x \mapsto v_1]$ *is consistent, and*
- $\rho[x \mapsto v_1] \vdash e_2 \Downarrow v$.

We prove parts 1, 2 and 3 by directly using the induction hypothesis on e_2.

Case 47 (BE-Let).
Reduces to an error.

Case 48 (B-Abs). $v = [\rho, \lambda x^\sigma.e_1]_\mathsf{c}$

Subcase 56 (T-Clos). $e' = [\rho, \lambda x^\sigma.e_1]_\mathsf{c}$, $\exists \Gamma'.\rho \models \Gamma'$ *and* $\Gamma' \vdash \lambda x^\sigma.e_1 \Rightarrow \lambda x^\sigma.e_1 : \tau\ ;\ \psi_{f+}|\psi_{f-}\ ;\ o_f$, $e = [\rho, \lambda x^\sigma.e_1]_\mathsf{c}$, $\psi_+ = \mathtt{tt}$, $\psi_- = \mathtt{ff}$, $o = \emptyset$
We assume some Γ', such that
- $\rho \models \Gamma'$
- $\Gamma' \vdash \lambda x^\sigma.e_1 : \tau\ ;\ \psi_+|\psi_-\ ;\ o$.

Note the last rule in the derivation of $\Gamma' \vdash \lambda x^\sigma.e_1 : \tau\ ;\ \psi_+|\psi_-\ ;\ o$ must be T-Abs, so $\psi_+ = \mathtt{tt}$, $\psi_- = \mathtt{ff}$ and $o = \emptyset$. Thus parts 1 and 2 hold for the same reasons as T-True. Part 3 holds as v has the same type as $\lambda x^\sigma.e_1$ under Γ'.

Case 49 (B-Abs). $v = [\rho, \lambda x^\sigma.e_1]_\mathsf{c}$, $\rho \vdash \lambda x^\tau.e_1 \Downarrow [\rho, \lambda x^\sigma.e_1]_\mathsf{c}$

Subcase 57 (T-Abs). $e' = \lambda x^\sigma.e_1'$, $\Gamma, \sigma_x \vdash e_1' \Rightarrow e_1 : \tau\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1$, $\vdash x{:}\sigma \xrightarrow[o_1]{\psi_{1+}|\psi_{1-}} \tau_1 <: \tau$, $\mathtt{tt} \vdash \psi_+$, $\mathtt{ff} \vdash \psi_-$, $o = \emptyset$
Parts 1 and 2 hold for the same reasons as T-True. Part 3 holds directly via T-Clos, since v must be a closure.

Case 50 (BE-Error). $\rho \vdash e \Downarrow \mathsf{err}$

Subcase 58 (T-Error). $e' = \mathsf{err}$, $e = \mathsf{err}$, $\tau = \bot$, $\psi_+ = \mathtt{ff}$, $\psi_- = \mathtt{ff}$, $o = \emptyset$
Trivially reduces to an error.

Theorem A.1 (Well-typed programs don't go wrong). *If* $\vdash e' \Rightarrow e : \tau \; ; \; \psi_+ | \psi_- \; ; \; o$ *then* $\not\vdash e \Downarrow$ *wrong.*

Proof. Corollary of lemma A.8, since by lemma A.8 when $\vdash e' \Rightarrow e : \tau \; ; \; \psi_+ | \psi_- \; ; \; o$, *either* $\vdash e \Downarrow v$ *or* $\vdash e \Downarrow \mathsf{err}$, *therefore* $\not\vdash e \Downarrow$ *wrong.*

Theorem A.2 (Type soundness). *If* $\Gamma \vdash e' \Rightarrow e : \tau \; ; \; \psi_+ | \psi_- \; ; \; o$ *and* $\rho \vdash e \Downarrow v$ *then* $\vdash v \Rightarrow v : \tau \; ; \; {\psi'}_+ | {\psi'}_- \; ; \; o'$ *for some* ${\psi'}_+$, ${\psi'}_-$ *and* o'.

Proof. Corollary of lemma A.8.

$$
\begin{array}{lll}
d, e & ::= x \mid v \mid (e\ e) \mid \lambda x^{\tau}.e \mid (\text{if } e\ e\ e) \mid (\text{do } e\ e) \mid (\text{let } [x\ e]\ e) \mid \beta \mid R \mid E \mid M \mid G & \text{Expressions} \\
v & ::= l \mid I \mid \{\} \mid c \mid n \mid s \mid m \mid [\rho, \lambda x^{\tau}.e]_{\mathsf{c}} \mid [v, t]_{\mathsf{m}} & \text{Values} \\
m & ::= \{\overrightarrow{v \mapsto v}\} & \text{Map Values} \\
c & ::= \mathit{class} \mid \mathit{n?} & \text{Constants} \\
G & ::= (\text{get } e\ e) \mid (\text{assoc } e\ e\ e) & \text{Hash Maps} \\
E & ::= (.\ e\ \mathit{fld}_C^C) \mid (.\ e\ (\mathit{mth}^C_{[[\overrightarrow{C}],C]}\ \overrightarrow{e})) \mid (\text{new}_{\overrightarrow{[C]}}\ C\ \overrightarrow{e}) & \text{Non-Reflectiv} \\
R & ::= (.\ e\ \mathit{fld}) \mid (.\ e\ (\mathit{mth}\ \overrightarrow{e})) \mid (\text{new } C\ \overrightarrow{e}) & \text{Reflective Jav} \\
M & ::= (\text{defmulti } \tau\ e) \mid (\text{defmethod } e\ e\ e) \mid (\text{isa? } e\ e) & \text{Immutable Fi}
\end{array}
$$

$$
\begin{array}{lll}
\sigma, \tau & ::= \top \mid C \mid (\mathbf{Val}\, l) \mid (\bigcup\ \overrightarrow{\tau}) \mid x{:}\tau \xrightarrow[o]{\psi|\psi} \tau \mid (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}) \mid (\mathbf{Multi}\, \tau\ \tau) & \text{Types} \\
\mathcal{M} & ::= \{\overrightarrow{k \mapsto \tau}\} & \text{HMap manda} \\
\mathcal{A} & ::= \{\overrightarrow{k}\} & \text{HMap absent} \\
\mathcal{E} & ::= \mathcal{C} \mid \mathcal{P} & \text{HMap comple} \\
l & ::= k \mid C \mid \mathsf{nil} \mid b & \text{Value types} \\
b & ::= \mathsf{true} \mid \mathsf{false} & \text{Boolean value} \\
\rho & ::= \{\overrightarrow{x \mapsto v}\} & \text{Value environ} \\
\psi & ::= \tau_{\pi(x)} \mid \overline{\tau}_{\pi(x)} \mid \psi \supset \psi \mid \psi \wedge \psi \mid \psi \vee \psi \mid \mathtt{tt} \mid \mathtt{ff} & \text{Propositions} \\
o & ::= \pi(x) \mid \emptyset & \text{Objects} \\
\pi & ::= \overrightarrow{pe} & \text{Paths} \\
pe & ::= \mathbf{class} \mid \mathbf{key}_k & \text{Path element} \\
\Gamma & ::= \overrightarrow{\psi} & \text{Proposition e} \\
t & ::= \{\overrightarrow{v \mapsto v}\} & \text{Dispatch tabl} \\
ce & ::= \{\mathsf{m} \mapsto \{\overrightarrow{\mathit{mth} \mapsto [[\overrightarrow{C}], C]}\}, \mathsf{f} \mapsto \{\overrightarrow{\mathit{fld} \mapsto C}\}, \mathsf{c} \mapsto \{[\overrightarrow{C}]\}\} & \text{Class descript} \\
\mathcal{CT} & ::= \{\overrightarrow{C \mapsto ce}\} & \text{Class Table} \\
C & ::= \mathbf{Object} \mid \mathbf{K} \mid \mathbf{Class} \mid \mathbf{B} \mid \mathbf{Fn} \mid \mathbf{Multi} \mid \mathbf{Map} \mid \mathbf{Void} & \text{Class literals} \\
I & ::= C\ \{\overrightarrow{\mathit{fld} : v}\} & \text{Class Values} \\
\beta & ::= \mathit{wrong} \mid \mathsf{err} & \text{Wrong or erro} \\
\alpha & ::= v \mid \beta & \text{Defined reduc} \\
\mathit{pol} & ::= \mathsf{pos} \mid \mathsf{neg} & \text{Substitution}
\end{array}
$$

Fig. A.1. Syntax of Terms, Types, Propositions, and Objects

$$
\begin{array}{ll}
\mathbf{nil} & \equiv (\mathbf{Val}\, \mathsf{nil}) \\
\mathbf{true} & \equiv (\mathbf{Val}\, \mathsf{true}) \\
\mathbf{false} & \equiv (\mathbf{Val}\, \mathsf{false})
\end{array}
$$

Fig. A.2. Type abbreviations

$$
\begin{array}{ll}
\Gamma \vdash e : \tau & \equiv \Gamma \vdash e : \tau \ ; \ \psi_+ | \psi_- \ ; \ o \text{ for some } \psi_+, \psi_- \text{and } o \\
\tau[o/x] & \equiv \tau[o/x]^{\mathsf{pos}} \\
\psi[o/x] & \equiv \psi[o/x]^{\mathsf{pos}} \\
\psi | \psi[o/x] & \equiv \psi | \psi[o/x]^{\mathsf{pos}} \\
o[o/x] & \equiv o[o/x]^{\mathsf{pos}}
\end{array}
$$

Fig. A.3. Judgment abbreviations

T-Local
$$\frac{\Gamma \vdash \tau_x \qquad \sigma = (\cup\ \mathbf{nil}\ \mathbf{false})}{\Gamma \vdash x : \tau\ ;\ \overline{\sigma}_x|\sigma_x\ ;\ x}$$

T-Const
$$\Gamma \vdash c : \delta_\tau(c)\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset$$

T-True
$$\Gamma \vdash \mathsf{true} : \mathbf{true}\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset$$

T-False
$$\Gamma \vdash \mathsf{false} : \mathbf{false}\ ;\ \mathtt{ff}|\mathtt{tt}\ ;\ \emptyset$$

T-Nil
$$\Gamma \vdash \mathsf{nil} : \mathbf{nil}\ ;\ \mathtt{ff}|\mathtt{tt}\ ;\ \emptyset$$

T-Num
$$\Gamma \vdash n : \mathbf{N}\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset$$

T-Do
$$\frac{\Gamma \vdash e_1 \Rightarrow e_1' : \tau_1\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1 \qquad \Gamma, \psi_{1+} \vee \psi_{1-} \vdash e \Rightarrow e' : \tau\ ;\ \psi_+|\psi_-\ ;\ o}{\Gamma \vdash (\text{do } e_1\ e) \Rightarrow (\text{do } e_1'\ e') : \tau\ ;\ \psi_+|\psi_-\ ;\ o}$$

T-If
$$\frac{\Gamma \vdash e_1 \Rightarrow e_1' : \tau_1\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1 \qquad \Gamma, \psi_{1+} \vdash e_2 \Rightarrow e_2' : \tau\ ;\ \psi_+|\psi_-\ ;\ o \qquad \Gamma, \psi_{1-} \vdash e_3 \Rightarrow e_3' : \tau\ ;\ \psi_+|\psi_-\ ;\ o \qquad e' = (\text{if } e_1'\ e_2'\ e_3')}{\Gamma \vdash (\text{if } e_1\ e_2\ e_3) \Rightarrow e' : \tau\ ;\ \psi_+|\psi_-\ ;\ o}$$

T-Let
$$\frac{\Gamma \vdash e_1 \Rightarrow e_1' : \sigma\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1 \qquad \psi' = \overline{(\cup\ \mathbf{nil}\ \mathbf{false})}_x \supset \psi_{1+} \qquad \psi'' = (\cup\ \mathbf{nil}\ \mathbf{false})_x \supset \psi_{1-} \qquad \Gamma, \sigma_x, \psi', \psi'' \vdash e_2 \Rightarrow e_2' : \tau\ ;\ \psi_+|\psi_-\ ;\ o}{\Gamma \vdash (\text{let } [x\ e_1]\ e_2) \Rightarrow (\text{let } [x\ e_1']\ e_2') : \tau[o_1/x]\ ;\ \psi_+|\psi_-[o_1/x]\ ;\ o[o_1/x]}$$

T-App
$$\frac{\Gamma \vdash e \Rightarrow e_1 : x{:}\sigma \xrightarrow[o_f]{\psi_{f+}|\psi_{f-}} \tau\ ;\ \psi_+|\psi_-\ ;\ o \qquad \Gamma \vdash e' \Rightarrow e_1' : \sigma\ ;\ \psi'_+|\psi'_-\ ;\ o'}{\Gamma \vdash (e\ e') \Rightarrow (e_1\ e_1') : \tau[o'/x]\ ;\ \psi_{f+}|\psi_{f-}[o'/x]\ ;\ o_f[o'/x]}$$

T-Abs
$$\frac{\Gamma, \sigma_x \vdash e \Rightarrow e' : \sigma'\ ;\ \psi_+|\psi_-\ ;\ o \qquad \tau = x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \sigma'}{\Gamma \vdash \lambda x^\sigma.e \Rightarrow \lambda x^\sigma.e' : \tau\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

T-Clos
$$\frac{\exists \Gamma.\rho \models \Gamma \text{ and } \Gamma \vdash \lambda x^\tau.e \Rightarrow \lambda x^\tau.e' : \sigma\ ;\ \psi_+|\psi_-\ ;\ o}{\vdash [\rho, \lambda x^\tau.e]_{\mathsf{c}} \Rightarrow [\rho, \lambda x^\tau.e']_{\mathsf{c}} : \sigma\ ;\ \psi_+|\psi_-\ ;\ o}$$

T-Error
$$\Gamma \vdash \mathsf{err} \Rightarrow \mathsf{err} : \bot\ ;\ \mathtt{ff}|\mathtt{ff}\ ;\ \emptyset$$

T-Subsume
$$\frac{\Gamma \vdash e \Rightarrow e' : \tau\ ;\ \psi_+|\psi_-\ ;\ o \qquad \Gamma, \psi_+ \vdash \psi'_+ \qquad \Gamma, \psi_- \vdash \psi'_- \qquad \vdash \tau <: \tau' \qquad \vdash o <: o'}{\Gamma \vdash e \Rightarrow e' : \tau'\ ;\ \psi'_+|\psi'_-\ ;\ o'}$$

Fig. A.4. Standard Typing Rules

T-New

$$\frac{[\overrightarrow{C_i}] \in \mathcal{CT}[C][\mathsf{c}] \qquad \overrightarrow{\mathsf{JT}_{\mathsf{nil}}(C_i) \;=\; \tau_i} \qquad \overrightarrow{\Gamma \vdash e_i \Rightarrow e_i' : \tau_i} \qquad \mathsf{JT}(C) \;=\; \tau}{\Gamma \vdash (\text{new } C\overrightarrow{e_i}) \Rightarrow (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i'}) : \tau \;;\; \mathtt{tt}|\mathtt{ff} \;;\; \emptyset}$$

T-NewStatic

$$\frac{\overrightarrow{\mathsf{JT}(C_i) \;=\; \tau_i} \qquad \mathsf{JT}(C) \;=\; \tau \qquad \overrightarrow{\Gamma \vdash e_i \Rightarrow e_i' : \tau_i}}{\Gamma \vdash (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i}) \Rightarrow (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i'}) : \tau \;;\; \mathtt{tt}|\mathtt{ff} \;;\; \emptyset}$$

T-Field

$$\frac{\Gamma \vdash e \Rightarrow e' : \sigma \quad \vdash \sigma <: \mathbf{Object} \quad \mathsf{TJ}(\sigma) \;=\; C_1 \quad fld \mapsto C_2 \in \mathcal{CT}[C_1][\mathsf{f}] \quad \mathsf{JT}_{\mathsf{nil}}(C_2) \;=\; \tau}{\Gamma \vdash (.\ e\ fld) \Rightarrow (.\ e'\ fld_{C_2}^{C_1}) : \tau \;;\; \mathtt{tt}|\mathtt{tt} \;;\; \emptyset}$$

T-FieldStatic

$$\frac{\mathsf{JT}(C_1) \;=\; \sigma \qquad \vdash \sigma <: \mathbf{Object} \qquad \mathsf{JT}_{\mathsf{nil}}(C_2) \;=\; \tau \qquad \Gamma \vdash e \Rightarrow e' : \sigma}{\Gamma \vdash (.\ e\ fld_{C_2}^{C_1}) \Rightarrow (.\ e'\ fld_{C_2}^{C_1}) : \tau \;;\; \mathtt{tt}|\mathtt{tt} \;;\; \emptyset}$$

T-Method

$$\frac{\Gamma \vdash e \Rightarrow e' : \sigma \qquad \mathsf{TJ}(\sigma) \;=\; C_1 \qquad mth \mapsto [[\overrightarrow{C_i}], C_2] \in \mathcal{CT}[C_1][\mathsf{m}] \qquad \overrightarrow{\mathsf{JT}_{\mathsf{nil}}(C_i) \;=\; \tau_i} \qquad \overrightarrow{\Gamma \vdash e_i \Rightarrow e_i' : \tau_i} \qquad \mathsf{JT}_{\mathsf{nil}}(C_2) \;=\; \tau \qquad \vdash \sigma <: \mathbf{Object}}{\Gamma \vdash (.\ e\ (mth\overrightarrow{e_i})) \Rightarrow (.\ e'\ (mth_{[[\overrightarrow{C_i}], C_2]}^{C_1}\ \overrightarrow{e_i'})) : \tau \;;\; \mathtt{tt}|\mathtt{tt} \;;\; \emptyset}$$

T-MethodStatic

$$\frac{\overrightarrow{\mathsf{JT}(C_i) \;=\; \tau_i} \qquad \mathsf{JT}(C_1) \;=\; \sigma \qquad \vdash \sigma <: \mathbf{Object} \qquad \mathsf{JT}_{\mathsf{nil}}(C_2) \;=\; \tau \qquad \Gamma \vdash e \Rightarrow e' : \sigma \qquad \overrightarrow{\Gamma \vdash e_i \Rightarrow e_i' : \tau_i}}{\Gamma \vdash (.\ e\ (mth_{[[\overrightarrow{C_i}], C_2]}^{C_1}\ \overrightarrow{e_i})) \Rightarrow (.\ e'\ (mth_{[[\overrightarrow{C_i}], C_2]}^{C_1}\ \overrightarrow{e_i'})) : \tau \;;\; \mathtt{tt}|\mathtt{tt} \;;\; \emptyset}$$

T-Class

$$\Gamma \vdash C : (\mathbf{Val}\, C) \;;\; \mathtt{tt}|\mathtt{ff} \;;\; \emptyset$$

T-Instance

$$\Gamma \vdash C\ \{\overrightarrow{fld : v}\} : C \;;\; \mathtt{tt}|\mathtt{ff} \;;\; \emptyset$$

Fig. A.5. Java Interop Typing Rules

T-DefMulti

$$\frac{\sigma = x{:}\tau \xrightarrow[o]{\psi_+|\psi_-} \tau' \qquad \sigma' = x{:}\tau \xrightarrow[o']{\psi'_+|\psi'_-} \tau'' \qquad \Gamma \vdash e \Rightarrow e' : \sigma'}{\Gamma \vdash (\text{defmulti } \sigma\ e) \Rightarrow (\text{defmulti } \sigma\ e') : (\mathbf{Multi}\,\sigma\ \sigma')\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

T-DefMethod

$$\frac{\begin{array}{c}\tau_m = x{:}\tau \xrightarrow[o]{\psi_+|\psi_-} \sigma \qquad \tau_d = x{:}\tau \xrightarrow[o']{\psi'_+|\psi'_-} \sigma' \qquad \Gamma \vdash e_m \Rightarrow e'_m : (\mathbf{Multi}\,\tau_m\ \tau_d) \\ \Gamma \vdash e_v \Rightarrow e'_v : \tau_v \qquad \mathsf{IsAProps}(o', \tau_v) = \psi''_+|\psi''_- \\ \Gamma, \tau_x, \psi''_+ \vdash e_b \Rightarrow e'_b : \sigma\ ;\ \psi_+|\psi_-\ ;\ o \qquad e' = (\text{defmethod } e'_m\ e'_v\ \lambda x^\tau.e'_b)\end{array}}{\Gamma \vdash (\text{defmethod } e_m\ e_v\ \lambda x^\tau.e_b) \Rightarrow e' : (\mathbf{Multi}\,\tau_m\ \tau_d)\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

T-IsA

$$\frac{\Gamma \vdash e \Rightarrow e_1 : \sigma\ ;\ \psi'_+|\psi'_-\ ;\ o \qquad \Gamma \vdash e' \Rightarrow e'_1 : \tau \qquad \mathsf{IsAProps}(o, \tau) = \psi_+|\psi_-}{\Gamma \vdash (\text{isa? } e\ e') \Rightarrow (\text{isa? } e_1\ e'_1) : \mathbf{B}\ ;\ \psi_+|\psi_-\ ;\ \emptyset}$$

T-Multi

$$\frac{\vdash v \Rightarrow v' : \tau \qquad \overrightarrow{\vdash v_k \Rightarrow v'_k : \top} \qquad \overrightarrow{\vdash v_v \Rightarrow v'_v : \sigma}}{\vdash [v, \{\overrightarrow{v_k \mapsto v_v}\}]_{\mathsf{m}} \Rightarrow [v', \{\overrightarrow{v'_k \mapsto v'_v}\}]_{\mathsf{m}} : (\mathbf{Multi}\,\sigma\ \tau)\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

Fig. A.6. Multimethod Typing Rules

$$\textsc{T-HMap}\quad \frac{\overrightarrow{\vdash v_k \Rightarrow v_k' : (\mathbf{Val}\, k)} \qquad \overrightarrow{\vdash v_v \Rightarrow v_v' : \tau_v} \qquad \mathcal{M} = \{\overrightarrow{k \mapsto \tau_v}\}}{\vdash \{\overrightarrow{v_k \mapsto v_v}\} \Rightarrow \{\overrightarrow{v_k' \mapsto v_v'}\} : (\mathbf{HMap}^{\mathcal{C}}\ \mathcal{M})\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

$$\textsc{T-Kw}\quad \Gamma \vdash k : (\mathbf{Val}\, k)\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset$$

$$\textsc{T-GetHMap}\quad \frac{\Gamma \vdash e \Rightarrow e' : (\bigcup\ \overrightarrow{(\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})}^{i})\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o \quad \Gamma \vdash e_k \Rightarrow e_k' : (\mathbf{Val}\, k) \quad \overrightarrow{\mathcal{M}[k] = \tau}^{i}}{\Gamma \vdash (\text{get}\ e\ e_k) \Rightarrow (\text{get}\ e'\ e_k') : (\bigcup\ \overrightarrow{\tau}^{i})\ ;\ \mathtt{tt}|\mathtt{tt}\ ;\ \mathbf{key}_k(x)[o/x]}$$

$$\textsc{T-GetHMapAbsent}\quad \frac{\Gamma \vdash e \Rightarrow e' : (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A})\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o \qquad \Gamma \vdash e_k \Rightarrow e_k' : (\mathbf{Val}\, k) \qquad k \in \mathcal{A}}{\Gamma \vdash (\text{get}\ e\ e_k) \Rightarrow (\text{get}\ e'\ e_k') : \mathbf{nil}\ ;\ \mathtt{tt}|\mathtt{tt}\ ;\ \mathbf{key}_k(x)[o/x]}$$

$$\textsc{T-GetHMapPartialDefault}\quad \frac{\begin{array}{c}\Gamma \vdash e \Rightarrow e' : (\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ \mathcal{A})\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o \\ \Gamma \vdash e_k \Rightarrow e_k' : (\mathbf{Val}\, k) \qquad k \notin dom(\mathcal{M}) \qquad k \notin \mathcal{A}\end{array}}{\Gamma \vdash (\text{get}\ e\ e_k) \Rightarrow (\text{get}\ e'\ e_k') : \top\ ;\ \mathtt{tt}|\mathtt{tt}\ ;\ \mathbf{key}_k(x)[o/x]}$$

$$\textsc{T-AssocHMap}\quad \frac{\Gamma \vdash e \Rightarrow (\text{assoc}\ e'\ e_k'\ e_v') : (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}) \quad \Gamma \vdash e_k \Rightarrow e_k' : (\mathbf{Val}\, k) \quad \Gamma \vdash e_v \Rightarrow e_v' : \tau \quad k \notin \mathcal{A}}{\Gamma \vdash (\text{assoc}\ e\ e_k\ e_v) \Rightarrow (\text{assoc}\ e'\ e_k'\ e_v') : (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}[k \mapsto \tau]\ \mathcal{A})\ ;\ \mathtt{tt}|\mathtt{ff}\ ;\ \emptyset}$$

Fig. A.7. Map Typing Rules

$$\textsc{SO-Refl}\quad \vdash o <: o \qquad\qquad \textsc{S-Refl}\quad \vdash \tau <: \tau$$

$$\textsc{SO-Top}\quad \vdash o <: \emptyset \qquad\qquad \textsc{S-Top}\quad \vdash \tau <: \top$$

$$\frac{\textsc{S-UnionSuper}\quad \exists i.\ \vdash \tau <: \sigma_i}{\vdash \tau <: (\bigcup\ \overrightarrow{\sigma}^i)} \quad \frac{\textsc{S-UnionSub}\quad \overrightarrow{\vdash \tau_i <: \sigma}^i}{\vdash (\bigcup\ \overrightarrow{\tau}^i) <: \sigma} \quad \textsc{S-FunMono}\quad \vdash x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau <: \mathbf{Fn}$$

$$\textsc{S-Object}\quad \vdash C <: \mathbf{Object}$$

$$\textsc{S-SClass}\quad \vdash (\mathbf{Val}\, C) <: \mathbf{Class}$$

$$\textsc{S-SBool}\quad \vdash (\mathbf{Val}\, b) <: \mathbf{B}$$

$$\textsc{S-SKw}\quad \vdash (\mathbf{Val}\, k) <: \mathbf{K}$$

$$\frac{\textsc{S-Fun}\quad \vdash \sigma' <: \sigma \qquad \vdash \tau <: \tau' \qquad \psi_+ \vdash \psi'_+ \qquad \psi_- \vdash \psi'_- \qquad \vdash o <: o'}{\vdash x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau <: x{:}\sigma' \xrightarrow[o']{\psi'_+|\psi'_-} \tau'}$$

$$\frac{\textsc{S-PMultiFn}\quad \vdash \sigma_t <: x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau \qquad \vdash \sigma_d <: x{:}\sigma \xrightarrow[o']{\psi'_+|\psi'_-} \tau'}{\vdash (\mathbf{Multi}\, \sigma_t\ \sigma_d) <: x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau} \quad \frac{\textsc{S-PMultiFn}\quad \vdash \sigma_t <: x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau \qquad \vdash \sigma_d <: x{:}\sigma \xrightarrow[o']{\psi'_+|\psi'_-} \tau'}{\vdash (\mathbf{Multi}\, \sigma_t\ \sigma_d) <: x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau}$$

$$\frac{\textsc{S-PMulti}\quad \vdash \sigma <: \sigma' \qquad \vdash \tau <: \tau'}{\vdash (\mathbf{Multi}\, \sigma\ \tau) <: (\mathbf{Multi}\, \sigma'\ \tau')}$$

$$\textsc{S-MultiMono}\quad \vdash (\mathbf{Multi}\, x{:}\sigma \xrightarrow[o]{\psi_+|\psi_-} \tau\ x{:}\sigma \xrightarrow[o']{\psi'_+|\psi'_-} \tau') <: \mathbf{Multi}$$

$$\frac{\textsc{S-HMapP}\quad \forall i.\ \mathcal{M}[k_i] = \sigma_i \text{ and } \vdash \sigma_i <: \tau_i}{\vdash (\mathbf{HMap}^{\mathcal{C}}\ \mathcal{M}\ \mathcal{A}') <: (\mathbf{HMap}^{\mathcal{P}}\ \overrightarrow{\{k \mapsto \tau\}}^i\ \mathcal{A})}$$

$$\frac{\textsc{S-HMap}\quad \forall i.\ \mathcal{M}[k_i] = \sigma_i \text{ and } \vdash \sigma_i <: \tau_i \qquad \mathcal{A}_1 \supseteq \mathcal{A}_2}{\vdash (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}_1) <: (\mathbf{HMap}^{\mathcal{E}}\ \overrightarrow{\{k \mapsto \tau\}}^i\ \mathcal{A}_2)} \qquad \textsc{S-HMapMono}\quad \vdash (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}) <: \mathbf{Map}$$

Fig. A.8. Subtyping rules

$$\begin{array}{lcl}
\mathsf{JT}(\mathbf{Void}) & = & \mathbf{nil} \\
\mathsf{JT}(C) & = & C \\
\mathsf{JT}_{\mathsf{nil}}(\mathbf{Void}) & = & \mathbf{nil} \\
\mathsf{JT}_{\mathsf{nil}}(C) & = & (\bigcup\ \mathbf{nil}\ C)
\end{array}$$

Fig. A.9. Java Type Conversion

$$\delta_\tau(class) = x{:}\top \xrightarrow[\mathbf{class}(x)]{\mathtt{tt}\,|\,\mathtt{tt}} (\bigcup\ \mathsf{nil}\ \ \mathbf{Class})$$
$$\delta_\tau(n?) \quad = x{:}\top \xrightarrow[\emptyset]{\mathbf{N}_x|\overline{\mathbf{N}}_x} \mathbf{B}$$

Fig. A.10. Constant Typing

$$\begin{array}{llll}
\delta(class, C\ \{\overrightarrow{fld : v}\}) = C & & \delta(class, \mathsf{true}) & = \mathbf{B} \\
\delta(class, C) & = \mathbf{Class} & \delta(class, \mathsf{false}) & = \mathbf{B} \\
\delta(class, [\rho, \lambda x^\tau.e]_\mathsf{c}) & = \mathbf{Fn} & \delta(class, \mathsf{nil}) & = \mathsf{nil} \\
\delta(class, [v_d, t]_\mathsf{m}) & = \mathbf{Multi} & & \\
\delta(class, m) & = \mathbf{Map} & \delta(n?, n) & = \mathsf{true} \\
\delta(class, k) & = \mathbf{K} & \delta(n?, e) & = \mathsf{false} \\
\delta(class, n) & = \mathbf{N} & otherwise &
\end{array}$$

Fig. A.11. Primitives

$$\begin{array}{lll}
\mathsf{IsAProps}(\mathbf{class}(\pi(x)), (\mathbf{Val}\, C)) & = C_{\pi(x)}|\overline{C}_{\pi(x)} & \\
\mathsf{IsAProps}(o, (\mathbf{Val}\, l)) & = ((\mathbf{Val}\, l)_x|\overline{(\mathbf{Val}\, l)}_x)[o/x] & \text{if } l \neq C \\
\mathsf{IsAProps}(o, \tau) & = \mathtt{tt}\,|\,\mathtt{tt} & \text{otherwise}
\end{array}$$
$$\mathsf{IsA}(v, v) \quad = \mathsf{true} \qquad v \neq C$$
$$\mathsf{IsA}(C, C') = \mathsf{true} \vdash C <: C'$$
$$\mathsf{IsA}(v, v') \quad = \mathsf{false}\ \text{otherwise}$$

Fig. A.12. Definition of isa?

$$\mathsf{GM}(t, v_e) = v_f \text{ if } \overrightarrow{v_{fs}} = \{v_f\} \text{ where } \overrightarrow{v_{fs}} = \{v_f | v_k \mapsto v_f \in t \text{ and } \mathsf{IsA}(v_e, v_k) = \mathsf{true}\}$$
$$\mathsf{GM}(t, v_e) = \mathsf{err}\ \text{otherwise}$$

Fig. A.13. Definition of get-method

$$\text{B-Local}\ \frac{\rho(x) = v}{\rho \vdash x \Downarrow v} \qquad \text{B-Do}\ \frac{\rho \vdash e_1 \Downarrow v_1 \quad \rho \vdash e \Downarrow v}{\rho \vdash (\text{do}\ e_1\ e) \Downarrow v} \qquad \text{B-Let}\ \frac{\rho \vdash e_a \Downarrow v_a \quad \rho[x \mapsto v_a] \vdash e \Downarrow v}{\rho \vdash (\text{let}\ [x\ e_a]\ e) \Downarrow v} \qquad \text{B-Val}\ \rho \vdash v \Downarrow v$$

$$\text{B-IfTrue}\ \frac{\rho \vdash e_1 \Downarrow v_1 \quad v_1 \neq \mathsf{false} \quad v_1 \neq \mathsf{nil} \quad \rho \vdash e_2 \Downarrow v}{\rho \vdash (\text{if}\ e_1\ e_2\ e_3) \Downarrow v} \qquad \text{B-IfFalse}\ \frac{\rho \vdash e_1 \Downarrow \mathsf{false}\ \text{ or }\ \rho \vdash e_1 \Downarrow \mathsf{nil} \quad \rho \vdash e_3 \Downarrow v}{\rho \vdash (\text{if}\ e_1\ e_2\ e_3) \Downarrow v}$$

$$\text{B-Abs}\ \rho \vdash \lambda x^{\tau}.e \Downarrow [\rho, \lambda x^{\tau}.e]_{\mathsf{c}} \qquad \text{B-BetaClosure}\ \frac{\rho \vdash e_f \Downarrow [\rho_c, \lambda x^{\tau}.e_b]_{\mathsf{c}} \quad \rho \vdash e_a \Downarrow v_a \quad \rho_c[x \mapsto v_a] \vdash e_b \Downarrow v}{\rho \vdash (e_f\ e_a) \Downarrow v} \qquad \text{B-Delta}\ \frac{\rho \vdash e \Downarrow c \quad \rho \vdash e' \Downarrow v \quad \delta(c, v) = v'}{\rho \vdash (e\ e') \Downarrow v'}$$

$$\text{B-BetaMulti}\ \frac{\rho \vdash e \Downarrow [v_d, t]_{\mathsf{m}} \quad \rho \vdash e' \Downarrow v' \quad \rho \vdash (v_d\ v') \Downarrow v_e \quad \mathsf{GM}(t, v_e) = v_f \quad \rho \vdash (v_f\ v') \Downarrow v}{\rho \vdash (e\ e') \Downarrow v}$$

$$\text{B-Field}\ \frac{\rho \vdash e \Downarrow v \qquad \mathsf{JVM}_{\mathsf{getstatic}}[C_1, v_1, fld, C_2] = v}{\rho \vdash (.\ e\ fld_{C_2}^{C_1}) \Downarrow v}$$

$$\text{B-Method}\ \frac{\rho \vdash e_m \Downarrow v_m \qquad \overrightarrow{\rho \vdash e_a \Downarrow v_a} \qquad \mathsf{JVM}_{\mathsf{invokestatic}}[C_1, v_m, mth, [\overrightarrow{C_a}], [\overrightarrow{v_a}], C_2] = v}{\rho \vdash (.\ e_m\ (mth^{C_1}_{[[\overrightarrow{C_a}], C_2]}\ \overrightarrow{e_a})) \Downarrow v}$$

$$\text{B-New}\ \frac{\overrightarrow{\rho \vdash e_i \Downarrow v_i} \qquad \mathsf{JVM}_{\mathsf{new}}[C_1, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = v}{\rho \vdash (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i}) \Downarrow v} \qquad \text{B-DefMulti}\ \frac{\rho \vdash e \Downarrow v_d \qquad v = [v_d, \{\}]_{\mathsf{m}}}{\rho \vdash (\text{defmulti}\ \tau\ e) \Downarrow v}$$

$$\text{B-DefMethod}\ \frac{\rho \vdash e \Downarrow [v_d, t]_{\mathsf{m}} \qquad \rho \vdash e' \Downarrow v_v \qquad \rho \vdash e_f \Downarrow v_f \qquad v = [v_d, t[v_v \mapsto v_f]]_{\mathsf{m}}}{\rho \vdash (\text{defmethod}\ e\ e'\ e_f) \Downarrow v}$$

$$\text{B-IsA}\ \frac{\rho \vdash e_1 \Downarrow v_1 \qquad \rho \vdash e_2 \Downarrow v_2 \qquad \mathsf{IsA}(v_1, v_2) = v}{\rho \vdash (\text{isa?}\ e_1\ e_2) \Downarrow v} \qquad \text{B-Assoc}\ \frac{\rho \vdash e \Downarrow m \qquad \rho \vdash e_k \Downarrow k \quad \rho \vdash e_v \Downarrow v_v}{\rho \vdash (\text{assoc}\ e\ e_k\ e_v) \Downarrow m[k \mapsto v_v]}$$

$$\text{B-Get}\ \frac{\rho \vdash e \Downarrow m \qquad \rho \vdash e' \Downarrow k \quad k \in dom(m)}{\rho \vdash (\text{get}\ e\ e') \Downarrow m[k]} \qquad \text{B-GetMissing}\ \frac{\rho \vdash e \Downarrow m \quad \rho \vdash e' \Downarrow k \qquad k \notin dom(m)}{\rho \vdash (\text{get}\ e\ e') \Downarrow \mathsf{nil}}$$

Fig. A.14. Operational Semantics

BS-MethodRefl
$\rho \vdash (.\ e\ (mth\ \overrightarrow{e})) \Downarrow wrong$

BS-FieldRefl
$\rho \vdash (.\ e\ fld) \Downarrow wrong$

BS-NewRefl
$\rho \vdash (.\ e\ fld) \Downarrow wrong$

BS-Beta
$$\frac{\rho \vdash e_f \Downarrow v \quad v \neq c \quad v \neq [v_d, t]_{\mathsf{m}} \quad v \neq [\rho_c, \lambda x^{\tau}.e_b]_{\mathsf{c}}}{\rho \vdash (e_f\ e_a) \Downarrow wrong}$$

BS-BetaMulti
$$\frac{\rho \vdash e_f \Downarrow [v, t]_{\mathsf{m}} \quad v \neq c \quad v \neq [v_d, t]_{\mathsf{m}} \quad v \neq [\rho_c, \lambda x^{\tau}.e_b]_{\mathsf{c}}}{\rho \vdash (e_f\ e_a) \Downarrow wrong}$$

BS-FieldTarget
$$\frac{\rho \vdash e \Downarrow v_1 \quad v \neq C_1\ \{\overrightarrow{fld_i : v_i}\}}{\rho \vdash (.\ e\ fld^{C_1}_{C_2}) \Downarrow wrong}$$

BS-FieldMissing
$$\frac{\rho \vdash e \Downarrow C_1\ \{\overrightarrow{fld_i : v_i}\} \quad fld \notin \{\overrightarrow{fld_i}\}}{\rho \vdash (.\ e\ fld^{C_1}_{C_2}) \Downarrow wrong}$$

BS-MethodTarget
$$\frac{\rho \vdash e_m \Downarrow v \quad v \neq C_1\ \{\overrightarrow{fld_i : v_i}\}}{\rho \vdash (.\ e_m\ (mth^{C_1}_{[[\overrightarrow{C_a}], C_2]}\ \overrightarrow{e_a})) \Downarrow wrong}$$

BS-MethodArity
$$\frac{i \neq a}{\rho \vdash (.\ e_m\ (mth^{C_1}_{[[\overrightarrow{C_i}], C_2]}\ \overrightarrow{e_a})) \Downarrow wrong}$$

BS-MethodArg
$$\frac{\rho \vdash e_m \Downarrow v_m \quad \overrightarrow{\rho \vdash e_a \Downarrow v_a} \quad \exists a.\ v_a \neq\ C_a\ \{\overrightarrow{fld_i : v_i}\}\ or\ v_a \neq \mathsf{nil}}{\rho \vdash (.\ e_m\ (mth^{C_1}_{[[\overrightarrow{C_a}], C_2]}\ \overrightarrow{e_a})) \Downarrow wrong}$$

BS-NewArg
$$\frac{\overrightarrow{\rho \vdash e_i \Downarrow v_i} \quad \exists i.\ v_i \neq\ C_i\ \{\overrightarrow{fld_i : v_i}\}\ or\ v_i \neq \mathsf{nil}}{\rho \vdash (\mathrm{new}_{\overrightarrow{[C_i]}}\ C\ \overrightarrow{e_i}) \Downarrow wrong}$$

BS-NewArity
$$\frac{i \neq a}{\rho \vdash (\mathrm{new}_{\overrightarrow{[C_i]}}\ C\ \overrightarrow{e_a}) \Downarrow wrong}$$

BS-AssocMap
$$\frac{\rho \vdash e_m \Downarrow v \quad v \neq \{\overrightarrow{(v_a\ v_b)}\}}{\rho \vdash (\mathrm{assoc}\ e_m\ e_k\ e_v) \Downarrow wrong}$$

BS-AssocKey
$$\frac{\rho \vdash e_m \Downarrow \{\overrightarrow{(v_a\ v_b)}\} \quad \rho \vdash e_k \Downarrow v_k \quad v_k \neq k}{\rho \vdash (\mathrm{assoc}\ e_m\ e_k\ e_v) \Downarrow wrong}$$

BS-GetMap
$$\frac{\rho \vdash e_m \Downarrow v \quad v \neq \{\overrightarrow{(v_a\ v_b)}\}}{\rho \vdash (\mathrm{get}\ e_m\ e_k) \Downarrow wrong}$$

BS-GetKey
$$\frac{\rho \vdash e_m \Downarrow v \quad \rho \vdash e_k \Downarrow v_k \quad v \neq k}{\rho \vdash (\mathrm{get}\ e_m\ e_k) \Downarrow wrong}$$

BS-Local
$$\frac{x \notin dom(\rho)}{\rho \vdash x \Downarrow wrong}$$

BS-DefMethod
$$\frac{\rho \vdash e_m \Downarrow v_m \quad v_m \neq [v_d, t]_{\mathsf{m}}}{\rho \vdash (\mathrm{defmethod}\ e_m\ e_v\ e_f) \Downarrow wrong}$$

Fig. A.15. Stuck programs

BE-ErrorWrong
$$\rho \vdash \beta \Downarrow \beta$$

BE-Let
$$\frac{\rho \vdash e_a \Downarrow \beta}{\rho \vdash (\text{let } [x\ e_a]\ e) \Downarrow \beta}$$

BE-Do1
$$\frac{\rho \vdash e_1 \Downarrow \beta}{\rho \vdash (\text{do } e_1\ e) \Downarrow \beta}$$

BE-Do2
$$\frac{\rho \vdash e_1 \Downarrow v_1 \quad \rho \vdash e \Downarrow \beta}{\rho \vdash (\text{do } e_1\ e) \Downarrow \beta}$$

BE-If
$$\frac{\rho \vdash e_1 \Downarrow \beta}{\rho \vdash (\text{if } e_1\ e_2\ e_3) \Downarrow \beta}$$

BE-IfTrue
$$\frac{\rho \vdash e_1 \Downarrow v_1 \quad v_1 \neq \mathsf{false} \quad v_1 \neq \mathsf{nil} \quad \rho \vdash e_2 \Downarrow \beta}{\rho \vdash (\text{if } e_1\ e_2\ e_3) \Downarrow \beta}$$

BE-IfFalse
$$\frac{\rho \vdash e_1 \Downarrow \mathsf{false} \ \text{ or } \ \rho \vdash e_1 \Downarrow \mathsf{nil} \quad \rho \vdash e_3 \Downarrow \beta}{\rho \vdash (\text{if } e_1\ e_2\ e_3) \Downarrow \beta}$$

BE-Beta1
$$\frac{\rho \vdash e_f \Downarrow \beta}{\rho \vdash (e_f\ e_a) \Downarrow \beta}$$

BE-Beta2
$$\frac{\rho \vdash e_f \Downarrow v_f \quad \rho \vdash e_a \Downarrow \beta}{\rho \vdash (e_f\ e_a) \Downarrow \beta}$$

BE-BetaClosure
$$\frac{\rho \vdash e_f \Downarrow [\rho_c, \lambda x^{\tau}.e_b]_{\mathsf{c}} \quad \rho \vdash e_a \Downarrow v_a \quad \rho_c[x \mapsto v_a] \vdash e_b \Downarrow \beta}{\rho \vdash (e_f\ e_a) \Downarrow \beta}$$

BE-BetaMulti1
$$\frac{\rho \vdash e_f \Downarrow [v_d, m]_{\mathsf{m}} \quad \rho \vdash e_a \Downarrow v_a \quad \rho \vdash (v_d\ v_a) \Downarrow \beta}{\rho \vdash (e_f\ e_a) \Downarrow \beta}$$

BE-BetaMulti2
$$\frac{\rho \vdash e_f \Downarrow [v_d, m]_{\mathsf{m}} \quad \rho \vdash e_a \Downarrow v_a \quad \rho \vdash (v_d\ v_a) \Downarrow v_e \quad \mathsf{GM}(t, v_e) = \mathsf{err}}{\rho \vdash (e_f\ e_a) \Downarrow \mathsf{err}}$$

BE-Delta
$$\frac{\rho \vdash e \Downarrow c \quad \rho \vdash e' \Downarrow v \quad \delta(c, v) = \beta}{\rho \vdash (e\ e') \Downarrow \beta}$$

BE-Field
$$\frac{\rho \vdash e \Downarrow \beta}{\rho \vdash (.\ e\ fld_{C_2}^{C_1}) \Downarrow \beta}$$

BE-Method1
$$\frac{\rho \vdash e_m \Downarrow \beta}{\rho \vdash (.\ e_m\ (mth_{[[\overrightarrow{C_a}],C_2]}^{C_1}\ \overrightarrow{e})) \Downarrow \beta}$$

BE-Method2
$$\frac{\rho \vdash e_m \Downarrow v_m \quad \overrightarrow{\rho \vdash e_{n-1} \Downarrow v_{n-1}} \quad \rho \vdash e_n \Downarrow \beta}{\rho \vdash (.\ e_m\ (mth_{[[\overrightarrow{C_a}],C_2]}^{C_1}\ \overrightarrow{e})) \Downarrow \beta}$$

BE-Method3
$$\frac{\rho \vdash e_m \Downarrow v_m \quad \overrightarrow{\rho \vdash e_a \Downarrow v_a} \quad \mathsf{JVM}_{\mathsf{invokestatic}}[C_1, v_m, mth, [\overrightarrow{C_a}], [\overrightarrow{v_a}], C_2] = \mathsf{err}}{\rho \vdash (.\ e_m\ (mth_{[[\overrightarrow{C_a}],C_2]}^{C_1}\ \overrightarrow{e_a})) \Downarrow \mathsf{err}}$$

BE-New1
$$\frac{\overrightarrow{\rho \vdash e_{n-1} \Downarrow v_{n-1}} \quad \rho \vdash e_n \Downarrow \beta}{\rho \vdash (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e}) \Downarrow \beta}$$

BE-New2
$$\frac{\overrightarrow{\rho \vdash e_i \Downarrow v_i} \quad \mathsf{JVM}_{\mathsf{new}}[C_1, [\overrightarrow{C_i}], [\overrightarrow{v_i}]] = \mathsf{err}}{\rho \vdash (\text{new}_{[\overrightarrow{C_i}]}\ C\ \overrightarrow{e_i}) \Downarrow \mathsf{err}}$$

BE-DefMulti
$$\frac{\rho \vdash e_d \Downarrow \beta}{\rho \vdash (\text{defmulti } \tau\ e_d) \Downarrow \beta}$$

BE-DefMethod1
$$\frac{\rho \vdash e_m \Downarrow \beta}{\rho \vdash (\text{defmethod } e_m\ e_v\ e_f) \Downarrow \beta}$$

BE-DefMethod2
$$\frac{\rho \vdash e_m \Downarrow [v_d, t]_{\mathsf{m}} \quad \rho \vdash e_v \Downarrow \beta}{\rho \vdash (\text{defmethod } e_m\ e_v\ e_f) \Downarrow \beta}$$

BE-DefMethod3
$$\frac{\rho \vdash e_m \Downarrow [v_d, t]_{\mathsf{m}} \quad \rho \vdash e_v \Downarrow v_v \quad \rho \vdash e_f \Downarrow \beta}{\rho \vdash (\text{defmethod } e_m\ e_v\ e_f) \Downarrow \beta}$$

BE-IsA1
$$\frac{\rho \vdash e_1 \Downarrow \beta}{\rho \vdash (\text{isa? } e_1\ e_2) \Downarrow \beta}$$

BE-IsA2
$$\frac{\rho \vdash e_1 \Downarrow v_1 \quad \rho \vdash e_2 \Downarrow \beta}{\rho \vdash (\text{isa? } e_1\ e_2) \Downarrow \beta}$$

BE-Assoc1
$$\frac{\rho \vdash e_m \Downarrow \beta}{\rho \vdash (\text{assoc } e_m\ e_k\ e_v) \Downarrow \beta}$$

BE-Assoc2
$$\frac{\rho \vdash e_m \Downarrow \{\overrightarrow{(v_a\ v_b)}\} \quad \rho \vdash e_k \Downarrow \beta}{\rho \vdash (\text{assoc } e_m\ e_k\ e_v) \Downarrow \beta}$$

BE-Assoc3
$$\frac{\rho \vdash e_m \Downarrow \{\overrightarrow{(v_a\ v_b)}\} \quad \rho \vdash e_k \Downarrow v_k \quad \rho \vdash e_v \Downarrow \beta}{\rho \vdash (\text{assoc } e_m\ e_k\ e_v) \Downarrow \beta}$$

BE-Get1
$$\frac{\rho \vdash e_m \Downarrow \beta}{\rho \vdash (\text{get } e_m\ e_k) \Downarrow \beta}$$

BE-Get2
$$\frac{\rho \vdash e_m \Downarrow \{\overrightarrow{(v_a\ v_b)}\} \quad \rho \vdash e_k \Downarrow \beta}{\rho \vdash (\text{get } e_m\ e_k) \Downarrow \beta}$$

$$
\begin{array}{lll}
\rho(x) & = v & (x, v) \in \rho \\
\rho(\mathbf{key}_k(o)) & = (\text{get } \rho(o)\ k) & \\
\rho(\mathbf{class}(o)) & = (\mathit{class}\ \rho(o)) &
\end{array}
$$

Fig. A.17. Path translation

$$
\begin{array}{lll}
\mathsf{update}((\bigcup\ \overrightarrow{\tau}), \nu, \pi) & = (\bigcup\ \overrightarrow{\mathsf{update}(\tau, \nu, \pi)}) & \\
\mathsf{update}(\tau, (\mathbf{Val}\, C), \pi :: \mathbf{class}) & = \mathsf{update}(\tau, C, \pi) & \\
\mathsf{update}(\tau, \nu, \pi :: \mathbf{class}) & = \tau & \\
\mathsf{update}((\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}), \nu, \pi :: \mathbf{key}_k) & = (\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}[k \mapsto \mathsf{update}(\tau, \nu, \pi)]\ \mathcal{A}) & \\
 & \quad \text{if } \mathcal{M}[k] = \tau & \\
\mathsf{update}((\mathbf{HMap}^{\mathcal{E}}\ \mathcal{M}\ \mathcal{A}), \nu, \pi :: \mathbf{key}_k) & = \bot \quad \text{if} \vdash \mathbf{nil} \not<: \nu \text{ and } k \in \mathcal{A} & \\
\mathsf{update}((\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ \mathcal{A}), \tau, \pi :: \mathbf{key}_k) & = (\cup\ (\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}[k \mapsto \tau]\ \mathcal{A}) & \\
 & \qquad (\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ (\mathcal{A} \cup \{k\}))) & \\
 & \quad \text{if} \vdash \mathbf{nil} <: \tau,\ k \notin \mathit{dom}(\mathcal{M}) \text{ and } k \notin \mathcal{A} & \\
\mathsf{update}((\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}\ \mathcal{A}), \nu, \pi :: \mathbf{key}_k) & = (\mathbf{HMap}^{\mathcal{P}}\ \mathcal{M}[k \mapsto \mathsf{update}(\top, \nu, \pi)]\ \mathcal{A}) & \\
 & \quad \text{if} \vdash \mathbf{nil} \not<: \nu,\ k \notin \mathit{dom}(\mathcal{M}) \text{ and } k \notin \mathcal{A} & \\
\mathsf{update}(\tau, \nu, \pi :: \mathbf{key}_k) & = \tau & \\
\mathsf{update}(\tau, \sigma, \epsilon) & = \mathsf{restrict}(\tau, \sigma) & \\
\mathsf{update}(\tau, \overline{\sigma}, \epsilon) & = \mathsf{remove}(\tau, \sigma) & \\
 & & \\
\mathsf{restrict}(\tau, \sigma) & = \bot & \text{if } \nexists v.\ \vdash v : \tau\ ;\ \psi\ ;\ o \text{ and} \vdash v : \sigma\ ;\ \psi'\ ; \\
\mathsf{restrict}(\tau, \sigma) & = \tau & \text{if} \vdash \tau <: \sigma \\
\mathsf{restrict}(\tau, \sigma) & = \sigma & \text{otherwise} \\
 & & \\
\mathsf{remove}(\tau, \sigma) & = \bot & \text{if} \vdash \tau <: \sigma \\
\mathsf{remove}(\tau, \sigma) & = \tau & \text{otherwise}
\end{array}
$$

Fig. A.18. Type Update

$$\textsc{M-Or}\ \frac{\rho \models \psi_1 \text{ or } \rho \models \psi_2}{\rho \models \psi_1 \vee \psi_2} \qquad \textsc{M-Imp}\ \frac{\rho \models \psi_1 \text{ implies } \rho \models \psi_2}{\rho \models \psi_1 \supset \psi_2} \qquad \textsc{M-And}\ \frac{\rho \models \psi_1 \qquad \rho \models \psi_2}{\rho \models \psi_1 \wedge \psi_2}$$

$$\textsc{M-Top}\ \rho \models \mathtt{tt}$$

$$\textsc{M-Type}\ \frac{\vdash \rho(\pi(x)) : \tau\ ;\ \psi_+|\psi_-\ ;\ o}{\rho \models \tau_{\pi(x)}}$$

$$\textsc{M-NotType}\ \frac{\vdash \rho(\pi(x)) : \sigma\ ;\ \psi_+|\psi_-\ ;\ o \quad \text{there is no } v \text{ such that } \vdash v : \tau\ ;\ \psi_{1+}|\psi_{1-}\ ;\ o_1 \text{ and } \vdash v : \sigma\ ;\ \psi_{2+}|\psi_{2-}\ ;\ o_2}{\rho \models \overline{\tau}_{\pi(x)}}$$

Fig. A.19. Satisfaction Relation

$$\textsc{L-Atom}\ \frac{\psi \in \Gamma}{\Gamma \vdash \psi} \qquad \textsc{L-True}\ \Gamma \vdash \mathtt{tt} \qquad \textsc{L-False}\ \frac{\Gamma \vdash \mathtt{ff}}{\Gamma \vdash \psi} \qquad \textsc{L-AndI}\ \frac{\Gamma \vdash \psi_1 \quad \Gamma \vdash \psi_2}{\Gamma \vdash \psi_1 \wedge \psi_2} \qquad \textsc{L-AndE}\ \frac{\Gamma, \psi_1, \psi_2 \vdash \psi}{\Gamma, \psi_1 \wedge \psi_2 \vdash \psi} \qquad \textsc{L-ImplI}\ \frac{\Gamma, \psi_1 \vdash \psi_2}{\Gamma \vdash \psi_1 \supset \psi_2}$$

$$\textsc{L-ImplE}\ \frac{\Gamma \vdash \psi_1 \quad \Gamma \vdash \psi_1 \supset \psi_2}{\Gamma \vdash \psi_2} \qquad \textsc{L-OrI}\ \frac{\Gamma \vdash \psi_1 \text{ or } \Gamma \vdash \psi_2}{\Gamma \vdash \psi_1 \vee \psi_2} \qquad \textsc{L-OrE}\ \frac{\Gamma, \psi_1 \vdash \psi \quad \Gamma, \psi_2 \vdash \psi}{\Gamma, \psi_1 \vee \psi_2 \vdash \psi} \qquad \textsc{L-Sub}\ \frac{\Gamma \vdash \tau_{\pi(x)} \qquad \vdash \tau <: \sigma}{\Gamma \vdash \sigma_{\pi(x)}}$$

$$\textsc{L-SubNot}\ \frac{\Gamma \vdash \overline{\sigma}_{\pi(x)} \qquad \vdash \tau <: \sigma}{\Gamma \vdash \overline{\tau}_{\pi(x)}} \qquad \textsc{L-Bot}\ \frac{\Gamma \vdash \bot_{\pi(x)}}{\Gamma \vdash \psi} \qquad \textsc{L-Update}\ \frac{\Gamma \vdash \tau_{\pi'(x)} \qquad \Gamma \vdash \nu_{\pi(\pi'(x))}}{\Gamma \vdash \mathsf{update}(\tau, \nu, \pi)_{\pi'(x)}}$$

(The metavariable ν ranges over τ and $\overline{\tau}$ (without variables).)

Fig. A.20. Proof System

$$
\begin{array}{lll}
\psi_+|\psi_-[o/x]^{pol} & = \psi_+[o/x]^{pol}|\psi_-[o/x]^{pol} & \\
\\
\nu_{\pi(x)}[\pi'(y)/x]^{pol} & = (\nu[\pi'(y)/x]^{pol})_{\pi(\pi'(y))} & \\
\nu_{\pi(x)}[\emptyset/x]^{\mathsf{pos}} & = \mathbb{tt} & \\
\nu_{\pi(x)}[\emptyset/x]^{\mathsf{neg}} & = \mathbb{ff} & \\
\nu_{\pi(x)}[o/z]^{pol} & = \nu_{\pi(x)} & x \neq z \text{ and } z \notin \mathsf{fv}(\nu) \\
\nu_{\pi(x)}[o/z]^{\mathsf{pos}} & = \mathbb{tt} & x \neq z \text{ and } z \in \mathsf{fv}(\nu) \\
\nu_{\pi(x)}[o/z]^{\mathsf{neg}} & = \mathbb{ff} & x \neq z \text{ and } z \in \mathsf{fv}(\nu) \\
\mathbb{tt}\,[o/x]^{pol} & = \mathbb{tt} & \\
\mathbb{ff}\,[o/x]^{pol} & = \mathbb{ff} & \\
(\psi_1 \supset \psi_2)[o/x]^{\mathsf{pos}} & = \psi_1[o/x]^{\mathsf{neg}} \supset \psi_2[o/x]^{\mathsf{pos}} & \\
(\psi_1 \supset \psi_2)[o/x]^{\mathsf{neg}} & = \psi_1[o/x]^{\mathsf{pos}} \supset \psi_2[o/x]^{\mathsf{neg}} & \\
(\psi_1 \vee \psi_2)[o/x]^{pol} & = \psi_1[o/x]^{pol} \vee \psi_2[o/x]^{pol} & \\
(\psi_1 \wedge \psi_2)[o/x]^{pol} & = \psi_1[o/x]^{pol} \wedge \psi_2[o/x]^{pol} & \\
\\
\pi(x)[\pi'(y)/x]^{pol} & = \pi(\pi'(y)) & \\
\pi(x)[\emptyset/x]^{pol} & = \emptyset & \\
\pi(x)[o/z]^{pol} & = \pi(x) & x \neq z \\
\emptyset[o/x]^{pol} & = \emptyset &
\end{array}
$$

Substitution on types is capture-avoiding structural recursion.

Fig. A.21. Substitution