Modular Typechecking for Hierarchically Extensible Datatypes and Functions*

Todd Millstein, Colin Bleckner, and Craig Chambers
Department of Computer Science and Engineering
University of Washington
{todd,colin,chambers}@cs.washington.edu

Technical Report UW-CSE-02-07-05
July 2002

Abstract

One promising approach for adding object-oriented (OO) facilities to functional languages like ML is to generalize the existing datatype and function constructs to be hierarchical and extensible, so that datatype variants simulate classes and function cases simulate methods. This approach allows existing datatypes to be easily extended with both new operations and new variants, resolving a long-standing conflict between the functional and OO styles. However, previous designs based on this approach have been forced to give up *modular* typechecking, requiring whole-program checks to ensure type safety. We describe Extensible ML (EML), an ML-like language that supports hierarchical, extensible datatypes and functions while preserving purely modular typechecking. To achieve this result, EML's type system imposes a few requirements on datatype and function extensibility, but EML is still able to express both traditional functional and OO idioms. We have formalized a core version of EML and proven the associated type system sound, and we have developed a prototype interpreter for the language.

*This technical report is an extended version of the paper of the same name in the 2002 International Conference on Functional Programming, Pittsburgh, PA, October 4-6, 2002.

1 Introduction

Many researchers have noted a difference in the extensibility benefits offered by the functional and object-oriented (OO) styles [26, 8, 23, 10, 18, 14, 28]. Functional languages like ML allow new operations to be easily added to existing datatypes (by adding new `fun` declarations), without requiring access to existing code. However, new data variants cannot be added without a potentially whole-program modification (since existing functions must be modified in place to handle the new variants). On the other hand, traditional OO approaches allow new data variants to be easily added to existing class hierarchies (by declaring subclasses with overriding methods), without modifying existing code. However, adding new operations to existing classes requires access to the source code for those classes (since methods cannot be added to existing classes without modifying them in place).

There have been several recent research efforts to integrate the benefits of the functional and OO styles in the context of ML. OCaml [24] adds OO features including class and method definitions to ML. The OO constructs essentially form their own sub-language which is largely separate from the existing ML `datatype` and `fun` constructs. Adding a set of new constructs has the advantage that existing language constructs are minimally affected by the extension, retaining their traditional semantics and typing properties. Further, the augmented language addresses the expressiveness differences of the functional and OO styles in a very simple way, by providing both options. However, such simplicity comes at a cost to programmers, who are forced to choose up front whether to represent an abstraction with datatypes or with classes. As described above, this decision impacts the kind of extensibility allowable for the abstraction. It may be difficult to determine *a priori* which kind of extensibility will be required, and it is difficult to change the decision after the fact. Further, it is not possible for the abstraction to enjoy both kinds of extensibility at once.

An alternative approach is to generalize existing ML constructs to support the OO style. OML [25], for example, introduces an `objtype` construct for modeling class hierarchies. This construct can be seen as a generalization of ML datatypes to be hierarchical and extensible. Therefore, programmers need not decide between datatypes and classes up front; both are embodied in the `objtype` construct. However, OML still maintains a distinction between methods and functions, which have different benefits. New methods may not be added to existing `objtype`s without modifying existing code, while ordinary ML functions may be. Methods dynamically dispatch on their associated `objtype`, while functions support ML-style pattern matching.

$ML_{\leq}$ [3] integrates the OO style further with existing ML constructs. Like OML, $ML_{\leq}$ generalizes ML datatypes to be hierarchical and extensible. Further, methods are simulated via function cases that use OO-style dynamic dispatching semantics. In this approach, programmers need not choose between two forms of extensibility; a single language mechanism supports the easy addition of both new operations and new variants to existing datatypes.

However, there are important ways in which $ML_{\leq}$ is not well integrated with existing ML language features. First, $ML_{\leq}$ does not support ML-style pattern matching. Patterns are essentially restricted to be top-level datatype constructor tests, which are the analogue of dynamic dispatch tests in OO languages. Other common ML-style patterns and patterns on sub-components cannot be programmed.

Second, extensible datatypes are of limited utility without extensible functions, which allow existing functions to be updated with new cases as new data variants are declared. However, $ML_{\leq}$ does not support extensible functions: all function cases are provided when a function is declared. The authors sketch a source-level language that supports extensible functions. Unfortunately, this critical generalization of their work causes a loss of *modular* reasoning: static typechecking of a program cannot be completed until link-time, when all modules are available. Therefore, important software engineering benefits are lost, including early detection of errors, libraries that are guaranteed to be typesafe in any context satisfying their interface requirements, independent development of typesafe modules by separate teams of programmers, and incremental modification (and subsequent incremental re-typechecking) of code.

The checks that must be delayed to link-time in $ML_{\leq}$ constitute what we call *implementation-side typechecking* (ITC), which ensures that each function in the program is completely and unambiguously implemented [7].[1] In traditional functional languages, ITC checks each function for *match nonexhaustive* and *match redundant* errors. Each function can be checked modularly, since a function declaration includes all of its cases and datatypes are not extensible. In traditional OO languages, ITC checks that each class declares or inherits a *most-specific* method for each supported operation. Each class can be checked modularly, since a class declaration includes all of its (non-inherited) methods and new operations cannot be added to existing classes.

The implicit restrictions in the traditional functional and OO settings that allow for modular ITC do not hold in

[1] Implementation-side typechecking contrasts with *client-side typechecking* of functions, which checks that each function *application* in the program is type-correct. Client-side typechecking is standard and can be performed modularly.

the presence of extensible datatypes and functions. Unlike traditional functional languages, no module is guaranteed to have access to all of a function's cases. Unlike traditional OO languages, no module is guaranteed to have access to all of a datatype variant's associated functions and function cases. Therefore, $ML_{\leq}$ is forced to perform ITC *globally*, when the whole program is available.

In this work, we describe an ML-like language called Extensible ML[2] (EML). EML introduces a `class` construct, which is a form of hierarchical, extensible datatype in the spirit of the constructs in OML and $ML_{\leq}$. As in $ML_{\leq}$, methods are simulated by function cases. In addition:

- EML generalizes the OO dispatching semantics in $ML_{\leq}$ to allow arbitrary ML-style patterns. This generalization provides idioms that are not expressible by either traditional functional or OO languages.

- EML supports extensible functions while preserving purely modular typechecking: each module can be typechecked given only the *interfaces* of the modules it *statically depends upon* (in a sense described later), with no whole-program checks required. To make per-module implementation-side typechecking sound without necessitating link-time checks, EML's type system imposes certain requirements via the notion of a function's *owner position*, which serves to coordinate otherwise independent extensions to the function. The owner position generalizes some of the properties of a method's receiver in traditional OO languages, shedding new light on how those languages achieve modular typechecking. Despite the imposed requirements, EML's classes and functions are still able to simultaneously express traditional functional and OO extensibility idioms. The requirements are adapted from our earlier work on Dubious [20, 21], a calculus designed to explore modular typechecking for OO languages based on multimethods.

The rest of the paper is organized as follows. Section 2 describes EML by example. Section 3 discusses the challenges for performing modular implementation-side typechecking in EML and presents our solution to these challenges. Section 4 defines MINI-EML, a core language for EML used to formalize our modular type system. Section 5 describes how the features of EML interact with an ML-style module system, including signature ascription and functors. Section 6 discusses related work, and section 7 concludes. The appendices contain the complete type soundness proof for MINI-EML.

2 EML by Example

Figure 1 shows an EML implementation of integer sets. Classes, functions, and function cases are declared in ML-style `struct`s. In our discussion we assume that `struct`s contain only those three kinds of declarations. This assumption is lifted in section 5, which describes the interaction of EML's features with an ML-style module system.

2.1 Classes

The `Set` class in figure 1 is the top of the integer set hierarchy. The `ListSet` class inherits from `Set`, implementing sets via lists. The `CListSet` class inherits from `ListSet`, additionally keeping track of the number of elements in the set. A program's subclass relation is the reflexive, transitive closure of the declared `extends` relation. Classes support only single inheritance. However, like Java [1, 15], EML supports a notion of `interface`, and a class can implement multiple interfaces. We ignore `interface`s in this paper for simplicity. The `Set` class is declared `abstract`, so it may not be instantiated, while its subclasses `ListSet` and `CListSet` are *concrete*.

Each class declares a record type of its instance variables, using the `of` clause. Superclass instance variables are inherited: the *representation type* of a class *C* is the representation type (recursively) of its direct superclass (if any) concatenated with the type in the `of` clause in *C*'s declaration. For example, the representation type of `CListSet` is {`es:int list,count:int`}, since `ListSet`'s representation type is {`es:int list`}.

Each class declaration also implicitly declares a constructor, similar to constructor declarations in OCaml [24] and XMOC [12], a core language for Moby [11]. For example, the `CListSet` constructor expects arguments `es` of type `int list` and `c` of type `int`, initializes inherited instance variables via the call `ListSet(es)` to the superclass constructor, and initializes the new `count` instance variable to `c`. In general, the arguments to the superclass constructor call and the instance-variable initializers may be arbitrary expressions. It would be straightforward to allow a class to have multiple constructors by introducing a separate `constructor` declaration, similar to "makers" in Moby.

Classes can be used to simulate ordinary ML-style datatypes. In particular, an ML datatype of the form

[2] not to be confused with *Extended* ML [17]

```
structure SetMod = struct
  abstract class Set() of {}
  class ListSet(es:int list) extends Set()
    of {es:int list = es}
  class CListSet(es:int list, c:int)
    extends ListSet(es) of {count:int = c}

  fun add:(int * #Set) → Set
  extend fun add (i, s as ListSet {es=es}) =
    if (member i es) then s else ListSet(i::es)
  extend fun add (i, s as CListSet {es=es,count=c}) =
    if (member i es) then s else CListSet(i::es,c+1)

  fun size:Set → int
  extend fun size (ListSet {es=es}) = length es
  extend fun size (CListSet {es=_,count=c}) = c

  fun elems:Set → int list
  extend fun elems (ListSet {es=es}) = es
end
```

Figure 1: A hierarchy of integer sets in EML.

$$\texttt{datatype DT = C}_1\ \texttt{of}\ \{\texttt{L}_{11}\texttt{:T}_{11}\texttt{,}\ldots\texttt{,L}_{1m}\texttt{:T}_{1m}\}\ \texttt{|}\ \cdots\ \texttt{|}\ \texttt{C}_r\ \texttt{of}\ \{\texttt{L}_{r1}\texttt{:T}_{r1}\texttt{,}\ldots\texttt{,L}_{rn}\texttt{:T}_{rn}\}$$

is encoded in EML by the following class declarations:

$$\texttt{abstract class DT of}\ \{\}$$
$$\texttt{class C}_1\texttt{(I}_{11}\texttt{:T}_{11}\texttt{,}\ldots\texttt{,I}_{1m}\texttt{:T}_{1m}\texttt{) extends DT() of}\ \{\texttt{L}_{11}\texttt{:T}_{11}\texttt{=I}_{11}\texttt{,}\ldots\texttt{,L}_{1m}\texttt{:T}_{1m}\texttt{=I}_{1m}\}$$
$$\ldots$$
$$\texttt{class C}_r\texttt{(I}_{r1}\texttt{:T}_{r1}\texttt{,}\ldots\texttt{,I}_{rn}\texttt{:T}_{rn}\texttt{) extends DT() of}\ \{\texttt{L}_{r1}\texttt{:T}_{r1}\texttt{=I}_{r1}\texttt{,}\ldots\texttt{,L}_{rn}\texttt{:T}_{rn}\texttt{=I}_{rn}\}$$

Unlike the variants in ordinary ML datatypes, classes are full-fledged types, and other classes may inherit from them.

A concrete class is instantiated by invoking its constructor. For example, the result of `ListSet([5,3])` is an instance of `ListSet` representing the set {5,3}. Like values of ML datatypes, class instances have no special object identity or mutable state; `ref`s can be used in a class's representation type for this purpose.

2.2 Functions and Function Cases

To make functions extensible, we break an ML-style function declaration into two pieces. The `fun` declaration introduces a function and specifies its type. The `size` function in figure 1, for example, is declared to accept an instance of `Set` or a subclass and to return an integer. The # in the `add` function's argument type signifies that the second argument to `add` is in the *owner position*. As a syntactic sugar, the owner position of a function is assumed to be the entire argument when no # is present in the function's argument type. A function and its cases must satisfy several requirements with respect to its owner position, to ensure that the function can be modularly checked for exhaustiveness and unambiguity. These requirements are discussed in section 3. The owner position has no dynamic effect.

The `extend fun` declaration adds a case to an existing function. The declaration specifies the name of the function being extended, a pattern guard, and the new case's body. There are two `size` function cases in figure 1, handling `ListSet`s and `CListSet`s, respectively. In a traditional OO language, these `size` cases would be declared as `size` methods in the `ListSet` and `CListSet` class declarations. The `extend fun` declaration is *imperative*, updating the set of cases associated with the specified function rather than creating a new function containing the extra case. The imperative semantics allows extensible functions to faithfully model OO-style methods, which conceptually update a "generic function" consisting of all methods that dynamically override some particular "top" method. The imperative semantics is necessary to support common OO idioms. For example, clients of an OO class hierarchy often import only

```
structure UnionMod = struct
  fun union:(#Set * Set) → Set
  extend fun union (s1, s2) = fold add s2 (elems s1)
  extend fun union (ListSet {es=e1}, ListSet {es=e2}) =
    ListSet {es=merge(sort(e1), sort(e2))}
end
```

Figure 2: Adding new functions in EML.

the abstract base class of the hierarchy, with any message sends through that class's interface dynamically dispatched to the appropriate methods of (potentially unknown) concrete subclasses.

An ML-style function consisting of *n* function cases is encoded in EML as a `fun` declaration followed by *n* `extend fun` declarations. EML functions can be passed to and returned from other functions, like lambdas and ML-style functions. However, a function's extensibility is second-class: new cases may only be added to statically known functions.

Patterns in EML subsume both OO-style dynamic dispatching and ML-style pattern matching. For example, the second `size` case in figure 1 is only applicable dynamically if the argument is an instance of `CListSet` or a subclass, whose instance variables match the given *representation pattern* (which in this case is fully general). As usual, the pattern also binds identifiers for use in the case's body.

An OO-style "best-match" policy decides which function case to invoke; their order does not matter. Given an application of function f with argument value v, first the *applicable* cases of f for v are retrieved. These are the cases that have a pattern that v matches. Of the applicable cases, the unique case that is *more specific* than all other applicable cases is invoked. Intuitively, case c_1 is more specific than case c_2 if the set of values matching c_1's pattern is a subset of the set of values matching c_2's pattern. We call the invoked case the *most-specific applicable* case. If a function application has no applicable cases, a *match nonexhaustive* error occurs. If a function application has at least one applicable case but no most-specific one, a *match ambiguous* error occurs.

For example, consider the invocation `size(CListSet([5,3],2))`. Both `size` cases in figure 1 are applicable to the argument value, and the second case is invoked because it is the more-specific one. The "best-match" semantics contrasts with the traditional "first-match" semantics of function cases in ML. The "first-match" semantics does not generalize naturally to handle extensible datatypes and functions, where typically the more-specific function cases are written *after* the less-specific ones, as new data variants are defined.

Implementation-side typechecking ensures that *match nonexhaustive* and *match ambiguous* errors cannot occur at run-time. Each module's typechecks include ITC for functions whose exhaustiveness and unambiguity may be affected by the module. These are functions declared in the module, functions with cases declared in the module, and functions that can accept instances of classes declared in the module. For example, ITC of `SetMod` in figure 1 checks the three functions declared there. Consider checking the `size` function for exhaustiveness and unambiguity. Any `ListSet` instance will invoke the first `size` case, and any `CListSet` instance will invoke the second `size` case. The `Set` class need not have a most-specific applicable case, because `Set` is declared `abstract`. Therefore, ITC for `size` succeeds. On the other hand, if the first `size` case were missing, a *match nonexhaustive* error would be signaled statically. Alternatively, if another `size` case with pattern `ListSet {es=es}` were declared, a *match ambiguous* error would be signaled statically.

2.3 Adding New Functions

As with ML datatypes, but unlike traditional classes, EML supports the easy addition of new functions to an existing class hierarchy. For example, figure 2 adds a function for computing the union of two `Set`s, without modifying any code in the `SetMod` module.[3] Two `union` function cases are provided. The first case is applicable to any pair of `Set`s. The second `union` case provides a more efficient implementation for two `ListSet`s. ITC of `UnionMod` checks `union` for exhaustiveness and unambiguity. Any pair of `ListSet`s and `CListSet`s will invoke the second `union` case, so the function's check succeeds.

[3] Technically, all references to `Set`, `ListSet`, `add`, and `elems` in `UnionMod` should instead be to `SetMod.Set`, `SetMod.ListSet`, `SetMod.add`, and `SetMod.elems`. For readability, we omit the full path names in examples when clear from context.

```
structure HashSetMod = struct
  class HashSet(ht:(int,unit) hashtable)
    extends Set() of {ht:(int,unit) hashtable = ht}

  extend fun add (i, s as HashSet {ht=ht}) =
    if containsKey(i,ht) then s else HashSet(put(i,(),ht))

  extend fun size (HashSet {ht=ht}) = numEntries(ht)

  extend fun elems (HashSet {ht=ht}) = keyList(ht)
end
```

Figure 3: Adding new data variants in EML.

```
structure SortedListSetMod = struct
  class SListSet(es:int list) extends ListSet(es) of {}

  extend fun add (i, s as SListSet {es=es}) =
    if (member i es) then s else
    let (lo,hi) = partition (fn j=>j<i) es
    in SListSet(lo@(i::hi)) end

  extend fun union (SListSet {es=e1}, SListSet {es=e2}) =
    SListSet(merge(e1,e2))

  fun getMin:SListSet → int
  extend fun getMin (SListSet {es=es}) = hd(es)
end
```

Figure 4: Class hierarchies in EML.

2.4 Adding New Data Variants

Unlike ML datatypes, classes in EML also support the easy addition of new data variants to existing hierarchies, without modifying existing code. An example is shown in figure 3, which provides a new implementation `HashSet` of sets using an existing implementation (not shown) of hash tables. Implementations of `add`, `size`, and `elems` are provided for the new kind of set. In a traditional OO language, `HashSetMod` corresponds to the declaration of a new subclass of `Set` with some overriding methods. ITC of `HashSetMod` re-checks `add`, `size`, and `elems` to ensure that they handle `HashSet` instances. For example, if the new `size` case were not declared, a *match nonexhaustive* error for `size` would be signaled statically.

`HashSetMod` and `UnionMod` from figure 2 illustrate EML's support for both OO and functional forms of extensibility in a single class hierarchy. The original `Set` abstraction is flexibly reused by clients, who add a specialized implementation (subclass) of the abstraction and also augment the abstraction with client-specific functionality, all without modifying existing code. `HashSetMod` and `UnionMod` are completely independent: either, both, or neither module could be linked into the final program. In this way, different versions of the `Set` abstraction may be used in different programs, depending on the needs of each application.

If both `UnionMod` and `HashSetMod` are present in a program, then `HashSet` implicitly supports the `union` operation and inherits any applicable cases. This expressiveness is at the heart of the problem of modular ITC. Because the two modules are independent, neither is "aware" of the other during its static typechecks. Therefore, neither module's ITC ensures that `union` is completely and unambiguously implemented for `HashSets`. In this example, `union` happens to have a case that handles `HashSets` (by handling any pair of sets). Without extra requirements, however, things do not always work out so well, as we show in section 3.

Another example of data-variant extensibility is illustrated in figure 4. A new subclass of `ListSet` is created, representing an implementation of sets via sorted lists. `SListSet` inherits the representation type of `ListSet` (adding

```
abstract class 'a Set() of {}
class 'a ListSet(es:'a list) extends 'a Set()
  of {es:'a list = es}
class 'a CListSet(es:'a list, c:int)
  extends 'a ListSet(es) of {count:int = c}

fun 'a add:  ('a * # 'a Set * ('a → 'a Set → bool)) → 'a Set
extend fun 'a add (i, s as ListSet {es=es}, member) =
  if (member i s) then s else 'a ListSet(i::es)
extend fun 'a add (i, s as CListSet {es=es,count=c}, member) =
  if (member i s) then s else 'a CListSet(i::es,c+1)
```

Figure 5: Polymorphic sets in EML.

no new instance variables) as well as the applicable function cases of `size` and `elems`. Overriding cases of `add` and `union` are provided, as well as a new operation for accessing the minimum element of a set implemented as a sorted list. ITC of `SortedListSetMod` checks `add`, `size`, `elems`, `union`, and `getMin` to ensure exhaustiveness and unambiguity for `SListSets`.

2.5 Parametric Polymorphism

EML supports a polymorphic type system. Class, function, and function case declarations optionally bind *type variables*. References to a polymorphic class or function specify a particular *type instantiation*. As an example, figure 5 shows some of the declarations for a polymorphic version of the sets in figure 1. Each class in the set hierarchy is now parameterized by the element type, as is the `add` function. Each function case is also explicitly parameterized, allowing its function's type variables to be renamed for use in the case's body. References to classes in a case's pattern do not contain type parameters. The appropriate type instantiation for such classes can be inferred from the declared argument type (for example, the reference to `CListSet` in the second `add` case's pattern is implicitly `'a CListSet`).

EML's polymorphic type system is deliberately simple in several ways. First, EML is explicitly typed. Second, we require that subclasses have the same type variables as their superclasses. This requirement is consistent with polymorphism in ML, where data variants have the same type variables as their associated datatype. Third, type parameters are *invariant*; for example, T_1 `ListSet` is a subtype of T_2 `Set` if and only if T_1=T_2. Finally, there is no support for bounded polymorphism, which would, for example, obviate the need to explicitly pass the membership function to `add`.

We have chosen to make the polymorphic type system simple because polymorphism is orthogonal to the problems of modular ITC that we address in this work. Those problems arise from the fact that some related classes, functions, and function cases are not modularly "aware" of one another; the problems are neither reduced nor exacerbated by polymorphic types. Therefore, our polymorphic type system could be generalized in standard ways without affecting our results. For example, we could adopt $ML_{\leq}$'s subtype-constrained polymorphic types [3] and associated decidable type system. Recent work [2] has presented a simplified account of $ML_{\leq}$'s type system and has additionally shown how to incorporate a form of type inference.

3 Modular Implementation-side Typechecking

This section focuses on the problem of modular ITC for EML. First we define our notion of modular typechecking. Next we illustrate the ways in which naive modular ITC is unsound. Finally we describe the requirements we impose to achieve modular type safety.

3.1 Modular Typechecking

We say that a language's typechecking scheme is *modular* if it has two properties. First, each module *m* can be typechecked given only the *interfaces* of other modules (without requiring access to the associated implementations).

```
structure ShapeMod = struct
  abstract class Shape() of {}
  fun intersect:(#Shape * Shape) → bool
end
structure CircleMod = struct
  class Circle() extends Shape() of {}
  extend fun intersect(Circle _, Shape _) = ···
end
```

```
structure RectMod = struct
  class Rect() extends Shape() of {}
  extend fun intersect(Shape _, Rect _) = ···
  fun print:Shape → unit
  extend fun print(Rect _) = ···
end
```

Figure 6: Challenges for modular implementation-side typechecking.

Second, *m* can be typechecked given only those interfaces that *m statically depends upon*. Module *m* statically depends upon interface *i* if either of the following conditions holds:

- Module *m* refers to a name that is bound in *i*.
- Module *m* statically depends upon module interface i', and i' refers to a name that is bound in *i*.

Traditional functional languages can support modular typechecking. For example, each structure in ML could be typechecked given only its statically depended-upon structure interfaces. A structure's interface is either an explicitly ascribed signature or else the structure's *principal signature*. Similarly, each class in a standard OO language can be typechecked given only the statically depended-upon class interfaces. Informally, the interface of a class consists of its list of superclasses, the types of its visible fields, and the headers, but not bodies, of its visible methods.

A modular typechecking scheme for EML must typecheck each structure given only the interfaces it statically depends upon. We implicitly use a structure's principal signature as its interface. The principal signature of an EML structure includes all of its class and function declarations, as well as the headers (but not the bodies) of all function case declarations. Explicit signatures provide a richer notion of structure interface, as described in section 5. Classes, functions, and cases that are declared in *m* or specified in an interface upon which *m* statically depends are said to be *available* during the typechecking of *m*. All other classes, functions, and cases are *unavailable* and may not be considered during the typechecking of *m*.

Our definition of modular typechecking validates the intuition that `union` of figure 2 and `HashSet` of figure 3 are not "aware" of one another. Neither `UnionMod` nor `HashSetMod` statically depends upon the other's interface. Therefore, `HashSet` is unavailable during modular typechecks on `UnionMod` and `union` is unavailable during modular typechecks on `HashSetMod`, so neither module's typechecks ensure that `union` properly handles `HashSet`s.

3.2 Implementation-side Typechecking and Modularity

Consider ITC for an EML module *m*. A straightforward approach to modular ITC checks each of *m*'s available functions *f* for exhaustiveness and unambiguity, given all available function cases and classes. We call this approach *naive modular ITC*. Unfortunately, naive modular ITC is unsound. The hierarchy of EML classes in figure 6 illustrates the kinds of problems that can occur. Naive modular ITC in `ShapeMod` checks `intersect` for exhaustiveness and unambiguity. Since `ShapeMod` doesn't statically depend upon any interfaces (other than its own), the check succeeds vacuously: `Shape` is abstract and so need not have an `intersect` implementation. Since `CircleMod` declares a new `intersect` case, `intersect` is again checked during naive modular ITC in `CircleMod`. `CircleMod` statically depends on the interface of `ShapeMod` but not that of `RectMod`, so `CircleMod`'s check does not consider the `Rect` class.[4] Therefore, the only argument to check from `CircleMod` is a pair of two `Circle`s. The `intersect` case in `CircleMod` is most-specific for two `Circle`s, so `intersect` is found to be exhaustive and unambiguous. By similar reasoning, `intersect` passes the checks from `RectMod`, since `RectMod` does not statically depend on the interface of `CircleMod`.

Therefore each module typechecks, with naive modular ITC declaring the `intersect` function to be both exhaustive and unambiguous. However, `intersect` has neither of these properties. If `intersect` is invoked on a pair of a `Rect` and a `Circle` (in that order), a *match nonexhaustive* error will occur since neither `intersect` case is applicable. If `intersect` is invoked on a pair of a `Circle` and a `Rect` (in that order), a *match ambiguous* error will occur since both `intersect` cases apply but neither is more specific than the other.

[4] Indeed, `RectMod` may not even have been written when `CircleMod` is typechecked.

A final problem concerns the print function in RectMod. Since RectMod does not statically depend on CircleMod's interface, RectMod's naive modular ITC finds print to be exhaustive and unambiguous. However, if a Circle is ever passed to print, a *match nonexhaustive* error will result.

3.3 Achieving Modular ITC

As we have seen, naive modular ITC is too permissive, allowing forms of extensibility that are not typesafe. To address this problem, we augment naive modular ITC with some requirements on EML modules that ensure the soundness of ITC. A fundamental design goal is that the requirements still allow the use of both functional and OO extensibility idioms in a single class hierarchy. We are willing to sacrifice other kinds of extensibility allowed by naive modular ITC to support the traditional functional and OO idioms in a modularly typesafe manner.

Functional languages allow a new function to be added to an existing datatype. Therefore, EML must allow a new function to be added to an existing class. OO languages allow a new subclass to be added to an existing class, along with associated overriding methods that have the new subclass as their receiver. To formulate this idiom in EML we employ a function's owner position, which generalizes a similar notion in the Dubious language [20]. A function's owner position has some properties in common with the receiver position in standard OO languages. Rather than forcing the owner position to be the "first" argument to a function, it can be specified as an arbitrary (and arbitrarily nested) position of the argument, via the # in a function's declared argument type. The type at the owner position in a function's argument type must be a class; that class is the function's *owner*. For example, Set is the owner of add in figure 1. To express the OO extensibility idiom in EML, we must allow a new subclass to be added to an existing class *C*, along with overriding cases of functions for which *C* is the owner.

For the purposes of our modular requirements, we partition functions into two categories. A function is called *internal* if it is declared in the same module as its owner; otherwise the function is *external*. An internal function is guaranteed to be available to all modules that declare subclasses of the function's owner, while that is not true of an external function. Therefore, an internal function can be thought of as part of the "initial" interfaces of its owner class and subclasses, while an external function is a later extension to those interfaces. External functions have no analogue in traditional OO languages, in which a class's methods must all be declared with the class. The special properties of internal functions are exploited in one of our three requirements, which are now discussed in turn.

3.3.1 Completeness Requirement for External Functions

Consider the completeness problem with the print function in RectMod in figure 6. Because new subclasses can be added to existing classes, some subclasses of a function's owner may not be available in the function's module. Indeed, Circle is not available in print's module. On the other hand, because print is external, there is no guarantee that print will be available to all modules declaring subclasses of Shape. Indeed, print is not available to Circle's module. Therefore, to modularly ensure that print is complete, we require its module to contain a *global default* case. A global default is a case whose pattern is applicable to all type-correct arguments to the function. In general, we require a module that declares an external function to include a global default case for the function.

Therefore, ITC on RectMod fails, because the global-default requirement is not satisfied for its external function print. If print had a case with, for example, pattern (Shape {}), then the requirement would be satisfied and the completeness problem for Circle would be avoided. As another example, the external function union in figure 2 satisfies the requirement because its first case is a global default, thereby handling the unavailable HashSet class of figure 3 and any other unavailable Set subclasses.

The global-default requirement does not impose an extra burden from the point of view of standard OO languages, as such languages do not even allow external functions to be declared. However, standard functional languages do allow external functions, without requiring global default cases. Those languages disallow data-variant extension, so an external function can be modularly checked against all possible data variants. EML's modular ITC must allow for the possibility of unavailable subclasses of a function's owner, thereby sometimes requiring the declaration of global default cases that will never be used. Section 5 introduces a mechanism for *sealing* class hierarchies, which can obviate the need for global default cases.

3.3.2 Completeness Requirement for Internal Functions

Consider the incompleteness for a pair of one Rect and one Circle in the internal intersect function of figure 6. One way to solve the problem would be to require a global default case, as we require for external functions. Indeed, if ShapeMod contained an intersect case that is applicable to any pair of Shapes, the incompleteness would be resolved. While requiring global default cases solves the problem, it is unnecessarily burdensome. As mentioned earlier, an internal function is guaranteed to be available to all modules declaring subclasses of the function's owner. Therefore, rather than requiring the function's module to handle all unknown subclasses, we can require each module that declares a concrete subclass of the function's owner to ensure completeness for its subclass. This idea is inspired by standard OO languages, in which a method in an abstract class may safely remain unimplemented, with each concrete subclass declaring or inheriting a concrete implementation of the method.

Our requirement is that each module declaring a concrete subclass *C* of an internal function's owner must also declare or inherit a *local default* case for the function. A local default case of a class *C* is a case whose pattern accepts only instances of *C* and subclasses at the owner position, while every other argument position can be passed any value of the appropriate type. Local default cases are the EML analogue of traditional OO methods, which dispatch on the surrounding class at the receiver position and do not dispatch on any other argument position. A class's local default cases ensure that the class completely implements all of the functions in its "initial" interface.

Given the local-default requirement, ITC on RectMod fails to typecheck because it does not declare or inherit a local default intersect case for Rect. (An isomorphic error would occur in CircleMod if the second argument position in the pair were designated the owner position.) The requirement would be satisfied, for example, if RectMod had an intersect case with pattern (Rect _, Shape _), accepting Rects at the owner position and accepting all Shapes in the other position. That case resolves the incompleteness for a pair of one Rect and one Circle. A global default case need not be written: intersect may still be safely left unimplemented for two Shapes. As another example, the internal add function in figure 1 does not have a global default case. Instead, it has local default cases for its two concrete subclasses ListSet and CListSet. When HashSet is introduced in figure 3, an associated local default is also declared, satisfying the requirement and ensuring that add is complete for HashSets.

The local-default requirement does not impose an extra burden from the point of view of standard OO languages. Whenever a local default case of some internal function *f* is required for a class *C*, an OO language would require *C*'s declaration to contain an *f* method, so that *C* is properly implemented. Therefore, the abstract-class idioms of traditional OO languages are preserved in EML. However, standard functional languages do allow internal functions, without requiring local default cases. As above, this is possible because such languages disallow data-variant extension. EML's ITC must always assume the possibility of unavailable subclasses of classes in non-owner positions of a function's argument type, thereby sometimes requiring the declaration of local default cases that will never be used. Again, we can use sealing, discussed in section 5, to obviate the need for local default cases.

3.3.3 Ambiguity Requirement

In figure 6 the two intersect cases are ambiguous, but neither CircleMod nor RectMod statically depends upon the other, so the ambiguity is not modularly detected. We address this problem by restricting EML's function extensibility such that cases declared in modules that do not statically depend upon one another are guaranteed to be *disjoint*: the cases are not applicable to a common value and hence are not ambiguous. Our restriction generalizes the implicit restrictions in standard functional and OO languages. First we introduce the concept of a function case's *owner*, which is the class (if any) at the owner position of the case's pattern. For example, ListSet is the owner of the second union case in figure 2 because it appears at the owner position, while the first union case has no owner.

In functional languages, each case must be declared in the module that declares the associated function. In OO languages, each method must be declared inside the method's receiver. Our requirement is the disjunction of these conditions: every function case must either be declared in the module that declares the case's function or in the module that declares the case's owner (if any).

RectMod now fails to typecheck because its intersect case does not satisfy our requirement: neither intersect nor Shape, the case's owner, is declared in RectMod. (An isomorphic error would occur in CircleMod if the second argument position in the pair were designated the owner position.) Therefore, RectMod may not extend intersect in that way. The requirement can be satisfied, for example, by modifying the intersect case's pattern to (Rect _, Shape _). This modification resolves the ambiguity for a pair of a Circle and a Rect, since the revised case is no longer applicable. As another example, the add cases in HashSetMod and SortedListSetMod of figures 3 and 4 are never compared for ambiguity, because the two modules do not statically depend upon one another. However, each case satisfies our requirement by following the traditional OO idiom of implementing an overriding method for a newly declared subclass. Therefore the two cases are guaranteed to be disjoint.

Since our ambiguity requirement is the disjunction of the implicit requirements in standard functional and OO

$$
\begin{array}{rcl}
\tau & ::= & \alpha \mid Ct \mid \tau_1 \rightarrow \tau_2 \mid \tau_1 * \cdots * \tau_k \\
Mt & ::= & \#\, Ct \mid \tau_1 * \cdots * \tau_{i-1} * Mt * \tau_{i+1} * \cdots * \tau_k \\
E & ::= & I \mid Fv \mid E_1\ E_2 \mid Ct(\overline{E}) \mid (\overline{E}) \mid Ct\ \{\overline{V} = \overline{E}\} \\
Pat & ::= & \_ \mid I\ \texttt{as}\ Pat \mid C\ \{\overline{V} = \overline{Pat}\} \mid (\overline{Pat}) \\
Ct & ::= & \overline{\tau}\, C \qquad\qquad Fv ::= \overline{\tau}\, F \\
C & ::= & Sn.Cn \qquad\quad V ::= Sn.Vn \\
F & ::= & Sn.Fn
\end{array}
$$

(a)

$$
\begin{array}{rcl}
S & ::= & \texttt{structure}\ Sn = \\
 & & \quad \texttt{struct depends upon}\ \overline{Sn}\ \overline{Ood}\ \texttt{end} \\
Ood & ::= & \texttt{<abstract>}\ \texttt{class}\ \overline{\alpha}\ Cn(\overline{I} : \overline{\tau}) \\
 & & \quad \texttt{<<extends}\ Ct(\overline{E})\ \texttt{>>}\ \texttt{of}\ \{\overline{Vn} : \overline{\tau_0} = \overline{E_0}\} \\
 & \mid & \texttt{fun}\ \overline{\alpha}\ Fn : Mt \rightarrow \tau \\
 & \mid & \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E
\end{array}
$$

(b)

Figure 7: (a) MINI-EML types, expressions, and patterns; (b) MINI-EML structures and declarations. Metavariable α ranges over type variable names, *I* over identifier names, *Sn* over structure names, *Cn* over class names, *Vn* over instance variable names, *Fn* over function names, and *Mn* over case names. $\overline{D}$ denotes a comma-separated list of elements (and is independent of any variable named *D*). Angle brackets (<>) and double angle brackets (<<>>) denote independent optional pieces of syntax. The notation $\overline{V} = \overline{E}$ abbreviates $V_1 = E_1, \ldots, V_k = E_k$ where $\overline{V}$ is $V_1, \ldots, V_k$ and $\overline{E}$ is $E_1, \ldots, V_k$ for some $k \geq 0$, and similarly for $\overline{V} = \overline{Pat}$, $\overline{Vn} : \overline{\tau_0} = \overline{E_0}$, and $\overline{I} : \overline{\tau}$.

languages, our requirement does not restrict those programming styles and allows them to coexist. Therefore, we have achieved our design goal of allowing the functional and OO extensibility idioms in a single class hierarchy while preserving modular type safety.[5] However, other useful kinds of extensibility are disallowed by the ambiguity requirement. For example, a client of both `UnionMod` and `HashSetMod` from figures 2 and 3 may want to implement `union` specially for `HashSet`s, so that these independent extensions of the `Set` abstraction will work well together. However, the new case would violate our ambiguity requirement, so `HashSet`s are forced to use the default `union` case (or `HashSetMod` must be modified in place to add the new case).

4 Mini-Eml

This section describes MINI-EML, a core language used to formalize the fundamental ideas in EML.

4.1 Syntax

Figure 7a defines the syntax of types, expressions, and patterns in MINI-EML. The syntax is essentially that of EML as informally presented so far, but we omit standard constructs including base types, conditionals, lambdas, local variables, references, and exceptions. MINI-EML types include type variables, class types, function types, and tuple types. The domain *Mt* represents *marked types*, which contain a # mark on a single component class type. Expressions include identifiers, function values, function application, constructor calls, tuples, and *instance expressions*. The instance expression $Ct\ \{\overline{V} = \overline{E}\}$ is not available at the source level, as instances may only be created via a constructor call $Ct(\overline{E})$. Patterns include the wildcard pattern, identifier binding, class patterns, and tuple patterns; a pattern of the form *I*, used in some of our earlier examples, is syntactic sugar for `(`*I* `as _)`.

The construct $\{\overline{V} = \overline{E}\}$ differs from an ordinary record in two ways. First, the labels are *scoped*: the name of the structure in which an instance variable was introduced becomes part of the instance variable's name. In the presence of the ability to make instance variables private (see section 5), scoping allows subclasses to introduce a new instance variable without conflicting with the name of a hidden one in the superclass. Instance variables in EML use this mechanism implicitly; regular static scoping rules determine which instance variable is referred to. Second, for simplicity the components of $\{\overline{V} = \overline{E}\}$ are ordered, unlike traditional records.

The notation and semantic style of MINI-EML were influenced by Featherweight Java [16], a core language for Java. As in that language, we formally represent classes by their names. A class is uniquely represented as *Sn.Cn*, where *Cn* is the name of the class and *Sn* is the name of the structure that declares *Cn*. Extensible functions are represented similarly.

The subset of expressions that are MINI-EML values is described by the following grammar, which includes class instances, function values, and tuple values:

$v ::= Ct\ \{\overline{V} = \overline{v}\} \mid Fv \mid (\overline{v})$

[5]In the presence of multiple *implementation* inheritance, other kinds of ambiguities that elude modular detection can arise, necessitating an extra requirement [21]. However, multiple *interface* inheritance, as in Java, cannot cause such ambiguities.

$\boxed{E \longrightarrow E'}$

$$\frac{Ct = (\overline{\tau}\, C) \qquad \text{concrete}(C) \qquad \text{rep}(Ct(\overline{E_0})) = \{\overline{V} = \overline{E_1}\}}{Ct(\overline{E_0}) \longrightarrow Ct\ \{\overline{V} = \overline{E_1}\}}\ \text{E-NEW}$$

$$\frac{E \longrightarrow E'}{Ct\ \{\overline{V_0} = \overline{v_0}, V = E, \overline{V_1} = \overline{E_1}\} \longrightarrow Ct\ \{\overline{V_0} = \overline{v_0}, V = E', \overline{V_1} = \overline{E_1}\}}\ \text{E-REP}$$

$$\frac{E \longrightarrow E'}{(\overline{v_0}, E, \overline{E_1}) \longrightarrow (\overline{v_0}, E', \overline{E_1})}\ \text{E-TUP}$$

$$\frac{E_1 \longrightarrow E_1'}{E_1\ E_2 \longrightarrow E_1'\ E_2}\ \text{E-APP1} \qquad \frac{E_2 \longrightarrow E_2'}{v_1\ E_2 \longrightarrow v_1\ E_2'}\ \text{E-APP2}$$

$$\frac{\text{most-specific-case-for}(Fv, v) = (\{(\overline{I}, \overline{v})\}, E)}{Fv\ v \longrightarrow [\overline{I} \mapsto \overline{v}]E}\ \text{E-APPRED}$$

(a)

$\boxed{\text{concrete}(C)}$

$$\frac{(\texttt{class}\ \overline{\alpha}\ Cn \ldots) \in ST(Sn)}{\text{concrete}(Sn.Cn)}\ \text{CONCRETE}$$

$\boxed{\text{rep}(Ct(\overline{E_0})) = \{\overline{V} = \overline{E}\}}$

$$\frac{\begin{array}{c}(<<\texttt{abstract}>>\ \texttt{class}\ \overline{\alpha}\ Cn(\overline{I} : \overline{\tau_1})\ <\texttt{extends}\ Ct(\overline{E_0})> \\ \texttt{of}\ \{\overline{Vn} : \overline{\tau_2} = \overline{E_2}\}) \in ST(Sn) \\ < \text{rep}(Ct(\overline{E_0})) = \{\overline{V} = \overline{E_1}\} >\end{array}}{\text{rep}((\overline{\tau}\ Sn.Cn)(\overline{E})) = [\overline{I} \mapsto \overline{E}][\overline{\alpha} \mapsto \overline{\tau}]\{< \overline{V} = \overline{E_1}, > Sn.\overline{Vn} = \overline{E_2}\}}\ \text{REP}$$

$\boxed{\text{most-specific-case-for}\ (Fv, v) = (\rho, E)}$

$$\frac{\begin{array}{c}(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn) \\ \text{match}(v, Pat) = \rho \\ \forall Sn' \in \text{dom}(ST).\forall(\texttt{extend fun}_{Mn'}\ \overline{\alpha'}\ F\ Pat' \ldots) \in ST(Sn'). \\ \forall \rho'.(\text{match}(v, Pat') = \rho' \wedge Sn.Mn \neq Sn'.Mn' \\ \Rightarrow Pat \leq Pat' \wedge Pat' \not\leq Pat)\end{array}}{\text{most-specific-case-for}\ ((\overline{\tau}\ F), v) = (\rho, [\overline{\alpha} \mapsto \overline{\tau}]E)}\ \text{LOOKUP}$$

(b)

Figure 8: (a) Evaluation rules for expressions. (b) Auxiliary inference rules. The notation $(\overline{I}, \overline{v})$ abbreviates $(I_1, v_1), \ldots, (I_k, v_k)$; $Sn.\overline{Vn} = \overline{E}$ abbreviates $Sn.Vn_1 = E_1, \ldots, Sn.Vn_k = E_k$.

The syntax of structures and declarations is shown in figure 7b. For convenience in the core language, each structure explicitly names the other structures (often including itself) whose interfaces it statically depends upon, via the `depends upon` $\overline{Sn}$ clause. ITC for a structure employs only the interfaces of the structures named in the `depends upon` clause. The static semantics ensures that the given dependency relation is well-formed, as described below. A structure consists of a sequence of class, extensible function, and function case declarations. The syntax of the three declarations is faithful to that of EML, except that cases now contain a *case name Mn*. This name is used in the semantics to uniquely identify each function case declaration (see section 4.2).

The class (function, case) names introduced in a given block are assumed to be distinct. The type variables parameterizing a given OO declaration are assumed to be distinct. The instance variable names introduced in a given class declaration are assumed to be distinct. The identifiers introduced in a given function case's pattern are assumed to be distinct.

Analogous with Featherweight Java, a MINI-EML program is a pair of a *structure table* and an expression. A structure table is a finite function from structure names to the associated structure declarations. The semantics assumes a fixed structure table denoted *ST*. The structure table *ST* is accessed by the dynamic and static semantics rules when information about a given OO declaration is required. The domain of a structure table *ST* is denoted dom(*ST*). The structure table is assumed to satisfy some sanity conditions: (1) $ST(Sn)$ = (`structure` *Sn* = `struct` …) for every $Sn \in \text{dom}(ST)$; (2) for every structure name *Sn* appearing anywhere in the program, we have $Sn \in \text{dom}(ST)$.

4.2 Dynamic Semantics

MINI-EML's dynamic semantics is defined as a mostly standard small-step operational semantics. The metavariable ρ ranges over *environments*, which are finite functions from identifiers to values. We use $|\overline{D}|$ to denote the length of the sequence $\overline{D}$. The notation $[I_1 \mapsto E_1, \ldots, I_k \mapsto E_k]D$ denotes the expression resulting from the simultaneous substitution of E_i for each occurrence of I_i in D, for $1 \leq i \leq k$, and similarly for $[\alpha_1 \mapsto \tau_1, \ldots, \alpha_k \mapsto \tau_k]D$. We use $[\overline{I} \mapsto \overline{E}]D$ as a shorthand when $\overline{I}$ and $\overline{E}$ have the same length, and similarly for $[\overline{\alpha} \mapsto \overline{\tau}]D$. In a given inference rule, fragments

$\boxed{\text{match}(v, Pat) = \rho}$

$$\frac{}{\text{match}(v, \_) = \{\}} \text{ E-MATCHWILD}$$

$$\frac{\text{match}(v, Pat) = \rho}{\text{match}(v, I \texttt{ as } Pat) = \rho \cup \{(I, v)\}} \text{ E-MATCHBIND}$$

$$\frac{C \leq C' \qquad \text{match}(\overline{v}, \overline{Pat}) = \overline{\rho}}{\text{match}(\overline{\tau}\, C\ \{\overline{V} = \overline{v}, \overline{V_1} = \overline{v_1}\},\ C'\ \{\overline{V} = \overline{Pat}\}) = \bigcup \overline{\rho}} \text{ E-MATCHCLASS}$$

$$\frac{\text{match}(\overline{v}, \overline{Pat}) = \overline{\rho}}{\text{match}((\overline{v}), (\overline{Pat})) = \bigcup \overline{\rho}} \text{ E-MATCHTUP}$$

(a)

$\boxed{Pat \leq Pat'}$

$$\frac{}{Pat \leq \_} \text{ SPECWILD}$$

$$\frac{Pat_1 \leq Pat_2}{I \texttt{ as } Pat_1 \leq Pat_2} \text{ SPECBIND1} \qquad \frac{Pat_1 \leq Pat_2}{Pat_1 \leq I \texttt{ as } Pat_2} \text{ SPECBIND2}$$

$$\frac{C \leq C' \qquad \overline{Pat_1} \leq \overline{Pat_2}}{C\ \{\overline{V} = \overline{Pat_1}, \overline{V_3} = \overline{Pat_3}\} \leq C'\ \{\overline{V} = \overline{Pat_2}\}} \text{ SPECCLASS}$$

$$\frac{\overline{Pat_1} \leq \overline{Pat_2}}{(\overline{Pat_1}) \leq (\overline{Pat_2})} \text{ SPECTUP}$$

(b)

Figure 9: (a) Pattern matching. (b) Pattern specificity. The notation $\text{match}(\overline{v}, \overline{Pat}) = \overline{\rho}$ abbreviates $\text{match}(v_1, Pat_1) = \rho_1 \cdots \text{match}(v_k, Pat_k) = \rho_k$, and similarly for $\overline{Pat_1} \leq \overline{Pat_2}$.

$\boxed{C \leq C'}$

$$\frac{}{C \leq C} \text{ SUBREF}$$

$$\frac{C_1 \leq C_2 \qquad C_2 \leq C_3}{C_1 \leq C_3} \text{ SUBTRANS}$$

$$\frac{(\texttt{<abstract>}\ \texttt{class}\ (\overline{\alpha}\ Cn)(\overline{I_1} : \overline{\tau_1})\ \texttt{extends}\ (\overline{\tau}\ C)\ \ldots) \in ST(Sn)}{Sn.Cn \leq C} \text{ SUBEXT}$$

Figure 10: Subclassing.

enclosed in <> must either be all present or all absent, and similarly for <<>>. We sometimes treat sequences as if they were sets. For example, $Ood \in \overline{Ood}$ means that Ood is one of the declarations in $\overline{Ood}$. We use $Ood \in ST(Sn)$ as shorthand for $(ST(Sn) = (\texttt{structure}\ Sn = \texttt{struct depends upon}\ \overline{Sn}\ \overline{Ood}\ \texttt{end})) \wedge Ood \in \overline{Ood}$.

Figure 8a contains the rules for evaluating expressions. For simplicity in the semantics, a constructor call is treated as syntactic sugar for a particular instance expression, obtained by expanding the constructor's definition. Rule E-NEW specifies this semantics, making use of the first two auxiliary rules in figure 8b. CONCRETE checks that the class to be instantiated was declared without the `abstract` keyword. REP initializes the fields of the new instance as directed by the class's implicit constructor, substituting the actual arguments to the constructor call for the formals. The semantics uses a type-passing style, so the instance's type parameters are also substituted for the class's type variables. Rule E-REP then evaluates instance expressions. It would be straightforward to instead use a call-by-value semantics for constructor calls, at the cost of some additional mechanism.

The last rule in figure 8b formalizes function-case lookup, used in E-APPRED. The top line of LOOKUP's premises specifies the case to invoke. The second line ensures that the chosen case is applicable: the argument value matches the case's pattern. The remaining premise ensures that the chosen case is most-specific: the case is strictly more specific than any other applicable case. The condition $Sn.Mn \neq Sn'.Mn'$ uses the case names to ensure that the chosen case is not compared for specificity with itself.

The rules for pattern matching and specificity are shown in figure 9. The matching rules are straightforward except for E-MATCHCLASS. The judgment $C \leq C'$ is defined in figure 10 as the reflexive, transitive closure of the declared class `extends` relation. Therefore, an instance of class C matches a class pattern of class C' if C subclasses C' and

$\boxed{S \text{ OK}}$

$$\frac{\overline{Sn} \vdash \overline{Ood} \text{ OK in } Sn}{\texttt{structure}\ \ Sn = \texttt{struct depends upon}\ \overline{Sn}\ \overline{Ood}\ \texttt{end} \text{ OK}}\ \textsc{StructOK}$$

$\boxed{\overline{Sn} \vdash Ood \text{ OK in } Sn}$

$$\frac{\begin{array}{c} < Ct = \overline{\alpha}\ Sn.Cn > \quad < \Gamma;\overline{\alpha} \vdash Ct(\overline{E}) \text{ OK} > \quad \overline{\alpha} \vdash \overline{\tau} \text{ OK} \quad \overline{\alpha} \vdash \overline{\tau_0} \text{ OK} \quad \Gamma = \{(\overline{I},\overline{\tau})\} \quad \Gamma;\overline{\alpha} \vdash \overline{E_0} : \overline{\tau_1} \\ \overline{\tau_1} \leq \overline{\tau_0} \quad \overline{Sn} \vdash Sn.Cn \text{ transDependedUpon} \quad \text{concrete}(Sn.Cn) \Rightarrow \overline{Sn} \vdash \text{funs-have-ldefault-for } Sn.Cn \end{array}}{\overline{Sn} \vdash \texttt{<<abstract>>}\ \texttt{class}\ \overline{\alpha}\ Cn(\overline{I} : \overline{\tau})\ \texttt{<extends}\ Ct(\overline{E}) > \texttt{of}\ \{\overline{Vn : \tau_0 = E_0}\} \text{ OK in } Sn}\ \textsc{ClassOK}$$

$$\frac{\overline{\alpha} \vdash \hat{Mt} \text{ OK} \quad \overline{\alpha} \vdash \tau \text{ OK} \quad \text{owner}(Sn.Fn) = Sn'.Cn \quad Sn \neq Sn' \Rightarrow \overline{Sn} \vdash Sn.Fn \text{ has-gdefault}}{\overline{Sn} \vdash \texttt{fun}\ \overline{\alpha}\ Fn : Mt \rightarrow \tau \text{ OK in } Sn}\ \textsc{FunOK}$$

$$\frac{\begin{array}{c} (\texttt{fun}\ \overline{\alpha'}\ Fn : Mt \rightarrow \tau) \in ST(Sn') \quad \text{matchType}([\overline{\alpha'} \mapsto \overline{\alpha}]\hat{Mt}, Pat) = (\Gamma, \tau_0) \quad \Gamma;\overline{\alpha} \vdash E : \tau' \\ \tau' \leq [\overline{\alpha'} \mapsto \overline{\alpha}]\tau \quad \overline{Sn} \vdash Sn'.Fn \text{ dependedUpon} \quad Sn;\overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ Sn'.Fn\ Pat = E \text{ unambiguous} \end{array}}{\overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ Sn'.Fn\ Pat = E \text{ OK in } Sn}\ \textsc{CaseOK}$$

Figure 11: Static semantics of structures and OO declarations. The notation $\overline{Sn} \vdash \overline{Ood}$ OK in Sn abbreviates $\overline{Sn} \vdash Ood_1$ OK in $Sn \cdots \overline{Sn} \vdash Ood_k$ OK in Sn; $\overline{\alpha} \vdash \overline{\tau}$ OK abbreviates $\overline{\alpha} \vdash \tau_1$ OK $\cdots$ $\overline{\alpha} \vdash \tau_k$ OK; $(\overline{I},\overline{\tau})$ abbreviates $(I_1,\tau_1),\ldots,(I_k,\tau_k)$; $\Gamma;\overline{\alpha} \vdash \overline{E} : \overline{\tau}$ abbreviates $\Gamma;\overline{\alpha} \vdash E_1 : \tau_1 \cdots \Gamma;\overline{\alpha} \vdash E_k : \tau_k$; $\overline{\tau_1} \leq \overline{\tau_0}$ abbreviates $\tau_{11} \leq \tau_{01} \cdots \tau_{1k} \leq \tau_{0k}$.

the instance's representation recursively matches the given representation pattern. This recursive matching is not supported in traditional OO languages or in $\text{ML}_{\leq}$. We allow an instance to have more instance variables than the given representation pattern, so that subclass instances can match superclass patterns. For example, the value `CListSet {es=[5,3],count=2}` matches the pattern in the `elems` case of figure 1.

The judgment $Pat \leq Pat'$ means that Pat is at least as specific as Pat'. The pattern specificity semantics generalizes OO-style "best-match" semantics to support ML-style patterns. Any pattern is at least as specific as the wildcard, and identifier binding has no effect on specificity. Class pattern specificity (SpecClass) follows the ordering induced by subclassing. Analogous with E-MatchClass, the more-specific pattern may contain extra instance variables. The natural rule SpecTup for tuple patterns makes pattern specificity a generalization of the "symmetric" *multimethod* specificity semantics in OO languages [5, 6]. When a tuple is used to send multiple arguments to a function, tuple patterns allow all arguments to be dynamically dispatched upon, and no argument position is more important than the rest. This contrasts with traditional *single dispatch*, as in Java, where only a unique *receiver* argument may be dispatched upon.

4.3 Static Semantics

Figure 11 contains the rules for typechecking structures and OO declarations. Γ is a *type environment*, mapping identifiers to types. The notation $\hat{Mt}$ denotes the type τ identical to Mt, but with the # mark removed. Structures are typechecked (StructOK) by checking each declaration in turn. It is assumed that S OK holds for each structure S in the range of ST.

The rules for typechecking the three OO declarations are largely straightforward. Rule ClassOK checks that a class's superclass constructor call is well-typed, that all types mentioned in the class declaration are well-formed, and that the instance-variable initializer expressions have the appropriate types. Rule FunOK checks that a function's declared type is well-formed. Rule CaseOK ensures that the case's pattern and body are compatible with the associated function's declared type. The "transDependedUpon" and "dependedUpon" judgments in ClassOK and FunOK ensure that each structure's declared dependency relation is well-formed; they are described below. Finally, each rule enforces one of our three modular requirements, discussed in more detail below: ClassOK enforces the local-default requirement ("funs-have-ldefault-for") if the class is concrete; FunOK enforces the global-default requirement ("has-gdefault") if the function is external; CaseOK performs ambiguity checking ("unambiguous") for the given case, which includes enforcement of the ambiguity requirement.

$\boxed{\overline{\alpha} \vdash \tau \text{ OK}}$

$$\frac{\alpha \in \overline{\alpha}}{\overline{\alpha} \vdash \alpha \text{ OK}} \ \textsc{TVarOK}$$

$$\frac{\begin{array}{c}(\texttt{<abstract>}\ \texttt{class}\ \overline{\alpha_0}\ Cn \ldots) \in ST(Sn) \\ \overline{\alpha} \vdash \overline{\tau} \text{ OK} \qquad |\overline{\alpha_0}| = |\overline{\tau}|\end{array}}{\overline{\alpha} \vdash \overline{\tau}\ Sn.Cn \text{ OK}} \ \textsc{ClassTypeOK}$$

$$\frac{\overline{\alpha} \vdash \tau_1 \text{ OK} \qquad \overline{\alpha} \vdash \tau_2 \text{ OK}}{\overline{\alpha} \vdash \tau_1 \rightarrow \tau_2 \text{ OK}} \ \textsc{FunTypeOK}$$

$$\frac{\overline{\alpha} \vdash \tau_1 \text{ OK} \qquad \cdots \qquad \overline{\alpha} \vdash \tau_k \text{ OK}}{\overline{\alpha} \vdash \tau_1 * \cdots * \tau_k \text{ OK}} \ \textsc{TupTypeOK}$$

$\boxed{\Gamma; \overline{\alpha} \vdash E : \tau}$

$$\frac{(I, \tau) \in \Gamma}{\Gamma; \overline{\alpha} \vdash I : \tau} \ \text{T-}\textsc{Id}$$

$$\frac{(\texttt{fun}\ \overline{\alpha_0}\ Fn : Mt \rightarrow \tau) \in ST(Sn) \qquad \overline{\alpha} \vdash \overline{\tau_0} \text{ OK}}{\Gamma; \overline{\alpha} \vdash \overline{\tau_0}\ Sn.Fn : [\overline{\alpha_0} \mapsto \overline{\tau_0}](\hat{Mt} \rightarrow \tau)} \ \text{T-}\textsc{Fun}$$

$$\frac{\Gamma; \overline{\alpha} \vdash E_1 : \tau_2 \rightarrow \tau \qquad \Gamma; \overline{\alpha} \vdash E_2 : \tau_2' \qquad \tau_2' \le \tau_2}{\Gamma; \overline{\alpha} \vdash E_1\ E_2 : \tau} \ \text{T-}\textsc{App}$$

$$\frac{\Gamma; \overline{\alpha} \vdash Ct(\overline{E}) \text{ OK} \qquad Ct = (\overline{\tau}\ C) \qquad \text{concrete}(C)}{\Gamma; \overline{\alpha} \vdash Ct(\overline{E}) : Ct} \ \text{T-}\textsc{New}$$

$$\frac{\Gamma; \overline{\alpha} \vdash E_1 : \tau_1 \qquad \cdots \qquad \Gamma; \overline{\alpha} \vdash E_k : \tau_k}{\Gamma; \overline{\alpha} \vdash (E_1, \ldots, E_k) : \tau_1 * \cdots * \tau_k} \ \text{T-}\textsc{Tup}$$

$$\frac{\begin{array}{c}\overline{\alpha} \vdash Ct \text{ OK} \qquad Ct = (\overline{\tau_0}\ C) \qquad \text{concrete}(C) \\ \text{repType}(Ct) = \{\overline{V} : \overline{\tau}\} \qquad \Gamma; \overline{\alpha} \vdash \overline{E} : \overline{\tau_1} \qquad \overline{\tau_1} \le \overline{\tau}\end{array}}{\Gamma; \overline{\alpha} \vdash Ct\ \{\overline{V} = \overline{E}\} : Ct} \ \text{T-}\textsc{Rep}$$

$\boxed{\Gamma; \overline{\alpha} \vdash Ct(\overline{E}) \text{ OK}}$

$$\frac{\begin{array}{c}\overline{\alpha} \vdash Ct \text{ OK} \qquad Ct = (\overline{\tau_0}\ Sn.Cn) \\ (\texttt{<abstract>}\ \texttt{class}\ \overline{\alpha_0}\ Cn(\overline{I} : \overline{\tau}) \ldots) \in ST(Sn) \\ \Gamma; \overline{\alpha} \vdash \overline{E} : \overline{\tau_1} \qquad \overline{\tau_1} \le [\overline{\alpha_0} \mapsto \overline{\tau_0}]\overline{\tau}\end{array}}{\Gamma; \overline{\alpha} \vdash Ct(\overline{E}) \text{ OK}} \ \text{T-}\textsc{Super}$$

$\boxed{\tau \le \tau'}$

$$\frac{}{\tau \le \tau} \ \textsc{SubTRef}$$

$$\frac{\tau_1 \le \tau_2 \qquad \tau_2 \le \tau_3}{\tau_1 \le \tau_3} \ \textsc{SubTTrans}$$

$$\frac{\begin{array}{c}(\texttt{<abstract>}\ \texttt{class}\ \overline{\alpha}\ Cn(\overline{I_1} : \overline{\tau_1}) \\ \texttt{extends}\ Ct \ldots) \in ST(Sn)\end{array}}{\overline{\tau}\ Sn.Cn \le [\overline{\alpha} \mapsto \overline{\tau}]Ct} \ \textsc{SubTExt}$$

$$\frac{\tau_1' \le \tau_1 \qquad \tau_2 \le \tau_2'}{\tau_1 \rightarrow \tau_2 \le \tau_1' \rightarrow \tau_2'} \ \textsc{SubTFun}$$

$$\frac{\tau_1 \le \tau_1' \qquad \cdots \qquad \tau_k \le \tau_k'}{\tau_1 * \cdots * \tau_k \le \tau_1' * \cdots * \tau_k'} \ \textsc{SubTTup}$$

$\boxed{\text{matchType}(\tau, Pat) = (\Gamma, \tau')}$

$$\frac{}{\text{matchType}(\tau, \_) = (\{\}, \tau)} \ \text{T-}\textsc{MatchWild}$$

$$\frac{\text{matchType}(\tau, Pat) = (\Gamma, \tau')}{\text{matchType}(\tau, I\ \texttt{as}\ Pat) = (\Gamma \cup \{(I, \tau')\}, \tau')} \ \text{T-}\textsc{MatchBind}$$

$$\frac{\begin{array}{c}C \le C' \qquad \text{repType}(\overline{\tau}\ C) = \{\overline{V} : \overline{\tau_0}\} \\ \text{matchType}(\overline{\tau_0}, \overline{Pat}) = (\overline{\Gamma}, \overline{\tau_1})\end{array}}{\begin{array}{c}\text{matchType}((\overline{\tau}\ C'), C\ \{\overline{V} = \overline{Pat}\}) = \\ (\bigcup \overline{\Gamma}, (\overline{\tau}\ C))\end{array}} \ \text{T-}\textsc{MatchClass}$$

$$\frac{\begin{array}{c}\text{matchType}(\tau_1, Pat_1) = (\Gamma_1, \tau_1') \\ \cdots \qquad \text{matchType}(\tau_k, Pat_k) = (\Gamma_k, \tau_k')\end{array}}{\begin{array}{c}\text{matchType}(\tau_1 * \cdots * \tau_k, (Pat_1, \ldots, Pat_k)) = \\ (\Gamma_1 \cup \ldots \cup \Gamma_k, \tau_1' * \cdots * \tau_k')\end{array}} \ \text{T-}\textsc{MatchTup}$$

$\boxed{\text{repType}(Ct) = \{\overline{V} : \overline{\tau}\}}$

$$\frac{\begin{array}{c}(\texttt{<<abstract>>}\ \texttt{class}\ \overline{\alpha}\ Cn(\overline{I} : \overline{\tau_1}) \\ \texttt{<extends}\ Ct(\overline{E_0}) > \texttt{of}\ \{\overline{Vn} : \overline{\tau_2} = \overline{E_2}\}) \in ST(Sn) \\ < \text{repType}(Ct) = \{\overline{V} : \overline{\tau_3}\} >\end{array}}{\begin{array}{c}\text{repType}(\overline{\tau}\ Sn.Cn) = \\ [\overline{\alpha} \mapsto \overline{\tau}]\{< \overline{V} : \overline{\tau_3}, > Sn.\overline{Vn} : \overline{\tau_2}\}\end{array}} \ \textsc{RepType}$$

Figure 12: Static semantics of types, expressions, and patterns. The notation $\text{matchType}(\overline{\tau_0}, \overline{Pat}) = (\overline{\Gamma}, \overline{\tau_1})$ abbreviates $\text{matchType}(\tau_1, Pat_1) = (\Gamma_1, \tau_1') \cdots \text{matchType}(\tau_k, Pat_k) = (\Gamma_k, \tau_k')$. The notation $Sn.\overline{Vn} : \overline{\tau}$ abbreviates $Sn.Vn_1 : \tau_1, \ldots, Sn.Vn_k : \tau_k$.

Figure 12 contains the static semantics of types, expressions, and patterns. The judgment $\overline{\alpha} \vdash \tau$ OK ensures that τ refers only to type variables in $\overline{\alpha}$ and that each class in τ has the correct number of type parameters. The subtyping relation $\tau \leq \tau'$ is completely standard. The judgment $\Gamma;\overline{\alpha} \vdash E : \tau$ ensures that an expression is well-typed in the context of the type environment and sequence of type variables currently in scope. The associated inference rules are straightforward and rely on the two helper rules at the bottom of figure 12. The judgment $\text{matchType}(\tau, Pat) = (\Gamma, \tau')$ checks that a pattern is compatible with type τ. The judgment produces a type environment mapping any identifiers in *Pat* to their types, used to typecheck the associated case's body. The type τ' represents the particular subtype of τ to which *Pat* conforms; it is used to give precise types to any identifiers bound to *Pat*.

Figure 13 contains the well-formedness rules for a structure's `depends upon` relation. Rule CLASSTRANSDEP is used by CLASSOK in figure 11 to ensure that a structure containing a class is declared to depend upon all structures that declare a (reflexive, transitive) superclass of the class. Rule FUNDEP is used by CASEOK to ensure that a structure containing a function case is declared to depend upon the structure containing the associated function. In either case, if *Sn* is required to declare a dependency on Sn', then *Sn* does indeed statically depend upon Sn' according to the definition of static dependency given in section 3.1. The declared dependency relation may include more structures than are statically depended upon, but the soundness proof relies only on the above two properties of the declared dependency relation, thereby ensuring that modularity is respected.

Figure 14 formalizes the portion of modular ITC that ensures functions are exhaustive, which consists of enforcement of the global-default and local-default requirements. Metavariable *Tm* ranges over both types and marked types, and metavariable *d* ranges over nonnegative integers. Rule GDEFAULT checks that a given function has a global default case, and LDEFAULT checks that all available functions whose owners are superclasses of a given class *C* have a local default case for *C*. Since a global default case of *F* is also a local default case of *F* for *C*, where *C* is the owner of *F*, the two requirements are able to share the helper rules that perform the checks.

Our strategy in performing the checks is to generate a *default pattern* representing a valid (global or local) default for a given function. We then check that the default pattern is at least as specific as the pattern of some available function case; if so, we say that case *covers* the default pattern. For example, consider checking in `HashSetMod` of figure 3 that `size` has a local default case for `HashSet`. We generate the default pattern `(HashSet {ht=_})`. The check then succeeds since the default pattern is at least as specific as `(HashSet {ht=ht})`, which is the pattern of the `size` case in `HashSetMod`. Therefore that `size` case is a valid local default. This strategy is formalized by rule DEFAULT.

The judgment $\text{defaultPat}(Tm, C, d) = Pat$ generates a default pattern of (possibly marked) type *Tm*. The default pattern dispatches on *C* in the marked position of *Tm* (if any) and accepts any type-correct argument in the other positions. The integer *d* represents the *nesting depth* which the generated pattern should have. It is sound to generate the default pattern to any depth, but greater depths can make the check more precise. For example, in checking `size` above we assumed that the default pattern was `(HashSet {ht=_})`. However, `(HashSet _)` is also a valid default pattern, since it dispatches on `HashSet` in the owner position. If this default pattern were instead used to check `size`, an incompleteness error would be signaled statically: the `size` case in `HashSetMod` no longer covers the default pattern and is therefore not seen as an appropriate local default case. Our type system chooses the depth non-deterministically in rule DEFAULT, and our soundness proof implies that any depth can be safely used. It is straightforward to find an appropriately precise depth to use — it is the maximum depth of any pattern in an available case of the function being checked. Our prototype interpreter implements this algorithm for choosing the depth.[6]

Figure 15 formalizes the portion of modular ITC that ensures functions are unambiguous. The top-level rule is AMB. That rule enforces the ambiguity requirement, ensuring that the given function case is declared in the same module as either its associated function or its owner. The ambiguity requirement ensures that the case is not ambiguous with unavailable cases. AMB then uses STRAMB to check that the given case is unambiguous with available function cases. STRAMB compares the given case individually with each available function case other than itself. Let *Pat* and Pat' be the patterns of the two cases. If the patterns are disjoint, then they are not ambiguous. Otherwise, the patterns have a non-empty *intersection*, formalized by the judgment $Pat \cap Pat' = Pat_0$: values matching both *Pat* and Pat' match Pat_0, and no other values match Pat_0. The two cases are then unambiguous if there exists a *resolving case*. A resolving case covers the intersection Pat_0, is at least as specific as both of the original cases, and is strictly more specific than at least one of them. An important degenerate scenario occurs when one of *Pat* and Pat' is more specific than the other. For example, the two `size` cases in figure 1 have a non-empty intersection. Since the second case is strictly more specific than the first, the second case itself is the resolving case.

[6] Because class patterns allow pattern matching on a class's representation, which may recursively involve class patterns, it is possible for patterns to have arbitrary depth. Therefore, there is in general no *a priori* maximal depth for the patterns of a given function.

$\boxed{\overline{Sn} \vdash Sn.Cn \text{ transDependedUpon}}$

$$\frac{\begin{array}{c}(<<\texttt{abstract}>>\ \texttt{class}\ (\overline{\alpha}\ Cn)(\overline{I}:\overline{\tau})\ <\texttt{extends}\ (\overline{\tau_0}\ C)(\overline{E}) > \ldots) \in ST(Sn) \\ Sn \in \overline{Sn} \qquad < \overline{Sn} \vdash C \text{ transDependedUpon} > \end{array}}{\overline{Sn} \vdash Sn.Cn \text{ transDependedUpon}}\ \textsc{ClassTransDep}$$

$\boxed{\overline{Sn} \vdash F \text{ dependedUpon}}$

$$\frac{Sn \in \overline{Sn}}{\overline{Sn} \vdash Sn.Fn \text{ dependedUpon}}\ \textsc{FunDep}$$

Figure 13: Well-formedness of the `depends-upon` relation.

$\boxed{\overline{Sn} \vdash F \text{ has-gdefault}}$

$$\frac{\text{owner}(F) = C \qquad \overline{Sn} \vdash F \text{ has-default-for } C}{\overline{Sn} \vdash F \text{ has-gdefault}}\ \textsc{GDefault}$$

$\boxed{\overline{Sn} \vdash \text{funs-have-ldefault-for } C}$

$$\frac{\forall F, C'.[(\overline{Sn} \vdash F \text{ dependedUpon} \wedge \text{owner}(F) = C' \wedge C \leq C') \Rightarrow \overline{Sn} \vdash F \text{ has-default-for } C]}{\overline{Sn} \vdash \text{funs-have-ldefault-for } C}\ \textsc{LDefault}$$

$\boxed{\overline{Sn} \vdash F \text{ has-default-for } C}$

$$\frac{\begin{array}{c} (\texttt{fun}\ \overline{\alpha}\ Fn : Mt \to \tau) \in ST(Sn) \\ \text{defaultPat}(Mt, C, d) = Pat \qquad (\texttt{extend}\ \texttt{fun}_{Mn}\ \overline{\alpha_0}\ Sn.Fn\ Pat' = E) \in ST(Sn') \qquad Pat \leq Pat' \qquad Sn' \in \overline{Sn} \end{array}}{\overline{Sn} \vdash Sn.Fn \text{ has-default-for } C}\ \textsc{Default}$$

$\boxed{\text{defaultPat}(Tm, C, d) = Pat}$

$$\frac{}{\text{defaultPat}(Tm, C, 0) = \_}\ \textsc{DefZero} \qquad \frac{d > 0}{\text{defaultPat}(\alpha, C, d) = \_}\ \textsc{DefTypeVar}$$

$$\frac{\begin{array}{c}\text{repType}(\overline{\tau}\ C') = \{\overline{V : \overline{\tau_0}}\} \\ \text{defaultPat}(\overline{\tau_0}, C, d-1) = \overline{Pat} \qquad d > 0\end{array}}{\text{defaultPat}((\overline{\tau}\ C'), C, d) = (C'\ \{\overline{V} = \overline{Pat}\})}\ \textsc{DefClassType}$$

$$\frac{\begin{array}{c}\text{repType}(\overline{\tau}\ C) = \{\overline{V : \overline{\tau_0}}\} \\ \text{defaultPat}(\overline{\tau_0}, C, d-1) = \overline{Pat} \\ d > 0\end{array}}{\text{defaultPat}(\#(\overline{\tau}\ C'), C, d) = (C\ \{\overline{V} = \overline{Pat}\})}\ \textsc{DefOwnerClassType}$$

$$\frac{\begin{array}{c}\text{defaultPat}(Tm_1, C, d-1) = Pat_1 \\ \ldots \\ \text{defaultPat}(Tm_k, C, d-1) = Pat_k \qquad d > 0\end{array}}{\text{defaultPat}(Tm_1 * \ldots * Tm_k, C, d) = (Pat_1, \ldots, Pat_k)}\ \textsc{DefTupType}$$

$$\frac{d > 0}{\text{defaultPat}(\tau_1 \to \tau_2, C, d) = \_}\ \textsc{DefFunType}$$

Figure 14: Exhaustiveness checking. The notation $\text{defaultPat}(\overline{\tau_0}, C, d-1) = \overline{Pat}$ abbreviates $\text{defaultPat}(\tau_1, C, d-1) = Pat_1 \cdots \text{defaultPat}(\tau_k, C, d-1) = Pat_k$.

$$\boxed{Sn;\overline{Sn} \vdash \texttt{extend fun} \ldots \text{ unambiguous}}$$

$$\frac{\text{owner}(Mt, Pat) = Sn''.Cn \qquad Sn = Sn' \vee Sn = Sn'' \qquad \begin{array}{c}(\texttt{fun}\ \overline{\alpha'}\ Fn : Mt \rightarrow \tau) \in ST(Sn') \\ \overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ Sn'.Fn\ Pat = E \text{unambiguous in } Sn\end{array}}{Sn;\overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ Sn'.FnPat = E \text{ unambiguous}} \text{ AMB}$$

$$\boxed{\overline{Sn} \vdash \texttt{extend fun} \ldots \text{ unambiguous in } Sn}$$

$$\frac{\begin{array}{c}\forall Sn' \in \overline{Sn}.\forall(\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E') \in ST(Sn'). \\ \forall Pat_0.[(Pat \cap Pat' = Pat_0 \wedge Sn.Mn \neq Sn'.Mn') \Rightarrow \\ \exists Sn'' \in \overline{Sn}.\exists(\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn''). \\ (Pat_0 \leq Pat'' \wedge Pat'' \leq Pat \wedge Pat'' \leq Pat' \wedge (Pat \not\leq Pat'' \vee Pat' \not\leq Pat''))]\end{array}}{\overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E \text{ unambiguous in } Sn} \text{ STRAMB}$$

$$\boxed{Pat_1 \cap Pat_2 = Pat}$$

$$\frac{}{\_ \cap Pat = Pat} \text{ PATINTWILD} \qquad \frac{Pat_1 \cap Pat_2 = Pat}{I\ \texttt{as}\ Pat_1 \cap Pat_2 = Pat} \text{ PATINTBIND}$$

$$\frac{C \leq C' \qquad \overline{Pat_1} \cap \overline{Pat_2} = \overline{Pat}}{C\ \{\overline{V} = \overline{Pat_1}, \overline{V_3} = \overline{Pat_3}\} \cap C'\ \{\overline{V} = \overline{Pat_2}\} = C\ \{\overline{V} = \overline{Pat}, \overline{V_3} = \overline{Pat_3}\}} \text{ PATINTCLASS}$$

$$\frac{\overline{Pat_1} \cap \overline{Pat_2} = \overline{Pat}}{(\overline{Pat_1}) \cap (\overline{Pat_2}) = (\overline{Pat})} \text{ PATINTTUP} \qquad \frac{Pat_2 \cap Pat_1 = Pat}{Pat_1 \cap Pat_2 = Pat} \text{ PATINTREV}$$

Figure 15: Unambiguity checking. The notation $\overline{Pat_1} \cap \overline{Pat_2} = \overline{Pat}$ abbreviates $Pat'_1 \cap Pat''_1 = Pat_1 \cdots Pat'_k \cap Pat''_k = Pat_k$.

$$\boxed{\text{owner}(F) = C}$$

$$\frac{\begin{array}{c}(\texttt{fun}\ \overline{\alpha}\ Fn : Mt \rightarrow \tau) \in ST(Sn) \\ \text{owner}(Mt) = C\end{array}}{\text{owner}(Sn.Fn) = C} \text{ OWNERFUN}$$

$$\boxed{\text{owner}(Mt) = C}$$

$$\frac{}{\text{owner}(\#\ \overline{\tau}\ C) = C} \text{ OWNERCLASS}$$

$$\frac{\text{owner}(Mt) = C}{\text{owner}(\tau_1 * \cdots * \tau_{i-1} * Mt * \tau_{i+1} * \cdots * \tau_k) = C} \text{ OWNERTUP}$$

$$\boxed{\text{owner}(Mt, Pat) = C}$$

$$\frac{\text{owner}(Mt, Pat) = C}{\text{owner}(Mt, I\ \texttt{as}\ Pat) = C} \text{ OWNERBINDPAT}$$

$$\frac{\text{owner}(Mt, Pat_i) = C}{\begin{array}{c}\text{owner}(\tau_1 * \cdots * \tau_{i-1} * Mt * \tau_{i+1} * \cdots * \tau_k, \\ (Pat_1, \ldots, Pat_k)) = C\end{array}} \text{ OWNERTUPPAT}$$

$$\frac{}{\text{owner}(\#Ct, C\ \{\overline{V} = \overline{Pat}\}) = C} \text{ OWNERCLASSPAT}$$

Figure 16: Accessing the owner.

```
structure BadMod = struct
  class C() of {}
  fun f:C → unit
  val bad = f(C())
  extend fun f (C {}) = ()
end
```

Figure 17: Value declarations and ITC.

```
signature ShapeSig = sig
  abstract class Shape() of {}
  fun bad:Shape → unit
  extend fun bad s
end
structure ShapeMod = struct
  abstract class Shape() of {}
  fun print:Shape → unit
  fun bad:Shape → unit
  extend fun bad s = print s
end :  ShapeSig
structure CircleMod
  class Circle() extends Shape() of {}
end
```

Figure 18: Unsoundnesses with hiding OO declarations.

Finally, figure 16 contains the helper judgments for accessing the class at the owner position of a function, type, and pattern.

4.4 Type Soundness

We have proven type soundness for MINI-EML. As usual, we prove type preservation and progress theorems. The notation $\vdash E : T$ denotes the typechecking of E in the context of the empty type environment and empty sequence of type variables.

Theorem 4.1 (Type Preservation) If $\vdash E : \tau$ and $E \longrightarrow E'$, then there exists τ' such that $\vdash E' : \tau'$ and $\tau' \leq \tau$.

Theorem 4.2 (Progress) If $\vdash E : \tau$ and E is not a value, then there exists E' such that $E \longrightarrow E'$.

The proofs of these two theorems are provided in appendices A and B, respectively. Proving type preservation is relatively straightforward, as it is completely independent of ITC. Proving progress requires reasoning about modular ITC, in order to show that function applications can always make progress. The key lemma says that a most-specific applicable function case exists for each type-correct application:

Lemma 4.1 If $\vdash Fv : \tau_2 \rightarrow \tau$ and $\vdash v : \tau_2'$ and $\tau_2' \leq \tau_2$, then there exist ρ and E such that most-specific-case-for(Fv,v) = (ρ, E).

5 ML-Style Modules

This section discusses how EML's features can interact with an ML-style module system including structures, signatures, and functors.

5.1 Structures

Thus far we have assumed that EML structures contain only a sequence of class, function, and function case declarations. We would also like to accommodate the ordinary ML declarations, including value, type, exception, and structure declarations. The latter three kinds of declarations can be straightforwardly incorporated, but special care is needed to handle value declarations. Figure 17 shows an example of the problems that can occur. ITC on `BadMod` will succeed, because function `f` has an appropriate case for `C`. However, at run-time a *match nonexhaustive* error will occur when the `val` declaration is executed, because `f`'s function case will have not yet been declared.

There are several approaches to handling this problem. We could adopt a two-pass style of structure evaluation. The first pass would evaluate all of the declarations except the value declarations, and the second pass would evaluate the value declarations. In our example, this semantics ensures that `f`'s function case is declared before `f` is invoked. An alternative approach is to make the unit of modularity used in our ITC requirements more fine-grained than an entire structure, with `val` declarations forming the boundaries of these units. For example, `BadMod` would consist of two units, one of which contains the first two declarations and the other containing the last declaration. When ITC is performed on the first unit, the incompleteness of `f` for `C` would result in a static error. Our prototype EML interpreter uses a variant of this approach. Instead of inferring the modular units, we introduce a new kind of OO declaration of the form *Ood* `and` *Ood*′ (similar syntactically, but not semantically, to the `and` construct in ML), which groups a sequence of class, function, and function case declarations. A group of `and`ed OO declarations is treated as a unit for the purposes of modular ITC.

5.2 Signature Ascription

Signature ascription provides information hiding in ML. Clients of a structure expression of the form $S : Sig$, where *Sig* is a signature, may only access *S*'s components via the interface provided in *Sig*. Signature ascription for EML provides forms of OO-style encapsulation. For example, classes, functions, and function cases can be hidden from clients, making them private to their enclosing structure. However, these declarations cannot be hidden arbitrarily, or else modular ITC would become unsound. Figure 18 shows a simple example of the problems that can occur. `ShapeMod` creates the abstract `Shape` class and two associated functions. ITC in `ShapeMod` finds `print` to be exhaustive and unambiguous, since `Shape` is abstract. Ascription to the `ShapeSig` signature hides `print`. Therefore, `print` is not part of `ShapeMod`'s interface, so `print` is not available to `CircleMod` and is therefore not checked again for exhaustiveness and unambiguity. If a `Circle` instance is passed to `bad`, however, `print` will be invoked, causing a *match nonexhaustive* error.

Our example is purposely similar to the `print` example in figure 6. In that case, the ITC requirements ensure that the problem is modularly detected. The same solution can be used here: a set of declarations can be safely hidden if that set could have been written as a separate module that passes modular ITC [21]. The `print` function in figure 18 does not satisfy this condition. If `print` were in its own module, the type system would force the existence of a global default case for `print`, which is now an external function. If `print` had such a case, then the function (and that case) could be safely hidden via signature ascription, and the problem for `Circle` would be resolved.

Aside from hiding entire declarations, it is useful to hide certain properties of a declaration. Several properties of classes may be hidden. First, a subset of a class's instance variables may be hidden. As mentioned in section 4, instance variables are scoped — the name of the structure declaring an instance variable is implicitly part of the name of the instance variable. Therefore, there is no conflict if a subclass in a new module creates an instance variable of the same name as a hidden one in the superclass. A concrete class can also be viewed as an abstract one, thereby disallowing clients from instantiating the class. Finally, a signature can declare a class *C* `sealed` [27], which prevents classes declared outside of *C*'s module from directly subclassing *C*. This construct can be used to faithfully model ML-style (non-extensible) datatypes. Our modular requirements can be relaxed in the presence of sealed hierarchies. For example, if an external function's owner and all available subclasses are sealed, then the function need not have a global default case, as in ML.

A function may be sealed by ascribing it and all associated cases to an ordinary ML-style value specification. Clients may still invoke the function but its extensibility is hidden, so clients may not add new cases. Therefore, function sealing allows us to model ML-style (non-extensible) functions. Function sealing is allowed under the same circumstances that the function and its cases may be hidden. Finally, a value specification of the form `val` $I : \tau$ may be replaced by `val` $I : \tau'$, where τ' is a supertype of τ.

Several forms of information hiding are not captured by our ascription rules. It would be useful to ascribe a class declaration to one that specifies only a transitive, rather than direct, superclass. Unfortunately, this flexibility makes modular ITC unsound. For example, a client of two classes C and C' can write ambiguous function cases that appear to be disjoint, and therefore pass static checks, if the fact that C subclasses C' is hidden from the client. It would also be useful to ascribe a class declaration to a type declaration, possibly augmented with Modula-3-style *partial revelations* [22] to reveal some of the class's underlying structure.

5.3 Functors

In the presence of EML's features, functors can provide a great deal of flexibility. Figure 19 illustrates the kinds of idioms we would like to express. The `Colorize` functor implements a form of *mixin* [4, 10, 13], which is a class parameterized by its superclass. The functor creates a colored version of some unknown subclass `APoint` of `Point`.

```
structure PointMod = struct
  abstract class Point()
  fun draw:Point → unit
end
signature APointSig = sig
  class APoint(x:int,y:int)
    extends Point of {x:int,y:int}
  extend fun draw (APoint {x=x,y=y})
end
```

```
functor Colorize(M:APointSig) = struct
  class ColorPoint(x:int,y:int,color:int)
    extends M.APoint(x,y) of {color:int=color}
  extend fun draw
    (ColorPoint {x=x,y=y,color=color}) = ...
  fun getColor:ColorPoint → int
  extend fun getColor
    (ColorPoint {x=x,y=y,color=color}) = color
end
```

Figure 19: Idioms involving EML functors.

An overriding case for the existing `draw` function is given, in order to draw colored points specially. The functor also introduces a new function for accessing the color of a colored point, with an associated case.

We would like to perform modular ITC once on a functor body, guaranteeing completeness and unambiguity of all relevant functions no matter how the functor is instantiated. The major challenge for modular ITC of functors like `Colorize` is the fact that the identities of some classes, for example `M.APoint`, are unknown. Instead we have only partial information about the relationship between `M.APoint` and other classes. To address this challenge, we can generalize the subclass relation in the static semantics to be *three-valued*, conservatively saying "don't know" when the partial class hierarchy information is inconclusive. We then appropriately generalize modular ITC to be conservative with respect to three-valued subclassing. Consider performing ITC on the body of `Colorize`. Although the identity of `M.APoint` is unknown, its relationship to `ColorPoint` is known, and this is enough information for modular ITC on `draw` to succeed. We have formalized this three-valued semantics in an earlier version of MINI-EML but have not proven it sound.

The restrictions on signature ascription described earlier limit the expressiveness of our `Colorize` functor. For example, the functor can only be instantiated with a class `APoint` that is a direct subclass of `Point`, rather than a transitive one. Also, `APoint`'s module must contain a `draw` case with exactly the pattern described in `APointSig`, and the module can have no other `draw` cases for `APoint` (e.g. a special case to handle the origin). However, we can safely remove these restrictions if we are willing to move some of the burden of ITC to clients of the functor. For example, we can allow `APoint` to be instantiated with a transitive subclass of `Point` on the condition that the resulting structure passes modular ITC. In the limit, this approach performs modular ITC once per instantiation of the functor, where the identities of all classes are known, rather than once on the functor body. However, it is possible that most of ITC could still be performed on the functor body in isolation, with only a few additional checks performed per instantiation.

6 Related Work

OML [25] and $ML_{\leq}$ [3] were described earlier. Zenger and Odersky [28] describe an extensible datatype mechanism in the context of an OO language. Extending a datatype has the effect of creating a new datatype that subtypes from the original one. To ensure exhaustiveness in the presence of datatype extension, all functions on extensible datatypes must include a global default case, while EML often requires only local defaults. Because Zenger's functions are not extensible, if new data variants require overriding function cases, a new function must be created that inherits the existing function cases and clients must be modified to invoke the new function. Like OML, Zenger's language includes both OO-style methods and ML-style functions. Zenger's language also retains a distinction between datatype "cases" and regular OO classes. Because Zenger's language supports subtyping between entire datatypes (rather than individual variants), it can provide more precise types than EML.

Garrigue shows how to use *polymorphic variants*, which are variants defined independent of any particular datatype, to obtain both modular data-variant and function extensibility in ML [14]. However, unlike EML, both kinds of extensibility require advance planning. When defining a type as a set of polymorphic variants, an extra type parameter must be used in place of recursive references to the type, to allow for future extension. Similarly, a function must take an extra parameter function to invoke in place of recursive references. As in Zenger's language, when a function is extended any clients that require the new functionality must be modified. Unlike EML, polymorphic variants preserve ML-style type inference.

Previous work on unifying functional and OO dispatching [9] provides ITC for patterns that are more general than those in EML, including conjunctions, disjunctions, and negations of arbitrary predicates. However, the ITC algorithm requires access to the entire program.

Jiazzi [19], a component system for Java, addresses issues of signature ascription and parameterized modules in the context of a traditional OO language. Jiazzi disallows hiding abstract methods because of problems analogous to the one shown in figure 18. Jiazzi also restricts the hiding of a superclass relationship, like EML, but Jiazzi allows such hiding if the superclass itself is also hidden. EML and Jiazzi each have challenges for information hiding that have no analogue in the other system: EML's unique challenges arise from its generalization of OO and functional dispatching semantics, and Jiazzi's unique challenges arise from cyclic linking.

EML's modular requirements are adapted from our previous work on Dubious [20, 21], a multimethod-based OO calculus supporting modular typechecking. In EML, we have generalized the requirements to fit an ML context and have also substantially simplified both their informal and formal presentations. The notion of modularity in Dubious is coarser than EML's static dependency relation: a Dubious module requires access to more of the program to soundly perform ITC than does an EML module. Dubious does not consider patterns, polymorphism, or ML-style modules.

7 Conclusions and Future Work

We described Extensible ML, an ML-like language that supports hierarchical, extensible datatypes and functions. Such constructs allow for the easy addition of both new data variants and new operations to existing abstractions, resolving a long-standing tension between the functional and object-oriented styles. At the same time, EML retains completely modular typechecking of function implementations. This contrasts with previous languages based on extensible datatypes and functions, which require link-time checks to ensure type safety. We have formalized EML in MINI-EML and proven its type system sound.

There are several directions for future work. We have built a prototype interpreter for the core of EML, and we plan to pursue case studies to gauge the utility of our modular type system in practice. Currently EML does not allow aliasing of classes or extensible functions. A general approach to handling aliasing would allow classes and extensible functions to be less second-class. Finally, more work is needed to integrate EML with ML-style modules, particularly functors. We will pursue the ideas presented in section 5, formalize this extension in MINI-EML, and implement it in our interpreter.

8 Acknowledgments

Thanks to Jonathan Aldrich, Sorin Lerner, and Vass Litvinov for helpful comments on the paper. This work was supported in part by NSF grant CCR-9970986, NSF Young Investigator Award CCR-9457767, gifts from Sun Microsystems and IBM, and a Wilma Bradley Graduate Fellowship.

References

[1] K. Arnold, J. Gosling, and D. Holmes. *The Java Programming Language Third Edition*. Addison-Wesley, Reading, MA, third edition, 2000.

[2] D. Bonniot. Type-checking multi-methods in ML (a modular approach). In *The Ninth International Workshop on Foundations of Object-Oriented Languages, FOOL 9*, Portland, Oregon, USA, January 2002.

[3] F. Bourdoncle and S. Merz. Type-checking higher-order polymorphic multi-methods. In *Conference Record of POPL '97: The 24th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 302–315, Paris, France, 15–17 Jan. 1997.

[4] G. Bracha and W. Cook. Mixin-based inheritance. In *ECOOP/OOPSLA '90*, pages 303–311, 1990.

[5] G. Castagna, G. Ghelli, and G. Longo. A calculus for overloaded functions with subtyping. *Information and Computation*, 117(1):115–135, Feb. 1995. A preliminary version appeared in *ACM Conference on LISP and Functional Programming*, June 1992 (pp. 182–192).

[6] C. Chambers. Object-oriented multi-methods in Cecil. In O. L. Madsen, editor, *ECOOP '92, European Conference on Object-Oriented Programming, Utrecht, The Netherlands*, volume 615 of *Lecture Notes in Computer Science*, pages 33–56. Springer-Verlag, New York, NY, 1992.

[7] C. Chambers and G. T. Leavens. Typechecking and modules for multimethods. *ACM Transactions on Programming Languages and Systems*, 17(6):805–843, Nov. 1995.

[8] W. R. Cook. Object-oriented programming versus abstract data types. In J. W. de Bakker, W. P. de Roever, and G. Rozenberg, editors, *Foundations of Object-Oriented Languages, REX School/Workshop, Noordwijkerhout, The Netherlands, May/June 1990*, volume 489 of *Lecture Notes in Computer Science*, pages 151–178. Springer-Verlag, New York, NY, 1991.

[9] M. Ernst, C. Kaplan, and C. Chambers. Predicate dispatching: A unified theory of dispatch. In E. Jul, editor, *ECOOP '98–Object-Oriented Programming*, volume 1445 of *Lecture Notes in Computer Science*, pages 186–211. Springer, 1998.

[10] R. B. Findler and M. Flatt. Modular object-oriented programming with units and mixins. In *Proceedings of the ACM SIGPLAN International Conference on Functional Programming (ICFP '98)*, volume 34(1) of *ACM SIGPLAN Notices*, pages 94–104. ACM, June 1998.

[11] K. Fisher and J. Reppy. The design of a class mechanism for MOBY. In *Proceedings of the ACM SIGPLAN '99 Conference on Programming Language Design and Implementation*, pages 37–49, Atlanta, Georgia, May 1–4, 1999.

[12] K. Fisher and J. Reppy. Extending Moby with inheritance-based subtyping. In *14th European Conference on Object-Oriented Programming*, volume 1850 of *Lecture Notes in Computer Science*, pages 83–107, June 2000.

[13] M. Flatt, S. Krishnamurthi, and M. Felleisen. Classes and mixins. In *Conference Record of POPL 98: The 25TH ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, San Diego, California*, pages 171–183, New York, NY, 1998.

[14] J. Garrigue. Code reuse through polymorphic variants. In *Workshop on Foundations of Software Engineering*, November 2000.

[15] J. Gosling, B. Joy, G. Steele, and G. Bracha. *The Java Language Specification Second Edition*. The Java Series. Addison-Wesley, Boston, Mass., 2000.

[16] A. Igarashi, B. C. Pierce, and P. Wadler. Featherweight Java: a minimal core calculus for Java and GJ. *ACM Transactions on Programming Languages and Systems*, 23(3):396–450, May 2001.

[17] S. Kahrs, D. Sannella, and A. Tarlecki. The definition of extended ML: A gentle introduction. *Theoretical Computer Science*, 173(2):445–484, 28 Feb. 1997.

[18] S. Krishnamurthi, M. Felleisen, and D. P. Friedman. Synthesizing object-oriented and functional design to promote re-use. In E. Jul, editor, *ECOOP'98–Object-Oriented Programming, 12th European Conference, Brussels, Belgium*, volume 1445 of *Lecture Notes in Computer Science*, pages 91–113. Springer-Verlag, July 1998.

[19] S. McDirmid, M. Flatt, and W. C. Hsieh. Jiazzi: new-age components for old-fashioned java. In *Proceedings of the OOPSLA '01 conference on Object Oriented Programming Systems Languages and Applications*, pages 211–222. ACM Press, 2001.

[20] T. Millstein and C. Chambers. Modular statically typed multimethods. In R. Guerraoui, editor, *ECOOP '99 – Object-Oriented Programming 13th European Conference, Lisbon Portugal*, volume 1628 of *Lecture Notes in Computer Science*, pages 279–303. Springer-Verlag, New York, NY, June 1999.

[21] T. Millstein and C. Chambers. Modular statically typed multimethods. *Information and Computation*, 175(1):76–118, May 2002.

[22] G. Nelson. *Systems Programming with Modula-3*. Prentice Hall, 1991.

[23] M. Odersky and P. Wadler. Pizza into Java: Translating theory into practice. In *Conference Record of POPL '97: The 24th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 146–159, Paris, France, 15–17 Jan. 1997.

[24] D. Rémy and J. Vouillon. Objective ML: An effective object-oriented extension of ML. *Theory and Practice of Object Systems*, 4(1):27–52, 1998.

[25] J. Reppy and J. Riecke. Simple objects for Standard ML. In *Proceedings of the ACM SIGPLAN '96 Conference on Programming Language Design and Implementation*, pages 171–180, Philadelphia, Pennsylvania, 21–24 May 1996.

[26] J. C. Reynolds. User defined types and procedural data structures as complementary approaches to data abstraction. In D. Gries, editor, *Programming Methodology, A Collection of Articles by IFIP WG2.3*, pages 309–317. Springer-Verlag, New York, NY, 1978.

[27] A. Shalit. *The Dylan Reference Manual: The Definitive Guide to the New Object-Oriented Dynamic Language*. Addison-Wesley, Reading, Mass., 1997.

[28] M. Zenger and M. Odersky. Extensible algebraic datatypes with defaults. In *Proceedings of the 2001 ACM SIGPLAN International Conference on Functional Programming*. ACM, September 3-5 2001.

A Type Preservation

A.1 Shared Preliminaries and Lemmas

These preliminaries and lemmas are also used in the progress proof in appendix B.

As in the inference rules, we assume a global structure table ST. We further assume that for each $Sn \in \mathrm{dom}(ST)$ we have $ST(Sn)$ OK. The empty sequence is denoted $\bullet$. The notation $\vdash E : \tau$ is shorthand for $\{\};\bullet \vdash E : \tau$.

Lemma A.1 If $\overline{\alpha} \vdash \tau$ OK, then all type variables in τ are in $\overline{\alpha}$.
Proof By (strong) induction on the depth of the derivation of $\overline{\alpha} \vdash \tau$ OK. Case analysis on the last rule used in the derivation. For TVarOK, τ has the form α and the premise ensures that $\alpha \in \overline{\alpha}$. All other cases are easily proven by induction. □

Lemma A.2 If $\overline{\alpha} \vdash \tau$ OK and $|\overline{\alpha}| = |\overline{\tau}|$ and $\overline{\alpha'} \vdash \overline{\tau}$ OK, then $\overline{\alpha'} \vdash [\overline{\alpha} \mapsto \overline{\tau}]\tau$ OK.
Proof By (strong) induction on the depth of the derivation of $\overline{\alpha} \vdash \tau$ OK. Case analysis on the last rule used in the derivation. For TVarOK, τ has the form α and the premise ensures that $\alpha \in \overline{\alpha}$. Therefore $[\overline{\alpha} \mapsto \overline{\tau}]\tau$ is some τ_0 in $\overline{\tau}$. By assumption $\overline{\alpha'} \vdash \tau_0$ OK so the result follows. All other cases are easily proven by induction. □

Lemma A.3 If $(\overline{\tau}\,C) \leq \tau$, then τ has the form $(\overline{\tau_1}\,C')$.
Proof By (strong) induction on the depth of the derivation of $(\overline{\tau}\,C) \leq \tau$. Case analysis of the last rule used in the derivation.

- Case SubTRef. Then $\tau = (\overline{\tau}\,C)$.
- Case SubTTrans. Then $(\overline{\tau}\,C) \leq \tau'$ and $\tau' \leq \tau$. By induction τ' has the form $(\overline{\tau_2}\,C'')$. Then by induction again, τ has the form $(\overline{\tau_1}\,C')$.
- Case SubTExt. Then τ has the form $[\overline{\alpha} \mapsto \overline{\tau}]Ct$, which is also of the form $(\overline{\tau_1}\,C')$.

□

Lemma A.4 If $(\overline{\tau}\,C) \leq (\overline{\tau_1}\,C')$, then $\overline{\tau} = \overline{\tau_1}$.
Proof By (strong) induction on the depth of the derivation of $(\overline{\tau}\,C) \leq (\overline{\tau_1}\,C')$. Case analysis of the last rule used in the derivation.

- Case SubTRef. Then $(\overline{\tau}\,C) = (\overline{\tau_1}\,C')$, so $\overline{\tau} = \overline{\tau_1}$.
- Case SubTTrans. Then $(\overline{\tau}\,C) \leq \tau$ and $\tau \leq (\overline{\tau_1}\,C')$. By Lemma A.3, τ has the form $(\overline{\tau_2}\,C'')$. Then by induction we have $\overline{\tau} = \overline{\tau_2}$ and $\overline{\tau_2} = \overline{\tau_1}$, so $\overline{\tau} = \overline{\tau_1}$.
- Case SubTExt. Then $C = Sn.Cn$ and $(\overline{\tau_1}\,C') = [\overline{\alpha} \mapsto \overline{\tau}](\overline{\tau_2}\,C')$ and (<`abstract`> `class` $\overline{\alpha}\;Cn(I_1 : \tau_1, \ldots, I_m : \tau_m)$ `extends` $(\overline{\tau_2}\,C')\ \ldots) \in ST(Sn)$. By ClassOK, we have $\overline{\tau_2} = \overline{\alpha}$. Therefore $(\overline{\tau_1}\,C') = [\overline{\alpha} \mapsto \overline{\tau}](\overline{\alpha}\,C') = (\overline{\tau}\,C')$. Therefore $\overline{\tau} = \overline{\tau_1}$.

□

Lemma A.5 If $(\overline{\tau}\,C) \leq (\overline{\tau_1}\,C')$ then $C \leq C'$.
Proof By (strong) induction on the depth of the derivation of $(\overline{\tau}\,C) \leq (\overline{\tau_1}\,C')$. Case analysis of the last rule used in the derivation.

- Case SubTRef. Then $(\overline{\tau}\,C) = (\overline{\tau_1}\,C')$, so $C = C'$. Then the result holds by SubRef.
- Case SubTTrans. Then $(\overline{\tau}\,C) \leq \tau$ and $\tau \leq (\overline{\tau_1}\,C')$. By Lemma A.3 τ has the form $(\overline{\tau_2}\,C'')$. Then by induction we have that $C \leq C''$ and $C'' \leq C'$. Therefore the result follows by SubTrans.
- Case SubTExt. Then $C = Sn.Cn$ and (<`abstract`> `class` $\overline{\alpha}\;Cn(\overline{I_0} : \overline{\tau_0})$ `extends` $(\overline{\tau_2}\,C')\ \ldots) \in ST(Sn)$. Then the result follows by SubExt.

□

Lemma A.6 If $\tau \leq \tau_1 * \cdots * \tau_k$, then τ has the form $\tau'_1 * \cdots * \tau'_k$, where for all $1 \leq i \leq k$ we have $\tau'_i \leq \tau_i$.
Proof By (strong) induction on the depth of the derivation of $\tau \leq \tau_1 * \cdots * \tau_k$. Case analysis of the last rule used in the derivation.

- Case SubTRef. Then $\tau = \tau_1 * \cdots * \tau_k$. By SubTRef, for all $1 \leq i \leq k$ we have $\tau_i \leq \tau_i$, so the result follows.
- Case SubTTrans. Then $\tau \leq \tau'$ and $\tau' \leq \tau_1 * \cdots * \tau_k$. By induction τ' has the form $\tau''_1 * \cdots * \tau''_k$, where for all $1 \leq i \leq k$ we have $\tau''_i \leq \tau_i$. Then by induction again, τ has the form $\tau'_1 * \cdots * \tau'_k$, where for all $1 \leq i \leq k$ we have $\tau'_i \leq \tau''_i$. Then by SubTTrans, for all $1 \leq i \leq k$ we have $\tau'_i \leq \tau_i$.
- Case SubTTup. Then τ has the form $\tau'_1 * \cdots * \tau'_k$, where for all $1 \leq i \leq k$ we have $\tau'_i \leq \tau_i$.

□

Lemma A.7 If $Sn.Cn \leq Sn'.Cn'$ and $\overline{\alpha_0} \vdash (\overline{\tau}\;Sn.Cn)$ OK then (1) $(\overline{\tau}\;Sn.Cn) \leq (\overline{\tau}\;Sn'.Cn')$; and (2) $\overline{\alpha_0} \vdash (\overline{\tau}\;Sn'.Cn')$ OK.
Proof By (strong) induction on the depth of the derivation of $Sn.Cn \leq Sn'.Cn'$. Case analysis of the last rule used in the derivation.

- Case SubRef. Then $Sn'.Cn' = Sn.Cn$. Then condition 1 follows from SubTRef, and condition 2 follows by assumption.

- Case SUBTRANS. Then $Sn.Cn \leq Sn''.Cn''$ and $Sn''.Cn'' \leq Sn'.Cn'$. By induction we have $(\overline{\tau}\ Sn.Cn) \leq (\overline{\tau}\ Sn''.Cn'')$ and $\overline{\alpha_0} \vdash (\overline{\tau}\ Sn''.Cn'')$ OK. Then by induction again we have $(\overline{\tau}\ Sn''.Cn'') \leq (\overline{\tau}\ Sn'.Cn')$ and $\overline{\alpha_0} \vdash (\overline{\tau}\ Sn'.Cn')$ OK. Therefore condition 2 is shown, and condition 1 follows from SubTTrans.
- Case SUBEXT. Then (<abstract> class $\overline{\alpha}\ Cn(\overline{I_0} : \overline{\tau_0})$ extends $(\overline{\tau'}\ Sn'.Cn')(\overline{E})\ \ldots) \in ST(Sn)$. Then by CLASSOK we have $\overline{\tau'} = \overline{\alpha}$. Since $\overline{\alpha_0} \vdash (\overline{\tau}\ Sn.Cn)$ OK, by CLASSTYPEOK we have $|\overline{\alpha}| = |\overline{\tau}|$ and $\overline{\alpha_0} \vdash \overline{\tau}$ OK. Therefore by SUBTEXT we have $(\overline{\tau}\ Sn.Cn) \leq [\overline{\alpha} \mapsto \overline{\tau}](\overline{\alpha}\ Sn'.Cn')$. Since $[\overline{\alpha} \mapsto \overline{\tau}](\overline{\alpha}\ Sn'.Cn') = (\overline{\tau}\ Sn'.Cn')$, condition 1 is shown. Also by CLASSOK $\overline{\alpha} \vdash (\overline{\alpha}\ Sn'.Cn')(\overline{E})$ OK, so by T-SUPER we have have $\overline{\alpha} \vdash (\overline{\alpha}\ Sn'.Cn')$ OK. Therefore by Lemma A.2 we have $\overline{\alpha_0} \vdash (\overline{\tau}\ Sn'.Cn')$ OK, so condition 2 is shown.

□

Lemma A.8 If $\overline{\alpha} \vdash Ct$ OK then repType(Ct) is well-defined and has the form $\{\overline{V_0 : \tau_0}\}$.
Proof Let $Ct = (\overline{\tau}\ Sn.Cn)$. We prove this lemma by induction on the length of the longest path in the superclass graph from $Sn.Cn$ (in other words, the number of non-trivial superclasses of $Sn.Cn$). By CLASSTYPEOK we have $\overline{\alpha} \vdash \overline{\tau}$ OK and (<abstract> class $\overline{\alpha_0}\ Cn(\overline{I_1 : \tau_1})$ <<extends $Ct'(\overline{E})$ >> of $\{\overline{Vn : \tau_2 = E_2}\}) \in ST(Sn)$ and $|\overline{\alpha_0}| = |\overline{\tau}|$. There are two cases to consider.

- The length of the longest path in the superclass graph from $Sn.Cn$ is 0. Then $Sn.Cn$ has no non-trivial superclasses, so the extends clause in the declaration of $Sn.Cn$ is absent. Then by REPTYPE we have repType(Ct) = $[\overline{\alpha_0} \mapsto \overline{\tau}]\{Sn.\overline{Vn : \tau_2}\}$, so the result follows.
- The length of the longest path in the superclass graph from $Sn.Cn$ is $i > 0$. Then $Sn.Cn$ has at least one non-trivial superclass, so the extends clause in the declaration of $Sn.Cn$ is present. Then by CLASSOK we have $\overline{\alpha_0} \vdash Ct'(\overline{E})$ OK, so by T-SUPER we have $\overline{\alpha_0} \vdash Ct'$ OK. Since Ct' must have the form $(\overline{\tau_1}\ Sn'.Cn')$, where the length of the longest path in the superclass graph from $Sn'.Cn'$ is $i-1$, by induction we have that repType(Ct') has the form $\{\overline{V_0 : \tau_0}\}$. Then by REPTYPE we have repType(Ct) = $[\overline{\alpha_0} \mapsto \overline{\tau}]\{\overline{V_0 : \tau_0}, Sn.\overline{Vn : \tau_2}\}$, so the result follows.

□

Lemma A.9 If $\overline{\alpha} \vdash Ct$ OK and $Ct \leq Ct'$, then $\overline{\alpha} \vdash Ct'$ OK.
Proof By (strong) induction on the depth of the derivation of $Ct \leq Ct'$. Case analysis of the last rule used in the derivation.

- Case SUBTREF. Then $Ct = Ct'$, so the result follows by assumption.
- Case SUBTTRANS. Then $Ct \leq \tau$ and $\tau \leq Ct'$. By Lemma A.3 τ has the form Ct''. Therefore by induction we have $\overline{\alpha} \vdash Ct''$ OK, and by induction again we have $\overline{\alpha} \vdash Ct'$ OK.
- Case SUBTEXT. Then $Ct = (\overline{\tau}\ Sn.Cn)$ and $Ct' = [\overline{\alpha_0} \mapsto \overline{\tau}]Ct''$ and (<abstract> class $\overline{\alpha_0}\ Cn(\overline{I_0} : \overline{\tau_0})$ extends $Ct''(\overline{E})\ \ldots) \in ST(Sn)$. By CLASSOK we have $\overline{\alpha_0} \vdash Ct''(\overline{E})$ OK, so by T-SUPER we have $\overline{\alpha_0} \vdash Ct''$ OK. Since $\overline{\alpha} \vdash Ct$ OK, by CLASSTYPEOK we have $\overline{\alpha} \vdash \overline{\tau}$ OK. Therefore by Lemma A.2 we have $\overline{\alpha} \vdash [\overline{\alpha_0} \mapsto \overline{\tau}]Ct''$ OK.

□

Lemma A.10 If repType$(Ct) = \{\overline{V : \tau}\}$ and $\overline{\alpha} \vdash Ct$ OK, then $\overline{\alpha} \vdash \overline{\tau}$ OK.
Proof By induction on the depth of the derivation of repType$(Ct) = \tau$. Then by RepType $Ct = (\overline{\tau_0}\ Sn.Cn)$ and $\{\overline{V : \tau}\} = [\overline{\alpha_0} \mapsto \overline{\tau_0}]\{< \overline{V_1 : \tau_1}, > Sn.\overline{Vn : \tau_2}\}$ and (<<abstract>> class $\overline{\alpha_0}\ Cn(\overline{I_0 : \tau_0})$ <extends $Ct'(\overline{E})$ > of $\{\overline{Vn : \tau_2 = E_2}\}) \in ST(Sn)$ and $<$ repType$(Ct') = \{\overline{V_1 : \tau_1}\}$. By CLASSOK we have $< \overline{\alpha_0} \vdash Ct'(\overline{E})$ OK $>$, so by T-SUPER we have $< \overline{\alpha_0} \vdash Ct'$ OK $>$. Then by induction we have have $< \overline{\alpha_0} \vdash \overline{\tau_1}$ OK. Also by CLASSOK we have $\overline{\alpha_0} \vdash \overline{\tau_2}$ OK. Since $\overline{\alpha} \vdash Ct$ OK, by CLASSTYPEOK we have that $\overline{\alpha} \vdash \overline{\tau_0}$ OK. Therefore by Lemma A.2 we have $< \overline{\alpha} \vdash [\overline{\alpha_0} \mapsto \overline{\tau_0}]\overline{\tau_1}$ OK $>$ and $\overline{\alpha} \vdash [\overline{\alpha_0} \mapsto \overline{\tau_0}]\overline{\tau_2}$ OK, so the result follows. □

Lemma A.11 If repType$(Ct) = \{\overline{V : \tau}\}$ and $|\overline{\alpha}| = |\overline{\tau}|$, then repType$([\overline{\alpha} \mapsto \overline{\tau}]Ct) = [\overline{\alpha} \mapsto \overline{\tau}]\{\overline{V : \tau}\}$.
Proof By induction on the depth of the derivation of repType$(Ct) = \{\overline{V : \tau}\}$. Then by REPTYPE $Ct = (\overline{\tau_0}\ Sn.Cn)$ and $\{\overline{V : \tau}\} = [\overline{\alpha_0} \mapsto \overline{\tau_0}]\{< \overline{V_1 : \tau_1}, > Sn.\overline{Vn : \tau_2}\}$ and (<<abstract>> class $\overline{\alpha_0}\ Cn(\overline{I_4 : \tau_4})$ <extends $Ct'(\overline{E})$ > of $\{\overline{Vn : \tau_2 = E_2}\}) \in ST(Sn)$ and $<$ repType$(Ct') = \{\overline{V_1 : \tau_1}\} >$. Therefore by REPTYPE we have repType$([\overline{\alpha} \mapsto \overline{\tau}](\overline{\tau_0}\ Sn.Cn)) = [\overline{\alpha_0} \mapsto [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0}]\{< \overline{V_1 : \tau_1}, > Sn.\overline{Vn : \tau_2}\}$. By CLASSOK we have $< \overline{\alpha_0} \vdash Ct'(\overline{E})$ OK $>$, so by T-SUPER we have $< \overline{\alpha_0} \vdash Ct'$ OK $>$. Then by Lemma A.10 we have $< \overline{\alpha_0} \vdash \overline{\tau_1}$ OK $>$, so by Lemma A.1 all type variables $\overline{\tau_1}$ are in $\overline{\alpha_0}$. Also by CLASSOK we have $\overline{\alpha_0} \vdash \overline{\tau_2}$ OK, so by Lemma A.1 all type variables in $\overline{\tau_2}$ are in $\overline{\alpha_0}$. Therefore $[\overline{\alpha_0} \mapsto [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0}]\{\overline{V_1 : \tau_1}, Sn.\overline{Vn : \tau_2}\}$ is equivalent to $[\overline{\alpha} \mapsto \overline{\tau}][\overline{\alpha_0} \mapsto \overline{\tau_0}]\{\overline{V_1 : \tau_1}, Sn.\overline{Vn : \tau_2}\}$, so the result follows. □

Lemma A.12 If $\bullet \vdash Ct$ OK and $Ct \leq Ct'$ then repType(Ct) has the form $\{\overline{V_1 : \tau_1}, \overline{V_2 : \tau_2}\}$ and repType(Ct') = $\{\overline{V_1 : \tau_1}\}$.
Proof By induction on the depth of the derivation of $Ct \leq Ct'$. Case analysis of the last rule used in the derivation.

- Case SUBTREF. Then $Ct = Ct'$. Since $\bullet \vdash Ct$ OK, by Lemma A.8 we have that repType(Ct) is well-defined and has the form $\{\overline{V : \tau}\}$. Therefore, repType(Ct') = $\{\overline{V : \tau}\}$ as well, so the result follows.
- Case SUBTTRANS. Then $Ct \leq \tau$ and $\tau \leq Ct'$. By Lemma A.3 τ has the form Ct''. Then by Lemma A.9 we have $\bullet \vdash Ct''$ OK and $\bullet \vdash Ct'$ OK. Therefore by induction we have repType(Ct) = $\{\overline{V_1 : \tau_1}, \overline{V_3 : \tau_3}, \overline{V_4 : \tau_4}\}$ and repType(Ct'') = $\{\overline{V_1 : \tau_1}, \overline{V_3 : \tau_3}\}$. By induction again we have repType(Ct') = $\{\overline{V_1 : \tau_1}\}$, so the result is shown.

- Case SUBTEXT. Then $Ct = (\overline{\tau}\ Sn.Cn)$ and $Ct' = [\overline{\alpha} \mapsto \overline{\tau}]Ct''$ and (<abstract> `class` $\overline{\alpha}\ Cn(\overline{I_0 : \tau_0})$ `extends` $Ct''(\overline{E})$ `of` $\{\overline{Vn : \tau_2 = E_2}\}) \in ST(Sn)$. Since $\bullet \vdash Ct$ OK, by Lemma A.8 we have that repType(Ct) is well defined and has the form $\{\overline{V_3 : \tau_3}\}$. Then by REPTYPE we have $\{\overline{V_3 : \tau_3}\} = [\overline{\alpha} \mapsto \overline{\tau}]\{\overline{V_1 : \tau_1}, Sn.\overline{Vn : \tau_2}\}$ and repType$(Ct'') = \{\overline{V_1 : \tau_1}\}$. Then by Lemma A.11 we have repType$(Ct') = [\overline{\alpha} \mapsto \overline{\tau}]\{\overline{V_1 : \tau_1}\}$, so the result follows.

□

A.2 Simple Lemmas

Lemma A.13 If $\tau \leq \tau_1 \to \tau_2$, then τ has the form $\tau_1' \to \tau_2'$, where $\tau_1 \leq \tau_1'$ and $\tau_2' \leq \tau_2$.
Proof By (strong) induction on the depth of the derivation of $\tau \leq \tau_1 \to \tau_2$. Case analysis on the last rule used in the derivation.

- Case SUBTREF. Therefore $\tau = \tau_1 \to \tau_2$, so $\tau_1' = \tau_1$ and $\tau_2' = \tau_2$. By SUBTREF we have $\tau_1 \leq \tau_1'$ and $\tau_2' \leq \tau_2$.
- Case SUBTTRANS. Therefore $\tau \leq \tau'$ and $\tau' \leq \tau_1 \to \tau_2$. By induction τ' has the form $\tau_1'' \to \tau_2''$, where $\tau_1 \leq \tau_1''$ and $\tau_2'' \leq \tau_2$. Therefore, again by induction τ has the form $\tau_1' \to \tau_2'$, where $\tau_1'' \leq \tau_1'$ and $\tau_2' \leq \tau_2''$. By SUBTTRANS we have $\tau_1 \leq \tau_1'$ and $\tau_2' \leq \tau_2$.
- Case SUBTFUN. Then τ has the form $\tau_1' \to \tau_2'$, where $\tau_1 \leq \tau_1'$ and $\tau_2' \leq \tau_2$.

□

Lemma A.14 If rep$(Ct(\overline{E}))$ = $\{\overline{V_1 = E_1}\}$ and repType(Ct) = $\{\overline{V_2 : \tau_2}\}$ then $\overline{V_1} = \overline{V_2}$.
Proof By induction on the depth of the derivation of rep$(Ct(\overline{E}))$ = $\{\overline{V_1 = E_1}\}$. By REP we have $Ct = (\overline{\tau}\ Sn.Cn)$ and (<<abstract>> `class` $\overline{\alpha}\ Cn(\overline{I_0 : \tau_0})$ <`extends` $Ct'(\overline{E_0})$> `of` $\{\overline{Vn : \tau_2 = E_2}\}) \in ST(Sn)$ and <rep$(Ct'(\overline{E_0}))$ = $\{\overline{V_3 = E_3}\}$> and $\overline{V_1}$ is equivalent to $<\overline{V_3},> Sn.\overline{Vn}$. Since repType($Ct$) = $\{\overline{V_2 : \tau_2}\}$, by REPTYPE we have <repType(Ct') = $\{\overline{V_4 : \tau_4}\}$>, so by induction $<\overline{V_3} = \overline{V_4}>$. Then by REPTYPE $\overline{V_2}$ is equivalent to $<\overline{V_3},> Sn.\overline{Vn}$. □

A.3 Type Substitution

Lemma A.15 If $\tau \leq \tau'$ and $|\overline{\alpha}| = |\overline{\tau}|$, then $[\overline{\alpha} \mapsto \overline{\tau}]\tau \leq [\overline{\alpha} \mapsto \overline{\tau}]\tau'$.
Proof By (strong) induction on the depth of the derivation of $\tau \leq \tau'$. Case analysis of the last rule used in the derivation. The only interesting case is SUBTEXT.

- Case SUBTEXT. Then τ has the form $\overline{\tau_0}\ Sn.Cn$ and τ' has the form $[\overline{\alpha_0} \mapsto \overline{\tau_0}]Ct$ and (<abstract> `class` $\overline{\alpha_0}\ Cn(\overline{I_3 : \tau_3})$ `extends` $Ct(\overline{E})\ \ldots) \in ST(Sn)$. Then by SUBTEXT we have $([\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0})\ Sn.Cn \leq [\overline{\alpha_0} \mapsto [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0}]Ct$. Note that $([\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0})\ Sn.Cn$ is equivalent to $[\overline{\alpha} \mapsto \overline{\tau}](\overline{\tau_0}\ Sn.Cn)$. Further, by CLASSOK we have that $\overline{\alpha_0} \vdash Ct(\overline{E})$ OK, so by T-SUPER also $\overline{\alpha_0} \vdash Ct$ OK. Therefore, by Lemma A.1 all type variables in Ct are in $\overline{\alpha_0}$. Therefore we have that $[\overline{\alpha_0} \mapsto [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0}]Ct$ is equivalent to $[\overline{\alpha} \mapsto \overline{\tau}][\overline{\alpha_0} \mapsto \overline{\tau_0}]Ct$. Therefore the result follows.

□

Lemma A.16 If $\Gamma;\overline{\alpha} \vdash E : \tau$ and $|\overline{\alpha}| = |\overline{\tau}|$ and $\overline{\alpha_0} \vdash \overline{\tau}$ OK, then $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma;\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]E : [\overline{\alpha} \mapsto \overline{\tau}]\tau$.
Proof By (strong) induction on the depth of the derivation of $\Gamma;\overline{\alpha} \vdash E : \tau$. Case analysis of the last rule used in the derivation.

- Case T-ID. Then $E = I$ and $(I,\tau) \in \Gamma$. Therefore, $(I, [\overline{\alpha} \mapsto \overline{\tau}]\tau) \in [\overline{\alpha} \mapsto \overline{\tau}]\Gamma$. Also, $I = [\overline{\alpha} \mapsto \overline{\tau}]I$. So by T-ID we have $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma;\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]E : [\overline{\alpha} \mapsto \overline{\tau}]\tau$.
- Case T-NEW. Then $E = Ct(\overline{E})$ and $\tau = Ct$ and $\overline{\alpha} \vdash Ct(\overline{E})$ OK and $Ct = (\overline{\tau_1}\ Sn.Cn)$ and concrete($Sn.Cn$). By T-SUPER we have $\overline{\alpha} \vdash Ct$ OK and (<abstract> `class` $\overline{\alpha_1}\ Cn(\overline{I_0 : \tau_0})\ \ldots) \in ST(Sn)$ and $\Gamma;\overline{\alpha} \vdash \overline{E : \tau_0'}$ and $\overline{\tau_0'} \leq [\overline{\alpha_1} \mapsto \overline{\tau_1}]\overline{\tau_0}$. By Lemma A.2 we have $\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]Ct$ OK. Since $Ct = (\overline{\tau_1}\ Sn.Cn)$ we have $[\overline{\alpha} \mapsto \overline{\tau}]Ct = [\overline{\alpha} \mapsto \overline{\tau}](\overline{\tau_1}\ Sn.Cn) = ([\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}\ Sn.Cn)$, which is of the form $(\overline{\tau_2}\ Sn.Cn)$. By induction we have $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma;\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]\overline{E} : [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0'}$. By Lemma A.15 we have $[\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0'} \leq [\overline{\alpha} \mapsto \overline{\tau}][\overline{\alpha_1} \mapsto \overline{\tau_1}]\overline{\tau_0}$. By CLASSOK we have $\overline{\alpha_1} \vdash \overline{\tau_0}$ OK, so by Lemma A.1 all type variables in each $\overline{\tau_0}$ are in $\overline{\alpha_1}$. Therefore $[\overline{\alpha} \mapsto \overline{\tau}][\overline{\alpha_1} \mapsto \overline{\tau_1}]\overline{\tau_0}$ is equivalent to $[\overline{\alpha_1} \mapsto [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}]\overline{\tau_0}$. Therefore by T-SUPER we have $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma;\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]E$ OK, and the result follows by T-NEW.
- Case T-REP. Then $E = Ct\ \{\overline{V = E}\}$ and $\tau = Ct$ and $\overline{\alpha} \vdash Ct$ OK and $Ct = (\overline{\tau_1}\ Sn.Cn)$ and concrete($Sn.Cn$) repType(Ct) = $\{\overline{V_0 : \tau_0}\}$ and $\Gamma;\overline{\alpha} \vdash \overline{E : \tau_0'}$ and $\overline{\tau_0'} \leq \overline{\tau_0}$. By Lemma A.2 we have $\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]Ct$ OK. Since $Ct = (\overline{\tau_1}\ Sn.Cn)$ we have $[\overline{\alpha} \mapsto \overline{\tau}]Ct = [\overline{\alpha} \mapsto \overline{\tau}](\overline{\tau_1}\ Sn.Cn) = ([\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}\ Sn.Cn)$, which is of the form $(\overline{\tau_2}\ Sn.Cn)$. By Lemma A.11 we have repType($[\overline{\alpha} \mapsto \overline{\tau}]Ct$) = $[\overline{\alpha} \mapsto \overline{\tau}]\{\overline{V_0 : \tau_0}\}$. By induction we have $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma;\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]\overline{E} : [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0'}$. By Lemma A.15 we have $[\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0'} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0}$. Therefore by T-REP the result follows.
- Case T-FUN. Then $E = \overline{\tau_1}\ Sn.Fn$ and $\tau = [\overline{\alpha_1} \mapsto \overline{\tau_1}](\hat{Mt} \to \tau')$ and $\overline{\alpha} \vdash \overline{\tau_1}$ OK and (`fun` $\overline{\alpha_1}\ Fn : Mt \to \tau') \in ST(Sn)$. By Lemma A.2 we have $\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}$ OK. Therefore by T-FUN we have $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma;\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}](\overline{\tau_1}\ Sn.Fn) : [\overline{\alpha} \mapsto \overline{\tau}][\overline{\alpha_1} \mapsto \overline{\tau_1}](\hat{Mt} \to \tau')$. By FUNOK we have $\overline{\alpha} \vdash \hat{Mt}$ OK and $\overline{\alpha} \vdash \tau'$ OK. Therefore by Lemma A.1 we have that all type variables in $\hat{Mt}$ and τ' are in $\overline{\alpha}$. Therefore, $[\overline{\alpha} \mapsto \overline{\tau}][\overline{\alpha_1} \mapsto \overline{\tau_1}](\hat{Mt} \to \tau')$ is equivalent to $[\overline{\alpha_1} \mapsto [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}](\hat{Mt} \to \tau')$, so the result follows.

- Case T-TUP. Then $E = (E_1, \ldots, E_k)$ and $\tau = \tau_1 * \cdots * \tau_k$ and for all $1 \leq i \leq k$ we have $\Gamma; \overline{\alpha} \vdash E_i : \tau_i$. Therefore by induction, for all $1 \leq i \leq k$ we have $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma; \overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]E_i : [\overline{\alpha} \mapsto \overline{\tau}]\tau_i$, and the result follows by T-TUP.
- Case T-APP. Then $E = E_1\ E_2$ and $\Gamma; \overline{\alpha} \vdash E_1 : \tau_2 \rightarrow \tau$ and $\Gamma; \overline{\alpha} \vdash E_2 : \tau_2'$ and $\tau_2' \leq \tau_2$. By induction we have $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma; \overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]E_1 : [\overline{\alpha} \mapsto \overline{\tau}](\tau_2 \rightarrow \tau)$ and $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma; \overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]E_2 : [\overline{\alpha} \mapsto \overline{\tau}]\tau_2'$. By Lemma A.15 we have $[\overline{\alpha} \mapsto \overline{\tau}]\tau_2' \leq [\overline{\alpha} \mapsto \overline{\tau}]\tau_2$, so the result follows by T-APP.

□

Lemma A.17 If matchType$(\tau, Pat) = (\Gamma, \tau')$ and $|\overline{\alpha}| = |\overline{\tau}|$, then matchType$([\overline{\alpha} \mapsto \overline{\tau}]\tau, Pat) = ([\overline{\alpha} \mapsto \overline{\tau}]\Gamma, [\overline{\alpha} \mapsto \overline{\tau}]\tau')$.
Proof By (strong) induction on the depth of the derivation of matchType$(\tau, Pat) = (\Gamma, \tau')$. Case analysis of the last rule used in the derivation.

- Case T-MATCHWILD. Then Pat has the form _ and $\Gamma = \{\}$ and $\tau' = \tau$. Then $[\overline{\alpha} \mapsto \overline{\tau}]\tau = [\overline{\alpha} \mapsto \overline{\tau}]\tau'$ and $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma = \{\}$, so the result follows by T-MATCHWILD.
- Case T-MATCHBIND. Then Pat has the form I `as` Pat' and $\Gamma = \Gamma' \cup \{(I, \tau')\}$ and matchType$(\tau, Pat') = (\Gamma', \tau')$. By induction we have matchType$([\overline{\alpha} \mapsto \overline{\tau}]\tau, Pat') = ([\overline{\alpha} \mapsto \overline{\tau}]\Gamma', [\overline{\alpha} \mapsto \overline{\tau}]\tau')$. Therefore by T-MATCHBIND we have matchType$([\overline{\alpha} \mapsto \overline{\tau}]\tau, (I$ `as` $Pat') = [\overline{\alpha} \mapsto \overline{\tau}]\Gamma' \cup \{(I, [\overline{\alpha} \mapsto \overline{\tau}]\tau')\}, [\overline{\alpha} \mapsto \overline{\tau}]\tau')$. Since $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma' \cup \{(I, [\overline{\alpha} \mapsto \overline{\tau}]\tau')\}$ is equivalent to $[\overline{\alpha} \mapsto \overline{\tau}](\Gamma' \cup \{(I, \tau')\})$, the result follows.
- Case T-MATCHTUP. Then $\tau = \tau_1 * \cdots * \tau_k$ and Pat has the form $(Pat_1, \ldots, Pat_k)$ and $\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_k$ and $\tau' = \tau_1' * \cdots * \tau_k'$ and for all $1 \leq i \leq k$ we have matchType$(\tau_i, Pat_i) = (\Gamma_i, \tau_i')$. By induction, for all $1 \leq i \leq k$ we have matchType$([\overline{\alpha} \mapsto \overline{\tau}]\tau_i, Pat_i) = ([\overline{\alpha} \mapsto \overline{\tau}]\Gamma_i, [\overline{\alpha} \mapsto \overline{\tau}]\tau_i')$. Therefore, the result follows by T-MATCHTUP.
- Case T-MATCHCLASS. Then Pat has the form $C\ \{\overline{V} = \overline{Pat}\}$ and $\tau = (\overline{\tau_1}\ C')$ and $\tau' = (\overline{\tau_1}\ C)$ and $\Gamma = \bigcup \overline{\Gamma}$ and $C \leq C'$ and repType$(\overline{\tau_1}\ C) = \{\overline{V} : \overline{\tau}\}$ and matchType$(\overline{\tau}, \overline{Pat}) = (\overline{\Gamma}, \overline{\tau'})$. By Lemma A.11 we have repType$([\overline{\alpha} \mapsto \overline{\tau}](\overline{\tau_1}\ C)) = [\overline{\alpha} \mapsto \overline{\tau}]\{\overline{V} : \overline{\tau}\}$. By induction we have matchType$([\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau}, \overline{Pat}) = ([\overline{\alpha} \mapsto \overline{\tau}]\overline{\Gamma}, [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau'})$. Therefore the result follows by T-MATCHCLASS.

□

A.4 Type Preservation

Lemma A.18 If $\vdash v : \tau''$ and $\tau'' \leq \tau$ and match$(v, Pat) = \rho$ and matchType$(\tau, Pat) = (\Gamma, \tau')$, then (1) $\tau'' \leq \tau'$; and (2) dom$(\Gamma) =$ dom(ρ) and for each $(I_0, \tau_0) \in \Gamma$, there exists $(I_0, v_0) \in \rho$ such that $\vdash v_0 : \tau_0'$, for some τ_0' such that $\tau_0' \leq \tau_0$.
Proof By (strong) induction on the length of the derivation of match$(v, Pat) = \rho$. Case analysis of the last rule used in the derivation:

- Case E-MATCHWILD. Then Pat has the form _ and $\rho = \{\}$. By T-MATCHWILD we have $\Gamma = \{\}$ and $\tau' = \tau$. Therefore, condition 1 follows from the assumption that $\tau'' \leq \tau$, and condition 2 holds vacuously.
- Case E-MATCHBIND. Then Pat has the form I `as` Pat' and $\rho = \rho' \cup \{(I, v)\}$ and match$(v, Pat') = \rho'$. By T-MATCHBIND we have $\Gamma = \Gamma' \cup \{(I, \tau')\}$ and matchType$(\tau, Pat') = (\Gamma', \tau')$. By induction we have that $\tau'' \leq \tau'$ and dom$(\Gamma') =$ dom(ρ') and for each $(I_0, \tau_0) \in \Gamma'$, there exists $(I_0, v_0) \in \rho'$ such that $\vdash v_0 : \tau_0'$, where $\tau_0' \leq \tau_0$. Therefore, we have $\tau'' \leq \tau'$ and dom$(\Gamma' \cup \{(I, \tau')\}) =$ dom$(\rho' \cup \{(I, v)\})$ and for each $(I_0, \tau_0) \in \Gamma' \cup \{(I, \tau')\}$, there exists $(I_0, v_0) \in \rho' \cup \{(I, v)\}$ such that $\vdash v_0 : \tau_0'$, where $\tau_0' \leq \tau_0$.
- Case E-MATCHTUP. Then $v = (v_1, \ldots, v_k)$ and Pat has the form $(Pat_1, \ldots, Pat_k)$ and $\rho = \rho_1 \cup \cdots \cup \rho_k$ and for all $1 \leq i \leq k$ we have match$(v_i, Pat_i) = \rho_i$. By T-MATCHTUP we have $\tau = \tau_1 * \cdots * \tau_k$ and $\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_k$ and $\tau' = \tau_1' \cdots * \tau_k'$ and for all $1 \leq i \leq k$ we have match$(\tau_i, Pat_i) = (\Gamma_i, \tau_i')$.

  Since we're given that $\vdash v : \tau''$, by T-TUP we have that $\tau'' = \tau_1'' * \cdots * \tau_k''$ and for all $1 \leq i \leq k$ we have $\vdash v_i : \tau_i''$. Since we're given that $\tau'' \leq \tau$, by Lemma A.6 we have $\tau_i'' \leq \tau_i$ for all $1 \leq i \leq k$. Then by induction, for all $1 \leq i \leq k$ we have $\tau_i'' \leq \tau_i'$. Then by SUBTTUP we have $\tau_1'' * \cdots * \tau_k'' \leq \tau_1' * \ldots * \tau_k'$, proving condition 1. Also by induction, dom$(\Gamma_i) =$ dom(ρ_i) and for each $(I_0, \tau_0) \in \Gamma_i$, there exists $(I_0, v_0) \in \rho_i$ such that $\vdash v_0 : \tau_0'$, where $\tau_0' \leq \tau_0$, so condition 2 follows.
- Case E-MATCHCLASS. Then $v = ((\overline{\tau}\ C)\ \{\overline{V_1} = \overline{v_1}, \overline{V_2} = \overline{v_2}\})$ and Pat has the form $(C'\ \{\overline{V_1} = \overline{Pat_1})$ and $C \leq C'$ and $\rho = \bigcup \overline{\rho_1}$ and match$(\overline{v_1}, \overline{Pat_1}) = \overline{\rho_1}$. By T-MATCHCLASS we have $\tau = (\overline{\tau'}\ C'')$ and $\tau' = (\overline{\tau'}\ C')$ and $\Gamma = \bigcup \overline{\Gamma_1}$ and $C' \leq C''$ and repType$(\overline{\tau'}\ C') = \{\overline{V_1} : \overline{\tau_1}\}$ and matchType$(\overline{\tau_1}, \overline{Pat_1}) = (\overline{\Gamma_1}, \overline{\tau_1'})$.

  Since $\vdash v : \tau''$ and $v = ((\overline{\tau}\ C)\ \{\overline{V_1} = \overline{v_1}, \overline{V_2} = \overline{v_2}\})$, by T-REP we have that $\tau'' = (\overline{\tau}\ C)$ and $\bullet \vdash (\overline{\tau}\ C)$ OK and and repType$(\overline{\tau}\ C) = \{\overline{V_1} : \overline{\tau_1''}, \overline{V_2} : \overline{\tau_2''}\}$ and $\vdash \overline{v_1} : \overline{\tau_1'''}$ and $\overline{\tau_1'''} \leq \overline{\tau_1''}$. Since $\tau'' \leq \tau$, we have $(\overline{\tau}\ C) \leq (\overline{\tau_1}\ C'')$, so by Lemma A.4 we have $\overline{\tau} = \overline{\tau_1}$. Since $C \leq C'$ and $\bullet \vdash (\overline{\tau}\ C)$ OK, by Lemma A.7 we have $(\overline{\tau}\ C) \leq (\overline{\tau}\ C')$, and since $\overline{\tau} = \overline{\tau_1}$, condition 1 is shown. By Lemma A.12 we have $\overline{\tau_1''} = \overline{\tau_1}$. Therefore $\vdash \overline{v_1} : \overline{\tau_1'''}$ and $\overline{\tau_1'''} \leq \overline{\tau_1}$ and match$(\overline{v_1}, \overline{Pat_1}) = \overline{\rho_1}$ and matchType$(\overline{\tau_1}, \overline{Pat_1}) = (\overline{\Gamma_1}, \overline{\tau_1'})$, so by induction we have that $\overline{\tau_1'''} \leq \overline{\tau_1'}$ and dom$(\bigcup \overline{\Gamma_1}) =$ dom$(\bigcup \overline{\rho_1})$ and for each $(I_0, \tau_0) \in \bigcup \overline{\Gamma_1}$, there exists $(I_0, v_0) \in \bigcup \overline{\rho_1}$ such that $\vdash v_0 : \tau_0'$, where $\tau_0' \leq \tau_0$.

□

Lemma A.19 (Substitution) If $\Gamma,\overline{\alpha_0} \vdash E : \tau$ and $\Gamma = \{(\overline{I_0},\overline{\tau_0})\}$ and $\Gamma_0;\overline{\alpha_0} \vdash \overline{E_0} : \overline{\tau_0}'$ and $\overline{\tau_0'} \leq \overline{\tau_0}$, then $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]E : \tau'$, for some τ' such that $\tau' \leq \tau$.

Proof By (strong) induction on the depth of the derivation of $\Gamma,\overline{\alpha_0} \vdash E : \tau$. Case analysis of the last rule used in the derivation.

- Case T-ID. Then $E = I$ and $(I,\tau) \in \Gamma$, so $I = I_j$ and $\tau = \tau_j$, for some $1 \leq j \leq k$, where $\overline{I_0} = I_1,\ldots,I_k$ and $\overline{\tau_0} = \tau_1,\ldots,\tau_k$ and $\overline{E_0} = E_1,\ldots,E_k$. Therefore $[\overline{I_0} \mapsto \overline{E_0}]E = E_j$. Since we're given that $\Gamma_0;\overline{\alpha_0} \vdash E_j : \tau'_j$ and $\tau'_j \leq \tau_j$, the result is shown.
- Case T-NEW. Then $E = Ct(\overline{E})$ and $\tau = Ct$ and $\overline{\alpha_0} \vdash Ct(\overline{E})$ OK and $Ct = (\overline{\tau_1}\ Sn.Cn)$ and concrete($Sn.Cn$). Then by T-SUPER we have $\overline{\alpha_0} \vdash Ct$ OK and (<abstract> class $\overline{\alpha_1}$ $Cn(\overline{I}:\overline{\tau})\ \ldots) \in ST(Sn)$ and $\Gamma;\overline{\alpha_0} \vdash \overline{E} : \overline{\tau'}$ and $\overline{\tau'} \leq [\overline{\alpha_1} \mapsto \overline{\tau_1}]\overline{\tau}$. Since $[\overline{I_0} \mapsto \overline{E_0}]Ct = Ct$ and $[\overline{I_0} \mapsto \overline{E_0}]Sn.Cn = Sn.Cn$, we have $\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]Ct$ OK and concrete($[\overline{I_0} \mapsto \overline{E_0}]Sn.Cn$). By induction we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]\overline{E} : \overline{\tau''}$ and $\overline{\tau''} \leq \overline{\tau'}$. Then by SUBTTRANS we have $\overline{\tau''} \leq [\overline{\alpha_1} \mapsto \overline{\tau_1}]\overline{\tau}'$. Therefore by T-SUPER we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]E$ OK, so by T-NEW we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]E : \tau$. By SUBTREF we have $\tau \leq \tau$, so the result is shown.
- Case T-REP. Then $E = Ct\ \{\overline{V} = \overline{E}\}$ and $\tau = Ct$ and $\overline{\alpha_0} \vdash Ct$ OK and $Ct = (\overline{\tau_1}\ Sn.Cn)$ and concrete($Sn.Cn$) and repType(Ct) = $\{\overline{V} : \overline{\tau}\}$ and $\Gamma;\overline{\alpha_0} \vdash \overline{E} : \overline{\tau'}$ and $\overline{\tau'} \leq \overline{\tau}$. Since $[\overline{I_0} \mapsto \overline{E_0}]Ct = Ct$ and $[\overline{I_0} \mapsto \overline{E_0}]Sn.Cn = Sn.Cn$, we have $\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]Ct$ OK and concrete($[\overline{I_0} \mapsto \overline{E_0}]Sn.Cn$) and and repType($[\overline{I_0} \mapsto \overline{E_0}]Ct$) = $\{\overline{V} : \overline{\tau}\}$. By induction we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]\overline{E} : \overline{\tau''}$ and $\overline{\tau''} \leq \overline{\tau'}$. Then by SUBTTRANS we have $\overline{\tau''} \leq \overline{\tau}$, so by T-Rep we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]E : \tau$. By SUBTREF we have $\tau \leq \tau$, so the result is shown.
- Case T-FUN. Then since Γ is not used at all in T-Fun and $\Gamma;\overline{\alpha_0} \vdash E : \tau$, also $\Gamma_0;\overline{\alpha_0} \vdash E : \tau$. Further, we have $E = Fv$, so $[\overline{I_0} \mapsto \overline{E_0}]E = E$. Therefore $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]E : \tau$, and by SUBTREF $\tau \leq \tau$, so the result is shown.
- Case T-TUP. Then $E = (E_1,\ldots,E_k)$ and $\tau = \tau_1 * \cdots * \tau_k$ and for all $1 \leq j \leq k$ we have $\Gamma;\overline{\alpha_0} \vdash E_j : \tau_j$. Then by induction, for all $1 \leq j \leq k$ we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]E_j : \tau'_j$ and $\tau'_j \leq \tau_j$. Then by T-TUP we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}](E_1,\ldots,E_k) : \tau'_1 * \cdots * \tau'_k$. Finally, by SUBTTUP we have $\tau'_1 * \cdots * \tau'_k \leq \tau_1 * \cdots * \tau_k$.
- Case T-APP. Then $E = E_1\ E_2$ and $\Gamma;\overline{\alpha_0} \vdash E_1 : \tau_2 \to \tau$ and $\Gamma;\overline{\alpha_0} \vdash E_2 : \tau'_2$ and $\tau'_2 \leq \tau_2$. By induction we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]E_1 : \tau_0$ and $\tau_0 \leq \tau_2 \to \tau$. Also by induction we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}]E_2 : \tau''_2$ and $\tau''_2 \leq \tau'_2$. Then by SUBTTRANS we have $\tau''_2 \leq \tau_2$. By Lemma A.13 τ_0 has the form $\tau_{arg} \to \tau_{res}$, where $\tau_2 \leq \tau_{arg}$ and $\tau_{res} \leq \tau$. Therefore by SUBTTRANS we have $\tau''_2 \leq \tau_{arg}$. Therefore by T-FUN we have $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_0} \mapsto \overline{E_0}](E'_1\ E'_2) : \tau_{res}$. We saw above that $\tau_{res} \leq \tau$, so the result is shown.

□

Lemma A.20 If $\Gamma_0;\overline{\alpha_0} \vdash Ct(\overline{E})$ OK and rep($Ct(\overline{E})$) = $\{\overline{V_0} = \overline{E_0}\}$ and repType(Ct) = $\{\overline{V_0} : \overline{\tau_0}\}$, then $\Gamma_0;\overline{\alpha_0} \vdash \overline{E_0} : \overline{\tau'_0}$, for some $\overline{\tau'_0}$ such that $\overline{\tau'_0} \leq \overline{\tau_0}$.

Proof Since $\Gamma_0;\overline{\alpha_0} \vdash Ct(\overline{E})$ OK, by T-SUPER we have $\overline{\alpha_0} \vdash Ct$ OK and $Ct = (\overline{\tau}\ Sn.Cn)$ and (<abstract> class $\overline{\alpha}$ $Cn(\overline{I_1} : \overline{\tau_1})\ \ldots) \in ST(Sn)$ and $\Gamma_0;\overline{\alpha_0} \vdash \overline{E} : \overline{\tau'_1}$ and $\overline{\tau'_1} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}$. Since $\overline{\alpha_0} \vdash Ct$ OK, by CLASSTYPEOK we have $\overline{\alpha_0} \vdash \overline{\tau}$ OK and $|\overline{\tau}| = |\overline{\alpha}|$. We prove the lemma by induction on the depth of the derivation of rep($Ct(\overline{E})$) = $\{\overline{V_0} = \overline{E_0}\}$.

By REP we have (<<abstract>> class $\overline{\alpha}$ $Cn(\overline{I_1} : \overline{\tau_1})$ <extends $Ct'(\overline{E_1})$ > of $\{\overline{Vn} : \overline{\tau_2} = \overline{E_2}\}) \in ST(Sn)$ and <rep($Ct'(\overline{E_1})$) = $\{\overline{V_3} = \overline{E_3}\}$ > and $\{\overline{V_0} = \overline{E_0}\}$ is equivalent to $[\overline{I_1} \mapsto \overline{E}][\overline{\alpha} \mapsto \overline{\tau}]\{< \overline{V_3} = \overline{E_3}, > Sn.\overline{Vn} = \overline{E_2}\}$. Since repType($Ct$) = $\{\overline{V_0} : \overline{\tau_0}\}$, by REPTYPE and Lemma A.14 we have that <repType(Ct') = $\{\overline{V_3} : \overline{\tau_3}\}$ > and $\{\overline{V_0} : \overline{\tau_0}\}$ is equivalent to $[\overline{\alpha} \mapsto \overline{\tau}]\{< \overline{V_3} : \overline{\tau_3}, > Sn.\overline{Vn} : \overline{\tau_2}\}$.

Let $\Gamma = \{(\overline{I_1},\overline{\tau_1})\}$. By CLASSOK we have $< \Gamma;\overline{\alpha} \vdash Ct'(\overline{E_1})$ OK $>$. Therefore by induction we have $< \Gamma;\overline{\alpha} \vdash \overline{E_3} : \overline{\tau'_3} >$ and $< \overline{\tau'_3} \leq \overline{\tau_3} >$. Also by CLASSOK we have $\Gamma;\overline{\alpha} \vdash \overline{E_2} : \overline{\tau'_2}$ and $\overline{\tau'_2} \leq \overline{\tau_2}$. Then by Lemmas A.16 and A.15 we have $< [\overline{\alpha} \mapsto \overline{\tau}]\Gamma;\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]\overline{E_3} : [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau'_3} >$ and $< [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau'_3} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_3} >$ and $[\overline{\alpha} \mapsto \overline{\tau}]\Gamma;\overline{\alpha_0} \vdash [\overline{\alpha} \mapsto \overline{\tau}]\overline{E_2} : [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau'_2}$ and $[\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau'_2} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_2}$. Then by Lemma A.19 we have $< \Gamma_0;\overline{\alpha_0} \vdash [\overline{I_1} \mapsto \overline{E}][\overline{\alpha} \mapsto \overline{\tau}]\overline{E_3} : \overline{\tau''_3} >$ and $< \overline{\tau''_3} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau'_3} >$ and $\Gamma_0;\overline{\alpha_0} \vdash [\overline{I_1} \mapsto \overline{E}][\overline{\alpha} \mapsto \overline{\tau}]\overline{E_2} : \overline{\tau''_2}$ and $\overline{\tau''_2} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau'_2}$. By SUBTRANS we have $< \overline{\tau''_3} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_3} >$ and $\overline{\tau''_2} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_2}$. Therefore we have shown $\Gamma_0;\overline{\alpha_0} \vdash \overline{E_0} : \overline{\tau'_0}$ and $\overline{\tau'_0} \leq \overline{\tau_0}$. □

Theorem 4.1 (Type Preservation) If $\vdash E : \tau$ and $E \longrightarrow E'$ then $\vdash E' : \tau'$, for some τ' such that $\tau' \leq \tau$.

Proof By (strong) induction on the depth of the derivation of $E \longrightarrow E'$. Case analysis of the last rule used in the derivation.

- Case E-NEW. Then E has the form $Ct(\overline{E})$ and E' has the form $Ct\ \{\overline{V_0} = \overline{E_0}\}$ and $Ct = (\overline{\tau}\ C)$ and concrete(C) and rep($Ct(\overline{E})$) = $\{\overline{V_0} = \overline{E_0}\}$. Since $\vdash E : \tau$, by T-NEW we have $\tau = Ct$ and $\bullet \vdash Ct(\overline{E})$ OK. Then by T-SUPER we have $\bullet \vdash Ct$ OK. Therefore by Lemmas A.8 and A.14 we have repType(Ct) = $\{\overline{V_0} : \overline{\tau_0}\}$. So we have $\vdash Ct(\overline{E})$ OK and rep($Ct(\overline{E})$) = $\{\overline{V_0} = \overline{E_0}\}$ and repType(Ct) = $\{\overline{V_0} : \overline{\tau_0}\}$, so by Lemma A.20 we have $\vdash \overline{E_0} : \overline{\tau'_0}$ and $\overline{\tau'_0} \leq \overline{\tau_0}$. Then by T-REP we have $\vdash Ct\ \{\overline{V_0} = \overline{E_0}\} : Ct$, and by SUBTREF we have $Ct \leq Ct$.
- Case E-REP. Then E has the form $Ct\ \{\overline{V_0} = \overline{v_0}, V_0 = E_0, \overline{V_1} = \overline{E_1}\}$ and E' has the form $Ct\ \{\overline{V_0} = \overline{v_0}, V_0 = E'_0, \overline{V_1} = \overline{E_1}\}$ and $E_0 \longrightarrow E'_0$. Since $\vdash E : \tau$, by T-REP we have $\tau = Ct$ and $\bullet \vdash Ct$ OK and repType(Ct) = $\{\overline{V_0} : \overline{\tau_0}, V_0 : \tau_0, \overline{V_1} : \overline{\tau_1}\}$ and $\vdash \overline{v_0} : \overline{\tau'_0}$ and $\overline{\tau'_0} \leq \overline{\tau_0}$ and $\vdash E_0 : \tau'_0$ and $\tau'_0 \leq \tau_0$ and $\vdash \overline{E_1} : \overline{\tau'_1}$ and $\overline{\tau'_1} \leq \overline{\tau_1}$. By induction we have $\vdash E'_0 : \tau''_0$, for some τ''_0 such that $\tau''_0 \leq \tau'_0$. Therefore by SUBTTRANS we have that $\tau''_0 \leq \tau_0$. Then by T-REP we have $\vdash Ct\ \{\overline{V_0} = \overline{v_0}, V_0 = E'_0, \overline{V_1} = \overline{E_1}\} : Ct$, and by SUBTREF we have $Ct \leq Ct$.

- Case E-TUP. Then E has the form $(v_1,\ldots,v_{i-1},E_i,\ldots,E_k)$ and E' has the form $(v_1,\ldots,v_{i-1},E'_i,E_{i+1},\ldots,E_k)$ and $E_i \longrightarrow E'_i$, where $1 \le i \le k$. Since $\vdash E : \tau$, by T-TUP we have that τ has the form $\tau_1 * \cdots * \tau_k$ and $\vdash v_j : \tau_j$ for all $1 \le j < i$ and $\vdash E_j : \tau_j$ for all $i \le j \le k$. Therefore by induction we have $\vdash E'_i : \tau'_i$ for some τ'_i such that $\tau'_i \le \tau_i$. Then by T-TUP we have $\vdash (v_1,\ldots,v_{i-1},E'_i,E_{i+1},\ldots,E_k) : \tau_1 * \cdots * \tau_{i-1} * \tau'_i * \tau_{i+1} * \cdots * \tau_k$. Finally, by SUBTREF we have that $\tau_j \le \tau_j$ for all $1 \le j \le k$, so by SUBTTUP we have $\tau_1 * \cdots * \tau_{i-1} * \tau'_i * \tau_{i+1} * \cdots * \tau_k \le \tau_1 * \cdots * \tau_k$.
- Case E-APP1. Then E has the form $E_1\ E_2$ and E' has the form $E'_1\ E_2$ and $E_1 \longrightarrow E'_1$. Since $\vdash E : \tau$, by (T-App) we have $\vdash E_1 : \tau_2 \to \tau$ and $\vdash E_2 : \tau'_2$ and $\tau'_2 \le \tau_2$. Therefore by induction we have $\vdash E'_1 : \tau'$, for some τ' such that $\tau' \le \tau_2 \to \tau$. By Lemma A.13 τ' has the form $\tau''_2 \to \tau''$, where $\tau_2 \le \tau''_2$ and $\tau'' \le \tau$. Therefore by SUBTTRANS we have $\tau'_2 \le \tau''_2$, so by T-APP we have $\vdash E'_1\ E_2 : \tau''$, where $\tau'' \le \tau$.
- Case E-APP2. Then E has the form $v_1\ E_2$ and E' has the form $v_1\ E'_2$ and $E_2 \longrightarrow E'_2$. Since $\vdash E : \tau$, by T-APP we have $\vdash v_1 : \tau_2 \to \tau$ and $\vdash E_2 : \tau'_2$ and $\tau'_2 \le \tau_2$. Therefore by induction we have $\vdash E'_2 : \tau''_2$, for some τ''_2 such that $\tau''_2 \le \tau'_2$. By SUBTTRANS we have $\tau''_2 \le \tau_2$, so by T-APP we have $\vdash v_1\ E'_2 : \tau$, and by SUBTREF we have $\tau \le \tau$.
- Case E-APPRED. Then $E = (\overline{\tau}\ F)\ v$ and $E' = [\overline{I_0} \mapsto \overline{v_0}]E_0$ and most-specific-case-for$((\overline{\tau}\ F), v)$ = $(\{(\overline{I_0},\overline{v_0})\}, E_0)$. Since $\vdash E : \tau$, by T-APP we have $\vdash (\overline{\tau}\ F) : \tau_2 \to \tau$ and $\vdash v : \tau'_2$ and $\tau'_2 \le \tau_2$. Then by T-FUN we have and $F = Sn.Fn$ and $\tau_2 \to \tau = [\overline{\alpha} \mapsto \overline{\tau}](\hat{Mt} \to \tau_0)$ and $(\texttt{fun}\ \overline{\alpha}\ Fn : Mt \to \tau_0) \in ST(Sn)$ and $\bullet \vdash \overline{\tau}$ OK. Therefore we have $\tau_2 = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}$ and $\tau = [\overline{\alpha} \mapsto \overline{\tau}]\tau_0$. By LOOKUP we have $E_0 = [\overline{\alpha_0} \mapsto \overline{\tau}]E'_0$ and $(\texttt{extend fun}_{Mn}\ \overline{\alpha_0}\ F\ Pat = E'_0) \in ST(Sn')$ and match$(v, Pat) = \{(\overline{I_0},\overline{v_0})\}$. Then by CASEOK we have $\overline{\alpha_0} \vdash$ matchType$([\overline{\alpha} \mapsto \overline{\alpha_0}]\hat{Mt}, Pat)$ = (Γ, τ'') and $\Gamma; \overline{\alpha_0} \vdash E'_0 : \tau'_0$ and $\tau'_0 \le [\overline{\alpha} \mapsto \overline{\alpha_0}]\tau_0$.

  By Lemma A.16 we have $[\overline{\alpha_0} \mapsto \overline{\tau}]\Gamma; \bullet \vdash [\overline{\alpha_0} \mapsto \overline{\tau}]E'_0 : [\overline{\alpha_0} \mapsto \overline{\tau}]\tau'_0$. By Lemma A.15 we have $[\overline{\alpha_0} \mapsto \overline{\tau}]\tau'_0 \le [\overline{\alpha_0} \mapsto \overline{\tau}][\overline{\alpha} \mapsto \overline{\alpha_0}]\tau_0$. By FUNOK we have $\overline{\alpha} \vdash \tau_0$ OK, so by Lemma A.1 all type variables in τ_0 are in $\overline{\alpha}$. Therefore $[\overline{\alpha_0} \mapsto \overline{\tau}][\overline{\alpha} \mapsto \overline{\alpha_0}]\tau_0$ is equivalent to $[\overline{\alpha} \mapsto \overline{\tau}]\tau_0 = \tau$, so we have $[\overline{\alpha_0} \mapsto \overline{\tau}]\tau'_0 \le \tau$.

  By Lemma A.17 we have $\bullet \vdash$ matchType$([\overline{\alpha_0} \mapsto \overline{\tau}][\overline{\alpha} \mapsto \overline{\alpha_0}]\hat{Mt}, Pat)$ = $([\overline{\alpha_0} \mapsto \overline{\tau}]\Gamma, [\overline{\alpha_0} \mapsto \overline{\tau}]\tau'')$. By FUNOK we have $\overline{\alpha} \vdash \hat{Mt}$ OK, so by Lemma A.1 all type variables in $\hat{Mt}$ are in $\overline{\alpha}$. Therefore $[\overline{\alpha_0} \mapsto \overline{\tau}][\overline{\alpha} \mapsto \overline{\alpha_0}]\hat{Mt}$ is equivalent to $[\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt} = \tau_2$, so we have $\bullet \vdash$ matchType(τ_2, Pat) = $([\overline{\alpha_0} \mapsto \overline{\tau}]\Gamma, [\overline{\alpha_0} \mapsto \overline{\tau}]\tau'')$.

  By Lemma A.18 we have $\tau'_2 \le [\overline{\alpha_0} \mapsto \overline{\tau}]\tau''$ and dom$([\overline{\alpha_0} \mapsto \overline{\tau}]\Gamma)$ = dom$(\{(\overline{I_0},\overline{v_0})\})$ and for each $(I_x, \tau_x) \in [\overline{\alpha_0} \mapsto \overline{\tau}]\Gamma$, there exists $(I_x, v_x) \in \{(\overline{I_0},\overline{v_0})\}$ such that $\vdash v_x : \tau'_x$, where $\tau'_x \le \tau_x$. Then by Lemma A.19 we have $\vdash [\overline{I_0} \mapsto \overline{v_0}][\overline{\alpha_0} \mapsto \overline{\tau}]E'_0 : \tau_{sub}$ and $\tau_{sub} \le [\overline{\alpha_0} \mapsto \overline{\tau}]\tau'_0$. We saw above that $[\overline{\alpha_0} \mapsto \overline{\tau}]\tau'_0 \le \tau$, so by SUBTTRANS we have $\tau_{sub} \le \tau$. Therefore we have shown $\vdash E' : \tau_{sub}$ and $\tau_{sub} \le \tau$.

□

B Progress

B.1 Preliminaries and Simple Lemmas

We say that $S \subseteq S'$, where S is either a set or a sequence and similarly for S', if for every element e such that $e \in S$, also $e \in S'$. The notation $Pat < Pat'$ is shorthand for $(Pat \le Pat' \wedge Pat' \not\le pat)$.

The proof makes use of the following notion of the *owner* of a value:

$\boxed{\text{owner}(Mt, v) = C}$

$$\frac{\text{owner}(Mt, v_i) = C}{\text{owner}(\tau_1 * \cdots * \tau_{i-1} * Mt * \tau_{i+1} * \cdots * \tau_k, (v_1,\ldots,v_k)) = C}\ \text{OWNERTUPVAL}$$

$$\frac{}{\text{owner}(\#Ct, (\overline{\tau}\ C)\ \{\overline{V} = \overline{v}\}) = C}\ \text{OWNERINSTANCE}$$

There are several lemmas:

Lemma B.1 If $\tau \le (\overline{\tau}\ C)$, then τ has the form $(\overline{\tau_1}\ C')$.
Proof By (strong) induction on the depth of the derivation of $\tau \le (\overline{\tau}\ C)$. Case analysis of the last rule used in the derivation.

- Case SUBTREF. Then $\tau = (\overline{\tau}\ C)$.
- Case SUBTTRANS. Then $\tau \le \tau'$ and $\tau' \le (\overline{\tau}\ C)$. By induction τ' has the form $(\overline{\tau_2}\ C'')$. Then by induction again, τ has the form $(\overline{\tau_1}\ C')$.
- Case SUBTEXT. Then τ has the form $(\overline{\tau_1} Sn.Cn)$, which is also of the form $(\overline{\tau_1}\ C')$.

□

Lemma B.2 If $\tau_1 \to \tau_2 \le \tau$, then τ has the form $\tau'_1 \to \tau'_2$.
Proof By (strong) induction on the depth of the derivation of $\tau_1 \to \tau_2 \le \tau$. Case analysis of the last rule used in the derivation.

- Case SUBTREF. Then $\tau = \tau_1 \to \tau_2$.
- Case SUBTTRANS. Then $\tau_1 \to \tau_2 \leq \tau'$ and $\tau' \leq \tau$. By induction τ' has the form $\tau''_1 \to \tau''_2$. Then by induction again, τ has the form $\tau'_1 \to \tau'_2$.
- Case SUBTFUN. Then τ has the form $\tau'_1 \to \tau'_2$.

□

Lemma B.3 If $\tau_1 * \cdots * \tau_k \leq \tau$, then τ has the form $\tau'_1 * \cdots * \tau'_k$, where for all $1 \leq i \leq k$ we have $\tau_i \leq \tau'_i$.
Proof By (strong) induction on the depth of the derivation of $\tau_1 * \cdots * \tau_k \leq \tau$. Case analysis of the last rule used in the derivation.

- Case SUBTREF. Then $\tau = \tau_1 * \cdots * \tau_k$. By SUBTREF, for all $1 \leq i \leq k$ we have $\tau_i \leq \tau_i$.
- Case SUBTTRANS. Then $\tau_1 * \cdots * \tau_k \leq \tau'$ and $\tau' \leq \tau$. By induction τ' has the form $\tau''_1 * \cdots * \tau''_k$, where for all $1 \leq i \leq k$ we have $\tau_i \leq \tau''_i$. Then by induction again, τ has the form $\tau'_1 * \cdots * \tau'_k$, where for all $1 \leq i \leq k$ we have $\tau''_i \leq \tau'_i$. By SUBTTRANS, for all $1 \leq i \leq k$ we have $\tau_i \leq \tau'_i$.
- Case SUBTTUP. Then τ has the form $\tau'_1 * \cdots * \tau'_k$, where for all $1 \leq i \leq k$ we have $\tau_i \leq \tau'_i$.

□

Lemma B.4 If $C_1 \leq C_2$ and $C_1 \leq C_3$, then either $C_2 \leq C_3$ or $C_3 \leq C_2$.
Proof By induction on the depth of the derivation of $C_1 \leq C_2$. Case analysis of the last rule used in the derivation.

- Case SUBREF. Then $C_1 = C_2$. Since $C_1 \leq C_3$, also $C_2 \leq C_3$.
- Case SUBTRANS. Then $C_1 \leq C_4$ and $C_4 \leq C_2$. So we have $C_1 \leq C_4$ and $C_1 \leq C_3$, and by induction either $C_4 \leq C_3$ or $C_3 \leq C_4$.
  - Case $C_4 \leq C_3$. Then we have $C_4 \leq C_2$ and $C_4 \leq C_3$, so by induction either $C_2 \leq C_3$ or $C_3 \leq C_2$.
  - Case $C_3 \leq C_4$. Then we have $C_3 \leq C_4$ and $C_4 \leq C_2$, so by SUBTRANS $C_3 \leq C_2$.
- Case SUBEXT. Then $C_1 = Sn_1.Cn_1$ and (<`abstract`> `class` $\overline{\alpha}$ $Cn_1(\overline{I_0} : \overline{\tau_0})$ `extends` $\overline{\tau}\, C_2\, \ldots) \in ST(Sn_1)$. Case analysis of the last rule used in the derivation of $C_1 \leq C_3$.
  - Case SUBREF. Then $C_1 = C_3$. Since $C_1 \leq C_2$, also $C_3 \leq C_2$.
  - Case SUBTRANS. Then $C_1 \leq C_4$ and $C_4 \leq C_3$. Assume WLOG that the derivation of $C_1 \leq C_4$ ends with a use of SUBEXT. Then (<`abstract`> `class` $\overline{\alpha}$ $Cn_1(\overline{I_0} : \overline{\tau_0})$ `extends` $\overline{\tau}\, C_4\, \ldots) \in ST(Sn_1)$, so $C_2 = C_4$. Since $C_4 \leq C_3$, also $C_2 \leq C_3$.
  - Case SUBEXT. Then (<`abstract`> `class` $\overline{\alpha}$ $Cn_1(\overline{I_0} : \overline{\tau_0})$ `extends` $\overline{\tau}\, C_3\, \ldots) \in ST(Sn_1)$, so $C_2 = C_3$. Then by SubRef $C_2 \leq C_3$.

□

Lemma B.5 If $C_1 \leq C_2$, then there is a path in the declared inheritance graph from C_1 to C_2.
Proof By induction on the depth of the derivation of $C_1 \leq C_2$. Case analysis of the last rule used in the derivation.

- Case SUBREF. Then $C_1 = C_2$, so there is a trivial path in the inheritance graph from C_1 to C_2.
- Case SUBTRANS. Then $C_1 \leq C_3$ and $C_3 \leq C_2$. By induction, there is a path in the inheritance graph from C_1 to C_3 and from C_3 to C_2, so the concatenation of these paths is a path from C_1 to C_2.
- Case SUBEXT. Then $C_1 = Sn_1.Cn_1$ and <`abstract`> `class` $\overline{\alpha_1}$ $Cn_1(\overline{I_0} : \overline{\tau_0})$ `extends` $\overline{\tau}\, C_2\, \ldots) \in ST(Sn_1)$. Therefore there is an edge from C_1 to C_2 in the declared inheritance graph, so there is also a path from C_1 to C_2.

□

Lemma B.6 If $C_1 \leq C_2$ and $C_2 \leq C_1$, then $C_1 = C_2$.
Proof By Lemma B.5, there is a path in the declared inheritance graph from C_1 to C_2 and a path from C_2 to C_1. By assumption, the declared inheritance graph is acyclic, so it must be the case that $C_1 = C_2$. □

Lemma B.7 If match(v, Pat) = ρ and $Pat \leq Pat'$, then there exists ρ' such that match(v, Pat') = ρ'.
Proof By induction on the depth of the derivation of $Pat \leq Pat'$. Case analysis of the last rule used in the derivation:

- Case SPECWILD. Then Pat' has the form _, so by E-MATCHWILD we have match$(v, _)$ = $\{\}$.
- Case SPECBIND1.: Then Pat has the form (I `as` Pat_1) and we have $Pat_1 \leq Pat'$. Since we're given that match(v, I `as` Pat_1) = ρ, by E-MATCHBIND we also have that match(v, Pat_1) = $\rho - \{(I, v)\}$. Therefore by induction there exists ρ' such that match(v, Pat') = ρ'.

- Case SPECBIND2.: Then Pat' has the form (I `as` Pat_2) and we have $Pat \leq Pat_2$. Therefore by induction we have that there exists ρ'' such that match(v, Pat_2) = ρ''. Then by E-MATCHBIND we have match(v, I `as` Pat_2) = $\rho'' \cup \{I, v\}$.

- Case SPECTUP. Then Pat has the form $(\overline{Pat})$ and Pat' has the form $(\overline{Pat'})$ and $\overline{Pat} \leq \overline{Pat'}$. Since we're given that match($v, (\overline{Pat})$) = ρ, by E-MATCHTUP we have that $v = (\overline{v})$ and match($\overline{v}, \overline{Pat}$) = $\overline{\rho}$. Therefore by induction we have match($\overline{v}, \overline{Pat'}$) = $\overline{\rho'}$. Then by E-MATCHTUP we have match($(\overline{v}), (\overline{Pat})$) = $\bigcup \overline{\rho'}$.

- Case SPECCLASS. Then Pat has the form $(C_1\ \{\overline{V} = \overline{Pat_1}, \overline{V_3} = \overline{Pat_3}\})$ and Pat' has the form $(C_2\ \{\overline{V} = \overline{Pat_2}\})$ and $C_1 \leq C_2$ and $\overline{Pat_1} \leq \overline{pat_2}$. Since we're given that match(v,$C_1\ \{\overline{V} = \overline{Pat_1}, \overline{V_3} = \overline{Pat_3}\}$) = ρ, by E-MATCHCLASS we have that $v = ((\overline{\tau}\, C_0)\ \{\overline{V} = \overline{v}, \overline{V_3} = \overline{v_3}, \overline{V_4} = \overline{v_4}\})$ and $C_0 \leq C_1$ and match($\overline{v}$, $\overline{Pat_1}$) = $\overline{\rho_1}$. Since $C_0 \leq C_1$ and $C_1 \leq C_2$, by SUBTRANS we have $C_0 \leq C_2$. By induction we have match($\overline{v}$, $\overline{Pat_2}$) = $\overline{\rho_2}$. Therefore by E-MATCHCLASS we have match($(\overline{\tau}\, C_0)\ \{\overline{V} = \overline{v}, \overline{V_3} = \overline{v_3}, \overline{V_4} = \overline{v_4}\}), C_2\ \{\overline{V} = \overline{Pat_2}\}$) = $\bigcup \overline{\rho_2}$.

□

Lemma B.8 If $\overline{Sn} \vdash C$ transDependedUpon and $C \leq Sn'.Cn'$, then $Sn' \in \overline{Sn}$.
Proof By induction on the depth of the derivation of $C \leq Sn'.Cn'$. Case analysis of the last rule in the derivation.

- Case SUBREF. Then $C = Sn'.Cn'$. Since we're given that $\overline{Sn} \vdash C$ transDependedUpon, by CLASSTRANSDEP we have $Sn' \in \overline{Sn}$.

- Case SUBTRANS. Then $C \leq Sn''.Cn''$ and $Sn''.Cn'' \leq Sn'.Cn'$. Assume WLOG that the derivation of $C \leq Sn''.Cn''$ ends with a use of SUBEXT. Let $C = Sn.Cn$. Therefore by SUBEXT we have (<`abstract`> `class` $\overline{\alpha}\ Cn(\overline{I_0} : \overline{\tau_0})$ `extends` $\overline{\tau_2}\ Sn''.Cn''$ $\ldots) \in ST(Sn)$. Since we're given that $\overline{Sn} \vdash C$ transDependedUpon, by CLASSTRANSDEP we have $\overline{Sn} \vdash Sn''.Cn''$ transDependedUpon. In addition, we showed above that $Sn''.Cn'' \leq Sn'.Cn'$, so by induction we have $Sn' \in \overline{Sn}$.

- Case SUBEXT. Then (<`abstract`> `class` $\overline{\alpha}$ $Cn(\overline{I_0} : \overline{\tau_0})$ `extends` $\overline{\tau_1}\ Sn'.Cn'\ \ldots) \in ST(Sn)$. Since we're given that $\overline{Sn} \vdash C$ transDependedUpon, by CLASSTRANSDEP we have $\overline{Sn} \vdash Sn'.Cn'$ transDependedUpon. Therefore by CLASSTRANSDEP we have $Sn' \in \overline{Sn}$.

□

Lemma B.9 If $\overline{\alpha} \vdash Ct$ OK and $Ct = (\overline{\tau}\, Sn.Cn)$ and (<`abstract`> `class` $\overline{\alpha_0}$ $Cn(\overline{I_0} : \overline{\tau_0})\ \ldots) \in ST(Sn)$ and $|\overline{E_0}| = |\overline{I_0}|$ then rep($Ct(\overline{E_0})$) is well-defined and has the form $\{\overline{V} = \overline{E}\}$.
Proof We prove this lemma by induction on the length of the longest path in the superclass graph from $Sn.Cn$ (in other words, the number of non-trivial superclasses of $Sn.Cn$). By CLASSTYPEOK we have $\overline{\alpha} \vdash \overline{\tau}$ OK and (<<`abstract`>> `class` $\overline{\alpha_0}$ $Cn(\overline{I_0} : \overline{\tau_0})$ <`extends` $Ct'(\overline{E'})$ > `of` $\overline{Vn} : \overline{\tau_2} = \overline{E_2}\}) \in ST(Sn)$ and $|\overline{\alpha_0}| = |\overline{\tau}|$. There are two cases to consider.

- The length of the longest path in the superclass graph from $Sn.Cn$ is 0. Then $Sn.Cn$ has no non-trivial superclasses, so the `extends` clause in the declaration of $Sn.Cn$ is absent. Then by REP we have that rep($Ct(\overline{E_0})$) is well-defined and has the form $\{\overline{V} = \overline{E}\}$.

- The length of the longest path in the superclass graph from $Sn.Cn$ is $i > 0$. Then $Sn.Cn$ has at least one non-trivial superclass, so the `extends` clause in the declaration of $Sn.Cn$ is present. Then by CLASSOK we have $\overline{\alpha_0} \vdash Ct'(\overline{E'})$ OK, so by T-SUPER we have $\overline{\alpha_0} \vdash Ct'$ OK and $Ct' = (\overline{\alpha_1}\ Sn'.Cn')$ and (<`abstract`> `class` $\overline{\alpha_0}$ $Cn'(\overline{I'_0} : \overline{\tau'_0})\ \ldots) \in ST(Sn')$ and $|\overline{I'_0}| = |\overline{E'}|$. Since Ct' must have the form $(\overline{\tau_1}\ Sn'.Cn')$, where the length of the longest path in the superclass graph from $Sn'.Cn'$ is $i-1$, by induction we have that rep($Ct'(\overline{E'})$) is well-defined and has the form $\{\overline{V} = \overline{E}\}$. Then by REP we have that rep($Ct(\overline{E_0})$) is well-defined and also has the appropriate form.

□

B.2 Completeness

These lemmas prove that all functions are complete.

Lemma B.10 If $\vdash v : \tau'$ and $\tau' \leq \tau$ and $\tau = [\overline{\alpha} \mapsto \overline{\tau}]\tau_0$ and defaultPat(τ_0, C_0, d) = Pat, then there exists ρ such that match(v, Pat) = ρ.
Proof By strong induction on the depth of the derivation of defaultPat(τ_0, C_0, d) = Pat. Case analysis of the last rule in the derivation.

- Case DEFZERO or DEFTYPEVAR or DEFFUNTYPE. Then Pat has the form _, so by E-MATCHWILD we have match(v, _) = $\{\}$.

- Case DEFCLASSTYPE. Then τ_0 has the form $(\overline{\tau_0}\ C)$ and Pat has the form $(C\ \{\overline{V} = \overline{Pat}\})$ and repType($\overline{\tau_0}\ C$) = $\{\overline{V} : \overline{\tau}\}$ and defaultPat($\overline{\tau}, C_0, d-1$) = $\overline{Pat}$ and $d > 0$. Since $\tau = [\overline{\alpha} \mapsto \overline{\tau}]\tau_0$, by Lemma A.11 we have repType(τ) = $[\overline{\alpha} \mapsto \overline{\tau}]\{\overline{V} : \overline{\tau}\}$. Further, $\tau = [\overline{\alpha} \mapsto \overline{\tau}](\overline{\tau_0}\ C) = ([\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0}\ C)$. Since $\tau' \leq \tau$, by Lemma B.1 τ' has the form $(\overline{\tau_1}\ C')$. Since $\vdash v : \tau'$, by T-REP v has the form $(\overline{\tau_1}\ C')\ \{\overline{V_1} = \overline{v_1}\}$ and $\bullet \vdash (\overline{\tau_1}\ C')$ OK and repType($\overline{\tau_1}\ C'$) = $\{\overline{V_1} : \overline{\tau_1}\}$ and $\vdash \overline{v_1} : \overline{\tau'_1}$ and $\overline{\tau'_1} \leq \overline{\tau_1}$.

Since $(\overline{\tau_1}\ C') \leq ([\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_0}\ C)$, by Lemma A.5 we have $C' \leq C$. Further, by Lemma A.12 we have that $\{\overline{V_1} : \overline{\tau_1}\} = \{\overline{V} : [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau}, \overline{V_2} : \overline{\tau_2}\}$. Therefore there is some prefix $\overline{\tau_3}$ of $\overline{\tau_1'}$ such that $\overline{\tau_3} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau}$. Therefore there is some prefix $\overline{v_3}$ of $\overline{v_1}$ such that $\vdash \overline{v_3} : \overline{\tau_3}$ and $\overline{\tau_3} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau}$ and defaultPat($\overline{\tau}, C_0, d-1$) = $\overline{Pat}$. Therefore by induction, match($\overline{v_3}, \overline{Pat}$) = $\overline{\rho}$. Therefore by E-MATCHCLASS we have match($(\overline{\tau_1}\ C')\ \{\overline{V_1} = \overline{v_1}\}$, $(C\ \{\overline{V} = \overline{Pat}\})$) = $\bigcup\overline{\rho}$.

- Case DEFTUPTYPE. Then τ_0 has the form $\tau_1 * \cdots * \tau_k$ and Pat has the form $(Pat_1, \ldots, Pat_k)$ and for all $1 \leq i \leq k$ we have defaultPat($\tau_i, C_0, d-1$) = Pat_i and $d > 0$. Since $\tau' \leq [\overline{\alpha} \mapsto \overline{\tau}](\tau_1 * \cdots * \tau_k)$, by Lemma A.6 we have that τ' has the form $\tau_1' * \cdots * \tau_k'$, where for all $1 \leq i \leq k$ we have $\tau_i' \leq [\overline{\alpha} \mapsto \overline{\tau}]\tau_i$. Since $\vdash v : \tau'$, by T-TUP we have that v has the form $(v_1, \ldots, v_k)$ and for all $1 \leq i \leq k$ we have $\vdash v_i : \tau_i'$. Therefore by induction, for all $1 \leq i \leq k$ we have that there exists some ρ_i such that match(v_i, Pat_i) = ρ_i. Then by E-MATCHTUP we have match(v, Pat) = $\rho_1 \cup \cdots \cup \rho_k$.

□

Lemma B.11 If owner(Mt, v) = C_0 and $C_0 \leq C$ and $\vdash v : \tau'$ and $\tau' \leq \tau$ and $\tau = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}$ and defaultPat(Mt, C, d) = Pat, then there exists ρ such that match(v, Pat) = ρ.

Proof By strong induction on the depth of the derivation of defaultPat(Mt, C, d) = Pat. Case analysis of the last rule in the derivation.

- Case DEFZERO. Then Pat has the form _, so by E-MATCHWILD we have match(v, _) = $\{\}$.
- Case DEFOWNERCLASSTYPE. Then Mt has the form #$(\overline{\tau_1}\ C')$ and Pat has the form $(C\ \{\overline{V} = \overline{Pat}\})$ and repType($\overline{\tau_1}\ C$) = $\{\overline{V} : \overline{\tau}\}$ and defaultPat($\overline{\tau}, C, d-1$) = $\overline{Pat}$ and $d > 0$. By Lemma A.11 we have repType($[\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}\ C$) = $[\overline{\alpha} \mapsto \overline{\tau}]\{\overline{V} : \overline{\tau}\}$. Since owner(#$(\overline{\tau_1}\ C'), v$) = C_0, by OWNERINSTANCE we have that v is of the form $(\overline{\tau_0}\ C_0)\ \{\overline{V_1} = \overline{v_1}\}$.

  Since we're given that $\vdash v : \tau'$, by T-REP we have that $\tau' = (\overline{\tau_0}\ C_0)$ and $\bullet \vdash (\overline{\tau_0}\ C_0)$ OK and repType($\overline{\tau_0}\ C_0$) = $\{\overline{V_2} : \overline{\tau_2}\}$ and $\vdash \overline{v_1} : \overline{\tau_2'}$ and $\overline{\tau_2'} \leq \overline{\tau_2}$. We're given that $\tau' \leq \tau$, so that means $(\overline{\tau_0}\ C_0) \leq ([\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}\ C')$, and by Lemma A.4 we have $\overline{\tau_0} = [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau_1}$. Since $C_0 \leq C$ and $\bullet \vdash (\overline{\tau_0}\ C_0)$ OK, by Lemma A.7 we have $(\overline{\tau_0}\ C_0) \leq (\overline{\tau_0}\ C)$. Therefore by Lemma A.12 we have $\{\overline{V_2} : \overline{\tau_2}\} = \{\overline{V} : [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau}, \overline{V_3} : \overline{\tau_3}\}$.

  Therefore there is some prefix $\overline{v_3}$ of $\overline{v_1}$ and some prefix $\overline{\tau_3}$ of $\overline{\tau_2'}$ such that $\vdash \overline{v_3} : \overline{\tau_3}$ and $\overline{\tau_3} \leq [\overline{\alpha} \mapsto \overline{\tau}]\overline{\tau}$ and defaultPat($\overline{\tau}, C, d-1$) = $\overline{Pat}$, so by Lemma B.10, there exists $\overline{\rho}$ such that match($\overline{v_3}, \overline{Pat}$) = $\bigcup\overline{\rho}$. Finally, we're given $C_0 \leq C$, so by E-MATCHCLASS we have match($(\overline{\tau_0}\ C_0)\ \{\overline{V_1} = \overline{v_1}\}$, $(C\ \{\overline{V} = \overline{Pat}\})$) = $\bigcup\overline{\rho}$.
- Case DEFTUPTYPE. Then Mt has the form $\tau_1 * \cdots * \tau_{i-1} * Mt_i * \tau_{i+1} * \cdots * \tau_k$ and Pat has the form $(Pat_1, \ldots, Pat_k)$ and for all $1 \leq j \leq k$ such that $j \neq i$ we have defaultPat($\tau_j, C, d-1$) = Pat_j and we have defaultPat($Mt_i, C, d-1$) = Pat_i. Let $\tau_i = \hat{Mt}_i$. Since $\tau' \leq [\overline{\alpha} \mapsto \overline{\tau}](\tau_1 * \cdots * \tau_k)$, by Lemma A.6 we have that τ' has the form $\tau_1' * \cdots * \tau_k'$, where for all $1 \leq j \leq k$ we have $\tau_j' \leq [\overline{\alpha} \mapsto \overline{\tau}]\tau_j$. Since $\vdash v : \tau'$, by T-TUP we have that v has the form $(v_1, \ldots, v_k)$ and for all $1 \leq j \leq k$ we have $\vdash v_j : \tau_j'$. Therefore by Lemma B.10, for all $1 \leq j \leq k$ such that $j \neq i$ we have that there exists some ρ_j such that match(v_j, Pat_j) = ρ_j. We're given that owner(Mt, v) = C_0, so by OWNERTUPVAL we have owner(Mt_i, v_i) = C_0. Therefore by induction we have that there exists some ρ_i such that match(v_i, Pat_i) = ρ_i. Then by E-MATCHTUP we have match(v, Pat) = $\rho_1 \cup \cdots \cup \rho_k$.

□

Lemma B.12 If $\vdash v : \tau_2'$ and $\tau_2' \leq \tau_2$ and $\tau_2 = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}$ and (`fun` $\overline{\alpha}\ Fn : Mt \to \tau_0$) $\in ST(Sn)$ and owner(Mt, v) = C_0 and $C_0 \leq C$ and $\overline{Sn} \vdash Sn.Fn$ has-default-for C, then there exists some $Sn' \in \overline{Sn}$, some (`extend fun`$_{Mn}$ $\overline{\alpha_1}\ Sn.Fn\ Pat = E$) $\in ST(Sn')$, and some environment ρ such that match(v, Pat) = ρ.

Proof Since $\overline{Sn} \vdash Sn.Fn$ has-default-for C, by DEFAULT we have defaultPat(Mt, C, d) = Pat'. Therefore we have owner(Mt, v) = C_0 and $C_0 \leq C$ and $\vdash v : \tau_2'$ and $\tau_2' \leq \tau_2$ and $\tau_2 = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}$ and defaultPat(Mt, C, d) = Pat', so by Lemma B.11 there exists ρ' such that match(v, Pat') = ρ'.

Also by DEFAULT we have (`extend fun`$_{Mn}$ $\overline{\alpha_1}\ Sn.Fn\ Pat = E$) $\in ST(Sn')$ and $Pat' \leq Pat$ and $Sn' \in \overline{Sn}$. By Lemma B.7 there exists ρ such that match(v, Pat) = ρ, so the result follows. □

Lemma B.13 If $\vdash v : \tau'$ and $\tau' \leq \tau$ and $\tau = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}$ and owner(Mt) = C', then there exists some class C such that owner(Mt, v) = C and concrete(C) and $C \leq C'$.

Proof By induction on the depth of the derivation of $\vdash v : \tau'$. Case analysis of the last rule used in the derivation.

- Case T-REP. Then v has the form $(\overline{\tau_0}\ C)\ \{\overline{V} = \overline{v}\}$ and $\tau' = (\overline{\tau_0}\ C)$ and concrete(C) and repType($\overline{\tau_0}\ C$) = $\{\overline{V} : \overline{\tau}\}$. Since $\tau' \leq \tau$, by Lemma A.3 τ has the form $(\overline{\tau_1}\ C'')$. Since $\tau = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}$, $\hat{Mt}$ has the form $(\overline{\tau_2}\ C'')$, and by the grammar for marked types Mt must be #$(\overline{\tau_2}\ C'')$. Then by OWNERINSTANCE we have owner(#$(\overline{\tau_2}\ C''), (\overline{\tau_0}\ C)\ \{\overline{V} = \overline{v}\}$) = C. We're given $\tau' \leq \tau$, so by Lemma A.5 we have $C \leq C''$. Since owner(Mt) = C', by OWNERCLASS we have $C' = C''$, so $C \leq C'$.
- Case T-FUN. Then v has the form $(\overline{\tau_1}\ F)$ and τ' has the form $\tau_1 \to \tau_2$. Therefore by Lemma B.2 τ has the form $\tau_1' \to \tau_2'$. Since $\tau = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}$, $\hat{Mt}$ has the form $\tau_1'' \to \tau_2''$, but this contradicts the grammar of marked types. Therefore, T-FUN cannot be the last rule in the derivation.
- Case T-Tup: Then v has the form $(v_1, \ldots, v_k)$ and τ' has the form $\tau_1' * \cdots * \tau_k'$ and for all $1 \leq j \leq k$ we have $\vdash v_j : \tau_j'$. Therefore by Lemma B.3 τ has the form $\tau_1 * \cdots * \tau_k$, where for all $1 \leq j \leq k$ we have $\tau_j' \leq \tau_j$. Since $\tau = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}$, $\hat{Mt}$ has the form

$\tau''_1 * \cdots * \tau''_k$, and by the grammar for marked types Mt must have the form $\tau''_1 * \cdots * \tau''_{i-1} * Mt_i * \tau''_{i+1} * \cdots * \tau''_k$, where $1 \leq i \leq k$ and $\hat{Mt}_i = \tau''_i$. We're given owner(Mt) = C', so by OWNERTUP we have owner(Mt_i) = C'.

Therefore we have $\vdash v_i : \tau'_i$ and $\tau'_i \leq \tau_i$ and $\tau_i = [\overline{\alpha} \mapsto \overline{\tau}]\hat{Mt}_i$ and owner(Mt_i) = C', so by induction there exists C such that owner(Mt_i, v_i) = C and concrete(C) and $C \leq C'$. By OWNERTUPVAL we have owner($\tau''_1 * \cdots * \tau''_{i-1} * Mt_i * \tau''_{i+1} * \cdots * \tau''_k, (v_1, \ldots, v_k)$) = C, so the result follows.

□

Lemma B.14 (Completeness) If $\vdash (\overline{\tau}\, F) : \tau_2 \to \tau$ and $\vdash v : \tau'_2$ and $\tau'_2 \leq \tau_2$, then there exists some $Sn' \in \text{dom}(ST)$, some (`extend fun`$_{Mn}$ $\overline{\alpha_1}$ F $Pat = E$) $\in ST(Sn')$, and some environment ρ such that match(v, Pat) = ρ.
Proof Since $\vdash (\overline{\tau}\, F) : \tau_2 \to \tau$, by T-FUN we have $F = Sn.Fn$ and (`fun` $\overline{\alpha}$ $Fn : Mt \to \tau_0$) $\in ST(Sn)$ and $|\overline{\alpha}| = |\overline{\tau}|$ and $\tau_2 \to \tau = [\overline{\alpha} \mapsto \overline{\tau}](\hat{Mt} \to \tau_0)$. Let $ST(Sn)$ = `structure` Sn = `struct depends upon` $\overline{Sn}$ $\overline{Ood}$ `end`. Then by STRUCTOK we have $\overline{Sn} \vdash$ (`fun` $\overline{\alpha}$ $Fn : Mt \to \tau_0$) OK in Sn, so by FUNOK we have that owner(Mt) = $Sn''.Cn$. Then by Lemma B.13 there exists some class C such that owner(Mt, v) = C and concrete(C) and $C \leq Sn''.Cn$. Also by FUNOK we have either $\overline{Sn} \vdash F$ has-gdefault or $Sn = Sn''$. We consider these cases separately.

- Case $\overline{Sn} \vdash F$ has-gdefault. By GDEFAULT we have owner(F) = C' and $\overline{Sn} \vdash F$ has-default-for C'. By OWNERFUN, $C' = Sn''.Cn$. Then by Lemma B.12 there exists some $Sn' \in \overline{Sn}$, some (`extend fun`$_{Mn}$ $\overline{\alpha_1}$ F $Pat = E$) $\in ST(Sn')$, and some environment ρ such that match(v, Pat) = ρ. Since $ST(Sn)$ = `structure` Sn = `struct depends upon` $\overline{Sn}$ $\overline{Ood}$ `end`, each member of $\overline{Sn}$ is mentioned in the program, so by sanity condition 2 we have $\overline{Sn} \subseteq \text{dom}(ST)$. Therefore $Sn' \in \text{dom}(ST)$, and the result is shown.
- Case $Sn = Sn''$. Let $C = Sn_0.Cn_0$. Since concrete(C), by CONCRETE we have (`class` $\overline{\alpha_0}$ $Cn_0 \ldots$) $\in ST(Sn_0)$. Let $ST(Sn_0)$ = `structure` Sn = `struct` Sn_0 `depends upon` $\overline{Sn_0}$ $\overline{Ood_0}$ `end`. Then by STRUCTOK we have $\overline{Sn_0} \vdash$ `class` $\overline{\alpha_0}$ $Cn_0 \ldots$ OK in Sn_0, so by CLASSOK we have concrete(C) $\Rightarrow \overline{Sn_0} \vdash$ funs-have-ldefault-for C. Since we have shown that concrete(C) holds, we have $\overline{Sn_0} \vdash$ funs-have-ldefault-for C.

  Also by CLASSOK we have $\overline{Sn_0} \vdash C$ transDependedUpon. Since $C \leq Sn''.Cn$ and $Sn'' = Sn$, by Lemma B.8 we have $Sn \in \overline{Sn_0}$.

  Since $F = Sn.Fn$ and $Sn \in \overline{Sn_0}$, by FUNDEP we have $\overline{Sn_0} \vdash F$ dependedUpon. Since (`fun` $\overline{\alpha}$ $Fn : Mt \to \tau_0$) $\in ST(Sn)$ and owner(Mt) = $Sn.Cn$, by OWNERFUN we have owner(F) = $Sn.Cn$. Also, we showed above that $C \leq Sn.Cn$. Therefore, since $\overline{Sn_0} \vdash$ funs-have-ldefault-for C, by LDEFAULT we have $\overline{Sn_0} \vdash F$ has-default-for C. By SUBREF $C \leq C$, so by Lemma B.12 there exists some $Sn' \in \overline{Sn_0}$, some (`extend fun`$_{Mn}$ $\overline{\alpha_1}$ $Sn.Fn$ $Pat = E$) $\in ST(Sn')$, and some environment ρ such that match(v, Pat) = ρ. Since $ST(Sn_0)$ = `structure` Sn_0 = `struct depends upon` $\overline{Sn_0}$ $\overline{Ood_0}$ `end`, each member of $\overline{Sn_0}$ is mentioned in the program, so by sanity condition (2) we have $\overline{Sn_0} \subseteq \text{dom}(ST)$. Therefore $Sn' \in \text{dom}(ST)$, and the result is shown.

□

B.3 Ambiguity

These lemmas ensure that all functions are unambiguous.

B.3.1 Pattern Specificity and Intersection

Lemma B.15 If $Pat \leq Pat'$ and $Pat' \leq Pat''$ then $Pat \leq Pat''$.
Proof By induction on the depth of the derivation of $Pat' \leq Pat''$. Case analysis of the last rule used in the derivation.

- Case SPECWILD. Then Pat'' has the form _, and by SPECWILD we have $Pat \leq Pat''$.
- Case SPECBIND1. Then Pat' has the form (I `as` Pat'_0) and we have $Pat'_0 \leq Pat''$. We prove this case by induction on the number of consecutive uses of rule SPECBIND1 ending the derivation of $Pat \leq$ (I `as` Pat'_0). Case analysis of the last rule used in the derivation.
  - Case SPECBIND1. Then Pat has the form (I' `as` Pat_0) and $Pat_0 \leq Pat'$. By the inner induction $Pat_0 \leq Pat''$, and by SPECBIND1 $Pat \leq Pat''$.
  - Case SPECBIND2. Then $Pat \leq Pat'_0$. Since also $Pat'_0 \leq Pat''$, by the outer induction we have $Pat \leq Pat''$.
- Case SPECBIND2. Then Pat'' has the form (I `as` Pat''_0) and we have $Pat' \leq Pat''_0$. By induction $Pat \leq Pat''_0$, and by SPECBIND2 $Pat \leq Pat''$.
- Case SPECTUP. Then Pat' has the form ($\overline{Pat'}$) and Pat'' has the form ($\overline{Pat''}$) and $\overline{Pat'} \leq \overline{Pat''}$. We prove this case by induction on the number of consecutive uses of rule SPECBIND1 ending the derivation of $Pat \leq Pat'$. Case analysis of the last rule used in the derivation.

– Case SpecBind1. Then Pat has the form (I `as` Pat_0) and we have $Pat_0 \leq Pat'$. By the inner induction $Pat_0 \leq Pat''$, so by SpecBind1 $Pat \leq Pat''$.

– Case SpecTup. Then Pat has the form $(\overline{Pat})$ $\overline{Pat} \leq \overline{Pat'}$. Therefore by the outer induction, $\overline{Pat} \leq \overline{Pat''}$. Therefore by SpecTup $Pat \leq Pat''$.

- Case SpecClass. Then Pat' has the form C' $\{\overline{V_1} = \overline{Pat'_1}, \overline{V_2} = \overline{Pat'_2}\}$ and Pat'' has the form C'' $\{\overline{V_1} = \overline{Pat''_1}\}$ and $C' \leq C''$ and $\overline{Pat'_1} \leq \overline{Pat''_1}$. We prove this case by induction on the number of consecutive uses of the rule SpecBind1 ending the derivation of $Pat \leq Pat'$. Case analysis of the last rule used in the derivation.

  – Case SpecBind1. Then Pat has the form (I `as` Pat_0) and we have $Pat_0 \leq Pat'$. By the inner induction $Pat_0 \leq Pat''$, so by SpecBind1 $Pat \leq Pat''$.

  – Case SpecClass. Then Pat has the form C $\{\overline{V_1} = \overline{Pat_1}, \overline{V_2} = \overline{Pat_2}, \overline{V_3} = \overline{Pat_3}\}$ and $C \leq C'$ and $\overline{Pat_1} \leq \overline{Pat'_1}$ and $\overline{Pat_2} \leq \overline{Pat'_2}$. Since $C \leq C'$ and $C' \leq C''$, by SubTrans we have $C \leq C''$. By the outer induction we have $\overline{Pat_1} \leq \overline{Pat''_1}$. Therefore by SpecClass $Pat \leq Pat''$.

□

Lemma B.16 If owner(Mt, Pat') = C' and owner(Mt, Pat'') = C'' and $Pat' \cap Pat'' = Pat$, then either $C' \leq C''$ or $C'' \leq C'$.
Proof By induction on the depth of the derivation of $Pat' \cap Pat'' = Pat$. Case analysis of the last rule used in the derivation.

- Case PatIntWild. Then Pat' has the form _. But then it cannot be the case that owner(Mt, Pat') = C', because none of the three associated rules applies to a wildcard pattern.
- Case PatIntBind. Then Pat' has the form I `as` Pat_0 and $Pat_0 \cap Pat'' = Pat$. Since owner(Mt, Pat') = C', by OwnerBindPat we have owner(Mt, Pat_0) = C'. Therefore by induction we have that either $C' \leq C''$ or $C'' \leq C'$.
- Case PatIntTup. Then Pat' has the form $(Pat'_1, \ldots, Pat'_k)$ and Pat'' has the form $(Pat''_1, \ldots, Pat''_k)$ and for all $1 \leq j \leq k$ we have $Pat'_j \cap Pat''_j = Pat_j$. Since owner($Mt, Pat'$) = C', by OwnerTupPat we have $Mt = \tau_1 * \cdots * \tau_{i-1} * Mt_i * \tau_{i+1} * \cdots * \tau_k$ and owner(Mt_i, Pat'_i) = C'. Since owner(Mt, Pat'') = C'', by OwnerTupPat we have owner(Mt_i, Pat''_i) = C''. Therefore by induction we have that either $C' \leq C''$ or $C'' \leq C'$.
- Case PatIntClass. Then Pat' has the form $(C_1$ $\{\overline{V} = \overline{Pat'}, \overline{V_2} = \overline{Pat_2}\})$ and Pat'' has the form $(C_2$ $\{\overline{V} = \overline{Pat''}\})$ and $C_1 \leq C_2$. Since owner(Mt, Pat') = C', by OwnerClassPat $C' = C_1$. Since owner(Mt, Pat'') = C'', by OwnerClassPat $C'' = C_2$. Therefore $C' \leq C''$.
- Case PatIntRev. Then $Pat'' \cap Pat' = Pat$, so by induction we have that either $C'' \leq C'$ or $C' \leq C''$.

□

Lemma B.17 If $\vdash v : \tau$ and match(v, Pat') = ρ' and match(v, Pat'') = ρ'' and matchType(τ', Pat') = (Γ', τ'_0) and matchType(τ'', Pat'') = (Γ'', τ''_0), then there exists some Pat such that $Pat' \cap Pat'' = Pat$.
Proof By induction on the depth of the derivation of match(v, Pat') = ρ'. Case analysis of the last rule used in the derivation.

- Case E-MatchWild. Then Pat' has the form _, so by PatIntWild we have $Pat' \cap Pat'' = Pat''$.
- Case E-MatchBind. Then Pat' has the form I `as` Pat'_0 and match(v, Pat'_0) = ρ'_0, for some ρ'_0. Since matchType(τ', Pat') = (Γ', τ'_0), by T-MatchBind we have matchType(τ', Pat'_0) = (Γ'_0, τ'_0). Then by induction there exists some Pat such that $Pat'_0 \cap Pat'' = Pat$, so by PatIntBind we have $Pat' \cap Pat'' = Pat$.
- Case E-MatchTup. Then $v = (v_1, \ldots, v_k)$ and Pat' has the form $(Pat'_1, \ldots, Pat'_k)$ and for all $1 \leq i \leq k$ we have match(v_i, Pat'_i) = ρ'_i, for some ρ'_i. We prove this case by induction on the number of consecutive uses of E-MatchBind ending the derivation of match(v, Pat'') = ρ''. Case analysis of the last rule used in the derivation.

  – Case E-MatchWild. Then Pat'' has the form _, so by PatIntWild we have $Pat'' \cap Pat' = Pat'$, and by PatIntRev $Pat' \cap Pat'' = Pat'$.

  – Case E-MatchBind. Then Pat'' has the form I `as` Pat''_0 and match(v, Pat''_0) = ρ''_0, for some ρ''_0. Since matchType(τ'', Pat'') = (Γ'', τ''_0), by T-MatchBind we have matchType(τ'', Pat''_0) = (Γ''_0, τ''_0). Then by the inner induction there exists some Pat such that $Pat' \cap Pat''_0 = Pat$. Then by PatIntRev $Pat''_0 \cap Pat' = Pat$, by PatIntBind $Pat'' \cap Pat' = Pat$, and again by PatIntRev $Pat' \cap Pat'' = Pat$.

  – Case E-MatchTup. Then Pat'' has the form $(Pat''_1, \ldots, Pat''_k)$ and for all $1 \leq i \leq k$ we have match(v_i, Pat''_i) = ρ''_i, for some ρ''_i. Since $\vdash v : \tau$, by T-Tup we have $\tau = \tau_1 * \cdots * \tau_k$ and $\vdash v_i : \tau_i$ for all $1 \leq i \leq k$. Since matchType(τ', Pat') = (Γ', τ'_0) and matchType(τ'', Pat'') = (Γ'', τ''_0), by T-MatchTup we have $\tau' = \tau'_1 * \cdots * \tau'_k$ and $\tau'' = \tau''_1 * \cdots * \tau''_k$ and for all $1 \leq i \leq k$ matchType(τ'_i, Pat') = (Γ'_i, τ'''_i) and matchType(τ''_i, Pat'') = (Γ''_i, τ''''_i). Then by the outer induction, for all $1 \leq i \leq k$ there exists Pat_i such that $Pat'_i \cap Pat''_i = Pat_i$. Then by PatIntTup there exists Pat such that $Pat' \cap Pat'' = Pat$.

  – Case E-MatchClass. Then $v = ((\overline{\tau}\ C)$ $\{\overline{V} = \overline{v}\})$, contradicting our assumption that $v = (v_1, \ldots, v_k)$.

- Case E-MATCHCLASS. Then $v = ((\overline{\tau}\, C)\ \{V_1 = v_1, \ldots, V_k = v_k\})$ and Pat' has the form $(C'\ \{V_1 = Pat'_1, \ldots, V_m = Pat'_m\})$ and $C \leq C'$ and $m \leq k$ and for all $1 \leq i \leq m$ we have match(v_i, Pat'_i) = ρ'_i for some ρ'_i. We prove this case by induction on the number of consecutive uses of E-MATCHBIND ending the derivation of match(v, Pat'') = ρ''. Case analysis of the last rule used in the derivation.
  - Case E-MATCHWILD. Then Pat'' has the form _, so by PATINTWILD we have $Pat'' \cap Pat' = Pat'$, and by PATINTREV $Pat' \cap Pat'' = Pat'$.
  - Case E-MATCHBIND. Then Pat'' has the form I `as` Pat''_0 and match(v, Pat''_0) = ρ''_0, for some ρ''_0. Since matchType(τ'', Pat'') = (Γ'', τ''_0), by T-MATCHBIND we have matchType(τ'', Pat''_0) = (Γ''_0, τ''_0). Then by the inner induction there exists some Pat such that $Pat' \cap Pat''_0 = Pat$. Then by PATINTREV $Pat''_0 \cap Pat' = Pat$, by PATINTBIND $Pat'' \cap Pat' = Pat$, and again by PATINTREV $Pat' \cap Pat'' = Pat$.
  - Case E-MATCHTUP. Then $v = (\overline{v})$, contradicting our assumption that $v = ((\overline{\tau}\, C)\ \{V_1 = v_1, \ldots, V_k = v_k\})$.
  - Case E-MATCHCLASS. Then Pat'' has the form $(C''\ \{V_1 = Pat''_1, \ldots, V_p = Pat''_p\})$ and $C \leq C''$ and $p \leq k$ and for all $1 \leq i \leq p$ we have match(v_i, Pat''_i) = ρ''_i for some ρ''_i. Since $\vdash v : \tau$, by T-REP we have $\bullet \vdash (\overline{\tau}\, C)$ OK and for all $1 \leq i \leq k$ we have $\vdash v_i : \tau_i$ for some τ_i. Since $C \leq C'$ and $C \leq C''$, by Lemma A.7 we have $\bullet \vdash (\overline{\tau}\, C')$ OK and $\bullet \vdash (\overline{\tau}\, C'')$ OK. Since matchType(τ', Pat') = (Γ', τ'_0) and matchType(τ'', Pat'') = (Γ'', τ''_0), by T-MATCHCLASS we have repType($\overline{\tau_0}\, C'$) has the form $\{V_1 : \tau'_1, \ldots, V_m : \tau'_m\}$ and repType($\overline{\tau_1}\, C''$) has the form $\{V_1 : \tau''_1, \ldots, V_p : \tau''_p\}$, for some $\overline{\tau_0}$ and $\overline{\tau_1}$. Therefore by inspection of REPTYPE, also repType($\overline{\tau}\, C'$) has the form $\{V_1 : \tau'''_1, \ldots, V_m : \tau'''_m\}$ and repType($\overline{\tau}\, C''$) has the form $\{V_1 : \tau''''_1, \ldots, V_p : \tau''''_p\}$. Also by T-MATCHCLASS, for all $1 \leq i \leq m$ we have matchType(τ'_i, Pat') = (Γ'_i, τ'''_i) and for all $1 \leq i \leq p$ we have matchType(τ''_i, Pat'') = (Γ''_i, τ''''_i). Since $C \leq C'$ and $C \leq C''$, by Lemma B.4 either $C' \leq C''$ or $C'' \leq C'$.
    - Case $C' \leq C''$. Since $\bullet \vdash (\overline{\tau}\, C')$ OK, by Lemma A.7 we have $(\overline{\tau}\, C') \leq (\overline{\tau}\, C'')$. Then by Lemma A.12 we have that $p \leq m$. Then by the outer induction we have that for all $1 \leq i \leq p$ there exists Pat_i such that $Pat'_i \cap Pat''_i = Pat_i$. Then by PATINTCLASS there exists Pat such that $Pat' \cap Pat'' = Pat$.
    - Case $C'' \leq C'$. Since $\bullet \vdash (\overline{\tau}\, C'')$ OK, by Lemma A.7 we have $(\overline{\tau}\, C'') \leq (\overline{\tau}\, C')$. Then by Lemma A.12 we have that $m \leq p$. Then by the outer induction we have that for all $1 \leq i \leq m$ there exists Pat_i such that $Pat'_i \cap Pat''_i = Pat_i$. Then by PATINTREV we have that for all $1 \leq i \leq m$ there exists Pat_i such that $Pat''_i \cap Pat'_i = Pat_i$. Then by PATINTCLASS there exists Pat such that $Pat'' \cap Pat' = Pat$, and the result follows by PATINTREV.

□

Lemma B.18 If match(v, Pat') = ρ' and match(v, Pat'') = ρ'' and $Pat' \cap Pat'' = Pat$, then there exists some ρ such that match(v, Pat) = ρ.

Proof By induction on the depth of the derivation of $Pat' \cap Pat'' = Pat$. Case analysis of the last rule used in the derivation.

- Case PATINTWILD. Then Pat is identical to Pat'', so match(v, Pat) = ρ''.
- Case PATINTBIND. Then Pat' has the form I `as` Pat'_0 and $Pat'_0 \cap Pat'' = Pat$. Since match(v, Pat') = ρ', by E-MATCHBIND there exists some ρ'_0 such that match(v, Pat'_0) = ρ'_0. Therefore by induction there exists some ρ such that match(v, Pat) = ρ.
- Case PATINTTUP. Then Pat' has the form $(\overline{Pat'})$ and Pat'' has the form $(\overline{Pat''})$ and Pat has the form $(\overline{Pat})$ and $\overline{Pat'} \cap \overline{Pat''} = \overline{Pat}$. Since match($v, Pat'$) = ρ', by E-MATCHTUP $v = (\overline{v})$ and match($\overline{v}, \overline{Pat'}$) = $\overline{\rho'}$. Since match(v, Pat'') = ρ'', by E-MATCHTUP match($\overline{v}, \overline{Pat''}$) = $\overline{\rho''}$. Therefore by induction match($\overline{v}, \overline{Pat}$) = $\overline{\rho}$. Then by E-MATCHTUP there exists ρ such that match(v, Pat) = ρ.
- Case PATINTCLASS. Then Pat' has the form $(C'\ \{V_1 = Pat'_1, \ldots, V_m = Pat'_m\})$ and Pat'' has the form $(C''\ \{V_1 = Pat''_1, \ldots, V_p = Pat''_p\})$ and $m \geq p$ and Pat has the form $(C'\ \{V_1 = Pat_1, \ldots, V_p = Pat_p, V_{p+1} = Pat'_{p+1}, \ldots, V_m = Pat'_m\})$ and $C' \leq C''$ and $Pat'_i \cap Pat''_i = Pat_i$ for all $1 \leq i \leq m$. Since match(v, Pat') = ρ', by E-MATCHCLASS $v = ((\overline{\tau}\, C)\ \{V_1 = v_1, \ldots, V_k = v_k\})$ and $C \leq C'$ and $k \geq m$ and match(v_i, Pat'_i) = ρ'_i for all $1 \leq i \leq m$. Since match(v, Pat'') = ρ'', by E-MATCHCLASS we have match(v_i, Pat''_i) = ρ''_i for all $1 \leq i \leq p$. Then by induction, there exists ρ_i such that match(v_i, Pat_i) = ρ_i, for all $1 \leq i \leq p$. Then by E-MATCHCLASS there exists ρ such that match(v, Pat) = ρ.
- Case PATINTREV. Then $Pat'' \cap Pat' = Pat$. Then by induction there exists ρ such that match(v, Pat) = ρ.

□

B.3.2 Ambiguity

Lemma B.19 If owner(Mt, Pat) = $Sn.Cn$ and $\overline{\alpha} \vdash$ matchType(τ, Pat) = (Γ, τ'), then there exists some (<`abstract`> `class` $\overline{\alpha_0}$ $Cn\ldots) \in ST(Sn)$.

Proof By induction on the depth of the derivation of owner(Mt, Pat) = $Sn.Cn$. Case analysis of the last rule used in the derivation.

- Case OWNERBINDPAT. Then Pat has the form I `as` Pat' and owner$(Mt, Pat') = Sn.Cn$. Since $\overline{\alpha} \vdash \text{matchType}(\tau, Pat) = (\Gamma, \tau')$, by T-MATCHBIND we have that there exists some Γ' such that $\overline{\alpha} \vdash \text{matchType}(\tau, Pat') = (\Gamma', \tau')$. Therefore by induction there exists some $(\langle\texttt{abstract}\rangle\ \texttt{class}\ \overline{\alpha_0}\ Cn\ldots) \in ST(Sn)$.

- Case OWNERTUPPAT. Then Pat has the form $(Pat_1, \ldots, Pat_k)$ and $Mt = \tau_1 * \cdots * \tau_{i-1} * Mt_i * \tau_{i+1} * \cdots * \tau_k$ and owner(Mt_i, Pat_i) $= Sn.Cn$. Since $\overline{\alpha} \vdash \text{matchType}(\tau, Pat) = (\Gamma, \tau')$, by T-MATCHTUP there exist some τ_i, Γ_i, and τ_i' such that $\overline{\alpha} \vdash \text{matchType}(\tau_i, Pat_i) = (\Gamma_i, \tau_i')$. Therefore by induction there exists some $(\langle\texttt{abstract}\rangle\ \texttt{class}\ \overline{\alpha_0}\ Cn\ldots) \in ST(Sn)$.

- Case OWNERCLASSPAT. Then Pat has the form $Sn.Cn\ \{\overline{V} = \overline{Pat}\}$. Since $\overline{\alpha} \vdash \text{matchType}(\tau, Pat) = (\Gamma, \tau')$, by T-MATCHCLASS we have $\tau = (\overline{\tau}\, C')$ and repType$(\overline{\tau}\, C) = \{\overline{V} : \overline{\tau_1}\}$. Then by REP there exists some $(\langle\texttt{abstract}\rangle\ \texttt{class}\ \overline{\alpha_0}\ Cn\ldots) \in ST(Sn)$.

□

The following lemma says that the modular ambiguity checks for a function case are enough to ensure global unambiguity of the function case.

Lemma B.20 (Unambiguity) If $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$, then $\text{dom}(ST) \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E$ unambiguous in Sn.

Proof Suppose not. Then we have $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in \overline{Ood}$, but it is not the case that $\text{dom}(ST) \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E$ unambiguous in Sn. Then by STRAMB we have that there exists some $Sn' \in \text{dom}(ST)$, some $(\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E') \in ST(Sn')$, and some Pat_0 such that $Pat \cap Pat' = Pat_0 \wedge Sn.Mn \neq Sn'.Mn' \wedge \neg\exists Sn'' \in \text{dom}(ST).\exists(\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn'').(Pat_0 \leq Pat'' \wedge Pat'' \leq Pat \wedge Pat'' \leq Pat' \wedge (Pat \not\leq Pat'' \vee Pat' \not\leq Pat''))$.

Let $ST(Sn)$ be $(\texttt{structure}\ Sn = \texttt{struct depends upon}\ \overline{Sn}\ \overline{Ood}\ \texttt{end})$. Since $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$, by STRUCTOK we have $\overline{Sn} \vdash (\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E)$ OK in Sn, so by CASEOK we have $Sn; \overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E$ unambiguous. Let $ST(Sn') = (\texttt{structure}\ Sn' = \texttt{struct depends upon}\ \overline{Sn'}\ \overline{Ood'}\ \texttt{end})$. Since $(\texttt{structure}\ Sn' = \texttt{struct depends upon}\ \overline{Sn'}\ \overline{Ood'}\ \texttt{end}) = ST(Sn')$ and $(\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E') \in ST(Sn')$, by STRUCTOK we have $\overline{Sn'} \vdash (\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E')$ OK in Sn, so by CASEOK we have $Sn'; \overline{Sn'} \vdash \texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E'$ unambiguous.

We divide the proof into several cases.

- Case $Sn' \in \overline{Sn}$. Since $Sn; \overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E$ unambiguous, by AMB we have $\overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E$ unambiguous in Sn. Since $Sn' \in \overline{Sn}$ and we saw above that $(\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E') \in ST(Sn')$ and $Pat \cap Pat' = Pat_0$ and $Sn.Mn \neq Sn'.Mn'$, by STRAMB we have $\exists Sn'' \in \overline{Sn}.\exists\ (\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn'').(Pat_0 \leq Pat'' \wedge Pat'' \leq Pat \wedge Pat'' \leq Pat' \wedge (Pat \not\leq Pat'' \vee Pat' \not\leq Pat''))$. Since $(\texttt{structure = struct}\ Sn\ \texttt{depends upon}\ \overline{Sn}\ \overline{Ood}\ \texttt{end}) = ST(Sn)$, each structure name in $\overline{Sn}$ appears in the program, so by sanity condition 2 we have $\overline{Sn} \subseteq \text{dom}(ST)$. Therefore we have $\exists Sn'' \in \text{dom}(ST).\exists(\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn'').(Pat_0 \leq Pat'' \wedge Pat'' \leq Pat \wedge Pat'' \leq Pat' \wedge (Pat \not\leq Pat'' \vee Pat' \not\leq Pat''))$, and we have a contradiction.

- Case $Sn \in \overline{Sn'}$. Since $Sn'; \overline{Sn'} \vdash \texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E'$ unambiguous, by AMB we have $\overline{Sn'} \vdash \texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E'$ unambiguous in Sn'. By assumption $Sn \in \overline{Sn'}$, and we're given that $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$. We're also given $Pat \cap Pat' = Pat_0$, so by PATINTREV also $Pat' \cap Pat = Pat_0$. Finally, we're given $Sn.Mn \neq Sn'.Mn'$. Therefore by STRAMB we have $\exists Sn'' \in \overline{Sn'}.\exists(\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn'').(Pat_0 \leq Pat'' \wedge Pat'' \leq Pat' \wedge Pat'' \leq Pat \wedge (Pat \not\leq Pat'' \vee Pat' \not\leq Pat''))$. Since $(\texttt{structure = struct}\ Sn'\ \texttt{depends upon}\ \overline{Sn'}\ \overline{Ood'}\ \texttt{end}) = ST(Sn')$, each structure name in $\overline{Sn'}$ appears in the program, so by sanity condition 2 we have $\overline{Sn'} \subseteq \text{dom}(ST)$. Therefore we have $\exists Sn'' \in \text{dom}(ST).\exists(\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn'').(Pat_0 \leq Pat'' \wedge Pat'' \leq Pat \wedge Pat'' \leq Pat' \wedge (Pat \not\leq Pat'' \vee Pat' \not\leq Pat''))$, and we have a contradiction.

- Case $Sn' \notin \overline{Sn}$ and $Sn \notin \overline{Sn'}$. Since $Sn; \overline{Sn} \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E$ unambiguous, by AMB we have $F = Sn_1.Fn$ and $(\texttt{fun}\ \overline{\alpha_3}\ Fn : Mt \to \tau) \in ST(Sn_1)$ and owner$(Mt, Pat) = Sn_2.Cn$ and $Sn = Sn_1 \vee Sn = Sn_2$. Since $Sn'; \overline{Sn'} \vdash \texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E'$ unambiguous, by AMB we have owner$(Mt, Pat') = Sn_3.Cn'$ and $Sn' = Sn_1 \vee Sn' = Sn_3$. We have three sub-cases.
  - Case $Sn' = Sn_1$. Since $\overline{Sn} \vdash (\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E)$ OK in Sn, by CASEOK we have $\overline{Sn} \vdash F$ dependedUpon, so by FUNDEP we have $Sn_1 \in \overline{Sn}$. Therefore we've shown $Sn' \in \overline{Sn}$, so we have a contradiction.
  - Case $Sn = Sn_1$. Since $\overline{Sn'} \vdash (\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E')$ OK in Sn', by CASEOK we have $\overline{Sn'} \vdash F$ dependedUpon, so by FUNDEP we have $Sn_1 \in \overline{Sn'}$. Therefore we've shown $Sn \in \overline{Sn'}$, so we have a contradiction.
  - Case $Sn' \neq Sn_1$ and $Sn \neq Sn_1$. Since $Sn = Sn_1 \vee Sn = Sn_2$, we have $Sn = Sn_2$. Since $Sn' = Sn_1 \vee Sn' = Sn_3$, we have $Sn' = Sn_3$. Since owner$(Mt, Pat) = Sn_2.Cn$ and owner$(Mt, Pat') = Sn_3.Cn'$ and $Pat \cap Pat' = Pat_0$, by Lemma B.16 we have that either $Sn_2.Cn \leq Sn_3.Cn'$ or $Sn_3.Cn' \leq Sn_2.Cn$. Equivalently, either $Sn.Cn \leq Sn'.Cn'$ or $Sn'.Cn' \leq Sn.Cn$. There are two subcases.
    - Case $Sn.Cn \leq Sn'.Cn'$. Since $\overline{Sn} \vdash (\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E)$ OK in Sn, by CASEOK we have $\overline{\alpha_0} \vdash \text{match}(\tau_0, Pat) = (\Gamma_0, \tau_0')$, for some $\overline{\alpha_0}, \tau_0, Pat, \Gamma_0$, and τ_0'. Since owner$(Mt, Pat) = Sn.Cn$, by Lemma B.19 there exists some $(\langle\texttt{abstract}\rangle\ \texttt{class}\ \overline{\alpha_4}\ Cn\ldots) \in ST(Sn)$. Therefore by STRUCTOK we have $\overline{Sn} \vdash (\langle\texttt{abstract}\rangle\ \texttt{class}\ \overline{\alpha_4}\ Cn\ldots)$ OK in Sn, so by CLASSOK we have $\overline{Sn} \vdash Sn.Cn$ transDependedUpon. Since $Sn.Cn \leq Sn'.Cn'$, by Lemma B.8 we have $Sn' \in \overline{Sn}$, which is a contradiction.

* Case $Sn'.Cn' \leq Sn.Cn$. Since $\overline{Sn'} \vdash (\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E')$ OK in Sn', by CASEOK we have $\overline{\alpha_0} \vdash \text{match}(\tau_0, Pat') = (\Gamma_0, \tau_0')$, for some $\overline{\alpha_0}, \tau_0, Pat, \Gamma_0$, and τ_0'. Since owner$(Mt, Pat') = Sn'.Cn'$, by Lemma B.19 there exists some (<abstract> class $\overline{\alpha_4}$ Cn' ...) $\in ST(Sn')$. Therefore by STRUCTOK we have $\overline{Sn'} \vdash$ (<abstract> class $\overline{\alpha_4}$ Cn' ...) OK in Sn', so by CLASSOK we have $\overline{Sn'} \vdash Sn'.Cn'$ transDependedUpon. Since $Sn'.Cn' \leq Sn.Cn$, by Lemma B.8 we have $Sn \in \overline{Sn'}$, which is a contradiction.

□

The following lemma says that if a value has at least one applicable function case then it has a most-specific applicable case. The lemma thereby validates our static notion of unambiguity by showing that it is sufficient to imply the success of function-case lookup.

Lemma B.21 If $\vdash v : \tau$ and $Sn \in \text{dom}(ST)$ and $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$ and match$(v, Pat) = \rho$, then there exists some $Sn' \in \text{dom}(ST)$, some $(\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E') \in ST(Sn')$, and some ρ' such that match$(v, Pat') = \rho'$ and $\forall Sn'' \in \text{dom}(ST).\forall(\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn'').\ \forall\rho''.((\text{match}(v, Pat'') = \rho'' \wedge Sn'.Mn' \neq Sn''.Mn'') \Rightarrow Pat' < Pat'')$.
Proof By (strong) induction on the number of function cases of the form $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0)$ such that $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0) \in ST(Sn_0)$ for some structure $Sn_0 \in \text{dom}(ST)$, and match$(v, Pat_0) = \rho_0$ for some ρ_0, and $Pat \not< Pat_0$.

- Case there are zero function cases of the form $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0)$ such that $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0)$ $\in ST(Sn_0)$ for some structure $Sn_0 \in \text{dom}(ST)$, and match$(v, Pat_0) = \rho_0$ for some ρ_0, and $Pat \not< Pat_0$.

  We're given that $Sn \in \text{dom}(ST)$ and $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$ and match$(v, Pat) = \rho$. Further, since it cannot both be the case that $Pat \leq Pat$ and $Pat \not\leq Pat$, we have $Pat \not< Pat$. Therefore, we have found a function case that contradicts the initial assumption of this case.

- Case there is exactly one function case of the form $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0)$ such that $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0) \in ST(Sn_0)$ for some structure $Sn_0 \in \text{dom}(ST)$, and match$(v, Pat_0) = \rho_0$ for some ρ_0, and $Pat \not< Pat_0$.

  As we saw in the previous case, $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$ and match$(v, Pat) = \rho$ and $Pat \not< Pat$, so $Sn.Mn$ is the single case satisfying all the conditions. Therefore it follows that $\forall Sn'' \in \text{dom}(ST).\forall(\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn'').\forall\rho''.((\text{match}(v, Pat'') = \rho'' \wedge Sn.Mn \neq Sn''.Mn'') \Rightarrow Pat < Pat'')$. Then the result follows.

- There are $k > 1$ function cases of the form $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0)$ such that $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0)$ $\in ST(Sn_0)$ for some structure $Sn_0 \in \text{dom}(ST)$, and match$(v, Pat_0) = \rho_0$ for some ρ_0, and $Pat \not< Pat_0$. Let $(\texttt{extend fun}_{Mn_1}\ \overline{\alpha_3}\ F\ Pat_1 = E_1)$ be one such function case, so $(\texttt{extend fun}_{Mn_1}\ \overline{\alpha_3}\ F\ Pat_1 = E_1) \in ST(Sn_1)$ for some structure $Sn_1 \in \text{dom}(ST)$, and match$(v, Pat_1) = \rho_1$ for some ρ_1, and $Pat \not< Pat_1$. Since $k > 1$, at least one of the function cases satisfying the conditions is not $Sn.Mn$, so assume WLOG that $Sn.Mn \neq Sn_1.Mn_1$.

  Since $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$ and $(\texttt{extend fun}_{Mn_1}\ \overline{\alpha_3}\ F\ Pat_1 = E_1) \in ST(Sn_1)$ and $Sn \in \text{dom}(ST)$ and $Sn_1 \in \text{dom}(ST)$, by CASEOK we have matchType$(\tau_0, Pat) = (\Gamma_0, \tau_0')$ and matchType$(\tau_1, Pat_1) = (\Gamma_1, \tau_1')$. We're given that $\vdash v : \tau$. Finally, we saw above that match$(v, Pat) = \rho$ and match$(v, Pat_1) = \rho_1$. Therefore by Lemma B.17 there exists some Pat_{int} such that $Pat \cap Pat_1 = Pat_{int}$. We're given that $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$, so by Lemma B.20 we have $\text{dom}(ST) \vdash \texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E$ unambiguous in Sn. Therefore by STRAMB there exists some $Sn_2 \in \text{dom}(ST)$ and some $(\texttt{extend fun}_{Mn_2}\ \overline{\alpha_4}\ F\ Pat_2 = E_2) \in ST(Sn_2)$ such that $Pat_{int} \leq Pat_2$ and $Pat_2 \leq Pat$ and $Pat_2 \leq Pat_1$ and ($Pat \not\leq Pat_2$ or $Pat_1 \not\leq Pat_2$). Since match$(v, Pat) = \rho$ and match$(v, Pat_1) = \rho_1$ and $Pat \cap Pat_1 = Pat_{int}$, by Lemma B.18 there exists some ρ_{int} such that match$(v, Pat_{int}) = \rho_{int}$. Then since $Pat_{int} \leq Pat_2$, by Lemma B.7 there exists ρ_2 such that match$(v, Pat_2) = \rho_2$.

  So we have shown there exists some $Sn_2 \in \text{dom}(ST)$ and some $(\texttt{extend fun}_{Mn_2}\ \overline{\alpha_4}\ F\ Pat_2 = E_2) \in ST(Sn_2)$ and some ρ_2 such that match$(v, Pat_2) = \rho_2$. Suppose there are l function cases of the form $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0)$ such that $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0) \in ST(Sn_0)$ for some structure $Sn_0 \in \text{dom}(ST)$, and match$(v, Pat_0) = \rho_0$ for some ρ_0, and $Pat_2 \not< Pat_0$. To finish this case, we will show that $l < k$, so that the result follows by induction with respect to Sn_2.

  Consider some structure $Sn_0 \in \text{dom}(ST)$, some $(\texttt{extend fun}_{Mn_0}\ \overline{\alpha_0}\ F\ Pat_0 = E_0) \in ST(Sn_0)$, and some ρ_0 such that match$(v, Pat_0) = \rho_0$ and $Pat_2 \not< Pat_0$. I claim that also $Pat \not< Pat_0$. Since $Pat_2 \not< Pat_0$, we have that ($Pat_2 \not\leq Pat_0$ or $Pat_0 \leq Pat_2$), so we consider these cases in turn.

  – Case $Pat_2 \not\leq Pat_0$. Then I claim that $Pat \not\leq Pat_0$, so also $Pat \not< Pat_0$. Suppose not, so $Pat \leq Pat_0$. Since $Pat_2 \leq Pat$, by Lemma B.15 we have $Pat_2 \leq Pat_0$, contradicting the assumption of this case.

  – Case $Pat_0 \leq Pat_2$. We showed above that $Pat_2 \leq Pat$, so by Lemma B.15 $Pat_0 \leq Pat$, so $Pat \not< Pat_0$.

  Therefore we have shown that every function case of the appropriate form with respect to $Sn_2.Mn_2$ is also of the appropriate form with respect to $Sn.Mn$, so $l \leq k$.

  To finish the proof, we show that there exists a function case of the appropriate form w.r.t. $Sn.Mn$ that is not of the appropriate form w.r.t. $Sn_2.Mn_2$. In particular, we showed in the first case above that $Sn.Mn$ is of the appropriate form w.r.t. itself, since $Pat \not< Pat$. To show that $Sn.Mn$ is not of the appropriate form w.r.t $Sn_2.Mn_2$, we must show that $Pat_2 < Pat$. We showed above that $Pat_2 \leq Pat$, so we simply need to prove that $Pat \not\leq Pat_2$. We showed above that either $Pat \not\leq Pat_2$ or $Pat_1 \not\leq Pat_2$, so we consider each case.

– Case $Pat \not\leq Pat_2$. Then $Pat \not\leq Pat_2$.

– Case $Pat_1 \not\leq Pat_2$ and $Pat \leq Pat_2$. We're given above that $Pat \not< Pat_1$, so either $Pat \not\leq Pat_1$ or $Pat_1 \leq Pat$. We saw above that $Pat_2 \leq Pat_1$, so since we assume $Pat \leq Pat_2$, by Lemma B.15 we have $Pat \leq Pat_1$. Therefore $Pat_1 \leq Pat$. Again since we assume $Pat \leq Pat_2$, by Lemma B.15 we have $Pat_1 \leq Pat_2$, contradicting the assumption of this case.

□

Lemma 4.1 If $\vdash (\overline{\tau}\, F) : \tau_2 \rightarrow \tau$ and $\vdash v : \tau_2'$ and $\tau_2' \leq \tau_2$ then there exist ρ_0 and E_0 such that most-specific-case-for $((\overline{\tau}\, F),v)$ = (ρ_0, E_0).

Proof By Lemma B.14, there exists some $Sn \in \text{dom}(ST)$, some $(\texttt{extend fun}_{Mn}\ \overline{\alpha}\ F\ Pat = E) \in ST(Sn)$, and some environment ρ such that match(v,Pat) = ρ. Then by Lemma B.21 there exists some $Sn' \in \text{dom}(ST)$, some $(\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E')$ $\in ST(Sn')$, and some ρ' such that match(v,Pat') = ρ' and $\forall Sn'' \in \text{dom}(ST).\forall(\texttt{extend fun}_{Mn''}\ \overline{\alpha_2}\ F\ Pat'' = E'') \in ST(Sn'').\forall\rho''.$ $((\text{match}(v,Pat'') = \rho'' \wedge Sn'.Mn' \neq Sn''.Mn'') \Rightarrow Pat' \leq Pat'' \wedge Pat'' \not\leq Pat')$. Since $\vdash (\overline{\tau}\, F) : \tau_2 \rightarrow \tau$, by T-FUN we have $F = Sn_0.Fn_0$ and $(\texttt{fun}\ \overline{\alpha_0}\ Fn_0 : Mt_0 \rightarrow \tau_0)$ and $|\overline{\alpha_0}| = |\overline{\tau}|$. Since $(\texttt{extend fun}_{Mn'}\ \overline{\alpha_1}\ F\ Pat' = E') \in ST(Sn')$, by CASEOK we have $|\overline{\alpha_1}| = |\overline{\alpha_0}|$. Therefore we have $|\overline{\alpha_1}| = |\overline{\tau}|$, so by LOOKUP there exists some ρ_0 and E_0 such that most-specific-case-for $((\overline{\tau}\, F),v)$ = (ρ_0, E_0). □

B.4 Progress

Theorem 4.2 (Progress): If $\vdash E : \tau$ and E is not a value, then there exists an E' such that $E \longrightarrow E'$.

Proof By (strong) induction on the depth of the derivation of $\vdash E : \tau$. Case analysis of the last rule used in the derivation.

- Case T-ID. Then $E = I$ and $(I,\tau) \in \{\}$, so we have a contradiction. Therefore this rule could not be the last rule used in the derivation.
- Case T-NEW. Then $E = Ct(\overline{E})$ and $Ct = (\overline{\tau}\ Sn.Cn)$ and $\bullet \vdash Ct(\overline{E})$ OK and concrete$(Sn.Cn)$. Then by T-SUPER also $\bullet \vdash (\overline{\tau}\ Sn.Cn)$ OK and and $(\texttt{<abstract>}\ \texttt{class}\ \overline{\alpha_0}\ Cn(\overline{I_0 : \tau_0})\ \ldots) \in ST(Sn)$ and $|\overline{I_0}| = |\overline{E}|$. Therefore by Lemma B.9 rep$(Ct(\overline{E})$ is well-defined and has the form $\{\overline{V_1 = E_1}\}$. Then by E-NEW we have $E \longrightarrow Ct\ \{\overline{V_1 = E_1}\}$.
- Case T-REP. Then $E = Ct\ \{V_1 = E_1, \ldots, V_k = E_k\}$ and for all $1 \leq i \leq k$ we have $\vdash E_i : \tau_i$ for some τ_i. We have two subcases:
  - For all $1 \leq i \leq k$, E_i is a value. Then E is a value, contradicting our assumption.
  - There exists some j such that $1 \leq j \leq k$ and E_j is not a value. WLOG, let j be the smallest integer satisfying this condition, so for all $1 \leq q < j$ we have that E_q is a value. By induction, there exists an E_j' such that $E_j \longrightarrow E_j'$. Therefore by E-REP we have $Ct\ \{V_1 = E_1, \ldots, V_k = E_k\} \longrightarrow Ct\ \{V_1 = E_1, \ldots, V_{j-1} = E_{j-1}, V_j = E_j', V_{j+1} = E_{j+1}, \ldots, V_k = E_k\}$.
- Case T-FUN. Then $E = \overline{\tau}\ Sn.Fn$. Then E is a value, contradicting our assumption.
- Case T-TUP. Then $E = (E_1, \ldots, E_k)$ and $\tau = \tau_1 * \cdots * \tau_k$ and for all $1 \leq i \leq k$ we have $\vdash E_i : \tau_i$. We have two subcases:
  - For all $1 \leq i \leq k$, E_i is a value. Then E is a value, contradicting our assumption.
  - There exists some j such that $1 \leq j \leq k$ and E_j is not a value. WLOG, let j be the smallest integer satisfying this condition, so for all $1 \leq q < j$ we have that E_q is a value. By induction, there exists an E_j' such that $E_j \longrightarrow E_j'$. Therefore by E-TUP we have $(E_1, \ldots, E_k) \longrightarrow (E_1, \ldots, E_{j-1}, E_j', E_{j+1}, \ldots, E_k)$.
- Case T-APP. Then $E = E_1\ E_2$ and $\vdash E_1 : \tau_2 \rightarrow \tau$ and $\vdash E_2 : \tau_2'$ and $\tau_2' \leq \tau_2$. We have three subcases:
  - E_1 is not a value. Then by induction, there exists an E_1' such that $E_1 \longrightarrow E_1'$. Therefore by E-APP1 we have $E_1\ E_2 \longrightarrow E_1'\ E_2$.
  - E_1 is a value, but E_2 is not a value. Then by induction, there exists an E_2' such that $E_2 \longrightarrow E_2'$. Therefore by E-APP2 we have $E_1\ E_2 \longrightarrow E_1\ E_2'$.
  - Both E_1 and E_2 are values. Since $\vdash E_1 : \tau_2 \rightarrow \tau$ and E_1 is a value, the last rule in the derivation of $\vdash E_1 : \tau_2 \rightarrow \tau$ must be T-FUN, so E_1 has the form Fv. Therefore by Lemma 4.1 we have that there exist ρ_0 and E_0 such that most-specific-case-for (Fv,E_2) = (ρ_0, E_0). Let $\rho_0 = \{(\overline{I}, \overline{v})\}$. Then by E-APPRED we have $Fv\ E_2 \longrightarrow [\overline{I} \mapsto \overline{v}]E_0$.

□