Math. Struct. in Comp. Science (1995), *vol.* 11, *pp.* 1–000

Higher-Order Intersection Types and Multiple Inheritance

ADRIANA B. COMPAGNONI and BENJAMIN C. PIERCE

Computer Laboratory, University of Cambridge
New Museums Site, Pembroke St., CB2 3QG, U.K.

Received 1994

We study a natural generalization of System F^ω with intersection types, establishing basic structural properties and constructing a semantic model based on partial equivalence relations to prove the soundness of typing. As an application of this calculus, we define a simple typed model of object-oriented programming with multiple inheritance.

1. Motivation

One of the first applications of subtyping in λ-calculi was modeling the refinement of interfaces in object-oriented programming languages [Cardelli, 1984]. The formal subtype relation $\Gamma \vdash S \leq T$ models the assertion that the objects in some collection S provide more services than those in T, so that it is safe to use a member of S in any context where a member of T is expected.

Subtyping itself is a straightforward concept, but it took years to build full-scale models of real object-oriented languages on this foundation. Treating the interaction between interface refinement and encapsulation of objects has required higher-order generalizations of subtyping — the F-bounded quantification of Canning, Cook, Hill, Olthoff, and Mitchell [Canning *et al.*, 1989, Cook *et al.*, 1990] or Cardelli and Mitchell's system $F^\omega_\leq$ [Cardelli, 1990, Mitchell, 1990a, Bruce and Mitchell, 1992]. Using these techniques, a number of fairly complete "foundational object models" related to those found in languages such as Smalltalk [Goldberg and Robson, 1983] and Self [Ungar and Smith, 1987] have recently appeared [Bruce, 1994, Mitchell *et al.*, 1993, Pierce and Turner, 1994, Fisher and Mitchell, 1994, Abadi, 1994, Abadi and Cardelli, 1994b, Abadi and Cardelli, 1994a, Abadi and Cardelli, 1996, Abadi *et al.*, 1996]. Current work in this area also includes models of the object-oriented features in languages such as CLOS [Castagna *et al.*, 1995, Castagna, 1992], which are less closely related to the results described here.

The common goal of these studies is to prove the safety of a type system describing a set of high-level syntactic constructs for object encapsulation, message passing, and inheritance. Most proceed either by mapping the high-level syntax directly into a denotational model and proving the soundness of this interpretation using standard semantic techniques or by reasoning directly on the operational semantics of the source calculus. Others translate the high-level syntax into a more conventional λ-calculus, whose own type-safety is established separately; the soundness of the typing rules for the object features then follows from the soundness of the target system. Both approaches have advantages, but the latter can often be simpler to use and understand, since it allows the implementation of complex mechanisms like inheritance to be considered as *programming* in a typed language as opposed to definition of a complex semantic interpretation function. We can verify type safety automatically using a typechecker for the underlying λ-calculus, and we can experiment easily with alternatives.

The object model of Pierce and Turner [1994], on which the present study is based, encodes objects as expressions of $F^{\omega}_{\leq}$, an extension of Girard's System F^{ω} [1972] with bounded quantification. Given a description `M` of a public interface — the names and types of a set of methods — the type `Object(M)` denotes the type of objects satisfying this description.† For example, if `PointM` describes the interface of one-dimensional point objects responding to the messages `setX` and `getX` then `Object(PointM)` is the type of points. Associated with each such collection of objects is a group of functions for sending messages, with types like

```
Point'setX  :  All(M < PointM) Object(M) -> Int -> Object(M)
```

for the function that invokes its `setX` method of any object whose interface refines that of points. The bounded quantifier `All(M<PointM)` expresses the fact that the message `setX` can actually be sent to any object whose interface refines the interface of points. Given such an object and an integer representing its new x-coordinate, `Point'setX` returns a new object with an appropriately updated position. (Note that `'` is used here as an ordinary character: `Point'setx` is a single identifier. Also, note that we are working with a functional style of object-oriented programming, where methods like `setX` return new objects instead of modifying existing ones. Prospects for extending our model to objects with mutable state are discussed in Section 6.)

The foregoing accounts for the fundamental features of object encapsulation and interface refinement (and correctly handles their interaction, which is the difficult part!). But it omits some characteristic features of popular object-oriented languages, notably inheritance.

In general terms, inheritance is a mechanism allowing the implementations of different sorts of objects that share some of their behavior to be factored so that the common behavior is written just once. Of the three common varieties of inheritance — subclassing as in Smalltalk, delegation as in Self, and generic functions as in CLOS — subclassing and delegation can be handled by similar techniques, while generic functions seem to require substantially different foundations. We consider a class-based language here.

A class is a data structure that can be used in two ways: as a template for creating new objects, and as the basis for defining subclasses by incremental extension. If `M` is an object interface, then `Class(M)` is the type of classes whose instances are objects of type `Object(M)`. The polymorphic function `new` maps a class into a new object:

† Technically, object interfaces are type operators of kind $\star \to \star$, i.e. maps from types to types, and `Object`$\in (\star \to \star) \to \star$ is a higher-order constructor. See Sections 2 and 5 for details and [Pierce and Turner, 1994] for a longer discussion.

```
new : All(M:*->*) Class(M) -> Object(M)
```

Another function, `extend`, takes an existing class and a description of some new methods and constructs a new class combining the old and new behaviors:

```
extend : All(SuperM:*->*)
         All(SelfM<SuperM)
           Class(SuperM) -> ... -> Class(SelfM)
```

(The details hidden here by `...` are revealed in the following section and Section 5.) The bounded quantifier `All(SelfM<SuperM)` ensures that the interface of the new class refines that of the old: `Object(SelfM)` is a subtype of `Object(SuperM)`.‡

To handle multiple inheritance in this setting, we must enrich the `extend` function to take two or more superclasses as arguments. Consider the case where the new class inherits methods from two superclasses. This version — call it `extend2` (there will be an analogous one for each n) — should have a type like:

```
extend2 : All(SuperM1:*->*)      % the interface of one superclass
          All(SuperM2:*->*)      % the interface of the other superclass
          All(SelfM<???)         % the interface of the class being built
               Class(SuperM1)    % the first superclass
            -> Class(SuperM2)    % the second superclass
            -> ...               % (how to build the new class)
            -> Class(SelfM)      % the new class itself
```

But the upper bound of `SelfM` presents a problem: we must ensure that `SelfM` is a subtype of *both* `SuperM1` and `SuperM2`, which falls outside the expressive scope of our target λ-calculus $F^{\omega}_{\leq}$.

Intuitively, what we want to write is

```
extend2 : All(SuperM1:*->*) All(SuperM2:*->*)
          All(SelfM < SuperM1 "and" SuperM2)
               Class(SuperM1)
            -> Class(SuperM2)
            -> ...
            -> Class(SelfM)
```

where `"and"` forms the conjunction of the two superclass specifications. Fortunately, a type constructor with exactly this meaning has already appeared in the literature.

First-order type systems with intersection types have been investigated by researchers

‡ There is a delicate technical point here. Cook, Hill, and Canning have argued [1990] that "subtyping is not inheritance," that the two concepts live in different categories — subtyping in the world of types, inheritance in the world of values — and must be considered separately to avoid confusion. It might appear, therefore, that we should be able to use inheritance to form new classes with arbitrary interfaces, not only subclasses with more refined interfaces. Indeed, this would be true if it were not for the rather subtle form of self-reference inherent in "sending messages to `self`" in most object-oriented languages, which we are also modeling here. A method defined in a superclass may refer, via `self`, to a different method of the same object. If this method is overriden in the definition of a subclass, the new behavior will be invoked instead. This overriding can only be type-safe if the the new method has a more refined type than the old one. Thus, in the presence of `self`, the inheritance hierarchy must follow the subtype hierarchy.

in Torino [Coppo and Dezani-Ciancaglini, 1978, Barendregt *et al.*, 1983] and elsewhere. (See [Cardone and Coppo, 1990] for background and further references.) A second-order λ-calculus with intersection types was studied by Pierce [1991]. The calculus needed here is the ω-order extension of this system. Since the first version of this paper was completed, the metatheory of this system has been studied in much greater detail by Compagnoni [Compagnoni, 1994, Compagnoni, 1995].

A type system combining intersection types with a powerful form of polymorphism is of independent interest. Reynolds [1988] has argued that intersection types can form the basis of elegant language designs. But his Forsythe language has only a first-order type system, and thus lacks some of the expressive possibilities of polymorphic languages like ML. Our work represents a step toward a synthesis of these styles of language design.

The following section shows some examples of multiple inheritance using a simple high-level syntax. Section 3, the core of the paper, defines the λ-calculus $F^\omega_\wedge$, an extension of System F^ω with intersection types, and establishes some of its basic properties. In Section 4 we prove the paper's main theoretical result: the soundness of typing and subtyping for a model based on partial equivalence relations. Section 5 develops an implementation of inheritance in this setting. Section 6 offers further comparisons with related work and suggestions for future research.

An earlier version of this paper appeared as University of Edinburgh Technical Report ECS-LFCS-93-275 and Catholic University Nijmegen C.S. Department Technical Report 93-18, under the title *Multiple Inheritance via Intersection Types.*

2. An Example of Multiple Inheritance

We further motivate the calculus $F^\omega_\wedge$ by recalling the encodings of some basic concepts of object-oriented programming in $F^\omega_\leq$ and showing a simple concrete example of multiple inheritance in this setting. Readers who feel more interested in $F^\omega_\wedge$ itself may safely skip this section.

In this setting, an object *interface specification* is modeled as a function from types to types, describing the behaviors of a collection of methods as transformations on the object's internal state. For example, the interface of one-dimensional point objects supporting the messages `getX`, `setX`, and `bump` is captured by the type operator

```
# PointM = Fun(Rep) {| setX: Rep->Int->Rep, getX: Rep->Int, bump: Rep->Rep |};
PointM : *->*
```

which expresses the fact that the `getX` method of a point interrogates its internal state and returns an integer, that the `set` method transforms the internal state and a new position into an updated internal state, and that `bump`, which increases the position by one, maps one internal state to another. (The `#` in the left-hand margin indicates that this expression has been checked by our implementation; the typechecker's response follows.) The abstraction over the type `Rep` of the internal state hides the actual internal state from outside view. Concretely, a point whose internal state type is `{|x:Int|}` — a one-field record containing an integer — will contain a record of methods with types

```
   {|  setX: {|x:Int|} -> Int -> {|x:Int|},
```

```
        getX: {|x:Int|} -> Int,
        bump: {|x:Int|} -> {|x:Int|}          |}
```

while a point whose internal state type is richer, say `{|x:Int,y:Int|}`, will have correspondingly richer concrete types for its methods:

```
    {|  setX: {|x:Int,y:Int|} -> Int -> {|x:Int,y:Int|},
        getX: {|x:Int,y:Int|} -> Int,
        bump: {|x:Int,y:Int|} -> {|x:Int,y:Int|}          |}
```

Externally, we expect the difference between these two to be invisible; thus, the public interface to the methods, `PointM`, abstracts away from any particular representation type. Both point objects are elements of the type `Object(PointM)`. (For present purposes, it is not important how `Object` itself is defined. One possible definition is `Object(M) = Some(R) R * M(R)` — i.e., an object is a pair of a current state and a collection of methods, with the type of the state hidden by an existential type. Cf. [Pierce and Turner, 1994, Hofmann and Pierce, 1995].)

New objects are created by applying the polymorphic function `new` to a *class*. Given an interface `M` and a class for this interface — that is, a class whose *instances* are objects with interface `M` — `new` creates and returns such an object. New classes, in turn, are created by applying the polymorphic function `extend` to an existing class along with a specification of an incremental change to its behavior:

```
extend = <val>
       : All(SuperM)
         All(SelfM<SuperM)
         All(SelfDiffR)
              (Class SuperM)
           -> SelfDiffR
           -> (All(FinalR)
                   (Extractor FinalR SelfDiffR)
                ->(SuperM FinalR)
                ->(SelfM FinalR)
                ->(SelfM FinalR))
           -> (Class SelfM)
```

In detail, the arguments expected by `extend` are:

- The interface `SuperM` of the existing class.
- The interface `SelfM` of the new class that will be returned by `extend`.
- The type `SelfDiffR`, which describes the difference between the representation of the superclass (whatever it may be) and the representation of the new class. In conventional terminology, this is the set of new instance variables introduced by the subclass.
- The superclass itself — an element of `Class(SuperM)` (our typechecker prints it as `Class SuperM`).
- An initial value — an element of `SelfDiffR` — for the new part of the state.
- A polymorphic "method builder" function.

Given all these, `extend` returns a class for the interface `SelfM`.

The method builder function, which does the work of constructing the vector of methods to be used in instances of the new class, must itself take several parameters:

— The "final" representation type `FinalR`, which is fixed at the moment when `new` is applied to a class.
— An "extractor," which provides a mapping back and forth between the final representation type and the local representation type, allowing the local methods to access the part of the state that interests them. For the moment, we shall not define extractors in detail; the definition appears in Section 5. (The fact that we need to work with extractors at all arises from our simple treatment of record types. A cleaner object model might be obtained, at the cost of some complication in the type theory, by using a more refined model of records related to those studied by Cardelli and Mitchell [1991].)
— The "super methods" of the existing class.
— The "self methods" of the new class, used to model the characteristic object-oriented feature of "sending a message to `self`."

Given these, the method builder must return a collection of methods for the new object.

For uniformity, let us assume that there is one base class — the class of "things," whose instances are objects with no behavior at all:

```
# ThingM = Fun(Rep) {| |};
ThingM : *->*
thingClass = <val> : Class ThingM
```

To build a class of points extending `thingClass`, we first choose the "local" part of the representation of points.

```
# PointDiffR = {| x:Int |};
PointDiffR : *
```

Now we create `pointClass` by applying `extend` as follows. (See Section 5 for more details.)

```
# pointClass =
#   extend
#     ThingM                            % superclass interface
#     PointM                            % interface for new class
#     PointDiffR                        % local state type
#     thingClass                        % the superclass itself
#     { x = 0 }                         % initial value for local state
#     (fun(FinalR)                      % "method builder" function...
#      fun(e: Extractor FinalR PointDiffR)   % mapping a "state extractor"
#      fun(super: ThingM FinalR)             % and the "super methods"
#      fun(self: PointM FinalR)              % and the "self methods"
#        {getX = fun(s:FinalR)               % to a getX method
#                  (e.get s).x,              %  that returns the local x field
#         setX = fun(s:FinalR)               % and a setX method
#                  fun(i:Int) e.put s {x=i}, %  that overwrites the x field
#         bump = fun(s:FinalR)               % and a bump method
#                  self.setX s               %  that calls setX on self to set x
#                    (plus (self.getX s) 1)  %  to one more than self.getX
#        });
pointClass = <val> : Class PointM
```

Of course, this definition of `pointClass` is quite verbose. Ultimately, we would want to have higher-level syntax for objects, message passing, and class extension more closely resembling ordinary object-oriented source code, giving high-level typing rules directly in terms of the high-level syntax. Since we are building a foundational model here, we prefer the low-level notation.

Similarly, we can define the interface for "colored objects" — objects supporting the messages `setC` and `getC` — as follows:

```
# ColoredM = Fun(Rep) {| setC: Rep->Color->Rep, getC: Rep->Color |};
ColoredM : *->*
```

Again, one instance variable suffices to represent the color of a colored object:

```
# ColoredDiffR = {| c:Color |};
ColoredDiffR : *
```

A class of colored objects can now be created by extending `thingClass` as we did to build `pointClass`:

```
# coloredClass =
#   extend ThingM ColoredM ColoredDiffR thingClass
#   { c = black }
#   (fun(FinalR)
#    fun(e: Extractor FinalR ColoredDiffR)
#    fun(super: ThingM FinalR)
#    fun(self: ColoredM FinalR)
#      {getC = fun(s:FinalR) (e.get s).c,
#       setC = fun(s:FinalR) fun(newc:Color) e.put s {c=newc}
#      });
coloredClass = <val> : Class ColoredM
```

Now we have reached the point where we can use *multiple* inheritance to combine the classes of point objects and colored objects, yielding a new class of colored points. The interface of colored points contains all the messages of both superclasses:

```
# CPointM = Fun(Rep) {| setX: Rep->Int->Rep, getX: Rep->Int, bump: Rep->Rep,
#                        setC: Rep->Color->Rep, getC: Rep->Color |};
CPointM : *->*
```

For this simple implementation, no additional instance variables are needed: we can set `CPointDiffR = {| |}`.

To make the example more interesting, we take the methods `getX`, `setC`, and `getC` unchanged from the superclasses, while *overriding* the definition of `setX` so that, in addition to setting the `x` coordinate as usual, it also sets the color to blue:

```
# cpointClass =
#   extend2 PointM ColoredM CPointM
#     CPointDiffR pointClass coloredClass { }
#     (fun(FinalR)
#      fun(e: Extractor FinalR CPointDiffR)
#      fun(super1: PointM FinalR)
#      fun(super2: ColoredM FinalR)
#      fun(self: CPointM FinalR)
```

```
#        {setX = fun(s:FinalR) fun(i:Int) % the new setX method:
#          let s1 = super1.setX s i in    % use pointClass's setX to set position
#          let s2 = super2.setC s1 blue   % and coloredClass's setC to set color
#          in s2   end end,
#         getX = super1.getX,             % copy all the remaining methods
#         bump = super1.bump,             % from the appropriate superclass
#         setC = super2.setC,
#         getC = super2.getC
#        });
cpointClass = <val> : Class CPointM
```

Here, the low level at which we are working is reflected in the fact that the old methods `getX`, `bump`, `setC`, and `getC` must be copied explicitly from the superclasses to the new class. This means that we do not need to address some of the issues that ordinarily arise when designing high-level languages with multiple inheritance (must each inherited method appear in only one of the superclasses? if it appears in more than one, which should be copied to the subclass? etc.). Effectively, we force the programmer to answer these questions manually, on a case-by-case basis. Of course, if we were to introduce a high-level syntax for a language with classes and multiple inheritance, the translation from this high-level syntax into the present low-level language would necessarily embody some solution to these issues.

Recall that, for each method interface `M`, we have a group of functions for sending messages to objects whose interfaces are refinements of `M`. For the interfaces `PointM` and `ColoredM`, these functions have the following types:

```
    Point'setX    :  All(M < PointM)   Object(M) -> Int -> Object(M)
    Point'getX    :  All(M < PointM)   Object(M) -> Int
    Point'bump    :  All(M < PointM)   Object(M) -> Object(M)
    Colored'setC  :  All(M < ColoredM) Object(M) -> Color -> Object(M)
    Colored'getC  :  All(M < ColoredM) Object(M) -> Color
    CPoint'setX   :  All(M < CPointM)  Object(M) -> Int -> Object(M)
    CPoint'getX   :  All(M < CPointM)  Object(M) -> Int
    CPoint'bump   :  All(M < CPointM)  Object(M) -> Object(M)
    CPoint'setC   :  All(M < CPointM)  Object(M) -> Color -> Object(M)
    CPoint'getC   :  All(M < CPointM)  Object(M) -> Color
```

Note that `Point'setX` is a single identifier; we include the name of the object type, `Point` or `Colored` or `CPoint`, in the names of the message-sending functions by convention. Intuitively, the behavior of these functions is just to extract the appropriate internal method of the object and apply it to the internal state, so, for example, `Colored'getC` and `CPoint'getC` give the same result when applied to a `CPoint` object.

To test what we have done, let's build a colored point and send it some messages.

```
# p = new CPointM cpointClass;
p = <val> : Object CPointM
# Colored'getC CPointM p;
black : Color
# p1 = Point'bump CPointM p;
p1 = <val> : Object CPointM
```

```
# Point'getX CPointM p1;
1 : Int
# Colored'getC CPointM p1;
blue : Color
```

Note that sending our colored point the `bump` method has the effect of changing its color to blue: the overriden behavior of the `setX` method is observable in the behavior of `bump` method, even though `bump` was not redefined in the subclass.

3. Syntax

We will return to the implementations of `Class` and `extend2` in Section 5. But first, we turn to the main theoretical development of the paper: the formal presentation and basic analysis of the typed λ-calculus in which we are working. We treat the typing and subtyping relations of the calculus formally, leaving equality between terms informal. (The intended intuition is that we have ordinary beta-reduction for both term and type applications. Reduction is studied formally in [Compagnoni, 1995].)

3.1. *Typing Rules*

We now present the rules for kinding, subtyping, and typing in $F^{\omega}_{\wedge}$. They are organized as proof systems for four interdependent judgement forms:

$\Gamma \vdash \mathrm{ok}$	well-formed context
$\Gamma \vdash T \in K$	well-kinded type
$\Gamma \vdash S \leq T$	subtype
$\Gamma \vdash e \in T$	well-typed term.

We sometimes use the metavariable Σ to range over statements (right-hand sides of judgements) of any of these four forms.

Most of the rules include premises of two rather different sorts: *structural premises*, which play an essential role in giving the rule its intended semantic force, and *well-formation premises*, which ensure that the entities named in the rule are of the expected sorts. In an algorithmic presentation of the system (on which an implementation might be based), the well-formation premises would be replaced by the meta-theoretic observation that "recursive calls" in the premises of all the rules preserve the well-formedness of the "arguments" named in the conclusion.

In the interest of brevity, we omit well-formation premises that can be derived from others. For example, in the rule S-Arrow, we drop the premise $\Gamma \vdash T_1 \to T_2 \in \star$, since it follows from $\Gamma \vdash S_1 \to S_2 \in \star$ using the properties proved in Section 3.2.

3.1.1. *Notation* The *kinds* of $F^{\omega}_{\wedge}$ are those of F^{ω}: the kind $\star$ of types and the kinds $K_1 \to K_2$ of functions on types (sometimes called type operators).

$$
\begin{array}{rcll}
K & ::= & \star & \text{types} \\
 & & K \to K & \text{type operators}
\end{array}
$$

The language of *types* of $F^{\omega}_{\wedge}$ is a straightforward higher-order extension of $F_{\leq}$, Cardelli and Wegner's second-order calculus of bounded quantification. Like $F_{\leq}$, it includes type variables (written X), function types ($T \rightarrow T'$), and polymorphic types ($\mathrm{All}\,(X \leq T{:}K)\,T'$), in which the bound type variable X ranges over all subtypes of the upper bound T. Moreover, like F^{ω}, we allow types to be abstracted on types ($\mathrm{Fun}\,(X{:}K)\,T$) and applied to argument types ($T\,T'$); in effect, these forms introduce a simply typed λ-calculus at the level of types. Finally, we allow arbitrary finite intersections ($\bigwedge^K [T_1..T_n]$), where all the T_i's are members of the same kind K.

$$
\begin{array}{lcll}
T & ::= & X & \text{type variable} \\
 & & T \rightarrow T & \text{function type} \\
 & & \mathrm{All}\,(X \leq T{:}K)\,T & \text{polymorphic type} \\
 & & \mathrm{Fun}\,(X{:}K)\,T & \text{operator abstraction} \\
 & & T\,T & \text{operator application} \\
 & & \bigwedge^K [T..T] & \text{intersection at kind } K
\end{array}
$$

We use the abbreviations $\top^K$ and $S \wedge^K T$ for nullary and binary intersection:

$$
\begin{array}{lcl}
\top^K & \triangleq & \bigwedge^K [\,] \\
S \wedge^K T & \triangleq & \bigwedge^K [S, T]
\end{array}
$$

We drop the maximal type *Top* of $F_{\leq}$, since its role is played here by the empty intersection $\top^{\star}$.

For technical convenience, we provide kind annotations on bound variables and intersections so that every type has an "obvious kind," which can be read off directly from its structure and the kind declarations in the context, and to distinguish the empty intersection at different kinds. In examples, however, we often omit these kind annotations. Our implementation includes a simple form of "kind inference" to support this convention. Also, we omit existential types and records from our formal treatment; existentials can be encoded in terms of universal quantifiers, and records can be treated using standard techniques [Reynolds, 1988].

The language of terms includes the variables (x), functional abstractions ($\mathrm{fun}\,(x{:}T)\,e$), and applications ($e\,e$) of the simply typed λ-calculus, plus the type abstraction and application ($\mathrm{fun}\,(X \leq T{:}K)\,e$ and $e\,T$) of F^{ω}, where, as in $F_{\leq}$, each type variable is given an upper bound at the point where it is introduced.

$$
\begin{array}{lcll}
e & ::= & x & \text{variable} \\
 & & \mathrm{fun}\,(x{:}T)\,e & \text{abstraction} \\
 & & e\,e & \text{application} \\
 & & \mathrm{fun}\,(X \leq T{:}K)\,e & \text{type abstraction} \\
 & & e\,T & \text{type application} \\
 & & \mathrm{for}\,(X \in T..T)\,e & \text{alternation}
\end{array}
$$

Intersection types are introduced by expressions of the form "$\mathrm{for}\,(X \in T_1..T_n)\,e$," which can be read as instructions to the typechecker to analyze the expression e separately under the assumptions $X \equiv T_1$, $X \equiv T_2$, $\ldots$, etc. and conjoin the results. For example, if $+ \in \text{Int}{\rightarrow}\text{Int}{\rightarrow}\text{Int} \wedge \text{Real}{\rightarrow}\text{Real}{\rightarrow}\text{Real}$, then we can derive

$$\text{for}\,(X \in \text{Int},\ \text{Real})\ \ \text{fun}\,(x{:}X)\ \ x + x \quad \in \quad \text{Int}{\rightarrow}\text{Int} \wedge \text{Real}{\rightarrow}\text{Real}.$$

(The "for" construct is not actually needed in our implementation of multiple inheritance, since we only use intersections to constrain one type to be a subtype of two others simultaneously. We include it here to complete the definition of the term language, since we are also interested in $F^{\omega}_{\wedge}$ in its own right.)

A *context* Γ is a finite sequence of typing and subtyping assumptions for a set of variables and type variables. The empty context is written $\emptyset$.

$\emptyset$	empty context
$\Gamma,\ x{:}T$	term variable declaration
$\Gamma,\ X{\leq}T{:}K$	type variable declaration

When writing nonempty contexts, we omit the initial $\emptyset$. The domain of Γ is written $\text{dom}(\Gamma)$. The functions $\text{FV}(\text{—})$ and $\text{FTV}(\text{—})$ give the sets of free variables and free type variables of a term, type, or context. Since we are careful to ensure that no variable is bound more than once, we sometimes abuse notation and consider contexts as finite functions: $\Gamma(X)$ yields the bound of X in Γ, where X is implicitly asserted to be in $\text{dom}(\Gamma)$.

Types, terms, contexts, statements, and derivations that differ only in the names of bound variables are considered identical. (The underlying idea is that bound variables are de Bruijn indexes [de Bruijn, 1972]).

The capture avoiding substitution of S for X in T is written $T[X{\leftarrow}S]$. Substitution is written similarly for terms, and is extended pointwise to contexts.

The usual one-step β-reduction of a type S to a type T is written $\rightarrow_{\beta}$. Conversion is written $=_{\beta}$.

3.1.2. *Contexts* The rules for well-formed contexts are the usual ones: a start rule for the empty context and rules allowing a given well-formed context to be extended with either a term variable binding or a type variable binding.

$$\emptyset \vdash \text{ok} \tag{C-Empty}$$

$$\frac{\Gamma \vdash T \in \star \qquad x \notin \text{dom}(\Gamma)}{\Gamma,\ x{:}T \vdash \text{ok}} \tag{C-Var}$$

$$\frac{\Gamma \vdash T \in K \qquad X \notin \text{dom}(\Gamma)}{\Gamma,\ X{\leq}T{:}K \vdash \text{ok}} \tag{C-TVar}$$

3.1.3. *Type Formation* For each type constructor, we give a rule specifying how it can be used to build well-formed type expressions. The critical rules are K-OAbs and K-OApp, which form type abstractions and type applications (essentially as in a simply typed λ-calculus).

The well-formedness premise $\Gamma \vdash \text{ok}$ in K-MEET (and in T-MEET below) is required for the case where $n = 0$.

$$\frac{\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash \text{ok}}{\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash X \in K} \qquad \text{(K-TVAR)}$$

$$\frac{\Gamma \vdash T_1 \in \star \qquad \Gamma \vdash T_2 \in \star}{\Gamma \vdash T_1{\rightarrow}T_2 \in \star} \qquad \text{(K-ARROW)}$$

$$\frac{\Gamma,\, X{\leq}T_1{:}K_1 \vdash T_2 \in \star}{\Gamma \vdash \text{All}\,(X{\leq}T_1{:}K_1)\,T_2 \in \star} \qquad \text{(K-ALL)}$$

$$\frac{\Gamma,\, X{\leq}\top^{K_1}{:}K_1 \vdash T_2 \in K_2}{\Gamma \vdash \text{Fun}\,(X{:}K_1)\,T_2 \in K_1{\rightarrow}K_2} \qquad \text{(K-OABS)}$$

$$\frac{\Gamma \vdash S \in K_1{\rightarrow}K_2 \qquad \Gamma \vdash T \in K_1}{\Gamma \vdash S\,T \in K_2} \qquad \text{(K-OAPP)}$$

$$\frac{\Gamma \vdash \text{ok} \qquad \text{for each } i,\ \Gamma \vdash T_i \in K}{\Gamma \vdash \bigwedge^K [T_1..T_n] \in K} \qquad \text{(K-MEET)}$$

3.1.4. *Subtyping* The rules defining the subtype relation are a natural extension of familiar calculi of bounded quantification. Aside from some extra well-formedness conditions, the rules S-TRANS, S-TVAR, S-ARROW, and S-ALL are the same as in the usual, second-order case. Rules S-OABS and S-OAPP extend the subtype relation pointwise to kinds other than $\star$.

The rule S-CONV embeds β-conversion of types in the subtyping relation and gives reflexivity of subtyping as a special case.

The rule S-ALL compares the bodies of two quantifiers assuming that the bounds are identical. In other words, we use the "Kernel Fun" variant of quantifier subtyping originally proposed by Cardelli and Wegner instead of the more powerful "full $F_\leq$ rule" [Curien and Ghelli, 1992]. The kernel fun variant is powerful enough for our purposes and has better syntactic properties.

Rules S-MEET-G and S-MEET-LB specify that an intersection of a set of types is their order-theoretic greatest lower bound. The rules S-MEET-ARROW, S-MEET-ALL, S-MEET-OABS, and S-MEET-OAPP allow intersections to distribute with the other operators.

As usual in systems with intersection types, the distributive laws S-MEET-ARROW through S-MEET-OAPP are actually equivalences: for each constructor, the opposite direction can be proved using S-MEET-LB, S-MEET-G, the subtyping law for that constructor, and Proposition 3.2.6.

$$\frac{\Gamma \vdash S \in K \qquad \Gamma \vdash T \in K' \qquad S =_\beta T}{\Gamma \vdash S \leq T} \qquad \text{(S-CONV)}$$

$$\frac{\Gamma \vdash S \leq T \qquad \Gamma \vdash T \leq U}{\Gamma \vdash S \leq U} \tag{S-Trans}$$

$$\frac{\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash \mathrm{ok}}{\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash X \leq T} \tag{S-TVar}$$

$$\frac{\Gamma \vdash T_1 \leq S_1 \qquad \Gamma \vdash S_2 \leq T_2 \qquad \Gamma \vdash S_1{\rightarrow}S_2 \in \star}{\Gamma \vdash S_1{\rightarrow}S_2 \leq T_1{\rightarrow}T_2} \tag{S-Arrow}$$

$$\frac{\Gamma,\, X{\leq}U{:}K_1 \vdash S_2 \leq T_2 \qquad \Gamma \vdash \mathrm{All}\,(X{\leq}U{:}K_1)\, S_2 \in \star}{\Gamma \vdash \mathrm{All}\,(X{\leq}U{:}K_1)\, S_2 \leq \mathrm{All}\,(X{\leq}U{:}K_1)\, T_2} \tag{S-All}$$

$$\frac{\Gamma,\, X{\leq}\top^K{:}K \vdash S \leq T}{\Gamma \vdash \mathrm{Fun}\,(X{:}K)\, S \leq \mathrm{Fun}\,(X{:}K)\, T} \tag{S-OAbs}$$

$$\frac{\Gamma \vdash S \leq T \qquad \Gamma \vdash S\,U \in K}{\Gamma \vdash S\,U \leq T\,U} \tag{S-OApp}$$

$$\frac{\text{for each } i,\; \Gamma \vdash S \leq T_i \qquad \Gamma \vdash S \in K}{\Gamma \vdash S \leq \bigwedge^K[T_1..T_n]} \tag{S-Meet-G}$$

$$\frac{\Gamma \vdash \bigwedge^K[T_1..T_n] \in K}{\Gamma \vdash \bigwedge^K[T_1..T_n] \leq T_i} \tag{S-Meet-LB}$$

$$\frac{\Gamma \vdash S \rightarrow \bigwedge^\star[T_1..T_n] \in \star}{\Gamma \vdash \bigwedge^\star[S{\rightarrow}T_1 \;..\; S{\rightarrow}T_n] \leq S \rightarrow \bigwedge^\star[T_1..T_n]} \tag{S-Meet-Arrow}$$

$$\frac{\Gamma \vdash \mathrm{All}\,(X{\leq}S{:}K)\; \bigwedge^\star[T_1..T_n] \in \star}{\Gamma \vdash \bigwedge^\star[\mathrm{All}\,(X{\leq}S{:}K)\, T_1 \;..\; \mathrm{All}\,(X{\leq}S{:}K)\, T_n] \leq \mathrm{All}\,(X{\leq}S{:}K)\; \bigwedge^\star[T_1..T_n]} \tag{S-Meet-All}$$

$$\frac{\Gamma \vdash \mathrm{Fun}\,(X{:}K_1)\; \bigwedge^{K_2}[T_1..T_n] \in K}{\Gamma \vdash \bigwedge^K[\mathrm{Fun}\,(X{:}K_1)\, T_1 \;..\; \mathrm{Fun}\,(X{:}K_1)\, T_n] \leq \mathrm{Fun}\,(X{:}K_1)\; \bigwedge^{K_2}[T_1..T_n]} \tag{S-Meet-OAbs}$$

$$\frac{\Gamma \vdash \bigwedge^{K_1}[T_1..T_n]\, U \in K}{\Gamma \vdash \bigwedge^K[T_1\,U \;..\; T_n\,U] \leq \bigwedge^{K_1}[T_1..T_n]\, U} \tag{S-Meet-OApp}$$

3.1.5. *Term Formation* Except for T-Meet and T-For, the term formation rules are precisely those of the second-order calculus of bounded quantification. T-For provides for typechecking under any of a set of alternate assumptions. For each S_i, the type derived for the instance of the body e when X is replaced by S_i is a valid type of the for expression itself. The T-Meet rule can then be used to collect these separate typings into a single intersection. Type-theoretically, T-Meet is the introduction rule for the $\wedge$ constructor; the corresponding elimination rule need not be given explicitly, since it follows from T-SUBSUMPTION and S-MEET-LB. F^{ω}'s rule of type conversion (if $\Gamma \vdash e \in T$ and $\Gamma \vdash T' \in K$, with $T =_{\beta} T'$, then $\Gamma \vdash e \in T'$) is admissible (using subsumption, Proposition 3.2.13, and S-CONV).

$$\frac{\Gamma_1,\, x{:}T,\, \Gamma_2 \vdash \mathrm{ok}}{\Gamma_1,\, x{:}T,\, \Gamma_2 \vdash x \in T} \qquad \text{(T-VAR)}$$

$$\frac{\Gamma,\, x{:}T_1 \vdash e \in T_2}{\Gamma \vdash \mathrm{fun}\,(x{:}T_1)\, e \in T_1 \rightarrow T_2} \qquad \text{(T-ABS)}$$

$$\frac{\Gamma \vdash f \in T_1 \rightarrow T_2 \qquad \Gamma \vdash a \in T_1}{\Gamma \vdash f\, a \in T_2} \qquad \text{(T-APP)}$$

$$\frac{\Gamma,\, X {\leq} T_1{:}K_1 \vdash e \in T_2}{\Gamma \vdash \mathrm{fun}\,(X {\leq} T_1{:}K_1)\, e \in \mathrm{All}\,(X {\leq} T_1{:}K_1)\, T_2} \qquad \text{(T-TABS)}$$

$$\frac{\Gamma \vdash f \in \mathrm{All}\,(X {\leq} T_1{:}K_1)\, T_2 \qquad \Gamma \vdash S \leq T_1}{\Gamma \vdash f\, S \in T_2[X \leftarrow S]} \qquad \text{(T-TAPP)}$$

$$\frac{\Gamma \vdash e[X \leftarrow S] \in T \qquad S \in \{S_1..S_n\}}{\Gamma \vdash \mathrm{for}\,(X \in S_1..S_n)\, e \in T} \qquad \text{(T-FOR)}$$

$$\frac{\Gamma \vdash \mathrm{ok} \qquad \text{for each } i,\ \Gamma \vdash e \in T_i}{\Gamma \vdash e \in \bigwedge^{\star}[T_1..T_n]} \qquad \text{(T-MEET)}$$

$$\frac{\Gamma \vdash e \in S \qquad \Gamma \vdash S \leq T}{\Gamma \vdash e \in T} \qquad \text{(T-SUBSUMPTION)}$$

3.2. *Basic Properties*

This section establishes a number of structural properties of the definition of $F^{\omega}_{\wedge}$. These properties do not constitute a complete metatheoratic study of $F^{\omega}_{\leq}$ (cf. [Compagnoni, 1994, Compagnoni, 1995]), but just enough to proceed with the sematics in Section 4. Except where noted, the proofs proceed by structural induction, and are straightforward when performed in the order given.

Lemma 3.2.1. If $\Gamma \vdash \Sigma$ and Γ_1 is a prefix of Γ, then $\Gamma_1 \vdash \mathrm{ok}$ as a subderivation. Moreover, except for the case $\Gamma_1 \equiv \Gamma$ and $\Sigma \equiv \mathrm{ok}$, the subderivation is strictly shorter.

Lemma 3.2.2. (Syntax-directedness of context judgements)

1 If $\Gamma_1,\, X {\leq} T{:}K,\, \Gamma_2 \vdash \mathrm{ok}$, then $\Gamma_1 \vdash T \in K$ by a proper subderivation.
2 If $\Gamma_1,\, x{:}T,\, \Gamma_2 \vdash \mathrm{ok}$, then $\Gamma_1 \vdash T \in \star$ by a proper subderivation.

Lemma 3.2.3. (Free variables) $\Gamma \vdash T \in K$ implies $FTV(T) \subseteq \mathrm{dom}(\Gamma)$.

Lemma 3.2.4. (Weakening/permutation) Let Γ and Γ' be contexts such that $\Gamma \subseteq \Gamma'$ and $\Gamma' \vdash \mathrm{ok}$. Then $\Gamma \vdash \Sigma$ implies $\Gamma' \vdash \Sigma$.

Proof. By induction on the length of a derivation of $\Gamma \vdash \Sigma$.

K-OABS We are given that $\Gamma,\ X{\leq}\top^{K_1}{:}K_1 \vdash T_2 \in K_2$. Applying K-MEET to $\Gamma' \vdash \mathrm{ok}$ we obtain $\Gamma' \vdash \top^{K_1} \in K_1$; we can assume, without loss of generality, that $X \notin \mathrm{dom}(\Gamma')$. Then, by C-TVAR, $\Gamma',\ X{\leq}\top^{K_1}{:}K_1 \vdash \mathrm{ok}$. By the induction hypothesis, $\Gamma',\ X{\leq}\top^{K_1}{:}K_1 \vdash T_2 \in K_2$, and the result follows applying K-OABS.

T-ABS We are given that $\Gamma,\ x{:}T_1 \vdash e \in T_2$. By Lemma 3.2.1 there exists a proper subderivation of $\Gamma,\ x{:}T_1 \vdash \mathrm{ok}$; by Lemma 3.2.2, there is a yet shorter subderivation of $\Gamma \vdash T_1 \in \star$. Now we can apply the induction hypothesis to obtain $\Gamma' \vdash T_1 \in \star$. As before, we can assume $x \notin \mathrm{dom}(\Gamma')$; by C-VAR, $\Gamma',\ x{:}T_1 \vdash \mathrm{ok}$. By the induction hypothesis we have $\Gamma',\ x{:}T_1 \vdash e \in T_2$, and applying T-ABS yields the desired result.

Other cases If $\Sigma \equiv \mathrm{ok}$ there is nothing to prove. K-TVAR, S-TVAR, T-MEET and T-VAR applying the corresponding rule to $\Gamma' \vdash \mathrm{ok}$. S-OABS is similar to K-OABS. K-ALL, S-ALL, T-TABS are similar to T-ABS. All the other cases follow by straightforward application of the induction hypothesis.

□

Lemma 3.2.5. (Context, kind, and term strengthening)

1 If $\Gamma_1,\ X{\leq}T{:}K,\ \Gamma_2 \vdash \mathrm{ok}$ and $X \notin \mathrm{FTV}(\Gamma_2)$, then $\Gamma_1,\ \Gamma_2 \vdash \mathrm{ok}$.

2 If $\Gamma_1,\ X{\leq}T{:}K,\ \Gamma_2 \vdash S \in K'$ and $X \notin \mathrm{FTV}(\Gamma_2) \cup \mathrm{FTV}(S)$, then $\Gamma_1,\ \Gamma_2 \vdash S \in K'$.

3 If $\Gamma_1,\ x{:}T,\ \Gamma_2 \vdash \Sigma$ and $x \notin \mathrm{FV}(\Sigma)$, then $\Gamma_1,\ \Gamma_2 \vdash \Sigma$.

Moreover, the derivations of the conclusions are strictly shorter than the derivation of the premises.

Proof. Parts 1 and 2 are proved by simultaneous induction on the length of derivations. Part 3 is proved by induction on the derivation of $\Gamma_1,\ x{:}T,\ \Gamma_2 \vdash \Sigma$.

1 C-EMPTY Vacuously true.

C-VAR By part 2 of the induction hypothesis and C-VAR.

C-TVAR $\Gamma_2 \equiv \emptyset$ The result follows from Lemma 3.2.1.

$\Gamma_2 \not\equiv \emptyset$ By part 2 of the induction hypothesis and C-TVAR.

2 K-TVAR By part 1 of the induction hypothesis and K-TVAR.

K-ARROW By part 2 of the induction hypothesis and K-ARROW.

K-ALL We are given that $\Gamma_1,\ X{\leq}T{:}K,\ \Gamma_2,\ Y{\leq}T_1{:}K_1 \vdash T_2 \in \star$, and $X \notin \mathrm{FTV}(\Gamma_2) \cup \mathrm{FTV}(\mathrm{All}(Y{\leq}T_1{:}K_1)\,T_2)$. In particular, $X \notin \mathrm{FTV}(T_1) \cup \mathrm{FTV}(T_2) - \{Y\}$. By our convention that names of bound variables are considered inessential, we may assume $X \not\equiv Y$. Then $X \notin \mathrm{FTV}(\Gamma_2,\ Y{\leq}T_1{:}K_1) \cup \mathrm{FTV}(T_2)$. Applying part 2 of the induction hypothesis and K-ALL the result follows.

K-OABS Similar to the case K-ALL.

K-OAPP By part 2 of the induction hypothesis and K-OAPP.

K-MEET By parts 1 and 2 of the induction hypothesis and K-OAPP.

3 Except for the cases we will consider below and the case for C-Empty, which is trivially true, the result follows by straightforward application of part 3 of the induction hypothesis and the corresponding rule in each case.

C-Var $\Gamma_2 \equiv \emptyset$ The result follows by Lemma 3.2.1.

$\Gamma_2 \not\equiv \emptyset$ By part 3 of the induction hypothesis and C-Var.

T-Abs Using part 3 of the induction hypothesis and T-Abs.

T-For Using that $\mathrm{FV}(e) = \mathrm{FV}(e[X\leftarrow S])$, part 3 of the induction hypothesis, and T-For.

□

Proposition 3.2.6. (Syntax-directedness of kinding)

1 $\Gamma \vdash X \in K$ implies $\Gamma \equiv \Gamma_1,\ X{\leq}T{:}K,\ \Gamma_2$ for some Γ_1, T, and Γ_2.
2 $\Gamma \vdash T_1{\rightarrow}T_2 \in K$ implies $K \equiv \star$ and $\Gamma \vdash T_1, T_2 \in \star$.
3 $\Gamma \vdash \mathrm{All}\,(X{\leq}T_1{:}K_1)\,T_2 \in K$ implies $K \equiv \star$ and $\Gamma,\ X{\leq}T_1{:}K_1 \vdash T_2 \in \star$.
4 $\Gamma \vdash \mathrm{Fun}\,(X{:}K_1)\,T_2 \in K$ implies $K \equiv K_1{\rightarrow}K_2$ and $\Gamma,\ X{\leq}\top^{K_1}{:}K_1 \vdash T_2 \in K_2$, for some K_2.
5 $\Gamma \vdash S\,T \in K$ implies $\Gamma \vdash S \in K'{\rightarrow}K$ and $\Gamma \vdash T \in K'$, for some K'.
6 $\Gamma \vdash \bigwedge^K [T_1..T_n] \in K'$ implies $K \equiv K'$ and $\Gamma \vdash \mathrm{ok}$ and $\Gamma \vdash T_i \in K$ for each i.

Moreover, the proofs of the consequents are all strictly shorter than the antecedents.

Proof. By inspection. □

Lemma 3.2.7. (Uniqueness of kinds) $\Gamma \vdash T \in K$ and $\Gamma \vdash T \in K'$, then $K \equiv K'$.

Lemma 3.2.8. (Type substitution) Let $\Gamma_1 \vdash T \in K_U$. (The subscript U of the metavariable K_U stands as a reminder that this is also the kind of the type U.) Then

1 If $\Gamma_1,\ X{\leq}U{:}K_U,\ \Gamma_2 \vdash S \in K_S$, then $\Gamma_1,\ \Gamma_2[X\leftarrow T] \vdash S[X\leftarrow T] \in K_S$.
2 If $\Gamma_1,\ X{\leq}U{:}K_U,\ \Gamma_2 \vdash \mathrm{ok}$, then $\Gamma_1,\ \Gamma_2[X\leftarrow T] \vdash \mathrm{ok}$.

Proof. By simultaneous induction on derivations of the premises. The proof of part 2 is straightforward using part 1 of the induction hypothesis. We consider the details of the proof of 1. The cases K-Arrow, K-All, K-OAbs, and K-OApp follow by straightforward application of part 1 of the induction hypothesis and the corresponding rule, while the case of K-Meet also uses part 2 of the induction hypothesis. Now take the case of K-TVar, where $S \equiv Y$ for some variable Y. By Proposition 3.2.6(1) $Y{\leq}T_Y{:}K_S \in (\Gamma_1,\ X{\leq}U{:}K_U,\ \Gamma_2)$ for some T_Y. There are three cases to consider.

$Y{\leq}T_Y{:}K_S \in \Gamma_1$ Then we also have $Y{\leq}T_Y{:}K_S \in (\Gamma_1,\ \Gamma_2[X\leftarrow T])$. By part 2 of the induction hypothesis, $\Gamma_1,\ \Gamma_2[X\leftarrow T] \vdash \mathrm{ok}$. Applying K-TVar, we get $\Gamma_1,\ \Gamma_2[X\leftarrow T] \vdash Y \in K_S$.

$Y{\leq}T_Y{:}K_S \equiv X{\leq}U{:}K_U$ We know that $\Gamma_1 \vdash T \in K_S \equiv K_U$. From the premise of K-TVar and part 2 of the induction hypothesis, we have $\Gamma_1,\ \Gamma_2[X\leftarrow T] \vdash \mathrm{ok}$. The result follows by weakening (3.2.4).

$Y{\leq}T_Y{:}K_S \in \Gamma_2$ Then we have $Y{\leq}T_Y[X\leftarrow T]{:}K_S \in (\Gamma_1,\ \Gamma_2[X\leftarrow T])$. By part 2 of the induction hypothesis, $\Gamma_1,\ \Gamma_2[X\leftarrow T] \vdash \mathrm{ok}$, from which the result follows from K-TVar.

□

Lemma 3.2.9. (Subject reduction for kinding judgements) If $S \twoheadrightarrow_\beta T$ and $\Gamma \vdash S \in K$, then $\Gamma \vdash T \in K$.

Proof. In order to prove this result it is enough to prove the following statements by simultaneous induction on the derivation of $\Gamma \vdash S \in K$. The rest follows by induction on the definition of $\twoheadrightarrow_\beta$.

1 $\Gamma \vdash$ ok and $\Gamma \rightarrow_\beta \Gamma'$ implies $\Gamma' \vdash$ ok.
2 $\Gamma \vdash S \in K$ and $S \rightarrow_\beta T$ implies $\Gamma \vdash T \in K$.
3 $\Gamma \vdash S \in K$ and $\Gamma \rightarrow_\beta \Gamma'$ implies $\Gamma' \vdash S \in K$.

□

Theorem 3.2.10. (Kind invariance under type conversion) If $\Gamma \vdash S \in K_S$ and $\Gamma \vdash T \in K_T$, with $S =_\beta T$, then $K_S \equiv K_T$.

Proof. By the (standard) Church-Rosser property for beta-conversion, there exists U such that $S \twoheadrightarrow_\beta U$ and $T \twoheadrightarrow_\beta U$, and the result follows by subject reduction and uniqueness of kinds. □

Lemma 3.2.11. (Context modification) If $\Gamma_1 \vdash U' \in K$ and Σ is either ok or $T \in K'$, then $\Gamma_1,\, X{\leq}U{:}K,\, \Gamma_2 \vdash \Sigma$ implies $\Gamma_1,\, X{\leq}U'{:}K,\, \Gamma_2 \vdash \Sigma$.

Proposition 3.2.12. (Well-kindedness of subtyping) If $\Gamma \vdash S \leq T$, then $\Gamma \vdash S \in K$ and $\Gamma \vdash T \in K$ for some K.

Proof. By induction on the derivation of $\Gamma \vdash S \leq T$.

S-Conv We are given that $\Gamma \vdash S \in K$ and $\Gamma \vdash T \in K'$ and $S =_\beta T$. By Lemma 3.2.10, $K \equiv K'$.

S-Trans By induction hypothesis and uniqueness of kinds (3.2.7).

S-TVar We are given $\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash$ ok. By K-TVar we get $\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash X \in K$. Moerover, by Lemma 3.2.2, $\Gamma_1 \vdash T \in K$, and by Lemma 3.2.4, $\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash T \in K$.

S-Arrow We are given $\Gamma \vdash T_1 \leq S_1$ and $\Gamma \vdash S_2 \leq T_2$ and $\Gamma \vdash S_1{\rightarrow}S_2 \in \star$. By Proposition 3.2.6 $\Gamma \vdash S_1, S_2 \in \star$. Further, by the induction hypothesis together with uniqueness of kinds (3.2.7), we have $\Gamma \vdash T_1, T_2 \in \star$. Finally, applying K-Arrow, the result follows.

S-All We are given that $\Gamma,\, X{\leq}U{:}K_1 \vdash S_2 \leq T_2$ and $\Gamma \vdash \mathrm{All}\,(X{\leq}U{:}K_1)\, S_2 \in \star$. By the induction hypothesis, there is some K_2 such that $\Gamma,\, X{\leq}U{:}K_1 \vdash S_2 \in K_2$ and $\Gamma,\, X{\leq}U{:}K_1 \vdash T_2 \in K_2$. By Proposition 3.2.6, $\Gamma,\, X{\leq}U{:}K_1 \vdash S_2 \in \star$, and by the uniqueness of kinds, $K_2 \equiv \star$, from which the result follows by applying K-All.

S-OAbs By induction hypothesis and K-OAbs.

S-OApp Similar to S-All.

S-Meet-G Using the induction hypothesis, Lemma 3.2.7, and K-Meet.

S-Meet-LB We are given $\Gamma \vdash \bigwedge^K[T_1..T_n] \in K$, which, by Proposition 3.2.6, implies $\Gamma \vdash T_i \in K$ for each i.

S-Meet-All We are given $\Gamma \vdash \mathrm{All}\,(X{\leq}S{:}K)\, \bigwedge^\star[T_1..T_n] \in \star$. We have to consider two cases.

$n = 0$ By Lemma 3.2.1, it follows that $\Gamma \vdash$ ok, and by K-Meet, $\Gamma \vdash \top^\star \in \star$.

$n \neq 0$ By Proposition 3.2.6 we have $\Gamma \vdash S \in K$ and $\Gamma,\ X{\leq}\top^K{:}K \vdash T_i \in \star$ for every i, which, by K-All, yields $\Gamma \vdash \mathrm{All}\,(X{\leq}S{:}K)\,T_i \in \star$ for each i. Finally, applying K-Meet the result follows.

Other cases The arguments for S-Meet-Arrow, S-Meet-OApp, and S-Meet-OAbs are similar to previous case.

□

Proposition 3.2.13. (Well-kindedness of typing) If $\Gamma \vdash e \in T$, then $\Gamma \vdash T \in \star$.

Proof. By induction on the derivation of $\Gamma \vdash e \in T$.

T-Var We are given $\Gamma_1,\ x{:}T,\ \Gamma_2 \vdash \mathrm{ok}$. The result follows by Lemma 3.2.2 and Lemma 3.2.4.

T-Abs We are given $\Gamma,\ x{:}T_1 \vdash e \in T_2$. By induction hypothesis $\Gamma,\ x{:}T_1 \vdash T_2 \in \star$. By Lemma 3.2.5, it follows that $\Gamma \vdash T_2 \in \star$. On the other hand, by Lemmas 3.2.1 and 3.2.2, $\Gamma \vdash T_1 \in \star$. Hence, K-Arrow yields $\Gamma \vdash T_1{\rightarrow}T_2 \in \star$.

T-App By induction hypothesis on $\Gamma \vdash f \in T_1{\rightarrow}T$ and Proposition 3.2.6.

T-TAbs We are given $\Gamma,\ X{\leq}T_1{:}K_1 \vdash e \in T_2$. By the induction hypothesis, $\Gamma,\ X{\leq}T_1{:}K_1 \vdash T_2 \in \star$. We obtain $\Gamma \vdash \mathrm{All}\,(X{\leq}T_1{:}K_1)\,T_2 \in \star$ by applying K-All .

T-TApp We know that $\Gamma \vdash f \in \mathrm{All}\,(X{\leq}T_1{:}K_1)\,T_2$ and also $\Gamma \vdash S \leq T_1$. By the induction hypothesis, $\Gamma \vdash \mathrm{All}\,(X{\leq}T_1{:}K_1)\,T_2 \in \star$ and, by proposition 3.2.6, $\Gamma,\ X{\leq}T_1{:}K_1 \vdash T_2 \in \star$. By lemmas 3.2.1 and 3.2.2, there exists a derivation of $\Gamma \vdash T_1 \in K_1$. By the well-kindedness of subtyping (proposition 3.2.12) and uniqueness of kinds (lemma 3.2.7), we have $\Gamma \vdash S \in K_1$. Then, by the type substitution lemma (lemma 3.2.8), $\Gamma \vdash T_2[X{\leftarrow}S] \in \star$.

T-For By induction hypothesis.

T-Meet We are given that $\Gamma \vdash \mathrm{ok}$ and that $\Gamma \vdash e \in T_i$ for each i. We have to consider two cases.

$n = 0$ Applying K-Meet to $\Gamma \vdash \mathrm{ok}$ we obtain $\Gamma \vdash \top^\star \in \star$.

$n \neq 0$ By the induction hypothesis, $\Gamma \vdash T_i \in \star$ for every i and, applying K-Meet, the result follows.

T-Subsumption By induction hypothesis using Proposition 3.2.12 and Lemma 3.2.7.

□

4. Semantics

Among simplest models for typed λ-calculi are those based on partial equivalence relations (PERs). A model in this style is essentially untyped: terms are interpreted by erasing all type information and interpreting the resulting pure λ-term as an element of the model. A type, in this setting, is just a subset of the model along with an appropriate notion of equivalence of elements. Coercions between types are interpreted as inclusion of PERs.

Our PER model for $F^\omega_\wedge$ extends the model of $F_\wedge$ given in [Pierce, 1991], which is based on Bruce and Longo's model for $F_\leq$ [1990]. The usual interpretation of a quantified type $\mathrm{All}\,(X)\,T$ in a PER model is the PER-indexed intersection of all possible instances of T. Bruce and Longo refined this definition to interpret $\mathrm{All}\,(X{\leq}S)\,T$ as the intersection of all the instances of T where X is interpreted as a sub-PER of the interpretation of S. This intuition also serves for intersection types: $\bigwedge^\star[T_1..T_n]$ is interpreted as the intersection of the PERs interpreting each of the T_i's. We generalize this model to ω-order polymorphism (and subtyping) by interpreting type operators as functions over PERs.

To deal correctly with intersection types, we need to make one significant technical departure here from PER models of ordinary bounded quantification: instead of allowing the elements of our PERs to be drawn from the carrier of an arbitrary partial combinatory algebra $\mathcal{D}$, we require that $\mathcal{D}$ be a *total* combinatory algebra. This restriction is needed to validate nullary instances of the distributive law S-Meet-Arrow, which have the form $\Gamma \vdash \top^\star \leq S \to \top^\star$. For example, let $S = \top^\star$. The empty intersection $\top^\star$ is interpreted by the everywhere-defined PER, i.e., $[\![\top^\star]\!]$ relates every m to itself. To validate the distributivity law, it must therefore be the case that $[\![\top^\star \to \top^\star]\!]$ relates every element to itself. But this will only be true if the application of any element to any other element is defined. This observation is due to QingMing Ma [personal communication, 1991].

Cardelli and Longo [1991] and Bruce and Mitchell [1992] have given related models for variants of F^ω with subtyping. (Cardelli and Longo's model interprets subtyping only for kind $\star$, not for type operators; neither model includes intersections.)

The notation and fundamental definitions used here are based on papers of Bruce and Longo [1990], Freyd, Mulry, Rosolini, and Scott [1990], and others. A helpful basic reference for PER models of second-order λ-calculi is [Mitchell, 1990b]; also see [Bruce *et al.*, 1990] for more general discussion of second-order models and [Barendregt, 1984, Hindley and Seldin, 1986] for general discussion of combinatory models.

4.1. *Total Combinatory Algebras*

A *total combinatory algebra* is a tuple $\mathcal{D} = \langle D, \cdot, k, s\rangle$ comprising a set D of *elements*, an *application function* $\cdot$ with type $D \to (D \to D)$, and distinguished elements $k, s \in D$ such that, for all $d_1, d_2, d_3 \in D$,

$$\begin{array}{lcl} k \cdot d_1 \cdot d_2 & = & d_1 \\ s \cdot d_1 \cdot d_2 \cdot d_3 & = & (d_1 \cdot d_3) \cdot (d_2 \cdot d_3). \end{array}$$

Throughout this section, we work with a fixed, but unspecified, total combinatory algebra $\mathcal{D}$. (Cf. [Scott, 1976] for examples.)

The set of *pure λ-terms* is defined by the following grammar:

$$M ::= x \mid \mathrm{fun}\,(x)\,M \mid M_1\ M_2$$

The set of *combinator terms* is:

$$C ::= x \mid C_1\ C_2 \mid K \mid S$$

The *bracket abstraction* of a combinator term C with respect to a variable x, written

$\mathrm{fun}^\star\,(x)\,C$, is defined as follows:

$$\begin{array}{lcll} \mathrm{fun}^\star\,(x)\,C & = & K\,C & \text{when } x \notin \mathrm{FV}(C) \\ \mathrm{fun}^\star\,(x)\,x & = & S\,K\,K & \\ \mathrm{fun}^\star\,(x)\,C_1\,C_2 & = & S\,(\mathrm{fun}^\star\,(x)\,C_1)\,(\mathrm{fun}^\star\,(x)\,C_2) & \text{when } x \in \mathrm{FV}(C_1\,C_2) \end{array}$$

The *combinator translation* of a pure λ-term M, written $|M|$, is defined as follows:

$$\begin{array}{lcl} |x| & = & x \\ |\mathrm{fun}\,(x)\,M| & = & \mathrm{fun}^\star\,(x)\,|M| \\ |M_1\,M_2| & = & |M_1|\,|M_2| \end{array}$$

A *term environment* η is a finite function from term variables to elements of D. When $x \notin \mathrm{dom}(\eta)$, we write $\eta[x{\leftarrow}d]$ for the environment that maps x to d and agrees with η everywhere else. We write $\eta\backslash x$ for the environment like η except that $\eta(x)$ is undefined; $\eta\backslash\Gamma$ is like η but undefined on all the variables in $\mathrm{dom}(\Gamma)$. We say that η' *extends* η when $\mathrm{dom}(\eta) \subseteq \mathrm{dom}(\eta')$ and η and η' agree on $\mathrm{dom}(\eta)$.

Let C be a combinator term and η a term environment such that $\mathrm{FV}(C) \subseteq \mathrm{dom}(\eta)$. Then the *interpretation* of C under η, written $[\![C]\!]_\eta$, is defined as follows:

$$\begin{array}{lcl} [\![x]\!]_\eta & = & \eta(x) \\ [\![C_1\,C_2]\!]_\eta & = & [\![C_1]\!]_\eta \cdot [\![C_2]\!]_\eta \\ [\![K]\!]_\eta & = & k \\ [\![S]\!]_\eta & = & s. \end{array}$$

Lemma 4.1.1.

1 If η' extends η and $\mathrm{FV}(C) \subseteq \mathrm{dom}(\eta)$, then $[\![C]\!]_\eta = [\![C]\!]_{\eta'}$.

2 $[\![\mathrm{fun}^\star\,(x)\,C]\!]_\eta \cdot m = [\![C]\!]_{\eta[x\leftarrow m]}$.

Proof. Standard. □

4.2. *Higher-Order Partial Equivalence Relations*

A *partial equivalence relation* (PER) on a combinatory algebra $\mathcal{D}$ is a symmetric and transitive relation A on D. We write $m\ \{A\}\ n$ when A relates m and n. The *domain* of A, written $\mathrm{dom}(A)$, is the set $\{n \mid n\ \{A\}\ n\}$. (Note that $m\ \{A\}\ n$ implies $m \in \mathrm{dom}(A)$.) We write **PER** for the class of all PERs.

If A and B are relations, then $A \to B$ is the relation where

$$m\ \{A \to B\}\ n \quad \text{iff} \quad p\ \{A\}\ q \quad \text{implies} \quad m{\cdot}p\ \{B\}\ n{\cdot}q \quad \text{for all } p, q \in D.$$

It is not hard to show that $A \to B$ is a PER when A and B are PERs, and that the intersection of any set of PERs is a PER.

To interpret type operators, we need to consider not only PERs, but arbitrary function spaces built on PER. An element of such a function space (including, as a special case, an element of PER itself), is called a *higher-order PER* (HOPER). The interpretation of a kind K is a suitable space of HOPERs:

$$\begin{array}{lcl} [\![\star]\!] & = & \mathbf{PER} \\ [\![K_1{\to}K_2]\!] & = & [\![K_1]\!] \to [\![K_2]\!]. \end{array}$$

We generalize the familiar graph-inclusion of relations to HOPERs as follows:

$$
\begin{array}{lll}
A \subseteq^{\star} B & \text{iff} & A, B \in [\![\star]\!] \text{ and } m\ \{A\}\ n \text{ implies } m\ \{B\}\ n \text{ for all } m, n \in D; \\
A \subseteq^{K_1 \to K_2} B & \text{iff} & A, B \in [\![K_1 \to K_2]\!] \text{ and } A\,P \subseteq^{K_2} B\,P \text{ for all } P \in [\![K_1]\!].
\end{array}
$$

Let $\{A_i \in [\![K]\!]\}_{i \in I}$ be a set of HOPERs indexed by a set I. Then $\bigcap^K_{i \in I} A_i$ is the HOPER defined by

$$
\begin{array}{lll}
m\ \{\bigcap^{\star}_{i \in I} A_i\}\ n & \text{iff} & \text{for every } i,\ m\ \{A_i\}\ n \\
\bigcap^{K_1 \to K_2}_{i \in I} A_i & = & \lambda P {\in} [\![K_1]\!].\ \bigcap^{K_2}_{i \in I} A_i\ P.
\end{array}
$$

Lemma 4.2.1.

1 Each $\subseteq^K$ is transitive.
2 If $A_j \in [\![K]\!]$ for each $j {\in} I$, then $\bigcap^K_{i \in I} A_i \in [\![K]\!]$.
3 If $A \subseteq^K B_j$ for each j, then $A \subseteq^K \bigcap^K_{i \in I} B_i$.
4 $\bigcap^K_{i \in I} A_i \subseteq^K A_j$ for each j.
5 $\bigcap^{\star}_{i \in I} A {\to} B_i \subseteq^{\star} A \to \bigcap^{\star}_{i \in I} B_i$.
6 $\bigcap^{\star}_{i \in I} \bigcap^{\star}_{P \subseteq^K A} B_{i,P} \subseteq^{\star} \bigcap^{\star}_{P \subseteq^K A} \bigcap^{\star}_{i \in I} B_{i,P}$.
7 $\bigcap^{K_1 \to K_2}_{i \in I} \lambda P {\in} [\![K_1]\!].\ B_i\ P \subseteq^{K_1 \to K_2} \lambda P {\in} [\![K_1]\!].\ \bigcap^{K_2}_{i \in I} B_i\ P$, when each $B_i \in [\![K_1 {\to} K_2]\!]$.
8 $\bigcap^{K_2}_{i \in I} A\ B_i \subseteq^{K_2} A\ (\bigcap^{K_1 \to K_2}_{i \in I} B_i)$.

Indeed, in cases 5 through 8 the inclusions are equalities.

Proof. Straightforward. □

Each collection $[\![K]\!]$ of HOPERs has a maximal element under the ordering $\subseteq^K$. This element is written $\top^K$ and can be calculated as follows:

— $\top^{\star}$ is the total relation on $\mathcal{D}$.
— $\top^{K_1 \to K_2} = \lambda P {\in} [\![K_1]\!].\ \top^{K_2}$.

Fact 4.2.2. Let $A \in [\![K]\!]$. Then:

1 $A \subseteq^K \top^K$.
2 $\top^K \subseteq^K A$ implies $A = \top^K$.

4.3. *HOPER Interpretation of $F^{\omega}_{\wedge}$*

An *environment* η is a finite function from type variables to HOPERs and from term variables to elements of D. The notations for environment extension, restriction, and agreement are carried over from term environments. By an abuse of notation, type environments are used in place of term environments from now on.

The *erasure* of an $F^{\omega}_{\wedge}$ term e, written $\mathrm{erase}(e)$, is the pure λ-term defined as follows:

$$
\begin{array}{lcl}
\mathrm{erase}(x) & = & x \\
\mathrm{erase}(\mathrm{fun}\,(x{:}T)\,e) & = & \mathrm{fun}\,(x)\,\mathrm{erase}(e) \\
\mathrm{erase}(e_1\ e_2) & = & \mathrm{erase}(e_1)\ \mathrm{erase}(e_2) \\
\mathrm{erase}(\mathrm{fun}\,(X{\leq}T{:}K)\,e) & = & \mathrm{erase}(e) \\
\mathrm{erase}(e\ T) & = & \mathrm{erase}(e) \\
\mathrm{erase}(\mathrm{for}\,(X{\in}T_1..T_n)\,e) & = & \mathrm{erase}(e).
\end{array}
$$

Let η be a term environment and e an expression such that $\mathrm{FV}(e) \subseteq \mathrm{dom}(\eta)$. Then the *interpretation* of e under η, written $[\![e]\!]_\eta$, is $[\![|\mathrm{erase}(e)|]\!]_\eta$.

If η is an environment and T a type expression such that $\mathrm{FTV}(T) \subseteq \mathrm{dom}(\eta)$, then the *interpretation* of T under η, written $[\![T]\!]_\eta$, is the HOPER defined as follows:

$$
\begin{array}{lcl}
[\![X]\!]_\eta & = & \eta(X) \\
[\![T_1 \to T_2]\!]_\eta & = & [\![T_1]\!]_\eta \to [\![T_2]\!]_\eta \\
[\![\mathrm{All}\,(X{\leq}T_1{:}K_1)\,T_2]\!]_\eta & = & \bigcap^{\star}_{P \subseteq^{K_1} [\![T_1]\!]_\eta} [\![T_2]\!]_{\eta[X \leftarrow P]} \\
[\![\bigwedge^K [T_1..T_n]]\!]_\eta & = & \bigcap^{K}_{1 \leq i \leq n} [\![T_i]\!]_\eta \\
[\![S\,T]\!]_\eta & = & [\![S]\!]_\eta\ [\![T]\!]_\eta \\
[\![\mathrm{Fun}\,(X{:}K)\,T]\!]_\eta & = & \lambda P{\in}[\![K]\!].\,[\![T]\!]_{\eta[X \leftarrow P]}
\end{array}
$$

Of course, for some η's and T's, the interpretation $[\![T]\!]_\eta$ given by these equations is nonsensical. We write $[\![T]\!]_\eta\!\downarrow$ when $[\![T]\!]_\eta$ is well defined and $[\![T]\!]_\eta\!\uparrow$ otherwise. Lemma 4.3.1 will show that the interpretation of a well-kinded type is always well defined.

We say that an environment η *satisfies* a context Γ, written $\eta \models \Gamma$, if $\mathrm{dom}(\eta) = \mathrm{dom}(\Gamma)$ and

1 $\Gamma \equiv \emptyset$; or
2 $\Gamma \equiv \Gamma_1,\, x{:}T$, where $\eta\backslash x$ satisfies Γ_1 and either $[\![T]\!]_{\eta\backslash x}\!\uparrow$ or $\eta(x) \in \mathrm{dom}([\![T]\!]_{\eta\backslash x})$; or
3 $\Gamma \equiv \Gamma_1,\, X{\leq}T{:}K$, where $\eta\backslash X$ satisfies Γ_1 and either $[\![T]\!]_{\eta\backslash X}\!\uparrow$ or $\eta(X) \subseteq^K [\![T]\!]_{\eta\backslash X}$.

Iterating the definition immediately yields that either $[\![T]\!]_{\eta\backslash\Gamma_2\backslash X}\!\uparrow$ or $[\![T]\!]_{\eta\backslash\Gamma_2\backslash X} \in [\![K]\!]$, whenever $\eta \models \Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2$. Also, note that if η' extends η and $\mathrm{FTV}(T) \subseteq \mathrm{dom}(\eta)$, then either $[\![T]\!]_\eta\!\uparrow$ and $[\![T]\!]_{\eta'}\!\uparrow$, or else both are defined and $[\![T]\!]_\eta = [\![T]\!]_{\eta'}$.

Lemma 4.3.1. Let T be a type, Γ a context, and η an environment such that $\mathrm{FTV}(T) \subseteq \mathrm{dom}(\eta)$ and $\eta \models \Gamma$. If $\Gamma \vdash T \in K$, then $[\![T]\!]_\eta\!\downarrow$ and $[\![T]\!]_\eta \in [\![K]\!]$.

Proof. We need to check the desired result together with an additional fact:

1 If $\Gamma \vdash T \in K$, then $[\![T]\!]_\eta$ is defined and $[\![T]\!]_\eta \in [\![K]\!]$.
2 If $\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash \mathrm{ok}$, then $[\![T]\!]_{\eta\backslash\Gamma_2\backslash X}\!\downarrow$ and $[\![T]\!]_{\eta\backslash\Gamma_2\backslash X} \in [\![K]\!]$.

The two are proved by simultaneous induction on derivations. We give only the interesting cases; the rest follow by straightforward use of the induction hypothesis and simple properties of HOPERs.

1 K-TVar We are given that $\Gamma \equiv \Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2$ and that $\Gamma \vdash \mathrm{ok}$. By part 2 of the

induction hypothesis, $[\![T]\!]_{\eta\backslash\Gamma_2\backslash X}\downarrow$. By the definition of satisfaction, we have $(\eta\backslash\Gamma_2)(X) \subseteq^K [\![T]\!]_{\eta\backslash\Gamma_2\backslash X}$, which implies in particular that $\eta(X) \in [\![K]\!]$. By the definition of interpretation, $[\![X]\!]_\eta = \eta(X) \in [\![K]\!]$.

K-ALL We are given that $K \equiv \star$ and $T \equiv \mathrm{All}\,(X{\leq}T_1{:}K_1)\,T_2$, and that $\Gamma,\ X{\leq}T_1{:}K_1 \vdash T_2 \in \star$. By lemma 3.2.1, there exists a shorter derivation of $\Gamma,\ X{\leq}T_1{:}K_1 \vdash$ ok, and, by part 2 of the induction hypothesis, we have that $[\![T_1]\!]_\eta\downarrow$ and $[\![T_1]\!]_\eta \in [\![K_1]\!]$. Now, suppose $P \subseteq^{K_1} [\![T_1]\!]_\eta$. Then the definition of satisfaction yields $\eta[X{\leftarrow}P] \models \Gamma,\ X{\leq}T_1{:}K_1$. By part 1 of the induction hypothesis, $[\![T_2]\!]_{\eta[X\leftarrow P]}\downarrow$ and $[\![T_2]\!]_{\eta[X\leftarrow P]} \in [\![\star]\!]$. Since PER is closed under intersections, $[\![T]\!]_\eta = \bigcap^{\star}_{P\subseteq^{K_1}[\![T_1]\!]_\eta} [\![T_2]\!]_{\eta[X\leftarrow P]} \in [\![\,\star\,]\!]$.

K-OABS Similar.

2 C-VAR We are given that $\Gamma \equiv \Gamma',\ x{:}S$, where $\Gamma' \equiv \Gamma_1,\ X{\leq}T{:}K,\ \Gamma_2'$ and that $\Gamma' \vdash S \in \star$. By Lemma 3.2.1, $\Gamma' \vdash$ ok. By the definition of satisfaction, $\eta\backslash x \models \Gamma'$. By the induction hypothesis, the result follows.

C-TVAR The case where $\Gamma_2 \not\equiv \emptyset$ is similar to the previous case. When $\Gamma_2 \equiv \emptyset$, we are given that $\Gamma \equiv \Gamma_1,\ X{\leq}T{:}K$ and that $\Gamma_1 \vdash T \in K$. By the definition of satisfaction, $\eta\backslash X \models \Gamma'$. By the induction hypothesis, the result follows.

□

In order to prove the soundness of subtyping we need some technical results about substitution and β-conversion.

Lemma 4.3.2. Let η be an environment with $X \notin \mathrm{dom}(\eta)$ and such that $\mathrm{FTV}(S[X{\leftarrow}T]) \subseteq \mathrm{dom}(\eta)$ and $[\![S]\!]_{\eta[X\leftarrow[\![T]\!]_\eta]}\downarrow$. Then $[\![S[X{\leftarrow}T]]\!]_\eta = [\![S]\!]_{\eta[X\leftarrow[\![T]\!]_\eta]}$.

Proof. By induction on the structure of S. □

Lemma 4.3.3. Let η be an environment such that $\mathrm{FTV}(S) \subseteq \mathrm{dom}(\eta)$. If $S =_\beta T$ and $[\![S]\!]_\eta\downarrow$, then $[\![S]\!]_\eta = [\![T]\!]_\eta$.

Proof. By induction on the definition of β-conversion, it is easy to see that it suffices to show the statement for a one-step reduction $S \rightarrow_\beta T$. This is proved by induction on the structure of S. The only interesting case is when S is a β-redex and T its reduct. Let $S \equiv (\mathrm{Fun}\,(X{:}K)\,T_2)T_1$ and $T \equiv T_1[X{\leftarrow}T_2]$. Then

$$\begin{array}{rcll} [\![(\mathrm{Fun}\,(X{:}K)\,T_2)T_1]\!]_\eta & = & (\lambda P{\in}[\![K]\!].\,[\![T_2]\!]_{\eta[X\leftarrow P]})[\![T_1]\!]_\eta & \text{by definition of } [\![\,-\,]\!]_\eta \\ & = & [\![T_2]\!]_{\eta[X\leftarrow[\![T_1]\!]_\eta]} & \\ & = & [\![T_2[X{\leftarrow}T_1]]\!]_\eta & \text{by Lemma 4.3.2.} \end{array}$$

□

Our main semantic results are the soundness of subtyping and typing.

Theorem 4.3.4. (Soundness of subtyping) If $\Gamma \vdash S \leq T$ and $\Gamma \vdash S \in K$, and if $\eta \models \Gamma$, then $[\![S]\!]_\eta \subseteq^K [\![T]\!]_\eta$.

Proof. The proof proceeds by induction on the structure of a derivation of $\Gamma \vdash S \leq T$. For the sake of readability, we often make implicit use of the fact that if $\Gamma \vdash S \leq T$ and

$\Gamma \vdash S \in K$, then, by Proposition 3.2.12 and Lemmas 3.2.7 and 4.3.1, $[\![S]\!]_\eta$ and $[\![T]\!]_\eta$ are defined and belong to $[\![K]\!]$ whenever $\eta \models \Gamma$.

S-Conv — We are given that $S =_\beta T$. Then, by Lemma 4.3.3, $[\![S]\!]_\eta = [\![T]\!]_\eta$

S-Trans — By the induction hypothesis and the transitivity of $\subseteq^K$ (4.2.1).

S-TVar — We are given $\Gamma_1,\, X{\leq}T{:}K,\, \Gamma_2 \vdash \text{ok}$. Now, $[\![X]\!]_\eta = \eta(X) \subseteq^K [\![T]\!]_{\eta\backslash X}$, because $\eta \models \Gamma$ and, as η extends $\eta\backslash X$, $[\![T]\!]_{\eta\backslash X} = [\![T]\!]_\eta$.

S-Arrow — We are given $\Gamma \vdash T_1 \leq S_1$ and $\Gamma \vdash S_2 \leq T_2$, with $\Gamma \vdash S_1{\rightarrow}S_2 \in \star$. By the uniqueness of kinds (3.2.7), $K \equiv \star$. Now by the well-kindedness of subtyping (3.2.12) and syntax directedness of kinds (3.2.6) we have $\Gamma \vdash S_2, T_1 \in \star$. By the induction hypothesis, $[\![S_2]\!]_\eta \subseteq^\star [\![T_2]\!]_\eta$ and $[\![T_1]\!]_\eta \subseteq^\star [\![S_1]\!]_\eta$. Hence, by the covariance on the right and contravariance on the left of the function space constructor on PERs (easily verified from its definition), $[\![S_1]\!]_\eta{\rightarrow}[\![S_2]\!]_\eta \subseteq^\star [\![T_1]\!]_\eta{\rightarrow}[\![T_2]\!]_\eta$, i.e. $[\![S_1{\rightarrow}S_2]\!]_\eta \subseteq^\star [\![T_1{\rightarrow}T_2]\!]_\eta$.

S-All — We are given that

$$\begin{array}{l}\Gamma,\, X{\leq}U{:}K_1 \vdash S_2 \leq T_2 \quad \text{and}\\ \Gamma \vdash \text{All}\,(X{\leq}U{:}K_1)\, S_2 \in \star.\end{array}$$

By proposition 3.2.6, $\Gamma,\, X{\leq}U{:}K_1 \vdash S_2 \in \star$. Let $P \in [\![U]\!]_\eta$. Then, by the definition of satisfaction, $\eta[X{\leftarrow}P] \models \Gamma,\, X{\leq}U{:}K_1$. Now, by the induction hypothesis, it follows that $[\![S_2]\!]_{\eta[X\leftarrow P]} \subseteq^\star [\![T_2]\!]_{\eta[X\leftarrow P]}$. Hence, $\bigcap^\star_{P \subseteq^{K_1} [\![U]\!]_\eta} [\![S_2]\!]_{\eta[X\leftarrow P]} \subseteq^\star \bigcap^\star_{P \subseteq^{K_1} [\![U]\!]_\eta} [\![T_2]\!]_{\eta[X\leftarrow P]}$. Consequently, we have $[\![\text{All}\,(X{\leq}U{:}K_1)\, S_2]\!]_\eta \subseteq^\star [\![\text{All}\,(X{\leq}U{:}K_1)\, T_2]\!]_\eta$.

S-OAbs — We are given $\Gamma,\, X{\leq}\top^{K_1}{:}K_1 \vdash S \leq T$ and $\Gamma \vdash \text{Fun}\,(X{:}K_1)\, S \in K$. By the syntax-directedness of kinding, $K \equiv K_1{\rightarrow}K_2$ and $\Gamma,\, X{\leq}\top^{K_1}{:}K_1 \vdash S \in K_2$ for some K_2. Let $P \in [\![K_1]\!]_\eta$. Then $\eta[X{\leftarrow}P] \models \Gamma,\, X{\leq}\top^{K_1}{:}K_1$. Now by the induction hypothesis, $[\![S]\!]_{\eta[X\leftarrow P]} \subseteq^{K_2} [\![T]\!]_{\eta[X\leftarrow P]}$. So we have $\lambda P \in [\![K_1]\!].\, [\![S]\!]_{\eta[X\leftarrow P]} \subseteq^{K_1\rightarrow K_2} \lambda P{\in}[\![K_1]\!].\, [\![T]\!]_{\eta[X\leftarrow P]}$, that is, $[\![\text{Fun}\,(X{:}K_1)\, S]\!]_\eta \subseteq^{K_1\rightarrow K_2} [\![\text{Fun}\,(X{:}K_1)\, T]\!]_\eta$.

S-OApp — By induction hypothesis, using the syntax-directedness of kinding.

S-Meet-G — By the induction hypothesis and Lemma 4.2.1(3).

S-Meet-LB — By Lemma 4.2.1(4).

S-Meet-Arrow — By Lemma 4.2.1(5).

S-Meet-All — By Lemma 4.2.1(6).

S-Meet-OAbs — By Lemma 4.2.1(7) (using the syntax-directedness of kinding and Lemma 4.3.3).

S-Meet-OApp — By Lemma 4.2.1(8).

Note that, in the four last cases it is even true that $[\![S]\!]_\eta = [\![T]\!]_\eta$. □

The *type context* Γ/TV *obtained from a context* Γ is defined in the obvious way:

$$\begin{array}{rcl}\emptyset/TV &=& \emptyset,\\ (\Gamma,\, x{:}T)/TV &=& \Gamma/TV,\\ (\Gamma,\, X{\leq}T{:}K)/TV &=& \Gamma/TV,\, X{\leq}T{:}K.\end{array}$$

Theorem 4.3.5. Let $\eta_1 \models \Gamma$ and $\eta_2 \models \Gamma$, such that $\eta_1/TV = \eta_2/TV$ and, for all $x \in \mathrm{dom}(\Gamma)$, $\eta_1(x)\ \{[\![\Gamma(x)]\!]_\eta\}\ \eta_2(x)$, where $\eta = \eta_1/TV$. If $\Gamma \vdash e \in T$, then $[\![e]\!]_{\eta_1}\ \{[\![T]\!]_\eta\}\ [\![e]\!]_{\eta_2}$.

Proof. From $\Gamma \vdash e \in T$ it follows by the well-kindedness of typing (3.2.13) that $\Gamma \vdash T \in \star$. Note that $\mathrm{FTV}(T) \subseteq \mathrm{dom}(\Gamma/TV)$; then, by strengthening (3.2.5), $\Gamma/TV \vdash T \in \star$. Note also that $\eta \models \Gamma/TV$; by Lemma 4.3.1, $[\![T]\!]_\eta$ is defined and in $[\![\star]\!]$. We often use this fact implicitly in the following. The proof now proceeds by induction on a derivation of $\Gamma \vdash e \in T$.

T-VAR: From the assumption that for every x in $\mathrm{dom}(\Gamma)$. $\eta_1(x)\ \{[\![\Gamma(x)]\!]_\eta\}\ \eta_2(x)$.

T-ABS: We are given that $\Gamma,\ x{:}T_1 \vdash e \in T_2$. Suppose that $p \in D$ and $q \in D$ are such that $p\ \{[\![T_1]\!]_\eta\}\ q$. Then $\eta_1[x{\leftarrow}p] \models \Gamma,\ x{:}T_1$ and $\eta_2[x{\leftarrow}q] \models \Gamma,\ x{:}T_1$. By the induction hypothesis, $[\![e]\!]_{\eta_1[x\leftarrow p]}\ \{[\![T_2]\!]_\eta\}\ [\![e]\!]_{\eta_2[x\leftarrow q]}$, that is, $[\![|\mathrm{erase}(e)|]\!]_{\eta_1[x\leftarrow p]}\ \{[\![T_2]\!]_\eta\}\ [\![|\mathrm{erase}(e)|]\!]_{\eta_2[x\leftarrow q]}$. From Lemma 4.1.1(2) it follows that $[\![\mathrm{fun}^\star\,(x)\ |\mathrm{erase}(e)|]\!]_{\eta_1} \cdot p\ \{[\![T_2]\!]_\eta\}\ [\![\mathrm{fun}^\star\,(x)\ |\mathrm{erase}(e)|]\!]_{\eta_2} \cdot q$, that is, $[\![\mathrm{fun}\,(x{:}T_1)\ e)]\!]_{\eta_1} \cdot p\ \{[\![T_2]\!]_\eta\}\ [\![\mathrm{fun}\,(x{:}T_1)\ e]\!]_{\eta_2} \cdot q$. Since p and q were chosen freely, we have $[\![\mathrm{fun}\,(x{:}T_1)\ e]\!]_{\eta_1}\ \{[\![T_1]\!]_\eta {\rightarrow} [\![T_2]\!]_\eta\}\ [\![\mathrm{fun}\,(x{:}T_1)\ e]\!]_{\eta_2}$, in other words $[\![\mathrm{fun}\,(x{:}T_1)\ e]\!]_{\eta_1}\ \{[\![T_1{\rightarrow}T_2]\!]_\eta\}\ [\![\mathrm{fun}\,(x{:}T_1)\ e]\!]_{\eta_2}$.

T-APP: By the induction hypothesis, using the fact that $[\![fa]\!]_\eta = [\![f]\!]_\eta [\![a]\!]_\eta$.

T-TABS: We are given that $\Gamma,\ X{\leq}T_1{:}K_1 \vdash e \in T_2$. Suppose that $P \subseteq^{K_1} [\![T_1]\!]_\eta$. Then $\eta_1[X{\leftarrow}P] \models \Gamma,\ X{\leq}T_1{:}K_1$ and $\eta_2[X{\leftarrow}P] \models \Gamma,\ X{\leq}T_1{:}K_1$. Since $[\![e]\!]_{\eta_1} = [\![e]\!]_{\eta_1[X\leftarrow P]}$, we have $[\![e]\!]_{\eta_1}\ \{[\![T_2]\!]_{\eta[X\leftarrow P]}\}\ [\![e]\!]_{\eta_2}$, by the induction hypothesis. Since P was chosen freely, $[\![e]\!]_{\eta_1}\ \{\bigcap^\star_{P\subseteq^{K_1}[\![T_1]\!]_\eta} [\![T_2]\!]_{\eta[X\leftarrow P]}\}\ [\![e]\!]_{\eta_2}$. Now the result follows from the definition $[\![-]\!]_\eta$ and the fact that $[\![\mathrm{fun}\,(X{\leq}T_1{:}K_1)\ e]\!]_\eta = [\![e]\!]_\eta = [\![e]\!]_{\eta[X\leftarrow P]}$.

T-TAPP: We are given that $\Gamma \vdash f \in \mathrm{All}\,(X{\leq}T_1{:}K_1)\,T_2$ and that $\Gamma \vdash S \leq T_1$. By the induction hypothesis, $[\![f]\!]_{\eta_1}\ \{[\![\mathrm{All}\,(X{\leq}T_1{:}K_1)\,]\!]_\eta\}\ [\![f]\!]_{\eta_2}$, that is, $[\![f]\!]_{\eta_1}\ \{\bigcap^\star_{P\subseteq^{K_1}} [\![T_2]\!]_{\eta[X\leftarrow P]}\}\ [\![f]\!]_{\eta_2}$. By the well-kindedness of typing, syntax directedness of kinds, and well-kindedness of subtyping, $\Gamma \vdash S \in K_1$, and, by soundness of subtyping, $[\![S]\!]_\eta \subseteq^{K_1} [\![T_1]\!]_\eta$. So we have $[\![f]\!]_{\eta_1}\ \{[\![T_2]\!]_{\eta[X\leftarrow[\![S]\!]_\eta]}\}\ [\![f]\!]_{\eta_2}$, which, by Lemma 4.3.2 and the fact that $[\![f]\!]_\eta = [\![fS]\!]_\eta$ for any η, is $[\![fS]\!]_{\eta_1}\ \{[\![T_2[X{\leftarrow}S]]\!]_\eta\}\ [\![fS]\!]_{\eta_2}$.

T-FOR: From the induction hypothesis, since $\mathrm{erase}(e[X{\leftarrow}S]) = \mathrm{erase}(e)$.

T-MEET: We are given that $\Gamma \vdash \mathrm{ok}$ and also $\Gamma \vdash e \in T_i$ for each i in $\{1\ ..\ n\}$. The result follows by the induction hypothesis and the definitions of $\bigcap^\star$ and $[\![-]\!]_\eta$.

T-SUBSUMPTION: We are given that $\Gamma \vdash e \in S$ and that $\Gamma \vdash S \leq T$. By the induction hypothesis, $[\![e]\!]_{\eta_1}\ \{[\![S]\!]_\eta\}\ [\![e]\!]_{\eta_2}$. By well-kindedness of typing $\Gamma \vdash S \in \star$, and by the soundness of subtyping $[\![S]\!]_\eta \subseteq^\star [\![T]\!]_\eta$. Hence, $[\![e]\!]_{\eta_1}\ \{[\![T]\!]_\eta\}\ [\![e]\!]_{\eta_2}$.

□

Corollary 4.3.6. (Soundness of typing) Let η be an environment such that $\eta \models \Gamma$. Then $\Gamma \vdash e \in T$ implies $[\![e]\!]_\eta \in \mathrm{dom}([\![T]\!]_\eta)$.

Proof. Take $\eta_1 = \eta_2 = \eta$. $\square$

Remark 4.3.7. If we now went on to study an equational theory for terms, it would be convenient to redefine the denotation of a typed term as an equivalence class in the model, rather than as an element of the underlying combinatory algebra, as we have done so far. When $\Gamma \vdash e \in T$, let

$$[\![e]\!]^T_\eta = \{n \mid n\ \{[\![T]\!]_\eta\}\ [\![e]\!]_\eta\}$$

This definition, which is justified by Corollary 4.3.6, is preferable to the one we have used so far because it satisfies extensionality.

5. Encoding Multiple Inheritance

We close with a full implementation of the `extend2` function from Section 2. As we suggested in the introduction, an intersection type must be used at one point (marked `***` in the definition of `extend2`) to obtain a sound typing; the rest is straightforward.

This implementation of classes and inheritance makes the local state of each class inaccessible both to clients of objects and to methods defined in subclasses. Other variations are possible; we chose this one to simplify the presentation of Section 2.

If `M` is an object interface, then `Class(M)` is the set of classes whose instances have type `Object(M)`. Each such class consists of a local representation type `MyR` (whose identity is hidden by an existential quantifier), an element `initstate` $\in$ `MyR` that is used as the initial value of the state in new objects created from this class, and a function `buildM` that can be used to construct the methods of the new objects:

```
# Class =
#   Fun(M:*->*)
#     Some(R)
#       {| initstate: R,
#          buildM: ClassMethods M R |};
Class : (*->*)->*
```

To cope with different representations of local state in subclasses, the method-building function is abstracted on two parameters: a type `FinalR` representing the "full" state of an eventual subclass, and an "extractor" giving access to the components of interest to the methods being built. The method builder is also abstracted on a collection of `self`-methods of the same types as its own methods. Given these, it yields a concrete collection of methods specialized to work properly in an object with representation type `FinalR`:

```
# ClassMethods =
#   Fun(MyM:*->*)
#   Fun(MyR)
#     All(FinalR)
#     (Extractor FinalR MyR) ->
#     (MyM(FinalR)) ->
#     (MyM(FinalR));
ClassMethods : (*->*)->*->*
```

Finally, an extractor is just a pair of maps, `get` and `put`.

```
# Extractor = Fun(SS) Fun(TT) {| get: SS->TT, put: SS->TT->SS |};
Extractor : *->*->*
```

Intuitively, `get` extracts the "superclass part" of an element of a subclass's state, while `put` overwrites the superclass part, yielding a new subclass state.

For example, the point class of Section 2 can be defined directly (rather than as an extension of `thingClass`) as follows:

```
# pointClass =
#   < {|x:Int|},
#     {initstate = {x=0},
#      buildM = fun(FinalR)
#               fun(e: Extractor FinalR {|x:Int|})
#               fun(self: PointM FinalR)
#                 {getX = fun(s:FinalR) (e.get s).x,
#                  setX = fun(s:FinalR) fun(i:Int) e.put s {x=i},
#                  bump = fun(s:FinalR) e.put s {x = plus 1 (e.get s).x}
#                 }}
#    > : Class PointM;
pointClass = <val> : Class PointM
```

(We use the ascii syntax "`<R,b>:T`" for introducing elements of existential types: `R` is the hidden witness type, `b` is the body, and `T` is the existential type where the result is to live. The corresponding elimination form is written "`open e as <R,x> in b`.")

A class with two superclasses generates objects whose internal states have three parts: one for each superclass and one for the new components local to the class itself. For example, an instance of `cpointClass` contains a point state of type `{|x:Int|}`, a colored-object state of type `{|c:Color|}`, and an empty local state. The `extend2` function takes two classes, an initial local state, and a function for incrementally building a collection of new methods from the old ones, and constructs a subclass of this form.

```
# extend2 =                                  %Arguments:
#  fun(SuperM1: *->*)                            %first superclass interface
#  fun(SuperM2: *->*)                            %second superclass interface
#  fun(MyM < SuperM1/\SuperM2)       % ***       %new subclass interface
#  fun(MyLocalR: *)                              %local state type
#  fun(superClass1: Class SuperM1)               %first superclass
#  fun(superClass2: Class SuperM2)               %second superclass
#  fun(myinitstate: MyLocalR)                    %initial local state
#  fun(mymethods:                                %method extension fn with args:
#         All(FinalR)                             %a final representation type
#           (Extractor FinalR MyLocalR) ->        %an extractor for the local state
#           (SuperM1(FinalR)) ->                  %the first superclass's methods
#           (SuperM2(FinalR)) ->                  %the second superclass's methods
#           (MyM(FinalR)) ->                      %the self-methods
#           (MyM(FinalR)))                        %returning the new methods
#  open superClass1 as <SuperR1,superData1> in  %open the first superclass
#  open superClass2 as <SuperR2,superData2> in  %open the second superclass
```

```
#  let MyR = Triple SuperR1 SuperR2 MyLocalR in %define the new state type
#
#   <                                       %Result: a new class (an existential)
#    MyR,                                      %with state type MyR
#    {initstate = triple                         %and initial state
#                   SuperR1 SuperR2 MyLocalR     %a triple of
#                    (superData1.initstate)      %first super's initial state
#                    (superData2.initstate)      %second super's initial state
#                    myinitstate,                %local initial state
#     buildM =                                 %and method-builder, a fun with args
#      fun(FinalR)                               %a final representation type
#      fun(e: Extractor FinalR MyR)              %and an extractor for the state
#      fun(self: MyM(FinalR))                    %and a collection of self-methods...
#        let eself =
#          composeExtractors
#             FinalR MyR MyLocalR e
#             (extract3of3 SuperR1 SuperR2 MyLocalR) in
#        let esuper1 =
#          composeExtractors
#             FinalR MyR SuperR1 e
#             (extract1of3 SuperR1 SuperR2 MyLocalR) in
#        let esuper2 =
#          composeExtractors
#             FinalR MyR SuperR2 e
#             (extract2of3 SuperR1 SuperR2 MyLocalR) in
#                                                %returning:
#        mymethods FinalR eself                    %methods built by mymethods
#          (superData1.buildM FinalR esuper1 self)   %using the concrete methods
#          (superData2.buildM FinalR esuper2 self)   % of the two superclasses
#          self                                      %and the self-methods
#        end end end}
#    > : Class MyM
#   end end end;
extend2 = <val>
        : All(SuperM1)
          All(SuperM2)
          All(MyM<SuperM1/\SuperM2)
          All(MyLocalR)
               (Class SuperM1)
            -> (Class SuperM2)
            -> MyLocalR
            -> (All(FinalR)
                    (Extractor FinalR MyLocalR)
                  ->(SuperM1 FinalR)
                  ->(SuperM2 FinalR)
                  ->(MyM FinalR)
                  ->(MyM FinalR))
```

```
           -> (Class MyM)
```

This definition uses a utility function for composing extractors in the obvious way:

```
# composeExtractors =
#   fun(T1) fun(T2) fun(T3)
#     fun(e1: Extractor T1 T2)
#       fun(e2: Extractor T2 T3)
#         {get = fun(t1:T1) e2.get (e1.get t1),
#          put = fun(t1:T1) fun(t3:T3)
#                  e1.put t1 (e2.put (e1.get t1) t3)};
composeExtractors = <val>
                  : All(T1)
                    All(T2)
                    All(T3)
                         (Extractor T1 T2)
                      -> (Extractor T2 T3)
                      -> {|get:T1->T3, put:T1->T3->T1|}
```

For forming triples, we use the type abbreviation

```
# Triple = Fun(T1) Fun(T2) Fun(T3) {| fst:T1, snd:T2, thd:T3 |};
Triple : *->*->*->*
```

with the constructor

```
# triple =
#   fun(T1) fun(T2) fun(T3)
#   fun(t1:T1) fun(t2:T2) fun(t3:T3)
#     {fst=t1, snd=t2, thd=t3};
triple = <val>
       : All(T1)
         All(T2)
         All(T3)
           T1 -> T2 -> T3 -> {|fst:T1, snd:T2, thd:T3|}
```

and the projections

```
# extract1of3 =
#  fun(T1) fun(T2) fun(T3)
#    {get = fun(p: Triple T1 T2 T3) p.fst,
#     put = fun(p: Triple T1 T2 T3) fun(t:T1) {fst=t, snd=p.snd, thd=p.thd} };
extract1of3 = <val>
            : All(T1)
              All(T2)
              All(T3)
                {|get: (Triple T1 T2 T3)->T1,
                  put: (Triple T1 T2 T3)->T1->{|fst:T1, snd:T2, thd:T3|}|}
```

and `extract2of3` and `extract3of3`, which are defined similarly.

A slightly different formulation of the `extend2` function provides an alternative perspective on its behavior. The original `extend2` is parametric on three class interfaces, `SuperM1`, `SuperM2`, and `MyM`, where `MyM` is constrained to refine both `SuperM1` and `SuperM2`. The type of the following function `extend2'` emphasizes the fact that `MyM` is typically formed by *adding* some new methods to those given by `SuperM1` and `SuperM2`: it is parameterized on `SuperM1`, `SuperM2`, and a "partial interface" `MyOwnM`, which is conjoined with the other two to form `MyM`:

```
# extend2' =
#  fun(SuperM1: *->*)                        % first superclass interface
#  fun(SuperM2: *->*)                        % second superclass interface
#  fun(MyOwnM: *->*)                         % new methods specification
#  let MyM = SuperM1/\SuperM2/\MyOwnM in     % new class interface
#     % ...(the rest, as before)...
extend2' = <val>
         : All(SuperM1)
           All(SuperM2)
           All(MyOwnM)
           All(MyLocalR)
                (Class SuperM1)
             -> (Class SuperM2)
             -> MyLocalR
             -> (All(FinalR)
                     (Extractor FinalR MyLocalR)
                   ->(SuperM1 FinalR)
                   ->(SuperM2 FinalR)
                   ->(SuperM1/\(SuperM2/\MyOwnM) FinalR)
                   ->(SuperM1/\(SuperM2/\MyOwnM) FinalR))
             -> (Class (SuperM1/\(SuperM2/\MyOwnM)))
```

Note that all of the quantifiers in this version are unbounded: bounded quantification has been replaced by unbounded quantification and intersection.

6. Discussion

For technical convenience, our model of multiple inheritance has been presented in a purely functional setting: sending a message that changes the internal state of an object yields a new object with appropriately modified state rather than updating the original object's state in-place. Extending the model to an object model including mutable internal state should be fairly straightforward, following [Pierce, 1993]. The principal difficulty lies in the fact that the type $\top^\star$, which classifies *all* terms (not only the well-behaved ones), is only sensible in a call-by-name setting, where we can be sure that an ill-behaved subterm will never be needed during evaluation. To move to a call-by-value setting, where the order of updates to mutable variables is easier to predict, we would need to replace $\top^\star$ by $F_\leq$'s less permissive maximal type *Top* and restrict the formation rules so that only nonempty intersections are allowed.

We have seen that a semantics of intersections can be given by a straightforward extension of a model of higher-order polymorphism. Indeed, it appears that even the combination of intersections and recursive types is semantically unproblematic [Cardone, personal communication, 1992]. This suggests that other existing accounts of typed object-oriented programming could be extended with multiple inheritance by a construction similar to ours. Indeed, accounts such as that of Bruce [1994], which interpret a high-level object syntax directly into a denotational model, should support this extension almost trivially: the need for intersection *types* (as opposed to intersections in the model) arose here from our requirement that the `extend` function itself be a term of the target λ-calculus. Extending accounts based on a translation into a λ-calculus with recursive records, on the other hand, may be more difficult, since no syntactic study has been made so far of a type system combining intersections and recursive types.

Acknowledgements

We are grateful for discussions with Henk Barendregt, Kim Bruce, Luca Cardelli, Bob Harper, John Reynolds, David Turner, and Benjamin Werner. Three referees made many helpful suggestions on an earlier draft.

This work was supported by funding from the U.K. Science and Engineering Research Council and the ESPRIT Basic Research Actions TYPES and CONFER, and from the Netherlands Organization for Scientific Research (N.W.O.).

References

[Abadi and Cardelli, 1994a] Martín Abadi and Luca Cardelli. A theory of primitive objects: Second-order systems. In *European Symposium on Programming (ESOP), Edinburgh, Scotland*, 1994.

[Abadi and Cardelli, 1994b] Martín Abadi and Luca Cardelli. A theory of primitive objects: Untyped and first-order systems. In *Theoretical Aspects of Computer Software (TACS), Sendai, Japan*, 1994.

[Abadi and Cardelli, 1996] Martín Abadi and Luca Cardelli. *A Theory of Objects.* Springer-Verlag, 1996. To appear.

[Abadi *et al.*, 1996] Martín Abadi, Luca Cardelli, and Ramesh Viswanathan. An interpretation of objects and object types. In Principles of Programming Languages, pages 396–409, 1996.

[Abadi, 1994] Martín Abadi. Baby Modula-3 and a theory of objects. *Journal of Functional Programming*, 4(2), April 1994. An earlier version appeared as DEC Systems Research Center Research Report 95, (February, 1993).

[Barendregt *et al.*, 1983] H. Barendregt, M. Coppo, and M. Dezani-Ciancaglini. A filter lambda model and the completeness of type assignment. *Journal of Symbolic Logic*, 48(4):931–940, 1983.

[Barendregt, 1984] H. P. Barendregt. *The Lambda Calculus.* North Holland, revised edition, 1984.

[Bruce and Longo, 1990] Kim B. Bruce and Giuseppe Longo. A modest model of records, inheritance, and bounded quantification. *Information and Computation*, 87:196–240, 1990. Also in Carl A. Gunter and John C. Mitchell, editors, *Theoretical Aspects of Object-Oriented Programming: Types, Semantics, and Language Design* (MIT Press, 1994). An earlier version appeared in the proceedings of the IEEE Symposium on Logic in Computer Science, 1988.

[Bruce and Mitchell, 1992] Kim Bruce and John Mitchell. PER models of subtyping, recursive types and higher-order polymorphism. In *Proceedings of the Nineteenth ACM Symposium on Principles of Programming Languages*, Albequerque, NM, January 1992.

[Bruce *et al.*, 1990] Kim B. Bruce, Albert R. Meyer, and John C. Mitchell. The semantics of second-order lambda calculus. In Huet [1990], pages 213–272. Also appeared in Information and Computation 84, 1 (January 1990).

[Bruce, 1994] Kim B. Bruce. A paradigmatic object-oriented programming language: Design, static typing and semantics. *Journal of Functional Programming*, 4(2), April 1994. A preliminary version appeared in POPL 1993 under the title "Safe Type Checking in a Statically Typed Object-Oriented Programming Language".

[Canning *et al.*, 1989] Peter Canning, William Cook, Walter Hill, Walter Olthoff, and John Mitchell. F-bounded quantification for object-oriented programming. In *Fourth International Conference on Functional Programming Languages and Computer Architecture*, pages 273–280, September 1989.

[Cardelli and Longo, 1991] Luca Cardelli and Giuseppe Longo. A semantic basis for Quest. *Journal of Functional Programming*, 1(4):417–458, October 1991. Preliminary version in ACM Conference on Lisp and Functional Programming, June 1990. Also available as DEC SRC Research Report 55, Feb. 1990.

[Cardelli and Mitchell, 1991] Luca Cardelli and John Mitchell. Operations on records. *Mathematical Structures in Computer Science*, 1:3–48, 1991. Also in Carl A. Gunter and John C. Mitchell, editors, *Theoretical Aspects of Object-Oriented Programming: Types, Semantics, and Language Design* (MIT Press, 1994); available as DEC Systems Research Center Research Report #48, August, 1989, and in the proceedings of MFPS '89, Springer LNCS volume 442.

[Cardelli, 1984] Luca Cardelli. A semantics of multiple inheritance. In G. Kahn, D. MacQueen, and G. Plotkin, editors, *Semantics of Data Types*, volume 173 of *Lecture Notes in Computer Science*, pages 51–67. Springer-Verlag, 1984. Full version in *Information and Computation* 76(2/3):138–164, 1988.

[Cardelli, 1990] Luca Cardelli. Notes about $F^{\omega}_{<:}$. Unpublished manuscript, October 1990.

[Cardone and Coppo, 1990] Felice Cardone and Mario Coppo. Two extensions of Curry's type inference system. In Piergiorgio Odifreddi, editor, *Logic and Computer Science*, number 31 in APIC Studies in Data Processing, pages 19–76. Academic Press, 1990.

[Castagna *et al.*, 1995] Giuseppe Castagna, Giorgio Ghelli, and Giuseppe Longo. A calculus for overloaded functions with subtyping. *Information and Computation*, 117(1):115–135, 15 February 1995. a preliminary version appeared in LISP and Functional Programming, July 1992 (pp. 182–192), and as Rapport de Recherche LIENS-92-4, Ecole Normale Supérieure, Paris.

[Castagna, 1992] Giuseppe Castagna. Strong typing in object-oriented paradigms. Rapport de Recherche LIENS-92-11, Ecole Normale Supérieure, Paris, May 1992.

[Compagnoni, 1994] Adriana B. Compagnoni. Decidability of higher-order subtyping with intersection types. In *Computer Science Logic*, September 1994. Kazimierz, Poland. Springer *Lecture Notes in Computer Science* 933, June 1995. Also available as University of Edinburgh, LFCS technical report ECS-LFCS-94-281, titled "Subtyping in $F^{\omega}_{\wedge}$ is decidable".

[Compagnoni, 1995] Adriana B. Compagnoni. *Higher-Order Subtyping with Intersection Types*. PhD thesis, Catholic University, Nigmegen, January 1995.

[Cook *et al.*, 1990] William R. Cook, Walter L. Hill, and Peter S. Canning. Inheritance is not subtyping. In *Seventeenth Annual ACM Symposium on Principles of Programming Languages*, pages 125–135, San Francisco, CA, January 1990. Also in Carl A. Gunter and John C. Mitchell, editors, *Theoretical Aspects of Object-Oriented Programming: Types, Semantics, and Language Design* (MIT Press, 1994).

[Coppo and Dezani-Ciancaglini, 1978] M. Coppo and M. Dezani-Ciancaglini. A new type-assignment for λ-terms. *Archiv. Math. Logik*, 19:139–156, 1978.

[Curien and Ghelli, 1992] Pierre-Louis Curien and Giorgio Ghelli. Coherence of subsumption: Minimum typing and type-checking in $F_{\leq}$. *Mathematical Structures in Computer Science*, 2:55–91, 1992. Also in Carl A. Gunter and John C. Mitchell, editors, *Theoretical Aspects of Object-Oriented Programming: Types, Semantics, and Language Design* (MIT Press, 1994).

[de Bruijn, 1972] Nicolas G. de Bruijn. Lambda-calculus notation with nameless dummies: a tool for automatic formula manipulation with application to the Church-Rosser theorem. *Indag. Math.*, 34(5):381–392, 1972.

[Fisher and Mitchell, 1994] Kathleen Fisher and John Mitchell. Notes on typed object-oriented programming. In *Proceedings of Theoretical Aspects of Computer Software, Sendai, Japan*, pages 844–885. Springer-Verlag, April 1994. LNCS 789.

[Freyd *et al.*, 1990] P. Freyd, P. Mulry, G. Rosolini, and D. Scott. Extensional PERs. In *Fifth Annual Symposium on Logic in Computer Science (Philadelphia, PA)*, pages 346–354. IEEE Computer Society Press, June 1990.

[Girard, 1972] Jean-Yves Girard. *Interprétation fonctionelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris VII, 1972.

[Goldberg and Robson, 1983] Adele Goldberg and David Robson. *Smalltalk-80: The Language and Its Implementation*. Addison-Wesley, Reading, MA, 1983.

[Hindley and Seldin, 1986] J. Roger Hindley and Jonathan P. Seldin. *Introduction to Combinators and λ-Calculus*, volume 1 of *London Mathematical Society Student Texts*. Cambridge University Press, 1986.

[Hofmann and Pierce, 1995] Martin Hofmann and Benjamin Pierce. A unifying type-theoretic framework for objects. *Journal of Functional Programming*, 1995. Previous versions appeared in the Symposium on Theoretical Aspects of Computer Science, 1994, (pages 251–262) and, under the title "An Abstract View of Objects and Subtyping (Preliminary Report)," as University of Edinburgh, LFCS technical report ECS-LFCS-92-226, 1992.

[Huet, 1990] Gérard Huet, editor. *Logical Foundations of Functional Programming*. University of Texas at Austin Year of Programming Series. Addison-Wesley, 1990.

[Mitchell *et al.*, 1993] John C. Mitchell, Furio Honsell, and Kathleen Fisher. A lambda calculus of objects and method specialization. In *1993 IEEE Symposium on Logic in Computer Science*, June 1993.

[Mitchell, 1990a] John C. Mitchell. Toward a typed foundation for method specialization and inheritance. In *Proceedings of the 17th ACM Symposium on Principles of Programming Languages*, pages 109–124, January 1990. Also in Carl A. Gunter and John C. Mitchell, editors, *Theoretical Aspects of Object-Oriented Programming: Types, Semantics, and Language Design* (MIT Press, 1994).

[Mitchell, 1990b] John C. Mitchell. A type-inference approach to reduction properties and semantics of polymorphic expressions. In Huet [1990], pages 195–212.

[Pierce and Turner, 1994] Benjamin C. Pierce and David N. Turner. Simple type-theoretic foundations for object-oriented programming. *Journal of Functional Programming*, 4(2):207–247, April 1994. A preliminary version appeared in Principles of Programming Languages, 1993, and as University of Edinburgh technical report ECS-LFCS-92-225, under the title "Object-Oriented Programming Without Recursive Types".

[Pierce, 1991] Benjamin C. Pierce. *Programming with Intersection Types and Bounded Polymorphism*. PhD thesis, Carnegie Mellon University, December 1991. Available as School of Computer Science technical report CMU-CS-91-205.

[Pierce, 1993] Benjamin C. Pierce. Mutable objects. Draft report; available electronically, June 1993.

[Reynolds, 1988] John C. Reynolds. Preliminary design of the programming language Forsythe. Technical Report CMU-CS-88-159, Carnegie Mellon University, June 1988.

[Scott, 1976] Dana Scott. Data types as lattices. *SIAM Journal on Computing*, 5(3):522–587, 1976.

[Ungar and Smith, 1987] D. Ungar and R. B. Smith. Self: The power of simplicity. In *Proceedings of the ACM Symposium on Object-Oriented Programming: Languages, Systems, and Applications (OOPSLA)*, pages 227–241, 1987.