A Theory of Primitive Objects
Second-Order Systems

Martín Abadi and Luca Cardelli

Digital Equipment Corporation, Systems Research Center

Abstract

We describe a second-order calculus of objects. The calculus supports object subsumption, method override, and the type Self. It is constructed as an extension of System **F** with subtyping, recursion, and first-order object types.

1. Introduction

To its founders and practitioners, object-oriented programming is a new computational paradigm distinct from ordinary procedural programming. Objects and method invocations, in their purest form, are meant to replace procedures and calls, and not simply to complement them. Is there, then, a corresponding "λ-calculus" of objects, based on primitives other than abstraction and application?

Such a specialized calculus may seem unnecessary, since untyped objects and methods can be reduced to untyped λ-terms. However, this reduction falters when we take typing and subtyping into account. It becomes even more problematic when we consider the peculiar second-order object-oriented concept of the Self type.

This paper is part of an effort to identify object calculi that are as simple and fruitful as λ-calculi. Towards this goal, we have considered untyped, first-order, and second-order systems, their equational theories, and their semantics. Here we describe, in essence, an object-oriented version of the polymorphic λ-calculus.

The starting point for this paper is a first-order calculus of objects and their types, introduced in [Abadi, Cardelli 1994c]. In this calculus, an object is a collection of methods. A method is a function having a special parameter, called *self*, that denotes the same object the method belongs to. The calculus supports *object subsumption* and *method override*. Subsumption is the ability to emulate an object by means of another object that has more refined methods. Override is the operation that modifies the behavior of an object, or class, by replacing one of its methods; the other methods are *inherited*. We review this calculus in section 2.

We add standard second-order constructs to the first-order calculus. The resulting system is an extension of Girard's System **F** [Girard, Lafont, Taylor 1989] with objects, subtyping, and recursion. Only the first-order object constructs are new. However, the interaction of second-order types, recursive types, and objects types is a prolific one.

Using all these constructs, we define an interesting new quantifier, ς (sigma), similar to the μ binder of recursive types. This quantifier satisfies desirable subtyping properties that μ does not satisfy, and that are important in examples with objects. Using ς and a covariance condition we formalize the notion of Self, which is the type of the self parameter.

We take advantage of Self in some challenging examples. One is a treatment of the traditional geometric points. Another is a calculator that modifies its own methods. A third one is an object-oriented version of Scott numerals, exploiting both Self and polymorphism.

Some modern object-oriented languages support Self, subsumption, and override (e.g., [Meyer 1988]). Correctness is obtained via rather subtle conditions, if at all. We explain Self by deriving its rules from those for more basic constructs. Thus, the problems of consistency are reduced, and hopefully clarified.

Our main emphasis is on sound typing rules for objects; because of this emphasis we restrict ourselves to a stateless computational model. However, our type theories should be largely applicable to imperative and concurrent variants of the model, and our equational theories reveal difficulties that carry over as well.

In the next section we review the first-order calculus. Section 3 concerns the second-order constructs, the Self quantifier, and matters of covariance and contravariance. In section 4 we combine the Self quantifier with object types to formalize the type Self, and we present examples. In section 5 we discuss the problem of overriding methods that return values of type Self. We conclude with a comparison with related work. The appendix lists all the typing and equational rules used in the body of the paper. In [Abadi, Cardelli 1994a] we give a denotational model for these rules.

2. First-Order Calculi

In this section we review the typed first-order object calculus introduced in [Abadi, Cardelli 1994c]. We also recall its limitations, which motivate the second-order systems that are the subject of this paper.

2.1 Informal Syntax and Semantics of Objects

We consider a minimal object calculus including *object formation*, *method invocation*, and *method override*. The calculus is very simple, with just four syntactic forms, and even without functions. It is patently object-oriented: it has built-in objects, methods with self, and the characteristic semantics of method invocation and override. It can express object-flavored examples in a direct way.

Syntax of the first-order ς-calculus

A,B ::=	$[l_i=B_i\ ^{i\in 1..n}]$	(l_i distinct)	types
a,b ::=			terms
	x		variable
	$[l_i=\varsigma(x_i:A)b_i\ ^{i\in 1..n}]$	(l_i distinct)	object
	a.l		field selection / method invocation
	$a.l \Leftarrow \varsigma(x:A)b$		field update / method override

Notation

- We use indexed notation of the form $\Phi_i\ ^{i\in 1..n}$ to denote sequences $\Phi_1,...,\Phi_n$.
- We use "$\triangleq$" for "equal by definition", "$\equiv$" for "syntactically identical", and "=" for "provably equal" when applied to two terms.
- [...l,l':A ...] stands for [...l:A, l':A...].
- [..., l=b, ...] stands for [..., $l=\varsigma(y:A)b$, ...], for an unused y. We call l=b a *field*.
- $o.l_j:=b$ stands for $o.l_j \Leftarrow \varsigma(y:A)b$, for an unused y. We call it an *update* operation.

- We write $b\{x\}$ to highlight that x may occur free in b. The substitution of a term c for the free occurrences of x in b is written $b\{x\leftarrow c\}$, or $b\{c\}$ where x is clear from context.
- We identify $\varsigma(x:A)b$ with $\varsigma(y:A)(b\{x\leftarrow y\})$, for any y not occurring free in b.

An object is a collection of components $l_i=a_i$, for distinct labels l_i and associated methods a_i; the order of these components does not matter. The object containing a given method is called the method's *host* object. The symbol ς is used as a binder for the self parameter of a method; $\varsigma(x:A)b$ is a method with self parameter x of type A, to be bound to the host object, and body b.

A *field* is a degenerate method that ignores its self parameter; we talk about *field selection* and *field update*. We use the terms selection and invocation and the terms update and override somewhat interchangeably.

A method invocation is written $o.l_j$, where l_j is a label of o. It equals the result of the substitution of the host object for the self parameter in the body of the method named l_j.

A method override is written $o.l_j \Leftarrow \varsigma(y:A)b$. The intent is to replace the method named l_j of o with $\varsigma(y:A)b$; this is a single operation that involves a construction binding y in b. A method override equals a copy of the host object where the overridden method has been replaced by the overriding one. The semantics of override is functional; an override on an object produces a modified copy of the object.

An object of type $[l_i:B_i\ ^{i\in 1..n}]$ can be formed from a collection of n methods whose self parameters have type $[l_i:B_i\ ^{i\in 1..n}]$ and whose bodies have types $B_1,...,B_n$. When writing $[l_i:B_i\ ^{i\in 1..n}]$, we always assume that the l_i are distinct and that permutations do not matter. The type $[l_i:B_i\ ^{i\in 1..n}]$ exhibits only the result types B_i, and not the types of ς-bound variables. The types of all these variables is $[l_i:B_i\ ^{i\in 1..n}]$. When the method named l_i is invoked, it produces a result of type B_i. A method can be overridden while preserving the type of its host object.

Self-substitution is at the core of the semantics. Because of this, it is easy to define non-terminating computations without explicit use of recursion:

$$\text{let } o \triangleq [l=\varsigma(x:[])x.l] \quad \text{then} \quad o.l = x.l\{x\leftarrow o\} \equiv o.l = \ldots$$

Using recursive types, it is possible for a method to return or to modify self:

$$\text{let } A \triangleq \mu(X)[l:X]$$
$$\text{let } o' \triangleq [l = \varsigma(x:A)x] \quad \text{then} \quad o'.l = x\{x\leftarrow o'\} \equiv o'$$
$$\text{let } o'' \triangleq [l = \varsigma(y:A)\,(y.l\Leftarrow\varsigma(x:A)x)] \quad \text{then} \quad o''.l = (o''.l\Leftarrow\varsigma(x:A)x) = o'$$

We place particular emphasis on the ability to modify self. In object-oriented languages, it is very common for a method to modify field components of self. Generalizing, we allow methods to override other methods of self, or even themselves. This feature does not significantly complicate the problems that we address.

We do not provide an operation to extract a method from an object as a function; such an operation is incompatible with object subsumption in typed calculi. Methods are inseparable from objects and cannot be recovered as functions; this consideration inspired the use of a specialized ς-notation instead of the familiar λ-notation for parameters.

Other choices of primitives are possible; some are discussed in [Abadi, Cardelli 1994c].

2.2 Object Typing and Subtyping

We now review the typing and subtyping rules for objects. Each rule has a number of antecedent judgments above a horizontal line and a single conclusion judgment below the line. Each judgment has the form $E \vdash \mathfrak{I}$, for an environment E and an assertion $\mathfrak{I}$ depending on the judgment. An antecedent of the form "$E,E_i \vdash \mathfrak{I}_i\ \ \forall i\in 1..n$" is an abbreviation for n antecedents

"$E,E_1 \vdash \Im_1$ ... $E,E_n \vdash \Im_n$" if n>0, and if n=0 for "$E \vdash \diamond$", which means "E is well-formed". Instead, a rule containing "$j \in 1..n$" indicates that there are n separate rules, one for each j. Environments contain typing assumptions for variables; later they will also contain type-variable declarations and subtyping assumptions.

First we give rules for proving type judgments $E \vdash B$ ("B is a well-formed type in the environment E") and value judgments $E \vdash b : B$ ("b has type B in E").

(Type Object) (l_i distinct) (Val x) (Val Object) (where $A \equiv [l_i:B_i \ ^{i \in 1..n}]$)

$$\frac{E \vdash B_i \quad \forall i \in 1..n}{E \vdash [l_i:B_i \ ^{i \in 1..n}]} \qquad \frac{E, x:A, E' \vdash \diamond}{E \vdash x: A} \qquad \frac{E, x_i:A \vdash b_i : B_i \quad \forall i \in 1..n}{E \vdash [l_i=\varsigma(x_i:A)b_i \ ^{i \in 1..n}] : A}$$

(Val Select) (Val Override) (where $A \equiv [l_i:B_i \ ^{i \in 1..n}]$)

$$\frac{E \vdash a : [l_i:B_i \ ^{i \in 1..n}] \quad j \in 1..n}{E \vdash a.l_j : B_j} \qquad \frac{E \vdash a : A \quad E, x:A \vdash b : B_j \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(x:A)b : A}$$

A characteristic of object-oriented languages is that an object can emulate another object that has fewer methods. We call this notion *subsumption*, and say that an object can *subsume* another one. We define a particular form of subsumption that is induced by a subtyping relation between object types. An object that belongs to a given object type A also belongs to any supertype B of A, and can subsume objects in B. The judgment $E \vdash A <: B$ asserts "A is a subtype of B in environment E".

(Type Top) (Sub Top) (Sub Object) (l_i distinct) (Val Subsumption)

$$\frac{E \vdash \diamond}{E \vdash Top} \qquad \frac{E \vdash A}{E \vdash A <: Top} \qquad \frac{E \vdash B_i \quad \forall i \in 1..n+m}{E \vdash [l_i:B_i \ ^{i \in 1..n+m}] <: [l_i:B_i \ ^{i \in 1..n}]} \qquad \frac{E \vdash a : A \quad E \vdash A <: B}{E \vdash a : B}$$

For convenience, we add a constant, Top, a supertype of every type. The subtyping rule for objects allows a longer object type $[l_i:B_i \ ^{i \in 1..n+m}]$ to be a subtype of a shorter object type $[l_i:B_i \ ^{i \in 1..n}]$. Moreover, object types are *invariant* in their components: $[l_i:B_i \ ^{i \in 1..n+m}] <: [l_i:B_i' \ ^{i \in 1..n}]$ requires $B_i \equiv B_i'$ for $i \in 1..n$. This is necessary for soundness.

The full first-order calculus of objects with subtyping is called $\mathbf{Ob_{1<:}}$; it can be described as a union of formal system fragments $\Delta_x \cup \Delta_K \cup \Delta_{Ob} \cup \Delta_{<:} \cup \Delta_{<:K} \cup \Delta_{<:Ob}$, which are listed in appendices A and C. To facilitate comparison with other first-order calculi, $\mathbf{Ob_{1<:}}$ includes constants and their sorts ($\Delta_K \cup \Delta_{<:K}$), but in this paper we mostly ignore the related issues.

2.3 Equational Theories

We associate an equational theory with $\mathbf{Ob_{1<:}}$, and with each of the calculi we study. The judgment $E \vdash b \leftrightarrow c : A$ asserts that b and c are equal as elements of A. The equational rules for $\mathbf{Ob_{1<:}}$ are $\Delta_= \cup \Delta_{=x} \cup \Delta_{=K} \cup \Delta_{=Ob} \cup \Delta_{=<:} \cup \Delta_{=<:Ob}$ from appendices A and D. We give only the main rules for objects and subtyping: two rules motivated by the use of subtyping, and two evaluation rules corresponding to the semantics of selection and override.

(Eq Subsumption)

$$\frac{E \vdash a \leftrightarrow a' : A \quad E \vdash A <: B}{E \vdash a \leftrightarrow a' : B}$$

(Eq Sub Object) (where $A \equiv [l_i:B_i\ ^{i\in 1..n}]$, $A' \equiv [l_i:B_i\ ^{i\in 1..n},\ l_j:B_j\ ^{j\in n+1..m}]$)

$$\frac{E, x_i:A \vdash b_i : B_i \quad \forall i \in 1..n \qquad E, x_j:A' \vdash b_j : B_j \quad \forall j \in n+1..m}{E \vdash [l_i=\varsigma(x_i:A)b_i\ ^{i\in 1..n}] \leftrightarrow [l_i=\varsigma(x_i:A')b_i\ ^{i\in 1..n+m}] : A}$$

(Eval Select) (where $A \equiv [l_i:B_i\ ^{i\in 1..n}]$, $a \equiv [l_i=\varsigma(x_i:A')b_i\ ^{i\in 1..n+m}]$)

$$\frac{E \vdash a : A \quad j \in 1..n}{E \vdash a.l_j \leftrightarrow b_j\{x_j \leftarrow a\} : B_j}$$

(Eval Override) (where $A \equiv [l_i:B_i\ ^{i\in 1..n}]$, $a \equiv [l_i=\varsigma(x_i:A')b_i\ ^{i\in 1..n+m}]$)

$$\frac{E \vdash a : A \qquad E, x:A \vdash b : B_j \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(x:A)b \leftrightarrow [l_i=\varsigma(x_i:A')b_i\ ^{i\in (1..n+m)-\{j\}},\ l_j=\varsigma(x:A')b]:A}$$

According to rule (Eq Sub Object), an object can be truncated to its externally visible methods, but only if those methods do not depend on hidden methods. The truncated object would not work otherwise.

2.4 Function Types and Recursive Types

Functions (in the form of λ-terms) can be added to $\mathbf{Ob}_{1<:}$ via standard rules, obtaining a calculus called $\mathbf{FOb}_{1<:}$. As discussed in section 3.2, functions can be encoded in terms of objects and second-order constructs.

Recursive types and values can also be added via standard rules, obtaining a calculus called $\mathbf{Ob}_{1<:\mu}$. In order to add recursive types $\mu(X)A$, we give a syntactic criterion for contractiveness in the sense of [MacQueen, Plotkin, Sethi 1986]. If A is formally contractive in the variable X, then the fixpoint $\mu(X)A$ exists and is unique. Object types are formally contractive in all their variables. The explicit isomorphism between $\mu(X)A$ and $A\{X \leftarrow \mu(X)A\}$ is given by two operators called fold and unfold.

The rules for functions and recursion are listed in appendices C and D.

2.5 The Shortcomings of First-Order Calculi

The $\mathbf{Ob}_{1<:\mu}$ calculus, consisting of objects with recursion and subtyping, is a plausible candidate as a paradigm for first-order object-oriented languages. It can be used to express many standard examples from the literature. In particular, we can write types of movable points:

$$P_1 \triangleq \mu(X)[x:\mathrm{Int},\ mv\_x:\mathrm{Int}\rightarrow X] \qquad \text{1-D movable points}$$
$$P_2 \triangleq \mu(X)[x,y:\mathrm{Int},\ mv\_x,mv\_y:\mathrm{Int}\rightarrow X] \qquad \text{2-D movable points}$$

We would then expect to obtain $P_2 <: P_1$, since intuitively P_2 extends P_1. But this is not provable, because the invariance of object types blocks the application of the recursive subtyping rule (Sub Rec) to the result type of mv_x.

Moreover, if we somehow allow $P_2 <: P_1$, we obtain an inconsistency. Briefly, suppose we use subsumption from $p:P_2$ to $p:P_1$, and then override the mv_x method of p with one that returns a proper element of P_1. Then, some other method of p may go wrong because it assumes that mv_x produces an element of P_2.

Hence, the failure of $P_2 <: P_1$ is necessary. At the same time, it is unfortunate: in the common situation where a method returns an updated self, we lose all useful subsumption relations. In [Abadi, Cardelli 1994c] we discuss the standard solution used in object-oriented languages such as Simula-67 and Modula-3. This solution sacrifices static typing information that must be

recovered dynamically, thus abandoning the static typing of subsumption. This paper describes another solution that preserves static typing by taking advantage of second-order constructs.

3. Second-Order Calculi

In this section we present standard second-order extensions of first-order calculi. No new or unusual constructions are introduced. However, second-order quantifiers can be combined with recursive types to produce an interesting new concept that is recognizable as formalizing the type Self. The interaction of Self with object types is the subject of section 4.

We first introduce universal quantifiers and existential quantifiers. From existential quantifiers and recursion we define the Self quantifier. For the purpose of defining Self, only existentials and recursion are needed; one could dispense with universals. For the purposes of object-oriented languages, only the Self quantifier is needed; one could dispense with most of the second-order baggage. However, as usual, universal quantifiers may still be useful to provide polymorphism, and existential quantifiers to provide data abstraction.

We use the notation $B\{X\}$ to single out the occurrences of X free in B; then $B\{A\}$ stands for $B\{X \leftarrow A\}$ when X is clear from the context.

3.1 Universal and Existential Quantifiers

Bounded universal quantifiers $\forall(X<:A)B$ are adopted with the rules of [Cardelli, *et al.* 1991; Curien, Ghelli 1992]. Bounded existential quantifiers $\exists(X<:A)B$ [Cardelli, Wegner 1985] can be encoded as $\forall(Y<:Top)(\forall(X<:A)B\{X\}\rightarrow Y)\rightarrow Y$. However, this encoding does not validate a natural and desirable η rule, called (Eval Repack<:) in appendix D. Therefore, we take bounded existentials as primitive.

We assemble the following second-order calculi using fragments defined in the appendix:

$$\mathbf{F}_{<:} \triangleq \Delta_X \cup \Delta_{\rightarrow} \cup \Delta_{<:} \cup \Delta_{<:X} \cup \Delta_{<:\rightarrow} \cup \Delta_{<:\forall} \cup \Delta_{<:\exists} \qquad \mathbf{F}_{<:\mu} \triangleq \mathbf{F}_{<:} \cup \Delta_{<:\mu}$$

$$\mathbf{Ob}_{<:} \triangleq \Delta_X \cup \Delta_{\mathbf{Ob}} \cup \Delta_{<:} \cup \Delta_{<:X} \cup \Delta_{<:\mathbf{Ob}} \cup \Delta_{<:\forall} \cup \Delta_{<:\exists} \qquad \mathbf{Ob}_{<:\mu} \triangleq \mathbf{Ob}_{<:} \cup \Delta_{<:\mu}$$

$$\mathbf{FOb}_{<:} \triangleq \mathbf{F}_{<:} \cup \Delta_{\mathbf{Ob}} \cup \Delta_{<:\mathbf{Ob}} \qquad \mathbf{FOb}_{<:\mu} \triangleq \mathbf{FOb}_{<:} \cup \Delta_{<:\mu}$$

$\mathbf{F}_{<:}$ is described in [Cardelli, *et al.* 1991], but we assume only the simpler equational theory used in [Curien, Ghelli 1992], and we add existentials. Constant types are left out because free algebras can be encoded [Böhm, Berarducci 1985]. The necessary equational fragments are left implicit, since they can be easily identified (see appendix D). For simplicity we adopt conservative equational rules for existentials, although more ambitious rules may have advantages in combination with objects.

Universals are contravariant and existentials are covariant in their bounds, as reflected by the rules (Sub All) and (Sub Exists). Moreover, if B is covariant in X (written $B\{X^+\}$), then $\exists(X<:A)B\{X^+\}$ is isomorphic to $B\{A^+\}$. This isomorphism does not necessarily hold otherwise. For example, $[l_i:B_i\{X^+\}^{\,i\in 1..n}]$ is not covariant in X even though each $B_i\{X^+\}$ is, and so $\exists(X<:A)[l_i:B_i\{X^+\}^{\,i\in 1..n}]$ is not isomorphic to $[l_i:B_i\{A^+\}^{\,i\in 1..n}]$.

In the next section we show that $\mathbf{Ob}_{<:}$ can encode $\mathbf{F}_{<:}$, and that $\mathbf{Ob}_{<:\mu}$ can encode $\mathbf{F}_{<:\mu}$ (ignoring the first-order η rule). We leave as an open problem whether $\mathbf{Ob}_{<:}$ can be translated into a typed λ-calculus without objects while preserving subtyping. In [Abadi, Cardelli 1994a] we deal with encodings that translate subtypings into coercions.

3.2 Encodings of Product and Function types

Object types can encode product and function types in calculi without subtyping [Abadi, Cardelli 1994c], validating β-reductions. When subtyping is added, the encodings yield invari-

ant product and function types. We review the translation of function types. Strictly speaking, it is defined on type derivations, but we write it as a translation of type-annotated λ-terms.

Translation of invariant function types

$$\langle\!\langle A\to B\rangle\!\rangle \triangleq [\mathrm{arg}:\langle\!\langle A\rangle\!\rangle, \mathrm{val}:\langle\!\langle B\rangle\!\rangle]$$

$$\langle\!\langle b_{A\to B}(a_A)\rangle\!\rangle\rho \triangleq \quad \rho \in \mathrm{Var}\to\mathrm{Term} \quad (\text{with } \langle\!\langle x_A\rangle\!\rangle\rho \triangleq \rho(x))$$
$$(\langle\!\langle b\rangle\!\rangle\rho.\mathrm{arg} \Leftarrow \varsigma(x:\langle\!\langle A\to B\rangle\!\rangle)\,\langle\!\langle a\rangle\!\rangle\rho).\mathrm{val} \quad \text{for } x \notin FV(\langle\!\langle a\rangle\!\rangle\rho)$$
$$\langle\!\langle \lambda(x:A)b_B\rangle\!\rangle\rho \triangleq$$
$$[\mathrm{arg} = \varsigma(x:\langle\!\langle A\to B\rangle\!\rangle)\,x.\mathrm{arg},$$
$$\mathrm{val} = \varsigma(x:\langle\!\langle A\to B\rangle\!\rangle)\,\langle\!\langle b\rangle\!\rangle\rho\{x\leftarrow x.\mathrm{arg}\}]$$

Similarly, product types can be defined by $\langle\!\langle A\times B\rangle\!\rangle \triangleq [\mathrm{fst}:\langle\!\langle A\rangle\!\rangle, \mathrm{snd}:\langle\!\langle B\rangle\!\rangle]$.

These encodings yield invariant product and function types because object types are invariant. At the second order, though, we have quantifiers that are variant in their bounds; combining them with object types, we can define a variant version of function types:

$$A \dot{\to} B \quad \triangleq \quad \forall(X<:A)\,\exists(Y<:B)\,[\mathrm{arg}:X, \mathrm{val}:Y]$$

We obtain $A\dot{\to}B <: A'\dot{\to}B'$ if $A' <: A$ and $B <: B'$.

Translation of variant function types

$$\langle\!\langle A\to B\rangle\!\rangle \triangleq \forall(X<:\langle\!\langle A\rangle\!\rangle)\,\exists(Y<:\langle\!\langle B\rangle\!\rangle)\,[\mathrm{arg}:X, \mathrm{val}:Y]$$

$$\langle\!\langle b_{A\to B}(a_A)\rangle\!\rangle\rho \triangleq \quad \rho \in \mathrm{Var}\to\mathrm{Term} \quad (\text{with } \langle\!\langle x_A\rangle\!\rangle\rho \triangleq \rho(x))$$
$$\text{open } \langle\!\langle b\rangle\!\rangle\rho(\langle\!\langle A\rangle\!\rangle) \text{ as } Y<:\langle\!\langle B\rangle\!\rangle, y:[\mathrm{arg}:\langle\!\langle A\rangle\!\rangle, \mathrm{val}:Y]$$
$$\text{in } (y.\mathrm{arg} \Leftarrow \varsigma(x:[\mathrm{arg}:\langle\!\langle A\rangle\!\rangle, \mathrm{val}:Y])\,\langle\!\langle a\rangle\!\rangle\rho).\mathrm{val} \quad \text{for } Y,y,x \notin FV(\langle\!\langle a\rangle\!\rangle\rho)$$
$$\langle\!\langle \lambda(x:A)b_B\rangle\!\rangle\rho \triangleq$$
$$\lambda(X<:\langle\!\langle A\rangle\!\rangle)$$
$$(\mathrm{pack}\ Y<:\langle\!\langle B\rangle\!\rangle=\langle\!\langle B\rangle\!\rangle,$$
$$[\mathrm{arg} = \varsigma(x:[\mathrm{arg}:X, \mathrm{val}:\langle\!\langle B\rangle\!\rangle])\,x.\mathrm{arg},$$
$$\mathrm{val} = \varsigma(x:[\mathrm{arg}:X, \mathrm{val}:\langle\!\langle B\rangle\!\rangle])\,\langle\!\langle b\rangle\!\rangle\rho\{x\leftarrow x.\mathrm{arg}\}]$$
$$: [\mathrm{arg}:X, \mathrm{val}:Y])$$

This idea gives rise to an encoding of the first-order λ-calculus with subtyping but no η rule into $\mathbf{Ob}_{<:}$. The translation can be extended to recursive types since $A\dot{\to}B$ is contractive in any X, and trivially also to second-order quantifiers. Hence our largest calculus, $\mathbf{FOb}_{<:\mu}$, can be embedded inside $\mathbf{Ob}_{<:\mu}$. We therefore consider $\mathbf{Ob}_{<:\mu}$ as our final pure object calculus.

Trivially, we can obtain covariant product types, since these can be represented in terms of universal quantifiers and variant function types in $\mathbf{F}_{<:}$. A direct encoding is possible as well:

$$A \dot{\times} B \quad \triangleq \quad \exists(X<:A)\,\exists(Y<:B)\,[\mathrm{fst}:X, \mathrm{snd}:Y]$$

We obtain $A\dot{\times}B <: A'\dot{\times}B'$ if $A <: A'$ and $B <: B'$.

In [Cardelli 1991] it is shown that covariant record types $\langle l_i:A_i\ ^{i\in 1..n}\rangle$ can be represented in $\mathbf{F}_{<:}$, using covariant product types. Hence, they are also available in $\mathbf{Ob}_{<:}$.

3.3 An Encoding of Variant Object Types

In [Abadi, Cardelli 1994c] we observe that a general covariance rule for object components is unsound. However, as in the encoding of the λ-calculus just given, we can make covariant

any component whose method is only invoked (like val), and contravariant any component whose method is only overridden (like arg).

The idea for obtaining covariance is exactly the one used for the λ-calculus. We rewrite an object type [m:B, ...] as $\exists(Y<:B)\ [m:Y, ...]$. The former is invariant in B, while the latter is covariant in B. The existential quantifier still allows the invocation of m, but blocks overrides of m from the outside, since the quantifier hides the representation type Y.

The idea for obtaining contravariance is more complicated; the technique used for the λ-calculus does not seem to generalize. To make a component m:B contravariant in an object type $A \triangleq [m:B, ...]$, we first rewrite the type as $A' \triangleq \mu(X)\ \exists(Y<:(X\to B)\to X)\ [m_{in}:Y, m:B, ...]$, where m_{in} is a new method name. Note that A' is still invariant in B. We simulate an override to the method m of an object o by writing the invocation $o.m_{in}(\lambda(s:A')b')$ instead of $o.m \Leftarrow \varsigma(s:A)b$, where b' imitates b. Our intent is that an invocation of m_{in} with argument $\lambda(s:A')b'$ will override m internally. Hence the code for a typical object o of type A' will be:

$$in([m_{in} = \varsigma(s:UA')\ \lambda(f:A'\to B)\ in(s.m \Leftarrow \varsigma(s:UA')\ f(in(s))),\ m = \varsigma(s:UA')\ s.m, ...]):\ A'$$

where $UA' \triangleq [m_{in}:(A'\to B)\to A', m:B, ...]$, and for any a:UA'

$$in(a):\ A' \triangleq fold(A', pack\ Y<:(A'\to B)\to A' = (A'\to B)\to A', a : [m_{in}:Y, m:B, ...])$$

Finally we use subsumption to forget the m component, so that o has the type:

$$\mu(X)\ \exists(Y<:(X\to B)\to X)\ [m_{in}:Y, ...]$$

which is contravariant in B. Once o has this type, its method m cannot be invoked from the outside since it is not even visible.

These techniques for obtaining covariance and contravariance are suggestive but not fully satisfactory. For example, after making two components covariant, we are no longer able to reorder them, since $\exists(X<:A)\ \exists(Y<:B)\ C$ and $\exists(Y<:B)\ \exists(X<:A)\ C$ are not equivalent types. Still, these techniques may inspire an encoding or a semantics for a language with built-in object types with covariant and contravariant components.

3.4 The Self Quantifier

Within the second-order ς-calculus with bounded quantifiers and recursion, $\mathbf{Ob}_{<:\mu}$, we can encode an interesting construction that we call the *Self quantifier*. The Self quantifier is a combination of recursion and bounded existentials, with recursion going "through the bound":

$$\varsigma(X)B \triangleq \mu(Y)\exists(X<:Y)B \qquad (Y \text{ not occurring in } B)$$

In general, any type B{A} can be transformed into a type $\exists(Y<:A)B\{Y\}$ covariant in A. (Recall though that these types are not always isomorphic.) An analogous technique applies to recursive types, and motivates our definition of the Self quantifier. Given an equation X = B{X}, we transform it into $X = \exists(Y<:X)B\{Y\}$. The solution to this equation, namely $\varsigma(X)B\{X\}$, satisfies the subtyping property:

$$\text{if } B\{Y\}<:B'\{Y\} \text{ then } \varsigma(X)B\{Y\} <: \varsigma(X)B'\{Y\},$$

even though we may not have $\mu(X)B\{X\} <: \mu(X)B'\{X\}$.

Modulo an unfolding, ς(X)B is the same as $\exists(X<:\varsigma(X)B)B$. Hence, by analogy with the standard interpretation of existential types, ς(X)B{X} can be understood informally as the type of pairs ⟨C, c⟩ consisting of a subtype C of ς(X)B{X} and an element c of B{C}.

For example, suppose we have an element x of type ς(X)X. Then, choosing ς(X)X as the required subtype of ς(X)X, we obtain ⟨ς(X)X, x⟩ : ς(X)X. Therefore we can construct:

$$\mu(x)\ \langle\varsigma(X)X, x\rangle\ :\ \varsigma(X)X$$

Less trivially, suppose we want to build a memory cell m:M with a read operation rd:Nat and a write operation wr:Nat→M. We can define:

$$M \triangleq \varsigma(X)[rd:Nat, wr:Nat\to X]$$

where the wr method should use its argument to override the rd field. For convenience, we adopt the following abbreviation to unfold a Self quantifier:

$$A(C) \triangleq B\{C\} \quad \text{whenever} \quad A \equiv \varsigma(X)B\{X\} \text{ and } C<:A$$

So, for example, $M(M)\equiv[rd:Nat, wr:Nat\to M]$.

To define a memory cell, we are going to use twice the fact that if x:M(M), then ⟨M, x⟩:M. First, we need a method body for wr that, with self s:M(M) and argument n:Nat, produces a result of type M. Since s.rd:=n has the same type as s, namely M(M), we can use ⟨M, s.rd:=n⟩:M as the body of the wr method. Therefore, we have:

$$m: M \triangleq \langle M, [rd = 0, wr = \varsigma(s:M(M))\ \lambda(n:Nat)\ \langle M, s.rd:=n\rangle]\rangle$$

Building on these intuitions, we now study the abstract properties of the Self quantifier. The two basic operations for ς are similar to the ones for existentials. One operation constructs an element of ς(X)B, given a subtype of ς(X)B and an appropriate value; it is the composition of pack for existentials and fold for recursive types. The other operation inspects an element of ς(X)B (as much as possible) and computes with its contents; it is the composition of unfold for recursive types and open for existentials.

The operation for constructing elements of type ς(X)B, in full generality, binds a type variable. Hence, we need a more complex syntax than the pairing ⟨-,-⟩ used above. We reuse the symbol ς for this second-order construct, in the same way we use λ for both first-order and second-order binders. We refine the notation ⟨C,b⟩ to ς(Y<:A=C)b. The term ς(Y<:A=C)b binds C to Y in b, and requires C to be a subtype of A. Within b, the types Y and C are equivalent. The type of the whole term is A.

We define, for $A\equiv\varsigma(X)B\{X\}$, C<:A, and b{C}:B{C}:

$$\varsigma(Y<:A=C)\ b\{Y\} \triangleq$$
$$\quad fold(A,\ (pack\ Y<:A=C,\ b\{Y\}:B\{Y\}))$$

and, for c:A and d{Y,y}:D, where Y does not occur in D:

$$(use\ c\ as\ Y<:A,\ y:B\{Y\}\ in\ d\{Y,y\}:D) \triangleq$$
$$\quad (open\ unfold(c)\ as\ Y<:A,\ y:B\{Y\}\ in\ d\{Y,y\}:D)$$

The following rules for the Self quantifier can be derived from the rules for μ and ∃. Note in particular the expected subtyping rule, (Sub Self).

Δ_ς

(Type Self)

$$\frac{E,X<:Top \vdash B \quad B>:X}{E \vdash \varsigma(X)B}$$

(Sub Self)

$$\frac{E,X<:Top \vdash B <: B' \quad B,B'>:X}{E \vdash \varsigma(X)B <: \varsigma(X)B'}$$

(Val Self) (where $A \equiv \varsigma(X)B\{X\}$)

$$\frac{E \vdash C <: A \quad E \vdash b\{C\} : B\{C\}}{E \vdash \varsigma(Y<:A=C)b\{Y\} : A}$$

(Val Use) (where $A \equiv \varsigma(X)B\{X\}$)

$$\frac{E \vdash c : A \quad E \vdash D \quad E, Y<:A, y:B\{Y\} \vdash d : D}{E \vdash (\text{use } c \text{ as } Y<:A, y:B\{Y\} \text{ in } d:D) : D}$$

$\Delta_{=\varsigma}$

(Eq Self) (where $A \equiv \varsigma(X)B\{X\}$, $A' \equiv \varsigma(X)B'\{X\}$)

$$\frac{E \vdash C <: A' \quad E \vdash A \quad E, X<:\text{Top} \vdash B'\{X\} <: B\{X\} \quad E \vdash b\{C\} \leftrightarrow b'\{C\} : B'\{C\}}{E \vdash \varsigma(Y<:A=C)b\{Y\} \leftrightarrow \varsigma(Y<:A'=C)b'\{Y\} : A}$$

(Eq Use) (where $A \equiv \varsigma(X)B\{X\}$)

$$\frac{E \vdash c \leftrightarrow c' : A \quad E \vdash D \quad E, Y<:A, y:B\{Y\} \vdash d \leftrightarrow d' : D}{E \vdash (\text{use } c \text{ as } Y<:A, y:B\{Y\} \text{ in } d:D) \leftrightarrow (\text{use } c' \text{ as } Y<:A, y:B\{Y\} \text{ in } d':D) : D}$$

(Eval Unself) (where $A \equiv \varsigma(X)B\{X\}$, $c \equiv \varsigma(Z<:A=C)b\{Z\}$)

$$\frac{E \vdash c : A \quad E \vdash D \quad E, Y<:A, y:B\{Y\} \vdash d\{Y,y\} : D}{E \vdash (\text{use } c \text{ as } Y<:A, y:B\{Y\} \text{ in } d\{Y,y\}:D) \leftrightarrow d\{C,b\{C\}\} : D}$$

(Eval Reself) (where $A \equiv \varsigma(X)B\{X\}$)

$$\frac{E \vdash b : A \quad E, y:A \vdash d\{y\} : D}{E \vdash (\text{use } b \text{ as } Y<:A, y:B\{Y\} \text{ in } d\{\varsigma(Y'<:A=Y)y\} :D) \leftrightarrow d\{b\} : D}$$

Notation We write:

- $\varsigma\langle A,c\rangle$ for $\varsigma(X<:A=A)c$ when X does not occur in c
- $\varsigma(X=A)c\{X\}$ for $\varsigma(X<:A=A)c\{X\}$

The memory cell definition can now be understood formally, with the $\varsigma\langle M,...\rangle$ notation replacing the informal notation $\langle M,...\rangle$:

$$M \triangleq \varsigma(\text{Self})[\text{rd:Nat}, \text{wr:Nat}\rightarrow\text{Self}]$$
$$m{:}\,M \triangleq \varsigma(\text{Self}=M)\,[\text{rd} = 0, \text{wr} = \varsigma(s:M(\text{Self}))\,\lambda(n:\text{Nat})\,\varsigma\langle \text{Self}, s.\text{rd}:=n\rangle]\rangle$$

Later examples frequently adopt this choice of Self as a bound variable.

3.5 A Pure Second-Order Object Calculus

We conclude this section by considering a pure second-order object calculus, **ςOb**, based exclusively on object types and the Self quantifier (see appendix E):

$$\textbf{ςOb} \triangleq \Delta_{\mathbf{x}} \cup \Delta_{\mathbf{Ob}} \cup \Delta_{<:} \cup \Delta_{<:\mathbf{X}} \cup \Delta_{<:\mathbf{Ob}} \cup \Delta_{\varsigma}$$

This calculus departs from second-order λ-calculi by omitting function types and the standard quantifiers. It seems that, in **ςOb**, the only function types that can be encoded are invariant, and that the standard second-order quantifiers are not expressible. Still, as the next section demonstrates, the Self quantifier provides an essential second-order feature of object calculi, namely the type Self, with a form of type recursion. Interestingly, then, **ςOb** is a very small second-order object calculus that covers a spectrum of object-oriented notions.

4. Object Types with Self

The payoff of the Self quantifier comes when it is used in conjunction with object types. Object types with Self are obtained by the combination of the simple object types of section 2.2 with the Self quantifier of section 3.4. These new types allow subsumption between objects containing methods that return self.

In this section, we first derive the rules for the combination of objects with Self. We then show how these derived rules can easily provide typings for some interesting examples. We work entirely within $\mathbf{Ob}_{<:\mu}$, that is, within the second-order calculus with bounded quantifiers, recursion, and simple object types.

4.1 ς-Objects

In this section we examine types of the form:

$$\varsigma(X)[l_i:B_i\{X^+\}^{i\in 1..n}] \qquad \text{where } B\{X^+\} \text{ indicates that X occurs only covariantly in B}$$

We call these structures ς-object types, and ς-objects their corresponding values. The parameter X in $\varsigma(X)[l_i:B_i\{X^+\}^{i\in 1..n}]$ is intended as the Self type. Note that we do not require that $[l_i:B_i\{X\}^{i\in 1..n}]$ be covariant in X, only that each $B_i\{X\}$ be covariant in X.

Although ς-object types are obtained by applying a Self quantifier (which has no covariance restrictions) to an object type, for the most part we consider $\varsigma(X)[l_i:B_i\{X^+\}^{i\in 1..n}]$ as a single type construction. The covariance requirement is necessary when selecting components of ς-objects. For emphasis, we use a special syntax for the combination of Self quantifiers, object types, and the covariance requirement:

$$\varsigma(X^+)[l_i:B_i\{X\}^{i\in 1..n}] \triangleq \varsigma(X)[l_i:B_i\{X\}^{i\in 1..n}] \quad \text{when X occurs only covariantly in the } B_i$$

The covariance requirement implies that X_i must not occur within any object type within B_i, since object types are invariant in their components. For example, ς(X)[l: ς(Y)[m:X, n:Y]] violates the covariance requirement. Hence, informally, we may say that Self types do not nest: there is a single meaningful Self type within each pair of object brackets.

It is often useful to consider an unfolding A(C) of a ς-object type A:

$$A(C) \triangleq [l_i:B_i\{C\}^{i\in 1..n}] \qquad \text{whenever} \quad A \equiv \varsigma(X^+)[l_i:B_i\{X\}^{i\in 1..n}] \text{ and } C<:A$$

We frequently consider A(X), for a variable X, and the *self-unfolding* A(A) of A. (When building an element of type A it is very common to build first an element of type A(A).) We say that a type C<:A and an element of A(C) constitute an *implementation* of A, since they can be used to build an element of A. Then C is the *representation type* for the implementation.

The operations on ς-objects are defined as follows. Assume that a has type A with $A\equiv \varsigma(X^+)[l_i:B_i\{X\}^{i\in 1..n}]$ and $A(X)\equiv[l_i:B_i\{X^+\}^{i\in 1..n}]$, and set, with some overloading of notation:

$$a.l_j \triangleq$$
(use a as Z<:A, y:A(Z) in $y.l_j : B_i\{A^+\}$)

$$a.l_j \Leftarrow \varsigma(Y<:A, y:A(Y), x:A(Y))b\{Y,y,x\} \triangleq$$
(use a as Z<:A, y:A(Z) in $\varsigma(Y<:A=Z)\ (y.l_j \Leftarrow \varsigma(x:A(Y))b\{Y,y,x\}) : A$)

The ς-object selection operation reduces fairly simply to a regular selection operation on the underlying object.

The ς-object override operation is more interesting, although similarly it reduces to an override operation on the underlying object. The overriding method b can take advantage of three variables: (1) Y<:A, the unknown subtype of A that was used to construct a; (2) y:A(Y),

the raw object inside a, which can be thought of as the *old self*; y is the value of self at the time the overriding takes place, containing the old version of method l_j; (3) x:A(Y), the regular self of the overriding method b. From these variables, b must produce a result of type $B_j\{Y^+\}$, parametrically in Y.

Combining the rules for objects and for Self quantification with the definitions above, we derive the rules given in appendix B.

The most remarkable fact is that the (Sub ςObject) rule holds for ς-object types. We recall that in section 2.5 we found that the analogous rule for recursive object types did not hold.

The (Val ςObject) rule can be used to build a ς-object $\varsigma(Y<:A=C)b\{Y\}$ from a subtype C of the desired ς-object type A, and from a regular object b{C}. The Y variable in b{Y} is the Self type, in case the methods of b need to refer to it.

When building a ς-object by (Val ςObject) we can take C<:A to be a concrete object type, often choosing C=A; we rarely need to work parametrically for an arbitrary X<:A. However, the flexibility of using an arbitrary subtype of A is critical in the derivation of (Val ςOverride). In section 5.1 we will see that this flexibility has a price.

The (Eq Sub ςObject) rule is of limited power because the same C appears on both sides of the conclusion. We can trace back this limitation to a similar one in the rules for existentials.

4.2 Examples

We are now ready to examine some object-oriented examples (cf. [Abadi, Cardelli 1994c]). We find that these examples can be typed rather easily when seen in terms of ς-objects, even when a method needs to return or to modify self. When constructing a fixed ς-object, its methods are not required to operate on an arbitrary self: they just need to match the given representation type of the object being constructed. That is, to construct a ς-object of type $A \equiv \varsigma(X^+)[l_i:B_i\{X\}^{\,i\in 1..n}]$ we need only a set of methods $b_j:B_j\{A^+\}$ (not $b_j:B_j\{X^+\}$ for an arbitrary X<:A). Moreover, each of these methods can assume the existence a self parameter $x_j:[l_i:B_i\{A^+\}^{\,i\in 1..n}]$. (See the rules (Val ςObject) and (Val Object).)

4.2.1 Movable Points

This is a modified version of the problematic example of section 2.5, obtained by replacing μ with ς. We define the types of one-dimensional and two-dimensional movable points:

$$P_1 \triangleq \varsigma(Self^+)[x:Int,\ mv\_x:Int\to Self]$$
$$P_2 \triangleq \varsigma(Self^+)[x,y:Int,\ mv\_x,mv\_y:Int\to Self]$$

We have the desirable property $P_2 <: P_1$, by (Sub ςObject).

Next we define the one-dimensional origin point, where Self is P_1:

$$origin_1 : P_1 \triangleq \varsigma(Self=P_1)\ [x=0,\ mv\_x=\varsigma(s:P_1(Self))\lambda(dx:Int)\varsigma\langle Self,\ s.x:=s.x+dx\rangle]$$

The rule (Val ςSelect) allows us to invoke methods whose type involves Self:

$$origin_1.mv\_x : Int\to P_1$$

Moreover, the equational theory allows us to derive expected equivalencies, such as:

$$origin_1.mv\_x(1)$$
$$\leftrightarrow\ \varsigma(Self=P_1)\ [x=1,\ mv\_x=\varsigma(s:P_1(Self))\lambda(dx:Int)\varsigma\langle Self,\ s.x:=s.x+dx\rangle]\ : P_1$$

that is, the unit point equals the result of moving the origin point.

4.2.2 Object-Oriented Natural Numbers

The type of Scott numerals [Wadsworth 1980] has an object-oriented counterpart:

$$N_{Ob} \triangleq \varsigma(Self^{+})[succ:Self,\ case:\forall(Z<:Top)Z\rightarrow(Self\rightarrow Z)\rightarrow Z]$$

This type is well-formed because $\forall(Z<:Top)Z\rightarrow(X\rightarrow Z)\rightarrow Z$ is covariant in X.

The zero numeral can be defined as:

$$\begin{aligned}&zero_{Ob} : N_{Ob} \triangleq\\ &\ \varsigma(Self=N_{Ob})\\ &\ \ [\ case = \lambda(Z<:Top)\ \lambda(z:Z)\ \lambda(f:Self\rightarrow Z)\ z,\\ &\ \ \ succ = \varsigma(n:N_{Ob}(Self))\ \varsigma\langle Self,\ n.case := \lambda(Z<:Top)\ \lambda(z:Z)\ \lambda(f:Self\rightarrow Z)\ f(\varsigma\langle Self,n\rangle)\rangle]\end{aligned}$$

The other numerals can be obtained from $zero_{Ob}$. Some familiar operations are expressible:

$$\begin{aligned}succ &: N_{Ob}\rightarrow N_{Ob} \triangleq \lambda(n:N_{Ob})\ n.succ\\ pred &: N_{Ob}\rightarrow N_{Ob} \triangleq \lambda(n:N_{Ob})\ n.case(N_{Ob})(zero_{Ob})(\lambda(p:N_{Ob})p)\\ iszero &: N_{Ob}\rightarrow Bool \triangleq \lambda(n:N_{Ob})\ n.case(Bool)(true)(\lambda(p:N_{Ob})false)\end{aligned}$$

4.2.3 A Calculator

Our final example is that of a calculator object. We exploit the ability to override methods to record the pending arithmetic operation. When an operation add or sub is entered, the equals method is overridden with code for addition or subtraction. The first two components (arg, acc) are needed for the internal operation of the calculator, while the other four (enter, add, sub, equals) provide the user interface.

$$C = \varsigma(Self^{+})[arg,acc:\ Real,\ enter:\ Real\rightarrow Self,\ add,sub:\ Self,\ equals:\ Real]$$

By subsumption, the calculator also has type:

$$Calc = \varsigma(Self^{+})[enter:\ Real\rightarrow Self,\ add,sub:\ Self,\ equals:\ Real]$$

This shorter Calc type is the one shown to users of the calculator.

$$\begin{aligned}&calculator:\ C \triangleq\\ &\ \varsigma(Self=C)\\ &\ \ [arg = 0.0,\\ &\ \ \ acc = 0.0,\\ &\ \ \ enter = \varsigma(s:C(Self))\ \lambda(n:Real)\ \varsigma\langle Self,\ s.arg := n\rangle,\\ &\ \ \ add = \varsigma(s:C(Self))\ \varsigma\langle Self,\ (s.acc := s.equals).equals \Leftarrow \varsigma(s':C(Self))\ s'.acc+s'.arg\rangle,\\ &\ \ \ sub = \varsigma(s:C(Self))\ \varsigma\langle Self,\ (s.acc := s.equals).equals \Leftarrow \varsigma(s':C(Self))\ s'.acc-s'.arg\rangle,\\ &\ \ \ equals = \varsigma(s:C(Self))\ s.arg]\end{aligned}$$

This definition is meant to provide the following behavior:

$$\begin{aligned}&calculator\ .enter(5.0)\ .equals && = && 5.0\\ &calculator\ .enter(5.0)\ .sub\ .enter(3.5)\ .equals && = && 1.5\\ &calculator\ .enter(5.0)\ .add\ .add\ .equals && = && 15.0\end{aligned}$$

A scientific calculator can also be defined, with additional state and operations. Its inner design could be quite different from that of our basic calculator, but the scientific calculator's type may still be a subtype of Calc.

5. Overriding and Self

In this section we discuss attempts to override methods that return self.

If we want to override a method of a ς-object of type A, the new method must work for any possible subtype of A. This is because the ς-object might have been constructed as an element of an unknown proper subtype of A. If the new method returns self, it is critical that the type of its result be the unknown subtype of A, because one of the other methods may be invoked on the result. We say that the overriding method must be "parametric in self "; this turns out to be a difficult criterion to meet.

It should not be too surprising that it is hard to override methods that return self. After all, the technique for obtaining ς-object subtypings is based on that of section 3.3 for obtaining covariant object components, which cannot be usefully overridden.

5.1 Overriding from the Outside

At the beginning of section 4.2 we remark how easy it is to create a ς-object, because its initial methods needs to work only for the actual type of the object being constructed. In particular, methods that override self present no difficulties. However, if we want to override a method of an existing ς-object o:A, the new method must work for any possible B<:A, because o might have been built as an element of B. We do not know either the "true type" of o, or the "true type" of the self parameters of its methods. When overriding a method of o, the overriding method can assume only that the object has been constructed from an unknown Self<:A. The same difficulty would likely surface at object-creation time, if we were creating objects incrementally, adding methods to an empty object, instead of creating full objects at once.

This is where we need the complex derived rule for overriding ς-objects, (Val ςOverride). Consider, for example, the type:

$$Q \triangleq \varsigma(\mathrm{Self}^+)[n,f:\mathrm{Int},\ m:\mathrm{Self}] \qquad \text{with} \qquad Q(X) \equiv [n,f:\mathrm{Int},\ m:X]$$

An overriding method for $o \equiv \varsigma(Y<:Q=C)b\{Y\}$ can use in its body the variables Self<:Q, x':Q(Self), and x:Q(Self), where x' is in fact b{C}, according to (Eval ςOverride), and x is the self of the new method. We can therefore override the f method of Q with any of the following method bodies:

o.f ⇐ ς(Self<:Q, x':Q(Self), x:Q(Self)) *(any of the following:)*

x'.n + 1	setting o.f to produce b.n + 1 (constantly)
x.n + 1	setting o.f to produce 1 + the value of n when f is invoked
(x.n:=x'.n).n	setting o.f to update n with b.n (constantly) when f is invoked

Let us now attempt to override the m method. The typing rule (Val ςOverride) requires that, from the variables Self<:Q, x':Q(Self), x:Q(Self) at its disposal, the overriding method must produce a value of type Self. Here are some possibilities:

o.m ⇐ ς(Self<:Q, x':Q(Self), x:Q(Self)) *(any of the following:)*

x'.m	setting o.m to produce the current b.m (constantly)
x.m	setting o.m to diverge

However, we cannot override o.m with anything useful. Note, first, that we cannot synthesize a value of type Self from scratch. Second, we cannot return x' or x, nor ς⟨Q,x'⟩ or ς⟨Q,x⟩, because none of these can be given type Self. Third, ς⟨Self,x⟩:Self is not derivable, for an unknown Self<:Q. Finally, any update to x' or x will preserve their original type, so the updated x' or x cannot be returned either.

Moreover, it would be unsound to ignore these typing problems and return, say, $\varsigma\langle Self,x\rangle$ or $\varsigma\langle Self,x'\rangle$. The reason for unsoundness can be traced back to the rule for constructing ς-objects. Because of the flexibility we have in constructing ς-objects out of proper subtypes of their types, the x and x' parameters at our disposal when overriding may be "shorter" than the subtype used originally when constructing the object.

In conclusion, we discover that the (Val ςOverride) rule, although very powerful for overriding simple methods and fields, is not sufficient to allow us to override methods that return a value of type Self. One solution to this problem is discussed in the next section.

5.2 Recoup

In this section we introduce a special method called *recoup* with an associated run-time invariant. Recoup is a method that returns self immediately. The invariant asserts that the result of recoup is its host object.

5.2.1 The Recoup Method

Let us redefine the type Q of section 5.1, by adding a method called recoup:

$$Q \triangleq \varsigma(Self^+)[\text{recoup: Self, n,f:Int, m:Self}]$$

We can build an element of Q as follows:

$$o : Q \triangleq \varsigma(Self=Q)\ b, \quad \text{where} \quad b \equiv [\text{recoup}=\varsigma(s:Q(Self))\varsigma\langle Self,s\rangle, n=..., f=..., m=...]$$

Then, we can typecheck:

$$o.m \Leftarrow \varsigma(Self<:Q, s':Q(Self), s:Q(Self))\ s'.\text{recoup} \ : \ Q$$

since s'.recoup has type Self. Moreover, the behavior obtained could be useful, and corresponds to storing the current object into the new object (like a "backup" operation).

We say that a method of the form $\varsigma(s:B(Self))\varsigma\langle Self,s\rangle$, in the context of a ς-object of the form $\varsigma(Self<:B=B)[...]$, is a recoup method. Intuitively, recoup allows us to recover a "parametric self " s'.recoup, which equals o but has type Self<:Q and not just type Q. This technique is particularly useful after an override on a value of type Self<:Q, because the result of the override only has type Q.

In general, if B has the form $\varsigma(Self^+)$[recoup:Self, ...] then we can write useful polymorphic functions of type $\forall(Self<:B)\ B(Self)\rightarrow Self$ that are not available without recoup, such as:

$$g : \forall(Self<:Q)\ Q(Self)\rightarrow Self \triangleq$$
$$\lambda(Self<:Q)\ \lambda(s:Q(Self))\ (s.m:=s.\text{recoup}).\text{recoup}$$

Such functions are sufficiently parametric to be used in overrides from the outside, as in:

$$o.m \Leftarrow \varsigma(Self<:Q, s':Q(Self), s:Q(Self))\ g(Self)(s)$$

The technique just described gives the correct result only as long as recoup is bound to $\varsigma(s:Q(Self))\varsigma\langle Self,s\rangle$. Otherwise, the operational behavior is not the expected one. The correctness of typing, on the other hand, does not depend on the recoup invariant.

An invariant of this kind is, we believe, perfectly acceptable for a programming language: recoup would be a distinguished component that is appropriately initialized and that cannot be overridden. Even without language support, we may be disciplined enough to preserve the recoup invariant, and thus we may solve the problem of overriding methods with result type Self.

5.2.2 Recoup as the Only True Method

Despite its trivial code, recoup has remarkable power: using recoup we can replace other proper methods with simple fields. We show this for an object type A without Self, but our technique might extend to ς-object types. Suppose we have:

$$A \triangleq [m:B]$$
$$o : A \triangleq [m=\varsigma(s:A)b]$$

We rewrite A and o, introducing a Self quantifier and a recoup method, and changing the method m into a field m' containing a function. This modification requires using the general Self quantifier without covariance restrictions (from section 3.4). We take:

$$A' \triangleq \varsigma(Self)[recoup:Self, m':Self\to B]$$
$$o' : A' \triangleq \varsigma(Self=A')\,[recoup=\varsigma(s:A'(Self))\varsigma\langle Self,s\rangle, m'=\lambda(s:Self)b']$$

Thus the proper method m=ς(s:A)b in o is replaced with the field m'=λ(s:A'(Self))b' in o'. Next we consider how to simulate operations on elements of A with operations on elements of A', and specifically how to encode invocation and overriding. Using our encoding of invocation and overriding, we can find a b' that imitates b.

We cannot give a type to o'.m'. (Self must not escape the scope of ς, and the contravariant occurrence of Self, unlike the covariant ones, cannot be replaced by its bound.) However, we can extract o'.m' inside the scope of ς and immediately apply it to o'.recoup, thus eliminating the single contravariant occurrence of Self before exiting the scope of the quantifier:

$$invoke(o', m') \triangleq \text{use } o' \text{ as } Y<:A', y:A'(Y) \text{ in } y.m'(y.recoup) : B$$

If o'.recoup is ς(s:A'(A'))ς⟨A',s⟩ as expected then invoke(o', m') has the same behavior as o.m.

Furthermore, m' can be overridden with any function f: ∀(Y<:A')Y→B:

$$override(o', m', f) \triangleq \text{use } o' \text{ as } Y<:A', y:A'(Y) \text{ in } \varsigma(X=Y)\ y.m':=f(X) : A'$$

More general override constructs are available as well, because what used to be methods can now be extracted as functions within the scope of an override. For example, when we have a movable point o' of type ς(Self)[recoup:Self, mv_x': Self→Int→Self, ...] we can override the move method (a function field) with one that runs the old method with a different parameter:

use o' as Y<:A', y:[recoup:Y, mv_x': Y→Int→Y, ...]
in ς(Self=Y) y.mv_x':=λ(s:Self)λ(n:Int)y.mv_x'(s)(n+1)
: ς(Self)[recoup:Self, mv_x': Self→Int→Self, ...]

Thus we can reuse the code of old methods, and not just their results, in defining new methods. This ability is reminiscent of that provided by "super" and "method wrappers" facilities.

6. Related Work

We finish with some comparisons with the most closely related work [Bruce 1993; Mitchell, Honsell, Fisher 1993], also discussed in [Abadi, Cardelli 1994c].

Mitchell *et al.* do not support subsumption but allow object extension; Bruce formalizes two distinct subtyping relations. We have fixed-size objects, and support subsumption by using a single subtyping relation. Like Mitchell *et al.* and unlike Bruce, we do not distinguish between objects and object generators, and we allow the overriding of proper methods in objects.

Many common examples can be expressed in all these systems, with some noticeable exceptions. (1) We cannot represent inheritance directly, for example to produce a color point

from an existing point, but we can imitate it [Abadi, Cardelli 1994b]. (2) Using quantifiers and the type Self, we are able to give uniform typings for Scott-style object-oriented numerals and similar terms. They do not include universal quantifiers.

Mitchell *et al.* and Bruce present first-order systems with primitive objects and with a built-in Self type. In contrast we have a full second-order system where Self is obtained by an encoding. The rules for Self are similar in all these systems. The rules are always complex, but ours are derivable from those for elementary objects without Self. Hence, we may claim some success in explaining Self.

Acknowledgments

John Lamping prompted us to think about encoding covariant components. Gordon Plotkin suggested we should have a system with the Self quantifier as the only second-order construct.

Appendix A: Simple-Objects Fragments

These are the typing and equality rules for simple objects.

Δ_{Ob}

(Type Object) (l_i distinct)

$$\frac{E \vdash B_j \quad \forall i \in 1..n}{E \vdash [l_i:B_{i\ i\in 1..n}]}$$

(Val Object) (where $A \equiv [l_i:B_{i\ i\in 1..n}]$)

$$\frac{E, x_j:A \vdash b_j : B_j \quad \forall i \in 1..n}{E \vdash [l_i=\varsigma(x_i:A)b_{i\ i\in 1..n}] : A}$$

(Val Select)

$$\frac{E \vdash a : [l_i:B_{i\ i\in 1..n}] \quad j \in 1..n}{E \vdash a.l_j : B_j}$$

(Val Override) (where $A \equiv [l_i:B_{i\ i\in 1..n}]$)

$$\frac{E \vdash a : A \quad E, x:A \vdash b : B_j \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(x:A)b : A}$$

$\Delta_{<:Ob}$

(Sub Object) (l_i distinct)

$$\frac{E \vdash B_i \quad \forall i \in 1..n+m}{E \vdash [l_i:B_{i\ i\in 1..n+m}] <: [l_i:B_{i\ i\in 1..n}]}$$

$\Delta_{=Ob}$

(Eq Object) (where $A \equiv [l_i:B_{i\ i\in 1..n}]$)

$$\frac{E, x_i:A \vdash b_i \leftrightarrow b_i' : B_i \quad \forall i \in 1..n}{E \vdash [l_i=\varsigma(x_i:A)b_{i\ i\in 1..n}] \leftrightarrow [l_i=\varsigma(x_i:A)b_i'_{\ i\in 1..n}] : A}$$

(Eq Select)

$$\frac{E \vdash a \leftrightarrow a' : [l_i:B_{i\ i\in 1..n}] \quad j \in 1..n}{E \vdash a.l_j \leftrightarrow a'.l_j : B_j}$$

(Eq Override) (where $A \equiv [l_i:B_{i\ i\in 1..n}]$)

$$\frac{E \vdash a \leftrightarrow a' : A \quad E, x:A \vdash b \leftrightarrow b' : B_j \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(x:A)b \leftrightarrow a'.l_j \Leftarrow \varsigma(x:A)b' : A}$$

(Eval Select)
$$\frac{E \vdash a : A \quad j \in 1..n}{E \vdash a.l_j \leftrightarrow b_j\{x_j \leftarrow a\} : B_j}$$

(Eval Override) (in both: $A \equiv [l_i : B_i\ ^{i \in 1..n}]$, $a \equiv [l_i = \varsigma(x_i : A')b_i\ ^{i \in 1..n+m}]$)
$$\frac{E \vdash a : A \quad E, x : A \vdash b : B_j \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(x:A)b \leftrightarrow [l_i = \varsigma(x_i : A')b_i\ ^{i \in (1..n+m)-\{j\}}, l_j = \varsigma(x:A')b] : A}$$

$\Delta_{=Ob<:}$

(Eq Sub Object) (where $A \equiv [l_i : B_i\ ^{i \in 1..n}]$, $A' \equiv [l_i : B_i\ ^{i \in 1..n}, l_j : B_j\ ^{j \in n+1..m}]$)
$$\frac{E, x_i : A \vdash b_i : B_i \quad \forall i \in 1..n \qquad E, x_j : A' \vdash b_j : B_j \quad \forall j \in n+1..m}{E \vdash [l_i = \varsigma(x_i : A)b_i\ ^{i \in 1..n}] \leftrightarrow [l_i = \varsigma(x_i : A')b_i\ ^{i \in 1..n+m}] : A}$$

Appendix B: ς-Objects Fragments (Derived Rules)

These are derived rules for the combination of simple objects and the Self quantifier.

$\Delta_{\varsigma+}$

(Type ςObject)
$$\frac{E, X <: Top \vdash B_i\{X^+\} \quad \forall i \in 1..n}{E \vdash \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n}]}$$

(Sub ςObject) (l_i distinct)
$$\frac{E, X <: Top \vdash B_i\{X^+\} \quad \forall i \in 1..n+m}{E \vdash \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n+m}] <: \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n}]}$$

(Val ςObject) (where $A \equiv \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n}]$)
$$\frac{E \vdash C <: A \quad E \vdash b\{C\} : A(C)}{E \vdash \varsigma(Y <: A = C)\, b\{Y\} : A}$$

(Val ςSelect)
$$\frac{E \vdash a : A \quad j \in 1..n}{E \vdash a.l_j : B_j\{A^+\}}$$

(Val ςOverride) (in both: $A \equiv \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n}]$)
$$\frac{E \vdash a : A \quad E, Y <: A, y : A(Y), x : A(Y) \vdash b : B_j\{Y^+\} \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(Y <: A, y : A(Y), x : A(Y))b : A}$$

$\Delta_{=\varsigma+}$

(Eq ςObject) (where $A \equiv \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n}]$, $A' \equiv \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n+m}]$)
$$\frac{E \vdash C <: A' \quad E \vdash b\{C\} \leftrightarrow b'\{C\} : A'(C)}{E \vdash \varsigma(Y <: A = C)b\{Y\} \leftrightarrow \varsigma(Y <: A' = C)b'\{Y\} : A}$$

(Eq Sub ςObject) (where $A \equiv \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n}]$, $A' \equiv \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n+m}]$)
$$\frac{E \vdash C <: A' \quad E, x_i : A(C) \vdash b_i\{C\} : B_i\{C\} \quad \forall i \in 1..n \qquad E, x_j : A'(C) \vdash b_j\{C\} : B_j\{C\} \quad \forall j \in n+1..m}{E \vdash \varsigma(Y <: A = C)[l_i = \varsigma(x_i : A(Y))b_i\{Y\}\ ^{i \in 1..n}] \leftrightarrow \varsigma(Y <: A' = C)[l_i = \varsigma(x_i : A'(Y))b_i\{Y\}\ ^{i \in 1..n+m}] : A}$$

(Eq ςSelect) (where $A \equiv \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n}]$)
$$\frac{E \vdash a \leftrightarrow a' : A \quad j \in 1..n}{E \vdash a.l_j \leftrightarrow a'.l_j : B_j\{A^+\}}$$

(Eq ςOverride) (where $A \equiv \varsigma(X^+)[l_i : B_i\{X\}\ ^{i \in 1..n}]$)
$$\frac{E \vdash a \leftrightarrow a' : A \quad E, Y <: A, y : A(Y), x : A(Y) \vdash b \leftrightarrow b' : B_j\{Y^+\} \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(Y <: A, y : A(Y), x : A(Y))b \leftrightarrow a'.l_j \Leftarrow \varsigma(Y <: A, y : A(Y), x : A(Y))b' : A}$$

(Eval ςSelect) (where $A \equiv \varsigma(X^+)[l_i:B_i\{X\}^{\ i\in 1..n}]$, $c \equiv \varsigma(Z<:A=C)a\{Z\}$)

$$\frac{E \vdash c : A \quad j \in 1..n}{E \vdash c.l_j \leftrightarrow a\{C\}.l_j : B_j\{A^+\}}$$

(Eval ςOverride) (where $A \equiv \varsigma(X^+)[l_i:B_i\{X\}^{\ i\in 1..n}]$, $c \equiv \varsigma(Z<:A=C)a\{Z\}$)

$$\frac{E \vdash c : A \quad E, Y<:A, y:A(Y), x:A(Y) \vdash b\{Y,y,x\} : B_j\{Y^+\} \quad j \in 1..n}{E \vdash c.l_j \Leftarrow \varsigma(Y<:A,y:A(Y),x:A(Y))b\{Y,y,x\} \leftrightarrow \varsigma(Z<:A=C)\ a\{Z\}.l_j \Leftarrow \varsigma(x:A(Z))b\{Z,a\{Z\},x\} : A}$$

Appendix C: Other Typing Fragments

Δ_x

(Env ∅)
$$\frac{}{\emptyset \vdash \diamond}$$

(Env x)
$$\frac{E \vdash A \quad x \notin dom(E)}{E,x:A \vdash \diamond}$$

(Val x)
$$\frac{E', x:A, E'' \vdash \diamond}{E', x:A, E'' \vdash x:A}$$

Δ_K

(Type Const)
$$\frac{E \vdash \diamond \quad K \in Sort}{E \vdash K}$$

(Val Const)
$$\frac{k \in Op(K_i^{\ i\in 1..n+1}) \quad E \vdash a_i : K_i \quad \forall i \in 1..n}{E \vdash k(a_i^{\ i\in 1..n}) : K_{n+1}}$$

$\Delta_{\rightarrow}$

(Type Arrow)
$$\frac{E \vdash A \quad E \vdash B}{E \vdash A \rightarrow B}$$

(Val Fun)
$$\frac{E, x:A \vdash b : B}{E \vdash \lambda(x:A)b : A \rightarrow B}$$

(Val Appl)
$$\frac{E \vdash b : A \rightarrow B \quad E \vdash a : A}{E \vdash b(a) : B}$$

$\Delta_{<:}$

(Sub Refl)
$$\frac{E \vdash A}{E \vdash A <: A}$$

(Sub Trans)
$$\frac{E \vdash A <: B \quad E \vdash B <: C}{E \vdash A <: C}$$

(Val Subsumption)
$$\frac{E \vdash a : A \quad E \vdash A <: B}{E \vdash a : B}$$

(Type Top)
$$\frac{E \vdash \diamond}{E \vdash Top}$$

(Sub Top)
$$\frac{E \vdash A}{E \vdash A <: Top}$$

$\Delta_{<:K}$

(Sub Sort)
$$\frac{E \vdash \diamond \quad (K,K') \in SubSort}{E \vdash K <: K'}$$

$\Delta_{<:\rightarrow}$

(Sub Arrow)

$$\frac{E \vdash A' <: A \quad E \vdash B <: B'}{E \vdash A \rightarrow B <: A' \rightarrow B'}$$

$\Delta_{<:X}$

(Env X<:)

$$\frac{E \vdash A \quad X \notin dom(E)}{E, X<:A \vdash \diamond}$$

(Type X<:)

$$\frac{E', X<:A, E'' \vdash \diamond}{E', X<:A, E'' \vdash X}$$

(Sub X)

$$\frac{E', X<:A, E'' \vdash \diamond}{E', X<:A, E'' \vdash X<:A}$$

$\Delta_{<:\mu}$

(Type Rec<:)

$$\frac{E, X<:Top \vdash A \quad A>X}{E \vdash \mu(X)A}$$

(Sub Rec)

$$\frac{E \vdash \mu(X)A \quad E \vdash \mu(Y)B \quad E, Y<:Top, X<:Y \vdash A<:B}{E \vdash \mu(X)A <: \mu(Y)B}$$

(Val Fold)

$$\frac{E \vdash a : A\{X \leftarrow \mu(X)A\}}{E \vdash fold(\mu(X)A, a) : \mu(X)A}$$

(Val Unfold)

$$\frac{E \vdash a : \mu(X)A}{E \vdash unfold(a) : A\{X \leftarrow \mu(X)A\}}$$

(Val Rec)

$$\frac{E, x:A \vdash a : A}{E \vdash \mu(x:A)a : A}$$

$\Delta_{<:\forall}$

(Type All<:)

$$\frac{E, X<:A \vdash B}{E \vdash \forall(X<:A)B}$$

(Sub All)

$$\frac{E \vdash A' <: A \quad E, X<:A' \vdash B <: B'}{E \vdash \forall(X<:A)B <: \forall(X<:A')B'}$$

(Val Fun2<:)

$$\frac{E, X<:A \vdash b : B}{E \vdash \lambda(X<:A)b : \forall(X<:A)B}$$

(Val Appl2<:)

$$\frac{E \vdash b : \forall(X<:A)B\{X\} \quad E \vdash A'<:A}{E \vdash b(A') : B\{A'\}}$$

$\Delta_{<:\exists}$

(Type Exists<:)

$$\frac{E, X<:A \vdash B}{E \vdash \exists(X<:A)B}$$

(Sub Exists)

$$\frac{E \vdash A <: A' \quad E, X<:A \vdash B <: B'}{E \vdash \exists(X<:A)B <: \exists(X<:A')B'}$$

(Val Pack<:)

$$\frac{E \vdash C <: A \quad E \vdash b\{C\} : B\{C\}}{E \vdash (pack\ X<:A=C, b\{X\}:B\{X\}) : \exists(X<:A)B\{X\}}$$

(Val Open<:)

$$\frac{E \vdash c : \exists(X<:A)B \quad E \vdash D \quad E, X<:A, x:B \vdash d : D}{E \vdash (open\ c\ as\ X<:A, x:B\ in\ d:D) : D}$$

The relation $A \succ Y$ (type expression A is formally contractive in variable Y) is:

$X \succ Y$	if $X \neq Y$	
$Top \succ Y$	always	
$[l_i:B_i\ ^{i\in 1..n}] \succ Y$	always	
$A \to B \succ Y$	always	
$\mu(X)A \succ Y$	if $A \succ Y$	
$\forall(X<:A)B \succ Y$	if $B \succ X$ and $B \succ Y$	(no requirement on A)
$\exists(X<:A)B \succ Y$	if $B \succ X$ and $B \succ Y$	(no requirement on A)

Appendix D: Other Equational Fragments

$\Delta_{\simeq}$

(Eq Symm)

$$\frac{E \vdash a \leftrightarrow b : A}{E \vdash b \leftrightarrow a : A}$$

(Eq Trans)

$$\frac{E \vdash a \leftrightarrow b : A \quad E \vdash b \leftrightarrow c : A}{E \vdash a \leftrightarrow c : A}$$

$\Delta_{\simeq x}$

(Eq x)

$$\frac{E', x:A, E'' \vdash \diamond}{E', x:A, E'' \vdash x \leftrightarrow x : A}$$

$\Delta_{\simeq K}$

(Eq Const)

$$\frac{k \in Op(K_i\ ^{i\in 1..n+1}) \quad E \vdash a_i \leftrightarrow a_i' : K_i \quad \forall i \in 1..n}{E \vdash k(a_i\ ^{i\in 1..n}) \leftrightarrow k(a_i'\ ^{i\in 1..n}) : K_{n+1}}$$

$\Delta_{\simeq \to}$

(Eq Fun)

$$\frac{E, x:A \vdash b \leftrightarrow b' : B}{E \vdash \lambda(x:A)b \leftrightarrow \lambda(x:A)b' : A \to B}$$

(Eq Appl)

$$\frac{E \vdash b \leftrightarrow b' : A \to B \quad E \vdash a \leftrightarrow a' : A}{E \vdash b(a) \leftrightarrow b'(a') : B}$$

(Eval Beta)

$$\frac{E \vdash \lambda(x:A)b : A \to B \quad E \vdash a : A}{E \vdash (\lambda(x:A)b)(a) \leftrightarrow b\{x \leftarrow a\} : B}$$

(Eval Eta)

$$\frac{E \vdash b : A \to B \quad x \notin dom(E)}{E \vdash \lambda(x:A)b(x) \leftrightarrow b : A \to B}$$

$\Delta_{\simeq <:}$

(Eq Subsumption)

$$\frac{E \vdash a \leftrightarrow a' : A \quad E \vdash A <: B}{E \vdash a \leftrightarrow a' : B}$$

(Eq Top)

$$\frac{E \vdash a:A \quad E \vdash b:B}{E \vdash a \leftrightarrow b : Top}$$

$\Delta_{=\mu<:}$

(Eq Fold)
$$\frac{E \vdash a \leftrightarrow a' : A\{X \leftarrow \mu(X)A\}}{E \vdash \text{fold}(\mu(X)A, a) \leftrightarrow \text{fold}(\mu(X)A, a') : \mu(X)A}$$

(Eq Unfold)
$$\frac{E \vdash a \leftrightarrow a' : \mu(X)A}{E \vdash \text{unfold}(a) \leftrightarrow \text{unfold}(a') : A\{X \leftarrow \mu(X)A\}}$$

(Eq Fold<:)
$$\frac{E \vdash \mu(X)A \quad E \vdash \mu(Y)B \quad E, Y<:\text{Top}, X<:Y \vdash A<:B \quad E \vdash a \leftrightarrow a' : A\{X \leftarrow \mu(X)A\}}{E \vdash \text{fold}(\mu(X)A, a) \leftrightarrow \text{fold}(\mu(Y)B, a') : \mu(Y)B}$$

(Eval Fold)
$$\frac{E \vdash a : \mu(X)A}{E \vdash \text{fold}(\mu(X)A, \text{unfold}(a)) \leftrightarrow a : \mu(X)A}$$

(Eval Unfold)
$$\frac{E \vdash a : A\{X \leftarrow \mu(X)A\}}{E \vdash \text{unfold}(\text{fold}(\mu(X)A, a)) \leftrightarrow a : A\{X \leftarrow \mu(X)A\}}$$

(Eq Rec)
$$\frac{E, x:A \vdash a \leftrightarrow a' : A}{E \vdash \mu(x:A)a \leftrightarrow \mu(x:A)a' : A}$$

(Eval Rec)
$$\frac{E, x:A \vdash a : A}{E \vdash \mu(x:A)a \leftrightarrow a\{x \leftarrow \mu(x:A)a\} : A}$$

$\Delta_{=<:\forall}$

(Eq Fun2<:)
$$\frac{E, X<:A \vdash b \leftrightarrow b' : B}{E \vdash \lambda(X<:A)b \leftrightarrow \lambda(X<:A)b' : \forall(X<:A)B}$$

(Eq Appl2<:)
$$\frac{E \vdash b \leftrightarrow b' : \forall(X<:A)B\{X\} \quad E \vdash A'<:A}{E \vdash b(A') \leftrightarrow b'(A') : B\{A'\}}$$

(Eval Beta2<:)
$$\frac{E \vdash \lambda(X<:A)b : \forall(X<:A)B \quad E \vdash C <: A}{E \vdash (\lambda(X<:A)b)(C) \leftrightarrow b\{X \leftarrow C\} : B\{X \leftarrow C\}}$$

(Eval Eta2<:)
$$\frac{E \vdash b : \forall(X<:A)B \quad X \notin \text{dom}(E)}{E \vdash \lambda(X<:A)b(X) \leftrightarrow b : \forall(X<:A)B}$$

$\Delta_{=<:\exists}$

(Eq Pack<:)
$$\frac{E \vdash C <: A' \quad E \vdash A'<:A \quad E, X<:A' \vdash B'\{X\}<:B\{X\} \quad E \vdash b\{C\} \leftrightarrow b'\{C\} : B'\{C\}}{E \vdash (\text{pack } X<:A=C, b\{X\}:B\{X\}) \leftrightarrow (\text{pack } X<:A'=C, b'\{X\}:B'\{X\}) : \exists(X<:A)B\{X\}}$$

(Eq Open<:)
$$\frac{E \vdash c \leftrightarrow c' : \exists(X<:A)B \quad E \vdash D \quad E, X<:A, x:B \vdash d \leftrightarrow d' : D}{E \vdash (\text{open } c \text{ as } X<:A, x:B \text{ in } d:D) \leftrightarrow (\text{open } c' \text{ as } X<:A, x:B \text{ in } d':D) : D}$$

(Eval Unpack<:) (where $c \equiv \text{pack } X<:A=C, b\{X\}:B\{X\}$)
$$\frac{E \vdash c : \exists(X<:A)B\{X\} \quad E \vdash D \quad E, X<:A, x:B\{X\} \vdash d\{X,x\} : D}{E \vdash (\text{open } c \text{ as } X<:A, x:B\{X\} \text{ in } d\{X,x\}:D) \leftrightarrow d\{C, b\{C\}\} : D}$$

(Eval Repack<:)
$$\frac{E \vdash b : \exists(X<:A)B\{X\} \quad E, y:\exists(X<:A)B\{X\} \vdash d\{y\} : D}{E \vdash (\text{open } b \text{ as } X<:A, x:B\{X\} \text{ in } d\{\text{pack } X'<:A=X, x:B\{X'\}\}:D) \leftrightarrow d\{b\} : D}$$

Appendix E: The ςOb Calculus

ςOb is our minimal second-order object calculus. It is obtained by combining the rules for object types (appendix A) with the Self quantifier (section 3.4) taken as a primitive, plus some general rules (appendix C and D). The rules for ς-objects (appendix B) are derivable from the ones shown here. The relation A>X is defined as in appendix C, with in addition ς(X)B ≻ Y if B>Y.

$$A,B \;::=\; X \mid \mathrm{Top} \mid [l_i{:}B_i\ ^{i\in 1..n}] \mid \varsigma(X)B$$
$$a,b \;::=\; x \mid [l_i{=}\varsigma(x_i{:}A)b_i\ ^{i\in 1..n}] \mid a.l \mid a.l \Leftarrow \varsigma(x{:}A)b \mid \varsigma(X{<:}A{=}B)b \mid \text{use a as } X{<:}A,\ y{:}B \text{ in } b{:}D$$

(Env ∅)
$$\frac{}{\emptyset \vdash \diamond}$$

(Env x)
$$\frac{E \vdash A \qquad x \notin \mathrm{dom}(E)}{E,x{:}A \vdash \diamond}$$

(Env X<:)
$$\frac{E \vdash A \qquad X \notin \mathrm{dom}(E)}{E,X{<:}A \vdash \diamond}$$

(Type X<:)
$$\frac{E',X{<:}A,E'' \vdash \diamond}{E',X{<:}A,E'' \vdash X}$$

(Type Top)
$$\frac{E \vdash \diamond}{E \vdash \mathrm{Top}}$$

(Type Object) (l_i distinct)
$$\frac{E \vdash B_i \qquad \forall i \in 1..n}{E \vdash [l_i{:}B_i\ ^{i\in 1..n}]}$$

(Type Self)
$$\frac{E,X{<:}\mathrm{Top} \vdash B \qquad B{>}X}{E \vdash \varsigma(X)B}$$

(Sub Refl)
$$\frac{E \vdash A}{E \vdash A <: A}$$

(Sub Trans)
$$\frac{E \vdash A <: B \qquad E \vdash B <: C}{E \vdash A <: C}$$

(Sub X)
$$\frac{E',X{<:}A,E'' \vdash \diamond}{E',X{<:}A,E'' \vdash X{<:}A}$$

(Sub Top)
$$\frac{E \vdash A}{E \vdash A <: \mathrm{Top}}$$

(Sub Object) (l_i distinct)
$$\frac{E \vdash B_i \qquad \forall i \in 1..n{+}m}{E \vdash [l_i{:}B_i\ ^{i\in 1..n+m}] <: [l_i{:}B_i\ ^{i\in 1..n}]}$$

(Sub Self)
$$\frac{E,X{<:}\mathrm{Top} \vdash B <: B' \qquad B,B'{>}X}{E \vdash \varsigma(X)B <: \varsigma(X)B'}$$

(Val Subsumption)
$$\frac{E \vdash a : A \qquad E \vdash A <: B}{E \vdash a : B}$$

(Val x)
$$\frac{E',x{:}A,E'' \vdash \diamond}{E',x{:}A,E'' \vdash x{:}A}$$

(Val Object) (where $A \equiv [l_i{:}B_i\ ^{i\in 1..n}]$)
$$\frac{E, x_i{:}A \vdash b_i : B_i \qquad \forall i \in 1..n}{E \vdash [l_i{=}\varsigma(x_i{:}A)b_i\ ^{i\in 1..n}] : A}$$

(Val Select)
$$\frac{E \vdash a : [l_i{:}B_i\ ^{i\in 1..n}] \qquad j \in 1..n}{E \vdash a.l_j : B_j}$$

(Val Override) (where $A \equiv [l_i{:}B_i\ ^{i\in 1..n}]$)
$$\frac{E \vdash a : A \qquad E, x{:}A \vdash b : B_j \qquad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(x{:}A)b : A}$$

(Val Self) (where $A \equiv \varsigma(X)B\{X\}$)
$$\frac{E \vdash C <: A \qquad E \vdash b\{C\} : B\{C\}}{E \vdash \varsigma(Y{<:}A{=}C)\, b\{Y\} : A}$$

(Val Use) (where $A \equiv \varsigma(X)B\{X\}$)
$$\frac{E \vdash c : A \qquad E \vdash D \qquad E,\ Y{<:}A,\ y{:}B\{Y\} \vdash d : D}{E \vdash (\text{use c as } Y{<:}A,\ y{:}B\{Y\} \text{ in d:D}) : D}$$

(Eq Symm)
$$\frac{E \vdash a \leftrightarrow b : A}{E \vdash b \leftrightarrow a : A}$$

(Eq Trans)
$$\frac{E \vdash a \leftrightarrow b : A \qquad E \vdash b \leftrightarrow c : A}{E \vdash a \leftrightarrow c : A}$$

(Eq Subsumption)

$$\frac{E \vdash a \leftrightarrow a' : A \quad E \vdash A <: B}{E \vdash a \leftrightarrow a' : B}$$

(Eq x)

$$\frac{E', x{:}A, E'' \vdash \diamond}{E', x{:}A, E'' \vdash x \leftrightarrow x : A}$$

(Eq Top)

$$\frac{E \vdash a{:}A \quad E \vdash b{:}B}{E \vdash a \leftrightarrow b : \mathrm{Top}}$$

(Eq Object) (where $A \equiv [l_i{:}B_i\ ^{i \in 1..n}]$)

$$\frac{E, x_i{:}A \vdash b_i \leftrightarrow b_i' : B_i \quad \forall i \in 1..n}{E \vdash [l_i = \varsigma(x_i{:}A) b_i\ ^{i \in 1..n}] \leftrightarrow [l_i = \varsigma(x_i{:}A) b_i'\ ^{i \in 1..n}] : A}$$

(Eq Sub Object) (where $A \equiv [l_i{:}B_i\ ^{i \in 1..n}]$, $A' \equiv [l_i{:}B_i\ ^{i \in 1..n}, l_j{:}B_j\ ^{j \in n+1..m}]$)

$$\frac{E, x_i{:}A \vdash b_i : B_i \quad \forall i \in 1..n \qquad E, x_j{:}A' \vdash b_j : B_j \quad \forall j \in n+1..m}{E \vdash [l_i = \varsigma(x_i{:}A) b_i\ ^{i \in 1..n}] \leftrightarrow [l_i = \varsigma(x_i{:}A') b_i\ ^{i \in 1..n+m}] : A}$$

(Eq Select)

$$\frac{E \vdash a \leftrightarrow a' : [l_i{:}B_i\ ^{i \in 1..n}] \quad j \in 1..n}{E \vdash a.l_j \leftrightarrow a'.l_j : B_j}$$

(Eq Override) (where $A \equiv [l_i{:}B_i\ ^{i \in 1..n}]$)

$$\frac{E \vdash a \leftrightarrow a' : A \qquad E, x{:}A \vdash b \leftrightarrow b' : B_j \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(x{:}A) b \leftrightarrow a'.l_j \Leftarrow \varsigma(x{:}A) b' : A}$$

(Eq Self) (where $A \equiv \varsigma(X)B\{X\}$, $A' \equiv \varsigma(X)B'\{X\}$)

$$\frac{E \vdash C <: A' \qquad E, X <: \mathrm{Top} \vdash B'\{X\} <: B\{X\} \qquad E \vdash b\{C\} \leftrightarrow b'\{C\} : B'\{C\}}{E \vdash \varsigma(Y <: A = C) b\{Y\} \leftrightarrow \varsigma(Y <: A' = C) b'\{Y\} : A}$$

(Eq Use) (where $A \equiv \varsigma(X)B\{X\}$)

$$\frac{E \vdash c \leftrightarrow c' : A \qquad E \vdash D \qquad E, Y <: A, y{:}B\{Y\} \vdash d \leftrightarrow d' : D}{E \vdash (\text{use } c \text{ as } Y <: A, y{:}B\{Y\} \text{ in } d{:}D) \leftrightarrow (\text{use } c' \text{ as } Y <: A, y{:}B\{Y\} \text{ in } d'{:}D) : D}$$

(Eval Select) (where $A \equiv [l_i{:}B_i\ ^{i \in 1..n}]$, $a \equiv [l_i = \varsigma(x_i{:}A') b_i\ ^{i \in 1..n+m}]$)

$$\frac{E \vdash a : A \quad j \in 1..n}{E \vdash a.l_j \leftrightarrow b_j\{x_j \leftarrow a\} : B_j}$$

(Eval Override) (where $A \equiv [l_i{:}B_i\ ^{i \in 1..n}]$, $a \equiv [l_i = \varsigma(x_i{:}A') b_i\ ^{i \in 1..n+m}]$)

$$\frac{E \vdash a : A \qquad E, x{:}A \vdash b : B_j \quad j \in 1..n}{E \vdash a.l_j \Leftarrow \varsigma(x{:}A) b \leftrightarrow [l_i = \varsigma(x_i{:}A') b_i\ ^{i \in (1..n+m)-\{j\}}, l_j = \varsigma(x{:}A') b] : A}$$

(Eval Unself) (where $A \equiv \varsigma(X)B\{X\}$, $c \equiv \varsigma(Z <: A = C) b\{Z\}$)

$$\frac{E \vdash c : A \qquad E \vdash D \qquad E, Y <: A, y{:}B\{Y\} \vdash d\{Y,y\} : D}{E \vdash (\text{use } c \text{ as } Y <: A, y{:}B\{Y\} \text{ in } d\{Y,y\}{:}D) \leftrightarrow d\{C, b\{C\}\} : D}$$

(Eval Reself) (where $A \equiv \varsigma(X)B\{X\}$)

$$\frac{E \vdash b : A \qquad E, y{:}A \vdash d\{y\} : D}{E \vdash (\text{use } b \text{ as } Y <: A, y{:}B\{Y\} \text{ in } d\{\varsigma(Y' <: A = Y) y\} : A) \leftrightarrow d\{b\} : D}$$

References

[Abadi, Cardelli 1994a] M. Abadi and L. Cardelli, **A semantics of object types**. *To appear.*

[Abadi, Cardelli 1994b] M. Abadi and L. Cardelli, **A theory of primitive objects**. *To appear.*

[Abadi, Cardelli 1994c] M. Abadi and L. Cardelli. **A theory of primitive objects: untyped and first-order systems**. *Proc. Theoretical Aspects of Computer Software*. Springer-Verlag.

[Böhm, Berarducci 1985] C. Böhm and A. Berarducci, **Automatic synthesis of typed λ-programs on term algebras**. *Theoretical Computer Science* **39**, 135-154.

[Bruce 1993] K. Bruce. **A paradigmatic object-oriented programming language: design, static typing, and semantics**. Technical Report No. CS-92-01, revised (to appear in the Journal of Functional Programming). Williams College.

[Cardelli 1991] L. Cardelli. **Extensible records in a pure calculus of subtyping**. Technical Report n.81. DEC Systems Research Center.

[Cardelli, *et al.* 1991] L. Cardelli, J.C. Mitchell, S. Martini, and A. Scedrov. **An extension of system F with subtyping**. *Proc. Theoretical Aspects of Computer Software*. Lecture Notes in Computer Science 526. Springer-Verlag.

[Cardelli, Wegner 1985] L. Cardelli and P. Wegner, **On understanding types, data abstraction and polymorphism**. *Computing Surveys* **17**(4), 471-522.

[Curien, Ghelli 1992] P.-L. Curien and G. Ghelli, **Coherence of subsumption, minimum typing and type-checking in $F_{\leq}$**. *Mathematical Structures in Computer Science* **2**(1), 55-91.

[Girard, Lafont, Taylor 1989] J.-Y. Girard, Y. Lafont, and P. Taylor, **Proofs and types**. Cambridge University Press.

[MacQueen, Plotkin, Sethi 1986] D.B. MacQueen, G.D. Plotkin, and R. Sethi, **An ideal model for recursive polymorphic types**. *Information and Control* **71**, 95-130.

[Meyer 1988] B. Meyer, **Object-oriented software construction**. Prentice Hall.

[Mitchell, Honsell, Fisher 1993] J.C. Mitchell, F. Honsell, and K. Fisher. **A lambda calculus of objects and method specialization**. *Proc. 8th Annual IEEE Symposium on Logic in Computer Science*.

[Wadsworth 1980] C. Wadsworth, **Some unusual λ-calculus numeral systems**. In *To H.B. Curry: Essays on combinatory logic, lambda calculus and formalism,* J.P. Seldin and J.R. Hindley, ed. Academic Press.