Citation for published version


DOI

Link to record in KAR

https://kar.kent.ac.uk/21687/

Document Version

UNSPECIFIED

Copyright & reuse
Content in the Kent Academic Repository is made available for research purposes. Unless otherwise stated all content is protected by copyright and in the absence of an open licence (eg Creative Commons), permissions for further reuse of content should be sought from the publisher, author or other copyright holder.

Versions of research
The version in the Kent Academic Repository may differ from the final published version. Users are advised to check http://kar.kent.ac.uk for the status of the paper. Users should always cite the published version of record.

Enquiries
For any further enquiries regarding the licence status of this document, please contact: researchsupport@kent.ac.uk

If you believe this document infringes copyright then please contact the KAR admin team with the take-down information provided at http://kar.kent.ac.uk/contact.html
Abstract

We present a refinement of the existential object model of Pierce and Turner [PT94]. In addition to signatures (or interfaces) as the types of objects, we also provide classes as the types of objects. These class types not only specify an interface, but also a particular implementation.

We show that class types can be interpreted in the standard PER model. Our main result is that the standard interpretation of subtyping in PER models – i.e. subtypes are subterms – is then behavioural subtyping in the sense of Leavens [Les90].

1 Introduction

Like most descriptions of objects in typed lambda calculus or typed object calculus, the existential object model of Pierce and Turner [PT94] provides signatures or interfaces as the types of objects, and provides the usual syntactic notion of subtyping on these types. We consider a more refined notion of class type as the type of an object. A class type is a subtype of an interface type, specified by a particular implementation and initial state.

The existential object encoding can be carried out in $F_k^<$, but the class types we want to consider are not encodable in $F_k^<$. Therefore we will define a simple object-oriented functional language $\Lambda^{OO}$, that is essentially just some syntactic sugar for the existential object encoding, but extended with a notion of class type.

The standard model of $F_k^<$ is a PER model, which interprets types as partial equivalence relations (pers), and interprets subtyping as subset inclusion between pers [BL90]. We show that class types can be interpreted in the PER model. For these interpretations of class types the subset relation turns out to be equivalent to the notion of behavioural subtyping as defined by Leavens [Les90].

It is important to note that class types can be behavioural subtypes even though they give completely unrelated implementations. Although class types correspond to particular implementations, behavioural subtyping between class types only concerns the observable behaviour of these implementations.

The interpretation of class types can also be viewed from the categorical perspective used in [Rei95] and [HP95]: class types are interpreted as sub-coalgebras of final coalgebras in the PER model.

We briefly review the different notions of (sub)typing for objects, and fix the terminology used for them in this paper.

Interface Types vs Class Types

There are at least two kinds of types that can be used for objects, which we will call interface types and class types. An interface type just specifies an interface (or signature), i.e. it lists the methods with their input and output types. A class type not only specifies the signatures of the methods, but also an implementation of the methods and an initial state. An important consequence of this is that the objects of a class type can be guaranteed to have some behaviour in common. The objects of an interface type on the other hand cannot be guaranteed to have any behaviour in common.

Most object-oriented languages provide classes as types. Most type-theoretical work on OO on the other hand concerns interface types (e.g. [Car88], many of the papers in [GM94], [Bru94], [FM94], [AC96]). A notable exception is [FM97], which gives an extensive comparison of interface types and class types.

Signature Subtyping vs Behavioural Subtyping

There are at least two notions of subtyping for object types, which we will call signature subtyping and behavioural subtyping.

Signature subtyping is a purely syntactic notion, defined by the usual contra/covariant rules (e.g. [Car88]). It concerns just the interfaces of objects: a signature subtype provides (at least) all the methods of the supertype with compatible signatures. Signature subtyping prevents type errors ("message not understood") from occurring at run-time: if $A$ is a signature subtype of $B$ then substituting $A$'s for $B$'s will not cause any type errors.

Behavioural subtyping is a more semantic notion, and concerns more than just signatures. It also tries to capture the intuition that objects in the subtype "behave like" objects in the supertype. It can informally be defined as follows: $A$ is a behavioural subtype of $B$ if using objects of...
type \( A \) in place of objects of type \( B \) does not cause any unexpected behaviour. Or, \( A \) is a behavioural subtype of \( B \) iff any property that holds for all objects of type \( B \) also holds for all objects of type \( A \). Another formulation is known as Liskov's substitution principle [Lis88]: "\( A \) is a behavioural subtype of \( B \) iff for every object \( a \) of type \( A \) there is an object \( b \) of type \( B \) such that for all programs \( p \) that use \( b \), the behaviour of \( p \) is unchanged when \( b \) is replaced with \( a \).

Behavioural subtyping is clearly a useful property for reasoning about programs. Behavioural subtyping is in general not decidable, unlike signature behavioural subtyping, which can be statically enforced by a typechecker.

There are different ways to give formal definitions of behavioural subtyping.

One way to define behavioural subtyping is to require that there exists a simulation relation between states of objects in the subtype and states of objects in the supertype such that for every object in the behavioural subtype there is an object in the supertype with a related state. This characterisation is the one we will use. It was introduce by Leavens in [Lea90], and is also used in [LW95] [Man95].

Another – more common – way to define behavioural subtyping is in terms of pre- and post-conditions of methods, and require that methods in a behavioural subtype have weaker pre-conditions and stronger post-conditions than the corresponding methods in the supertypes, so that behavioural subtypes correspond to stronger specifications. This is supported to a certain extent in the programming language Eiffel [Mey88], and is widely used in the literature, e.g. [Ame89] [Lea90] [LW95] [LW94] [Pre97] [Llo97]. This second approach can combine with the first in order to cope with pre- and post-conditions that refer to the abstract values of objects. For example, suppose objects of type \( \text{List}_A \) are specified in terms of the sequences in \( A \) they represent, and objects of type \( \text{Set}_A \) in terms of the sets in \( P(A) \) they represent. Then a (simulation) relation \( R \subseteq \text{Set}_A \times P(A) \) could be used to relate these specifications. This approach is used in [Lea90]. It is also used in [Amo89] [LW94], where simulation relations are restricted to functions.

The rest of this paper is organised as follows. Section 2 gives some examples to illustrate the notions mentioned above. Section 3 then gives a formal definition of \( \lambda^{OO} \). Section 4 discusses the PER model for \( \lambda^{OO} \), which provides a PER model for \( \lambda^{OO} \) without class types. This PER model is then used in Section 5 as the basis of a PER model for \( \lambda^{OO} \) including the class types, and we show that subtyping between class types in this model is behavioural subtyping. We conclude in Section 6.

2 Informal Introduction to \( \lambda^{OO} \)

We give some simple examples to introduce \( \lambda^{OO} \) and the existential object model, and to explain the notions of interface types, class types, signature subtyping, and behavioural subtyping in more detail.

2.1 Objects and Interface Types

The interface type

\[
\text{Counter} = \text{Sig}(X)[\text{getcount} : \text{Nat}, \text{count} : X]
\]

is the type of objects with methods \text{getcount} and \text{count}, where \text{getcount} returns a natural number and \text{count} a new object of the same type. We write \( o=1 \) for the invocation of method \( I \) of object \( o \). So, if \( o : \text{Counter} \) then \( o\cdot\text{getcount} : \text{Nat} \) and \( o\cdot\text{count} : \text{Counter} \).

An object of type \( \text{Counter} \) – a counter – can be constructed from a state \( s \) of some type \( \text{Rep} \) and a method table \( m : \text{Rep}\rightarrow\text{CounterI}(\text{Rep}) \) that gives the implementation of the methods, where

\[
\text{CounterI}(X) = \{\text{getcount} : \text{Nat}, \text{count} : X\}.
\]

This object is written as \text{object} \( (s,m) \) for

\[
\text{object} \ (s,m)\ |
\text{getcount} = (m,s)\cdot\text{getcount}
\]

\[
\text{object} \ (s,m)\ |
\text{count} = \text{object} \ ((m,s)\cdot\text{count},m)
\]

For example, if \( o \equiv \text{object} \ ((x = 5),m) \), then \( o\cdot\text{getcount} = 5 \) and \( o\cdot\text{count} = \text{object} \ ((x = 6),m) \). Note that the methods \text{count} and \text{getcount} are treated differently, because \text{count} returns an object of the same class and \text{getcount} just returns a natural number. We will call a method such as \text{count} a mutator and a method such as \text{getcount} an observer.

In general, to invoke a method \( l \) we apply the method table to the state and select \( l \) component, and, if the method is mutator, we wrap up the new state with the old method table to produce an object.

Everything described so far is just syntactic sugar for the existential object encoding of [PT94]. We have written \text{Sig} \text{CounterI} for

\[
\exists \text{Rep} : \text{Rep} \times (\text{Rep}\rightarrow\text{CounterI}(\text{Rep}))
\]

and \text{object} \( (s,m) \) for

\[
\text{pack} \ ((\text{Rep},(s,m))) \rightarrow \exists \text{Rep} : \text{Rep} \times (\text{Rep}\rightarrow\text{CounterI}(\text{Rep}))
\]

where \( \text{Rep} \) is the type of \( s \).

Existential types model abstract types [MP88]. The existential type above hides the type \( \text{Rep} \) that used to represent the state of an object, so that the state \( s \) of an object \text{object} \( (s,m) \) can only be observed indirectly by invoking the methods \text{getcount} and \text{count}.

In certain models – including the PER model we will use – the existential type above is interpreted as a final coalgebra [PA93][Has94]. Then equality of objects is \text{bisimulation}:

\text{object} \( (s_1,m_1) \) and \text{object} \( (s_2,m_2) \) of type \text{Counter} are equal if their states are related by some simulation relation \( \sim \), i.e. if \( s_1 \sim s_2 \) for some relation \( \sim \) such that

\[
x_1 \sim x_2 \Rightarrow \ (m_1,x_1)\cdot\text{getcount} \equiv_{\text{Nat}} (m_2,x_2)\cdot\text{getcount} \quad (m_1,x_1)\cdot\text{count} \sim (m_2,x_2)\cdot\text{count}
\]
2.2 Subtyping on Interface Types

An example of a signature subtype of Counter is

\[ \text{RCounter} = \text{Sig RCounterI}, \]

where

\[ \text{RCounterI}(X) = \{ \text{getcount} : \text{Nat}, \text{count} : X, \text{reset} : X \}. \]

RCounter is type of counters that in addition to methods count and getcount also have a method count.

The PER model does indeed interpret RCounter and Counter as subsets: \([\text{RCounter}] \subseteq [\text{Counter}]\). We can think of the partial equivalence relations \([\text{RCounter}]\) and \([\text{Counter}]\) as the notion of equality for counters and resetable counters, respectively. Then \([\text{RCounter}] \subseteq [\text{Counter}]\) means that \([\text{Counter}]\) is a coarser notion of equality than \([\text{RCounter}]\). This can be understood as follows. Suppose we have two objects that can not be distinguished by invoking just the methods count and getcount, but that can be distinguished by invoking the methods count, getcount and reset. These objects would then be identified by \([\text{Counter}]\), but would not be identified by \([\text{RCounter}]\).

The subtyping between \(\text{RCounter}\) and \(\text{Counter}\) is a degenerated instance of behavioural subtyping. For interface types such as \(\text{RCounter}\) and \(\text{Counter}\) the notions of signature subtyping and behavioural subtyping are identical, because these types do not make any behavioural guarantees.

2.3 Class Types

The class types we consider not only specify an interface, but also fix the type used for the representation, the implementation of the methods, and an initial state. An example of a class type is

\[ \text{CounterClass} = (\text{Class CounterI with init, m}) \]

where

\[ \text{init} = \{ x = 1 \} \]
\[ \text{m} = \lambda x : \text{Nat}. \{ \text{get} = \text{sx}, \text{count} = \{ x = \text{sx} + 1 \} \} \]

Intuitively, \(\text{CounterClass}\) is the following inductively defined set:

- \(\text{object } (\text{init}, m) : \text{CounterClass}\).
- if \(c : \text{CounterClass}\) then \(c.e = \text{count} : \text{CounterClass}\).

\(\text{CounterClass}\) can be understood as the smallest subset of \(\text{Counter}\) that contains \(\text{object } (\text{init}, m)\) and is closed under method invocation.

\(\text{CounterClass}\) is like a class definition in a standard OO language, in that it introduces a type together with an implementation and initialisation for the objects of that type. In a programming language we might write something like "\(\text{new CounterClass}\)" for \(\text{object } (\text{init}, m)\).

Because the objects in \(\text{CounterClass}\) all have \(m\) as their method table and all have a hidden state of type \(\{ x : \text{Nat} \}\) that is "reachable" from the initial state \(s\) by method invocations, they have some behaviour in common. For example,

\[ o \gets \text{getcount} \geq 1 \]

and

\[ (o \gets \text{count}) \gets \text{getcount} = o \times \text{getcount} + 1 \]

for all \(o : \text{CounterClass}\).

Interpreting class types in the PER model is not a problem, and we get the expected relation between the pers interpreting \(\text{CounterClass}\) and \(\text{CounterClass} : [\text{CounterClass}] \subseteq [\text{Counter}]\). The pers \([\text{CounterClass}]\) and \([\text{Counter}]\) provide the same notion of equality, i.e. all \([\text{CounterClass}]\) equivalence classes are also \([\text{Counter}]\) equivalence classes, but there are fewer \([\text{CounterClass}]\) equivalence classes than there are \([\text{Counter}]\) equivalence classes.

2.4 Subtyping on Class Types

Assume there is a type \(\text{natlist}\) of lists of natural numbers, with the usual constructors \(\text{nil}\) and \(\text{cons}\). The class type below uses a state of type \(\{y : \text{natlist}\}\) to represent the state of a resetable counter:

\[ \text{RCounterClass} = (\text{Class RCounterI with init, m}) \]

where

\[ \text{init} = \{ y = \text{cons} 0 \{ \text{cons} 0 \text{nil} \} \} \]
\[ \text{m} = \lambda x : \text{natlist}. \{ \text{getcount} = \text{length}(s, y) \}
\]
\[ \text{count} = \{ y = \text{cons} 0 s, y \} \]
\[ \text{reset} = \{ y = \text{cons} 2 (\text{cons} 2 \text{nil}) \} \]

\(\text{RCounterClass}\) can be understood as the smallest subset of \(\text{RCounter}\) that contains \(\text{object } (\text{init}, m)\) and is closed under method invocation.

\(\text{RCounterClass}\) can be viewed as a behavioural subtype of \(\text{CounterClass}\), because, despite their different implementations, the objects in \(\text{RCounterClass}\) behave just like objects in \(\text{CounterClass}\). By invoking only the methods count and getcount, it is not possible to distinguish the objects in \(\text{RCounterClass}\) from those in \(\text{CounterClass}\), since for every object \(o' : \text{RCounterClass}\) there is a \(o : \text{CounterClass}\) that is indistinguishable from \(o'\). More formally, we can say that \(\text{RCounterClass}\) is a behavioural subtype of \(\text{CounterClass}\) because there exists a relation \(\sim \subseteq \{ x : \text{Nat} \} \times \{ y : \text{natlist} \}\) such that

\[ s \sim s' \implies \left\{ \begin{array}{l}
(m s).\text{getcount} = \text{Nat} (m R s').\text{getcount} \\
(m s).\text{count} \sim (m R s').\text{count}
\end{array} \right\} \]

(i)

and

\[ \forall o' : \text{RCounterClass}. \]
\[ \exists o : \text{CounterClass}. \]
\[ o.e = \text{count} \]
\[ \text{the states of } o \text{ and } o' \text{ are related by } \sim. \]

(ii)

This relation \(\sim\) is of course

\[ s \sim s' \iff s.x = \text{length}(s'.y). \]

Together conditions (i) and (ii) guarantee that for every \(o' : \text{RCounterClass}\) there is a \(o : \text{CounterClass}\) such that \(o\) is indistinguishable from \(o'\) if we are only allowed to invoke their getcount and count methods.

Intuitively, the conditions above guarantee that objects in \(\text{RCounterClass}\) have the properties that all objects in \(\text{CounterClass}\) have, and maybe more. For instance, note that \(o \gets \text{getcount} \geq 2\) for all \(o : \text{RCounterClass}\).

Examples of classes that are not behavioural subtypes of \(\text{CounterClass}\) are

\[ \text{CounterClass1} = (\text{Class CounterI with init, m}) \]
\[ \text{RCounterClass1} = (\text{Class CounterI with init, m}) \]
with
\[ m' = \lambda x : \text{Nat}. \, \{ \text{get} = s.x, \text{count} = \{ x = s.x + 2 \} \} \]
\[ m_R = \lambda y : \text{natList}. \{ \text{getCount} = \text{length}(s.y), \, \text{count} = \{ y = \text{cons} \, 0 \, y \} \}
\]
\[ \text{reset} = \{ y = \text{nil} \} \]

These classes are not behavioural subtypes of \textit{CounterClass}, for slightly different reasons. For \textit{CounterClass} we cannot find a suitable simulation relation. For \textit{RCounterClass} there is an obvious simulation relation, namely the same one we used for \textit{RCounterClass}. However, there is a object in \textit{RCounterClass} for which there is no related object in \textit{CounterClass}: resetting a counter in \textit{RCounterClass} produces an object \( o \equiv \text{object} \{ \{ y = \text{nil} \}, m \} \) for which \( o \mapsto \text{count} = 0 \), and this object cannot be related to any object in \textit{CounterClass}, since all counters in \textit{CounterClass} have a \texttt{getCount} greater than 0.

For class types, the interpretation of subtyping in the PER model – subtypes are subtypes – turns out to be equivalent to the informal notion of behavioural subtyping introduced here, i.e. given by properties such as (i) and (ii). So in the PER model
\[
\begin{align*}
\llbracket \text{RCounterClass} \rrbracket & \subseteq \llbracket \text{CounterClass} \rrbracket \\
\llbracket \text{CounterClass} \rrbracket & \subseteq \llbracket \text{CounterClass} \rrbracket \\
\llbracket \text{RCounterClass} \rrbracket & \subseteq \llbracket \text{CounterClass} \rrbracket
\end{align*}
\]
The fact that the PER model already provides bisimulation as the notion of equality plays a vital role here.

3 Definition of $\lambda^{oo}$

The raw syntax of the terms \( a \), \textit{types} \( A \) and \textit{signatures} \( I \) of \( \lambda^{oo} \) is given by the following grammar
\[
\begin{align*}
a & ::= x \mid \lambda x : A \, a \mid a \, a \mid \{ l_1 = a, \ldots, l_n = a \} \mid a \, l \\
A & ::= X \mid \{ A \rightarrow A' \} \mid \{ l_1 : A_1, \ldots, l_n : A_n \} \mid \text{Sig} \mid \text{Class} \mid \text{with} \, A, a, a \\
I & ::= \{ X \mid l_1 : A_1 \rightarrow A, \ldots, l_n : A_n \rightarrow A \}
\end{align*}
\]

Here \( x \) ranges over \textit{term variables}, \( X \) ranges over \textit{type variables}, and \( I \) over a countable set \( \mathcal{L} \) of labels. The type variable \( X \) is bound in \( \{ X \} \), and if \( I \equiv \{ X \}A \) we write \( I(B) \) for \( \{ B/X \}A \), where \( \{ B/X \}A \) denotes the capture-free substitution of \( B \) for \( X \) in \( A \). Expressions equal up to the names of bound variables and permutation of fields are identified as usual, and we assume that the same label never occurs twice in a record (\textit{type}) or interface.

For simplicity, we divide \( \mathcal{L} \) into a set \( \mathcal{L}_{\text{obs}} \) of labels that can be used as names for \textit{observer methods} and a set \( \mathcal{L}_{\text{mut}} \) of labels that can be used as names for \textit{mutator methods}, and we insist that
\[
\begin{align*}
l_i & \in \mathcal{L}_{\text{obs}} \Rightarrow X \not\in \text{FV}(A_i \rightarrow B_i) \\
l_i & \in \mathcal{L}_{\text{mut}} \Rightarrow X \not\in \text{FV}(A_i) \land X \equiv B_i
\end{align*}
\]
for any signature \( \{ X \mid l_1 : A_1 \rightarrow B_1, \ldots, l_n : A_n \rightarrow B_n \} \).

The \textit{contexts} of \( \lambda^{oo} \) are given by
\[
\Gamma ::= \epsilon \mid \Gamma, x : A
\]
with no variable occurring twice.

The subtyping and typing rules of \( \lambda^{oo} \) are given in tables 1 and 3. The rules for well-formedness of contexts and types are given in Table 2. These are needed because there are types with terms as subexpressions, namely the class types. Only the well-formedness rule for class types is given, for the other are trivial. (E.g., \( A \rightarrow B \) is well-formed in \( \Gamma \) if \( A \) and \( B \) are well-formed in \( \Gamma \), etc.)

The \textit{reduction relation} \( \triangleright \) on terms is given by the rules
\[
(x:A)\,b \triangleright [a/x]b
\]
\[
\begin{align*}
l_i = a_1, \ldots, l_n = a_n & \triangleright a_i \\
(\text{object}, (s,m)) \leftrightarrow l(a) & \triangleright (m \, s) \, l \, a
\end{align*}
\]
where \([a/x]b\) denotes the capture-free substitution of \( a \) for \( x \) in \( b \).

We write \( \equiv \) for the reflexive, transitive, and symmetric closure of \( \triangleright \), and \( \Gamma \triangleright a \equiv a' : A \) for \( \Gamma \triangleright a : A \land \Gamma \triangleright a' : A \land a \equiv a' \).

4 PER Model for $\lambda^{oo}$ without Class Types

As we mentioned earlier, with the exception of the class types, \( \lambda^{oo} \) just introduces some syntactical sugar for the existential object encoding of objects in \( F^{oo} \) given in [PT94]. In fact, we only need the subsystem \( F^{oo}_{\text{S}} \) as target system.\footnote{In [PT94] \( F^{oo}_{\text{S}} \) rather than \( F^{oo} \) is needed to type generic method invocations, i.e. method invocations not yet applied to a particular object, which in our syntax would be written as \( \langle \_\_ \_ \_ \_ \_ \rangle \). We don’t have these in \( \lambda^{oo} \).} So any model of \( F^{oo}_{\text{S}} \) can be used as model for \( \lambda^{oo} \) without classes.

The model we use is the PER model of [PAC94]. This model combines the PER models of [BL90] and [BFAS90]: it is essentially just the model of [BL90] – and interprets subtypes as subterms –, but it uses the interpretation of polymorphic types given in [BFAS90] – rather than the more standard one used in [BL90] – to ensure parametricity. The vital property of this model that we are interested in is that the existential types \( \exists X. X \times \{ X \rightarrow I(X) \} \) are interpreted as \textit{final coalgbeoms}, as is proved in [Has94] and [PA93].

First we make precise how \( \lambda^{oo} \) without class types can be regarded as syntactic sugar for \( F^{oo}_{\text{S}} \).

As far as types are concerned the types, interface types abbreviate existential types:
\[
\text{Sig} \, I = \exists X. X \times \{ X \rightarrow I(X) \}
\]

Remark 4.1 Here \( x \) and \( \exists \) stand for the usual \( F^{oo}_{\text{S}} \) encodings. The record types we have in \( \lambda^{oo} \) are not part of \( F^{oo}_{\text{S}} \), but these can be encoded in \( F^{oo}_{\text{S}} \) using the trick of [Car92].

We assume there is some enumeration of the labels and we represent the record type \( \{ l_1 : A_1, \ldots, l_n : A_n \} \) by the product \( B_1 \times \ldots \times B_m \) where \( m \) is the greatest index of the \( l_i \) and \( B_j = A_l \) if \( j \) is the index of \( l_i \) and \( B = \text{Top} \) if \( j \) is not the index of any of the \( l_i \). Product types can of course be encoded in \( F^{oo}_{\text{S}} \) in the usual way.

The encodings of existential types, product types and record types will be left implicit, so we use the normal notation for existentials, products, and records as abbreviation for their \( F^{oo}_{\text{S}} \)-encodings.
\[
\begin{align*}
A \leq A' & \quad \leq \text{refl} \\
A \leq B' & \quad \leq \text{trans} \\
A' \leq A & \quad B \leq B' & \quad \leq \rightarrow \\
A \rightarrow B \leq A' \rightarrow B' & \quad \leq \rightarrow \\
\text{Sig}(X)A \leq \text{Sig}(X)B & \quad \leq \text{sig} \\
A_1 \leq B_1, \ldots, A_n \leq B_n & \quad m \geq n \\
\{l_1; A_1, \ldots, l_n; A_n\} \leq \{l_1; B_1, \ldots, l_n; B_n\} & \quad \leq \text{record} \\
\text{Class I with meth, init} & \leq \text{Sig I} & \quad \leq \text{class}
\end{align*}
\]

Table 1. Subtyping

\[
\begin{align*}
\varepsilon \vdash \text{ok} \\
\varnothing \vdash \text{empty-ok} \\
\Gamma \vdash \text{ok} & \quad \Gamma \vdash \text{A ok} & \quad \text{weaken-ok}
\end{align*}
\]

Table 2. Well-formedness

\[
\begin{align*}
\Gamma, x : A, \Gamma' \vdash \text{ok} & \quad \text{var} \\
\Gamma, x : A, \Gamma' \vdash x : A & \quad \text{sub} \\
\Gamma \vdash a_1 : A_1 & \quad \ldots & \quad \Gamma \vdash a_n : A_n \\
\Gamma \vdash \{l_1 = a_1, \ldots, l_n = a_n\} : \{l_1; A_1, \ldots, l_n; A_n\} & \quad \text{record-I} \\
\Gamma \vdash s : \text{Rep} & \quad \Gamma \vdash m : \text{Rep} \rightarrow \text{I}(\text{Rep}) \\
\Gamma \vdash \text{object-I} (s, m) : \text{Sig I} & \quad \text{object-I1} \\
\Gamma \vdash o : \text{SC} & \quad \Gamma \vdash a : A & \quad \Gamma \in \mathcal{L}_{\text{obs}} \\
\Gamma \vdash o \leftarrow I(a) : B & \quad \text{object-E-obs} \\
\Gamma \vdash o \leftarrow I(a) : B & \quad \text{E}
\end{align*}
\]

Table 3. Typing

The \(\lambda^{\text{IO}}\) syntax for object formation and method invocation can be interpreted by the following \(F_{\leq}\)-terms:

- \(\text{object}\_I (s, m) = \text{pack} (\text{Rep}_i (s, m)) \rightarrow \text{Sig I}\)
- \(o \leftarrow I(a) = \text{open} \text{o as} (X_i, (s, m)) \in (m \ s) I a\)
  if \(i \in \mathcal{L}_{\text{obs}}\)
- \(o \leftarrow I(a) = \text{open} \text{o as} (X_i, (s, m)) \in (\text{pack (X_i, (m \ s) I a, m)} \rightarrow \text{Sig I})\)
  if \(i \in \mathcal{L}_{\text{mut}}\)

Note that some type information is missing in the \(\lambda^{\text{IO}}\)-terms; namely the type \(\text{Rep}\) of \(s\) in the first clause and \(\text{Sig I}\) in the last clause. However, type information in terms does not play a role in the interpretation of terms in the PER model that we are interested in, so we can safely ignore this.

We now consider the PER model of \(\text{PAC94}\). Here types are interpreted as partial equivalence relations (pers) on \(\mathbb{N}_1\), and terms are interpreted as natural numbers, using some enumeration of the partial recursive functions.

The \text{per} interpreting a type \(A\) is written as \(\llbracket A \rrbracket_{\xi}\), where \(\xi\) is a type environment that maps from type variables to pers. The natural number interpreting a term \(a\) is written as \(\llbracket a \rrbracket_{\eta}\), where \(\eta\) is an environment that maps to natural numbers. Another way of looking at the PER model is to interpret a type \(A\) as the set of \(\llbracket A \rrbracket_{\xi}\)-equivalence classes, and to interpret a term \(a : A\) as the \(\llbracket A \rrbracket_{\xi}\)-equivalence class that contains \(\llbracket a \rrbracket_{\eta}\).

\(\lambda^{\text{IO}}\) without class types can be interpreted in this PER model for \(F_{\leq}\) by interpreting interface types, objects, and method invocations by their \(F_{\leq}\)-counterparts:

- \(\llbracket \text{Sig I} \rrbracket_{\xi} = \llbracket \exists X. X \times (X \rightarrow I(X)) \rrbracket_{\xi}\)
- \(\llbracket \text{object}_I (s, m) \rrbracket_{\eta} = \llbracket \text{pack (Rep}_i (s, m)) \rightarrow \text{Sig I} \rrbracket_{\eta}\)
- \(\llbracket o \leftarrow I(a) \rrbracket_{\eta} = \llbracket \text{open} \text{o as} (X_i, (s, m)) \in (m \ s) I a \rrbracket_{\eta}\)
  if \(i \in \mathcal{L}_{\text{obs}}\)
- \(\llbracket o \leftarrow I(a) \rrbracket_{\eta} = \llbracket \text{open} \text{o as} (X_i, (s, m)) \in \text{pack (X}_i, (m \ s) I a, m) \rightarrow \text{Sig I} \rrbracket_{\eta}\)
  if \(i \in \mathcal{L}_{\text{mut}}\)

A pair \((\eta, \xi)\) satisfies a context \(\Gamma - \text{written} (\eta, \xi) = \Gamma - \text{iff} (\eta(x), \eta(x)) \in \llbracket A \rrbracket_{\xi}\) for all declarations \(x : A\) in \(\Gamma\). Given that the PER model is a sound model for \(F_{\leq}\), it is also a sound model for \(\lambda^{\text{IO}}\).

**Theorem 4.2**

If \(\Gamma \vdash a \simeq a' : A\) in \(\lambda^{\text{IO}}\) without class types, then \(\llbracket a \rrbracket_{\eta}, \llbracket a' \rrbracket_{\eta} \in \llbracket A \rrbracket_{\eta}\) for all \((\eta, \xi)\) that \(\Gamma\).

We will now look at the interpretations of class types and interface types in more detail. Some properties of these interpretations will be used to interpret class types in the next section.

First a few definitions. We write \(n \rightarrow m\) for the \(n\)-th partial recursive function applied to \(m\), and \(\llbracket x. E(x) \rrbracket_{n = E(n)}\) for the index of a partial recursive function for which \(\llbracket x. E(x) \rrbracket_{n = E(n)}\) where \(E(x)\) is a partial recursive description of a natural number depending on \(x\).

We write \(\llbracket n \rrbracket_{E}\) for the \(R\)-equivalence containing \(n\), and \(\mathbb{N}_1 / R\) for the set of \(R\)-equivalence classes. For pers \(R\) and \(S\), the per \(R \Rightarrow S\) is defined as

- \(R \Rightarrow S = \{(f, f') : \mathbb{N} \times \mathbb{N} \mid \forall (a, a') : A. (f \cdot a, f' \cdot a') \in B\}\)
We write \( n \in R \) as abbreviation for \( (n, n) \in R \).

The category \( \text{PER} \) is defined as in [BFAS90] and [Has94] as the category with as objects pers on \( \mathbb{N} \) and as the arrows from \( R \) to \( S \) total functions from \( \mathbb{N}/R \) to \( \mathbb{N}/S \) named by a partial recursive functions in \( R \to S \).

### 4.1 Interpretation of objects

We define \( \text{obj}(x) \) and \( \sim \) as the interpretations of object \( (x, x) \) and \( \sim \) in the \( \text{PER} \) model. So

\[
\text{obj}_I(s, m) = \text{obj}((s, [m])_I)
\]

and

\[
\sim_\text{I}(a, b)_I = \sim([a]_I, [b]_I).
\]

Looking at the interpretations of the \( F \)-terms that \( \text{obj}() \) and \( \sim \) denote, we find that

\[
\text{obj}(s, m) \sim a = \begin{cases} (m \cdot s) \cdot a & \text{if } I \in \mathbb{L}_{\text{out}} \\ \text{obj}((m \cdot s) \cdot a, m) & \text{if } I \in \mathbb{L}_{\text{in}} \end{cases}
\]

Note that we abuse our notation for field selection here and write "\( \text{I} \)" for the selection of the \( l \)-field, when we should really use the interpretation of the \( l \)-projection under the encoding of records as products discussed in Remark 4.1.

### 4.2 Interpretation of interface types

The interesting property of the \( \text{PER} \) model is that the existential types of the form \( \exists X. X \times (X \to I(X)) \) – i.e., interface types – are interpreted as final coalgebras, as is proved in [Has94] and [PA93].

We define \( \text{SIG}(\cdot) \) as the interpretation of \( \text{Sig}(\cdot) \) in the \( \text{PER} \) model. So

\[
\text{SIG}_I(l) = \exists X. X \times (X \to I(X)) \subseteq \mathbb{L}_l
\]

Let \( I : \text{PER} \to \text{PER} \) be the functor interpreting some interface \( I \) in some environment \( \xi \), i.e. \( I = [I]_\xi \). We define \( \text{out}_I \) as

\[
\text{out}_I = \lambda o. [I](\lambda s. \text{obj}(s, \text{snd}(o))) \cdot (\text{snd}(o) \cdot \text{fst}(o)).
\]

Another way of defining \( \text{out}_I \) is as the interpretation of \( \text{out}_I : \text{Sig} I \to \text{I}(\text{Sig} I) \), defined as follows

\[
\text{out}_I = \lambda o. \text{open} o \cdot \lambda x. \text{obj}(x, (s, m)) \cdot \text{I}_m(\lambda x. \text{object}_I(x, m)) \cdot (m s)
\]

\[
\text{Sig} I \to \text{I}(\text{Sig} I)
\]

Here \( I_m \) is the action of \( I \) on functions, with \( I_m(f) : I(A) \to I(B) \) for any \( f : A \to B \), defined in the usual way by induction on \( I \).

The pair \( \langle \text{Sig}(I), \text{out}_I \rangle \) is a final coalgebra [Has94][PA93].

So

\[
\text{out}_I \subseteq \text{Sig}(I) \Rightarrow I(\text{Sig}(I)),
\]

and we have the following properties:

**Property 4.3** Let \( s_i \in \text{Rep}_I \) and \( m_i \in \text{Rep}_I \to I(\text{Rep}_I) \) for certain pers \( \text{Rep}_I \), \( i = 1, 2 \).

Then

\[
(\text{obj}(s_1, m_1), \text{obj}(s_2, m_2)) \in \text{Sig}(I) \iff \exists \sim \in \mathbb{N} \times \mathbb{N}. \sim = \text{Rep}_I \sim \text{Rep}_I \iff s_1 \sim s_2 \wedge (m_1, m_2) \in \sim \Rightarrow I(\sim)
\]

Here \( \circ \) denotes composition of relations.

**Property 4.4** For any relation \( \sim \subseteq \mathbb{N} \times \mathbb{N} \), \( \text{out}_I \sim \Rightarrow I(\sim) \). Then \( \text{out}_I \equiv \sim \Rightarrow \text{Sig}(I) \).

In other words, \( \text{Sig}(I) \) is the maximum bisimulation.

These properties are particular cases of Theorems 7 and 11 in [PA93]. A direct consequence (take \( \sim = \text{Rep}_I = \text{Rep} \)) of Property 4.3 is:

**Corollary 4.5** Let \( (s_1, s_2) \in \text{Rep} \) and \( (m_1, m_2) \in \text{Rep} \), then \( \text{obj}(s_1, m_1), \text{obj}(s_2, m_2) \in \text{SIG}(I) \).

The mapping \( \text{out}_I \) is related to the interpretation of method invocations \( \sim \) as follows:

**Property 4.6** Let \( I = [I]_\xi \) for some \( \xi \), with \( I \) an interface that contains a method \( l \). Then

\[
o \sim a = (\text{out}_I \cdot o) \cdot l \cdot a
\]

As before, we abuse our notation for field selection here.

### 5 Model for \( \lambda^{OO} \) with Class Types

We now extend the interpretation of \( \lambda^{OO} \) without class types in the \( \text{PER} \) model of [PA94] to an interpretation of the full \( \lambda^{OO} \) including the class types.

**Definition 5.1** The relation \( \subseteq \) on pers is defined by

\[
R \subseteq S \iff N/R \subseteq N/S
\]

An equivalent definition is

\[
R \subseteq S \iff R \subseteq S \wedge R = S; R; S.
\]

The relation \( \subseteq \) is used to define the interpretation of a class types:

**Definition 5.2** For \( I : \text{PER} \to \text{PER} \) and \( m, n \in \mathbb{N} \) we define \( \text{CLASS}(I, s, m) \) as follows

\[
\text{CLASS}(I, s, m) = \left\{ X \subseteq \text{SIG}(I) \mid \text{obj}(s, m) \in X \wedge \text{out}_I \subseteq X \Rightarrow I(X) \right\}.
\]

This defines \( N/\text{CLASS}(I, s, m) \) as the smallest subset of \( N/\text{SIG}(I) \) that contains \( \text{obj}(s, m) \) and is closed under method invocations.

**Lemma 5.3** Let \( I : \text{PER} \to \text{PER} \). Suppose that \( I \) is continuous – i.e., \( I(\bigcap X_i) = \bigcap I(X_i) \) – and suppose that \( I(R) ; I(S) \subseteq I(R; S) \) for all pers \( R \) and \( S \). Then

1. \( \text{CLASS}(I, s, m) \subseteq \text{SIG}(I) \)
2. \( \text{obj}(s, m) \in \text{CLASS}(I, s, m) \)
3. \( \text{outI} \in \text{CLASS}(I, s, m) \Rightarrow I(\text{CLASS}(I, s, m)) \)
4. Let \((s_1, s_2) \in \text{Rep} \) and \((m_1, m_2) \in \text{Rep} \Rightarrow I(\text{Rep}) \).
   Then \( \text{CLASS}(I, s_1, m_1) = \text{CLASS}(I, s_2, m_2) \).

Proof. These properties easily follow from the definition of CLASS and the assumptions on \( I \). For 4, use Corollary 4.5 to deduce that
\[
(s, m) \in X \iff (s', m') \in X \quad \text{for any } X \subseteq \text{SIG}(I)
\]
from the assumptions on \( s_1 \) and \( m_1 \).

It is easy to verify that any \( I \) that is the interpretation of a \( \lambda^{\text{OO}} \)-signature will satisfy the conditions of the lemma above.

CLASS will now be used to extend the PER model of \( \lambda^{\text{OO}} \) without class types to a model for the full \( \lambda^{\text{OO}} \). The definition of this model is given below.

As far as terms is concerned nothing changes. In \( \lambda^{\text{OO}} \) without class types we have the same terms as in \( \lambda^{\text{OO}} \) with class type, so the terms can be interpreted as in the PER model discussed in the previous section.

**Definition 5.4** The interpretation \( [a]_\eta \in \text{IN} \) of a \( \lambda^{\text{OO}} \)-term \( M \) in term environment \( \eta \) is defined as
\[
[a]_\eta = [\text{Emse}(a)]_\eta,
\]
where
- \( \text{Emse}(\text{object}(s, m)) = \text{object}(\text{Emse}(s), \text{Emse}(m)) \)
- \( \text{Emse}(\text{ov-l}(a)) = \text{Emse}(a) \text{ov-l}(\text{Emse}(a)) \)
- \( \text{Emse}(\text{lxr}(b)) = \text{lxr}(\text{Emse}(b)) \)
- \( \text{Emse}(\text{fa}(a)) = \text{Emse}(f) \text{Emse}(a) \)
- \( \text{Emse}(\text{ail}(a)) = \text{Emse}(a) \text{ail} \)
- \( \text{Emse}(\text{ej}(\{l_1 = a_1, \ldots, l_n = a_n\})) = \{l_1 = \text{Emse}(a_1), \ldots, l_n = \text{Emse}(a_n)\} \)

and he interpretation of emse terms is defined by
\[
[\text{f}]_\eta = \eta(x), \\
[lx. \text{e}]_\eta = \lambda x. [\text{e}]_{\eta[x/\text{e}]}, \\
[\text{f}0]_\eta = \{[\text{f}]_\eta, [\text{e}]_\eta\}, \\
[\text{object}(s, m)]_\eta = \text{obj}([a]_\eta, [m]_\eta), \\
[o \text{-l}(a)]_\eta = [a]_\eta \text{-l} [a]_\eta, \\
[l\{l_1 = a_1, \ldots, l_n = a_n\}]_\eta = \{l_1 = [a_1]_\eta, \ldots, l_n = [a_n]_\eta\}, \\
[a/l]_\eta = [a]_\eta [l]
\]

Here we again abuse our notation for records and field selection as shorthand for their interpretations under the encoding discussed in Remark 4.1.

Because class types contain terms as subexpressions, the interpretation of types now has to be given w.r.t. a term environment \( \eta \) as well as a type environment \( \xi \):

**Definition 5.5** The interpretation \( [A]_{\eta, \xi} \) of a type \( A \) in environment \( \eta, \xi \) is given by
\[
[X]_{\eta, \xi} = \xi(X), \\
[A-B]_{\eta, \xi} = [A]_{\eta, \xi} \rightarrow [B]_{\eta, \xi}, \\
[l\{l_1 = A_1, \ldots, l_n = A_n\}]_{\eta, \xi} = \{l_1 = [A_1]_{\eta, \xi}, \ldots, l_n = [A_n]_{\eta, \xi}\}, \\
[\text{Sig} I]_{\eta, \xi} = \text{CLASS}([I]_{\eta, \xi}, [\text{init}]_{\eta}, [m]_{\eta})
\]

Again, the notation for record types is abused as shorthand for their interpretations under the encoding discussed in Remark 4.1.

**Theorem 5.6** If \( \Gamma \vdash a \simeq a' : A \) in \( \lambda^{\text{OO}} \)
then \( ([a]_{\eta, \xi}, [a']_{\eta, \xi}) \in [A]_{\eta, \xi} \) for all \( \eta, \xi \models \Gamma \).

Proof. Soundness of type assignment, i.e.,

\[
\Gamma \vdash a : A \land \eta, \xi \models \Gamma \Rightarrow [a]_{\eta, \xi} \in [A]_{\eta, \xi},
\]
can be proved in the usual way. Lemma 5.3.1 is needed for soundness of the subtyping rule for classes, 5.3.2 for soundness of the introduction rule for classes, and 5.3.3 – together with Lemma 4.6 – for soundness of the elimination rules for classes.

No extra work is needed to prove soundness of reduction: we can reuse the following property of the PER-interpretation of \( F_{\leq} : [a]_{\eta, \xi} \) and \( [a']_{\eta, \xi} \) are defined, then
\[
a \simeq a' \Rightarrow [a]_{\eta, \xi} = [a']_{\eta, \xi}.
\]

Since the mapping from \( \lambda^{\text{OO}} \) to \( F_{\leq} \) preserves reduction, we immediately have the property that if \( [a]_{\eta, \xi} \) and \( [a']_{\eta, \xi} \) are defined, then
\[
a \simeq a' \Rightarrow [a]_{\eta, \xi} = [a']_{\eta, \xi}.
\]

### 5.1 Subtyping is Behavioural Subtyping

We now show that in the PER model subtyping between class types corresponds with the notion of behavioural subtyping as we informally explained it in Section 2.

**Definition 5.7** For \( \text{init} \in \text{Rep} \) and \( m \in \text{Rep} \Rightarrow (\text{Rep}) \) the per \( \text{REACH}(I, \text{Rep}, \text{init}, m) \) is defined as follows:
\[
\text{REACH}(I, \text{Rep}, \text{init}, m) = \{X \subseteq \text{IN} \mid X \subseteq \{X \mid \text{init} \subseteq X \land m \in X \Rightarrow I(X)\}\}
\]

\( \text{IN} / \text{REACH}(I, \text{Rep}, \text{init}, m) \) is the set of those \( \text{Rep} \)-equivalence classes reachable from the state \( \text{init} \) using the method implementations \( m \). Note the similarity between the definition of \( \text{REACH} \) and the definition of \( \text{CLASS} \). There is close relationship between the two:

**Lemma 5.8** Let \( I : \text{PER} \Rightarrow \text{PER} \). Suppose that \( I \) is continuous – i.e., \( I(\bigcap X_i) = \bigcap I(X_i) \) – and that \( I(R); I(S) \subseteq I(R; S) \) for all pers \( R \) and \( S \). Then
\[
\text{IN} / \text{CLASS}(I, \text{init}, m) = \{[\text{obj}(s, m)]_{\text{SIG}(I)} \mid s \in \text{REACH}(I, \text{Rep}, \text{init}, m)\}
\]

Proof. (Sketch) First we consider \( \subseteq \). Define the per \( X \) as
\[
X = \text{Rep} \cap (f; \text{CLASS}(I, \text{init}, m); f^\rightarrow),
\]
where \( f \subseteq \text{IN} \times \text{IN} \) is the relation \( \{s, \text{obj}(s, m) \mid s \in \text{IN}\} \) and \( f^\rightarrow \) its inverse. We can prove the following properties of \( X \):
\[
\begin{align*}
X & \subseteq \text{Rep}, \\
\text{init} & \subseteq X,
\end{align*}
\]
It then follows by the definition of \( \text{REACH} \) that
\[
\text{REACH}(I, \text{Rep}, \text{init}, m) \subseteq X,
\]
and so
\[
f^{-1} \circ \text{REACH}(I, \text{Rep}, \text{init}, m) \subseteq X,
\]
from which we can prove \((\Rightarrow)\).

Now to prove \((\Leftarrow)\). Define
\[
Y = \Sigma I(I); f^{-1} \circ \text{REACH}(I, \text{Rep}, \text{init}, m); f \circ \Sigma I(I)
\]
for \(I\) we can prove the following properties:
- \(Y \supseteq \Sigma I(I)\),
- \((\text{init}, m) \in Y\),
- \(\text{out}_2 \in Y \Rightarrow I(Y)\).

It then follows by the definition of \( \text{CLASS} \) that
\[
\text{CLASS}(I, \text{init}, m) \subseteq Y,
\]
from which we can prove \((\Leftarrow)\).

The relation below defines subtyping between interpretations of signatures:

**Definition 5.9** The relation \(\leq\) on \(\text{PER} \rightarrow \text{PER}\) is defined as follows:
\[
I_1 \leq I_2 \iff I_1(X) \subseteq I_2(X) \text{ for all pers } X \text{ and both } I_i \text{ are continuous with } I_i(R); I_i(S) \text{ for all pers } R \text{ and } S.
\]

We can now state our main result, namely that, for interpretations of class types, the subset relation on pers is equivalent with the notion of behavioural subtyping that we described in Section 2.

**Theorem 5.10 (Subtyping is Behavioural Subtyping)**

Suppose \(\text{init}_i, m_i \in \text{Rep}_i\) and \(m_i \in \text{Rep}_i \Rightarrow I_i(\text{Rep}_i)\), for certain pers \(\text{Rep}_i\) for \(i = 1, 2\). If \(I_1 \leq I_2\) then
\[
\text{CLASS}(I_1, \text{init}_1, m_1) \subseteq \text{CLASS}(I_2, \text{init}_2, m_2) \iff \exists \sim \subseteq \mathbb{N} \times \mathbb{N}. \sim = \text{Rep}_1; \sim; \text{Rep}_2 \wedge (m_1, m_2) \in \sim \Rightarrow I_2(\sim) \wedge \forall s_1 \in \text{REACH}(I_1, \text{Rep}_1, \text{init}_1, m_1). \exists s_2 \in \text{REACH}(I_2, \text{Rep}_2, \text{init}_2, m_2). s_1 \sim s_2
\]
The second part of this theorem is a formal definition of the notion of behavioural subtyping discussed in Section 2: The condition
\[
(m_1, m_2) \in \sim \Rightarrow I_2(\sim)
\]
corresponds to condition (i) on page 3, and the condition
\[
\forall s_1 \in \text{REACH}(I_1, \text{Rep}_1, \text{init}_1, m_1). \exists s_2 \in \text{REACH}(I_2, \text{Rep}_2, \text{init}_2, m_2). s_1 \sim s_2
\]
corresponds to condition (ii) on page 3.

*Proof. (Sketch) Define \(C_i = \text{CLASS}(I_i, \text{init}_i, m_i)\) and \(R_i = \text{REACH}(I_i, \text{Rep}_i, \text{init}_i, m_i)\).

\[\Rightarrow\) Let \(C_1 \subseteq C_2\).
Define \(\sim \subseteq \mathbb{N} \times \mathbb{N}\) as follows
\[
\sim = \text{Rep}_1; f_1; \Sigma I(I); f_2^{-1}; \text{Rep}_2,
\]
where \(f_1 = \{(s, \text{obj}(s, m_1)) | s \in \mathbb{N}\}\). For this relation \(\sim\) the required properties can be proven.

\(\Leftarrow\) Let \(\sim \subseteq \mathbb{N} \times \mathbb{N}\) be such that
\[
(i) \sim = \text{Rep}_1; \sim; \text{Rep}_2,
(ii) (m_1, m_2) \in \sim \Rightarrow I_2(\sim),
(iii) \forall s_1 \in R_1. \exists s_2 \in R_2. s_1 \sim s_2.
\]
Suppose that \(o_1 \in C_1\). Then by Lemma 5.8(\(\subseteq\)) there is an \(s_1 \in R_1\) such that \((o_1, (s_1, m_1)) \in \Sigma I(I_1)\). Then by (iii) there is an \(s_2 \in R_2\) such that \(s_1 \sim s_2\). By Property 4.3 it now follows that \((\text{obj}(s_1, m_1), \text{obj}(s_2, m_2)) \in \Sigma I(I_2)\), and then \((s_2, m_2) \in C_2\) by Lemma 5.8(\(\Rightarrow\)). Moreover, by \(\Sigma I(I_1) \subseteq \Sigma I(I_2)\) and the transitivity of pers \((o_1, \text{obj}(s_2, m_2)) \in \Sigma I(I_2)\).

This proves
\[
o_1 \in C_1 \Rightarrow \exists o_2 \in C_2. (o_1, o_2) \in \Sigma I(I_2).
\]
From this property we can now deduce \(C_1 \subseteq C_2\) using \(C_i \subseteq \Sigma I(I_i)\) and some basic properties of \(\subseteq\).

**6 Conclusions and directions for future work**

This paper establishes a link between three different strands of research on object-oriented languages, namely
- the type-theoretic approach to objects of [PT94],
- the work on behavioural subtyping of [Lea90],
- the categorical approach to objects of [Rei95].

For an extension of the type-theoretic encoding of object of Pierce and Turner [PT94] we have shown that the standard interpretation of subtyping in PER models – subtypes are supertypes – provides exactly the notion of behavioural subtyping defined by Leavens [Lea90]. The crucial property is that object types are interpreted as final co-algebras. The correspondence between the existential object encoding and final coalgebras noted in [HP95] extends to our class types and sub-coalgebras of the final coalgebra. Sub-coalgebras are used in [Rei95] and [Jac96] as specifications of objects; our class types can of course be regarded as specifications, where we specify objects by giving a particular implementation.

The usefulness of the coalgebraic view of objects suggests that it might be better to use a primitive notion of coinductive type to present the existential object model, rather than an encoding of such types using existential types. The existential object model could for instance be carried out using Hagino’s categorical datatypes [Hag87] extended with subtyping (The interface types of \(\lambda^{O\,O}\) are essentially coalgebraic types in the sense of [Hag87]). An advantage would be that coinductive types only require a first-order type system, whereas existential types require a second-order type system.

One subject for future work is a more general description of a model for \(\lambda^{O\,O}\) in categorical terms, in which interface
types are interpreted as final coalgebras, class types as sub-
coalgebras, and subtyping as coercions between them. We
hope this will streamline much of the theory, and allow a
presentation giving more than just sketches of proofs. (Note
that $\tau$-coalgebras are only defined up to isomorphism, but
the PER model here relies on the construction of a particular
one of these as the interpretation of an interface type.)

We have not mentioned inheritance here. Inheritance
for the existential model encoding is described in [PT94].
Now that we have a notion of behavioural subtyping, the
interesting problem to look at is: "When does inheritance
produce behavioural subtypes?" Ideally we would want to
formulate general conditions that are sufficient to guarantee
that a class defined by inheritance is a behavioural subtype
of the class it inherits from.

$\lambda\omega$ could be extended with subtyping between class
types, where this subtyping between class types is declared
by the programmer. It would have to be the responsibility
of the programmer that such declared subtyping is sound, as
this is not something that can be decided by a typechecker.
We would then really want a logic for reasoning about pro-
grams in which soundness of subtyping between class types
can be expressed and (dis)proved. Such a logic would be
an major topic for further investigation. Here it might be
possible to use existing work on behavioural subtyping.

Finally, it would be interesting to see if the PER mod-
els of the other object encodings, e.g. those discussed in
[BCP97], can also provide a notion of behavioural subtyp-
ing for class types. This would be more difficult: these other
object encodings are in type systems with unrestricted re-
cursion, and it is not clear what the effect of recursion would
be. Also, the method updates allowed by some of these en-
codings would cause complications. These would have to be
ruled out if we want to statically guarantee that all objects
of a class type have the same method table.

References

[AC96] Martin Abadi and Luca Cardelli. A Theory of Ob-

of object-oriented programs. In TAPSOFT '97: The-

[Ame89] Pierre America. A Behavioural Approach to Sub-
typing in Object-Oriented Languages. Technical

[BCP97] Kim B. Bruce, Luca Cardelli, and Benjamin C.
Pierce. Comparing object encodings. In Theo-
retical Aspects of Computer Software (TACS '97), Sendai, Japan, volume 1281, pages 415–438.
Springer LNCS, September 1997.

[BMAS90] E.S. Bainbridge, P.J. Freyd, A. Scedrov, and P.J.
Scott. Functorial polymorphism. Theoretical

[BL90] Kim B. Bruce and Giuseppe Longo. A modest
model of records, inheritance, and bounded quanti-
fication. Information and Computation, 87:196–
240, 1990. Also in [GM94].

programming language: Design, static typing and
semantics. Journal of Functional Programming,

[Car88] Luca Cardelli. A semantics of multiple inher-

[Car92] Luca Cardelli. Extensible records in a pure cal-
culus of subtyping. Research report 81, DEC Sys-
tems Research Center, 1992. Also in [GM94].

typed object-oriented programming. In Proceed-
ings of Theoretical Aspects of Computer Software
(TACS'94), Sendai, Japan, volume 789 of LNCS,

[FM97] K. Fisher and J.C. Mitchell. On the relation-
ship between classes, objects, and data abstrac-
tion. In Proceedings of the International Sum-
mer School on Mathematics of Program, LNCS.

[GM94] Carl A. Gunter and John C. Mitchell. Theo-
retical Aspects of Object-Oriented Program-
ming: Types, Semantics, and Language Design.

[Hag87] Tatsuya Hagino. A typed lambda calculus with
categorical type constructors. In D.H. Pitt,
A Poigné, and D.E. Rydeheard, editors, Category
and Computer Science, pages 140–157. Springer,
September 1987.

[Has94] Tyu Hasegawa. Categorical data types in para-
metric polymorphism. Mathematical Structures

[HP95] Martin Hofmann and Benjamin C. Pierce. A uni-
fying type-theoretic framework for objects. Jour-
nal of Functional Programming, 5(4):593–635,
1995.

[Jac96] Bart Jacobs. Objects and classes, co-
algebraically. In Object-Orientation with Par-
allelism and Persistence, pages 83–103. Kluwer

[Lea90] Gary T. Leavens. Modular verification of object-
oriented programs with subtypes. Technical Re-
port 90-09, Department of Computer Science,
Iowa State University, Ames, Iowa, 50011, July
1990.

[Lis88] Barbara H. Liskov. Data abstraction and hierar-

A behavioral notion of subtyping. TOPLAS,

[LW95] Gary T. Leavens and William E. Weihl. Specifi-
cation and verification of object-oriented programs
using supertype abstraction. Acta Informatica,

[Man95] Ian Maung. On simulation, subtyping and sub-
stitutability in sequential object systems. Formal


