Dynamic Overloading with Copy Semantics in Object-Oriented Languages: a Formal Account

Lorenzo Bettini 1  Sara Capecchi 1  Betti Venneri 2

1 Dipartimento di Informatica, Università di Torino,
{bettini,capecchi}@di.unito.it
2 Dipartimento di Sistemi e Informatica, Università di Firenze,
venneri@dsi.unifi.it

Abstract. Mainstream object-oriented languages often fail to provide complete powerful features altogether, such as, multiple inheritance, dynamic overloading and copy semantics of inheritance. In this paper we present a core object-oriented imperative language that integrates all these features in a formal framework. We define a static type system and a translation of the language into the meta-language $\lambda_{\text{object}}$, in order to account for semantic issues and prove type safety of our proposal.

Subject Classifications: 68N15 [Programming Languages], 68N18 [Functional programming and lambda calculus], 68Q55 [Semantics].

1 Introduction

The dynamic flexibility of object-oriented languages is essentially based on the concepts of polymorphism and dynamic binding. The former, together with subtyping and substitutivity, allows the programmer to treat different, but related, objects uniformly. The latter ensures that the right operation is performed when a message is sent to such objects, according to their actual type. The choice of combining dynamic binding with static (polymorphic) typing seems to be the suitable solution to achieve both flexibility and reliability in most popular languages, such as Java [AGH00] and C++ [Str97].

However, static typing raises some limitations in exploiting dynamic method selection. An interesting case concerns method overloading, i.e., the ability to write methods with the same name, which associate different bodies to different parameter types. In mainstream languages, the interpretation of overloading is static, since the actual code to execute in a method call is selected by the compiler, according to static types of the parameters. Thus polymorphism is not exploited fully (e.g., [CW85] calls this kind of polymorphism "ad-hoc"). To overcome this limitation, a common programming practice is to resort to RTTI (run time type information) mechanisms and if statements, in order to explore manually the run-time type of an object, and to type downcasts, in order to force the view of an object according to its run-time representation. These techniques are discouraged by object-oriented design, since they undermine re-usability and evade the constraints of static type checking. Another alternative is to implement double dispatch [Ing86], for example using the Visitor pattern [GHJV95]. This solution, however, requires the programmer extra effort since the dynamic dispatch mechanism must be explicitly programmed. Moreover, a cyclic dependence arises from the structure of the pattern, so undermining code re-usability.

Multi-methods [DG87,MHH91,Cas95,BC97] naturally support dynamic overloading: the same message name is associated to a set of different bodies (branches) and the run-time selection of the body to invoke depends not only on the actual type of the receiver (single dispatch) but also on the dynamic types of the arguments (multiple dispatch). A major advantage of multi-methods is to enable a safe covariant

\* This work has been partially supported by EU Project Software Engineering for Service-Oriented Overlay Computers (SENSORIA, contract IST-3-016004-IP-09) and by MIUR project EOS DUE.
specialization of methods, where subclasses are allowed to redefine a method by specializing its arguments. There is general evidence that covariant code specialization is an indispensable practice in many situations [Mey91,BDK92]: its most expressive application appears with binary methods [BCC+ 95], i.e., methods that act on objects of the same type as the receiver.

In this paper our main goal is to investigate the interaction between dynamic overloading and (multiple) inheritance in a formal framework, combine them in a theoretical model, and prove type safety of the proposed approach. To this aim we define DOCS (Dynamic Overloading with Copy Semantics), a lightweight class-based language that brings basic object-oriented mechanisms into an imperative setting, while adding multiple inheritance and multi-methods. Concerning the interpretation of inheritance, DOCS adopts a copy semantics, in the sense that all the inherited overloaded methods are intended to be directly copied into the subclass. This avoids a too restrictive overloading resolution policy that leads to “strange” compilation errors or unexpected behaviors. We note that the above features, multiple inheritance, multi-methods and copy semantics, are not provided altogether in related approaches (see, e.g., [BC97,CLCM00,Cas95,IPW01,LM98]).

We base the foundation of our proposal on $\lambda$-object [Cas95,Cas97], an extended typed lambda-calculus which can be used as a meta language for modeling object oriented features in a functional context. DOCS semantics is defined by translation into $\lambda$-object; this provides a deeper understanding of the integration of dynamic overloading with other features, such as encapsulation (any object encapsulates its methods) and copy semantics. Since $\lambda$-object is type safe, by proving that every well typed DOCS program is translated in a well typed $\lambda$-object term, we obtain an indirect proof of static type safety for DOCS, i.e., well typed programs will not generate type errors at run time. Moreover, $\lambda$-object is very close to actual object-oriented programming language implementations: this is particularly evident in that class methods are basically translated into functions that take the receiver of method invocation as a parameter (see, e.g., [Lip96]). Thus, the semantics of DOCS into $\lambda$-object gives practical hints to drive the language implementation according to the formal specification. The semantics of DOCS is inspired by KOOL [Cas95,Cas97] translation into $\lambda$-object for what concerns some basic language expressions. Instead, there is a crucial difference in multi-method interpretation, because of the copy semantics characterizing our approach. Furthermore, since translational semantics is type-driven, then differences in typing lead to significant differences between DOCS and KOOL semantics.

1.1 Design issues

In this section we discuss the main choices that characterize our approach with respect to other proposals. DOCS implements dynamic overloading by supporting multi-methods. Indeed a standard method is seen as a particular case of a multi-method with only one branch; thus the distinction between static and dynamic overloading is made at the level of method invocation (DOCS provides two different constructs for message sending). This choice increases the flexibility of programming and the reuse of classes: methods are declared in a uniform way and then used through method calls, by choosing the most suitable overloading policy.

Concerning multi-methods, DOCS aims at being an integration of different design choices. We can distinguish two kinds of multi-methods in the literature: 1) the encapsulated multi-methods that preserve the class-based encapsulation property (as in [BC97]), 2) the view of multi-methods as global functions external to classes (as in [Kee89,Sha97,CGL93,LM98]). In the former approach the principle that an object has a set of associated methods is preserved.

In method selection, dispatch can be asymmetric in the sense that the receiver (and possibly other parameters) has the precedence over other parameters during selection. When the receiver and other parameters participate together in determining the version of the method to be executed we have symmetric dispatch.

Usually encapsulated multi-methods are equated to asymmetric multiple dispatch [BCC+ 95] while, in our opinion, the two aspects are orthogonal. Obviously it seems more natural to have asymmetric dispatch when methods are encapsulated: since there is a privileged receiver, we can think of it as the parameter
driving method selection. Instead, there are extensions of single dispatching languages to encapsulated multi-methods that simulate symmetric dispatch [CLCM00,BCV06] and languages, such as CLOS [Kee89], adopting asymmetric dispatch for selecting the right body of generic functions. Indeed, the choice between symmetric or asymmetric dispatch can be also driven by the need for modularity: an order on parameters during method selection can resolve the ambiguities that arise when linking together software modules defining behaviors for the same message. For instance, asymmetric dispatch is a solution for a language like CLOS, which is dynamically typed, in order to avoid ambiguities at run time; another example is the extension of Java with parasitic methods [BC97] which gives the precedence to the receiver object in method selection, to obtain modular type checking.

Clearly, method selection with symmetric dispatch is a more flexible mechanism, since it can choose among all the available versions defined for a message name (it does not restrict the choice to the bodies defined in the class of the receiver). The problem is that with symmetric dispatch it is hard to obtain a good compromise between type safety [Smi03,FDR00] and flexibility [LM98].

The approach chosen for DOCS is to adopt encapsulated multi-methods and symmetric dispatch, while preserving type safety and programming flexibility.

As for the inheritance mechanism, we chose to consider multiple inheritance, since single inheritance is not expressive enough to design class hierarchies and it may lead to duplicate code since it fails in factoring out all the common features shared by classes in a complex hierarchy. Multiple inheritance is rather expressive but it complicates the issue of “ambiguities resolution” already introduced by multiple dispatch. Indeed, considering the interaction between multiple inheritance and multiple dispatch makes our approach more general; the adaptation to the single inheritance case is straightforward, while the other way round is not.

Concerning the interpretation of inheritance, [ADZ01] points out that semantics of overloading and inheritance is rather “clean” if it is interpreted through a copy semantics, where all the inherited overloaded methods are intended to be copied into the subclass (apart for those explicitly redefined by the subclass itself). In DOCS, we adopt copy semantics of inheritance as a strategy for the resolution of possible ambiguities due to overloading (not as an implementation technique). We note that the resolution policy for static overloading in Java has followed copy semantics since version 1.4. From a foundational point of view, following B. Meyer [Mey01], inheritance nicely fits a framework where classes are viewed as functions, a special case of sets; the basic idea for modeling inheritance is that a class is the “union” of its own definition and those of its parent(s) (according to the model of [AC96]). The “flattening” of classes is also adopted in engineering of object oriented systems in particular to study the impact of inheritance on object oriented metrics [BLS00] and for specifying the semantics of classes that use traits [DNS+06].

DOCS is equipped with a type system in order to model the considered features and their interaction in a type safe way. Indeed the main goal of our approach is to guarantee type safety (other approaches do not enjoy this property [Car02,DLS+01,Ale01]): typing rules ensure that no run time error will occur due to missing or ambiguous branches during dynamic multi-method invocation. The key notion of well formed multi-type (used to type multi-methods) is inspired by [Cas95,Cas97] but differs from it in that it takes into account that copy semantics is implemented in deducing multi-types. As a consequence, for instance, many static ambiguities that could be raised using the rules of [Cas95,Cas97] are automatically resolved in DOCS, in particular when single inheritance is involved. In Section 2 we present an example to show how copy semantics combines encapsulated multi-methods with symmetric dispatch.

Finally, we mention that the issue of modularity is out of the scope of the present paper, where we type-check each DOCS program as a single module containing all the classes that are used in it. Indeed modularity is a key problem when integrating multi-methods with symmetric dispatch into a language: modules developed separately, which pass type checking in isolation, may cause type errors when combined. Some works on multi-methods have resolved the problem either by relying on a global type checking [LM98,CL96] or by adopting asymmetric dispatch [BC97,BCC+95]. Other approaches are the result of the effort spent on modular type checking in the presence of multi-methods [MC02,CLCM00,CL95]. Concern-
class Inspector {
    Report Inspect(EURO0 *c){...}
    Report Inspect(EURO1 *c){...}
}

class Inspector_2006: Inspector {
    Report Inspect (EURO2 *c){...}
}

class Inspector_2007: Inspector_2006 {
    Report Inspect(EURO0 *c){...}
    Report Inspect(EURO1 *c){...}
    Report Inspect(EURO2 *c){...}
}

Listing 1: The gas emission example, where EURO2 is a subtype of EURO1, which is a subtype of EURO0.

class Inspector {
    Report Inspect(EURO0 *c){...}
    Report Inspect(EURO1 *c){...}
}

class Inspector_2006: Inspector {
    Report Inspect(EURO0 *c){...} // copied down from class Inspector
    Report Inspect(EURO1 *c){...} // copied down from class Inspector
    Report Inspect(EURO2 *c){...}
}

class Inspector_2007: Inspector_2006 {
    Report Inspect(EURO0 *c){...}
    Report Inspect(EURO1 *c){...}
    Report Inspect(EURO2 *c){...} // copied down from class Inspector_2006
}

Listing 2: The gas emission example with copy semantics

ing our proposal, the solutions presented in [MC02,CLCM00,CL95] can be exploited to obtain a type safe composition of DOCS modules.

2 Example

The integration of dynamic overloading in a language increases the complexity of ambiguities resolution during method selection since the set of applicable methods becomes larger when considering also the dynamic type of the parameters. Since type safety is a primary goal for us, the risk is that of adopting a resolution policy that is too strict. To show the advantages of copy semantics we use the example in Listing 1. The class Inspector represents inspectors checking cars gas emission according to European Commission’s standards. Cars are classified according to their gas emission in different categories (EURO0, EURO1, EURO2), so the method Inspect is defined on different car types and returns a Report object including information about the inspection. Now let us suppose that, at the time when class Inspector was designed, the available categories where EURO0 and EURO1. In the year 2006 the category EURO2 is added so asubclass
program ::= classdef * body

classdef ::= class A : A_h, k ∈ H { 
B_i f_i: j ∈ J
branchdef[j]: j ∈ J 
}

branchdef ::= m branches 
B'_k (B_k x_k) {body}_k ; k ∈ K

end

body ::= localdecl; stmt; return exp

localdecl ::= A_1 x_1 = exp_1; ...; A_n x_n = exp_n

Table 1. Syntax of DOCS: classes, methods and programs.

Inspector_2006 is defined to deal with these new rules. Finally, in the year 2007 the rules to evaluate older vehicles (EURO0 and EURO1) become stricter so we redefine in a new class Inspector_2007 the Inspect method for parameter of type EURO0 and EURO1; instead the rules for EURO2 are still valid so we do not need to redefine the branch for EURO2 in the class Inspector_2007 (we simply inherit it).

Let us consider the semantics of the call Insp.Inspect(car), when Insp and car have dynamic types Inspector_2007 and EURO2, respectively.

Adopting symmetric dispatch (the receiver and the parameter participate together in method selection), the above call should be considered ambiguous. Indeed the version of Inspect defined in class Inspector_2006 is the most specific w.r.t. the argument type, while both versions defined in Inspector_2007 are more specific w.r.t. the receiver type. Should we detect the ambiguity rejecting the definition of method Inspect or reject ambiguous method calls? In both cases the code would be rejected because unsafe resulting in a too restrictive policy.

A second alternative is to choose asymmetric dispatch. In this case the receiver has priority in method selection, so the body to execute must be chosen among the versions defined in Inspector_2007. This way, we partially lose the flexibility of dynamic dispatch, since the version for EURO2 is not considered.

Instead, let us consider an interpretation based on copy semantics: all the method versions defined in the superclass are indented to be copied into the subclass (Listing 2). Thus, the body of Inspect, with parameter EURO2 copied in Inspector_2007, is selected as the most specialized version for both the receiver and the argument.

In summary by the use of copy semantics of inheritance we obtain a symmetric dispatch semantics with encapsulated multi-methods without renouncing static type safety and programming flexibility.

3 The core language DOCS

DOCS is proposed as a contender for a minimal core calculus, including basic imperative features of standard object-oriented languages such as C++ and Java, together with more advanced features like encapsulated multi-methods and copy semantics of inheritance.

The syntax of DOCS is defined in Table 1 and 2 starting from

- a set ClassNames of class names denoted by A, B, C, (A_i, B_i, C_i)
- a set Fields of names for record fields denoted by f
- a set Identifiers of identifiers including the set Var of standard variables denoted by x, y, and the set MethNames of method names denoted by m, n, m_i, n_i. We use ℓ to denote any identifier x or m. We denote with MethNames(p) the set of names of the methods defined in a program p.
\[ \text{exp ::= x} \]
\[ \text{ | this} \]
\[ \text{ | this.f} \]
\[ \text{ | methinvok} \]
\[ \text{ | new A(exp_1, \ldots, exp_n)} \]

\[ \text{stmt ::= methinvok} \]
\[ \text{ | left = exp} \]
\[ \text{ | stmt_1; stmt_2} \]

\[ \text{left ::= x} \]
\[ \text{ | this.f} \]

\[ \text{methinvok ::= receiver \leftarrow m(exp')} \]
\[ \text{ | receiver \leftarrow m(exp')} \]

\[ \text{receiver ::= exp} \]
\[ \text{ | super(A)} \]

**Table 2. Syntax of DOCS: expressions and statements**

**Notation.** Let \( \text{program} = \text{classdef}^* \text{ body} \) then \( \text{MethNames(classdef}^* \text{)} \) will denote \( \text{MethNames(program)} \).

With respect to the object-oriented core of standard mainstream languages, we adopt the following main simplifications, concerning features that are no relevant for our purpose:

- all methods accept only one parameter;
- we do not consider field access since is an orthogonal feature w.r.t. the problem a issue; thus class fields are all private, and field selection can be performed only on \textit{this}; let us note that the construct \textit{this.f} allow us to model mutable objects;
- in order to simplify the presentation of typing, the programmer of the subclass is required to repeat all the instance variables of the superclass, as suggested in [Cas97];

In Table 1 the structure of a program is defined as

\[ \text{classdef}^* \text{ body} \]

where \textit{classdef}^* is a sequence (possibly empty) of class definitions. Each class definition can refer to any other class, including its sub-classes, in defining its fields and methods. Class definitions are followed by a body that plays the same role of \textit{main} in C++ and Java. Let us note that in class definitions, the set of superclasses \( A_h \in H \) can be empty.

Since our core language is essentially imperative, we want to treat assignments and side-effects, thus we need to deal with references. In particular, all class fields and method local variables are considered as updatable memory cells (i.e., all variables are to be considered as Java or C++ references). As in Java, we do not want to specify this behavior in the program: instead of declaring a variable as \textit{ref T x} we simply write \( T \ x \) with the same meaning. Accordingly, the assignment between variables \( x = y \) has to be intended as \( x = \uparrow y \), where \( \uparrow y \) is the value referred to by \( y \). The distinction between a reference or location and the value stored in that location is hidden to the programmer, while it will be explicit in formal specifications of typing and semantics. This makes it significantly easier to write type-checking rules and translational semantics.

A \textit{multi-method} is as a collection of overloaded methods associated to the same message (method name). We will refer to a single overloaded method of a multi-method \( m \) as a \textit{branch} of \( m \). Class (overloaded) methods are written according to the \textit{branchdef} rule.

**Notation.** If \( b = m_j \text{ branches } B'_{k_j} \{ B_{k_j} x_{k_j} \} \{ \text{body}_{k_j} \} ; k_j \in K_j \text{ end} \) then we use the notation \( \text{name}(b) = m_j \).
We allow method bodies to call the implementation of a method in a super-class with the construct `super(A)`, where `A` is a super-class of the current class method. If we considered only single inheritance, we could simply use `super()`.

Concerning method invocation, dynamic binding is employed, in any case, but when `super(A)` is explicitly used, thus always selecting the most redefined implementation. In particular, all branches of a multi-method declared in a superclass are intended to be implicitly inherited by derived classes, thus implementing a full form of copy semantics of inheritance [ADZ01]. Note that in our syntax we only consider multi-methods: standard methods are multi-methods with only one branch. We distinguish two different linguistic constructs for method invocation, denoted by ← and ⇐ that will be associated to different mechanisms for selecting the right branch of the method in DOCS semantics:

- `receiver ← m(exp)` is used for the standard static overloaded method invocation, i.e., the branch of the multi-method is selected statically according to the static type of the parameter (static overloading), and dynamically according to the run time type of the receiver (single dispatch);
- `receiver ⇐ m(exp)` is used for dynamic overloading method invocation, where the branch of the multi-method is selected dynamically according both to the run time type of the receiver and to the run time type of the parameter (double dispatch);

Note that the `receiver` of a method invocation can be either an expression `exp` or `super(A)` where `A ∈ ClassNames`.

## 4 Typing

The typing system is straightforward as far as basic object-oriented features are concerned. Our focus is on rules for typing multi-methods, class definitions and then programs. Indeed our primary goal is to ensure that neither “method not understood” nor “method ambiguous” errors can occur in multi-methods dispatch. The notion of multi-type to be associated to multi-methods and its well formedness are widely inspired by [Cas95,Cas97]. However, the adoption of copy semantics of inheritance makes our rules different from [Cas95,Cas97] in some crucial points (for instance the multi-type union constructor, Definition 8) leading to a totally different typing of a program as a whole. As a consequence, many static ambiguities that could be raised using the rules of [Cas95,Cas97] are automatically resolved in DOCS.

Following the approach of Featherweight Java [JPW01], we build a class table `CT(p)` that contains type information for all the classes in a program `p`. This table is crucial to type checking multi-method declarations with branches whose parameter types are associated to classes that have not been defined yet: indeed, a class `B` can use the name `A` and vice versa without any issue about which class is defined first. This is a general feature of mainstream languages, such as Java, that is modeled in DOCS. Then we first generate the class table `CT(p)` from class definitions, which associates to each class name both the type representing its fields and its superclass relations. Using `CT(p)` the declarative part is type checked in order to produce the type environment that is needed to type the rest of the program.

The section is organized as follows:

- in Section 4.1 and in Section 4.2 we define the syntax of types and we specify the subtyping relation respectively;
- in Section 4.3 we formalize the notion of well formed types;
- in Section 4.4 we define typing rules for DOCS programs. The typing rules presented in this section are parameterized w.r.t. a type environment, which is a triple `<C,S,Γ>`;
- in Section 4.5 we finally formalize well typedness for DOCS programs: we first define how to generate the triple `<C_p,S_p,Γ_p>`, from any program `p`, then we use `<C_p,S_p,Γ_p>` for type checking the rest of the program (method bodies and the main body), according to the rules of Section 4.4.
\[
A ::= \text{ClassNames} \quad \text{(atomic types)}
\]
\[
I ::= (A \times A) \quad \text{(input types)}
\]
\[
R ::= \langle \langle f_1 : \text{ref} A_1; \ldots; f_k : \text{ref} A_k \rangle \rangle \quad \text{(record types)}
\]
\[
T ::= A | I | T \rightarrow T | \text{ref} A | \text{unit} \quad \{I_1 \rightarrow T_1, \ldots, I_n \rightarrow T_n\} \quad \text{(Types)}
\]

Table 3. Syntax of types

4.1 Syntax

The syntax of types is defined in Table 3. Atomic types are class names. It is straightforward to include built-in types as atomic types so, when convenient, we will use atomic types such as boolean, real, integers etc. We denote by \textbf{AtomicTypes} the set of atomic types. Input types are used to represent types of the input in arrow types, namely input types for methods in our case. Record types are used to represent the types of the instance variables of objects. Let us consider the following class definition:

\[
\text{class } A : A_1, \ldots, A_n \{ \quad \text{branchdef}_j; \ j \in J \quad \text{if } j \in H \quad \text{ref}_j; \ h \in H \}
\]

then the record type associated to objects of class \( A \) is \( \langle \langle f_1 : \text{ref} B_1; \ldots; f_k : \text{ref} B_k \rangle \rangle \) where \( H = \{1, \ldots, k\} \).

\( U, U_i, T, T_i \) will denote types of our system, thus including:

- atomic types
- arrow types
- product types
- reference types (\text{ref} \( A \))
- \text{unit} (denoting the type of assignments)
- multi-types (\{\( I_1 \rightarrow T_1, \ldots, I_n \rightarrow T_n \})

\textit{Multi-types} are sets of arrow types representing branches of multi-methods. A multi-type \( \Sigma \) is of the form

\[
\Sigma = \{I_1 \rightarrow T_1, \ldots, I_n \rightarrow T_n\}
\]

where each input type \( I_j \) is a pair type, \((A \times B)\).

Reference types are used to represent updatable variables. In order to take into account that any variable \( x \) of type \text{ref} \( A \) denotes a location which can store a value of type \( A \), we introduce the following type operation on \( T, \tilde{T} \), in order to distinguish between the type of \( x \) and the type of the value stored in that location.

**Definition 1 (ref destructor).**

\[
\tilde{T} = \begin{cases} T & \text{if } T \equiv \text{ref} \ A \\ A & \text{otherwise} \end{cases}
\]
4.2 Subtyping.

Now we define the notion of subtyping \(\leq\) on types. The subtyping relation is assumed to be given on atomic types in a type constraint environment. Then we define rules to extend subtyping to all types.

**Definition 2 (Type constraint environment \(C\)).** A type constraint environment \(C\) is the definition of an order relation on atomic types, such that:

1. \(\forall A \in \text{AtomicTypes} (A, A) \in C\)
2. \((A, B) \in C\) and \((B, A) \in C \Rightarrow A = B\)
3. \((A, B) \in C\) and \((B, C) \in C \Rightarrow (A, C) \in C\)

**Definition 3 (Rules for subtyping relation \(\leq\)).**

\[
C \vdash A \leq B \quad C \vdash T \leq T \quad C \vdash T_1 \leq T_2 \quad C \vdash T_2 \leq T_3 \quad C \vdash A \leq A_1 \quad C \vdash B \leq B_1
\]

for \((A, B) \in C\)

\[
C \vdash \langle \{f_1 : \text{ref} A_1; \ldots; f_k : \text{ref} A_k; \ldots; f_{k+j} : \text{ref} A_{k+j}\} \rangle \leq \langle \{f_1 : \text{ref} A_1; \ldots; f_k : \text{ref} A_k\} \rangle
\]

\[
C \vdash T \leq T_1 \quad C \vdash U \leq U_1 \quad C \vdash T_1 \rightarrow U \leq T_2 \rightarrow U_1
\]

\[
\forall k \in K, \exists j \in J \text{ such that } C \vdash I_k \leq I_j \text{ and } C \vdash T_k \equiv T_j
\]

We will write \(C \vdash A \leq B\) if \(C \vdash A \leq B\) can be proved by using rules of the above Definition, by omitting \(C\) when it is clear from the context. Let us observe that subtyping on atomic types is an order relation; instead, subtyping on types is a preorder, only for the case of multi-types. Namely, given two multi-types \(\Sigma_1\) and \(\Sigma_2\), \(\Sigma_1 \leq \Sigma_2\) if and only if for every arrow type in \(\Sigma_2\) there is at least one arrow type with greater input type and equal return type in \(\Sigma_1\). Now, if \(A' \leq A\) then \(\{A \rightarrow T\} \leq \{A' \rightarrow T\}\) and \(\{A \rightarrow T, A' \rightarrow T\} \leq \{A \rightarrow T\}\), which does not imply \(\{A \rightarrow T, A' \rightarrow T\} = \{A \rightarrow T\}\): see [Cas97], page 117, for details on this subject. In our language, since we do not have higher order functions, this is not a big issue: our input types consist of pairs of atomic types (Table 3), for which the subtyping is an order.

Thus \(C\) is intended as a set of assumptions on atomic types and it will be used to record subtyping relations on them. The subtyping relation induced by \(C\) on atomic types is assumed to be acyclic.

4.3 Well formed types

The notion of well formedness, formally stated in Definition 5, introduces a suitable restriction on multi-types, depending on a subtyping relation on atomic types. From now on we will call \(\text{pretypes}\) the types that are (possibly) not well formed, while \(\text{Types}\) will denote the set of well formed types and the membership to \(\text{Types}\) is indexed by the type constraint system \(C\) (\(\in C\)) on which well formedness relies.

We denote by \(\text{RecordTypes}\) the set of record types whose fields are typed by well formed types.

**Definition 4 (Maximal types).** Let \(G\) be a set of input types such that \(G \subseteq \text{Types}\) and \(C\) be a type constraint environment. The set \(\text{Top}_C(G)\) of maximal types of \(G\) with respect to \(C\) is so defined:

\[
\text{Top}_C(G) = \{I \in G \mid \forall I' \in G \text{ s.t. } I' \neq I : C \vdash I \nsubseteq I'\}
\]

In the following definition, \(\text{LB}_C(I_j, I_i)\) denotes the set of common lower bounds of input types \(I_j\) and \(I_i\).
(A_1 \times B_3) \leq (A_2 \times B_3) \leq (A_2 \times B_2)

(A_3 \times B_3) \leq (A_3 \times B_2) \leq (A_2 \times B_2)

Fig. 1. Subtyping relations between input types

Definition 5 (Well formed types).

(i) \( A \in C \) Types

unit \( \in C \) Types for any type constraint system \( C \)

(ii) if \( A, B, T_1, T_2 \in C \) Types then \( T_1 \rightarrow T_2 \in C \) Types, \( (A \times B) \in C \) Types and ref \( A \in C \) Types

(iii) if for all \( j, i \in K, K = \{1, \ldots, n\} \)

(a) \( I_{j(i)}, I_{j(i)} \in C \) Types

(b) if \( i \neq j \) then \( I_{i} \neq I_{j} \)

(c) if \( C \vdash I_{i} \leq I_{j} \) then \( T_{j} \equiv T_{i} \)

(d) for all maximal types \( I' \) in \( LB_C(I_j, I_l) \) (i.e. for all \( I' \in \text{Top}_C(LB_C(I_j, I_l)) \) there exists \( h \in K \) such that

\( I_{h} = I' \)

then \( \{I_{k} \rightarrow T_{k}\}_{k \in K} \in C \) Types.

Then atomic types are well formed types (point (i)) and also arrow and product types whose internal types are well formed (point (ii)).

Multi-types (point (iii)) are constrained by the crucial consistency conditions of the above definition, that are checked statically. Condition (b) is quite standard on overloaded definitions also in C++ and Java\(^1\). Condition (c) guarantees that a branch specialization maintains the same return type. Condition (d) is the most crucial one: it implies that for any type \( I \), such that \( I \leq I_{j} \) and \( I \leq I_{l} \), there must be one input type in \( \{I_{k} \rightarrow T_{k}\}_{k \in K} \), say \( I_{h} \), such that \( I_{h} \leq I_{l} \), \( I_{h} \leq I_{l} \) and \( I_{h} \leq I_{j} \). Informally speaking, let us consider the following type constraint system:

\[ C = \{A_2 \leq A_1, B_2 \leq B_1, A_3 \leq A_2, B_3 \leq B_2\} \]

and two branches in a multi-type \( \Sigma \) whose input types are \( I = (A_1 \times B_2) \) and \( I' = (A_2 \times B_1) \). We first build the set of common lower bounds of \( I \) and \( I' \) w.r.t. the class hierarchy represented by \( C \):

\[ LB_C(I, I') = \{(A_2 \times B_2), (A_2 \times B_3), (A_3 \times B_2), (A_3 \times B_3)\} \]

Then we build the set of maximal types of this set, that is, any maximal type of a chain of lower bounds of \( I, I' \) (see Figure 1):

\[ \text{Top}_C(LB_C(I, I')) = \{(A_2 \times B_2)\} \]

To satisfy condition (iii), \( (A_2 \times B_2) \) has to belong to \( \Sigma \). This last condition will play a crucial role in catching at compile time any possible static and dynamic ambiguity in multi-method calls, since it ensures that for every potentially ambiguous pair of (receiver type \times parameter type) there is always an input type solving the ambiguity (in the above example, it is \( A_2 \times B_2 \)). Its meaning will become clear when discussing the typing of method invocation.

\(^1\) For simplicity, we adopt the restriction of requiring the return types to be equal, thus concentrating our attention on parameters types which play the crucial role in dynamic method selection. We note that, in our approach, no technical difficulty would arise if the above definition of well formedness was extended to covariance of return types, as in [Cas95,Cas97]. In most programming languages return types are not used in overloading resolution; in Java, for instance, \( T_{i} \) and \( T_{j} \) can be completely unrelated and this is sound because overloading resolution is static (namely, resolution of static overloading and covariance of return types are two unrelated features in Java and C++).
4.4 Typing DOCS constructs

In this section we define a type system for assigning types to expressions, method bodies and the main body of a program in a given type environment consisting in the triple \( \langle C, S, \Gamma \rangle \) where:

- \( C \) is a type-constraint environment (see Definition 2)
- \( S \) is an environment recording the internal representation of classes; namely, a set \( \{ A_1 : R_1, \ldots, A_n : R_n \} \) where \( A_i \)'s are class names and \( R_i \)'s are record types representing the types of \( A_i \)'s fields
- \( \Gamma \) is a type environment associating types to identifiers (this, variables and multi-method names)

Record environment \( S \). A record environment \( S \) is a finite set (possibly empty) \( \{ A_1 : R_1, \ldots, A_n : R_n \} \) where \( R_1, \ldots, R_n \) are record types of the shape \( \langle \langle f_1 : \text{ref} \ B_1; \ldots ; f_h : \text{ref} \ B_h \rangle \rangle \). \( A_1, \ldots, A_n \) are the subjects of \( S \), as for the type environments \( C \) and \( \Gamma \). All subjects of \( S \) are pairwise disjoint and \( \text{Dom}(S) = \{ A | A : R \in S \} \). \( S \) associates to each atomic type the representation of the objects of the corresponding class.

For instance, given the following class definition:

\[
\text{class } A : A_1, \ldots, A_n \{
    B_i f_i; \quad \text{for } i \in I
    \text{branchdef } j; \quad \text{for } j \in J
\}
\]

then a record environment \( S \) can be updated for recording the representation of \( A \) in the following way:

\[
S \cup \{ A : \langle \langle f_1 : \text{ref} \ B_1; \ldots ; f_k : \text{ref} \ B_k \rangle \rangle \}
\]

provided that \( A \notin \text{Dom}(S) \). We write \( S(A) = R \) to denote that \( A : R \in S \).

Type environment \( \Gamma \). The static environment \( \Gamma \) is a finite set (possibly empty) \( \{ \ell_1 : T_1, \ldots, \ell_n : T_n \} \) where:

- \( \ell_1, \ldots, \ell_n \) are called the subjects of \( \Gamma \)
- we denote by \( \text{Dom}(\Gamma) = \{ \ell | \ell : T \in \Gamma \} \) the domain of \( \Gamma \)
- \( \ell_i \neq \ell_j \) for each \( \ell_i, \ell_j \in \text{Dom}(\Gamma) \) (\( i \neq j \))

Then, if \( \ell : T \in \Gamma \) we write \( \Gamma(\ell) = T \). Let us note that, according to DOCS syntax, identifiers \( \ell_i \) can only be:

- variables i.e. \( x : T \)
- the special identifier \( \text{this} \), then \( \Gamma(\text{this}) = A \) for some class name \( A \)
- method names, then \( m : \Sigma \) implies that \( \Sigma \) is a multi-type; informally, \( \Sigma \) records the type of the branches of each multi-method in the form \( (A \times B) \rightarrow T \), where \( A \) is the type of the class where the branch has been defined and \( B \) is the type of the argument of the branch.

In the following we define the notion of consistency for the triple \( \langle C, S, \Gamma \rangle \).

**Definition 6** \( \langle C, S, \Gamma \rangle \) \text{ consistency}. The triple \( \langle C, S, \Gamma \rangle \) is a consistent environment if and only if:

1. \( C \) is consistent with \( S \), that is if \( C \vdash A \leq B \) then \( C \vdash S(A) \leq S(B) \).
2. \( \Gamma \) is consistent with \( C \) and \( S \)
   - if \( \text{exp} : \text{ref} \ A \in \Gamma \) or \( \text{exp} : A \in \Gamma \) then \( S(A) = R \) for some \( R \)
   - if \( m : \Sigma \in \Gamma \) then \( \Sigma \in C \text{ Types} \) (that is \( \Sigma \) is well formed w.r.t. the subtyping relations of \( C \))

Notice that point (1) implies that all fields of the superclass \( A \) are repeated in the subclass \( B \).

Given a consistent environment \( \langle C, S, \Gamma \rangle \), \( \langle C, S, \Gamma' \{ \ell \leftarrow T' \} \rangle \) will denote the consistent environment \( \langle C, S, \Gamma' \rangle \) where \( \Gamma' = \Gamma \setminus \{ \ell : T \} \cup \{ \ell : T' \} \). Typing rules use formulas of the shape \( C, S, \Gamma \vdash t : T \), where \( t \) is a DOCS term (i.e., a program, a body, an expression, a statement or a class definition), \( T \) is a well formed type w.r.t. \( C \) and the triple \( \langle C, S, \Gamma \rangle \) is assumed to be consistent.
Table 4. Typing rules: expressions, statements and bodies
is updated by adding reference types of variables and parameters and the type of any possible input type \( \Gamma \) branch exists it can be selected without ambiguities.

\[ \forall k \in K_j, j \in J \\
C.S.\Gamma \vdash \text{ref } B_k | \text{this } \vdash \{ \text{body}_k \} : U_k \\
C \vdash U_k \leq B'_k \]

\[ C.S.\Gamma \vdash \text{p } : T \]

Table 5. Typing rule for programs

Typing rules. Typing rules, parameterized on \( <C, S, \Gamma> \), are presented in Tables 4 and 5. Let us observe that the environment \( \Gamma \) is never updated but in the case of rule [BODY] and [PROGRAM-CLASS]: the context \( \Gamma \) is updated by adding reference types of variables and parameters and the type of this, in order to check that the method body is well typed.

Multi-method invocation. In [DOVMETHCALL] and [SOVMETHCALL] rules, we search for the most appropriate (specialized) branch for the invocation assuming that \( \Gamma \) associates to \( m \) the corresponding well formed multi-type. Note that, thanks to the definition of well-formed type (predicate \( \in_C \text{Types} \)), if such a branch exists it can be selected without ambiguities.

Let us discuss this in further details. If a multi-method invocation is well typed, with type \( \Sigma \), then for any possible input type \( I = (A \times B) \) the set \( IT_{(A \times B)} \) of invocable branches input types

\[ IT_{(A \times B)} = \{(A_i \times B_i) \mid (A \times B) \leq (A_i \times B_i)\} \]

selected from \( \Sigma \), is not empty. This means that there will always exist a possible choice of a branch to call for all actual choices of static types \( (A \times B) \) and dynamic subtypes of \( (A \times B) \). This ensures that in a well typed program no message-ambiguous error will take place.

Moreover, since \( \Sigma \) is well-formed, the above set \( IT_{(A \times B)} \) contains a minimum input type, say \( I_k = (A_k \times B_k) \), i.e., \( (A_k \times B_k) \leq (A_j \times B_j) \) for all \( (A_j \times B_j) \in IT_{(A \times B)} \), by condition (iiid) (in Definition 5) of well-formedness. The branch of type \( I_k \rightarrow T_k \) is the only one that “best approximates” the input type \( I = (A \times B) \). This means that there is one and only one most specific applicable branch for any possible choice of \( I \), i.e., in a well typed program no message-ambiguous error will take place during the execution.

Let us stress that the above argument motivating the absence of message-ambiguous holds not only for any static input type \( I \), but also for any dynamic input subtype \( I^* \leq I \). In this case the set of input types of matching branches, \( IT^* \), could become larger (\( IT^* \subseteq IT_{(A \times B)} \)), and so the best approximating branch to be selected dynamically (minimum input type) could have a more specialized input type. The existence and the uniqueness of such branch are still ensured by condition (iiid) of well-formedness, as explained above.

Summarizing, the static well typedness property guarantees that, for each possible choice of dynamic input type:

1. the static return type is unique and preserved during evaluation.
2. there will always be one and only one most specialized branch to be selected.

Formally, this property will be proved in Section 7 by providing a translational semantics into \( \lambda, \text{object} \) and then by lifting the type safety of \( \lambda, \text{object} \) to DOCS.

Typing programs. Rule [PROGRAM-CLASS] (Table 5) shows how the typing algorithm proceeds in the case of a program, given the type environment \( <C, S, \Gamma> \). This rule checks well typedness for multi-method definitions, namely that type of each branch definition of \( m \) is consistent with the well formed multi-type
that is associated to \( m \) in \( \Gamma \). The body is type checked (rule [\textsc{Body}], Table 4) in the environment \( \Gamma' \) updated with the types of the parameter and of \textit{this}. Instead, the correctness of inheritance w.r.t. fields (namely that all the fields of the superclasses are repeated in the class definition), is assured by the consistency condition of the triple \( < C, S, \Gamma > \) (see definition 6).

We conclude this section with a basic property that characterizes the expressions of \textit{DOCS}, in particular their types.

\textbf{Property 1.} For any expression \( \text{exp} \) and body \( \text{body} \),

1. if \( C; S; \Gamma \vdash \text{exp} : T \), then \( T \equiv \text{A} \) or \( T \equiv \text{ref} \ A \) for some class name \( A \).
2. if \( C; S; \Gamma \vdash \{ \text{body} \} : T \), then \( T \equiv \text{A} \) for some class name \( A \).

\textbf{Proof.} 1. Straightforward by rules [\textsc{Taut}], [\textsc{New}], [\textsc{Read}], [\textsc{DovMethCall}], [\textsc{SovMethCall}].

2. By rule [\textsc{Body}] and point 1.

4.5 Well typedness of \textit{DOCS} programs

Well typedness of \textit{DOCS} programs is expressed by the formula \( \triangleright\triangleright p : T \) (read as "\( p \) has type \( T \")) where \( p \) is a program and \( T \) is an atomic type (i.e., \( T \) is well formed w.r.t. any \( C \)).

The statement \( \triangleright\triangleright p : T \) is formalized in Definition 12 after the definition of the class table \( CT(p) \) and the type environment \( \Gamma_p \) that are associated to the program \( p \).

We first explain the use of \( CT(p) \) in checking the well typedness of \textit{DOCS} programs. In \textit{DOCS} a method \( m \) in a class \( A \) can have a parameter of type \( B \), where class \( B \) is defined after the declaration of \( A \); the same holds for types of fields. This reflects the style of Featherweight Java: we view the set of class names as being given from the beginning, so that there is no issue about which class is defined first. Thus we have to collect the type information concerning all class definitions in a program \( p \), before checking each class. Given a \textit{DOCS} program \( p \), \( CT(p) \) records, for each class \( A \) defined in \( p \):

- the record type representing its fields
- the subtyping relations (on atomic types) induced by the inheritance hierarchy
- the method definitions of the branches defined in \( A \)

The third part of the table, recording the method definitions associated to each class, will be used only to define \textit{DOCS} semantics (Section 6).

\textbf{Definition 7 (Class table \( CT \)).}

\textit{Let} \( p = \text{classdef}^+ \text{ body} \text{ be a DOCS program, then}

1. for any class definition in \( \text{classdef}^+ \text{ of the shape}

\[
\text{class } A : A_1, \ldots, A_n \{ \\
\quad B_i f_i; \ (i \in I) \\
\quad m_j \text{ branches} \\
\quad \quad B'_k (B_k x_k) \{ \text{body}_k \}; \ (k \in K_j) \\
\quad \text{end} \}_{j \in J} \\
\}
\]

\textit{we define:}

- \( C_p(A) = \langle \langle f_i : \text{ref} B_i \ i \in I \rangle \rangle \)
- \( S_p(A) = \{ A \leq A_1, \ldots, A \leq A_n \} \)
- \( BT_p(A, m_j, B_k) = \{ \text{body}_k \} \)
2. \( CT(p) \) is the class table built from \( \text{classdef}^* \) in the following way:

\[
CT(p) = \langle C_p, S_p, BT_p \rangle
\]

We assume that \( CT(p) \) satisfies some sanity conditions:

- any class name \( A \) is defined only once
- if \( A_1 \leq A_j \in S_p \) then \( C_p(A_1) \leq C_p(A_j) \), namely the subclass relation is consistent with subtyping on the corresponding record types
- there are no cycles in the subclass relations recorded in \( CT(p) \), that is if \( A \leq B \in S_p \) then \( B \) cannot be a subclass of \( A \).

Similarly to \( S_p, C_p \) and \( BT_p \), we also need to generate the type environment \( \Gamma_p \) which associates to each multi-method \( m \) in \( p \) its multi-type \( \Sigma \). For example, let us consider a program with the following class definitions:

\[
\begin{align*}
\text{class } A & \{ \\
\text{m branches} & \{ \\
T & (D x)\{\text{body}_1\}; \\
\text{end} & \}
\}
\end{align*}
\]

\[
\begin{align*}
\text{class } B & \{ \\
\text{m branches} & \{ \\
T & (D x)\{\text{body}_2\}; \\
\text{end} & \}
\}
\end{align*}
\]

\[
\begin{align*}
\text{class } C : A, B & \{ \\
\text{m branches} & \{ \\
T & (D x)\{\text{body}_3\}; \\
\text{end} & \}
\}
\end{align*}
\]

Then \( C_p = \{ C \leq A, C \leq B \} \). The multi-type associated to \( m \) in class \( B \), \( \{(A \times D) \rightarrow T, (B \times D) \rightarrow T\} \), is not well formed w.r.t. \( C_p \) since it does not satisfy condition (d) in Definition 5. The problem is due to the fact that, when we check the branch defined in class \( B \), we have not already encountered class \( C \) which defines the disambiguating branch while \( C_p \) already includes the relations \( C \leq A \) and \( C \leq B \).

Thus we have to generate the environment \( \Gamma_p \) in a preliminary scan of \( p \), using the function \( \text{MT}(\text{classdef}^*) \) which is a finite set of associations of the form \( \{m_1 : \Sigma_1, \ldots, m_n : \Sigma_n\} \) where the subjects \( m_i \)'s are method names belonging to \( \text{classdef}^* \) and \( \Sigma_i \)'s are multi-types possibly not well formed (pretypes). If \( m : \Sigma \) belongs to \( \text{MT}(\text{classdef}^*) \) then \( \text{MT}(\text{classdef}^*)(m) = \Sigma \). Since each method name \( m \) can be the subject of at most one association, we will write

\[
\text{MT}(\text{classdef}^*) \cup \{m_i : \Sigma'_i\}
\]

to denote

\[
(\text{MT}(\text{classdef}^*) \setminus \{m_i : \Sigma_i\}) \cup \{m_i : \Sigma'_i\}
\]

when updating \( \text{MT} \).

We introduce two operators on multi-types that will be used for the construction of \( \text{MT} \):

- \( \cup \) merges two multi-types performing copy semantics of inheritance at the typing level
- \( \downarrow \) returns the branch types defined in a given class

**Definition 8 (Multi-method type union \( \cup \)).** Given two multi-types \( \Sigma_1 \) and \( \Sigma_2 \) and a type constraint system \( C \), the new multi-type \( \Sigma_1 \cup_C \Sigma_2 \) is defined as follows:

\[
\Sigma_1 \cup_C \Sigma_2 = \Sigma_1 \cup \Sigma_2 \cup \{(A \times D) \rightarrow T \mid (A_i \times D) \rightarrow T \in \Sigma_1 \land C \vdash A \leq A_i \}
\]

Informally speaking the operator \( \cup \) copies each arrow type \( D \rightarrow T \) defined in a superclass \( A_i \) into the subclass \( A \) (thus changing the receiver type) since every branch not redefined in \( A \) is considered to be explicitly inherited.
Definition 9 (Restriction ↓). If \( \Sigma \) is a multi-type and \( A \) a class name, then \( \Sigma \downarrow A \) selects from a multi-type \( \Sigma \) the branch types where the type of the receiver is \( A \):

\[
\Sigma \downarrow A = \{ B \to T \mid (A \times B) \to T \in \Sigma \}
\]

Definition 10 (MT).

Let \( \text{classdef}^* = \text{classdef}_1, \ldots, \text{classdef}_n \) be a set of class definitions then we define \( \text{MT}(\text{classdef}^*) \) by cases on the cardinality of \( \text{classdef}^* \) as in the following:

1. \( \text{MT}(\emptyset) = \emptyset \)
2. \( \text{MT}(\text{classdef}_1, \ldots, \text{classdef}_n) = \text{MT}(\text{classdef}_1, \ldots, \text{classdef}_{n-1}) \cup \{ m_j : \Sigma_j \uplus \{ (A \leq A_k) \leftharpoonup \{ (A \times B_k) \to T_k \}^{k \in K_j} \} \mid j \in J \}

if \( \text{classdef}_n = \text{class} A : A_h \text{ branchdef}_j : j \in J \), and

\[
\text{branchdef}_j = m_j \text{ branches } T_{k_j} (B_{k_j}, x_{k_j}) \{ \text{body}_{k_j} \}; k_j \in K_j \end{branchdef}
\]

where

\[
\Sigma_j = \begin{cases} \text{MT}(\text{classdef}_1, \ldots, \text{classdef}_{n-1})(m_j) & \text{if } m_j \in \operatorname{MethNames}(\text{classdef}_1, \ldots, \text{classdef}_{n-1}) \\ \emptyset & \text{otherwise} \end{cases}
\]

provided that,

\[
\forall j \in J \text{ and } l, l' \in \text{H}, \Sigma_j \downarrow A_l \cap \Sigma_j \downarrow A_{l'} \subseteq \{ B_{k_j} \to T_{k_j} \}^{k_j \in K_j}
\]

Thus, at each recursive step, for each multi-method \( m_j \) defined in the current class, the type \( \Sigma_j \) of the multi-method class is updated as in the following (let us note that \( \Sigma_j = \emptyset \) if \( m_j \) has not already been encountered):

\[
\Sigma_j \uplus \{ (A \leq A_k) \leftharpoonup \{ (A \times B_k) \to T_k \}^{k_j \in K_j} \}
\]

where:

- all the arrow types of the branches defined in the current class are collected in the multi-type \( \{ (A \times B_k) \to T_k \}^{k_j \in K_j} \)
- the union between the two multi-types is performed using the operator \( \uplus \)

By using the operator \( \uplus \) all the branches of a superclass are implicitly inherited by derived classes, apart from those redefined by the derived class itself. For instance, if the multi-method \( m \) has type \( \Sigma_1 = \{ (A_1 \times B_1) \to T \} \) in the base class \( A_1 \) and type \( \Sigma_2 = \{ (A_2 \times B_2) \to T \} \) in the derived class \( A_2 \), then it will be given the type \( \Sigma_1 \uplus (A_2 \leq A_1) \Sigma_2 = \{ (A_1 \times B_1) \to T, (A_2 \times B_1) \to T, (A_2 \times B_2) \to T \} \). This corresponds to the intuition that branches that are not redefined in the subclass are intended to be inherited. In the context of copy semantics it means that the branch code that is inherited is copied down in the subclass: from the typing view this branch is assigned the new type where the input type is updated replacing the class where the branch has been defined with the current class.

Due to multiple inheritance, we have to check that two superclasses do not define the same method branch with the same signatures, or, in case they do, we must ensure that the derived class provides a declaration for such branch, in order to avoid ambiguities. Note that our policy is to avoid a silent resolution of such ambiguities (as, e.g., in [Sha97]) and to force the programmer to deal with them.

For instance, if \( m \) has type \( (A \times D) \to T \) in class \( A \) and type \( (B \times D) \to T \) in class \( B \) and class \( C \) inherits both from \( A \) and \( B \), then we must check that the branch \( D \to T \) is redefined in \( C \) in order to univocally associate a body to the branch of \( m \) with type \( (C \times D) \to T \). This check relies on the operators of restriction (\( \downarrow \)) and intersection (\( \cap \)). The two operators are needed to collect the set of common branches definitions for a multi-method \( m \) into two different classes. Indeed, to catch ambiguities due to multiple inheritance for each pair of superclasses \( A_I, A_{I'} \) we perform the following checks:
1. we select the branches defined in the two superclasses with the operator $\downarrow$: $\Sigma_j \downarrow A_l, \Sigma_j \downarrow A_r$.
2. we collect the set of arrow types common to the two classes: $\Sigma_j \downarrow A_l \cap \Sigma_j \downarrow A_r$.
3. finally we check that the arrow types common to the two superclasses are redefined in the current class $\Sigma_j \downarrow A_l \cap \Sigma_j \downarrow A_r \subseteq \{B_{k_j} \rightarrow T_{k_j}\}_{k_j \in E_j}$.

Thus, the construction of $\Sigma_j$ is intended to fail if a method inherited by two superclasses is not redefined.

Concluding, we stress on two distinctive features of our approach, concerning the type checking of multi-methods definitions. First, we remark that with copy semantics we obtain a less restrictive mechanism w.r.t. standard inheritance. Let us consider the two following classes:

```
class A{
  m branches
  T (B' x){body1};
end
```
```
class B : A{
  m branches
  T (A' x){body2};
end
```

where $B' \leq A'$, and let $\Sigma_1 = \{(A \times B') \rightarrow T\}, \Sigma_2 = \{(B \times A') \rightarrow T\}$ be the types of $m$ in $A$ and $B$ respectively. The multi-type $\Sigma_1 \cup \Sigma_2 = \{(A \times B') \rightarrow T, (B \times A') \rightarrow T\}$, obtained by standard inheritance, is not well formed because there is no most specific branch for the input type $(B \times B')$, thus condition iii(d) of well formedness on multi-types should be violated. With copy semantics of inheritance we obtain a well formed multi-type:

$$\Sigma_1 \cup_{(B \leq A)} \Sigma_2 = \{(A \times B') \rightarrow T, (B \times A') \rightarrow T, (B \times B') \rightarrow T\}.$$

Second, even if this mechanism is more flexible, we check inconsistencies due to multiple inheritance, so we do not solve silently ambiguities that have to be explicitly solved by the programmer.

Using MT we can define the type environment $\Gamma_p$.

**Definition 11 ($\Gamma_p$).**

Let $p =$ classdef $^+$ body be a DOCS program. Let $C_p$ be defined as in Definition 7. Then $\Gamma_p$ will denote the following environment:

$$\Gamma_p = \text{MT(classdef }^+)$$

if and only if for each association $m : \Sigma \in \text{MT(classdef }^+)$ then

$$\Sigma \in_{C_p} \text{Types}$$

**Definition 12 (Well typedness of DOCS programs).**

Let $p$ be a DOCS program. We say that $p$ is well typed, denoted by $\Leftarrow p : A$, if

$$\Leftarrow p : A \iff C_p, S_p, \Gamma_p \vdash p : A \quad \text{for some } A$$

where $C_p$, $S_p$ and $\Gamma_p$ are defined in Definitions 7 and 11.

It is trivial to verify that $< C_p, S_p, \Gamma_p >$ is a consistent environment by construction of $C_p$, $S_p$ and $\Gamma_p$. Summarizing, the typing algorithm of a program $p$ can be described as a procedure performing two steps.

First we analyze the declarative part of the program collecting:

- the subtype relations induced by the inheritance hierarchy ($C_p$)
- the record types associated to the classes ($S_p$)
- the multi-type associated to each multi-method ($\Gamma_p$)

Then, the triple $< C_p, S_p, \Gamma_p >$, produced in the first step, is used to type expressions and bodies in the program. Namely:

- rule [PROGRAM-CLASS] checks method definitions relying on rule [BODY];
- rule [BODY] gives type to the main body of the program.
5 The meta-language $\lambda_{\text{object}}$

In this section we briefly introduce $\lambda_{\text{object}}$, a meta-language for reasoning about properties of constructs of object-oriented languages introduced in [Cas95]. $\lambda_{\text{object}}$ is essentially defined as an extension of the simply typed lambda calculus to model basic object-oriented mechanisms. Since we want to represent DOCS into $\lambda_{\text{object}}$, we use an imperative version of $\lambda_{\text{object}}$ which is characterized by the representation of the store $S$ (it is sketched in [Cas97], section 9.1.2). Namely, special typed identifiers $id^T$ will denote references to (addresses of) memory locations holding values of type $T$ (differently from variables $x^T$ denoting values of type $T$).

Let us first discuss, in an informal way, two crucial ideas underlying $\lambda_{\text{object}}$, concerning the representation of objects and overloaded functions.

**Objects.** Let us consider a simple definition of a class $A$ in DOCS:

```plaintext
class A{
    int x = 0;
    char y = 'a';
    ....
}
```

This will correspond, in $\lambda_{\text{object}}$, to the definition of an atomic type $A$ that is associated to the record type of its instance variables:

$$\langle\langle x : \text{ref int}, y : \text{ref char}\rangle\rangle$$

Let us note that $x$ and $y$ are mutable instance variables denoting memory locations whose content can be updated by side effects. Indeed, the creation of an object of a class $A$ in DOCS involves the allocation of free memory associated to fields $x$ an $y$ in an exclusive way. To this aim two fresh identifiers, $id_1^{\text{int}}$ and $id_2^{\text{char}}$ (of type $\text{ref int}$ and $\text{ref char}$, respectively) will be introduced at the moment of the creation of an object, that will perform the following operations:

$$id_1^{\text{int}} := 0; id_2^{\text{char}} := 'a'; in^A(\langle x = id_1^{\text{int}}, y = id_2^{\text{char}}\rangle)$$

where $in^A$ is the constructor that is tagged by the type name $A$. Thus the object $in^A(\langle x := id_1^{\text{int}}, y := id_2^{\text{char}}\rangle)$ is the object formed only by the values stored in $id_1$ and $id_2$ (its internal state) and by the tag $A$ denoting its type. This approach to the problem of object representation is a distinctive feature of $\lambda_{\text{object}}$ w.r.t. the record based model [Car88].

In order to access instance variables of objects we use the construct $out^A : A \rightarrow T$ which composed with $in$ gives the identity. To select the $j^{th}$ field we use the selection operator $.$ which returns the identifier associated to the selected field:

$$\langle f_i = id_i^{B_i}, i \in I \rangle, f_j = id_j^B$$

$$out^A(in^A(\langle f_i = id_i^{B_i}, i \in I \rangle)), f_j = id_j^B$$

**Overloaded functions.** Overloaded functions are the $\lambda_{\text{object}}$ terms representing multi-methods. An overloaded function is formed by a set of ordinary functions ($\lambda$-abstractions) each one constituting a different branch. Overloaded functions are built as lists starting with an empty overloaded function denoted by $\varepsilon$ and concatenating new branches by means of $\&$:

$$\varepsilon \& M_1 \& \ldots \& M_n$$
Expressions $M ::= x^T | \lambda x^T M | M \cdot M | \varepsilon | M^T & M | M \star M | \langle M, M \rangle$

$| \, \text{super}^T (M) | \in^T (M) | \text{out}^T (M) | \pi_1 (M) | \pi_2 (M)$

$| \, \text{id}^T | \uparrow M | M := M | M, M | \text{nil}$

Terms $P ::= M | \text{let } A \leq A, ..., A \in P \mid \text{let } A \text{ hide } T \text{ in } P$

Table 6. $\lambda_{\text{object}}$ terms

where $M \equiv \lambda x.N_i$ and $N_i$ is a $\lambda_{\text{object}}$ expression representing the body of the $\lambda$ abstraction (see Table 6) and $M_1 \ldots M_n$ correspond to the branches of a multi-method. Furthermore, the $&$ conjunctions are explicitly typed as well as all terms of $\lambda_{\text{object}}$: these types will be used to select the branch in method invocation and to type check multi-methods:

$$\varepsilon & T_1 M_1 & T_2 \ldots & T_n M_n$$

The branches are concatenated so that subtypes always precede supertypes; thus, in the overloaded term $\varepsilon & T_1 M_1 & T_2 \ldots & T_n M_n$ either $T_1$ and $T_2$ are unrelated or $T_1 \leq T_2$ (see section 6.2 for explanations of type ordering in overloaded functions). To perform an application $M \cdot N$, of the overloaded term $M$ to an argument, we first reduce $N$ to a value (tagged with its type) and $M$ to an overloaded term $\varepsilon & T_1 M_1 & T_2 \ldots & T_n M_n$. Then the branch selection is performed according to the tag of the argument, which is the actual type of the value obtained by reducing $N$. This way, method call implements dynamic overloading.

In the following sections we summarize formal definitions of $\lambda_{\text{object}}$ that are relevant for DOCS; we refer the reader to [Cas97] for further details about $\lambda_{\text{object}}$.

5.1 $\lambda_{\text{object}}$: syntax

First of all, $\lambda_{\text{object}}$ is not a language but a meta-language: this means that it must have very few constructs in order to making proofs about languages as simple as possible. For instance, records are not included in the syntax since they can be completely encoded (see encoding of records by overloaded functions in [Cas97] section 4.5.2). In the following sections we will explicitly use record and record types only to simplify the presentation of our translation from DOCS to $\lambda_{\text{object}}$. It is clear that the language version using records and record types can be automatically translated into the equivalent form not including them.

Terms in $\lambda_{\text{object}}$ are composed by an expression preceded by a (possibly empty) suite of declarations (see Table 6). Since $\text{coerce}^T (M)$ is not interesting in our context we do not consider it in the syntax.

Some notes about terms:

- $\text{super}^T (M)$: the type of $M$ is upcast to $A$. In $\lambda_{\text{object}}$ super does not necessarily appear in the receiver position but it is a first class value.
- $\text{id}^T$ is the identifier of a location of type $\text{ref} T$ while $\uparrow M$ is the content of the location $M$.
- The declaration $\text{let } A \text{ hide } T$ in $P$ declares the atomic type $A$ and associates it to the type $T$ used for its representation. This declaration is coupled with the two constructors $\text{in}^A : T \rightarrow A$ and $\text{out}^A : A \rightarrow T$.

A program in $\lambda_{\text{object}}$ is a closed term $P$ different from $\varepsilon$ (since $\varepsilon$ is the empty function, it makes no sense to consider it a valid program since it could not be used in any application).

---

1. In [Cas97] the syntax of tuples is $< M, M >$ while here is $\langle M, M \rangle$ to distinguish it from record notation.
5.2 \(\lambda_{\text{object}}\): typing

The types in \(\lambda_{\text{object}}\) are defined starting from a set of pre-types which is then restricted to well formed types.

\[
D ::= A \mid D \times D
\]
\[
T ::= A \mid T \rightarrow T \mid (T \times T) \mid \{D \rightarrow T, \ldots, D \rightarrow T\} \mid \text{ref } T \mid \text{unit};
\]

Let us note that the types of \(\lambda_{\text{object}}\) are a superset of the types of DOCS (Section 4) so we will use only a subset of \(\lambda_{\text{object}}\) types. The definition of the subtyping relation and of well typedness are the same as the ones defined for DOCS respectively in Section 4.2 and section 4.3.

As for the language DOCS, the rules are parametric w.r.t. a type constraint environment \(C\) and a record environment \(S\) (see Section 4 for a definition of \(C\) and \(S\)). \(\lambda_{\text{object}}\) typing rules are listed in Table 7 and 8.

**Notations.** We will use \(I\) as in DOCS to denote a pair of atomic types \((A \times B)\) and \(\Sigma\) to denote a type of the shape \(\{I_1 \rightarrow T_1, \ldots, I_n \rightarrow T_n\}\).

The following definition is used to update a multi-type.

**Definition 13 (Overloading composition).**

\[
\{I_1 \rightarrow T_1, \ldots, I_n \rightarrow T_n\} \oplus (I \rightarrow T) =
\begin{cases}
\{I_1 \rightarrow T_1, \ldots, I_{i-1} \rightarrow T_{i-1}, I_{i+1} \rightarrow T_{i+1}, \ldots, I_n \rightarrow T_n, I \rightarrow T\} & \text{if } I = I_i \\
\{I_1 \rightarrow T_1, \ldots, I_n \rightarrow T_n, I \rightarrow T\} & \text{otherwise}
\end{cases}
\]

**Remark 1.** With respect to the method selection, the order of the type indexing the \& is crucial (see rule \([\{}\]INTRO and Definition 13 for the construction of the types indexing the \&’s). For instance, the two terms

\[
\epsilon \& M_1 \& (U \rightarrow V) M_2 \& (U \rightarrow V, U' \rightarrow V) M_3
\]

and

\[
\epsilon \& M_1 \& (U \rightarrow V) M_2 \& (U' \rightarrow V, U \rightarrow V) M_3
\]

where \(U' \leq U\), are both well typed but they behave differently if applied to an argument of type \(U\): in the first case we execute \(M_2\), while in the second case we execute \(M_3\). This matter raises also in the semantics (interpretation) of DOCS multi-methods (Section 6.2) where we will use a permutation operator to generate the \(\lambda_{\text{object}}\) multi-method branches in the correct order (Definition 21).

5.3 \(\lambda_{\text{object}}\): operational semantics

\(\lambda_{\text{object}}\) operational semantics is given by the reduction \(\Rightarrow\); this reduction is defined on configurations of the shape \((C, \mathcal{S}, M)\) where:

- \(C\) is a type constraint system that is built along the reduction by the declarations \(\text{let } A \leq A_1 \ldots A_n \text{ in } P\) and that is used by the rules for the selection of the branch;
- \(\mathcal{S}\) is a global store associating identifiers \(id^T\) to values;
- \(M\) is the \(\lambda_{\text{object}}\) term to reduce.

\(\text{unit}\) is the type denoted as () in [Cas97]. We preferred to adopt this notation for the sake of readability.
axioms and two rules describe overloaded function application, denoted by out. The axioms and a rule describe the behavior of can perform its selection on. The tag D of the &-term. Thus, the overloaded application is implemented by a call-by-value reduction. The standard argument must be reduced to a tagged value and, lastly, the application is performed according to the index min where each term is a λ-term.

The axioms and rules of the operational semantics are listed in Tables 9 and 10, respectively. Three
values are terms that can be considered as acceptable result of an execution and are defined as follows:

\[
G ::= ε | x^T | (\lambda x^T.M) | (M \&^T M) | \text{nil} | \text{id}^T | (G, G) | \text{super}^A(M) | (G^{A_1}, \ldots, G^{A_n})
\]

We call object values values of the shape in\(^D\)(M). A tagged value is everything an overloaded function can perform its selection on. The tag D can be either an atomic type or a product of atomic types:

\[
\text{Tagged values } G^D ::= \text{in}^D(M) | \text{super}^D(M) | (G^{A_1}, \ldots, G^{A_n})
\]

The axioms and rules of the operational semantics are listed in Tables 9 and 10, respectively. Three axioms and a rule describe the behavior of out and give it access to the internal state of an object. Three axioms and two rules describe overloaded function application, denoted by •. We use \(\bar{D}\) to denote the min\(\in\{1, \ldots, n\}\) \(D_i\) s.t. \(C \vdash D \leq D_i\). In an overloaded application, we first reduce the term on the left to a &-term, where each term is a λ-abstraction, taking into account that we do not reduce inside λ-abstractions; then the argument must be reduced to a tagged value and, lastly, the application is performed according to the index of the &-term. Thus, the overloaded application is implemented by a call-by-value reduction. The standard
\[ \lambda \text{object typing rules (part II)} \]

| Super | \[
\frac{C; S \vdash M : B}{C; S \vdash \text{super}^A(M) : A} \] \(\beta\)-rule is also formalized; in this case, the application (denoted by \(\cdot\)) can be reduced also when the argument is not in normal form. However, in our context this is not an issue, since \(\beta\)-reduction is not involved in the application of overloaded functions. When the tagged value is a super, the super is used only for the selection while only the argument is passed to the selected branch. To model the erasing of super we define the function ers which removes the occurrences of super in a tagged value: 

\[
\text{ers}(G_D) = \begin{cases} 
M & \text{if } G_D \equiv \text{super}^A(M) \\
\text{ers}(G_{A_1}) \ldots, \text{ers}(G_{A_n}) & \text{if } G_D \equiv (G_{A_1}, \ldots, G_{A_n}) \\
G_D & \text{otherwise}
\end{cases}
\]

| In | \[
\frac{C; S \vdash M : T}{C; S \vdash \text{in}^A(M) : A} \] \(C \vdash B \leq A \in C, S \text{ Types}\)

| Out | \[
\frac{C; S \vdash M : B}{C; S \vdash \text{out}^A(M) : S(A)} \] \(C \vdash B \leq A \in C, S \text{ Types}\)

| Nil | \[
C; S \vdash \text{nil} : \text{unit} \]

| Ref Intro | \[
\frac{C; S \vdash \text{id}^T : \text{ref} T}{C; S \vdash M : \text{ref} T} \]

| Ref Elim | \[
\frac{C; S \vdash M : \text{ref} T}{C; S \vdash \text{↑} M : T} \]

| Assign | \[
\frac{C; S \vdash M : \text{ref} T \quad C; S \vdash N : U \leq T}{C; S \vdash M := N : U} \quad \text{Types}\]

| Seq | \[
\frac{C; S \vdash M : U \quad C; S \vdash N : T}{C; S \vdash M; N : T} \quad \text{Types}\]

The declaration \(\textbf{let } A \leq A_1 \ldots A_n \textbf{ in } P\) modifies the type constraint in which to evaluate the body \(P\). While \(\textbf{let } A \textbf{ hide } T \textbf{ in } P\) is used only by the type checker to check \(P\) and thus is discarded in the semantics.

The operation \(\mathcal{S}[\text{id}^T \leftarrow G]\) either updates the association for \(\text{id}^T\) in \(\mathcal{S}\), or it introduces the new association if there is no association for \(\text{id}^T\) in \(\mathcal{S}\). Thus, \(\lambda_{\text{object}}\) does not have a specific \texttt{ref} operator in the syntax as, e.g., in [WF94,Bru02]; when in \(\lambda_{\text{object}}\) we write \(\text{id}^T := G\) with \(\text{id}\) fresh we mean the same behavior of \(\text{ref} G\) (which allocates a brand-new cell in the memory, maps it to \(G\) and returns the cell itself). When we dereferentiate an identifier, \(\text{↑ id}^T\), we retrieve its associated value in the store. For the sake of simplicity, we also avoid to introduce the null references in the syntax, and then to formalize (and type) the run-time error resulting from the evaluation of a reference that points to no object (for a throughout treatment of null references we refer to [Bru02]). In our context, the null-pointer error is represented by the attempt to evaluate \(\text{↑ id}^T\) when \(\text{id}^T\) has not been previously initialized by a suitable tagged value (object). In this case, \(\mathcal{S}(\text{id}^T)\) is undefined: this is the only way in which a computation of a well typed program may get stuck, as formalized in the following theorems.
\[ (C, \mathcal{V}, \pi((G_1, \ldots, G_n))) \Rightarrow (C, \mathcal{V}, G_1) \]

\[ (C, \mathcal{V}, \text{out}^A(\text{id}^M(M))) \Rightarrow (C, \mathcal{V}, M) \]

\[ (C, \mathcal{V}, \text{out}^A(\text{super}^M(M))) \Rightarrow (C, \mathcal{V}, \text{out}^A(M)) \]

\[ (C, \mathcal{V}, (\lambda x^T.M) \cdot N) \Rightarrow (C, \mathcal{V}, M[x := N]) \]

\[ (C, \mathcal{V}, (M_1 \& (D_1 \rightarrow T_1 \ldots D_n \rightarrow T_n) M_2) \cdot G^D) \Rightarrow (C, \mathcal{V}, M_1 \& G^D) \] if \( D_n \neq \overline{D} \)

\[ (C, \mathcal{V}, (M_1 \& (D_1 \rightarrow T_1 \ldots D_n \rightarrow T_n) M_2) \cdot G^D) \Rightarrow (C, \mathcal{V}, M_2 \cdot \text{ers}(G^D)) \] if \( D_n = \overline{D} \)

\[ (C, \mathcal{V}, \text{let } A \text{ hide } T \text{ in } P) \Rightarrow (C, \mathcal{V}, P) \]

\[ (C, \mathcal{V}, \text{id}^T \triangleq G) \Rightarrow (C, \mathcal{V}, [\text{id}^T \triangleq G], \text{nil}) \]

\[ (C, \mathcal{V}, \uparrow \text{id}^T) \Rightarrow (C, \mathcal{V}, [\text{id}^T]) \]

\[ (C, \mathcal{V}, G; M) \Rightarrow (C, \mathcal{V}, M) \]

\[ \text{Table 9. } \lambda_{\text{object}} \text{ operational semantics: axioms} \]

\[ (C, \mathcal{V}, M) \Rightarrow (C', \mathcal{V}', M') \]

\[ (C, \mathcal{V}, \text{out}^A(M)) \Rightarrow (C', \mathcal{V}', \text{out}^A(M')) \]

\[ (C, \mathcal{V}, M) \Rightarrow (C', \mathcal{V}', M') \]

\[ (C, \mathcal{V}, \pi(M)) \Rightarrow (C', \mathcal{V}', \pi(M')) \]

\[ (C, \mathcal{V}, M) \Rightarrow (C', \mathcal{V}', M') \]

\[ (C, \mathcal{V}, M \circ N) \Rightarrow (C', \mathcal{V}', M' \circ N) \]

\[ (C, \mathcal{V}, N \triangleq := M) \Rightarrow (C', \mathcal{V}', N := M') \]

\[ (C, \mathcal{V}, M; N) \Rightarrow (C', \mathcal{V}', M'; N) \]

\[ (C, \mathcal{V}, M) \Rightarrow (C', \mathcal{V}', M') \]

\[ (C, \mathcal{V}, (M, N)) \Rightarrow (C', \mathcal{V}', (M', N)) \]

\[ (C, \mathcal{V}, (M, N)) \Rightarrow (C', \mathcal{V}', (M', N)) \]

\[ (C, \mathcal{V}, (N_1 \& N_2) \cdot M) \Rightarrow (C', \mathcal{V}', (N_1 \& N_2) \cdot M') \]

\[ (C, \mathcal{V}, M := G) \Rightarrow (C', \mathcal{V}', M' := G) \]

\[ (C, \mathcal{V}, M := G) \Rightarrow (C', \mathcal{V}', M' := G) \]

\[ (C, \mathcal{V}, M := G) \Rightarrow (C', \mathcal{V}', M' := G) \]

\[ \text{Table 10. } \lambda_{\text{object}} \text{ operational semantics: context rules (} \circ \text{ stands for both } \& \text{ and } \cdot). \]
Definition 14 (⇒). We denote by ⇒ the reflexive and transitive closure of →.

Definition 15 (Normal form). Given a configuration (C, C, M), we say that M is in normal form with respect to C and C if (C, C, M) ≠ . We say also that (C, C, M) is a normal form configuration.

Definition 16 (Error configuration). If M is in normal form with respect to C and C, and M contains a term ↑ id such that C(id) is undefined, then we say that (C, C, M) is an error configuration.

Theorem 1 (Subject reduction). Let P be a λ-object program. If C; S ⊢ P : T and (C, C, P) ⇒ (C′, C′, P′), for some C′, C′, P′ and P′, then C′; S ⊢ P′ : T′ where C′ ⊢ T′ ≤ T.

Theorem 2 (Progress). Let (C, C, M) be a normal form configuration such that it is not an error configuration. If M is a closed term and is typed by a (possibly unary) product of atomic types, then M is a tagged value.

The two above theorems show the standard type safety property for λ-object. We point out that their proofs are fully presented in [Cas97] (section 8.2) for the basic calculus, that is λ-object without the imperative part. However, the extensions of both proofs to our version of λ-object are straightforward: we just need to add a few cases, dealing with the imperative constructs, which do not present any significant technical difficulty.

6 Semantics of DOCS

We define the semantics of DOCS by translating DOCS into λ-object. The translation of DOCS expressions, statements, bodies and programs (Section 6.3) is defined by using the interpretation function [][<C,S,T,BT>] which returns the λ-object term associated to the argument. In particular, multi-methods are translated into λ-object overloaded functions (Section 6.2).

We define the translation from DOCS expressions, (statements, bodies and programs) to Terms (the set of terms of λ-object) using the function [][<C,S,T,BT>]:

[[]]<C,S,T,BT> : L → Envs → Terms

where
- L is the set of DOCS expressions, statements, bodies and programs
- Envs is a tuple of environments as defined in Section 4.4 plus the body environment BT, mapping multi-methods’ definitions to class names.
- Γ records the type of the identifiers and associates to self the current class, as explained later.

In the following we define the notion of consistency for the tuple <C, S, Γ, BT >.

Definition 17 (<C, S, Γ, BT > consistency). The tuple <C, S, Γ, BT > is consistent if

- <C, S, Γ > is a consistent environment according to Definition 6
- if m branches . . . end ∈ BT then m ∈ Dom(Γ)

Remark 2. We do not translate DOCS types into λ-object types since, as we noted in Section 5.2, DOCS types are a subset of λ-object types. The only difference between DOCS and λ-object types concerns multi-types: in λ-object the arrow types in a multi-type must be ordered according to the subtyping relation on input types (in particular the types that tag the &, see Section 6.2 for details). This ordering is relevant only for the semantics, in particular for the selection of an overloaded term, but not for the typing. Thus, we did not consider this ordering in DOCS since we only give the type system of DOCS, while, for semantics, we rely on a translation into λ-object; during this translation we must keep the ordering of multi-types into account.
In a tuple \( <C,S,\Gamma, BT> \), \( C \) and \( S \) will be used only in the interpretation of static overloading and object instantiation (see Definition 19), while \( BT \) will be used only for the interpretation of multi-methods (see Definition 23). In particular, during the interpretation of a DOCS term, \( C, S \) and \( BT \) will never change, while \( \Gamma \) will change (e.g., during the interpretation of a method body). Thus, from now on, for simplicity, when \( C, S \) and \( BT \) are not necessary, we will write only \( \Gamma \) instead of \( <C,S,\Gamma, BT> \), and \( \Gamma \) should always be intended as \( \Gamma \) \( \begin{bmatrix} <C,S,\Gamma, BT> \end{bmatrix} \).

While defining the translation function \( \Gamma \) \( \begin{bmatrix} <C,S,\Gamma, BT> \end{bmatrix} \) we will assume that \( <C,S,\Gamma, BT> \) contains all the information needed to interpret DOCS programs. Indeed, in section 6.3 we define the translation of well typed DOCS programs into \( \lambda_object \), thus \( <C,S,\Gamma, BT> \) will contain all the informations collected while checking the declarative part of programs.

### 6.1 Interpretation of expressions, statements and bodies

We first introduce an auxiliary function, \textit{deref}, that deals with references.

**Definition 18 (Definition of deref function).** Given a DOCS expression, \( \exp \), the function \( \text{deref}(\exp_r) \) is defined on the syntax of \( \exp \):

- \( \text{deref}(\[\text{x}\]_r) = \[\text{x}\]_r \) if \( \Gamma(x) = \text{ref} A \) for some \( A \)
- \( \text{deref}(\[\text{this} \_\text{f}]_r) = \[\text{this} \_\text{f}\]_r \)
- \( \text{deref}(\exp_i) \) \( = \exp_i \) in all other cases

In some sense, the function \( \text{deref} \) is the semantics counter- and complementary part of the \textit{ref destructor} operator in the type system (Definition 1) and returns the content of mutable instance variables.

In the following we define the translation (interpretation) of expressions, statements and bodies into \( \lambda_object \).

**Definition 19 (Interpretation of DOCS expression, statements and bodies).** We define the translation of expression, statements and bodies as in the following:

1. \( \[\text{x}\]_r = x^{\Gamma(x)} \)
2. \( \[m]\_r = m^{\Gamma(m)} \)
3. \( \[\text{this}\]_r = \text{self}^{\Gamma(\text{this})} \)
4. \( \[\text{this} \_\text{f}]_r = \text{out}^{\Gamma(\text{this})}(\text{self}^{\Gamma(\text{this})}) \cdot f \)
5. \( \Gamma^{\text{receiver} \leftarrow m(\exp)} \Gamma = \[m]\_r \bullet (\text{deref}(\[\text{receiver}\]_r), \text{super}^A(\text{deref}(\exp)) \) \)
   for some \( A \) such that \( C,S,\Gamma=r \exp : T \) and \( A = \tilde{T} \)
6. \( \Gamma^{\text{receiver} \leftarrow m(\exp)} = \[m]\_r \bullet (\text{deref}(\[\text{receiver}\]_r), \text{deref}(\exp)) \)
7. \( \Gamma^{\{A_1 x_1 = \exp_1; ...; A_n x_n = \exp_n; \text{stmnt}; \text{return} \exp\} \} = \text{id}^{A_1} : = \text{deref}(\exp_1) ; ... ; \text{id}^{A_n} : = \text{deref}(\exp_n) ; (\lambda (x_1^{\text{ref} A_1} ... x_n^{\text{ref} A_n}) . \text{stmnt} ; \text{return} \exp) \} \)
   where \( \Gamma' = \Gamma[x_1^{\text{ref} A_1} ... x_n^{\text{ref} A_n}] \)
   and \( \text{id}_1, ... , \text{id}_n \) are fresh identifiers.
8. \( \text{new}(A(\exp^{\text{ref} f})) = \text{id}^{\tilde{B}_i} : = \text{deref}(\exp) ; \text{in}^A((f_i = \text{id}^{\tilde{B}_i})); \)\( \text{id}_i \)’s are fresh identifiers.
9. \( \text{super}(A) = \text{super}^A(\[\text{this}\]_r) \)
10. \( \text{left} = \exp_r = \text{left}_r = \text{deref}(\[\exp\]_r) \)
11. \( \text{stmnt}_1 ; \text{stmnt}_2 \} = \[\text{stmnt}_1 \_\text{r}; \text{stmnt}_2 \_\text{r}] \)
12. \( \text{return} \exp = \text{deref}(\exp) \)

We note that:
- in field selection (4) out unpacks self into a record and it selects its f component;
- a method invocation (5, 6) is translated in an application of an overloaded function: thus, in the operational semantics of the translated term, the selection of the right branch is driven by the dynamic type of both the receiver and the static (5) or dynamic (6) parameter \( \text{exp} \) (see Table 9). Note that, in the case of static overloading, we force the argument to its static type; in order to do this we need the type of the argument as inferred by the type system. In this case case we need to refer to the type system \( C, S, \) and \( \Gamma \). This corresponds to the fact that static overloading method selection is made at compile time.
- a DOCS body (7) is composed by a (possibly empty) sequence of local variable declarations and initializations \( \Lambda_1 x_1 = \text{exp}_1; \ldots; A_n x_n = \text{exp}_n \), a (possibly empty) sequence of statements and a return. The corresponding \( \lambda \)-object term is a \( \lambda \)-abstraction

\[
\lambda (x_1^{\text{ref } A_1} \ldots x_n^{\text{ref } A_n}).\llbracket \text{body} \rrbracket_{\Gamma'}
\]

applied to the fresh identifiers \( id_1^{A_1} \ldots id_n^{A_n} \) initialized with the evaluation of the corresponding expressions: thus, \( id_1^{A_1} \ldots id_n^{A_n} \) will replace the occurrences of the DOCS variables \( x_1, \ldots, x_n \) in the first step of the evaluation of the \( \lambda \)-object term obtained by translation. As a consequence, during evaluation, we will manage only identifiers \( id^A \) instead of DOCS variables and the store \( \mathcal{S} \) will associate to \( id^A \) values of type \( A \) according to rule \( (C, \mathcal{S}, id^A := \text{exp}) \Rightarrow (C, \mathcal{S}[id^A ← \text{exp}], \text{nil}) \).
- the creation of an object (8) is translated in:
  - a sequence of assignments of the shape \( id_i^{B_i} := \text{deref}(\llbracket \text{exp}_i \rrbracket_{\Gamma'}) \) to assign to each identifier \( id_i^{B_i} \) the evaluation of the \( i \)-th argument expression
  - the construction of an object of type \( A \) using the \( \text{in} \) operator with a record which associates to each field \( f_i \) the corresponding identifier \( id_i \).

Thus, as in point 7, we will manage identifiers \( id^B \) instead of field labels, during the evaluation of the translated terms. As in the previous case all the identifiers are fresh, thus each object will have its own state.

6.2 Interpretation of multi-methods

DOCS multi-methods are translated into \( \lambda \)-object overloaded functions. We briefly discuss the informal idea and some crucial points, before giving the formal definitions.

Let us consider, for example, the following class definition:

```plaintext
class A {
  m branches
  T (B x) {body_1};
  T (C x) {body_2};
}
```

Then, the multi-method \( m \) will be translated into the following \( \lambda \)-object overloaded function:

\[
\varepsilon^{\llbracket A \times B \rrbracket → T} \lambda (\text{self}^A, \text{self}^B).M_1
\]

\[
&^{\llbracket (A \times B) → T, (A \times C) → T} \lambda (\text{self}^A, \text{self}^C).M_2
\]

where each branch of the multi-method is translated in a \( \lambda \)-abstraction (\( M_1 \) and \( M_2 \) are the \( \lambda \)-object terms obtained by translating the definition of the bodies of the related branches). The \( \lambda \)-abstraction has parameters \( \text{self}^A \) (which represents the receiver of the message, this is translated into \( \text{self}^A \)) and \( \text{self}^C \) (which represents the parameter of type \( C \) of the method) and \( A \) denotes the current class.
All the \( \lambda \)-abstractions are then concatenated through the conjunctions \& which are tagged with the type of the corresponding branch (the one on the right of \&). When tagging the conjunctions with the multi-type a problem arises. Suppose we have three classes \( A, B \) and \( C \) with \( C \) inheriting both from \( A \) and \( B \). Suppose also that a branch with type parameter \( D \) for multi-method \( m \) is defined both in \( A \) and \( B \); then by conditions of well formedness on multi-types we need to redefine the branch also in \( C \) (see condition (iii) in Definition 5). In DOCS the simplest solution is to define the branches in \( A \) and \( B \) and then to add the branch to \( C \) at the moment of \( C \) definition:

\[
\text{class } A \{ \\
\quad \text{\( m \) branches} \\
\quad T \langle D.x \rangle \{ \text{body}_1 \};
\} \\
\text{class } B \{ \\
\quad \text{\( m \) branches} \\
\quad T \langle D.x \rangle \{ \text{body}_2 \};
\} \\
\text{class } C : A, B \{ \\
\quad \text{\( m \) branches} \\
\quad T \langle D.x \rangle \{ \text{body}_3 \};
\}
\]

Hence, the corresponding translation of \( m \) in \( \lambda \_\text{object} \) would be:

\[
\varepsilon \& [(A \times D) \to T] \lambda (\text{self}^A, x^D).M_1
\]

\[
\& [(A \times D) \to T, (B \times D) \to T] \lambda (\text{self}^B, x^D).M_2
\]

\[
\& [(A \times D) \to T, (B \times D) \to T, (C \times D) \to T] \lambda (\text{self}^C, x^D).M_3
\]

where \( M_1, M_2 \) and \( M_3 \) are the \( \lambda \_\text{object} \) terms obtained by translating the bodies of the branches of method \( m \).

However, in the above overloaded term the second type index (\( [(A \times D) \to T, (B \times D) \to T] \)) is not well formed since it does not satisfy condition (d) in Definition 5: if we consider the input type \( (C \times D) \) there is not a most specific branch applying. The problem is due to the fact that, when we translate the branch defined in class \( B \), we have not already encountered class \( C \); for this reason the branch written to solve ambiguities due to multiple inheritance has to precede at least one of the branches of its direct ancestors\(^4\). Indeed, the following overloaded term is well formed:

\[
\varepsilon \& [(C \times D) \to T] \lambda (\text{self}^C, x^D).M_3
\]

\[
\& [(C \times D) \to T, (B \times D) \to T] \lambda (\text{self}^B, x^D).M_2
\]

\[
\& [(C \times D) \to T, (B \times D) \to T, (A \times D) \to T] \lambda (\text{self}^A, x^D).M_1
\]

where the \( \lambda \)-abstractions are concatenated in an ascending order w.r.t. the subtyping relation on the pair type of the \( \lambda \)-abstraction. Concluding, in order to build well typed overloaded functions (namely overloaded functions where all the \&’s are indexed with well formed multi-types) we need to concatenate the branches in a suitable order.

Thus, to translate DOCS multi-methods we have to scan the program from the bottom to the top to build well typed overloaded terms using the following functions:

- \( *\mathcal{M}_p <C,S,T,\text{BT}> (m) *\) returns the overloaded term associated to the message \( m \) by the definition in \( p \);
- \( *\mathcal{T}_p(m) *\) returns the (pre)type that indexes the \& concatenating the branches of the translation of \( m \). Obviously, if \( p \) is well typed we expect that \( *\mathcal{M}_p <C,S,T,\text{BT}> (m) : *\mathcal{T}_p (m) (\text{see Lemma 5}); *\)

\(^4\) The technical reason of this problem concerns the features of the \( \lambda \& \) calculus (on which \( \lambda \_\text{object} \) is based): \( \lambda \& \) totally lacks of the notion of time. Atomic types are given at once and there is no perception of the temporal dependence of type definitions. Further comments on this topic can be found in [CGL95].
Summarizing, every method is translated in a $\lambda$-abstraction (always parameterized over self$^A$, where $A$ is the class of the receiver), and method names, i.e., messages, become identifiers of these functions. So, in $\lambda$-object each method actually becomes a function parameterized also over the receiver object.\footnote{This makes $\lambda$-object pretty close to implementations of mainstream object-oriented languages where methods are basically translated into functions where the implicit object, this, is implicitly passed as the first parameter, see, e.g., [Lip96].}

Now, let us consider the case of an invocation of the multi-method $m$ and its translation (Definition 19):

$$\llbracket \text{new } C(\ldots) \ll m(\text{new } D(\ldots)) \rrbracket_T =$$
$$\llbracket m \rrbracket_T \bullet (\text{deref}(\llbracket \text{new } C(\ldots) \rrbracket_T), \text{deref}(\llbracket \text{new } D(\ldots) \rrbracket_T)) =$$
$$\llbracket m \rrbracket_T \bullet (\text{in}^C(), \text{in}^D()) =$$

$\varepsilon \& (\text{in}^D \to T) \lambda (\text{self}^C, x^D). M_3$

$\& (\text{in}^D \to T) \lambda (\text{self}^B, x^D). M_2$

$\& (\text{in}^D \to T) \lambda (\text{self}^A, x^D). M_1 \bullet (\text{in}^C(), \text{in}^D())$

According to the semantic rule for overloaded function application (see Table 5.3), the branches of the function are scanned until the input of the last element indexing the $\&$ coincides with the type of the input (condition $D = D_n$ in the semantic rule); then, in the example, the selected branch is $\lambda (\text{self}^C, x^D). M_3$ since the input type is $(C \times D)$.

This will give to the invocation of $m$ the expected behavior. Indeed, in a direct operational semantics of DOCS the rule for multi-method invocation would be very simple (see, for instance, [MC02]):

1. extract the set of the associated implementations of $m$ matching the type of the receiver and the parameters
2. choose the most specific one in the above set
3. evaluate the chosen implementation in the suitable context.

Our interpretation into $\lambda$-object, mapping the multi-method in an overloaded function and its invocation in an application term, formalizes and implements the above operational rule in a typed $\lambda$-calculus.

Finally, we remark that:

- DOCS typing rules guarantee that there always exist one and only one most specialized branch to be selected (see Section 4.4) w.r.t an input type $I$
- the translation into $\lambda$-object guarantees that the body of this most specialized version is associated to the branch of the overloaded function in which the last arrow type (indexing the $\&$) has input type $I$ (see Definitions 22, and 23.)

Now we formally define the interpretation function $M$ after some auxiliary definitions.

**Auxiliary definitions** The functions $\mathcal{F}$ and $\mathcal{M}$ use the auxiliary function $\mathcal{F}$ to implement copy semantics of inheritance. Given a class name $A$ and a method name $m$, $\mathcal{F}(A, m)$ returns a set of branch types $(A_i \times B_k) \to T_k$ where $A_i$ is either $A$ or a superclass of $A$ in the hierarchy and $B_k \to T_k$ is the type of a branch definition of $m$ in $A_i$. So, the branch types collected in this set are both the ones inherited and the ones defined in $A$, abstracting away from branches that are specifically introduced by copy semantics inheritance. Indeed $\mathcal{F}(A, m)$ scans the branches of $m$ defined in $A$ and recursively all the superclasses of $A$, thus the program
\( p \) containing the definition of \( A \) (and its superclasses) is an implicit parameter of \( \mathcal{F} \). However, we shall omit such argument since it will be always clear from the context. Note that \( \mathcal{F}(A, m) \) is simply a set of types (which may not be well formed) and not a multi-type. For this reason we denote with \textbf{MultiTypes} the codomain of \( \mathcal{F} \), instead of Types.

**Definition 20** (Definition of \( \mathcal{F} \) and \( L \)).

Let

\[
p = \text{class } A : A_h \text{ } h \in H \{ C_i f_i : i \in I \}
\]

\( m_j \) branches \( T_{kj} (B_{kj}, x_{kj}) \{ \text{body}_{kj} \}, k_j \in K_j \text{ } \text{end} \ j \in J \}

\( p' \)

then the function

\[
\mathcal{F} : (\text{ClassNames} \times \text{MethodNames}) \rightarrow \text{MultiTypes}
\]

is defined as follows:

\[
\mathcal{F}(A, m_j) = \{(A \times B_k) \rightarrow T_{kj}^{k_j \in K_j} \} \cup
\{(A_h \times B_l) \rightarrow T_l \mid (A_h \times B_l) \rightarrow T_l \in \mathcal{F}(A_h, m), h \in H, \ell \not\in K_j \}
\]

where \( \ell \not\in K_j \) assures that the branch \( B_k \rightarrow T_l \) is not defined in class \( A \).

Moreover,

\[
L(\mathcal{F}(A, m)) = \{ \ell \mid (A_i \times B_l) \rightarrow T_l \in \mathcal{F}(A, m) \}
\]

\( L(\mathcal{F}(A, m)) \) permits accessing the types of the signatures of branch definitions of \( m \) in the hierarchy of \( A \). By definition of \( \mathcal{F} \), we have the following property:

**Property 2.** Let \( A \) be a class name and \( m \) a method name, then for each \( (A_i \times B_j) \rightarrow T_j \in \mathcal{F}(A, m) \), we have:

- either \( A_i \equiv A \) and there is a branch of \( m \) in \( A \) with type \( B_j \rightarrow T_j \) or
- \( A \leq A_i \) and \( (A_i \times B_j) \rightarrow T_j \in \mathcal{F}(A, m) \) and for each \( (A_h \times B_l) \rightarrow T_l \in \mathcal{F}(A, m) \) if \( A_i \leq A_k \) and \( i \neq k \) then \( l \neq j \).

This property ensures that we collect all the types of the branches defined in a class and all the most redefined versions inherited from superclasses (that are not redefined by the class itself).

The following definition of permutation orders the types within multi-types in ascending order according to the subtype relation, i.e., leftmost arrow types are those with smallest input types. This is a crucial issue to guarantee that multi-method selection will work correctly (see Remark 1).

**Definition 21** (Permutation). Given an overloaded type \( \{I_h \rightarrow T_h\} \ h \in H \), we denote by \( \{I_{\sigma(h)} \rightarrow T_{\sigma(h)}\} \ h \in H \) the type obtained applying to the indexes the permutation \( \sigma \) that orders the \( I_h \)’s in such a way that \( I_h \leq I_k \Rightarrow \sigma(h) \leq \sigma(k) \).

We now define \( \mathcal{F}, \mathcal{M} \) to build multi-types. We assume that the type environment \( \Gamma \) associates to each multi-method \( m \) in \( p \) its equivalent multi-type \( \mathcal{F}[p](m) \).

**Definition 22** (Definition of \( \mathcal{F} \)).

Let

\[
p = \text{class } A : A_h \text{ } h \in H \{ C_i f_i : i \in I \}
\]

\( m_j \) branches \( T_{kj} (B_{kj}, x_{kj}) \{ \text{body}_{kj} \}, k_j \in K_j \text{ } \text{end} \ j \in J \}

\( p' \)

29
then we define

\[
\mathcal{T}[p](m) = \begin{cases} 
\mathcal{T}[p'](m_j) \oplus (A \times B_{\sigma(1)}) \rightarrow T_{\sigma(1)} \oplus \ldots \oplus (A \times B_{\sigma(n)}) \rightarrow T_{\sigma(n)} \\
\text{if } m = m_j \text{ for some } j \in J \text{ and } L(\mathcal{T}(A,m_j)) = \{1, \ldots, n\} \\
\mathcal{T}[p'](m) \\
\text{otherwise}
\end{cases}
\]

where \( L(\mathcal{T}(A,m_j)) \) is defined in Definition 20 and \( \oplus \) in Definition 13.

\( \mathcal{T}[\_](m) \) is the function that returns \( \{ \} \) in all the other cases.

Summarizing, for each multi-method declaration, in each class definition, \( \mathcal{T} \) performs the following steps:

1. it lists the arrow types of the branches defined in the class and in its super classes for a multi-method \( m_j \) using \( L(\mathcal{T}(A,m_j)) \);
2. for each arrow type collected in point (1) it replaces, in the input type, the first element of the pair with the type of the current class: this substitution implements copy semantics of inheritance at typing level;
3. it orders the arrow types so collected according to an ascending order on the parameter types w.r.t. subtyping relation: this is done by applying the permutation \( \sigma \) on the indexes of the second elements of the input type pairs;
4. finally, it concatenates the resulting multi-type to the multi-type obtained by translating the rest of the program (\( \mathcal{T}[p'](m) \)), namely to remaining class definitions. The concatenation is performed through the operator \( \oplus \).

Let us note that the multi-type obtained by the function \( \mathcal{T}[p](m) \) is the same multi-type that \( \Gamma_p \) associates to \( m \) in \( \text{DOCS} \) typing. The only difference is that the arrow types in the multi-type \( \mathcal{T}[p](m) \) are ordered while in \( \text{DOCS} \) typing the order of arrow types in a multi-type is not relevant (Remark 2). For instance, if we have three branches for the multi-method \( m \) in class \( A \) with parameters \( B_1, B_2 \) and \( B_3 \) (and return type \( B' \)), where \( B_1 \leq B_2 \leq B_1 \), since \( \sigma(3) \leq \sigma(2) \leq \sigma(1) \), then the types indexing the \& will be generated in this order: \( \{(A \times B_3) \rightarrow B'\}, \{(A \times B_1) \rightarrow B', (A \times B_2) \rightarrow B'\} \) and \( \{(A \times B_1) \rightarrow B', (A \times B_2) \rightarrow B', (A \times B_1) \rightarrow B'\} \).

Since conditions of well formedness on multi-types do not rely on the order of arrow types in multi-types (indeed multi-types are sets), it is easy to verify that if (Definition 5) \( \Gamma_p(m) \) is well formed also \( \mathcal{T}[p](m) \) is well formed. Thus, from the typing point of view, \( \Gamma_p(m) \) and \( \mathcal{T}[p](m) \) can be considered equivalent.

Property 3. Let \( p \) be a well typed \( \text{DOCS} \) program, then \( \forall m \in \text{MethNames}(p), \mathcal{T}[p](m) \) is well formed.

Proof. By contradiction, it is easy to show that if \( \mathcal{T}[p](m) \) is not well formed, then \( p \) cannot be well typed.

In the following we define the function \( \mathcal{M} \) that is devoted to translate multi-methods of a program into overloaded functions of \( \lambda \text{-object} \).

Definition 23 (Definition of \( \mathcal{M} \)). Let

\[
p = \text{class } A : A_h \text{ : } \{ C_i \mid (j \in I) \} \text{ branches } T_{k_j} (B_{k_j} x_{k_j}) \{ \text{body}_x_{k_j} \}; j \in J, \text{ end } i \in I \}; \text{p'}
\]

be a \( \text{DOCS} \) program. We define \( \mathcal{M}[p],_{C,i,F,B,T}^< \) as follows:

1. if \( m = m_j \) for some \( j \in J \), then let
   \( L(\mathcal{T}(A,m_j)) = \{1, \ldots, n\} \) and
   \( \mathcal{T}(A,m_j) = \{(D_{B_1} \times B_1) \rightarrow T_1, \ldots, (D_{B_n} \times B_n) \rightarrow T_n\} \)

30
where each \( D_B \) is either \( A \) or one of its superclasses. Then,
\[
\mathcal{M}[p]_{<C,S,T,B,T_p>} (m) = \\
(\ldots (\mathcal{M}[p']_{<C,S,T,B,T_p>} (m) \\
\& \mathcal{T}[p']_{<(A \times B)_{\sigma(1)} \rightarrow T_{\sigma(1)}}) \\
\lambda \left( \text{sel}^A, \text{perm}^B_{\sigma(1)} \right). \left[ \mathcal{B}(m_j, D_{B_{\sigma(1)}}, B_{\sigma(1)}) \right]_{\Gamma^\text{this}\rightarrow A, A_{\sigma(1)} \rightarrow B_{\sigma(1)}} \\
\ldots \\
\& \mathcal{T}[p']_{<(A \times B)_{\sigma(n-1)} \rightarrow T_{\sigma(n-1)}} \oplus \{(A \times B)_{\sigma(n)} \rightarrow T_{\sigma(n)}\} \\
\lambda \left( \text{sel}^A, \text{perm}^B_{\sigma(n)} \right). \left[ \mathcal{B}(m_j, D_{B_{\sigma(n)}}, B_{\sigma(n)}) \right]_{\Gamma^\text{this}\rightarrow A, A_{\sigma(n)} \rightarrow B_{\sigma(n)}})
\]
where \( p_0 \) defines \( \mathcal{T} \).
1. \( \mathcal{M} \) builds the overloaded term associated to each multi-method defined in a DOCS program. Each branch declaration in a class \( A \) is translated in a \( \lambda \)-abstraction. The body of the \( \lambda \)-abstraction is obtained using the body table \( BT \) (see Definition 7). Note that \( \mathcal{T} \) searches for the definition of the branch body using the class where the method has been originally defined. In this way, if the method is inherited from a superclass, the body is “copied” in the current class. Finally, the \( \lambda \)-abstractions are concatenated by \& (using the permutation \( \sigma \)).

In the definition of \( \mathcal{T} \) we did not consider (mutually) recursive methods. The definition of \( \mathcal{T} \) can be easily extended to cope with recursive methods, using the fix-point technique as suggested in [Cas95], but it is not particularly relevant in our context so we skip this technicality that would only make proofs more complex. Note, however that the definition of \( \mathcal{T} \) do not need to be changed.

6.3 Semantics of DOCS programs

We define the interpretation of any program \( p, \Omega(p) \), as a composition of the interpretation of its main body and multi-methods, in the specific environment \( <C_{p}, S_{p}, C_{p}, B_{p}, T_{p}> \) induced by the declarations of \( p \).

Definition 24 (Type environment \( \Gamma\mathcal{T}[p] \)). Let \( p \) be a DOCS program. Then we define the type environment \( \mathcal{T}[p] \) as follows:
\[
\Gamma\mathcal{T}[p] = \{ m : \mathcal{T}[p](m) \mid m \in \text{MethNames}(p) \}
\]

For simplicity, since \( \Gamma\mathcal{T}[p] \) is equivalent to the environment \( \Gamma_p \) used to type check DOCS programs (see Definition 11), modulo the order of arrow types in multi-types (namely \( \Gamma\mathcal{T}[p](m) \approx \Gamma_p(m) \forall m \in \text{MethNames}(p) \)), from now on we will use \( \Gamma_p \) to denote \( \Gamma\mathcal{T}[p] \). This abuse of notation will simplify the proof of main properties.

Now, we can define the interpretation of programs.

Definition 25 (Interpretation of DOCS programs). Let \( p = \text{class}\{ * \text{body} \} \) be a well-typed DOCS program, and
\[
\text{class}\{ * \text{body} \} = \text{class}\ A_1, \ldots, A_n \{ \\
C_{j} f_j : \Gamma_{h} \\
m_j \text{ branches} \\
\quad T_k (B_{h} x_k) \{ \text{body}_k \}; k \in K_j \\
\quad \text{end} \\
\} \}
\]

Then we define
\[
\Omega(p) \overset{\text{def}}{=} \left[ \text{body} \right]_{<C_{p}, S_{p}, C_{p}, B_{p}, T_{p}>} [m_j]^{\Gamma_h(m_j)} := \mathcal{M}[p]_{<C_{p}, S_{p}, C_{p}, B_{p}, T_{p}>} (m_j)
\]
for each \( j \in J_h \) and \( h \in H \).
To clarify the use of the type environment $\Gamma_p$, we remark a key aspect of the translation of DOCS multi-methods into $\lambda$-object overloaded functions. Let us consider the following code:

```c
class A{
  m branches
  T (B x){body_1};
}

class B{
  n branches
  T (B x){body_2};
}
```

The method $m$ defined in class $A$ has a branch with parameter of type $B$. When translating programs in $\lambda$-object, methods definitions are put “inline” with methods declarations (see Definition 23). The problem is that the body of the branch $A::m(B x)$ uses the method $n$ defined in class $B$, which has not already been translated. Thus, $n \notin \text{Dom}(\Gamma)$ and cannot be interpreted into $\lambda$-object (indeed $[n]_\Gamma = n^\Gamma(\Gamma)$). We adopt the following solution:

- we first build the multi-types associated to each multi-method defined in a program $p$ with the function $\mathcal{T}[p](m_i)$ (see Definition 22);
- the multi-types $\mathcal{T}[p](m_i)$ are collected in the environment $\Gamma_p$ which is used by the translation function $\Omega$.

From an algorithmic point of view, the translation of a DOCS program $p$ into $\Omega(p)$ can be seen as a procedure consisting of the following steps:

1. the prescan of the declarative part of $p$ (classdef *) constructs $<C_p,S_p,\Gamma_p,BT_p>$, and associates to each method name $m$ in $p$ its (ordered) multi-type $\mathcal{T}[p](m)$;
2. the interpretation of the program translates the main body of $p$ using $<C_p,S_p,\Gamma_p,BT_p>$;
3. the interpretation of multi-methods into overloaded functions associates to each multi-method name $m^\Gamma_p(m)$ the $\lambda$-object term $\mathcal{M}[p]<C_p,S_p,\Gamma_p,BT_p>(m)$ (this step scans again the program $p$ from the beginning since it works on the declarative part). Finally, each method identifier $m^\Gamma_p(m)$ is replaced by $\mathcal{M}[p]<C_p,S_p,\Gamma_p,BT_p>(m)$.

The semantics of $p$ is intended to be defined as the operational semantics of the $\lambda$-object term $\Omega(p)$, according to the rules of Tables 9 and 10 (Section 5.3).

**Definition 26 (Semantics of DOCS programs).** Let $p$ be a well-typed DOCS program. The semantics of $p$ is the evaluation of the $\lambda$-object term $\Omega(p)$, starting from the type constraints $C_p$ and an empty store, i.e.,

$$(C_p, \emptyset, \Omega(p))$$

Let us note that in [Cas95] the type constraint system $C$ used in the evaluation of a program is built along the reduction by the declarations let $A \leq A_1, \ldots, A_n$ in $p$ (indeed, the evaluation of a program starts from an empty $C$). In our case, instead, since we need $C_p$ to translate the program into a $\lambda$-object term, we avoid the generation of all the let’s: these would only generate a type constraint system equal to $C_p$. 

32
7 DOCS is type safe

In this section we prove that any well typed DOCS program is translated into a well-typed \( \lambda_{\text{object}} \) program, namely, types are preserved upon translation (type preservation). Thus, type safety of \( \lambda_{\text{object}} \) results in an indirect proof of type safety for the language DOCS (Theorem 3). In particular this proves the correctness of DOCS typing rules.

Type safety for DOCS programs, formalized in Theorem 4, relies on:

- type preservation under translation for expressions and statements (Lemma 2)
- type preservation under translation for bodies (Lemma 3)
- type preservation under translation for programs (Theorem 3)
- type correctness of the substitutions \( [m_j \mapsto (m_j) := \mathcal{M}[[p]]_{C_pS_pB_pBT_p}(m_j)]_{j \in J} \) used in the interpretation (Lemma 5)

Lemma 1 (Type of \( \text{deref} \)). Let \( m \in \text{exp} \) be a DOCS expression. Then for every consistent environment \( C,S,\Gamma, BT > \)

\[
\text{if } C,S,\Gamma \vdash \text{exp} : T \text{ then } C,S \vdash \text{deref}(\text{exp} )_{C,S,\Gamma, BT >} : \bar{T}
\]

Proof. By structural induction on \( \text{exp} \). The only interesting case is \( \text{exp} \equiv \text{methinvok}: \text{deref}(\text{methinvok})_{\Gamma} = \text{deref}(\text{exp})_{\Gamma} \)

then the result follows from the induction hypothesis.

Lemma 2 (Type preservation for expression and statements). Let \( t \) be a well typed DOCS expression or statement. Then for every consistent environment \( C,S,\Gamma, BT > \)

\[
\text{if } C,S,\Gamma \vdash t : T \text{ then } C,S \vdash [t]_{C,S,\Gamma, BT >} : T
\]

Proof. By structural induction on \( t \). Let us consider the case \( t \equiv \text{return} \leftarrow m(\text{exp}) \).

By rule [DOVMETHCALL] we have:

- \( C,S,\Gamma \vdash m : \{ k \mapsto U_k \}_{k \in K} \)
- \( C,S,\Gamma \vdash \text{return} : T \)
- \( C,S,\Gamma \vdash \text{exp} : T \)
- \( I_b = \min_{k \in K} \{ I_k | C \vdash (\bar{T} \times \bar{T}') \leq I_k \} \)

\[
[\text{return} \leftarrow m(\text{exp})]_{\Gamma} = [m]_{\Gamma} \circ (\text{deref}(\text{return} )_{\Gamma} \circ \text{deref}(\text{exp} )_{\Gamma})
\]

Then we have:

- \( C,S \vdash [m]_{\Gamma} : \{ k \mapsto U_k \}_{k \in K} \)
- \( C,S \vdash [\text{return}]_{\Gamma} : T \) by induction hypothesis
- \( I_b = \min_{k \in K} \{ I_k | C \vdash (\bar{T} \times \bar{T}') \leq I_k \} \)

Then, the thesis follows from the \( \lambda_{\text{object}} \) rule \( [\}] \text{ELIM} \).

The case \( t \equiv \text{receiver} \leftarrow m(\text{exp}) \) is similar. The other cases are trivial.

Lemma 3 (Type preservation for bodies). Let

\[
\{ A_1 \texttt{x}_1 = \texttt{exp}_1; \ldots; A_n \texttt{x}_n = \texttt{exp}_n; \texttt{stmt} ; \texttt{return} \texttt{exp} \}
\]

be a DOCS body. Then for every consistent environment \( C,S,\Gamma, BT > \) if:

\[
C,S,\Gamma \vdash \{ A_1 \texttt{x}_1 = \texttt{exp}_1; \ldots; A_n \texttt{x}_n = \texttt{exp}_n; \texttt{stmt} ; \texttt{return} \texttt{exp} \} : T
\]

then

\[
C,S \vdash [\{ A_1 \texttt{x}_1 = \texttt{exp}_1; \ldots; A_n \texttt{x}_n = \texttt{exp}_n; \texttt{stmt} ; \texttt{return} \texttt{exp} \}]_{C,S,\Gamma, BT >} : T
\]
Proof. $\llbracket A_1 \ \cdot \ x_1 = \ exp_1; \ldots ; A_n \ \cdot \ x_n = \ exp_n; \ \text{stmt; return exp} \rrbracket_r = \ \lambda (x_1 \ \text{ref}^{A_1} \ \ldots ; x_n \ \text{ref}^{A_n}). \llbracket \text{stmt} \rrbracket_r; \ \llbracket \text{return exp} \rrbracket_r; (\ \text{id}^{A_1} \ \ldots ; \text{id}^{A_n})$.

By DOCS rule \textsc{[Body]} and Lemma 2 we have $C; S \vdash \llbracket \text{stmt} \rrbracket_r; \ \llbracket \text{return exp} \rrbracket_r : \tilde{T}'$.

The thesis comes from $\lambda \_ \text{object}$ rules \textsc{[\text{\rightarrow INTRO}]} and \textsc{[\text{\rightarrow ELIM}]}.

The following lemma is a technical step for proving lemma 5: it states that the types of the branches of the overloaded function $\mathcal{M}[p]_{<C;S,T,B,T>}(m)$ have the same types labeling the conjunctions &.

**Lemma 4** (Well typedness of $\mathcal{M}$ branches). Let $p$ be

$$
class A : A_h \ \text{h} \in H \{ 
C_1; j_1; \ \text{\ldots ; j} \in J 
m_j \ \text{branches} \ T_{k_j} (B_{k_j}, x_{k_j}) \{ \text{body}_{k_j} \}; k_j \in K_j \ \text{end} \ \text{\textit{\&}} \ j \in J
\} : p'
$$

be a well typed DOCS program. Let $\mathcal{M}[p]_{<C;S,T,B,T>}(m_j)$

$$\mathcal{M}[p]_{<C;S,T,B,T>}(m_j) = \ (\ldots (\mathcal{M}[p']_{<C;S,T,B,T>}(m_j) \ \& \ P[p']_{<C;S,T,B,T>}(m_j) ; T_{(\text{this}\_\text{\&} A_j \ \text{\&} B_i)}) \ \& \ P[p]_{<C;S,T,B,T>}(m_j) ; T_{(\text{this}\_\text{\&} A_j \ \text{\&} B_i)}) \ \ldots
\lambda (self^{A_j}, B_i^{B_j(1)}). \llbracket T \ (m_j, D_{B_i^{B_j}}, B_i) \rrbracket_{\text{\textit{\&}}} (\text{this} \_\text{\&} A_j \ \text{\&} B_i) \ \llbracket T \ (m_j, D_{B_i^{B_j}}, B_i) \rrbracket_{\text{\textit{\&}}} (\text{this} \_\text{\&} A_j \ \text{\&} B_i) \ \ldots
\lambda (self^{A_j}, B_i^{B_j(n)}). \llbracket T \ (m_j, D_{B_i^{B_j}}, B_i) \rrbracket_{\text{\textit{\&}}} (\text{this} \_\text{\&} A_j \ \text{\&} B_i) \ \llbracket T \ (m_j, D_{B_i^{B_j}}, B_i) \rrbracket_{\text{\textit{\&}}} (\text{this} \_\text{\&} A_j \ \text{\&} B_i) \$$

be the interpretation in $\lambda \_ \text{object}$ of the methods defined in class $A$ according to Definition 23, where

$$L(\mathcal{F}(A, m_j)) = \{1, \ldots , n\} \ \text{and}
\mathcal{F}(A, m_j) = \{ (D_{B_1 \ \text{\&} B_1} \ \rightarrow \ T_1, \ldots, (D_{B_n \ \text{\&} B_n} \ \rightarrow \ T_n)\}
$$

where each $D_{B_i}$ is either $A$ or one of its superclasses.

Then:

$$\ C; S \ \vdash \ \lambda (self^{A_j}, B_i^{B_j(1)}). \llbracket T \ (m_j, D_{B_i^{B_j}}, B_i) \rrbracket_{\text{\textit{\&}}} (\text{this} \_\text{\&} A_j \ \text{\&} B_i) : (A \ \text{\&} B_i) \ \rightarrow \ T_i
$$

for each $l \in \{\sigma(1), \ldots , \sigma(n)\}$

Proof. The body of each lambda abstraction is built by

$$\llbracket T \ (m_j, D_{B_i^{B_j}}, B_i) \rrbracket_{\text{\textit{\&}}} (\text{this} \_\text{\&} A_j \ \text{\&} B_i) = \llbracket \text{body} \rrbracket_{\text{\textit{\&}}} (\text{this} \_\text{\&} A_j \ \text{\&} B_i)
$$

Since $p$ is well typed we have $C; S; I \vdash \text{body} : U$ with $U \ \leq \ T_i$ (from DOCS rule \textsc{[Program-class]}). By Lemma 2. $C; S \vdash \llbracket \text{body} \rrbracket_{\text{\textit{\&}}} \llbracket \text{this} \_\text{\&} A_j \ \text{\&} B_i \rrbracket : U$. The result comes from $\lambda \_ \text{object}$ rule \textsc{[\text{\rightarrow INTRO}]}.

Now, in order to guarantee that the substitutions $m_j \Gamma_j(m_j) := \mathcal{M}[p]_{<C;S,T,B,T>}(m_j)$ preserve well typedness we have to prove that $\mathcal{M}[p]_{<C;S,T,B,T>}(m_j)$ has type $\mathcal{F}[p](m_j)$ for all $j \in \text{MethNames}(p)$, since $\Gamma_j(m_j) = \mathcal{F}[p](m_j)$.

**Lemma 5** (Type correctness of method translation). Given a well typed DOCS program $p$

$$\vdash p : T \ (\text{i.e.,} \ C_p; S_p; \Gamma_p \vdash p : T)
$$

then for each $m \in \text{MethNames}(p)$

$$C_p; S_p \vdash \mathcal{M}[p]_{<C_p;S_p,T,B,T>}(m) : \mathcal{F}[p](m)
$$
Proof. By induction on the cardinality \( N \) of classdef \(^*\).

- \( (N = 1) \), then \( p \) is defined as in the following

\[
p \equiv \text{class } A : \{ \\
  C_i \mid i \in I \\
  m_j \text{ branches } T_k (B_k x_k) \{ \text{body}_k \}; k \in K_j \text{ end } j \in J \\
}; \text{body}
\]

The thesis is proved by induction on the number \( n \) of the branches of \( \mathcal{M} [\mathcal{P}] < C_p, S_p, [\mathcal{P},BT_p] > (m_j) \) (which coincides with the cardinality of the set \( L(\mathcal{F}(A,m_j)) \)).

- The base case \( (n = 0) \) is trivial.
- Let us assume \( \forall l \leq n \mathcal{M} [\mathcal{P}] < C_p, S_p, [\mathcal{P},BT_p] > (m_j) ; \mathcal{T} [\mathcal{P}] (m_j) \); then we want to prove that

\[
\mathcal{M} [\mathcal{P}] < C_p, S_p, [\mathcal{P},BT_p] > (m_j) ; \mathcal{T} [\mathcal{P}] (m_j)
\]

where \( m_j \) has \( n + 1 \) branches. The result comes from \( \lambda \) \( \_ \text{object} \) rule \([\{\} \text{INTRO} \), Lemma 4, the induction hypothesis and by using the definition of \( \mathcal{M} [\mathcal{P}] < C,S,I,\mathcal{T}> (m_j) \) and \( \mathcal{T} [\mathcal{P}] (m_j) \).

- \( (N > 1) \)

\[
p \equiv \text{class } A : A_h \{ \\
  C_i \mid i \in I \\
  m_j \text{ branches } T_k (B_k x_k) \{ \text{body}_k \}; k \in K_j \text{ end } j \in J \\
}; \text{body}
\]

We have to prove that \( \forall j \in J: \)

\[
\mathcal{M} [\mathcal{P}] < C,S,I,\mathcal{T}> (m_j) = \\
(\ldots (\mathcal{M} [\mathcal{P}] < C,S,I,\mathcal{T}> (m_j) ) \\
\& \mathcal{T} [\mathcal{P}] (m) \equiv \{(A \times B_{\sigma_1}) \rightarrow T_{\sigma_1} \}) \\
\mathcal{\lambda} (\text{sel}^A, x_{B_{\sigma_1}}) \{ \mathcal{BT}(m_j, D_{B_{\sigma_1}}, B_{\sigma_1}) \} \mathcal{\Gamma}(\text{this} \leftarrow A, x_{B_{\sigma_1}} \rightarrow B_{\sigma_1}) \\
\vdots \\
\& \mathcal{T} [\mathcal{P}] (m) \equiv \{(A \times B_{\sigma_n}) \rightarrow T_{\sigma_n} \}) \equiv \{(A \times B_{\sigma_n}) \rightarrow T_{\sigma_n} \}) \\
\mathcal{\lambda} (\text{sel}^A, x_{B_{\sigma_n}}) \{ \mathcal{BT}(m_j, D_{B_{\sigma_n}}, B_{\sigma_n}) \} \mathcal{\Gamma}(\text{this} \leftarrow A, x_{B_{\sigma_n}} \rightarrow B_{\sigma_n})
\]

is of type \( \mathcal{T} [\mathcal{P}] (m_j) \), where

\[
L(\mathcal{F}(A,m_j)) = \{ 1, \ldots , n \} \text{ and } \\
\mathcal{F}(A,m_j) = \{(D_{B_1} \times B_1) \rightarrow T_1, \ldots , (D_{B_n} \times B_n) \rightarrow T_n \}
\]

where each \( D_{B_i} \) is either \( A \) or one of its superclasses.

By induction hypothesis \( C ; S \vdash \mathcal{M} [\mathcal{P}] < C_p, S_p, [\mathcal{P},BT_p] > (m_j) ; \mathcal{T} [\mathcal{P}] (m_j) \). Then the proof proceeds as in the previous case.

Theorem 3 (Type preservation under semantic translation). Let \( p \) be a well typed closed DOCS program. Then

\[
C_p ; S_p ; \Gamma_p \vdash p : A \text{ implies } C_p ; S_p \vdash \Omega(p) : A
\]

Proof. Let \( p = \text{classdef}^* \text{ body} \). Then:
\[ \mapsto p : A \equiv C_p; S_p; \Gamma_p \vdash p : A \] 
by definition

\[ \Rightarrow C_p; S_p; \Gamma_p \vdash \text{body} : A \] 
by iterate application

\[ \Rightarrow C_p; S_p \vdash \llbracket \text{body} \rrbracket_{\llbracket C_p; S_p; \Gamma_p \rrbracket} : A \] 
by Lemma 3.

\[ \Rightarrow C_p; S_p \vdash \llbracket \text{body} \rrbracket_{\llbracket C_p; S_p; \Gamma_p, BT_p \rrbracket} : \llbracket \lambda \llbracket C_p; S_p; \Gamma_p \rrbracket \rrbracket \llbracket \beta \rrbracket \llbracket \mu \rrbracket : A \] 
by Lemma 5 and by

the substitution property of \( \lambda \_\text{object} \), [Cas95]

that is, \( C_p; S_p \vdash \Omega \_\text{(p)} : A \) by Definition 26.

If \( \Omega \_\text{(p)} \) is well typed, then the execution of \( \Omega \_\text{(p)} \) cannot result in a run time type error, because \( \lambda \_\text{object} \) is type safe. We recall that, in a well typed program \( p \), all local variables are initialized and, when creating an object, suitable expressions are provided to initialize all the fields of that objects. As a consequence, during the translation of \( p \) into \( \lambda \_\text{object} \), any creation of a fresh identifier \( id^{T} \) will be associated to an assignment for \( id^{T} \). Thus, taking into account the semantics of the assignment operation, we can conclude that the computation starting from \( \Omega \_\text{(p)} \) cannot produce an error configuration, and then the execution of \( p \) never gets stuck.

**Theorem 4 (DOCS is type safe).** The execution of a well typed (closed) DOCS program \( p \) cannot result in a type error.

**Proof.** If \( p \) is well typed (\( \mapsto p : T \)) then \( \Omega \_\text{(p)} \) is well typed (\( C_p; S_p \vdash \Omega \_\text{(p)} : T \)) by Theorem 3. The execution of \( \Omega \_\text{(p)} \), according to the operational semantics of \( \lambda \_\text{object} \), cannot produce run time type errors by type safety of \( \lambda \_\text{object} \).

### 8 Related works

Various languages have been proposed to study multi-methods with dynamic overloading. *CLOS* [BDG+89] is a class-based language with a linearization approach to multi-methods: they are ordered by prioritizing argument position with earlier argument positions completely dominating later ones. This automatic handling of ambiguities may lead to programming errors. In *Dylan* [Sha97] methods are not encapsulated in classes but in generic functions which are first class objects. When a generic function is called it finds the methods that are applicable to the arguments and selects the most specific one. *BeCecil* [CL96] is a prototype based language with multi-methods. Multi-methods are collected in first-class generic function objects which can extend other objects. Even if this language is object-based, it provides a static type system, scoping and encapsulation of all declarations; however, its approach, being object-based is radically different from our class-based setting. *Fortress* [ACH+06] is an object-oriented language supporting methods within *traits* [SDNB03] and functions defined outside traits. It also provides components (units of compilation) which contain declarations of objects, traits and functions. Fortress differs from mainstream languages since it is not class-based. Parasitic multi-methods [BC97] are a variant of the encapsulated multi-methods of [BCC+95,Cas97] applied to Java. This extension is rather flexible and indeed provides modular dynamic overloading. The goal of modularity has influenced many aspects of the design: method selection is asymmetric; parasitic methods are complicated by the use of textual order of methods in order to resolve ambiguities for selecting the right branch; all methods must be declared in the class of the receiver in order to eliminate class dependences. *MultiJava* [CLCM00] is an extension of Java that supports multi-methods by using open classes (classes to which new methods can be added without editing the class directly) and multi-methods.

Concerning core languages and calculi, we can compare *DOCS* to *FJ* [IPW01]: *DOCS* models a set of features that are in between a minimal core language as *FJ* and a concrete language. Indeed, while *FJ*
abstracts the functional core of Java, DOCS abstracts the imperative part by integrating in this core advanced features that language extension experiments can rely on. Note that, passing to a version of DOCS with less powerful features is straightforward.

KOOL [Cas97] integrates multi-methods and overloaded functions (external to classes) in a functional kernel object-oriented language in a type safe way. KOOL type system and its semantics by translation into $\lambda$ _object_ were the starting point to build DOCS; indeed the notion of well formedness for DOCS types is widely inspired by the one defined in [Cas97]. Both KOOL and DOCS aim at being light and compact in presenting kernel object-oriented features, however, they are quite different since they have two different goals. KOOL includes both encapsulated multi-methods and overloaded functions external to classes (not included in DOCS) thus unifying in a single language two different styles of programming. As it is explained in [Cas97] (section 3.5) KOOL aims at defining a formalism in which to study the features of object-oriented programming so the choice in the design was “to keep the language small simple and easily comprehensible but keep it from being a realistic programming language”. For this reason KOOL omits imperative features in its presentation (although chapter 9 of [Cas97] introduced imperative features that we extended). On the other hand DOCS is designed to study the interaction of complex mechanisms in a context as close as possible to real languages so we include imperative features; we also allow forward declarations in methods class definitions, namely, we let the programmer write a method with a parameter of type $A$ in a class no matter if the class $A$ is defined before or after the current class. This feature (included in mainstream languages such as Java and C++), which is not supported by KOOL, influenced the typing of DOCS: first the declarative part is checked producing a class table which is used to type check method declarations and definitions. Finally, KOOL does not interpret overloading by copy semantics, so many multi-method definitions which are well typed in DOCS are discarded in KOOL. Thus DOCS allows a less restrictive overloading resolution policy still maintaining the primary goal of type safety.

[CL95] presents a polynomial-time static type checking algorithm that checks the conformance, completeness, and consistency of a group of method implementations with respect to declared message signatures. This result can be used also in our approach to address the efficiency issue of the typing procedure.

Tuple [LM98] is a simple object-oriented language designed to integrate multiple dispatch in single dispatching languages by adding tuples as primitive expressions. Tuple is statically typed and it is proved to be type safe. In Tuple methods can be defined either inside classes or in tuple classes (external to standard classes). Message look-up on methods defined in a tuple supports dynamic overloading: messages are sent to tuples of arguments dynamically involved in method selection. There are some key differences between Tuple and DOCS. First, Tuple supports dynamic overloading only for methods external to classes thus adopting a mechanism which is closer to multiple dispatching languages. As a consequence in Tuple the distinction between static and dynamic overloading is made at method definition while in DOCS it is deferred at the time of method calls thus increasing flexibility.

Dubious [MC02] is a core calculus designed to study modular static type checking of multi-methods in modules. Dubious is classless and includes multi-methods with symmetric dispatch in the form of generic functions defined in modules that can be checked separately and then linked in a type safe way. In [MC02] several type systems are discussed in order to find the right balance between flexibility and type safety. Dubious and DOCS share some basic goals such as the symmetry of dispatch, a clear policy for ambiguities resolution (avoiding linearization of parameters or of superclasses) and static type safety. On the other hand the two languages are totally different since DOCS is based on classes and does not address the issue of separate type checking.

9 Conclusions

In this paper we presented DOCS (Dynamic Overloading with Copy Semantics), an object-oriented imperative kernel language, including basic features of many mainstream programming languages, combined with advanced features: multiple inheritance, dynamic overloading and copy semantics. Indeed, DOCS gives a
type-based foundation to dynamic overloading with copy semantics. We defined a translational semantics of DOCS into the meta-language $\lambda_{\text{object}}$ [Cas95,Cas97].

Therefore, DOCS can be thought of as a formal framework to design and develop language extensions and to prove theoretical properties of such extensions. For instance, we exploited this framework to study and implement an extension of C++ with dynamic overloading in [BCV06], where dynamic overloading is implemented by using only dynamic binding and static overloading. This extended C++ has been implemented and the correctness of this implementation has been proven using the semantics of DOCS (the implementation is freely available at http://doublecpp.sf.net/).

Acknowledgments We thank Franco Barbanera and Mariangiola Dezani for many helpful remarks and suggestions. We also thank the anonymous referees for useful suggestions on how to improve the paper.

References


