

A Syntactic Model of Mutation and Aliasing

Paola Giannini*

Computer Science Institute, DiSIT, Università del Piemonte Orientale
Italy

paola.giannini@uniupo.it

Marco Servetto

School of Engineering and Computer Science, Victoria University of Wellington
New Zealand

servetto@ecs.vuw.ac.nz

Elena Zucca

DIBRIS, Università di Genova
Italy

elena.zucca@unige.it

Traditionally, semantic models of imperative languages use an auxiliary structure which mimics memory. In this way, ownership and other encapsulation properties need to be reconstructed from the graph structure of such global memory. We present an alternative *syntactic* model where memory is encoded as part of the program rather than as a separate resource. This means that execution can be modelled by just rewriting source code terms, as in semantic models for functional programs. Formally, this is achieved by the block construct, introducing local variable declarations, which play the role of memory when their initializing expressions have been evaluated. In this way, we obtain a language semantics which directly represents at the syntactic level constraints on aliasing, allowing simpler reasoning about related properties. To illustrate this advantage, we consider the issue, widely studied in the literature, of characterizing an isolated portion of memory, which cannot be reached through external references. In the syntactic model, closed block values, called *capsules*, provide a simple representation of isolated portions of memory, and capsules can be safely moved to another location in the memory, without introducing sharing, by means of *affine* variables. We prove that the syntactic model can be encoded in the conventional one, hence efficiently implemented.

1 Introduction

In languages with state and mutations, keeping control of aliasing relations is a key issue for correctness. This is exacerbated by concurrency mechanisms, since side-effects in one thread can affect the behaviour of another thread, hence unpredicted aliasing can induce unplanned/unsafe communication.

For these reasons, the last few decades have seen considerable interest in type systems for controlling sharing and interference, to make programs easier to maintain and understand, notably using *qualifiers* to restrict the usage of references [29, 20, 25, 12].

In particular, in an ongoing stream of work [27, 15, 17, 16, 18, 14, 19], we have adopted an innovative execution model [26, 9] for imperative languages which, differently from traditional ones, is a *reduction relation on language terms*. That is, we do not add an auxiliary structure which mimics physical memory, but such structure is encoded in the language itself. Whereas this makes no difference from a programmer's point of view, it is important on the foundational side, since, as will be informally illustrated below, language semantics directly represents at the syntactic level constraints on aliasing, allowing simpler reasoning about related properties.

In this paper, we focus on the operational model itself, rather than on type systems, and formalize its relation with the conventional model, where an auxiliary global structure mimics memory.

*This original research has the financial support of the Università del Piemonte Orientale.

To informally introduce this syntactic calculus, we show examples of reduction sequences. The main idea is to use variable declarations to directly represent the memory. That is, a declared variable is not replaced by its value, as in standard `let`, but the association is kept and used when necessary, as it happens, with different aims and technical problems, in cyclic lambda calculi [4, 23, 3]. Assuming a program (class table) where class `C` has two fields `f1` and `f2` of type `D`, and class `D` has a field `f` of type `D`, the term

```
D x=new D(y); D y=new D(x); C w={D z=new D(z); x.f=x; new C(z,z)}; w.f1
```

starts with two declarations that can be seen as a memory consisting of two mutually referring objects. Then there is a declaration whose right-hand-side needs to be evaluated and the final expression returns the value of a field of the object associated with this last variable. The reduction of the term is as follows.

```
D x=new D(y); D y=new D(x); C w={D z=new D(z); x.f=x; new C(z,z)}; w.f1 →
D x=new D(x); D y=new D(x); C w={D z=new D(z); new C(z,z)}; w.f1 →
D x=new D(x); D y=new D(x); D z=new D(z); C w={new C(z,z)}; w.f1 ≅
D x=new D(x); D y=new D(x); D z=new D(z); C w=new C(z,z); w.f1 →
D x=new D(x); D y=new D(x); D z=new D(z); C w=new C(z,z); z →
D z=new D(z); z
```

Evaluation proceeds left to right. We emphasize at each step the declarations which can be seen as the store (in grey). We start evaluating the right-hand-side of the declaration for `w`, by updating the field `f` of `x`. Then, in order to evaluate the field access `w.f1`, we need to move the declaration of `z` outside of the inner block. A block with no declarations is considered equivalent to its body, as expressed by \cong . Now the field access `w.f1` can be performed, getting `z`, and the last step removes declarations (memory) which are not reachable from `z`, giving as final result a memory consisting of only one cyclic object.

To illustrate how aliasing constraints are directly represented in this syntactic model, we consider an important example: how to characterize an isolated portion of memory, which cannot be reached through external references. This allows programmers (and static analyses) to identify portions of memory that can be safely handled by a thread. This property has been widely studied in the literature, under different names and variants, such as *isolated* [20], *unique* [8] and *externally unique* [11], *balloon* [2], *island* [13].

In the syntactic calculus, block values with no free variables, called *capsules*, provide a simple representation of portions of memory which are trivially isolated. For instance, in the following example:

```
(ex1) D x=new D(x); D y=new D(x); Ca w={D z=new D(z); new C(z,z)}; x.f=x
```

the right-hand side of the declaration of `w` is a capsule. To allow the programmer to *safely rely* on the fact that `w` denotes an isolated portion of memory, which nobody else in the program can affect, we introduce the qualifier `a`, as shown above, for *affine* variables/parameters, which should be initialized with capsules.

If the term is, instead:

```
(ex2) D x=new D(x); D y=new D(x); Ca w={D z=new D(z); new C(z,y)}; x.f=x
```

then the inner block is *not* a capsule, hence its use to initialize an affine variable is an error to be prevented, otherwise a programmer using `w` would erroneously rely on the capsule property. In the syntactic calculus, this error can be easily detected at runtime in a modular way, that is, by looking only at the block itself. For instance, in (ex1) the runtime check succeeds, whereas in (ex2) it fails, hence normal execution cannot proceed, since the block contains the free variable `y`.¹

¹In the formalization presented in this paper, the term is simply stuck. A different choice could be to introduce explicit *error* terms. In our previous work [27, 15, 17, 16, 18] we have designed type systems which are able to statically prevent such error.

Note that, in the conventional calculus, detecting that a reference denotes an isolated portion of memory requires, instead, a dependency analysis involving surrounding code and memory. For instance, in the examples (EX1) and (EX2) above, execution will reach respectively the following step:

$$\begin{aligned} \text{(EX1)} \quad C^a \ w = \text{new } C(l_z, l_z); \ l_x.f = l_x | \mu \\ \text{(EX2)} \quad C^a \ w = \text{new } C(l_z, l_y); \ l_x.f = l_x | \mu \end{aligned}$$

where the domain of the memory μ are *object identifiers* l , modeling *global* names which, differently from variables, do not support shadowing and α -renaming. Here $\mu = l_x \mapsto \text{new } D(l_x), l_y \mapsto \text{new } D(l_x), l_z \mapsto \text{new } D(l_z)$. It is clear that the two situations cannot be distinguished by only looking locally at the initialization expression of w . Instead, we must check that the memory portion reachable from such initialization expression is isolated, that is, cannot be reached from references used in other parts of the program. This is true for (EX1), since there is no sharing between l_z and the reference l_x used in the external code $l_x.f = l_x$. For (EX2), instead, there is sharing between l_y and l_x , and indeed the execution of such external code affects the portion of memory reachable from $\text{new } C(l_y, l_z)$. In the general case, detecting sharing through dependency analysis is an expensive check, which could even be impossible in a distributed environment.

As said above, by using an affine variable/parameter x the programmer can safely rely on the fact that x denotes an isolated portion of memory. On the other hand, the capsule property should be preserved when x is used. This is ensured by the constraint that affine variables/parameters can be used at most once, and by a special reduction semantics, motivated and described below.

As already shown, for (non-affine) variable declarations reduction is as follows:

$$\begin{aligned} D \ x = \text{new } D(x); \ D \ y = \text{new } D(x); \ C \ w = \{D \ z = \text{new } D(z); \ \text{new } C(z, z)\}; \ w.f1 \longrightarrow \\ D \ x = \text{new } D(x); \ D \ y = \text{new } D(x); \ D \ z = \text{new } D(z); \ C \ w = \{\text{new } C(z, z)\}; \ w.f1 \cong \\ D \ x = \text{new } D(x); \ D \ y = \text{new } D(x); \ D \ z = \text{new } D(z); \ C \ w = \text{new } C(z, z); \ w.f1 \longrightarrow \dots \end{aligned}$$

That is, the block is flattened, hence the capsule property is lost. This corresponds to the fact that, if we get access to a portion of memory through an ordinary variable, then sharing could be introduced through such variable, hence, in particular, a portion of memory which was isolated is not guaranteed to remain such. To preserve the property, affine variables have a special semantics, which allow a capsule to be moved to another location in the memory, or passed as argument to a method. In the above example, reduction would be as follows:

$$\begin{aligned} D \ x = \text{new } D(x); \ D \ y = \text{new } D(x); \ C^a \ w = \{D \ z = \text{new } D(z); \ \text{new } C(z, z)\}; \ w.f1 \longrightarrow \\ D \ x = \text{new } D(x); \ D \ y = \text{new } D(x); \ \{D \ z = \text{new } D(z); \ \text{new } C(z, z)\}.f1 \longrightarrow \\ D \ x = \text{new } D(x); \ D \ y = \text{new } D(x); \ \{D \ z = \text{new } D(z); \ \text{new } C(z, z).f1\} \longrightarrow \\ D \ x = \text{new } D(x); \ D \ y = \text{new } D(x); \ \{D \ z = \text{new } D(z); \ z\} \longrightarrow \\ D \ z = \text{new } D(z); \ z \end{aligned}$$

Differently from the previous reduction, the block occurring as right-hand side of the declaration of w is *not* flattened, but, rather, used to replace w . That is, affine variables have a substitution semantics. Then, the field access is propagated inside the block to be performed.

In Sect.2 and Sect.3 we define the conventional and the syntactic calculus, respectively. In Sect.4 we show that the syntactic model can be encoded in the conventional one, hence efficiently implemented, and prove that the dynamic semantics is preserved by the encoding. Finally, in Sect.5 we draw some conclusions.

2 The conventional calculus

We illustrate our approach in the context of calculi with an object-oriented flavour, inspired by Featherweight Java [22] (FJ for short). This is only a presentation choice: the ideas and results of the paper could be rephrased in different imperative calculi, e.g., supporting data type constructors and reference types. For the same reason, we omit features such as inheritance and late binding, which are orthogonal to our focus.

The conventional calculus is given in Fig. 1. It is similar to other imperative variants of FJ which can be found in the literature [1, 6, 5]. We assume sets of *variables* x, y, z , *class names* C, D , *field names* f , and *method names* m . We adopt the convention that a metavariable which ends in s is implicitly defined as a (possibly empty) sequence in which elements may or may not be separated by commas. In particular, ds (and dvs in the next section) are sequences of d (and dv) and es, vs and xs are sequences of e, v and x separated by commas.

$e ::= x \mid e.f \mid e.f=e' \mid \text{new } C(es) \mid e.m(es) \mid \{ds\} e \mid \iota$	expression
$d ::= Cx=e;$	declaration
$v ::= \iota$	value
$\mathcal{E} ::= [] \mid \mathcal{E}.f \mid \mathcal{E}.f=e' \mid \iota.f=\mathcal{E} \mid \text{new } C(vs, \mathcal{E}, es) \mid \mathcal{E}.m(es) \mid \iota.m(vs, \mathcal{E}, es) \mid \{Cx=\mathcal{E}; ds\} e$	evaluation context
$(\text{ALPHA}) \{ds\} Cx=e; ds' e' \cong \{ds[y/x]\} Cy=e[y/x]; ds'[y/x] e'[y/x]$ $(\text{BLOCK-ELIM}) \{e\} \cong e$	
$(\text{CTX}) \frac{e \mu \Longrightarrow e' \mu'}{\mathcal{E}[e] \mu \Longrightarrow \mathcal{E}[e'] \mu'}$ $(\text{FIELD-ACCESS}) \iota.f_i \mu \Longrightarrow v_i \mu$ $\mu(\iota) = \text{new } C(v_1, \dots, v_n)$ $\text{fields}(C) = C_1 f_1 \dots C_n f_n \wedge 1 \leq i \leq n$	
$(\text{FIELD-ASSIGN}) \iota.f_i=v \mu \Longrightarrow v \mu^{\iota.i=v}$ $\mu(\iota) = \text{new } C(vs)$ $\text{fields}(C) = C_1 f_1 \dots C_n f_n \wedge 1 \leq i \leq n$	
$(\text{NEW}) \text{new } C(vs) \mu \Longrightarrow \iota \mu[\text{new } C(vs)/\iota] \quad \iota \notin \text{dom}(\mu)$	
$(\text{INVK}) \iota.m(v_1, \dots, v_n) \mu \Longrightarrow \{C_1 \text{this}=\iota; C_1 x_1=v_1; \dots C_n x_n=v_n; e\} \mu$ $\mu(\iota) = \text{new } C(vs)$ $\text{meth}(C, m) = \langle x_1 \dots x_n, e \rangle$	
$(\text{DEC}) \{Cx=\iota; ds\} e \mu \Longrightarrow \{ds\} e[\iota/x] \mu$	

Figure 1: Conventional calculus

An expression can be a variable (including the special variable `this` denoting the receiver in a method body), a field access, a field assignment, a constructor invocation, a method invocation, or a block consisting of a sequence of local variable declarations and a body. In addition, a (runtime) expression can be an *object identifier* ι . Blocks are included to have a more direct correspondence with the syntactic calculus. In a block, a declaration specifies a type (class name), a variable and an initialization expression. We assume that in well-formed blocks there are no multiple declarations for the same variable, that is, ds can be seen as a map from variables to expressions: $\text{dom}(ds)$ denotes the set of variables declared in ds and $ds(x)$ the initialization expression for x in ds , if any.

In the examples, we generally omit the brackets of the outermost block, and abbreviate $\{Tx=e; e'\}$

by $e; e'$ when x does not occur free in e' . We also assume integer constants, which are not included in the formalization.

Expressions are identified modulo congruence, denoted by \cong , defined as the smallest congruence satisfying the axioms in the mid section of Fig.1. Rule (ALPHA) is the usual α -conversion. The condition $x, y \notin \text{dom}(ds ds')$ is implicit by well-formedness of blocks. Rule (BLOCK-ELIM) identifies a block without declarations with its body.

The class table is abstractly modelled by the following functions:

- $\text{fields}(C)$ gives, for each declared class C , the sequence $C_1 f_1 \dots C_n f_n$ of its fields declarations.
- $\text{meth}(C, m)$ gives, for each method m declared in class C , the pair consisting of its parameters and body.

The reduction relation \Longrightarrow is defined on pairs $e|\mu$ where a *memory* μ is a finite map from object identifiers ι into object states of shape $\text{new } C(vs)$. Values are object identifiers (we do not identify the two sets since, extending the language, values would be extended to include, e.g., primitive values such as integers).

Evaluation contexts and reduction rules are straightforward. In rule (FIELD-ASSIGN) , we denote by $\mu^{i,v}$ the memory where the i -th field of the object state associated to ι has been replaced by v . In rule (INVK) , we take advantage of the block construct to provide a modular semantics, where a method call is reduced to a block where declarations of the appropriate type for `this` and the parameters are initialized with the receiver and the arguments, respectively, and the body is the method body. Indeed, this rule plus a sequence of applications of rule (DEC) is equivalent to the standard FJ rule $\iota.m(v_1, \dots, v_n)|\mu \Longrightarrow e[\iota/\text{this}][v_1/x_1 \dots v_n/x_n]|\mu$. Local variable declarations have the standard substitution semantics, and are elaborated in the usual left-to-right order (no recursion is allowed).

3 The syntactic calculus

The syntax of the expressions, given in Fig.2, is the same as the conventional calculus, except that runtime expressions (object identifiers) are not needed. To lighten the notation, we use the same metavariables.

e	$::= x \mid e.f \mid e.f=e' \mid \text{new } C(es) \mid e.m(es) \mid \{^X ds e\}$	expression
d	$::= Tx=e;$	declaration
T	$::= C^q$	declaration type
q	$::= \varepsilon \mid a$	optional qualifier
v	$::= x \mid \{^X dvs x\}$	value
dv	$::= Cx=\text{new } C(xs);$	evaluated declaration
\mathcal{E}	$::= [] \mid \mathcal{E}.f \mid \mathcal{E}.f=e' \mid x.f=\mathcal{E} \mid \text{new } C(xs, \mathcal{E}, es) \mid \mathcal{E}.m(es) \mid x.m(vs, \mathcal{E}, es) \mid \mathcal{E}_b$	evaluation context
\mathcal{E}_b	$::= \{^X dvs Cy=\mathcal{E}; ds e\} \mid \{^X dvs \mathcal{E}\}$	block context
\mathcal{E}_v	$::= [] .f \mid [] .f=e' \mid x.f=[] \mid \text{new } C(xs, [], es) \mid [] .m(es)$	value context

Figure 2: Syntactic calculus: syntax, values, and evaluation contexts

Moreover, some annotations are inserted in terms. Namely:

- Local variable declarations (and method parameters) are possibly annotated with a qualifier a , which, if present, indicates that the variable is *affine*. An affine variable can occur at most once in its scope, and should be initialized with a *capsule*, that is, an isolated portion of store. In this

way, it can be used as a temporary reference, to “move” a capsule to another location in the store, without introducing sharing.

- Blocks are annotated with a set X of variables, assumed to be a subset of the declared variables. During reduction, if a block $\{^X ds e\}$ should reduce to a capsule, only declarations of variables which are not in X can be safely moved outside of the block, see rule (MOVE-DEC). In this paper, since our focus is on the operational model, we do not care about how block annotations are generated. Of course, a trivial overapproximation consists in taking as X the set of all declared variables; a better approximation is taking only those which are used (that is, have some free occurrence in initialization expressions/body), or, even better, only those which are transitively used by the body, in the sense formally defined below. We have shown in previous work [17, 16, 18] that through a type and effect system it is possible to obtain a much more precise approximation, computing X to be the set of the variables which *will be possibly connected with the final result of the block*.

A sequence dvs of *evaluated declarations* plays the role of the memory in the conventional calculus, that is, each dv can be seen as an association of an *object state* $\text{new } C(xs)$ to a reference.

A value is a reference to an object, possibly enclosed in a block where all declarations are evaluated (hence, correspond to a local memory).

We assume that, in a block value $\{^X dvs x\}$, $dvs \neq \varepsilon$ and $dvs|_x = dvs$, where, given a sequence of declarations $ds \equiv T_1 x_1 = e_1; \dots T_n x_n = e_n$; and an expression e , $ds|_e$ are the declarations of variables (transitively) used by e , that is, free either in e or in some e_i such that x_i is transitively used by e .

We write $FV(ds)$ and $FV(e)$ for the free variables of a sequence of declarations and of an expression, respectively, and $X[y/x]$, $ds[y/x]$, and $e[y/x]$ for the capture-avoiding variable substitution on a set of variables, a sequence of declarations, and an expression, respectively, all defined in the standard way.

In the syntactic calculus, capsules can be characterized in a very simple way: indeed, a value is a capsule, written $\text{caps}(v)$, if it is a closed block value, that is, of shape $\{dvs x\}$ with no free variables. The above requirement that all local variables must be transitively used by x is needed, indeed, since otherwise a block value containing unused free variables, e.g., $\{Cx = \text{new } C(); Dy = \text{new } D(z); x\}$ would be not recognized to be a capsule. Unused evaluated declarations are removed by rule (GARBAGE).

Evaluation contexts \mathcal{E} are mostly standard. Note that values are assumed to be references, apart from arguments of method calls, which are allowed to be block values. This models the fact that block values (hence, capsules) are first-class values which can be passed to methods. However, they need to be “opened” when we perform an actual operation on them. We distinguish, among evaluation context, *block contexts*, \mathcal{E}_b , having the shape of a block, which play a special role in the reduction rules.

The *hole binders* of a context \mathcal{E} , dubbed $\text{HB}(\mathcal{E})$, are the variables bound by the context, defined by:

- $\text{HB}([\]) = \emptyset$, $\text{HB}(\mathcal{E}.f) = \dots = \text{HB}(x.m(vs, \mathcal{E}, es)) = \text{HB}(\mathcal{E})$
- $\text{HB}(\{^X dvs Cy = \mathcal{E}; ds e\}) = \text{dom}(dvs ds) \cup \{y\} \cup \text{HB}(\mathcal{E})$ and $\text{HB}(\{^X dvs \mathcal{E}\}) = \text{dom}(dvs) \cup \text{HB}(\mathcal{E})$.

Moreover, given $\mathcal{E}_b = \{^X dvs Cy = \mathcal{E}; ds e\}$ or $\mathcal{E}_b = \{^X dvs \mathcal{E}\}$, we define

- $\text{get}(\mathcal{E}_b, x) = dvs(x)$, i.e., the object state associated to x in dvs , if $x \in \text{dom}(dvs)$, and
- $\text{inner}(\mathcal{E}_b) = \text{HB}(\mathcal{E})$, i.e., the set of variables declared in the direct subcontext \mathcal{E} of \mathcal{E}_b .

A *value context* \mathcal{E}_v is an evaluation context with the shape of either a field access, or a field assignment, or a constructor invocation, or a method invocation, where the hole (expected to be filled with a block value) is a direct subterm (the receiver in the last case).

Expressions are identified modulo congruence, denoted by \cong , defined as the smallest congruence satisfying the axioms in Fig.3. Rules (ALPHA) and (BLOCK-ELIM) are as in the conventional calculus. Rule

(ALPHA) $\{^X ds Cx=e; ds' e'\} \cong \{^{X[y/x]} ds[y/x] Cy=e[y/x]; ds'[y/x] e'[y/x]\}$	(BLOCK-ELIM) $\{\emptyset e\} \cong e$
(REORDER) $\{^X ds dv ds' e\} \cong \{^X dv ds ds' e\}$	

Figure 3: Syntactic calculus: congruence rules

(REORDER) states that we can move evaluated declarations in an arbitrary order. Note that, instead, ds and ds' cannot be swapped, because this could change the order of side effects.

Reduction rules are given in Fig.4. We explicitly distinguish the relation \xrightarrow{c} defined by *computational rules* only, and reduction \longrightarrow , defined as its contextual closure. In other words, in rule (CTX) we assume that \mathcal{E} is a maximal context. This simplifies proofs in Sect.4. More importantly, in this way we can prevent reduction of a constructor call in a declaration context, see comments to rule (NEW) below.

(CTX) $\frac{e \xrightarrow{c} e'}{\mathcal{E}[e] \longrightarrow \mathcal{E}[e']}$	(NEW) $\mathcal{E}[\mathbf{new} C(xs)] \longrightarrow \mathcal{E}[\{\{^x\} Cx=\mathbf{new} C(xs); x\}] \quad \mathcal{E} \neq \mathcal{E}'[\{^X dvs Cy=[]; ds e\}]$
(FIELD-ACCESS) $\mathcal{E}_b[x.f_i] \xrightarrow{c} \mathcal{E}_b[x_i]$	$\begin{aligned} \text{get}(\mathcal{E}_b, x) &= \mathbf{new} C(x_1, \dots, x_n) \wedge x \notin \text{inner}(\mathcal{E}_b) \\ \text{fields}(C) &= C_1 f_1 \dots C_n f_n \wedge 1 \leq i \leq n \\ x_i &\notin \text{inner}(\mathcal{E}_b) \end{aligned}$
(FIELD-ASSIGN) $\mathcal{E}_b[x.f_i=y] \xrightarrow{c} \mathcal{E}_b^{x_i=y}[y]$	$\begin{aligned} \text{get}(\mathcal{E}_b, x) &= \mathbf{new} C(xs) \wedge x \notin \text{inner}(\mathcal{E}_b) \\ \text{fields}(C) &= C_1 f_1 \dots C_n f_n \wedge 1 \leq i \leq n \\ y &\notin \text{inner}(\mathcal{E}_b) \end{aligned}$
(INVK) $\mathcal{E}_b[x.m(v_1, \dots, v_n)] \xrightarrow{c} \mathcal{E}_b[\{C \mathbf{this}=x; C_1^{q_1} x_1=v_1; \dots, C_n^{q_n} x_n=v_n; e\}]$	$\begin{aligned} \text{get}(\mathcal{E}_b, x) &= \mathbf{new} C(xs) \\ x &\notin \text{inner}(\mathcal{E}_b) \\ \text{meth}(C, m) &= (C_1^{q_1} x_1, \dots, C_n^{q_n} x_n, e) \end{aligned}$
(ALIAS-ELIM) $\{^X dvs Cx=y; ds e\} \xrightarrow{c} \{^{X \setminus \{x\}} dvs ds[y/x] e[y/x]\}$	
(AFFINE-ELIM) $\{^X dvs C^a x=v; ds e\} \xrightarrow{c} \{^{X \setminus \{x\}} dvs ds[v/x] e[v/x]\} \quad \text{caps}(v)$	
(GARBAGE) $\{^X dvs ds e\} \xrightarrow{c} \{^{X \setminus \text{dom}(dvs)} ds e\} \quad (\text{FV}(ds) \cup \text{FV}(e)) \cap \text{dom}(dvs) = \emptyset$	
(MOVE-DEC) $\{^Y dvs C^a x=\{^X dvs' ds e\}; ds' e'\} \xrightarrow{c} \{^Y dvs dvs' C^a x=\{^X ds e\}; ds' e'\}$	$\begin{aligned} \text{FV}(dvs') \cap \text{dom}(ds) &= \emptyset \\ \text{FV}(dvs ds' e') \cap \text{dom}(dvs') &= \emptyset \\ q = a &\Rightarrow \text{dom}(dvs') \cap X = \emptyset \end{aligned}$
(MOVE-BODY) $\{^Y dvs \{^X dvs' ds e\}\} \xrightarrow{c} \{^Y dvs dvs' \{^X ds_2 e\}\}$	$\begin{aligned} \text{FV}(dvs') \cap \text{dom}(ds) &= \emptyset \\ \text{FV}(dvs) \cap \text{dom}(dvs') &= \emptyset \end{aligned}$
(MOVE-SUBTERM) $\mathcal{E}_v[\{^X dvs dvs' x\}] \xrightarrow{c} \{^{X \cap \text{dom}(dvs)} dvs \mathcal{E}_v[\{^{X \setminus \text{dom}(dvs)} dvs' x\}]\}$	$\begin{aligned} \text{FV}(dvs) \cap \text{dom}(dvs') &= \emptyset \\ \text{FV}(\mathcal{E}_v) \cap \text{dom}(dvs) &= \emptyset \end{aligned}$

Figure 4: Syntactic calculus: reduction rules

Rule (CTX) is the usual contextual closure.

In rule (NEW), a constructor invocation where all arguments are references is reduced to an elementary block where a new object is allocated. However, this reduction is not allowed when the constructor invocation occurs as right-hand side of a declaration, to prevent non-terminating reduction sequences

such as the following:

$$\{Cx=\text{new } C(x); x\} \longrightarrow \{Cx=\{Cx=\text{new } C(x); x\}; x\} \longrightarrow \dots$$

Note that, if the constructor invocation occurs, instead, on the right-side of a declaration of an affine variable, the rule is applicable and does not produce a non-terminating reduction sequence. For instance:

$$\{C^a x=\text{new } C(x); x\} \longrightarrow \{C^a x=\{Cx=\text{new } C(x); x\}; x\}$$

and rule (NEW) is no longer applicable.

In rule (FIELD-ACCESS), a field access of shape $x.f$ is evaluated in the block context containing the first enclosing (evaluated) declaration for x , as expressed by the first side condition and the definition of $\text{get}(\mathcal{E}_b, x)$. The fields of the class C of x are retrieved from the class table. If f is the name of a field of C , say, the i -th, then the field access is reduced to the reference x_i stored in this field. The condition $x_i \notin \text{inner}(\mathcal{E}_b)$ ensures that there are no inner declarations for x_i (otherwise x_i would be erroneously bound). This can always be obtained by rule (ALPHA) of Fig.3. For instance, assuming a class table where class A has an `int` field, and class B has an `A` field `f`, without this side condition, the term:

```
A a=new A(0); B b=new B(a); {A a=new A(1); b.f}
```

would reduce to

```
A a=new A(0); B b=new B(a); {A a=new A(1); a}
```

whereas this reduction is forbidden by the side condition. However, by rule (ALPHA) of Fig.3, the term is congruent to one that can be reduced to

```
A a=new A(0); B b=new B(a); {A a1=new A(1); a}
```

In rule (FIELD-ASSIGN), a field assignment of shape $x.f=y$ is evaluated in the block context containing the first enclosing (evaluated) declaration for x , as expressed by the first side condition. The fields of the class C of x are retrieved from the class table. If f is the name of a field of C , say, the i -th, then this first enclosing declaration is updated, by replacing the i -th constructor argument by y obtaining the declaration $Cx=\text{new } C(x_1, x_{i-1}, y, x_{i+1}, \dots, x_n)$; as expressed by the notation $\mathcal{E}_b^{x.i=y}$ (whose obvious formal definition is omitted). Analogously to rule (FIELD-ACCESS), we have the side condition that $y \notin \text{inner}(\mathcal{E}_b)$. This side condition, requiring that there are no inner declarations for y , prevents scope extrusion, since if $y \in \text{inner}(\mathcal{E}_b)$, $\mathcal{E}_b^{x.i=y}$ would take y outside the scope of its definition. For example, without this side condition, the term

```
A a=new A(0); B b=new B(a); {A a1=new A(1); b.f=a1}
```

would reduce to

```
A a=new A(0); B b=new B(a1); {A a1=new A(1); a1}
```

which is not correct since `a1` is a free variable. The rules (MOVE-DEC) and (MOVE-BODY) (see below) can be used to move the declaration of y outside its declaration block. So the term reduces, instead, to

```
A a=new A(0); B b=new B(a); A a1=new A(1); b.f=a1
```

by applying first rule (MOVE-BODY), and then congruence rule (BLOCK-ELIM). Now the term correctly reduces to

```
A a=new A(0); B b=new B(a1); A a1=new A(1); a1
```

In rule (INVK), a method call of shape $x.m(v_1, \dots, v_n)$ is evaluated in the block context containing the first enclosing (evaluated) declaration for x , as expressed by the first side condition. Method m of C , if any, is retrieved from the class table. The call is reduced to a block where declarations of the appropriate type for `this` and the parameters are initialized with the receiver and the arguments, respectively, and

the body is the method body. If a parameter is affine, then the corresponding argument will be checked to be a capsule when the formal parameter will be substituted with the associated value by rule (AFFINE-ELIM), see below. We assume that parameters which are affine occur at most once in the body of the method.

The following two rules eliminate declarations from a block.

In rule (ALIAS-ELIM), a reference (non affine variable) x which is initialized as an alias of another reference y is eliminated by replacing all its occurrences. In rule (AFFINE-ELIM), an affine variable is eliminated by replacing its unique occurrence with the value associated to its declaration. The rule can only be applied if such value is a capsule. Such side condition formally models that execution includes a runtime check in this case, as it happens, e.g., in Java downcasts. Note also that, even ignoring the a qualifier in the latter, the two rules do not overlap, since a reference y is trivially not a capsule.

Rule (GARBAGE) states that we can remove an unused sequence of evaluated declarations from a block. Note that it is only possible to safely remove declarations which are evaluated, since they do not have side effects.

With the remaining rules we can move a sequence of evaluated declarations from a block to the directly enclosing block, as it happens with rules for *scope extension* in the π -calculus [24].

In rules (MOVE-DEC) and (MOVE-BODY), the inner block is the right-hand side of a declaration, or the body, respectively, of the enclosing block. The first two side conditions ensure that moving the declarations dvs' does cause neither scope extrusion nor capture of free variables. More precisely: the first prevents moving outside a declaration dvs' which depends on local variables of the inner block. The second prevents capturing with dvs' free variables of the enclosing block. Note that the second condition can be obtained by α -conversion of the inner block, but the first cannot. Finally, when the block initializes an affine variable, the third side condition of rule (DEC) forbids to move outside the block declarations of variables that are in the annotation X of the block. Indeed, annotations can be rough or very precise, as discussed before, but in any case such that variables not in X cannot be possibly connected to the final result of the block, hence can be safely moved outside without “breaking” the capsule property (that the block should ultimately reduce to a closed expression). In case of a non affine declaration, instead, this is not a problem.

Rule (MOVE-SUBTERM) handles the cases when the inner block is a subterm of a field access, field assignment, constructor invocation, or method invocation. Note that in this case the inner block is necessarily a (block) value. We use value contexts to express all such cases in a compact way.

4 Preservation of semantics

In this section, for clarity, we use \hat{e} and \hat{ds} to range over expressions and sequences of declarations of the conventional calculus, which could include object identifiers.

We show that, if an expression has a reduction sequence in the syntactic calculus, then it has an “equivalent” reduction sequence in the conventional calculus. Note that the converse does not hold, since an expression which is stuck in the syntactic calculus, since a capsule runtime check (side condition of rule (AFFINE-ELIM)) fails, could reduce in the conventional calculus. That is, in the syntactic calculus, by declaring x affine, the programmer can rely on the fact that during computation x will always denote an isolated portion of memory², otherwise an exception would be raised.

In order to state the preservation results (Theorem 1 and Corollary 1), we define a *matching* relation $\hat{e} \rightsquigarrow^p$ between expressions e of the syntactic calculus and pairs $\hat{e}|\mu$ of the conventional calculus. The

²Hence, nobody else in the program can affect memory reachable from x , hence such memory can be safely handled by a thread.

relation is labelled by an injective mapping ρ from object identifiers in the domain of μ to variables. Intuitively, $e \overset{\rho}{\rightsquigarrow} \hat{e}|\mu$ holds if variables in the image of ρ are all those declared in evaluated declarations in e and all such declarations are removed in \hat{e} . More precisely, since the same variable could be declared in different blocks inside an expression, the mapping ρ should be from object identifiers to *binding occurrences* of variables. To make the formal treatment simpler, we can assume that each variable is declared at most once in expressions of the syntactic calculus. This can be obtained by α -renaming.

Formally the relation is inductively defined by the rules in Fig.5.

A variable in the syntactic calculus is matched in the conventional calculus by a pair where the expression is the corresponding object identifier in ρ , if any, rule (OID), otherwise the variable itself, rule (VAR). The former case happens when the variable declaration is evaluated in the syntactic calculus.

Rules (FIELD-ACCESS), (FIELD-ASSIGN), (NEW), and (INVK) just propagate matching to subterms. For $es = e_1, \dots, e_n$, $\hat{es} = \hat{e}_1, \dots, \hat{e}_n$, we use $es \overset{\rho}{\rightsquigarrow} \hat{es}|\mu$ to abbreviate $e_i \overset{\rho}{\rightsquigarrow} \hat{e}_i|\mu \ \forall i \in 1..n$.

In rule (BLOCK), a block $\{^x dvs \ ds \ e\}$ in the syntactic calculus is matched by a block and memory $\{\hat{ds} \ \hat{e}\}|\mu$ of the conventional calculus if evaluated declarations dvs are matched by memory μ , as expressed by the auxiliary judgment $dvs \overset{\rho}{\rightsquigarrow} \mu$, and matching is propagated to other subterms. For $ds = d_1 \dots d_n$, $\hat{ds} = \hat{d}_1 \dots \hat{d}_n$, we use $ds \overset{\rho}{\rightsquigarrow} \hat{ds}|\mu$ to abbreviate $d_i \overset{\rho}{\rightsquigarrow} \hat{d}_i|\mu \ \forall i \in 1..n$, and analogously for $dvs \overset{\rho}{\rightsquigarrow} \mu$.

(OID) $\frac{}{x \overset{\rho}{\rightsquigarrow} \iota \mu} \ \rho(\iota) = x$	(VAR) $\frac{}{x \overset{\rho}{\rightsquigarrow} x \mu} \ x \notin \text{img}(\rho)$
(FIELD-ACCESS) $\frac{e \overset{\rho}{\rightsquigarrow} \hat{e} \mu}{e.f \overset{\rho}{\rightsquigarrow} \hat{e}.f \mu}$	(FIELD-ASSIGN) $\frac{e \overset{\rho}{\rightsquigarrow} \hat{e} \mu \quad e' \overset{\rho}{\rightsquigarrow} \hat{e}' \mu}{e.f=e' \overset{\rho}{\rightsquigarrow} \hat{e}.f=\hat{e}' \mu}$
(NEW) $\frac{es \overset{\rho}{\rightsquigarrow} \hat{es} \mu}{\text{new } C(es) \overset{\rho}{\rightsquigarrow} \text{new } C(\hat{es}) \mu}$	(INVK) $\frac{e \overset{\rho}{\rightsquigarrow} \hat{e} \mu \quad es \overset{\rho}{\rightsquigarrow} \hat{es} \mu}{e.m(es) \overset{\rho}{\rightsquigarrow} \hat{e}.m(\hat{es}) \mu}$
(BLOCK) $\frac{dvs \overset{\rho}{\rightsquigarrow} \mu \quad ds \overset{\rho}{\rightsquigarrow} \hat{ds} \mu \quad e \overset{\rho}{\rightsquigarrow} \hat{e} \mu}{\{^x dvs \ ds \ e\} \overset{\rho}{\rightsquigarrow} \{\hat{ds} \ \hat{e}\} \mu}$	(DEC) $\frac{e \overset{\rho}{\rightsquigarrow} \hat{e} \mu}{C^q x=e; \overset{\rho}{\rightsquigarrow} Cx=\hat{e}; \mu} \ C^q x=e; \neq dv$
(EV-DEC) $\frac{}{Cx=\text{new } C(x_1, \dots, x_n); \overset{\rho}{\rightsquigarrow} \mu} \ \mu(\rho^{-1}(x)) = \text{new } C(\rho^{-1}(x_1), \dots, \rho^{-1}(x_n))$	

Figure 5: Matching relation between terms

The matching relation can be extended, in the obvious way, to evaluation contexts of the syntactic calculus and pairs evaluation context and memory of the conventional calculus, i.e., $\mathcal{E} \overset{\rho}{\rightsquigarrow} \hat{\mathcal{E}}|\mu$. The formal definition is given in Fig.6.

It is easy to show the following lemma.

Lemma 1. $\mathcal{E}[e] \overset{\rho}{\rightsquigarrow} \hat{\mathcal{E}}|\mu$ if and only if $\hat{e}' = \hat{\mathcal{E}}[\hat{e}]$ such that $\mathcal{E} \overset{\rho}{\rightsquigarrow} \hat{\mathcal{E}}|\mu$ and $e \overset{\rho}{\rightsquigarrow} \hat{e}|\mu$.

Note that, when $\mathcal{E}[e]$ is closed, all the free variables in e are declared in \mathcal{E} and their declaration is evaluated. Therefore, the previous lemma implies that they are in the image of ρ , and so in \hat{e} they match object identifiers.

The following lemma asserts the conditions on which a value in the syntactic calculus is matched by a pairs of value and memory in the conventional one.

Lemma 2. Let v be such that $v \overset{\rho}{\rightsquigarrow} \hat{e}|\mu$ for some \hat{e} , ρ and μ . Then:

1. if $v = x$, then either $\hat{e} = \iota$ for some ι and $\rho(\iota) = x$, or $\hat{e} = x$

$$\begin{array}{c}
\text{(C-EMPTY)} \frac{}{[] \rightsquigarrow []|\mu} \quad \text{(C-FIELD-ACCESS)} \frac{\mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu}{\mathcal{E}.f \rightsquigarrow \widehat{\mathcal{E}}.f|\mu} \\
\text{(C-FIELD-ASSIGN-L)} \frac{\mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu \quad e \rightsquigarrow \widehat{e}|\mu}{\mathcal{E}.f=e \rightsquigarrow \widehat{\mathcal{E}}.f=\widehat{e}|\mu} \quad \text{(C-FIELD-ASSIGN-R)} \frac{\mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu \quad x \rightsquigarrow \iota|\mu}{x.f=\mathcal{E} \rightsquigarrow \iota.f=\widehat{\mathcal{E}}|\mu} \\
\text{(C-NEW)} \frac{\mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu \quad es \rightsquigarrow \widehat{es}|\mu \quad xs \rightsquigarrow \iota_1, \dots, \iota_n|\mu}{\text{new } C(xs, \mathcal{E}, es) \rightsquigarrow \text{new } C(\iota_1, \dots, \iota_n, \widehat{\mathcal{E}}, \widehat{es})|\mu} \\
\text{(C-INVK-RCV)} \frac{\mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu \quad es \rightsquigarrow \widehat{es}|\mu}{\mathcal{E}.m(es) \rightsquigarrow \widehat{\mathcal{E}}.m(\widehat{es})|\mu} \quad \text{(C-INVK-ARG)} \frac{\mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu \quad es \rightsquigarrow \widehat{es}|\mu \quad vs \rightsquigarrow \iota_1, \dots, \iota_n|\mu}{x.m(vs, \mathcal{E}, es) \rightsquigarrow \iota.m(\iota_1, \dots, \iota_n, \widehat{\mathcal{E}}, \widehat{es})|\mu} \\
\text{(C-BLK-DEC)} \frac{dvs \rightsquigarrow \mu \quad \mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu \quad ds \rightsquigarrow \widehat{ds}|\mu \quad e \rightsquigarrow \widehat{e}|\mu}{\{^X dvs \ Cy=\mathcal{E}; \ ds \ e\} \rightsquigarrow \{^X Cy=\widehat{\mathcal{E}}; \ \widehat{ds} \ \widehat{e}\}|\mu} \quad \text{(C-BLK-BODY)} \frac{dvs \rightsquigarrow \mu \quad \mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu}{\{^X dvs \ \mathcal{E}\} \rightsquigarrow \widehat{\mathcal{E}}|\mu}
\end{array}$$

Figure 6: Matching relation between evaluation contexts

2. if $v = \{^X dvs \ x\}$, then $\widehat{e} = \iota$ and $\rho(\iota) = x$.

Proof. 1. The judgment $x \rightsquigarrow \widehat{e}|\mu$ has been necessarily derived by rule either (OID) or (VAR) in Fig.5.

2. First observe that dvs cannot be empty and that $Cx=\text{new } C(xs)$; must be in dvs . The judgment $\{^X dvs \ x\} \rightsquigarrow \widehat{e}|\mu$ has been necessarily derived by rule (BLOCK) in Fig.5. Therefore $dvs \rightsquigarrow \mu$, and, since for each declaration in dvs we have applied rule (EV-DEC), all the variables in dvs must be in the image of ρ and $\widehat{e} = \iota$ such that $\rho(\iota) = x$. □

From the previous lemma we have that, if all the free variables of v are in the image of ρ , then v can only match an object identifier.

A step in the reduction of a closed expression e in the syntactic calculus can be simulated by a possibly empty sequence of reduction steps of the matching configuration $\widehat{e}|\mu$ in the conventional calculus.

Theorem 1. *If $FV(e) = \emptyset$, $e \rightsquigarrow \widehat{e}|\mu$, and $e \longrightarrow e'$, then $\widehat{e}|\mu \Longrightarrow^* \widehat{e}'|\mu'$ such that $e' \rightsquigarrow \widehat{e}'|\mu'$, for some \widehat{e}' , ρ' , μ' such that $\rho \subseteq \rho'$, $\text{dom}(\mu) \subseteq \text{dom}(\mu')$.*

Proof. If $e \longrightarrow e'$, then either rule (CTX) or rule (NEW) of Fig.4 were applied.

Consider first rule (CTX). Then $e = \mathcal{E}[e_1]$, $e' = \mathcal{E}[e'_1]$ and $e_1 \xrightarrow{c} e'_1$. From $e \rightsquigarrow \widehat{e}|\mu$ and Lemma 1 we have that $\widehat{e} = \widehat{\mathcal{E}}[\widehat{e}_1]$ where $\mathcal{E} \rightsquigarrow \widehat{\mathcal{E}}|\mu$ and $e_1 \rightsquigarrow \widehat{e}_1|\mu$.

By cases on the reduction rule of Fig.4 applied to reduce e_1 to e'_1 . We consider (FIELD-ASSIGN), (AFFINE-ELIM), (MOVE-DEC) and (MOVE-SUBTERM). The proof for the other rules is similar.

Rule (FIELD-ASSIGN). Then

(i) $e_1 = \mathcal{E}_b[x.f_i=y]$,

(ii) $e'_1 = \mathcal{E}_b^{x.i=y}[y]$,

(iii) $\text{get}(\mathcal{E}_b, x) = \text{new } C(x_1, \dots, x_n)$, and

(iv) $\text{fields}(C) = C_1.f_1 \dots C_n.f_n \wedge 1 \leq i \leq n$.

From $e_1 \xrightarrow{\rho} \hat{e}_1|\mu$ and Lemma 1 we have that $\hat{e}_1 = \hat{\mathcal{E}}_b[\hat{e}_2]$ with $\mathcal{E}_b \xrightarrow{\rho} \hat{\mathcal{E}}_b|\mu$ and $x.f_i=y \xrightarrow{\rho} \hat{e}_2|\mu$ for some \hat{e}_2 . Since e is a closed term we get that x and y are defined in the evaluated declarations of $\mathcal{E}[\mathcal{E}_b]$. Therefore \hat{e}_2 is $\iota.f_i=\iota'$ for some ι and ι' such that $\rho(\iota) = x$ and $\rho(\iota') = y$. Moreover, from rules (BLOCK) and (EV-DEC) and (iii), it must be $\mu(\iota) = \text{new } C(\iota_1, \dots, \iota_n)$ for some ι_i such that $\rho(\iota_i) = x_i$ for $i \in 1, \dots, n$. From (iv) and rule (CTX) with premise (INVK) of Fig.1 we get $\hat{\mathcal{E}}_b[\iota.f_i=\iota']|\mu \Longrightarrow \hat{\mathcal{E}}_b[\iota']|\mu^{\iota.i=\iota'}$. Since we have assumed no shadowing of variables, in \mathcal{E} there is no declaration of x and so

$$(a) \mathcal{E} \xrightarrow{\rho} \hat{\mathcal{E}}|\mu^{\iota.i=\iota'}$$

From $\mathcal{E}_b \xrightarrow{\rho} \hat{\mathcal{E}}_b|\mu$, $\rho(\iota) = x$, $\rho(\iota') = y$ and $\mu(\iota) = \text{new } C(\iota_1, \dots, \iota_n)$ we get

$$(b) \mathcal{E}_b^{x.i=y} \xrightarrow{\rho} \hat{\mathcal{E}}_b|\mu^{\iota.i=\iota'}$$

Finally from (a), (b), $\rho(\iota') = y$ and Lemma 1 we derive that $\mathcal{E}[\mathcal{E}_b^{x.i=y}[y]] \xrightarrow{\rho} \hat{\mathcal{E}}[\hat{\mathcal{E}}_b[\iota']|\mu^{\iota.i=\iota'}$.

Rule (AFFINE-ELIM). Then

- (i) $e_1 = \{^X dvs \ C^a x=v; \ ds \ e_b\}$,
- (ii) $e'_1 = \{^{X \setminus \{x\}} dvs \ ds[v/x] \ e_b[v/x]\}$ and
- (iii) $\text{caps}(v)$.

From (iii) v is closed and so $v = \{^Y dvs' \ y\}$ for some Y , dvs' , and y . From $e_1 \xrightarrow{\rho} \hat{e}_1|\mu$, (i), rule (BLOCK) of Fig.5, Lemma 2.2 we have that

$$(a) \hat{e}_1 = \{C x=\iota; \ \widehat{ds} \ \widehat{e}_b\}, \ dvs \ dvs' \xrightarrow{\rho} \mu, \ ds \xrightarrow{\rho} \widehat{ds}|\mu, \ e_b \xrightarrow{\rho} \widehat{e}_b|\mu,$$

$$(b) \rho(\iota) = y \text{ and } v \xrightarrow{\rho} \iota|\mu.$$

Applying reduction rule (DEC) of Fig.1 we get $\{C x=\iota; \ \widehat{ds} \ \widehat{e}_b\}|\mu \Longrightarrow \{\widehat{ds} \ \widehat{e}_b\}[\iota/x]|\mu$. Since $C^a x=v$; is not an evaluated declaration $x \notin \text{img}(\rho)$. Therefore the occurrence of x in e_1 is in the matching relation with an occurrence of x in \hat{e}_1 and there is only one such occurrence. Therefore from (a) and (b) we have

$$(c) \{^{X \setminus \{x\}} dvs \ ds[v/x] \ e_b[v/x]\} \xrightarrow{\rho} \{\widehat{ds} \ \widehat{e}_b\}[\iota/x]|\mu.$$

From $\mathcal{E} \xrightarrow{\rho} \hat{\mathcal{E}}|\mu$, (i), (a), (c) and Lemma 1 we derive that $\mathcal{E}[e_1] \xrightarrow{\rho} \mathcal{E}[\hat{e}_1]|\mu$.

Rule (MOVE-DEC). Then

- (i) $e_1 = \{^Y dvs \ C^q x=\{^X dvs' \ ds \ e_b\}; \ ds' \ e'\}$ and
- (ii) $e'_1 = \{^Y dvs \ dvs' \ C^q x=\{^X ds \ e_b\}; \ ds' \ e'\}$

We consider two cases:

1. either $\{^X ds \ e_b\} \cong \text{new } C(x_1, \dots, x_n)$ for some x_1, \dots, x_n
2. or this is not the case.

Case 1. Then

$$(iii) e_1 = \{^Y dvs \ C^q x=\{^X dvs' \ \text{new } C(x_1, \dots, x_n)\}; \ ds' \ e'\} \text{ and}$$

$$(iv) e'_1 = \{^Y dvs \ dvs' \ C^q x=\text{new } C(x_1, \dots, x_n); \ ds' \ e'\}.$$

From $e_1 \xrightarrow{\rho} \hat{e}_1|\mu$, Lemma 1 and rules (NEW) and (BLOCK) of Fig.5 we have that

$$(a) \hat{e}_1 = \{C x=\text{new } C(\iota_1, \dots, \iota_n); \ \widehat{ds}' \ \widehat{e}'\},$$

$$(b) dvs \ dvs' \xrightarrow{\rho} \mu, \ ds' \xrightarrow{\rho} \widehat{ds}'|\mu, \ e' \xrightarrow{\rho} \widehat{e}'|\mu \text{ and}$$

$$(c) \rho(\iota_i) = x_i \text{ for } i \in 1, \dots, n.$$

Applying reduction rule (NEW) of Fig.1 we have that $\text{new } C(t_1, \dots, t_n) | \mu \Longrightarrow \iota | \mu'$ where $\iota \notin \text{dom}(\mu)$ and $\mu' = \mu[\text{new } C(t_1, \dots, t_n) / \iota]$. Then, applying rule (BLOCK) of Fig.1 we get $\{Cx=\iota; \widehat{ds}' \hat{e}'\} | \mu' \Longrightarrow \{\widehat{ds}'[\iota/x] \hat{e}'[\iota/x]\} | \mu'$. Let $\rho' = \rho[x/\iota]$, from (iv), (b), (c) and rule (BLOCK) of Fig.5 we get that $e'_1 \xrightarrow{\rho'} \{\widehat{ds}'[\iota/x] \hat{e}'[\iota/x]\} | \mu'$, and so by Lemma 1 we derive $\mathcal{E}[e'_1] \xrightarrow{\rho'} \widehat{\mathcal{E}}[\{\widehat{ds}'[\iota/x] \hat{e}'[\iota/x]\} | \mu']$ where $\rho \subseteq \rho'$ and $\text{dom}(\mu) \subseteq \text{dom}(\mu')$.

Case 2. In this case from $e_1 \xrightarrow{\rho} \hat{e}_1 | \mu$, Lemma 1 and rule (BLOCK) of Fig.5 we get

(d) $\hat{e}_1 = \{Cx=\widehat{ds e_b}\}; \widehat{ds}' \hat{e}'\}$ where

(e) $dvs dvs' \xrightarrow{\rho} \mu$, $ds' \xrightarrow{\rho} \widehat{ds}' | \mu$, $e' \xrightarrow{\rho} \hat{e}' | \mu$, and $\{ds e_b\} \xrightarrow{\rho} \{\widehat{ds e_b}\} | \mu$

From (ii), (d), (e) and rule (BLOCK) of Fig.5 we derive that $e'_1 \xrightarrow{\rho} \hat{e}'_1 | \mu$ and by Lemma 1 we have $\mathcal{E}[e'_1] \xrightarrow{\rho} \widehat{\mathcal{E}}[\hat{e}'_1] | \mu$. Since $\widehat{\mathcal{E}}[\hat{e}'_1] | \mu$ reduces in 0 steps to itself we get the result.

Rule (MOVE-SUBTERM). We consider the value context $\text{new } C(x_1, \dots, x_n, [], es)$. The other contexts are similar and easier. Then

(i) $e_1 = \text{new } C(x_1, \dots, x_n, \{^X dvs dvs' x\}, es)$ and

(ii) $e'_1 = \{^{X \cap \text{dom}(dvs)} dvs \text{ new } C(x_1, \dots, x_n, \{^X dvs' x\}, es)\}$.

From $e_1 \xrightarrow{\rho} \hat{e}_1 | \mu$, (i), rule (NEW) and rule (BLOCK) of Fig.5, we have that

(a) $\hat{e}_1 = \text{new } C(t_1, \dots, t_n, \iota, \widehat{es})$,

(b) $dvs dvs' \xrightarrow{\rho} \mu$, $x_1, \dots, x_n \xrightarrow{\rho} t_1, \dots, t_n | \mu$, $\{^X dvs dvs' x\} \xrightarrow{\rho} \iota | \mu$ and $es \xrightarrow{\rho} \widehat{es} | \mu$.

From (b) we derive that $\{^X dvs' x\} \xrightarrow{\rho} \iota | \mu$. Therefore

(c) $\{^{X \cap \text{dom}(dvs)} dvs \text{ new } C(x_1, \dots, x_n, \{^X dvs' x\}, es)\} \xrightarrow{\rho} \text{new } C(t_1, \dots, t_n, \iota, \widehat{es}) | \mu$.

From $\mathcal{E} \xrightarrow{\rho} \widehat{\mathcal{E}} | \mu$, (i), (a) and Lemma 1 we derive that $\mathcal{E}[e_1] \xrightarrow{\rho} \widehat{\mathcal{E}}[\hat{e}_1] | \mu$. Since $\widehat{\mathcal{E}}[\hat{e}_1] | \mu$ reduces in 0 steps to itself we get the result.

Consider now rule (NEW). Then

(i) $e = \mathcal{E}[\text{new } C(x_1, \dots, x_n)]$ and

(ii) $e' = \mathcal{E}[\{^{\{x\}} Cx=\text{new } C(x_1, \dots, x_n); x\}]$.

From $e \xrightarrow{\rho} \hat{e} | \mu$, Lemma 1 and rule (NEW) of Fig.5 we have that

(a) $\hat{e} = \widehat{\mathcal{E}}[\text{new } C(t_1, \dots, t_n)]$,

(b) $\mathcal{E} \xrightarrow{\rho} \widehat{\mathcal{E}} | \mu$ and $\rho(t_i) = x_i$ for $i \in 1, \dots, n$.

Applying rule (NEW) of Fig.1 we have that $\text{new } C(t_1, \dots, t_n) | \mu \Longrightarrow \iota | \mu'$ where $\mu' = \mu[\text{new } C(t_1, \dots, t_n) / \iota]$ and $\iota \notin \text{dom}(\mu)$. Let $\rho' = \rho[x/\iota]$, from (ii) and rule (BLOCK) of Fig.5 we get that $e' \xrightarrow{\rho'} \iota | \mu'$ with $\rho \subseteq \rho'$ and $\text{dom}(\mu) \subseteq \text{dom}(\mu')$, which proves the result. \square

Corollary 1. *If $FV(e) = \emptyset$, $e \longrightarrow^* v$, and $e \xrightarrow{\rho} \hat{e} | \mu$, then $\hat{e} | \mu \Longrightarrow^* \iota | \mu'$ with $v \xrightarrow{\rho'} \iota | \mu'$ for some ρ', μ' such that $\rho \subseteq \rho'$, and $\text{dom}(\mu) \subseteq \text{dom}(\mu')$.*

Proof. By arithmetic induction on the number of steps.

Base If $e \longrightarrow^0 v$, then $e = v$, and $v \xrightarrow{\rho} \hat{e} | \mu$. Since e has no free variables, we have that $v = \{^X dvs x\}$ for some X, dvs , and x . From Lemma 2.2, $\hat{e} = \iota$ for some ι such that $\rho(\iota) = x$. Therefore $\iota | \mu$ reduces in zero steps to $\iota | \mu$ and the thesis holds.

Inductive step If $e \rightarrow^{n+1} v$, then $e \rightarrow e'$ and $e' \rightarrow^n v$. By inductive hypothesis we have that, if $e' \xrightarrow{\rho'} \hat{e}'|\mu'$, then $\hat{e}'|\mu' \Longrightarrow^* \iota|\mu''$ and $v \xrightarrow{\rho''} \iota|\mu''$, for some ρ'', μ'' such that $\rho' \subseteq \rho'', \text{dom}(\mu') \subseteq \text{dom}(\mu'')$. Then, the thesis follows by Theorem 1. \square

The crucial point for the preservation theorem is that the substitution semantics, modeling “moving” capsules from a location to another in the memory, see rule (AFFINE-ELIM), is indeed equivalent to the conventional semantics. Note that this only holds for variables which are used at most once. Consider, for instance, the following reduction sequence in the syntactic calculus, where we omit block annotations for simplicity and we mention rule (CTX) only when the context is different from $[\]$:

$$\begin{aligned} \{C^a x = \text{new } C(0); x.f\} &\longrightarrow && \text{(NEW)} \\ \{C^a x = \{C y = \text{new } C(0); y\}; x.f\} &\longrightarrow && \text{(AFFINE-ELIM)} \\ \{C y = \text{new } C(0); y\}.f &\longrightarrow && \text{(MOVE-SUBTERM)} \\ \{C y = \text{new } C(0); y.f\} &\longrightarrow && \text{(FIELD-ACCESS)} \\ \{C y = \text{new } C(0); 0\} &\longrightarrow && \text{(GARBAGE)} \\ 0 &&& \end{aligned}$$

In the conventional calculus, we get the following corresponding reduction sequence:

$$\begin{aligned} \{C x = \text{new } C(0); x.f\}|\emptyset &\Longrightarrow && \text{(NEW)} + \text{(CTX)} \\ \{C x = \iota; x.f\}|\iota \mapsto \text{new } C(0) &\Longrightarrow && \text{(DEC)} \\ \iota.f|\iota \mapsto \text{new } C(0) &\Longrightarrow^0 && \\ \iota.f|\iota \mapsto \text{new } C(0) &\Longrightarrow && \text{(FIELD-ACCESS)} \\ 0|\iota \mapsto \text{new } C(0) &\Longrightarrow^0 && \\ 0|\iota \mapsto \text{new } C(0) &&& \end{aligned}$$

Consider, instead, a similar example where the affine variable is used twice:

$$\begin{aligned} e &= \{C^a x = \{C y = \text{new } C(0); y\}; x.f=3; x.f\} \longrightarrow && \text{(AFFINE-ELIM)} \\ e' &= \{C y = \text{new } C(0); y\}.f=3; \{C y = \text{new } C(0); y\}.f \longrightarrow && \text{(MOVE-SUBTERM)} + \text{(CTX)} \\ &\{C y = \text{new } C(0); y.f=3\}; \{C y = \text{new } C(0); y\}.f \longrightarrow && \text{(FIELD-ASSIGN)} + \text{(CTX)} \\ &\{C y = \text{new } C(3); 3\}; \{C y = \text{new } C(0); y\}.f \longrightarrow && \text{(GARBAGE)} + \text{(CTX)} \\ &3; \{C y = \text{new } C(0); y\}.f \longrightarrow && \text{(GARBAGE)} \\ &\{C y = \text{new } C(0); y\}.f \longrightarrow^* && \text{as above} \\ &0 && \end{aligned}$$

(To understand the second (GARBAGE) reduction, recall that $e; e'$ is an abbreviation for $\{T x = e; e'\}$ if x not free in e' .)

The term \hat{e} equivalent to e through $\rho(\iota) = y$, with the conventional semantics, reduces to 3:

$$\begin{aligned} \hat{e} &= \{C x = \iota; x.f=3; x.f\}|\iota \mapsto \text{new } C(0) \Longrightarrow && \text{(DEC)} \\ \hat{e}' &= \iota.f=3; \iota.f|\iota \mapsto \text{new } C(0) \Longrightarrow && \text{(FIELD-ASSIGN)} \\ &3; \iota.f|\iota \mapsto \text{new } C(3) \Longrightarrow && \text{(GARBAGE)} \\ &\iota.f|\iota \mapsto \text{new } C(3) \Longrightarrow && \text{(FIELD-ACCESS)} \\ &3|\iota \mapsto \text{new } C(3) && \end{aligned}$$

Hence, in this case the two reduction sequences are *not* equivalent, and Theorem 1 does not hold. Indeed, the first reduction step in the syntactic calculus does *not* preserve the matching relation. Notably, there is no way to find a mapping making terms e' and \hat{e}' to match, since such mapping should map ι in two different variables, one declared in the first block and one in the second (the fact that they are two different variables can be made explicit by α -renaming term e'). In more informal words, the substitution semantics *duplicates memory* (rather than just moving) if adopted for non-affine variables.

5 Conclusion

In this paper we presented a calculus for an imperative object-oriented language whose distinguished features are the following.

- Local variable declarations are used to directly represent the memory. That is, a declared (non affine) variable is not replaced by its value, as in standard `let`, but the association is kept and used when necessary.
- In this way, there are language values (block values) which represent (a portion of) memory, and the fact that such portion of memory is isolated can be *modularly* checked by inspecting only the value itself, without any need to explore the whole graph structure of the global memory as it would be in the conventional model.
- To safely handle capsules, the syntactic calculus supports *affine* variables with a special semantics. Runtime checks ensure that their initializing value is a capsule, and their (unique by definition) occurrence is replaced by their capsule value (rule (AFFINE-ELIM)).
- *Block annotations* allow a variable declaration to be moved outside of a block only if such variable will *not* be part of its final result. This additional runtime check prevents to “break” capsules before they are moved.

In previous work [9, 27, 15, 17, 18, 19, 14], we have designed type systems which statically ensure that such runtime checks succeed, hence execution is not stuck. In this paper we prove that the syntactic calculus preserves the standard semantics of imperative calculi relying on a global memory. In such calculi reasoning about program properties such as sharing requires the formalization of invariants on the memory and the proof of their preservation under reduction, whereas in ours this can be done by structural induction on terms.

The wider context of the paper is the huge amount of research on mechanisms for controlling sharing and interference. In this paper we focus on the property that the subgraph reachable from a reference x is an isolated portion of store, that is, all its (non immutable) nodes can be reached only through this reference. This property has many variants in literature [11, 2, 21, 13, 20]. Examples of other relevant properties of references studied in literature are the following:

- x is *immutable*, that is, the subgraph reachable from x is an *immutable* portion of store. An immutable reference can be safely shared in a multithreaded environment.
- x is *lent*, that is, the subgraph reachable from x can be manipulated, but not shared, by a client [27, 15, 18]. This is also called *borrowed* in literature [7, 25].
- x is *read-only* if no modification is permitted through x . Note that there is no immutability guarantee.

A specular approach to the use of qualifiers to restrict the usage of references is that on *ownership* (see an overview in [10]), where a formal way is provided to express and prove the ownership invariants. Among the many works in this stream, we mention Rust [28], which uses ownership and qualifiers for memory management.

In future work we plan to add the modelling of immutable references. We will also investigate (a form of) Hoare logic on top of our model.

Acknowledgements

We would like to thank the anonymous DCM referees for their helpful comments.

References

- [1] Alexander Joseph Ahern & Nobuko Yoshida (2005): *Formalising Java RMI with explicit code mobility*. In Ralph E. Johnson & Richard P. Gabriel, editors: *ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA 2005)*, ACM Press, pp. 403–422, doi:10.1145/1094811.1094843.
- [2] Paulo Sérgio Almeida (1997): *Balloon Types: Controlling Sharing of State in Data Types*. In: *ECOOP'97 - Object-Oriented Programming, Lecture Notes in Computer Science 1241*, Springer, pp. 32–59, doi:10.1007/BFb0053373.
- [3] Zena M. Ariola & Stefan Blom (2002): *Skew confluence and the lambda calculus with letrec*. *Ann. Pure Appl. Logic* 117(1-3), pp. 95–168, doi:10.1016/S0168-0072(01)00104-X.
- [4] Zena M. Ariola & Matthias Felleisen (1997): *Journ. of Functional Programming* 7(3), pp. 265–301, doi:10.1017/S0956796897002724.
- [5] Lorenzo Bettini, Ferruccio Damiani & Ina Schäfer (2010): *IFJ: a minimal imperative variant of FJ*. Technical Report 133/2010, Dipartimento di Informatica, Università di Torino.
- [6] Gavin M. Bierman & Matthew J. Parkinson (2003): *Effects and effect inference for a core Java calculus*. *Electr. Notes Theor. Comput. Sci.* 82(7), pp. 82–107, doi:10.1016/S1571-0661(04)80803-X.
- [7] John Boyland (2001): *Alias Burying: Unique Variables Without Destructive Reads*. *Softw. Pract. Exper.* 31(6), pp. 533–553, doi:10.1002/spe.370.
- [8] John Boyland (2010): *Semantics of Fractional Permissions with Nesting*. *ACM Transactions on Programming Languages and Systems* 32(6), doi:10.1145/1749608.1749611.
- [9] Andrea Capriccioli, Marco Servetto & Elena Zucca (2016): *An imperative pure calculus*. *Electronic Notes in Theoretical Computer Science* 322, pp. 87–102, doi:10.1016/j.entcs.2016.03.007.
- [10] Dave Clarke, Johan Östlund, Ilya Sergey & Tobias Wrigstad (2013): *Ownership Types: A Survey*. In Dave Clarke, James Noble & Tobias Wrigstad, editors: *Aliasing in Object-Oriented Programming. Types, Analysis and Verification, Lecture Notes in Computer Science 7850*, Springer, pp. 15–58, doi:10.1007/978-3-642-36946-9-3.
- [11] David Clarke & Tobias Wrigstad (2003): *External Uniqueness is Unique Enough*. In Luca Cardelli, editor: *ECOOP'03 - Object-Oriented Programming, Lecture Notes in Computer Science 2473*, Springer, pp. 176–200, doi:10.1006/inco.1996.2613.
- [12] Sylvan Clebsch, Sophia Drossopoulou, Sebastian Blessing & Andy McNeil (2015): *Deny capabilities for safe, fast actors*. In Elisa Gonzalez Boix, Philipp Haller, Alessandro Ricci & Carlos Varela, editors: *International Workshop on Programming Based on Actors, Agents, and Decentralized Control, AGERE! 2015*, ACM Press, pp. 1–12, doi:10.1145/2824815.2824816.
- [13] Werner Dietl, Sophia Drossopoulou & Peter Müller (2007): *Generic Universe Types*. In Erik Ernst, editor: *ECOOP'07 - Object-Oriented Programming, Lecture Notes in Computer Science 4609*, Springer, pp. 28–53, doi:10.1007/BFb0054091.
- [14] Paola Giannini, Tim Richter, Marco Servetto & Elena Zucca (2019): *Tracing sharing in an imperative pure calculus*. *Science of Computer Programming* 172, pp. 180 – 202, doi:10.1016/j.scico.2018.11.007.
- [15] Paola Giannini, Marco Servetto & Elena Zucca (2016): *Types for Immutability and Aliasing Control*. In: *ICTCS'16 - Italian Conf. on Theoretical Computer Science, CEUR Workshop Proceedings 1720*, CEUR-WS.org, pp. 62–74, doi:10.1145/2824815.2824816.
- [16] Paola Giannini, Marco Servetto & Elena Zucca (2017): *Tracing sharing in an imperative pure calculus: extended abstract*. In: *FTfJP'17 - Formal Techniques for Java-like Programs*, ACM Press, pp. 6:1–6:6, doi:10.1145/3103111.3104038.
- [17] Paola Giannini, Marco Servetto & Elena Zucca (2017): *A type and effect system for sharing*. In Ahmed Seffah, Birgit Penzenstadler, Carina Alves & Xin Peng, editors: *OOPS'17 - Object-Oriented Programming*

- Languages and Systems, Track at SAC'17 - ACM Symp. on Applied Computing*, ACM Press, pp. 1513–1515, doi:10.1145/3019612.3019890.
- [18] Paola Giannini, Marco Servetto & Elena Zucca (2018): *A type and effect system for uniqueness and immutability*. In Hisham M. Haddad, Roger L. Wainwright & Richard Chbeir, editors: *OOPS'18 - Object-Oriented Programming Languages and Systems, Track at SAC'18 - ACM Symp. on Applied Computing*, ACM Press, pp. 1038–1045, doi:10.1145/3167132.3167245.
- [19] Paola Giannini, Marco Servetto, Elena Zucca & James Cone (2019): *Flexible recovery of uniqueness and immutability*. *Theoretical Computer Science* 764, pp. 145 – 172, doi:10.1016/j.tcs.2018.09.001.
- [20] Colin S. Gordon, Matthew J. Parkinson, Jared Parsons, Aleks Bromfield & Joe Duffy (2012): *Uniqueness and reference immutability for safe parallelism*. In Gary T. Leavens & Matthew B. Dwyer, editors: *ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA 2012)*, ACM Press, pp. 21–40, doi:10.1145/2398857.2384619.
- [21] John Hogg (1991): *Islands: Aliasing Protection in Object-oriented Languages*. In Andreas Paepcke, editor: *ACM Symp. on Object-Oriented Programming: Systems, Languages and Applications 1991*, ACM Press, pp. 271–285, doi:10.1145/118014.117975.
- [22] Atsushi Igarashi, Benjamin C. Pierce & Philip Wadler (2001): *Featherweight Java: a minimal core calculus for Java and GJ*. *ACM Transactions on Programming Languages and Systems* 23(3), pp. 396–450, doi:10.1145/503502.503505.
- [23] John Maraist, Martin Odersky & Philip Wadler (1998): *The Call-by-Need Lambda Calculus*. *Journ. of Functional Programming* 8(3), pp. 275–317, doi:10.1017/S0956796898003037.
- [24] Robin Milner (1999): *Communicating and mobile systems - the Pi-calculus*. Cambridge University Press, doi:10.1017/S0956796898003037.
- [25] Karl Naden, Robert Bocchino, Jonathan Aldrich & Kevin Bierhoff (2012): *A type system for borrowing permissions*. In: *ACM Symp. on Principles of Programming Languages 2012*, ACM Press, pp. 557–570, doi:10.1145/2103656.2103722.
- [26] Marco Servetto & Lindsay Groves (2013): *True small-step reduction for imperative object-oriented languages*. *FTFJP'13- Formal Techniques for Java-like Programs*, doi:10.1145/2489804.2489805.
- [27] Marco Servetto & Elena Zucca (2015): *Aliasing Control in an Imperative Pure Calculus*. In Xinyu Feng & Sungwoo Park, editors: *Programming Languages and Systems - 13th Asian Symposium (APLAS), Lecture Notes in Computer Science* 9458, Springer, pp. 208–228, doi:10.1007/978-3-319-26529-2_12.
- [28] Aaron Turon (2017): *Rust: from POPL to practice (keynote)*. In Giuseppe Castagna & Andrew D. Gordon, editors: *ACM Symp. on Principles of Programming Languages 2017*, ACM Press, p. 2, doi:10.1145/3009837.3011999.
- [29] Yoav Zibin, Alex Potanin, Paley Li, Mahmood Ali & Michael D. Ernst (2010): *Ownership and immutability in generic Java*. In: *ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages and Applications (OOPSLA 2010)*, pp. 598–617, doi:10.1145/1869459.1869509.