Game Semantics for Interface Middleweight Java *

Andrzej S. Murawski
DIMAP and Department of Computer Science
University of Warwick

Nikos Tzevelekos
School of Electronic Engineering and Computer Science
Queen Mary, University of London

Abstract
We consider an object calculus in which open terms interact with the environment through interfaces. The calculus is intended to capture the essence of contextual interactions of Middleweight Java code. Using game semantics, we provide fully abstract models for the induced notions of contextual approximation and equivalence. These are the first denotational models of this kind.

Categories and Subject Descriptors D.3.1 [Formal Definitions and Theory]: Semantics; F.3.2 [Semantics of Programming Languages]: Denotational semantics

Keywords Full Abstraction, Game Semantics, Contextual Equivalence, Java

1. Introduction
Denotational semantics is charged with the construction of mathematical universes (denotations) that capture program behaviour. It concentrates on compositional, syntax-independent modelling with the aim of illuminating the structure of computation and facilitating reasoning about programs. Many developments in denotational semantics have been driven by the quest for full abstraction [21]: a model is fully abstract if the interpretations of two programs are the same precisely when the programs behave in the same way (i.e. are contextually equivalent). A faithful correspondence like this opens the path to a broad range of applications, such as compiler optimisation and program transformation, in which the preservation of semantics is of paramount importance.

Recent years have seen game semantics emerge as a robust denotational paradigm [4, 6, 12]. It has been used to construct the first fully abstract models for a wide spectrum of programming languages, previously out of reach of denotational semantics. Game semantics models computation as an exchange of moves between two players, representing respectively the program and its computational environment. Accordingly, a program is interpreted as a strategy in a game corresponding to its type. Intuitively, the plays that game semantics generates constitute the observable patterns that a program produces when interacting with its environment, and this is what underlies the full abstraction results. Game semantics is compositional: the strategy corresponding to a compound program phrase is obtained by canonical combinations of those corresponding to its sub-phrases. An important advance in game semantics was the development of nominal games [3, 17, 26], which underpinned full abstraction results for languages with dynamic generative behaviours, such as the λ-calculus [3], higher-order concurrency [18] and ML references [24]. A distinctive feature of nominal game models is the presence of names (e.g. memory locations, references names) in game moves, often along with some abstraction of the store.

The aim of the present paper is to extend the range of the game approach towards real-life programming languages, by focussing on Java-style objects. To that end, we define an imperative object calculus, called Interface Middleweight Java (IMJ), intended to capture contextual interactions of code written in Middleweight Java (MJ) [9], as specified by interfaces with inheritance. We present both equational (contextual equivalence) and inequational (contextual approximation) full abstraction results for the language. To the best of our knowledge, these are the first denotational models of this kind.

Related Work While the operational semantics of Java has been researched extensively [7], there have been relatively few results regarding its denotational semantics. More generally, most existing models of object-oriented languages, such as [8, 15], have been based on global state and consequently could not be fully abstract.

On the other hand, contextual equivalence in Java-like languages has been studied successfully using operational approaches such as trace semantics [2, 13, 14] and environmental bisimulation [16]. The trace-based approaches are closest to ours and the three papers listed also provide characterizations of contextual equivalence. The main difference is that traces are derived operationally through a carefully designed labelled transition system and, thus, do not admit an immediate compositional description in the style of denotational semantics.

However, similarities between traces and plays in game semantics indicate a deeper correspondence between the two areas, which also manifested itself in other cases, e.g. [20] vs [19]. At the time of writing, there is no general methodology for moving smoothly between the two approaches, but we believe that there is scope for unifying the two fields in the not so distant future.

In comparison to other game models, ours has quite lightweight structure. For the most part, playing consists of calling the opponent’s methods and returning results to calls made by the opponent. In particular, there are no justification pointers between moves. This can be attributed to the fact that Java does not feature first-class higher-order functions and that methods in Java objects cannot be updated. On the other hand, the absence of pointers makes definitions of simple notions, such as wellBracketing, less direct, since the dependencies between moves are not given explicitly any...
more and need to be inferred from plays. The latter renders strategy composition non-standard. Because it is impossible to determine statically to which arena a move belongs, the switching conditions (cf. [6]) governing interactions become crucial for determining the strategy responsible for each move. Finally, it is worth noting that traditional copilot links are by definition excluded from our setting: a call/call move for a given object cannot be copyswapped by the other player, as the move has a fixed polarity, determined by the ownership of the object. In fact, identity strategies contain plays of the other player, as the move has a fixed polarity, determined by the ownership of the object. In fact, identity strategies contain plays of length at most two!

**Further Directions** In future work, we would like to look for automata-theoretic representations of fragments of our model in order to use them as a foundation for a program generation tool for Java programs. Our aim is to take advantage of the latest developments in automata theory over infinite alphabets [10], and fresh-register automata in particular [23, 27], to account for the nominal developments in automata theory over infinite alphabets [10], and fresh-

![Figure 1. Typing rules for IMJ terms and method-set implementations](image)

An interface table $\Delta$ is **well-formed** if, for all interface types $\mathcal{I}, \mathcal{I}'$

- if $\mathcal{I}'$ appears in $\Delta(\mathcal{I})$ then $\mathcal{I}' \in \text{dom}(\Delta)$,
- if $(\mathcal{I}(\mathcal{I}')) : \Theta \in \text{dom}(\Delta(\mathcal{I}')) \cap \text{dom}(\Theta) = \emptyset$.

Henceforth we assume that interface tables are well-formed. Interface extensions yield a subtyping relation. Given a table $\Delta$, we define $\Delta \vdash \theta_1 \leq \theta_2$ by the following rules.

$$\frac{}{\Delta \vdash \theta \leq \theta} \quad \frac{}{\Delta \vdash \theta \leq \theta}$$

We might omit $\Delta$ from subtyping judgements for economy.

**Definition 2.** Let $\mathcal{A}$ be a countably infinite set of **object names**, which we range over by $a$ and $\mathcal{V}$. IMJ **terms** are listed below, where we let $x$ range over a set of variables Vars, and $i$ over $\mathcal{I}$. Moreover, $\oplus$ is selected from some set of binary numeric operators, $\mathcal{M}$ is a **method-set implementation**. Again, we stipulate that each $m$ appear in each $\mathcal{M}$ at most once.

$$\begin{align*}
\mathcal{M} &::= x \mid a \mid \text{skip} \mid \text{null} \mid i \mid \mathcal{M} \oplus \mathcal{M} & | \text{let } x = M \text{ in } M \\
| M &= M \mid (\mathcal{I} \mid M \mid \text{new}(x ; \mathcal{I} ; M)) & | M.f \mid M.f := M \mid \mathcal{M}(\mathcal{M}) \\
\end{align*}$$

The terms are typed in contexts comprising an interface table $\Delta$ and a variable context $\Gamma = \{x_1 \mapsto \theta_1, \ldots, x_n \mapsto \theta_n\} \cup \{a_1 \mapsto \mathcal{I}_1, \ldots, a_m \mapsto \mathcal{I}_m\}$ such that any interface in $\Gamma$ occurs in $\text{dom}(\Delta)$. The typing rules are given in Figure 1.

For the operational semantics, we define the sets of **term values**, **heap configurations** and **states** by:

$$\begin{align*}
\mathcal{V} ::= \text{skip} \mid \text{null} \mid a \\
\mathcal{H} ::= V \mid \emptyset \mid (f : V), V \\
\mathcal{S} ::= S : \mathcal{A} \rightarrow \mathcal{Ints} \times (\mathcal{HCasts} \times \mathcal{MImps})
\end{align*}$$

If $S(a) = (\mathcal{I}, (V, M))$ then we write $S(a) : \mathcal{I}$, while $S(a).f$ and $S(a).m$ stand for $V.f$ and $M.m$ respectively, for each $f$ and $m$.

Given an interface table $\Delta$ such that $\mathcal{I} \in \text{dom}(\Delta)$, we let the default heap configuration of type $\mathcal{I}$ be

$$V_\mathcal{I} = \{f : v_f \mid \Delta(\mathcal{I}).f = \theta\},$$

where $v_\text{null} = \text{skip}$, $v_\text{int} = 0$ and $v_\text{null} = \text{null}$. The operational semantics of IMJ is given by means of a small-step transition relation
between terms-in-state, presented in Figure 2. The transition relation uses evaluation contexts \( E \) that are defined as follows.

\[
E ::= \text{let } x = \_ \text{ in } M | \_ \oplus M | i \oplus _{} | \_ = M | a = _{} \\
\mid \text{if } _{} \text{ then } M \text{ else } M' | (I) = \_ | \_ \cdot f = \_ | a.f = _{}
\]

Given \( \Delta[0] \vdash M : \text{void} \), we write \( M \downarrow \) if there exists \( S \) such that \( (0, M) \rightarrow^* (S, \text{skip}) \).

**Definition 3.** Given \( \Delta[I] \vdash M_i : \theta \) (\( i = 1, 2 \)), we shall say that
\[
\Delta[I] \vdash M_i : \theta \text{ contextually approximates } \Delta[I] \vdash M_2 : \theta
\]
if, for all \( \Delta' \supseteq \Delta \) and all contexts \( C \) such that \( \Delta'[0] \vdash C[M_i] : \text{void} \), void if \( C[M_i] \Downarrow \downarrow \) then \( C[M_2] \Downarrow \downarrow \). We then write \( \Delta[I] \vdash M_i \equiv M_2 : \theta \). Two terms are contextually equivalent (written \( \Delta[I] \vdash M_1 \equiv M_2 : \theta \)) if they approximate each other.

For technical convenience, IMJ features the let construct, even though it is definable: given \( \Delta[I], x : \theta' \vdash M : \theta \) and \( \Delta[I] \vdash M' : \theta' \), consider \( \text{new}(x : I; m : \lambda x. M).m(M') \), where \( I \) is a fresh interface with a single method \( m : \theta \rightarrow \theta' \). As usual, we write \( M : M' \) for \( \text{let } x = M \text{ in } M' \), where \( x \) is not free in \( M' \).

Although IMJ does not have explicit local variables, they could easily be introduced by taking \( \text{let } x = \text{new}(y : I_0; i) \ldots \), where \( I_0 \) has a single field of type \( \theta \). In the same manner, one can define variables and methods that are private to objects, and invisible to the environment through interfaces.

**Example 1 ([16]).** Let \( \Delta = \{ \text{Empty : } \emptyset, \text{Cell : } \lambda (get : \text{void} \mapsto \text{Empty}, \text{set : } \text{void} \mapsto \text{void}), \text{Var} : \lambda (val : \text{Empty}), \text{Var} : \lambda (val : \text{int}) \} \) and consider the terms \( \Delta[0] \vdash M_i : \text{Cell} (i = 1, 2) \) defined by:

\[
M_1 \equiv \text{let } v = \text{new}(x : \text{Var}; i) \in \text{new}(x : \text{Cell}; M_1)
\]

\[
M_2 \equiv \text{let } b = \text{new}(x : \text{Var}; i) \in \text{new}(v_1 : \text{Var}; e_1)
\]

\[
\text{let } v_2 = \text{new}(x : \text{Var}; e_2) \in \text{new}(x : \text{Cell}; M_2)
\]

with

\[
M_1 = (\text{get : } \lambda (.) \cdot v. \text{val}, \text{set : } \lambda y. (v. \text{val} := y))
\]

\[
M_2 = (\text{get : } \lambda (.) \cdot (b. \text{val} := 0; v_1. \text{val}), \text{set : } \lambda y. (v_1. \text{val} := y; v_2. \text{val} := y))
\]

We have \( \Delta[0] \vdash M_1 \equiv M_2 : \text{Cell} \). Intuitively, each of the two implementations of Cell corresponds to recording a single value of type \( \text{Empty} \) (using set) and providing access to it via get. The difference lies in the way the value is stored: a single private variable is used in \( M_1 \), while two variables are used in \( M_2 \). However, in the latter case the variables always hold the same value, so it does not matter which of the variables is used to return the value.

The game semantics of the two terms will turn out to consist of plays of the shape \( s^0 n^0 \cdot s^1 G_1^0 \cdots s_k G_k^0 \), where

\[
G_i = \begin{cases} \text{call } n.\text{get}(\ast) & i = 0 \\
\text{call } n.\text{get}(\ast) & i > 0 \end{cases}
\]

and \( S_i = \{ n \mapsto \text{Cell}(\emptyset) \} \cup \{ n_j \mapsto \{ \text{Empty, } \emptyset \} \mid 0 < j \leq i \} \). Intuitively, the plays describe all possible interactions of a Cell object. The first two moves \( s^0 n^0 \) correspond to object creation. After that, the \( G_i \) segments represent the environment reading the current content (initially having null value), while the \( S_i \) segments correspond to updating the content with a reference name provided by the environment. The stores \( S_i \) attached to moves consist of all names that have been introduced during the interaction so far.

It is worth noting that, because IMJ has explicit casting, a context can always guess the actual interface of an object and extract any information we may want to hide through casting.

**Example 2.** Let \( \Delta = \{ \text{Empty : } \emptyset, \text{Point(Empty) : } (x : \text{int}, y : \text{int}) \} \) and consider the terms \( \Delta[0] \vdash M_i : \text{Empty} (i = 1, 2) \) defined by:

\[
M_1 \equiv \text{new}(x : \text{Empty}; )
\]

\[
M_2 \equiv \text{let } p = \text{new}(x : \text{Point}; ) \in p.x := 0; p.y := 1; (\text{Empty})p
\]

In our model they will be interpreted by the strategies \( \sigma_1 = \{ \epsilon, s^0 n^0 (\text{Empty, } \emptyset) \} \) and \( \sigma_2 = \{ \epsilon, s^0 n^0 (\text{Point, } \{ x : 0, y : 0 \}) \} \) respectively. Using e.g. the casting context \( C = \{ \text{Point} \}; \text{skip} \), we can see that \( \Delta[0] \vdash M_2 \not \subseteq M_1 : \text{Empty} \). On the other hand, Theorem 20 will imply \( \Delta[0] \vdash M_1 \subseteq M_2 : \text{Empty} \).

On the whole, IMJ is a compact calculus that strips down Middleweight Java to the essentials needed for interface-based interaction. Accordingly, we suppressed the introduction of explicit class hierarchy, as it would remain invisible to the environment anyway and any class-based internal computations can be represented using standard object encodings [1].

At the moment the calculus allows for single inheritance for interfaces only, but extending it to multiple inheritance is not problematic. The following semantic developments only rely on the assumption that \( \leq \) must not give rise to circularities.

### 3. The game model

In our discussion below we assume a fixed interface table \( \Delta \).

The game model will be constructed using mathematical objects (moves, plays, strategies) that feature names drawn from the set \( \mathcal{A} \). Although names underpin various elements of our model, we do not want to delve into the precise nature of the sets containing them. Hence, all of our definitions preserve name-invariance, i.e. our objects are (strong) nominal sets [11, 26]. Note that we do not
need the full power of the theory but mainly the basic notion of name-permutation. For an element \( x \) belonging to a (nominal) set \( X \) we write \( \nu(x) \) for its name-support, which is the set of names occurring in \( x \). Moreover, for any \( x, y \in X \), we write \( x \sim y \) if there is a permutation \( \pi \) such that \( x = \pi(y) \).

We proceed to define a category of games. The objects of our category will be **arenas**, which are nominal sets carrying specific type information.

**Definition 4.** An arena is a pair \((A, \xi_A)\) where:

- \( A \) is a nominal set of moves;
- \( \xi_A : A \to (\mathcal{A} \to \text{Ints}) \) is a nominal typing function;
- such that, for all \( m \in A \), \( \text{dom}(\xi_A(m)) = \nu(m) \).

We start by defining the following basic arenas,

\[
1 = \{(*)\}, \{(*,0)\}, \quad \mathbb{Z} = \{(i,0)\}, \quad \mathcal{I} = (\mathcal{A} \cup \{\text{nul}\}) \cup \{(a,a,\mathcal{I})\},
\]

for all interfaces \( \mathcal{I} \). Given arenas \( A \) and \( B \), we can form the arena \( A \times B \) by:

\[
M_{A \times B} = \{(m,n) \in M_A \times M_B | a \in \nu(m) \cap \nu(n) \} = \{(\xi_A(m,a),\xi_B(n,a)) | \xi_A(m,a) \leq \xi_B(n,a) \}.
\]

Another important arena is \( \#(\mathcal{I}_1, \ldots, \mathcal{I}_n) \), with:

\[
M_{\#(\mathcal{I})} = \{(a_1, \ldots, a_n) \in A^n | a_i \text{'s distinct} \} = \mathcal{I}^n \quad \text{for all } n \in \mathbb{N}.
\]

For each type \( \theta \), we set \( \text{Val}_\theta \) to be the set of semantic values of type \( \theta \), given by:

\[
\text{Val}_\theta = M_1, \quad \text{Val}_{\text{int}} = M_{\mathbb{Z}}, \quad \text{Val}_{\mathcal{I}} = M_{\mathcal{I}}.
\]

For each type sequence \( \theta = \theta_1, \ldots, \theta_n \), we set \( \text{Val}_{\theta} = \text{Val}_{\theta_1} \times \cdots \times \text{Val}_{\theta_n} \).

We let a store \( \Sigma \) be a type-preserving finite partial function from names to object types and field assignments, that is, \( \Sigma : \mathcal{A} \to \text{Ints} \times (\text{Fields} \to \text{Val}) \) such that \( |\Sigma| \) is finite and

\[
\Sigma(a) : \mathcal{I} \land \Delta(\mathcal{I}), f = \theta \implies (a,f) \in \Sigma(\mathcal{I}), f = v \land \Sigma \vdash v \leq \theta,
\]

where the new notation is explained below. First, assuming \( (a,f) \in \Sigma(\mathcal{I}) \), the judgement \( (a,f) \in \Sigma(\mathcal{I}) \) holds if \( \mathcal{I} = \mathcal{I}' \) and \( \Sigma(a).f \) stands for \( \phi(f) \). Next we define typing rules for values in store contexts:

\[
v \in \text{Val}_{\text{void}}, \quad v \in \text{Val}_{\text{int}}, \quad \text{Val}(\mathcal{I} \lor v = \text{nu1})
\]

and write \( \Sigma \vdash v \leq \theta \) for \( \Sigma \vdash v : \theta \lor (\Sigma \vdash v : \mathcal{I}' \land \mathcal{I}' \leq \theta) \).

We let \( \text{Sto} \) be the set of all stores. We write \( \text{dom}(\Sigma(a)) \) for the set of all \( f \) such that \( (a,f) \in \Sigma(a) \). We let \( \text{Sto}_0 \) contain all stores \( \Sigma \) such that:

\[
\forall a \in \text{dom}(\Sigma), f \in \text{dom}(\Sigma(a)), \Sigma(a).f \in \{*,0,\text{nu1}\}
\]

and we call such a \( \Sigma \) a default store.

Given arenas \( A \) and \( B \), plays in \( AB \) will consist of sequences of moves (with store) which will be either moves from \( M_A \cup M_B \), or moves representing method calls and returns. Formally, we define:

\[
M_{A \cup B} = M_A \cup M_B \cup \text{Calls} \cup \text{Retns}
\]

where we set \( \text{Calls} = \{\text{call } a.m(\bar{v}) | a \in \mathcal{A} \land \bar{v} \in \text{Val}^*\} \) and \( \text{Retns} = \{\text{ret } a.m(v) | a \in \mathcal{A} \land v \in \text{Val}\} \).

**Definition 5.** A legal sequence in \( AB \) is a sequence of moves from \( M_{AB} \) that adheres to the following grammar (Well-Bracketing), where \( m_A \) and \( m_B \) range over \( M_A \) and \( M_B \) respectively.

\[
L_{AB} ::= \epsilon \mid m_A X \mid m_A Y m_B X \quad X ::= Y \mid Y (\text{call } a.m(\bar{v})) \quad Y ::= \epsilon \mid YY \mid (\text{call } a.m(\bar{v})) Y (\text{ret } a.m(v))
\]

We write \( L_{AB} \) for the set of legal sequences in \( AB \). In the last clause above, we say that \( a.m(\bar{v}) \) justifies \( \text{ret } a.m(v) \).

To each \( s \in L_{AB} \) we assign a polarity \( p \) from move occurrences in \( s \) to the set \( \mathcal{P}_s = \{O,P\} \). Polariities represent the two players in our game reading of programs: \( O \) is the Opponent and \( P \) is the Proponent in the game. The latter corresponds to the modelled program, while the former models the possible computational environments surrounding the program. Polarieties are complemented via \( \overline{O} = \{P\} \) and \( \overline{P} = \{O\} \). In addition, the polarity function must satisfy the condition:

- For all \( m_X \in M_X \) \((X = A,B)\) occurring in \( s \) we have \( p(m_X) = O \) and \( p(m_B) = P \) (O-starting).
- If \( mn \) are consecutive moves in \( s \) then \( p(n) = \overline{p(m)} \). (Alternation)

It follows that there is a unique \( p \) for each legal sequence \( s \), namely the one which assigns \( O \) precisely to those moves appearing in odd positions in \( s \).

A **move-with-store** in \( AB \) is a pair \( m^\Sigma \) with \( \Sigma \in \text{Sto} \) and \( m \in M_{AB} \). For each sequence \( s \) of moves-with-store we define the set of available names of \( s \) by:

\[
\text{Av}(\epsilon) = \emptyset, \quad \text{Av}(sm^\Sigma) = \Sigma^* (\text{Av}(s) \cup \nu(m))
\]

where, for each \( X \subseteq A \), we let \( \Sigma^*(X) = \bigcup_j \Sigma^j(X) \), with \( \Sigma^0(X) = X \) and \( \Sigma^j+1(X) = \nu(\Sigma^j(X)) \).

That is, a name is available in \( s \) just if it appears inside a move in \( s \), or it can be reached from an available name through some store in \( s \). We write \( s_1 \) for the underlying sequence of moves of \( s \) (i.e. \( \pi_1(s) \)), and let \( \subseteq \subseteq \) denote the prefix relation between sequences. If \( s^m_{\Sigma} \subseteq \subseteq s \) and \( a \in \nu(m^\Sigma) \cup \nu(s) \) then we say \( a \) is introduced by \( m^\Sigma \) in \( s \). In such a case, we define the owner of the name \( a \) in \( s \), written \( o(a) \), to be \( p(m) \) (where \( p \) is the polarity associated with \( s \)). For each polarity \( X \in \{O,P\} \) we let \( X(s) = \{a | a \in \nu(s) | o(a) = X\} \) be the set of names in \( s \) owned by \( X \).

**Definition 6.** A play in \( AB \) is a sequence of moves-with-store \( s \) such that \( s \) is a legal sequence and, moreover, for all \( s' m^\Sigma \subseteq \subseteq s \):

- It holds that \( \text{dom}(\Sigma) = \text{Av}(s'm^\Sigma) \). (Frugality)
- If \( a \in \text{dom}(\Sigma) \) with \( \Sigma(a) : \mathcal{I} \) then:
  - \( \text{if } m \in M_X \), for \( X \in \{A,B\} \), then \( \mathcal{I} \leq \xi_X(m,a) \);
  - \( \text{for all } n^T \in s', \text{if } a \in \text{dom}(T) \) then \( T(a) : \mathcal{I} \);
  - \( \text{if } \Delta(\mathcal{I}).m = \theta \rightarrow \theta \) then:
    - \( \text{if } m = \text{call } a.m(\bar{v}) \) then \( \Sigma \vdash \bar{v} : \theta^d \) for some \( \theta^d \leq \theta \);
    - \( \text{if } m = \text{ret } a.m(v) \) then \( \Sigma \vdash v : \theta^d \) for some \( \theta^d \leq \theta \). (Well-calling)
- If \( m = \text{call } a.m(\bar{v}) \) then \( o(a) \in p(m) \). (Well-calling)

We write \( P_{AB} \) for the set of plays in \( AB \).
Note above that, because of well-bracketing and alternation, if \( m = \text{ret } a.m(v) \) then well-calling implies \( o(a) = p(m) \). Thus, the frugality condition stipulates that names cannot appear in a play in unreachable parts of a store (cf. [17]). Moreover, well-calling ensures that the typing information in stores is consistent and adheres to the constraints imposed by \( \Delta \) and the underlying arenas. Finally, well-calling implements the specification that each player need only call the other player’s methods. This is because calls to each player’s own methods cannot in general be observed and so should not be accounted for in plays.

Given arenas \( A, B, C \), next we define interaction sequences, which show how plays from \( AB \) and \( BC \) can interact to produce a play in \( AC \). The sequences will rely on moves with stores, where the moves come from the set:

\[
M_{ABC} = M_A \cup M_B \cup M_C \cup \text{Calls} \cup \text{Retns}.
\]

The moves will be assigned polarities from the set:

\[
\text{Pol}_2 = \{ O_L, P_L, O_L P_R, P_L O_R, O_R, P_R \}.
\]

The index \( L \) stands for “left”, while \( R \) means “right”. The indices indicate which part of the interaction (\( A, B \) or \( C \)) a move comes from, and what polarity it has therein. We also consider an auxiliary notion of pseudo-polarities:

\[
\begin{align*}
\text{OO} &= \{ O_L, O_R \}, \\
\text{PO} &= \{ P_L, P_L O_R \}, \\
\text{OP} &= \{ P_R, O_L P_R \}.
\end{align*}
\]

Each polarity has an opposite pseudo-polarity determined by:

\[
\begin{align*}
\text{OA}_L &= \text{OA}_R, \\
\text{PA}_R &= \text{PA}_L, \\
\text{OP} &= \text{PO}.
\end{align*}
\]

Finally, each \( X \in \{ AB, BC, AC \} \) has designated set of polarities given by:

\[
\begin{align*}
p(AB) &= \{ O_L, P_L, P_L O_R, P_L O_R \}, \\
p(BC) &= \{ O_R, P_R, O_L P_R, P_R O_R \}, \\
p(AC) &= \{ O_L, P_L, O_R, P_R \}.
\end{align*}
\]

Note the slight abuse of notation with \( p_0 \), as it is also used for move polarities.

Suppose \( X \in \{ AB, BC, AC \} \). Consider a sequence \( s \) of moves-with-store from \( ABC \) (i.e. a sequence with elements \( m^x \) with \( m \in M_{ABC} \)) along with an assignment of polarities from \( \text{Pol}_2 \) to moves of \( s \). Let \( \gamma : X \rightharpoonup 0 \) be the subsequence of \( s \) containing those moves-with-store \( m^x \) for which \( p(m) \in p(X) \). Additionally, we define \( \gamma : X \rightharpoonup 0 \) to be \( \gamma(s \restriction X) \), where the function \( \gamma \) acts on moves-with-store by restricting the domains of stores to available names:

\[
\gamma(\epsilon) = \epsilon, \quad \gamma(s \Sigma \epsilon) = \gamma(s) \Sigma \epsilon \gamma(A \omega(s \Sigma \epsilon)).
\]

Definition 7. An interaction sequence in \( ABC \) is a sequence \( s \) of moves-with-store in \( ABC \) satisfying the following conditions:

- For each \( s', m^x \subseteq s \), \( \text{dom}(\Sigma) = \omega(A \varphi(s \Sigma \epsilon)) \). (Frugality)
- If \( s', m^x \subseteq s \) and \( a \in \text{dom}(\Sigma) \) with \( \Sigma(a) : T \) then:
  - if \( m \in M_X \), for \( X \in \{ A, B, C \} \), then \( T \leq \chi(m, a) \);
  - for all \( n \leq s' \), if \( a \in \text{dom}(T) \) then \( T(a) : T \);
  - if \( \Delta(T), m = \vartheta \mapsto \theta \) then:
    - if \( m = \text{call } a.m(v) \) then \( \Sigma \rightharpoonup (\vartheta \mapsto \theta) \) for some \( \theta \leq \vartheta \);
    - if \( m = \text{ret } a.m(v) \) then \( \Sigma \rightharpoonup v : \theta \) for some \( \theta' \leq \theta \). (Well-calling)
- There is a polarity function \( p \) from move occurrences in \( \Sigma \) to \( \text{Pol}_2 \) such that:
  - For all \( m \in M_X \) (\( X = A, B, C \) occurring in \( s \) we have \( p(m_A) = O_L \), \( p(m_B) = P_L O_R \), \( p(m_C) = P_R \));
  - If \( mn \) are consecutive moves in \( s \) then \( p(n) \subseteq p(m) \). (Alternation)

\[
\begin{align*}
\text{OO} &= \{ O_L, O_R \}, \\
\text{PL} &= \{ P_L, O_L P_R \}, \\
\text{OR} &= \{ O_R, P_L O_R \}, \\
\text{OPR} &= \{ P_R, O_L P_R \}, \\
\text{POL} &= \{ O_L, P_L \}, \\
\text{POR} &= \{ O_R, P_R \}, \\
\text{PlO} &= \{ P_L O_R, P_R O_R \}, \\
\text{OP} &= \{ P_R, O_L P_R \}.
\end{align*}
\]

Figure 3. Interaction diagram for \( \text{Int}(ABC) \). The diagram specifies the alternation of polarities in interaction sequences. Transitions are labelled by move polarities, while \( OO \) is the initial state.

- If \( s \Sigma \epsilon \subseteq s \) then \( m = \text{call } a.m(v) \) implies \( o(a) = p(m) \). (Well-calling)
- For each \( X \in \{ AB, BC, AC \} \), \( s \restriction X \subseteq L_X \). (Projecting)
- If \( s \Sigma \epsilon \subseteq s \) and \( m = \text{ret } a.m(v) \) then there is a move \( n^y \) in \( s' \) such that, for all \( X \), such that \( p(m) \subseteq p(X) \), \( n \) is the justifier of \( m \) in \( s \restriction X \). (Well-returning)
- Laird’s conditions [17]:
  - \( P(s \rightharpoonup \gamma(AB)) \cap P(s \rightharpoonup \gamma(BC)) = \emptyset \);
  - \( \{ P(s \rightharpoonup \gamma(AB)) \cap P(s \rightharpoonup \gamma(AC)) \} \subseteq X \}, \quad AC \}
  - For each \( s' \subseteq s \) ending in \( m^x \leq n^x \) and each \( a \in \text{dom}(T) \), if \( p(m) \subseteq PO \) and \( a \notin u(s' \rightharpoonup \gamma(AB)), \quad u(s' \rightharpoonup \gamma(BC)), \quad u(s' \rightharpoonup \gamma(AC)) \), then \( \Sigma(a) = T(a) \).

We write \( \text{Int}(ABC) \) for the set of interaction sequences in \( ABC \).

Note that, by projecting and well-returning, each return move in \( s \) has a unique justifier. Next we show that the polarities of moves inside an interaction sequence are uniquely determined by the interaction diagram of Figure 3. The diagram can be seen as an automaton accepting \( s \), for each \( s \in \text{Int}(ABC) \). The edges represent moves by their polarities, while the labels of vertices specify the polarity of the next (outgoing) move. For example, from \( OO \) we can only have a move \( m \) with \( p(m) \in \{ O_L, O_R \} \), for any \( p \).

Lemma 1. Each \( s \in \text{Int}(ABC) \) has a unique polarity function \( p \).

Proof. Suppose \( s \in \text{Int}(ABC) \). We claim that the alternation, well-calling, projecting and well-returning conditions uniquely specify \( p \). Consider the interaction diagram of Figure 3, which we read as an automaton accepting \( s \), call it \( A \). The edges represent moves by their polarities, while the labels of vertices specify the polarity of the next (outgoing) move. By projecting we obtain that the first element of \( s \) is some \( m_A \) and, by alternation, its polarity is \( O_L \). Thus, \( OO \) is the initial state.

We now use induction on \( |s| \) to show that \( A \) has a unique run on \( s \). The base case is trivial, so suppose \( s = s' \). By induction hypothesis, \( A \) has a unique run on \( s' \), which reaches some state \( X \). We do a case analysis on \( m \). If \( m \in M_A \cup M_B \cup M_C \) then there is a unique edge accepting \( m \) and, by alternation, this edge must depart from \( X \). If, on the other hand, \( m = \text{call } a.m(v) \) then the fact that \( o(a) = p(m) \) gives two possible edges for accepting \( m \). But observe that no combination of such edges can depart from \( X \).

Finally, if \( m = \text{ret } a.m(v) \) then \( \vartheta \leq \theta \). Thus, if \( m \) is accepted by \( p \), then \( n \) is accepted by \( P_L \).

Next we show that interaction sequences project to plays. The projection of interaction sequences in \( ABC \) on \( AB, BC \) and \( AC \)
leads to the following definition of projections of polarities,
\[ \pi_{AB}(X_L) = X \quad \pi_{AB}(XLYR) = X \quad \pi_{AB}(YR) = \text{undef.} \]
\[ \pi_{BC}(X_L) = \text{undef.} \quad \pi_{BC}(XLYR) = Y \quad \pi_{BC}(YR) = Y \]
where \( X, Y \in \{O, P\} \). We can now show the following.

**Lemma 2.** Let \( s \in \text{Int}(ABC) \). Then, for each \( X \in \{AB, BC, AC\} \) and each \( m^2 \in s \), if \( p(m) \in \pi(x) \) then \( \pi_{X}(p(m)) = p_X(m) \), where \( p_X \) is the polarity function of \( X \).

**Proof.** We show this for \( X = AB \); the other cases are proven similarly, by induction on \( s \geq 0 \); the base case is trivial. For the inductive case, if \( m \) is the first move in \( s \) with polarity in \( p(AB) \) then, by projecting, \( m \in M_A \) and therefore \( p(m) = O_L \) and \( p(AB)(m) = O \), as required. Otherwise, let \( m \) be the last move in \( s \) with polarity in \( p(AB) \) before \( m \). By \( \Pi \), \( p(AB)(m) = \pi_{AB}(p(n)) \). Now, by projecting, \( p(AB)(m) = p(AB)_n \) and observe that, for all \( X \in p(n) \), \( \pi_{AB}(X) = \pi_{AB}(p(n)) \), so in particular \( \pi_{AB}(p(m)) = \pi_{AB}(p(n)) = p(AB)(m) = p(AB)(n) \).

The following lemma formulates a taxonomy on names appearing in interaction sequences.

**Lemma 3.** Let \( s \in \text{Int}(ABC) \). Then,
1. \( \nu(s) = O(\nu(s) \upharpoonright AC) \upharpoonright P(s \upharpoonright AB) \upharpoonright P(s \upharpoonright BC) \);
2. if \( s = tm^2 \) then:
   - \( p(m) \in \text{OO} \) and \( s \upharpoonright AC = t'm^2 \).
   - or \( p(m) \in \text{PO} \) and \( s \upharpoonright AB = t'm^2 \).
   - or \( p(m) \in \text{OP} \) and \( s \upharpoonright BC = t'm^2 \).

   \[ \nu(t) \cap \nu(t)^v \subseteq \nu(t) \text{ and, in particular, if } m \text{ introduces name } a \text{ in } t'm^2 \text{ then } m \text{ introduces a in } s. \]

**Proof.** For 1, by definition of interactions we have that these sets are disjoint. It therefore suffices to show the left-to-right inclusion. Suppose that \( a \in \nu(s) \) is introduced in some \( m^2 \) in \( s \), with \( p(m) \in \text{PO} \), and let \( s \upharpoonright AC = AB \ldots m^2 \ldots \). If \( a \in \nu(m^2) \) then \( a \in P(s \upharpoonright AB) \), as required. Otherwise, by Laird’s last set of conditions, a is copied from the move of the move preceding \( m^2 \) in \( s \), a contradiction to its being introduced at \( m^2 \). Similarly if \( p(m) \in \text{OO} \). Finally, if \( p(m) \in \text{OO} \) then we similarly, considering \( O(s \upharpoonright AC) \).

For 2, we show the first case, and the other cases are similar. It suffices to show that \( \nu(m^2) \setminus \nu(t)^v \cap \nu(t) = \emptyset \). Suppose \( a \in \nu(m^2) \setminus \nu(t)^v \), therefore \( a \in O(s \upharpoonright AC) \). But then we cannot have \( a \in \nu(t) \) as the latter, by item 1, would imply \( a \in P(s \upharpoonright AB) \cup P(s \upharpoonright BC) \).

**Proposition 4.** For all \( s \in \text{Int}(ABC) \), the projections \( s \upharpoonright AB, s \upharpoonright BC \) and \( s \upharpoonright AC \) are plays in \( AB, BC \) and \( AC \) respectively.

**Proof.** By frugality of \( s \) and application of \( \gamma \), all projections satisfy frugality. Moreover, well-classing is preserved by projections. For well-calling, let \( m = \text{call}(s) \) be a move in \( s \) and let \( m^2 \) be the move introducing a in \( s \). Suppose \( p(m) \in \text{PO} \) and let us assume \( p(AB)(m) = O \). We need to show that \( o_{AB}(m) = P \). By \( \Pi \) we obtain that \( p(m) \in \{O_L, O_P, P\} \) and, by well-calling of \( s \), we have that \( a \in O \). Thus, \( p(n) \in \text{PO} \) and, by Lemma 3, it introduces a in \( s \upharpoonright AB \) and therefore \( o_{AB}(m) = P \). As \( s \upharpoonright AB \) and therefore \( \text{OO} \) and \( P \), as required. If, on the other hand \( p(AB)(m) = P \) then we obtain \( p(n) \in \text{OO} \cup \text{OP} \) and therefore, by Lemma 3, \( a \in P(s \upharpoonright AB) \cup O(s \upharpoonright AC) \). Thus, by the same lemma, \( \frac{a \notin P(s \upharpoonright AB) \text{ and hence } o_{AB}(a) = O. \text{ The cases for the other projections are shown similarly.} \)

In our setting programs will be represented by strategies between arenas. We shall introduce them next after a few auxiliary definitions. Intuitively, strategies capture the observable computational patterns produced by a program.

Let us define the following notion of subtyping between stores.
For \( \Sigma, \Sigma' \in \text{Sta} \leq \Sigma \) holds if, for all names \( a \),
\[ \Sigma(a) : T' \Longrightarrow \Sigma'(a) \leq T \land \forall \gamma \in \text{dom}(\Sigma(a)), \Sigma(a).f = \Sigma'(a).f. \]

In particular, if \( a \) is in the domain of \( \Sigma' \), \( \Sigma \) may contain more information about \( a \) because of assigning to \( a \) a larger interface. Accordingly, for plays \( s', s' \in \text{PAB} \), we say that \( s \) is an O-extension of \( s' \) if \( s \) and \( s' \) agree on their underlying sequences, while their stores may differ due to subtyping related to O-names. Where such subtyping leads to \( s \) having stores with more fields than those in \( s' \), \( P \) is assumed to copy the values of those fields. Formally, \( s \leq_O s' \) is defined by the rules:

\[ s \leq_O e \quad s \leq_O s' \quad \Sigma \leq \Sigma' \quad \Sigma \cap \text{P}(\text{sm}^2) \subseteq \Sigma' \quad \text{P}(m) = O \]

\[ \text{sn}^2 \leq s' \quad \Sigma \leq \Sigma' \quad \Sigma \text{ extends } \Sigma' \text{ by } T \quad \text{P}(m) = P \]

where \( \Sigma \) extends \( \Sigma' \) by \( T \) if:
- for all \( a \in \text{dom}(\Sigma) \setminus \text{dom}(\Sigma') \), \( \Sigma(a) = T(a); \)
- for all \( a \in \text{dom}(\Sigma) \setminus \text{dom}(\Sigma') \), \( \Sigma(a).f = T(a).f. \)

The utility of O-extension is to express semantically the fact that the environment of a program may use up-casting to inject in its objects additional fields (and methods) not accessible to the program.

**Definition 8.** A strategy \( \sigma \in AB \) is a non-empty set of even-length plays from \( PAB \) satisfying the conditions:
- if \( \text{sm}^2 \sim \text{sn}^2 \) then \( s \in \text{EFC} \).
- if \( \Sigma \in \text{EFC} \), \( \text{sn}^2 \neq \sigma \) then \( \text{sm}^2 \sim \text{sn}^2 \).
- if \( \Sigma \in \text{sm}^2 \) and \( \sigma \in \Sigma \).
- if \( \Sigma \in \text{sm}^2 \) and \( \sigma \in \Sigma \).

The utility of O-extension is to express semantically the fact that the environment of a program may use up-casting to inject in its objects additional fields (and methods) not accessible to the program.

**Definition 8.** A strategy \( \sigma \in AB \) is a non-empty set of even-length plays from \( PAB \) satisfying the conditions:
- if \( \text{sm}^2 \sim \text{sn}^2 \) then \( s \in \text{EFC} \).
- if \( \Sigma \in \text{sm}^2 \), \( \sigma \in \Sigma \).
- if \( \Sigma \in \text{EFC} \), \( \sigma \in \Sigma \).

The utility of O-extension is to express semantically the fact that the environment of a program may use up-casting to inject in its objects additional fields (and methods) not accessible to the program.
with \( s'm^n = sm^n \mid \gamma AB \) and \( s'n^T = sn^T \mid \gamma AB \). We therefore have \( (s', m^n) \sim (s', n^T) \) and, trivially, \( (s, s') \sim (s, s') \).

Moreover, by Lemma 3, \( \nu(m^n) \cap \nu(s) \subseteq \nu(s') \) and \( \nu(n^T) \cap \nu(s) \subseteq \nu(s') \) hence, by Strong Support Lemma [26], \( sm^n \sim sn^T \).

By Laird’s last set of conditions, the remaining values of \( \Sigma, T \) are determined by the last store in \( s, hence \( sm^n \sim sn^T \).}

}\]

**Lemma 6.** If \( s_1, s_2 \in \sigma|\tau \) end in moves with polarities in \( p(AC) \) and \( s_1 |\gamma AC = s_2 |\gamma AC \) then \( s_1 \sim s_2 \).

*Proof.* By induction on \( |\gamma AC | \geq 0 \). The base case is encompassed in \( s_1 = s_2m^n \) with \( p(m) \in OO, i = 1, 2 \), where note that by IH \( m \) will have the same polarity in \( s_1, s_2 \). Then, by IH we get \( s_1 = \pi \cdot s_2 \), for some \( \pi \). Let \( s_1'm^n = s_1 |\gamma AC \), for \( i = 1, 2 \), so in particular \( s_1' = \pi : s_2' \) and therefore \( (s_1, s_1') \sim (s_2, s_2') \). Moreover, by hypothesis, we trivially have \( (m^n, s_1') \sim (m^n, s_2') \) and hence, by Lemma 3 and Strong Support Lemma [26], we obtain \( s_1'm^n \sim s_2'm^n \) which implies \( s_1 \sim s_2 \) by Laird’s conditions.

Suppose now \( s_1 = s_2m^n, i = 1, 2 \), with \( p(m) \in P(AC) \setminus OO \) and the last move in \( s_1 \) being the last move in \( s_2 \), having polarity in \( p(AC) \). By IH, \( s_1 \sim s_2 \). Then, by consecutive applications of Lemma 5, we obtain \( s_1 \sim s_2 \).

}\]

**Proposition 7.** If \( \sigma : A \rightarrow B \) and \( \tau : B \rightarrow C \) then \( \sigma; \tau : A \rightarrow C \).

*Proof.* We show that \( \sigma; \tau \) is a strategy. Even-prefix closure and equivariance are clear. Moreover, since each \( s \in \sigma|\tau \) has even-length projections in \( AB \) and \( BC \), we can show that its projection in \( AC \) is even-length too. For O-extension, if \( s \in \sigma|\tau \) and \( t \leq s \) with \( u = u |\gamma AC \) and \( u \in \sigma|\tau \), we can construct \( v |\gamma AC \) such that \( t = v |\gamma AC \) and \( v \leq u \), where \( \leq u \) is defined for intersection sequences in an analogous way as for plays (with condition \( p(m) = O \) replaced by \( p(m) \in OO \), and \( p(m) = P \) by \( p(m) \in PO \cup OP \)). Moreover, \( v |\gamma AB \leq u |\gamma AB \) and \( v \mid |\gamma BC \leq u \mid |\gamma BC \), so \( t \in \sigma|\tau \). Finally, for determinacy, let \( \sigma = \sigma \mid \gamma \) be due to \( s_1,m, s_2,m^{n'} \) in \( \sigma|\gamma \) respectively, where \( s_1, s_2 \) both end in the last move of \( s \). By Lemma 6, we have \( s_1 \sim s_2 \) and thus, by consecutive applications of Lemma 5, we get \( s_1,m^{n'} \sim s_2,m^{n'} \), hence \( sm^n \sim sn^T \).

The above result shows that strategies are closed under composition. We can prove that composition is associative and, consequently, obtain a category of games.

**Proposition 8.** For all \( \rho : A \rightarrow B, \sigma : B \rightarrow C \) and \( \tau : C \rightarrow D \), \( (\rho; \sigma; \tau) = (\rho; (\sigma; \tau)) \).

*Definition 9.* Given a class table \( \Delta \), we define the category \( G_\Delta \) of arenas as objects and strategies as morphisms. Identity morphisms are given by \( \text{id}_A \) for each arena \( A \).

Note that neutrality of identity strategies easily follows from the definitions and, hence, \( G_\Delta \) is well defined. In the sequel, when \( \Delta \) can be inferred from the context, we shall write \( G_\Delta \) simply as \( G \).

As a final note, for class tables \( \Delta \subseteq \Delta' \), we can define a functor \( \Delta/\Delta' : G_\Delta \rightarrow G_{\Delta'} \) which acts as the identity map on arenas, and sends each \( \sigma : A \rightarrow B \) of \( G_\Delta \) to:

\[
(\Delta/\Delta') (\sigma) = \{ s \in P^\Delta_{AB} \mid \exists t \in \sigma, s \leq t \}
\]

where \( P^\Delta_{AB} \) refers to plays in \( G_{\Delta} \). In the other direction, we can define a strategy transformation:

\[
(\Delta'/\Delta) (\sigma) = \sigma \cap P^\Delta_{AB}
\]

which satisfies \( \Delta'/\Delta (\Delta/\Delta' (\sigma)) = \sigma \).

**4. Soundness**

Here we introduce constructions that will allow us to build a model of IMJ. We begin by defining a special class of strategies. A strategy \( \sigma : A \rightarrow B \) is called **evaluated** if there is a function \( f_\sigma : MA \rightarrow MB \) such that:

\[
\sigma = \{ m^\Sigma_A m^\Sigma_B \in P_{AB} \mid m_B = f_\sigma(m_A) \}.
\]

Note that equivariance of \( \sigma \) implies that, for all \( m_A \in MA \) and permutations \( \tau \), it holds that \( \tau \cdot f_\sigma(m_A) = f_\sigma(\tau \cdot m_A) \). Thus, in particular, \( f_\sigma(m_A) \subseteq \nu(m_A) \).

Recall that, for arenas \( A \) and \( B \), we can construct a product arena \( A \times B \). We can also define projection strategies:

\[
\pi_1 : A \times B \rightarrow A = \{(m_A, m_B) \in P(A \times B)A \}
\]

and, analogously, \( \pi_2 : A \times B \rightarrow B \). Note that the projections are evaluated. Moreover, for each object \( A \),

\[
\Pi_A = \{ m^\Sigma_A \in P_{A1} \}
\]

is the unique evaluated strategy of type \( A \rightarrow 1 \).

Given strategies \( \sigma : A \rightarrow B \) and \( \tau : A \rightarrow C \), with \( \tau \) evaluated, we define:

\[
(\sigma, \tau) : A \rightarrow B \times C = \{ m^\Sigma_A \mid \exists (m_B, f_\sigma(m_A)) \in P_{AB} A \}
\]

where we write \( s[m^n/|m_B] \) for the sequence obtained from \( s \) by replacing any occurrences of \( m_B \) in it by \( m^n \) (note that there can be at most one occurrence of \( m_B \) in \( s \)).

The above structure yields products for evaluated strategies.

**Lemma 9.** Evaluated strategies form a wide subcategory of \( G \) which has finite products, given by the above constructions.

Moreover, for all \( \sigma : A \rightarrow B \) and \( \tau : A \rightarrow C \) with \( \tau \) evaluated,

\[
(\sigma, \tau) : A \rightarrow B \times C = \{ m^\Sigma_A \mid \exists (m_B, f_\sigma(m_A))/|m_B] \}
\]

where \( \Sigma = \{ (\sigma, \tau) \} \). The above represents a notion of **left-pairing** of \( \sigma \) and \( \tau \), where the effects of \( \sigma \) precede those of \( \tau \). We can also define a **left-tensor** between strategies:

\[
\sigma \times \tau = A \rightarrow B \times C = \{ (\sigma_1, \sigma_2) \mid \exists (\sigma, \tau) \}
\]

for any \( \sigma : A \rightarrow A' \times B' \).

**Lemma 10.** Let \( \tau' : A' \rightarrow A, \sigma : A \rightarrow B_1, \tau : A \rightarrow B_2, \sigma_1 : B_1 \times B_2 \rightarrow C_1 \) and \( \sigma_2 : B_2 \rightarrow C_2 \) with \( \tau \) and \( \tau' \) evaluated. Then \( \tau' \cdot (\sigma, \tau) \cdot (\sigma_1, \sigma_2) = (\tau' \cdot \sigma, \tau \cdot \sigma_1, \tau' \cdot \sigma_2) \).

*Proof.* The result follows from the simpler statements:

\[
\tau; (\sigma, 1d) = (\tau; \sigma, \tau) = (\sigma, \tau; d); (\sigma', 1d) = (\sigma; \sigma'; d),
\]

for all appropriately typed \( \sigma, \sigma', \tau, \tau' \).

An immediate consequence of the above is:

\[
A \rightarrow B_1 \times B_2 \rightarrow C_1 \times C_2 = A \rightarrow B_1 \times B_2 \rightarrow C_1 \times C_2
\]

More generally, Lemma 10 provides us with naturality conditions similar to those present in **Freyd categories** [25] or, equivalently, categories with monadic products [22].

We also introduce the following weak notion of coproduct.

Given strategies \( \sigma, \tau : A \rightarrow B \), we define:

\[
[s, \tau] : A \rightarrow B = \{ (1, m^\Sigma_A s) \mid m^\Sigma_A s \in \sigma \}
\]

\[
\cup \{ (0, m^\Sigma_A s) \mid m^\Sigma_A s \in \tau \}
\]


Setting $\tilde{i} : 1 \to Z = \{\ast i\}$, for each $i \in Z$, we can follow the showing.

**Lemma 11.** For all strategies $\sigma' : A' \to A$ and $\sigma, \tau : A \to B$,

- $\langle \{\tilde{1}, \tilde{0}, \tilde{i}, \tilde{id}\} : [\sigma, \tilde{id}] = \tau$ and $\langle \{\tilde{1}, \tilde{i}, \tilde{id}\} : [\sigma, \tilde{id}] = \sigma'$;

- if $\sigma'$ is evaluated then $\langle 1 \Delta . \times \sigma' \rangle \{[\sigma, \tilde{id}] = [\sigma', \tilde{id}]. \tau\} = \tau$.

Method definitions in IMJ induce a form of exponentiation:

$$\bigwedge_{n=1}^\infty (\Delta(\Gamma \cup \langle 1 \Delta . \times \sigma' \rangle \{[\sigma, \tilde{id}] = [\sigma', \tilde{id}] \times \tau\}) \in \Delta(\Gamma \cup \langle 1 \Delta . \times \sigma' \rangle \{[\sigma, \tilde{id}] = [\sigma', \tilde{id}] \times \tau\})$$

the modelling of which requires some extra semantic machinery. Traditionally, in call-by-value game models, exponentiation leads to 'effectless' strategies, corresponding to higher-order value terms. In our case, higher-order values are methods, manifesting themselves via the objects they may inhabit. Hence, exponentiation necessarily passes through generation of fresh object names containing these values. These considerations give rise to two classes of strategies introduced below.

We say that an even-length play $s \in P_{AB}$ is total if it is either empty or $s = m_1^A m_2^B w T s'$ and:

- $T \in Stoo$ and $\nu(m_B) \land \nu(\Sigma) \subseteq \nu(m_A)$,
- $s' = s'' m_B w T$ and $a \in \dom(\Sigma) \subseteq \nu(\gamma(m_0^A m_B w T s'))$ for $\Sigma_0 \in Stoo$ such that $\gamma(m_0^A m_B w T s') \in P_{AB}$, then $a \notin \nu(n)$ and $T(a) = \Sigma'(a)$.

We write $P_{AB}^\ast$ for the set of total plays in $AB$. Thus, in total plays, the initial move $m_A$ is immediately followed by a move $m_B$, and the initial store $\Sigma$ is invisible to $P$ in the sense that $P$ cannot use its names nor their values. A strategy $\phi : A \to B$ is called single-threaded if it consists of total plays and satisfies the conditions:

- for all $m_A^\Sigma \in P_{AB}$ there is $m_A^\Sigma m_B^T s' \in \phi$;
- if $m_A^\Sigma m_B^T s \in \phi$ then $\gamma(m_A^\Sigma m_B^T s') \in \phi$, for $\Sigma_0 \in Stoo$;
- if $m_A^\Sigma m_B^T s \in \phi$ then $a \in \nu(T)$ then $s = e$.

Thus, single-threaded strategies reply to every initial move $m_A^\Sigma$ with a move $m_B^T$ which depends only on $m_A^\Sigma$ (i.e. $P$ does not read before playing). Moreover, $m_B^T$ does not change the values of $\Sigma$ ($P$ does not write) and may introduce some fresh objects, albeit with default values. Finally, plays of single-threaded strategies consist of just one thread, where a thread is a total play in which there can be at most one call to names introduced by its second move.

Conversely, given a total play starting with $m_A^\Sigma m_B^T s$, we can extract its threads by tracing back for each move in $s$ the method call of the object $a \in \nu(T)$ (it is related to $F$). Formally, for each total play $s = m_A^\Sigma m_B^T s'$ with $|s'| > 0$, the threader move of $s$, written thr$(s)$, is given by induction:

- thr$(s' m_B^{\nu(T)}) = thr (s')$, if $p(m) = P$;
- thr$(s' a. m.(\tilde{v})^{\Sigma'}) = call a. m.(\tilde{v})^{\Sigma'}$, if $a \in \nu(T)$;
- thr$(s' a. n^{T'}) = thr (s' a. n^{T'})$, if $a \in \nu(T) ;$ and $n$ introduces $a$.
- thr$(s' n^{T'}) = thr (s' n^{T'})$, if $p(m) = O$ and $n$ justifies $m$.

If $s = s' n^{T'} s''$ with $|s'| \geq 2$, we set thr$(n^{T'}) = thr (s' n^{T'} s'')$. Then, the current thread of $s$ is the subsequence of $s$ containing only moves with the same threader move as $s$, that is, if thr$(s) = m_B^{\nu(T)}$ and $s = m_A^\Sigma m_B^T s'$ then

$$[s] = m_A^\Sigma m_B^T s' \in \Sigma'$$

Note that the use of the term "thread" here is internal to game semantics parlance and in particular should not be confused with Java threads.

where the restriction retains only those moves $n^{T'}$ of $s'$ such that thr$(n^{T'} m^{\nu(T)}) = m^{\nu(T)}$. We extend this to the case of $|s| \leq 2$ by setting $[s] = s$. Finally, we call a total play $s \in P_{AB}$ thread-independent if for all $s' m_B^{\nu(T)} \subseteq s$ with $|s'| > 2$:

- if $\gamma([s' m^{\nu(T)}]) = s'' m^{\nu(T)}$ then $\nu(\gamma([s' m^{\nu(T)}]))$ then $\Sigma'n(a) = T'(a)$.

We write $P_{AB}^\ast$ for the set of thread-independent plays in $AB$.

We can now define strategies which occur as interleavings of single-threaded ones. Let $\phi : A \to B$ be a single-threaded strategy. We define:

$$\phi^1 = \{s \in P_{AB}^\ast | \forall s' \in \nu(s), \gamma([s']) \in \phi \}.$$
Let now $\sigma_1, \ldots, \sigma_n$ be strategies with $\sigma_i : A \times [\bar{v}] \to [\theta_i]$.
For each $i$, we define the single-threaded strategy $\Lambda(\sigma_i) : A \to \mathcal{I}$:
$$\Lambda(\sigma_i) = \{ m_{A} A \oplus \Sigma_{\mathcal{T}} \text{call } a.m.(\bar{v})^{T} s \in P_{\mathcal{A}} \mid \gamma((m_{A}, \bar{v})^{T} s) \in \sigma_i \}$$
where $\gamma(a, \bar{v})^{T} s$ is the name of the object we want to return. The name $a'$ serves as a store where the handle of the method implementations, that is, the name created by the second move of $[M]$, will be passed. The strategy $\kappa_{\Sigma_{\mathcal{T}}}$, upon receiving a request $\text{call } a.m.(\bar{v})^{T}$, simply forwards it to the respective method of $a'$. If, and only if it receives a return value, copies it back as the return value of the original call.

Finally we define, for each field $f$, the object creation involving creating a pair of names $(\alpha, \alpha')$ with $a : \mathcal{T}$ and $a' : \mathcal{T}'$, where $\alpha$ is the name of the object we want to return. The name $\alpha'$ serves as a store where the handle of the method implementations, that is, the name created by the second move of $[M]$, will be passed. The strategy $\kappa_{\Sigma_{\mathcal{T}}}$, upon receiving a request $\text{call } a.m.(\bar{v})^{T}$, simply forwards it to the respective method of $\alpha'$. If, and only if it receives a return value, copies it back as the return value of the original call.

We next define the following natural mapping from groups of strategies $\Sigma_{\mathcal{T}}$ to thread-independent ones in $A \to [\theta]$ to thread-independent ones in $A \to [\theta]$. We can now show the following natural mapping from groups of strategies in $A \times [\bar{v}] \to [\theta]$ to thread-independent ones in $A \to [\theta]$.

**Lemma 14.** Let $\sigma_1, \ldots, \sigma_n$ be as above, and let $\tau : \Delta' \to \Delta$ be evaluated. Then,
$$\bullet \Lambda(\sigma_1, \ldots, \sigma_n) \times \text{id} ; ev_{\theta} = \sigma_i,$$
$$\circ \Lambda(\sigma_1, \ldots, \sigma_n) \times (\tau \times \text{id}) ; ev_{\theta} = \Lambda(\tau \times \text{id}) ; \sigma_1, \ldots, (\tau \times \text{id}) ; \sigma_n.$$
commute (we write $A$ for $[\Gamma] \ni \theta$),

\[
\begin{array}{c}
\frac{[\Gamma] \ni \alpha_i : \mathcal{I}_i}{[\Gamma] \ni \alpha_i : \mathcal{I}_i} \\
\frac{[\Gamma] \ni \alpha_i : \mathcal{I}_i}{[\Gamma] \ni \alpha_i : \mathcal{I}_i}
\end{array}
\]

\[
\begin{array}{c}
\frac{[\Gamma] \ni \alpha_i : \mathcal{I}_i}{[\Gamma] \ni \alpha_i : \mathcal{I}_i} \\
\frac{[\Gamma] \ni \alpha_i : \mathcal{I}_i}{[\Gamma] \ni \alpha_i : \mathcal{I}_i}
\end{array}
\]

that the copy of $\mathcal{M}_i$ differs from the original just in the handle name (the one returned in the codomain of $[\mathcal{M}_i]$), but the latter is hidden via composition with $\psi_m$. The latter diagram stipulates that if we create a $\vec{a}$ with methods $\vec{M}$, then calling $\alpha_i$ on $m$ is the same as calling $\mathcal{M}_i$ on $m$. The latter holds because of the way that $\kappa_{\vec{m}}$ manipulates calls inside the interaction, by delegating calls to methods of $\alpha_i$ to $\mathcal{M}_i$.

\begin{proposition}[Computational Soundness] For all $\vdash \Gamma : \text{void}$, if $\mathcal{M} \upharpoonright \{\ast\}$ then $[\mathcal{M}] = \{\ast\}$ (i.e. $[\mathcal{M}] = [\text{skip}]$).
\end{proposition}

\begin{proof}
This directly follows from Correctness.
\end{proof}

\begin{proposition}[Computational Adequacy] For all $\vdash \Gamma : \text{void}$, if $[\mathcal{M}] = \{\ast\}$ then $\mathcal{M} \upharpoonright \{\ast\}$.
\end{proposition}

\begin{proof}
Suppose, for the sake of contradiction, that $[\mathcal{M}] = \{\ast\}$ and $\mathcal{M} \upharpoonright \{\ast\}$. We notice that, by definition of the translation for blocking constructs (castings and conditionals may block) and due to Correctness, if $\mathcal{M} \upharpoonright \{\ast\}$ due to some reduction step being blocked then the semantics would also block. Thus, $\mathcal{M} \upharpoonright \{\ast\}$ must be due to divergence. Now, the relation reduction restricted to all rules but METHODCL. is strongly normalising, as each transition decreases the size of the term. Hence, if $\mathcal{M}$ diverges then it must involve infinitely many METHODCL. reductions and our argument below shows that the latter would imply $[\mathcal{M}] = \{\epsilon\}$.

For any term $\Gamma \vdash \mathcal{N} : \theta$ and $\vec{a} \in \mathcal{A} \setminus \text{dom}(\Gamma)$, construct $\Gamma_{\vec{a}} \vdash \mathcal{N}_{\vec{a}}$, where $\Gamma_{\vec{a}} = \Gamma \upharpoonright \{a : \alpha\}$, by recursively replacing each subterm of $\mathcal{N}$ of the shape $\mathcal{N}.m(\vec{N})$ with $\vec{a} := (\vec{a} + 1); N'.m(\vec{N})$. 

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure4.png}
\caption{The semantic translation of IMJ.}
\end{figure}
Var I is an interface with a sole field f : int. Observe that each s ∈ [I + N] induces some s′ ∈ [Γa + Na] such that a appears in s′ only in stores (and in a single place in the initial move) and O never changes the value of a.f, while P never decreases the value of a.f. We write [Γa + Na] for the subset of [I + Na] containing precisely these plays. Then, take M0, to be the term let s = new(x : Var I) in (M0[x/a]:x.f), where x a fresh variable. Because ∗∗ ∈ [M], we get s ∈ [M0] for some j ∈ Z. Consider now the infinite reduction sequence of (∅, M). It must have infinitely many MethodCL steps, so suppose (∅, M) −→ (S, M′) contains j + 1 such steps. Then, we obtain (∅, M0) −→ (S0, (M′0)α; a.f), with S0(a).f = j + 1. By Correctness, we have that s+j ∈ [S0, (M′0)α; a.f] = [Sα; (ιd×#)]; ((M′0)α; a.f)α. Since in [(M′0)α]a the value of a cannot decrease, and its initial value is j + 1 (as stipulated by Sα), we reach a contradiction.

5. Full Abstraction

Recall that, given plays s, s′, we call an O-extension of s′ (written s ≤ O s′) if s, s′ are identical except the type information regarding O-names present in stores: the types of O-names in s may be subtypes of those in s′. We shall write s ≤ p s′ for the dual notion involving P-names, i.e., s ≤ p s′ if s, s′ are the same, but the types of P-names in s′ may be subtypes of those in s. Then, given X ∈ {O, P} and fixed A, B, let us define cl(x)(s) = {s′ ∈ PA(B); s′ ≤ x s} and cl(x)(σ) = U ∈∈ cl(x)(s). We write PA+[I;θ] for P[1][I;θ]. A play will be called complete if it is of the form m1,Y m2,Y.

Next we establish a definability result stating that any complete play (together with other plays implied by O-closure) originates from a term.

Lemma 18 (Definability). Let s ∈ P[Δ[I;θ] be a complete play. There exists Δ′ ⊇ Δ and Δ′[I;θ] M : 0 such that ∑Δ′[I;θ] M : θ = clO(s).

Proof. The argument proceeds by induction on ∣s∣. For s = ϵ, any divergent term suffices. For example, one can take Δ′ = ∆ ⊕ [Div m : void → void], and pre-compose any term of type ϵ with new(x : Div; m : Λ(0)(m)) : Λ(0)(m). Suppose s ≠ ϵ. Then the second move can be a question or an answer. We first show how to reduce the former case to the latter, so that only the latter needs to be attacked directly.

Suppose s = qΣv call o.m(⟨u⟩ Σi s1 ret o.m(v) Σ2 s2 Σ3 s3, where o : (I′ and Δ(⟨I′⟩) : m : I′) → IR. Consider Δ′ = ∆ ⊕ (Δ′[I′] m : I′ → θ) and the following play from P[Δ[I;θ]]:

s′ = qΣv pΣy s′1 call p.m(ν) Σ′2 s′2 ret p.m(ν) Σ′3 s′3, where p /∈ v(s), Σ′ = Σi ⊇ Σ = {p → (⟨I′′⟩, f′ → u)} and s′j is the same as sj except that each store is extended by Σ. If Δ′[I;θ] M : θ satisfies the Lemma for s′ then, for s, one can take the case that points at o in Σv. Thanks to the reduction given above we can now assume that s ∈ P[Δ[I;θ] is non-empty and

s = qΣv m0 Σ1 m1 Σ2 m2k Σ2k, where m0 is an answer. We are going to enrich s in two ways so that it is easier to decompose. Ultimately, the decomposition of s will be based on the observation that the m1 Σ2 m2k segment can be viewed as an interleaving of threads, each of which is started by a move of the form call p for some P-name p. A thread consists of the starting move and is generated according to the following two rules: m0 begins to the thread of m2k−1 and every answer-move belongs to the same thread as the corresponding question-move.

• The first transformation of s brings forward the point of P-name creation to the second move. In this way, threads will never create objects and, consequently, it will be possible to compose them without facing the problem of object fusion.

Suppose P(s) = p⊥ and p⊥ : I0. Let Δ′ = Δ ⊕ (I0 → f; I0). Consider s′ = (p, q)Σv m0 Σ1 m1 Σ2 m2k Σ2k, where Σv = Σi ⊇ {n → (Ip, null)} and Σi = Σi ⊇ {n → (Ip, p⊥)} ⊕ {p1 → (I0, null)} | Σi(πj) undefined, p1 ∈ P(s).

• The second transformation consists in storing the unfolding play in a global variable. It should be clear that the recursive structure of types along with the ability to store names is sufficient to store plays in objects. Let Iplay be a signature that makes this possible. This will be used to enforce the intended interleaving of threads after their composition (in the style of Innocent Factorization [5]). Let Δ′ = Δ ⊕ (History → play : Iplay) and Γ′ = {xk : History} ⊇ Γ. Consider

s′ = (h, n, q)Σv m0 Σ1 m1 Σ2 m2k Σ2k with

Σv = Σj ⊇ {h → (History, play → null)}.

Now we shall decompose m1 Σ2 m2k into threads. Recall that each of them is a subsequence of s′ of the form

call p.m(ν)Σv t ret p.m(ν)Σv,

where the segment t contains moves of the form call o or ret o for some o ∈ O(s). We would now like to invoke the IH for each thread but, since a thread is not a play, we do so for the closely related play (h, n, q, w)Σv t′ v′. Let us call the resultant term Mp,m,wκ,Σ. Next we combine terms related to the same p : Ip into an object definition by

M_p ≜ new(x : Ip : m : Λκ.case(u : Σκ)(M_p,m,wκ,Σκ)).

The case statement, which can be implemented in IMJ using nested ifs, is needed to recognize instances of u and Σκ that really occur in threads related to p. In such cases the corresponding term Mp,m,wκ,Σκ will be run. Otherwise, the statement leads to divergence.

The term M for s can now be obtained by taking

let x_n = new(x : Ip) in
let x_h = new(x : History) in
let x_p = M_p in
assert(qΣv); x_n.f_t = x_p.f; make(Σv); play(m0)}

where x_p = M_p represents a series of bindings (one for each P-name p, p ∈ P(s)), assert(h, n, q)Σv is a conditional that converges if and only if the initial values of free Θ identifiers as well as values accessible through them are consistent with Σv and S, respectively, make(Σv) is a sequence of assignments that set values to those specified in Σv (up-casts need to be performed to ensure typability) and play(m0) is skip, i, null, or if, m0 is a name,
Proof. The Lemma holds because, on the one hand, it relies on contexts of a specific shape and, on the other hand, any closing context $C[-]$ for $M$ can be presented in the above form with test $\equiv C[z, f(x_1, \ldots, x_k)]$.

Given a term $\Delta[M] = \theta$, let us write $[\Delta[M] = \theta]$ for the set of complete plays from $\{[\Delta[M] = \theta]\}$ in what follows. We shall often omit $\Delta_\theta$ for brevity.

Theorem 21 (Equational full abstraction). Given $\Delta[M_1] \equiv \theta$ (i.e., $\Delta[M_1] = \theta$).

The preceding result implies that $M_1 \cong M_2$ if and only if $cl_P([\Delta[M_1] = \theta]) = cl_P([\Delta[M_2] = \theta])$. We show that this implies $Cl([\Delta[M_1] = \theta]) = cl_P([\Delta[M_2] = \theta])$. Let $s \in [\Delta[M_1] = \theta]$. By $cl_P([\Delta[M_1] = \theta]) = cl_P([\Delta[M_2] = \theta])$, it must be the case that $s \in cl_P([\Delta[M_2] = \theta])$, i.e., there exists $s' \in [\Delta[M_2] = \theta]$ such that $s \in cl_P(s')$. Again, by $cl_P([\Delta[M_1] = \theta]) = cl_P([\Delta[M_2] = \theta])$, it follows that $s' \in cl_P([\Delta[M_2] = \theta])$.

References