Separability, Expressiveness, and Decidability in the Ambient Logic
Daniel Hirschkoff, E. Lozes, D. Sangiorgi

To cite this version:

HAL Id: hal-02101816
https://hal-lara.archives-ouvertes.fr/hal-02101816
Submitted on 17 Apr 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Separability, Expressiveness, and Decidability in the Ambient Logic

Daniel Hirschkoff¹, Étienne Lozes¹, and Davide Sangiorgi²

¹ LIP - ENS Lyon, France
² INRIA Sophia Antipolis, France

April 2002

Research Report N° 2002-18
Separability, Expressiveness, and Decidability in the Ambient Logic

Daniel Hirschkoff¹, Étienne Lozes¹, and Davide Sangiorgi²

¹ LIP - ENS Lyon, France
² INRIA Sophia Antipolis, France

April 2002

Abstract

The Ambient Logic (AL) has been proposed for expressing properties of process mobility in the calculus of Mobile Ambients (MA), and as a basis for query languages on semistructured data.

We study some basic questions concerning the descriptive and discriminating power of AL, focusing on the equivalence on processes induced by the logic (≈ₐ). We consider MA and two Turing complete subsets of it, MAIF and MAIFsyn, respectively defined by imposing a semantic and a syntactic constraint on process prefixes.

The main contributions include: coinductive and inductive operational characterisations of ≈ₐ; an axiomatisation of ≈ₐ on MAIFsyn; the construction of characteristic formulas for the processes in MAIF with respect to ≈ₐ; the decidability of ≈ₐ on MAIF and on MAIFsyn, and its undecidability on MA.

Keywords: Distributed and mobile systems, modal logics, Mobile Ambients, decidability, expressiveness, characteristic formula

Résumé

La Logique des Ambients (AL) a été introduite pour exprimer des propriétés ayant trait à la mobilité des processus dans le calcul des Ambients Mobiles (MA), ainsi qu'en tant que fondement pour des langages de requêtes pour des données semi-structurées.

Nous étudions un certain nombre de questions fondamentales ayant trait au pouvoir expressif de cette logique, en nous intéressant à l'équivalence sur les processus induite par la logique (≈ₐ). Nous considérons AM, ainsi que deux sous-ensemble Turing complets de ce calcul, MAIF et MAIFsyn, définis par le biais de restrictions syntaxique et sémantique sur les termes préfixes.

Parmi nos principales contributions, nous pouvons mentionner: deux caractérisations, coinductive et inductive, de ≈ₐ; une axiomatisation de ≈ₐ sur MAIFsyn; la construction de formules caractéristiques pour ≈ₐ pour les processus de MAIF; la décidabilité de ≈ₐ sur MAIF et sur MAIFsyn, et la non-décidabilité de cette relation sur MA.

Mots-clés: Systèmes distribués et mobiles, logique modale, Ambients mobiles, décidabilité, expressivité, formule caractéristique
1 Introduction

The Ambient Logic, AL, [9] is a modal logic for expressing properties of processes in the calculus of Mobile Ambients, MA [7, 8]. In MA the unit of movement is an ambient, which, intuitively, is a named location. An ambient may contain other ambients, and capabilities, which determine the ambient movements. The primitives for movement allow: an ambient to enter a sibling ambient; an ambient to exit the parent ambient; a process to dissolve an ambient boundary. MA has a replication operator to make a process persistent, that is, to make infinite copies of the process available.

An ambient can be thought of as a labelled tree. The sibling relation on subtrees represents spatial contiguity; the subtree relation represents spatial nesting. A label may represent an ambient name or a capability; moreover, a replication tag on labels indicates the resources that are persistent.\footnote{We are using a tree representation different from that of Cardelli and Gordon, but more convenient to our purposes.} The trees are unordered: the order of the children of a node is not important. As an example, the process $P \overset{\text{def}}{=} \lambda a \mid \text{open } a$.b\{0\} is represented by the tree:

$$
\begin{array}{c}
\lambda a \\
\text{in c} \\
\downarrow \\
b \\
\end{array} \quad \text{open} \ a
$$

The replication $\lambda a$ indicates that the resource $a \mid \text{in c}$ is persistent: unboundedly many such ambients can be spawned. By contrast, open $a$ is ephemeral: it can open only one ambient.

Syntactically, each tree is finite. Semantically, however, due to replications, a tree is an infinite object. As a consequence, the temporal developments of a tree can be quite rich. The process $P$ above (we freely switch between processes and their tree representation) has only one reduction, to in c $\mid \lambda a \mid \text{in c} \mid b\{0\}$. However, the process $\lambda a \mid \text{in c} \mid \text{open} a \cdot b\{0\}$ can evolve into any process of the form

$$
in \ c \mid \ldots \mid \text{in c} \mid b\{0\} \mid \ldots \mid b\{0\} \mid \lambda a \mid \text{in c} \mid \text{open} a \cdot b\{0\}.
$$

In general, a tree may have an infinite temporal branching, that is, it can evolve into an infinite number of trees, possibly quite different from each other (for instance, pairwise behaviourally unrelated). Technically, this means that the trees are not image-finite.

In summary, MA is a calculus of dynamically-evolving unordered edge-labelled trees. AL is a logic for reasoning on such trees. Indeed, the actual definition of satisfaction of the formulas is given on MA processes quotiented by a relation of structural congruence, which equates processes with the same tree representation. (This relation is similar to Milner's structural congruence for the $\pi$-calculus [18].)

AL has also been advocated as a foundation of query languages for semistructured data [5]. Here, the laws of the logic are used to describe query rewriting rules and query optimisations. This line of work exploits the similarities between dynamically-evolving edge-labelled trees and standard models of semistructured data.

AL has a connective that talks about time, that is, how processes can evolve. The logic has also connectives that talk about space, that is, the shape of the
edge-labelled trees that describe process distributions. AL is quite different from
standard modal logics. First, such logics do not talk about space. Secondly,
they have more precise temporal connectives. The only temporal connective
of AL talks about the many-step evolution of a system on its own. In stan-
standard modal logics, by contrast, the temporal connectives also talk about
the potential interactions between a process and its environment. For instance, in
the Hennessy-Milner logic [15], the temporal modality $\langle \mu \rangle$. $A$ is satisfied by
the processes that can perform the action $\mu$ and become a process that satisfies $A$.
The action $\mu$ can be a reduction, but also an input or an output.

In this paper we study some basic questions concerning the descriptive and
discriminating power of AL. We consider, besides the calculus MA, two subsets
of it, obtained by imposing constraints on the processes underneath capabilities.
In $\text{MA}_{IF}^\text{sym}$, these processes must be image-finite; in $\text{MA}_{IF}^\text{sym}$, they must be finite.
These definitions might appear ad hoc, but they express precisely the constraints
needed in some of our results. A further interest of $\text{MA}_{IF}^\text{sym}$ is that its definition
is purely syntactic. Both $\text{MA}_{IF}$ and $\text{MA}_{IF}^\text{sym}$ are Turing complete, and contain
processes that are not image-finite.

We describe the main contributions of the paper. We write $=_L$ to indicate
the process equivalence induced by the logic, whereby two terms are equated if
they satisfy the same sets of formulas. First, we exhibit two operational char-
acterisations of $=_L$ on MA, which do not mention the logic. Characterisations
of the equivalence of a logic allow us to understand the notion of equality on
processes – a fundamental notion in process calculi – induced by the logic. One
characterisation is inductive, as a form of labelled bisimilarity. The other is
inductive, and uses a well-founded measure on the structure of processes.

Second, we prove that $=_L$ coincides with structural congruence on $\text{MA}_{IF}^\text{sym}$.
This gives us an axiomatisation of $=_L$ on $\text{MA}_{IF}^\text{sym}$. This axiomatic characterisa-
tion is false on the larger class $\text{MA}_{IF}$.

Our third contribution is the construction of characteristic formulas for
equivalence classes for $=_L$ in $\text{MA}_{IF}$. We define, for any process $P \in \text{MA}_{IF}$,
a formula $\mathcal{F}_P$ such that $Q |_\mathcal{F}_P$ holds iff $Q =_L P$, for all $Q \in \text{MA}$. The result
shows that we can talk about the discriminating power of the logic from within
the logic itself; at least under some image-finiteness conditions. A corollary is
the undecidability of the model-checking problem on $\text{MA}_{IF}^\text{sym}$ and richer calculi.

Our fourth contribution is on (un)decidability. As a consequence of the
inductive characterisation of $=_L$, we can prove that $=_L$ is decidable on $\text{MA}_{IF}$
and $\text{MA}_{IF}^\text{sym}$. However, if we drop the image-finiteness conditions of $\text{MA}_{IF}$, then
$=_L$ becomes undecidable. We show this via an encoding of the halting problem
of Turing Machines. The encoding of Turing Machines is actually in $\text{MA}_{IF}^\text{sym}$,
which is thus proved to be Turing Complete. This result is not in contradic-
tion with the decidability of $=_L$ in $\text{MA}_{IF}$ and $\text{MA}_{IF}^\text{sym}$, because the encoding is correct
for reductions but not behaviourally (the process encoding a machine and its
derivatives do not need to be in the relation $=_L$).

Most of the results mentioned above are rather different from the usual re-
results of modal logics. Typically, the definition of characteristic formulas exploits
fixed-point operators, and the characterised processes are finite-state [14, 21].
AL, by contrast, has no fixed point operator; moreover the image-finiteness condi-
tion on processes is weaker than finite-state. (‘Image-finite’ expresses finite-
ness on internal reductions, whereas ‘finite-state’ also takes into account com-
putations containing visible actions such as input and output actions.)
Also, coinductive characterisations of an inductive relation or of the equivalence of a logic usually rely on either image-finiteness of the processes, or on some infinitary operator of the logics, such as infinite conjunctions. In our case we need none of these hypotheses. Further, the inductive relation is not the stratification of the coinductive relation [17], but uses a structural measure on processes. Finally, in process calculi decidability is usually unrelated to image-finiteness: for instance, the transition relation of the π-calculus is image-finite, yet strong bisimilarity is undecidable [20].

Also the actual form of image-finiteness that we use is non-standard. Behavioural equivalence in MA is insensitive to stuttering phenomena, originated by processes that may repeatedly enter and exit an ambient. As a consequence, a computation in which all visible actions are stuttering is semantically equivalent to an internal reduction.

In the proofs of the results two groups of technical lemmas are important. The first is about the construction of formulas for describing all forms of labels of the trees of MA. The formulas for the replicated labels give us (some of) the power of the ! operator ('of course') of linear logic; this was somehow unexpected, because AL has no infinitary operators, or operators that talk about resources with infinite multiplicity. (We obtain only some of this power, because we have to impose constraints on the replicated formulas.)

Other useful formulas that we have derived are the following: a formula \( \phi_{\text{fin}} \) that characterises the ephemeral processes (that is, \( P \models \phi_{\text{fin}} \) iff the tree of \( P \) has no replicated labels); for any set \( S \) of names, a formula \( \text{refers} \, S \) that characterises the processes whose set of free names is precisely \( S \).

The second group of technical lemmas captures decomposition properties of processes. For instance, Lemma 3.6 shows that any two processes \( P \) and \( Q \) in the relation =\( _L \) admit decompositions \( P = C[P] \) and \( Q = D[Q] \) where the contexts \( C \) and \( D \) are of a certain syntactic form, and, moreover, both the contexts \( C \) and \( D \), and the continuations \( P \) and \( Q \) (more precisely, processes obtained from appropriate transformation of these) are equivalent.

There are strong connections among all the results discussed above. For instance, both the characterisations of =\( _L \) and the characteristic formulas talk about the separability power of AL. The connections are explicit in the proofs: for instance, the proof of undecidability relies on most of the other results.

**Related work.** Characterisations and axiomatisations of =\( _L \) have already been presented in [19], on finite MA (without replications). The proofs rely on the ephemeral nature of the processes, precisely on the property that all (complete) computations of a process, comprising its interactions with the environment, are finite and terminate with the 0 process. Therefore we could not adapt these proofs to processes with replications. The need for stuttering in MA is already pointed out in [19], but all examples use trees with unbounded depth.

We are not aware of other axiomatisations of semantic equivalences in non-finite higher-order process calculi, and of characteristic formulas for logics for mobile processes. Formulas in AL, or similar logics, that characterise the free names of processes were known [10, 2], but use additional operators (notably the revelation operator). The undecidability of the model-checking problem of AL – in fact of an even smaller logic – had already been established, using different techniques [11].

3
2 Background

\[
a, b, \ldots, n, m
\]

<table>
<thead>
<tr>
<th>Names</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \text{Capabilities} )</td>
<td>( P, Q, R ::= 0 ) (nil)</td>
</tr>
<tr>
<td>( \text{cap} ::= ) in ( n ) ( ) (enter)</td>
<td>( P</td>
</tr>
<tr>
<td>( )</td>
<td>( \cap ). ( P ) (prefixing)</td>
</tr>
<tr>
<td>( )</td>
<td>( n[P] ) (ambient)</td>
</tr>
<tr>
<td>( )</td>
<td>( !P ) (replication)</td>
</tr>
</tbody>
</table>

| open \( n \) (open) | \( \) |

Table 1: The syntax of MA

We recall here the syntax of ‘pure’ MA, from [7]. (‘Pure’ means that computation is only movement; there are no communications.) Also, as in [9, 5, 6], the calculus has no restriction operator for creating new names. The restriction-free calculus is simpler, and has a more direct correspondence with edge-labelled trees and semistructured data. Table 1 presents the syntax. The set of names is infinite. \( \text{Capabilities} \) are ranged over by \( \text{cap} \), processes by \( P, Q, R, S \). Processes

\[
\begin{align*}
\text{Red-In} & \quad n[m \cdot P_1 | P_2 | m[Q] \to m[n \cdot P_1 | P_2 | Q] } \\
\text{Red-Out} & \quad \overline{m}[n \cdot \text{out } m \cdot P_1 | P_2 | Q \to n[P_1 | P_2 | m[Q]] } \\
\text{Red-Open} & \quad \text{open } n \cdot P | n[Q] \to P | Q \\
\text{Red-Par} & \quad P \to P' | Q \\
\text{Red-Amb} & \quad n[P] \to n[P'] \\
\text{Red-Stx} & \quad P_1 \equiv P_2 \quad P' \equiv P'' \quad P'' \equiv P''' \\
\end{align*}
\]

Table 2: The rules for reduction

with the same internal structure are identified. This is expressed by means of the structural congruence relation, \( \equiv \), the smallest congruence such that \( (0, !) \) is a multiset algebra, that is, satisfies the following rules:

\[
\begin{align*}
P | 0 & \equiv P \\
P | Q & \equiv Q | P \\
P | (Q | R) & \equiv (P | Q) | R \\
!P & \equiv !P | P \\
!(P | Q) & \equiv !P | Q \\
!!P & \equiv !P \\
0 & \equiv 0 .
\end{align*}
\]
Relation \( \equiv \) is decidable on \( \text{MA} \), as well as in other calculi such as the \( \pi \)-calculus \([12, 13]\). The rules for the reduction relation, \( \rightarrow \), are given in Table 2. The reflexive and transitive closure of \( \rightarrow \) is written \( \implies \).

**Definition 2.1 (Labelled transitions and stuttering)** We write:

- \( P \overset{\text{cap}}{\rightarrow} P' \), if \( P \equiv \text{cap}.P_1 \mid P_2 \) and \( P' = P_1 \mid P_2 \).

- (stuttering) \( P \overset{(M_1, M_2)^*}{\rightarrow} P' \) if there are \( r \geq 1 \) and processes \( P_1, \ldots, P_r \) with \( P = P_1 \) such that \( P_i \Rightarrow M_i \Rightarrow M_{i+1} \) for all \( 1 \leq i < r \), and \( P_r \Rightarrow P' \).

- Finally, \( \overset{\text{cap}}{\rightarrow} \) is a convenient notation for compacting statements involving capability transitions. \( \overset{\text{in n}}{\rightarrow} \) is \( \overset{(\text{in } n)}{\rightarrow} \); similarly \( \overset{\text{out n}}{\rightarrow} \) is \( \overset{(\text{out } n)}{\rightarrow} \); and \( \overset{\text{open n}}{\rightarrow} \) is \( \overset{(\text{open } n)}{\rightarrow} \).

Some of our results are proved by induction on the sequentiality degree of a process, which is the maximal depth of nesting of capabilities in the process.

**Definition 2.2 (Sequentiality degree, ds)** The sequentiality degree of a term is defined as follows:

- \( ds(0) = 0 \), \( ds(P \mid Q) = \max\{ds(P), ds(Q)\} \);

- \( ds(!P) = ds(P) \);

- \( ds(\text{cap}.P) = 1 + ds(P) \).

Note that this definition relies on the presence of the \(!\) operator (instead of a recursion operator) in the calculus. An important property of \( ds(P) \) is the following:

**Lemma 2.3** If \( P \rightarrow Q \) or \( P \overset{\text{cap}}{\rightarrow} Q \) then \( ds(P) \geq ds(Q) \).

\[
\begin{array}{l}
A ::= \top \mid \neg A \mid A \lor B \mid \forall x.A \quad (\text{classical logic})
\mid \Diamond A \mid 0 \mid \eta[A] \mid A \mid B \quad (\text{temporal and spatial connectives})
\mid A @\eta \mid A > B \quad (\text{logical adjuncts})
\end{array}
\]

Table 3: The syntax of logical formulas

---

**The logic.** To define the set of formulas of the Ambient Logic (AL—Table 3) we introduce an infinite set of variables, ranged over with \( x, y, z \); \( \eta \) ranges over names and variables. The logic has the propositional connectives, \( \top, \neg A, A \lor B \), and universal quantification on names, \( \forall x.A \), with the standard logical interpretation. The temporal connective, \( \Diamond A \) has been briefly discussed in the
Introduction. The spatial connectives, \( \bar{A} \mid B \), and \( \eta[A] \), are the logical counterpart of the corresponding constructions on processes. \( \bar{A} \ni B \) and \( A \oplus \eta \) are the logical adjuncts of \( \bar{A} \mid B \) and \( \eta[A] \), in the sense of being, roughly, their inverse (see below). A formula without free variables is closed.

**Definition 2.4** The satisfaction relation is defined on closed formulas as follows:

\[
\begin{align*}
P & \models \top \quad \text{def} \quad \text{always true} \\
P & \models \forall x . A \quad \text{def} \quad \text{for any } n, P \models A[n/x] \\
P & \models \neg A \quad \text{def} \quad \text{not } P \models A \\
P & \models A_1 \mid A_2 \quad \text{def} \quad \exists P_1, P_2 \text{ s.t. } P \equiv P_1 \mid P_2 \\
& \quad \quad \text{and } P_i \models A_i, \ i = 1, 2 \\
P & \models A \lor B \quad \text{def} \quad P \models A \text{ or } P \models B \\
P & \models n[A] \quad \text{def} \quad \exists P' \text{ s.t. } P \equiv n[P'] \text{ and } P' \models A \\
P & \models 0 \quad \text{def} \quad P \equiv 0 \\
P & \models \diamond A \quad \text{def} \quad \exists P' \text{ s.t. } P \implies P' \text{ and } P' \models A \\
P & \models A \oplus n \quad \text{def} \quad n[P] \models A \\
P & \models A \ni B \quad \text{def} \quad \forall R, A \models P \text{ implies } P \mid R \models B
\end{align*}
\]

The logic in [9] has also a somewhere connective that holds of a process containing, at some arbitrary level of nesting of ambients, an ambient whose content satisfies \( A \). The addition of this connective would not change the results in the paper.

We give \( \lor \) and \( \wedge \) the least syntactic precedence, thus \( A_1 \ni A_2 \wedge A_3 \) reads \((A_1 \ni A_2) \wedge A_3\), and \( A_1 \ni (\diamond A_2 \land \diamond A_3) \) reads \( A_1 \ni ((\diamond A_2) \land (\diamond A_3))\). We shall use the dual of some connectives, namely the duals of linear implication \( \langle A \ni B \rangle \), of the sometime modality \( \Box A \), of the parallel operator \( \parallel \), and the standard duals of universal quantification \( (\exists x . A) \) and disjunction \( (A \wedge B) \). We also define (classical) implication \( (A \rightarrow B) \).

\[
\begin{align*}
A \land B & \quad \text{def} \quad \neg (\neg A \lor \neg B) \\
\Box A & \quad \text{def} \quad \neg \diamond A \\
A \rightarrow B & \quad \text{def} \quad \neg A \lor B \\
A \ni B & \quad \text{def} \quad \neg (\neg A \land \neg B) \\
(\exists x . A) & \quad \text{def} \quad \neg \forall x . \neg A \\
A \langle B \rangle & \quad \text{def} \quad \neg (A \ni \neg B)
\end{align*}
\]

Thus \( P \models A \langle B \rangle \) iff there exists \( Q \) with \( Q \models A \) and \( P \mid Q \models B \), and \( P \models \Box A \) iff \( P' \models A \) for all \( P' \) such that \( P \implies P' \). The formula \( A \langle \top \rangle \) is \( A \parallel \top \), from [9], is satisfied by \( P \) iff for any \( Q, R \) such that \( P \equiv Q \mid R \), it holds that \( Q \models A \).

**Definition 2.5 (Process logical equivalence)** For processes \( P \) and \( Q \), we write \( P \equiv Q \) if for all closed formulas \( A \) it holds that \( P \models A \) iff \( Q \models A \).

## 3 Coinductive and inductive operational relations

The coinductive relation below follows the definition of intensional bisimilarity in finite MA [19].

**Definition 3.1 (Intensional bisimilarity)** Intensional bisimilarity is the largest symmetric relation \( \approx_{\text{bis}} \) on processes such that \( P \approx_{\text{bis}} Q \) implies:

\[
3 \text{ Coinductive and inductive operational relations}
\]

The coinductive relation below follows the definition of intensional bisimilarity in finite MA [19].

**Definition 3.1 (Intensional bisimilarity)** Intensional bisimilarity is the largest symmetric relation \( \approx_{\text{bis}} \) on processes such that \( P \approx_{\text{bis}} Q \) implies:
1. If $P \equiv P_1 \mid P_2$ then there are $Q_1, Q_2$ such that $Q \equiv Q_1 \mid Q_2$ and $P_i \simeq_{\text{bis}} Q_i$, for $i = 1, 2$.

2. If $P \equiv 0$ then $Q \equiv 0$.

3. If $P \rightarrow P'$ then there is $Q'$ such that $Q \rightarrow Q'$ and $P' \simeq_{\text{bis}} Q'$.

4. For any cap, if $P \xrightarrow{\text{cap}} P'$ then there is $Q'$ such that $Q \xrightarrow{\text{cap}} Q'$ and $P' \simeq_{\text{bis}} Q'$.

5. If $P \equiv n[P']$ then there is $Q'$ such that $Q \equiv n[Q']$ and $P' \simeq_{\text{bis}} Q'$.

With respect to standard bisimilarities for process calculi, $\simeq_{\text{bis}}$ has intensional clauses, namely (1), (2) and (5), which allow us to observe parallel compositions, terminated process, and ambients. These clauses correspond to the intensional connectives ‘$\mid$’, ‘0’, and $n[\cdot]$ of the logic. The other main peculiarity of $\simeq_{\text{bis}}$ are the stuttering relations. The need for stuttering on infinite trees (i.e., MA with a recursion operator) has been pointed out in [19]. We show that stuttering is also needed on finite trees with replication.

**Example 1** Consider the processes $P_0 \overset{\text{def}}{=} \open n.\in n.\out n.\n.\n[0] \mid n[0]$, and $P_1 \overset{\text{def}}{=} \open n.\in n.\out n.\n.\n[0] \mid n.\out n.\n[0]$. It holds that $P_0 \not\simeq_{\text{bis}} P_1$; however, since

$$P_0 = [(n.\out n)]^* \leadsto P_1 = [(n.\out n)]^* \leadsto P_0,$$

we have out $n.P_0 \simeq_{\text{bis}}$ out $n.P_1$. Without stuttering this equivalence would not hold.

The proof of congruence of $\simeq_{\text{bis}}$ follows the proof of the analogous result in [19], using a technique similar to Howe’s for proving congruence of bisimilarity in higher-order languages [16].

**Theorem 3.2 (Soundness of $\simeq_{\text{bis}}$)** In MA, $\simeq_{\text{bis}} \subseteq L$.

Completeness – the hard implication – is proved in Section 4. Below we show an inductive characterisation of $\simeq_{\text{bis}}$. The crux of this result is Lemma 3.4, which gives us a decomposition property for bisimilar processes in terms of special forms of contexts.

**Definition 3.3 (Contexts)** A context (ranged over with $\mathcal{C}, \mathcal{D}$) is a process term with some holes $[\cdot]$, in it, each hole occurring once. A context is active if each hole appears underneath exactly one capability. A coloured context $\mathcal{C}(\sigma)$ is given by an active context $\mathcal{C}$ and a colouring function $\sigma$, assigning a colour to each hole (we assume there are infinitely many colours available).

Structural congruence is defined on coloured contexts as on processes, but with the additional rule for holes saying that $[\cdot]_i \equiv [\cdot]_j$ if the two holes have the same colour.

**Lemma 3.4 (Decomposition lemma)** Suppose $P \simeq_{\text{bis}} Q$. Then there are two active contexts $\mathcal{C}$ and $\mathcal{D}$, and two vectors of processes $\overline{P}, \overline{Q}$ such that $P \equiv \mathcal{C}[\overline{P}], Q \equiv \mathcal{D}[\overline{Q}]$ and there is a colouring function $\sigma$ such that
1. $C(\sigma) \equiv D(\sigma)$,

2. for any $i, j$, if $[\!\! \! i \!\!]$ and $[\!\! \! j \!\!]$ are some holes of $C$ or $D$ having the same colour.
then they are underneath the same capability $\text{cap}_i$. Moreover, there are
$P', Q'_j$ such that $P_i \xrightarrow{\text{cap}_i} P' \cong_{\text{bis}} Q_j$, and $Q_j \xrightarrow{\text{cap}_j} Q'_j \cong_{\text{bis}} P_i$.

In the lemma, subcomponents $\tilde{P}$ and $\tilde{Q}$, and their derivatives $P', Q'_j$, have a
sequentiality degree (that is, the depth of nesting of capabilities) strictly smaller
than that of the original processes $P$ and $Q$ (for the derivatives, this is given
by Lemma 2.3). We can therefore exploit this result to obtain an inductive
characterisation of $\cong_{\text{bis}}$. Let $\sim_{\text{ind}}$ be this inductive relation, i.e. $\sim_{\text{ind}}$ is the
least relation such that whenever two active contexts $C, D$ and two vectors of
processes $\tilde{P}$ and $\tilde{Q}$ satisfy the clause of the lemma, where $\cong_{\text{bis}}$ is replaced by
$\sim_{\text{ind}}$, then also $P \sim_{\text{ind}} Q$, for all processes $P, Q$ with $P \equiv C[P], Q \equiv D[Q]$.

**Theorem 3.5** Relations $\cong_{\text{bis}}$ and $\sim_{\text{ind}}$ coincide on $MA$.

Lemma 3.4, and therefore also the definition of $\sim_{\text{ind}}$, contain a heavy hidden
universal quantification, due to the decompositions of $P$ and $Q$ up to $\equiv$, for an
equivalence class of $\equiv$ contains an infinite number of processes. The following
lemma shows however that the active context decomposition of a process is
essentially unique.

**Lemma 3.6 (Active context decomposition)** Suppose there are processes
$P, P_i$, and active contexts $C_i$ ($i = 1, 2$), such that $P \equiv C_i[P_i]$. Then there is a
colouring function $\sigma$ such that

1. $C_i(\sigma) \equiv C_2(\sigma)$;

2. for any $i, j$, if $[\!\! \! i \!\!]$ and $[\!\! \! j \!\!]$ have the same colour, then $P_i \equiv Q_j$, and the
two holes are underneath the same capability.

We define some subclass of processes, used in the statements of some of our
results.

**Definition 3.7 (Image-finite processes, finite processes, $MA_{IF}, MA_{syn}$)**

A process $P$ is image finite if the set $\{P' \mid P \xrightarrow{\text{cap}} P'\}$, quotiented by $\cong_{\text{bis}}$, is
finite for all $\text{cap}$. $P$ is finite if there is $Q$ such that $P \equiv Q$ and $Q$ has no
replication operator. The classes $MA_{IF}$ and $MA_{syn}$ are obtained by adding to the
grammar of Table 1 the following constraints on the production $\text{cap} P$: in
$MA_{IF}$, the continuation $P$ must be an image-finite process of $MA_{IF}$; in $MA_{syn}$,
the continuation $P$ must be finite.

All the above classes of processes are closed under transition. The inclusions
$MA_{syn} \subseteq MA_{IF} \subseteq MA$ are strict. The processes $P_0$ and $P_1$ in Example 1 are in
$MA_{syn}$ and image-finite; however out $n.P_0$ and out $n.P_1$ are in $MA_{IF}$ but not in
$MA_{syn}$. The process $P = \text{open} n.(\text{open} a \mid \text{in} [b[0]])$ is in $MA$, but not in $MA_{IF}$,
because $\text{open} a \mid \text{in} [b[0]]$ is not image finite.

$MA_{syn}$, and hence also $MA_{IF}$, contains processes that are not image-finite:
for instance, the processes used to encode Turing Machines in Section 5.

Another consequence of Theorem 3.5 is:
Theorem 3.8 (Characterisation of $\succeq_{\text{bis}}$ on $\text{MA}^{\text{syn}}_{\text{IF}}$) Let $P \in \text{MA}^{\text{syn}}_{\text{IF}}$. Then for all $Q \in \text{MA}$, $P \succeq_{\text{bis}} Q$ iff $P \equiv Q$.

The equality out n. $P_0 \succeq_{\text{bis}}$ out n. $P_1$ of Example 1 shows that Theorem 3.8 cannot be extended to $\text{MA}_{\text{IF}}$: the $\text{MA}^{\text{syn}}_{\text{IF}}$ requirement of finiteness for the processes underneath capabilities seems essential for the theorem.

4 Characteristic formulas and completeness

A characteristic formula of a process $P$ is a formula that is satisfied by all and only the processes $Q$ in the relation $\succeq_{\text{bis}}$ with $P$. In this section we derive characteristic formulas for the processes in $\text{MA}_{\text{IF}}$.

An $\text{MA}$ process can be viewed as a finite labelled tree in which labels can be ambient names, capabilities, replicated ambients, and replicated capabilities. If we can define formulas that describe all these labels, then we will be able to derive the characteristic formulas using standard techniques for image-finite processes with finite tree representation [14, 21]. AL has formulas $\llbracket A \rrbracket$ that talk about ambient labels. We have to construct the formulas for the other labels. Formulas for capabilities are presented in [19], for finite $\text{MA}$; they are also correct on $\text{MA}$:

Lemma 4.1 (Formulas for capabilities) There is a computable function that associates to each capability $\text{cap}$ and formula $A$ a formula $\langle \text{cap} \rangle . A$ such that $P \models \langle \text{cap} \rangle . A$ iff there are $P'$ and $P''$ such that $P \equiv \text{cap}. P'$ and $P' \models_P \text{cap} P''$ with $P'' \models_A$.

A formula $\langle \text{cap} \rangle . A$ expresses possibility (in Lemma 4.1, at least one derivative of $P'$ satisfies $A$). We also need formulas $\llbracket \text{cap} \rrbracket . A$ for necessity (all derivatives of $P'$ satisfy $A$). Such formulas are not the dual of the possibility formulas, as in standard modal logics, because of the spatial aspects of AL. For instance, $\llbracket \langle n \rangle . \top \rrbracket$ is different from $\langle \langle n \rangle . \top \rangle$: the latter is actually equivalent to $\top$. We set:

$$\llbracket \text{cap} \rrbracket . A \overset{\text{def}}{=} \langle \text{cap} \rangle . A \land \lnot \langle \text{cap} \rangle . \lnot A.$$  

The challenging part, however, is the definition of replicated formulas $\llbracket 4 \rrbracket$ with the property

$$P \models \llbracket 4 \rrbracket \iff \text{ there are } r > 1, s \geq r, P_i (1 \leq i \leq s)$$

such that $P \equiv \Pi_{1 \leq i \leq r} P_i \mid \Pi_{r+1 \leq i \leq s} P_i$,

and $P_i \models \llbracket A \rrbracket$ for all $1 \leq i \leq s$,

where $\Pi_{1 \leq i \leq s} Q_i$ abbreviates $Q_1 \mid \ldots \mid Q_s$.

We say that a component of a process is at top level if the component is not underneath a capability or inside an ambient. A process is single if it is structurally congruent to a process of the form $\llbracket n[P] \rrbracket$ or $\llbracket \text{cap}. P \rrbracket$. The formula $1\text{Comp} \overset{\text{def}}{=} \llbracket 0 \rrbracket \land \lnot \llbracket 0 \rrbracket$ (from [19]) characterises the single processes.

The definition of $\llbracket 4 \rrbracket$ has two parts. The first part says that if $P \models \llbracket 4 \rrbracket$ then all parallel components in $P$ that are single and at top level satisfy $\llbracket A \rrbracket$. This is expressed by the formula

$$\llbracket A \rrbracket^r \overset{\text{def}}{=} (1\text{Comp} \rightarrow \llbracket A \rrbracket)^r.$$
The second part of the definition of $!A$ addresses persistence, by saying that there are infinitely many processes at top level that satisfy $A$. We have to say that these infinite copies are at top level: for instance, $!\langle \text{cap} \rangle.0$ (or, in fact, any other replicated formula) should not be satisfied by $\text{cap}.!\text{cap}.0$. We can talk about the top level because we can express in the logic the maximal depth of nesting of capabilities (the sequentiality depth, Section 2) and the maximal depth of nesting of ambient processes. Indeed, a component of $P$ is at top level if it has the same depths of nesting as $P$. As a consequence, however, we have to impose a constraint on the definition of $!A$: all processes that satisfy $A$ should have the same depths of nesting. We say that these formulas have fixed model depth.

The other constraint we need on $A$ roughly requires that all the processes that satisfy $A$ should be single and have the same outermost operator. Precisely, either $P \models A$ should imply $P \equiv \text{cap}.P'$, for some $\text{cap}, P'$ (in this case, $A$ is single for $\text{cap}$); or $P \models A$ should imply $P \equiv \mathsf{n}[P']$, for some $\mathsf{n}, P'$ (then $A$ is single for $\mathsf{n}$). Moreover, the construction of $!A$ depends on such outermost operator.

The definition of $!A$ is given in Table 6, at the end of the paper (the formulas for the Rep construction). Here we only show an example:

$$
!\langle \text{open } n \rangle.A \overset{\text{def}}{=} ([\text{open } n].A)^\omega \land (n[0])^\omega \vdash \square ([\text{open } n].A \mid \top).
$$

**Lemma 4.2** For each capability cap there is a computable function that associates to each formula $A$ that is single for cap and has fixed model depth, a formula $!A$ with the property (1).

The assertion for the formulas single for names is similar.

We show some concrete examples of characteristic formulas. The general definitions are given in Table 4 at the end of the paper. A characteristic formula for $\text{open } n.n[0]$ is $!\langle \text{open } n \rangle.n[0]$. A characteristic formula for $\text{open } n.(\text{open } n \mid n[0])$ is

$$
\mathcal{F}_1^\omega \land (n[0])^\omega \vdash \square (\mathcal{F}_1 \mid \top) \quad \text{where}
$$

$$
\begin{cases}
\mathcal{F}_1 \overset{\text{def}}{=} \langle \text{open } n \rangle.\mathcal{F}_2 \land [\text{open } n].(\mathcal{F}_2 \lor 0) \\
\mathcal{F}_2 \overset{\text{def}}{=} [\text{open } n].0 \mid n[0]
\end{cases}
$$

and $\mathcal{F}_2$ is a characteristic formula for $\text{open } n \mid n[0]$.

**Theorem 4.3 (Characteristic formulas for MAIF)** There is a computable function that associates to each $P \in \text{MAIF}$ a formula $\mathcal{F}_P$ such that for any $Q \in \text{MA}$,

$$
Q \models \mathcal{F}_P \quad \text{iff} \quad P \simeq_{\text{bis}} Q.
$$

We shall see that $\simeq_{\text{bis}}$ coincides with $=_{L}$, thus the result can also be formulated in terms of characteristic formulas for $=_{L}$.

For some of the constructions above we use some special formulas that are of independent interest. One such formula is satisfied by precisely the finite processes. It is derived by exploiting the lemma below, which gives us an operational characterisation of 'finiteness'.

**Lemma 4.4** $P \in \text{MA}$ is finite iff there are $Q,R,n$ such that $n[P \mid Q] \mid R \Rightarrow 0$. 

10
**Proposition 4.5** Let $\phi_{\text{fin}} \overset{\text{def}}{=} \exists x. \left( \top \vdash (\top \vdash \diamond 0)@x \right)$. For any $P \in MA$, $P \models \phi_{\text{fin}}$ iff $P$ is finite.

We can also define, for any finite set $S$ of names, a formula satisfied by those processes whose set of free names is precisely $S$. For this construction we exploit the ability, using the modal formulas for capabilities, to detect unguarded occurrences of names, together with Lemma 4.6. A process $P$ is flat if the only process underneath all capabilities and inside all ambients of $P$ is 0.

**Lemma 4.6** For all $P, n, n \in \operatorname{fn}(P)$ iff for any name $m$, there are some flat processes $Q, R$ such that $n \notin \operatorname{fn}(Q, R)$, and a process $S$ with an occurrence of $n$ at top level such that $m[P \mid Q] \mid R \rightarrow m[S]$.

**Proposition 4.7** There is a computable function that associates to each finite set $S$ of names a formula refers $S$ such that for any $P \in MA$

$$P \models \text{refers } S \iff S = \operatorname{fn}(P).$$

The definition of refers $S$ is given in Table 4.

We derive completeness of $\simeq_{\text{bis}}$ by exploiting the formulas introduced above. However, since we work on the whole calculus MA, we cannot assume any image finiteness hypothesis. Instead, we rely on another form of finiteness of the restriction-free MA.

Define $\text{cont}(P)$ as the set of all subterms of $P$ appearing under at least one capability, quotiented by $\equiv$. We have the following properties:

**Lemma 4.8**

- For any process $P$, $\text{cont}(P)$ is finite.

- Let $P, Q$ be two terms such that $P \rightarrow Q$ or $P \overset{\text{cap}}{\rightarrow} P$; then $\text{cont}(Q) \subseteq \text{cont}(P)$.

Along the lines of the definitions above, it is not difficult to define a formula to characterise the active context of a term. The only missing information to get a characteristic formula has then to do with the terms that should be placed after the capabilities. We did not find a general way to express this. However, to obtain completeness, it is enough to work with a restricted notion of characteristic formula. Lemma 4.8 allows us indeed to establish the following result:

**Lemma 4.9 (Restricted characteristic formula)** For any two terms $P, Q$ of MA, there exists a formula $F_{P, Q}$ such that for any $Q'$ and cap satisfying $Q \overset{\text{cap}}{\rightarrow} Q'$,

$$Q' \models F_{P, Q} \iff Q' \simeq_{\text{bis}} P.$$

As a direct important consequence, we have:

**Theorem 4.10 (Completeness of $\simeq_{\text{bis}}$)** In MA, it holds that $=_{L} \subseteq \simeq_{\text{bis}}$.

**Corollary 4.11** In MA, relations $=_{L}$, $\simeq_{\text{bis}}$ and $\simeq_{\text{ind}}$ coincide. Further, on $MA_{\text{syn}}^{\text{IF}}$, they also coincide with $\equiv$. 

11
**Model-checking and tautologies.** In AL, the construction of characteristic formulas has connections with the decidability of other problems related to the logic, namely model-checking (whether $P \models A$ holds, for any given process $P$ and formula $A$) and validity (whether a given formula $A$ is satisfied by all processes). These problems have been addressed in [11, 4]. In particular, for AL, in [11] the undecidability of tautologies is established on a small fragment of the logic, a result that entails the undecidability of model-checking.

Using characteristic formulas, we can derive results similar, albeit weaker, to those in [11] proceeding the other way around (they are weaker because undecidability is established on a larger language). Indeed, we have, for all $P, Q, R \in \text{MA}^{\text{syn}}$: 

$$P \models \mathcal{F}_Q \land \diamond \mathcal{F}_R \iff P \equiv Q \implies R.$$ 

Now, since $\implies$ is undecidable on $\text{MA}^{\text{syn}}$ (as will be shown in Section 5), so is the model checking problem.

More generally, the existence of characteristic formulas allows us to consider validity and model-checking to be equivalent decision problems. To see why, first remark that validity can be encoded inside model-checking [9], thanks to the $\triangleright$ connective. Conversely, we can encode the model-checking problem inside validity using characteristic formulas as follows (recall that $\mathcal{F}_P$ is the characteristic formula of process $P$):

$$\text{for all } P \in \text{MA}_{\text{IF}}, \text{ for all } A, \ P \models A \iff \mathcal{F}_P \rightarrow A.$$ 

In [11] and [4], model-checking and validity turn out to be either both decidable or both undecidable, the key issue being the presence of name quantification in the logic. We do not know at present whether characteristic formulas could be derived in the setting of [4].

## 5 (Un)decidability of the logical equivalence

The undecidability of $=_L$ on MA is obtained via an encoding of Turing Machines (TM’s) in the subcalculus $\text{MA}^{\text{syn}}$.

The encoding and its correctness proof are conceptually simple. The proof, however, is long and tedious, due to the complexity of the TM encoding. Our encoding follows the ideas of Cardelli and Gordon’s [7]. We had however to add or expand some components, because: (1) we do not have the restriction operator, used in [7]; (2) we cannot use coarse behavioural equivalences such as testing or barbed equivalence to reason on processes, as customary in process calculus encodings; we are only allowed to use $\equiv$, which is a very strong equivalence (on $\text{MA}^{\text{syn}}$, $\equiv$ and $=_L$ coincide, Theorem 3.8); therefore, for instance, we cannot algebraically garbage collect deadlocked processes: we have to add into the encoding special processes that explicitly perform garbage collection; (3) we need the simulation of a TM to be (almost) deterministic; to obtain this, we have to add some components that force sequentialisations. We are not aware of correctness results concerning the encoding of [7].

A TM is defined by a *ribbon*, a *transition relation* on some set of *states*, initial and accepting states. A ribbon is a finite sequence of cells, each containing a binary information. In the encoding, a ribbon of length $k$ is represented by a nesting of $k$ ambients named *cell* Each such ambient has a subambient $d[0]$, where $d \in \{tt, ff\}$ represents the content of the cell. The Turing machine moves
left and right by exercising in cell and out cell capabilities. After each movement, an ambient representing the head of the machine reads the value of the current cell, rewrites it, and triggers the next movement.

For the correctness, the central result roughly says that if a given Turing machine $\mathcal{M}$ in state $S_0$ recognises a word $w$ of input and terminates in a state $S_t$ with a word $w'$ on the ribbon, then

$$\text{TM}(w, S_0) \rightarrow^* \text{TM}(w', S_t),$$

where $\text{TM}(v, S)$ represents the encoding of the TM in state $S$ and with $v$ as content of the ribbon, and the relation $\rightarrow^*$ is defined as follows: write $P \rightarrow Q$ if $P \rightarrow Q$ and for any $Q'$ such that $P \rightarrow Q'$, either $Q' \not\rightarrow$ or $Q \equiv Q'$; then $\rightarrow^*$ is the reflexive and transitive closure of $\rightarrow$. Thus $P \rightarrow^* Q$ says that $P$ can reduce to $Q$ and, moreover, the reduction is almost deterministic. (What prevents pure determinism are blocking states that arise in the encoding of if-then-else statements in the TM.)

Moreover, we relate the halting problem of TM's to the existence of certain loops: given a Turing machine $\mathcal{M}$ and an input word $w$, there are appropriate processes $P_0$ and $P_1$ obtained from the encoding of the TM such that

$$\mathcal{M} \text{ halts on input } w \iff P_0 \Rightarrow P_1 \Rightarrow P_0. \quad (2)$$

**Theorem 5.1** $=_L$ is an undecidable relation on $\mathcal{M}A$.

**Proof:** Consider processes $P_0$ and $P_1$ from (2). These processes are in $\mathcal{M}A_{\text{IF}}^{\text{syn}}$. Using Corollary 4.11, the definition of $\simeq_{\text{bin}}$, and Theorem 3.8, we have:

- $\text{open } n.P_0 =_L \text{ open } n.P_1$
- $\text{iff } \text{open } n.P_0 \simeq_{\text{bin}} \text{ open } n.P_1$
- $\text{iff } P_0 \Rightarrow \simeq_{\text{bin}} P_1 \Rightarrow \simeq_{\text{bin}} P_0$

(from Theorem 3.8, $\Rightarrow \simeq_{\text{bin}}$ is $\Rightarrow$ on $\mathcal{M}A_{\text{IF}}^{\text{syn}}$). Then undecidability follows from (2).

**Proposition 5.2** (Decidability of $=_L$ on $\mathcal{M}A_{\text{IF}}$ and $\mathcal{M}A_{\text{IF}}^{\text{syn}}$) $=_L$ is a decidable relation on $\mathcal{M}A_{\text{IF}}$ and $\mathcal{M}A_{\text{IF}}^{\text{syn}}$.

**Proof:** These results are proved using the inductive characterisation of $=_L$ (Corollary 4.11) and the image-finiteness conditions in the definitions of the calculi. For $\mathcal{M}A_{\text{IF}}^{\text{syn}}$, the result also follows directly from Theorem 3.8.

The encoding of TM's only uses processes in $\mathcal{M}A_{\text{IF}}^{\text{syn}}$. The language $\mathcal{M}A_{\text{IF}}^{\text{syn}}$ is therefore proved to be Turing complete. This might seem in contradiction with the decidability of $=_{L}$ in $\mathcal{M}A_{\text{IF}}^{\text{syn}}$. The proof of Theorem 5.1 does not work for $\mathcal{M}A_{\text{IF}}^{\text{syn}}$ because open $n.P_0$ and open $n.P_1$ do not belong to this language. Indeed, concerning $\mathcal{M}A_{\text{IF}}^{\text{syn}}$ we can only derive, from (2), that reachability (whether $P \Rightarrow P'$ holds, for any $P, P'$) is undecidable.

Busi and Zavattaro [1] have independently obtained an encoding of Random Access Machines in $\mathcal{M}A_{\text{IF}}^{\text{syn}}$ (although this sublanguage is not explicitly mentioned in the paper).

### 6 Extensions

The syntax of MA in [9] also includes communication, i.e., operators $\langle V \rangle$ for the emission of a value, and $(x)P$ for reception. The value $V$ can be a name, a capability, or a path of capabilities (a string of capabilities).
The results we have presented can be extended to MA with communication of names. In the statement of the results, the main difference is that on $\text{MA}_\text{ip}^\text{sym}$, $=_L$ coincides with $\equiv_E$, the (decidable) relation obtained by adding the eta-equality

$$(x)(\langle x \rangle | \langle y \rangle P) = (y)P$$

to the axioms of $\equiv$ (a similar result was known for finite MA [19]). We believe that also the addition of communication of capabilities is easy to handle.

Recent work on spatial logics [3] considers a one-step semantics for the $\Diamond$ construct, recovering the many-steps semantics by means of a recursion operator in the logic. We believe that in such a framework $=_L$ coincides with $\equiv$ on the whole MA.

Usually [7, 8], the syntax of MA also has the restriction operator. In [10], Cardelli and Gordon propose an extension of AL with logical connectives to describe restriction. We do not know at present whether our results continue to hold with such an extension. In particular, the proof technique involved for the completeness result without image-finiteness does not seem to be extensible to a calculus with name restriction, since it would allow infinite name generation and would break the finiteness property of the set of continuation terms. Also, we do not know whether the results hold for an MA calculus with a recursion operator instead of replication, since recursion gives us trees with infinite depth.

Acknowledgments. This work has been supported by european project FET-Global computing PROFUNDIS.

References


\[ A^n \overset{\text{def}}{=} (1\text{Comp} \to A)^n \]
\[ m = n \overset{\text{def}}{=} (n[\top])\oplus m \] (this formula is from [9])
\[ \text{flat } m \overset{\text{def}}{=} \left[ \text{in } m \right] . 0 \lor \left[ \text{out } m \right] . 0 \lor \left[ \text{open } m \right] . 0 \lor m[0] \]
\[ \text{flatcond } n \overset{\text{def}}{=} \left( \exists m. \neg(m = n) \land \text{flat } m \right)^n \]
\[ \text{toplevelcond } n \overset{\text{def}}{=} \left( \langle \text{in } n \rangle . \top \lor \langle \text{out } n \rangle . \top \lor \langle \text{open } n \rangle . \top \lor n[\top] \right) \mid \top \]
\[ \text{refers1 } n \overset{\text{def}}{=} \forall m. \text{flatcond } n \triangleright \left( \text{flatcond } n \triangleright \diamond m[\text{toplevelcond } n] \right) \oplus m \]
\[ \text{refers } \{n_1, \ldots, n_k\} \overset{\text{def}}{=} \bigwedge_{i=0}^{k-1} \text{refers1 } n_i \land \forall x. \text{refers1 } x \to \bigvee_{i=0}^{k-1} x = n_i \]

Table 4: Formulas for free names

\[
\begin{align*}
1\text{Comp} & \overset{\text{def}}{=} \neg 0 \land 0[0] \\
1\text{Cap} & \overset{\text{def}}{=} 1\text{Comp} \land \neg \exists x. x[\top] \\
\langle \text{in } n \rangle . A & \overset{\text{def}}{=} 1\text{Cap} \land \forall x. (n[0] \triangleright \diamond n[x[A]]) \oplus x \\
\langle \text{out } n \rangle . A & \overset{\text{def}}{=} 1\text{Cap} \land \forall m. ((\diamond m[A] \mid n[0]) \oplus n) \oplus m \\
\langle \text{open } n \rangle . A & \overset{\text{def}}{=} 1\text{Cap} \land \forall m. (n[m[0]] \triangleright \diamond m[0] \mid A) \\
\text{[cap]} . A & \overset{\text{def}}{=} \langle \text{cap} \rangle . \top \land \neg \langle \text{cap} \rangle . \neg A \quad \text{for any capability cap}
\end{align*}
\]

Table 5: Formulas for (ephemeral) capabilities
\[
\begin{align*}
\text{Rep}_{\text{in}} (A) & \overset{\text{def}}= A^\omega \land \forall m. \neg \text{refers1 } m \rightarrow\left(\llbracket \text{out } n, 0 \rrbracket^\omega \triangleright (n[0] \triangleright \Box \Diamond (n[m[A | \top]]) )\right) @ m \\
\text{Rep}_{\text{out}} (A) & \overset{\text{def}}= A^\omega \land \forall m. \neg \text{refers1 } m \rightarrow\left(\llbracket \text{in } n, 0 \rrbracket^\omega \triangleright (n[0] \triangleright \Box \Diamond (m[\mathcal{A} | \top] | n[0]) )\right) @ m \\
\text{Rep}_{\text{open}} (A) & \overset{\text{def}}= A^\omega \land \left(\llbracket n[0] \rrbracket^\omega \triangleright \Box (\mathcal{A} | \top) \right)
\end{align*}
\]

Table 6: Formulas for persistent single terms

\[
\begin{align*}
\mathcal{F}_0 & \overset{\text{def}}= 0 \\
\mathcal{F}_{n[P]} & \overset{\text{def}}= n[\mathcal{F}_P] \\
\mathcal{F}_{\text{in}[P]} & \overset{\text{def}}= \text{Rep}_{\text{in}}(\mathcal{F}_P) \\
\mathcal{F}_{\text{cap}.p} & \overset{\text{def}}= \langle \text{cap}. \rangle \mathcal{F}_P \land \llbracket \text{cap} \rrbracket \lor_{\mathcal{F}_P{\rightarrow\rightarrow} \mathcal{F}_P} \mathcal{F}_P \\
\mathcal{F}_{\text{cap}.p} & \overset{\text{def}}= \text{Rep}_{\text{cap}}(\mathcal{F}_{\text{cap}.p})
\end{align*}
\]

Table 7: Characteristic formulas