Fixed Points in the Ambient Logic

Silvano Dal Zilio

Microsoft Research

Abstract. We present an extension of the ambient logic with fixed points operators in the style of the μ-calculus. We give a simple syntactic condition for the equivalence between minimal and maximal fixpoint formulas and show how to subsume spatial analogues of the usual box and diamond operators.

1 Introduction

The *ambient calculus* of Cardelli and Gordon [4] is a process algebra for describing mobile computation where processes may reside and move within a hierarchy of locations, called ambients. In this framework, each location is a cluster of processes and sub-ambients that can move as a group.

The ambient calculus serves as model for the *ambient logic* [3], a new modal logic introduced to express properties of mobile processes. A key feature of this logic is its ability to describe organizational as well as behavioral properties of processes. In particular, whereas usual logics for concurrent systems, such as the Hennessy-Milner logic, usually focus on the computational behavior of systems, the ambient logic also provides the ability to reason about spatial structures (and is therefore more intentional.) Another interesting feature of this logic is its lack of sensitivity to the details of the process calculus being studied, which make it easily transposable to other settings, like the π-calculus for example [1].

In this paper, we will only consider the calculus restricted to spatial (and static) operators, and the subset of the logic associated to this fragment. This corresponds essentially to a logic over finite, unordered, edge-labelled trees. A contribution of this paper is the extension of the ambient logic with fixed points, in the style of the μ-calculus [6]. The subset considered here is not simplistic; in particular, it serves as the basis for the definition of a query language for semi-structured databases [2].

The first result presented in this paper is a simple syntactical criterion for the equivalence between minimal and maximal fixpoint formulas. While this result is not completely surprising, it provides a valuable decidable class of formulas, ϕ, such that $\nu\mathrm{X}.\phi$ and $\mu\mathrm{X}.\phi$ have the same semantics. Informally, minimal and maximal fixpoints are separated only by infinite (or divergent) behaviors, and the ambient processes considered in this paper are finite. As often, the formal proof of apparently simple results can be quite difficult, and we formalize our intuition in Section 3 using an elegant proof technique based on set-theoretic methods.

The present result answers an open problem stated in [2] and is interesting in the context of a query language implementation. Indeed, whereas least fixpoint operators can be implemented using classical iterative techniques, it is not clear how to handle greatest fixpoints. Moreover, this result allows to simplify negative requests (the query language of [2] has a negation operator built-in), by replacing occurrences of $\neg\mu\mathrm{X}.\phi$ with $\mu\mathrm{Y}.\neg\phi\{\mathrm{X}\leftarrow\neg\mathrm{Y}\}$.

A second result of this paper is a characterization of the somewhere and everywhere operators introduced in [3], which are the spatial analogues of the usual box and diamond modal operators, using recursive formulas.

2 The Static Ambient Calculus and a Modal Logic with Fixed Points

In our simplified setting, a process is a parallel composition of ambients, $n[Q]$, where each ambient has a name, n, taken from a denumerable set Λ, and encapsulates a sub-process, Q. A process may also be empty, denoted $\mathbf{0}$.

Processes:

$$P, Q, R, \ldots \;::=\; \mathbf{0} \;\;\big|\;\; n[P] \;\;\big|\;\; P \mid Q$$

As usual, we consider processes up-to a structural equivalence relation, $\equiv$, which is the smallest congruence realtion such that $P \mid Q \equiv Q \mid P$, and $(P \mid Q) \mid R \equiv P \mid (Q \mid R)$ and $P \mid \mathbf{0} \equiv P$. We use Π to denote the set of processes modulo $\equiv$, and 2^{Π} for the associated powerset.

There is a direct analogy between processes and (rooted) edge-labeled unordered trees with finite degree, which is at the heart of Cardelli and Ghelli's query language for semi-structured data [2].

Logical formulas, $\phi, \psi, \ldots$, are defined by the following grammar, where η stands for a name, $n \in \Lambda$, or a "name variable", $x, y, \ldots$. We say that a formula is closed whenever it has no free (name) variables and, for simplicity reason, we only consider closed formulas in this restricted abstract. We also consider a set of propositional variables, $\mathrm{X}, \mathrm{Y}, \ldots$

Logical Formulas:

η	a name n or a variable x		
$\phi, \psi ::=$	formula		
ff	false	$\neg\phi$	negation
$\phi \wedge \psi$	conjunction	$\exists x.\phi$	existential quantification
$\mathbf{0}$	void	$\phi \mid \psi$	composition match
$\eta[\phi]$	ambient match		
X	propositional variable	$\mu\mathrm{X}.\phi$	minimal fixpoint

The core of the logic is a (first-order) classical propositional logic augmented with spatial connectives and an existential quantification over names. We use ff to denote the false formula, and tt as a shorthand for $\neg\mathit{ff}$. We introduce a minimal fixpoint operator, $\mu\mathrm{X}.\phi$, where ϕ is *monotonic* in the variable X, that is, X occurs under an even number of negation. A maximal fixpoint, $\nu\mathrm{X}.\phi$, is also definable. The definition of monotonic formulas can be adapted to the full logic [1].

The meaning of a closed formula, ϕ, is given by a set of processes, $[\![\phi]\!]_v$, namely the set of all processes that satisfy the property denoted by ϕ. The meaning of ϕ is determined by a valuation function, v, that maps subsets of Π to free propositional variables of ϕ.

In the definition of $[\![\phi]\!]_v$, we use the symbols $\mathcal{S}, \mathcal{T}$ to range over sets of processes (closed by $\equiv$) and $\mathcal{S} - \mathcal{T}$ to denote set subtraction, that is, the set of processes in $\mathcal{S}$ and not in $\mathcal{T}$. Following a set-theoretic approach, we also naturally extend the operators of the calculus to set of processes as follows: $n[\mathcal{S}] \triangleq \{P \mid P \equiv n[Q] \text{ and } Q \in \mathcal{S}\}$ and $\mathcal{S} \mid \mathcal{T} \triangleq \{P \mid P \equiv Q \mid R \text{ and } Q \in \mathcal{S} \text{ and } R \in \mathcal{T}\}$.

Semantics of a Formula ϕ:

$[\![\mathit{ff}]\!]_v \triangleq \emptyset$	$[\![\phi \wedge \psi]\!]_v \triangleq [\![\phi]\!]_v \cap [\![\psi]\!]_v$	$[\![\neg\phi]\!]_v \triangleq \Pi - [\![\phi]\!]_v$
$[\![\exists x.\phi]\!]_v \triangleq \bigcup_{n\in\Lambda} [\![\phi\{x\leftarrow n\}]\!]_v$	$[\![\mathbf{0}]\!]_v \triangleq \{P \mid P \equiv \mathbf{0}\}$	$[\![X]\!]_v \triangleq v(X)$

$$[\![n[\phi]]\!]_v \triangleq \{P \mid P \equiv n[Q] \text{ and } Q \in [\![\phi]\!]_v\}$$

$$[\![\phi \mid \psi]\!]_v \triangleq \{P \mid P \equiv Q \mid R \text{ and } Q \in [\![\phi]\!]_v \text{ and } R \in [\![\psi]\!]_v\}$$

$$[\![\mu\mathrm{X}.\phi]\!]_v \triangleq \bigcap \{\mathcal{S} \subseteq \Pi \mid [\![\phi]\!]_{v\{\mathrm{X}\leftarrow\mathcal{S}\}} \subseteq \mathcal{S}\}$$

We use $\phi(\mathrm{X})$ for a formula ϕ with a free propositional variable X and $\phi(\psi)$ for the formula $\phi\{\mathrm{X}\leftarrow\psi\}$. A simple induction on the definition of ϕ is enough to prove that if ϕ is monotonic in X, then the function $\lambda\mathcal{S}.([\![\phi]\!]_{v\{X\leftarrow\mathcal{S}\}})$ is monotonic (and continuous) on the complete lattice $(2^{\Pi}, \cap, \cup)$. Therefore, by the well-known Knaster-Tarski theorem, whenever ϕ is monotonic in X, we have that $\mu\mathrm{X}.\phi$ and $\nu\mathrm{X}.\phi$ are well-defined and:

$$[\![\mu\mathrm{X}.\phi]\!]_v = \bigcup_{k\in\mathbb{N}} [\![\phi^k(\mathit{ff})]\!]_v \tag{2.1}$$

$$[\![\nu\mathrm{X}.\phi]\!]_v = \bigcap_{k\in\mathbb{N}} [\![\phi^k(tt)]\!]_v \tag{2.2}$$

Where $\phi^k(X)$ stands for the k^{th} iteration of ϕ. Note that, since parallel composition only introduces finite branching degrees, we can avoid transfinite iterations.

Definition 2.1. *Based on the semantics of formulas, we say that P* satisfies *ϕ, written $P \models \phi$, if $P \in [\![\phi]\!]_v$ for all possible valuation v. We say that ϕ* entails *ψ, written $\phi \vdash \psi$, if and only if $[\![\phi]\!]_v \subseteq [\![\psi]\!]_v$ for all v or, equivalently, $[\![\phi \Rightarrow \psi]\!]_v = [\![\mathrm{tt}]\!]_v$.*

The structure defined by the spatial operators is not without interest, in particular, $(\Pi, \subseteq, \vee, \mid, \mathbf{0})$ is a quantale [5].

3 Equivalence Between Minimal and Maximal Fixpoint

We define the *depth* of a process, $\mathrm{d}(P)$, as the depth of its underlying (spatial) tree, that is, the function inductively defined by: $\mathrm{d}(\mathbf{0}) = 0$, $\mathrm{d}(n[P]) = 1 + \mathrm{d}(P)$ and $\mathrm{d}(P \mid Q) = \max\{\mathrm{d}(P), \mathrm{d}(Q)\}$. We extend the notion of depth to formulas, with $\mathrm{d}(\phi)$ defining the minimal depth of the processes satisfying ϕ. In particular, ff is of infinite depth and $n[tt]$ has depth 1.

$$\mathrm{d}(\phi) \triangleq \min\{\mathrm{d}(P) \mid P \models \phi\}$$

We say that the formula ϕ is *guarded* in X, if X always occurs under a location operator, $\eta[\ ]$.

Let $\phi - \psi$ denotes the formula $\phi \wedge \neg\psi$.

Lemma 3.1. *If ϕ is guarded and monotonic in X and if $P \models \phi(\psi_1) - \phi(\psi_2)$, then $\mathrm{d}(P) \geq 1 + \mathrm{d}(\psi_1 - \psi_2)$. Conversely, if ϕ is anti-monotonic and $P \models \phi(\psi_1) - \phi(\psi_2)$, then $\mathrm{d}(P) \geq 1 + \mathrm{d}(\psi_2 - \psi_1)$.*

Lemma 3.1 allows us to prove that the minimal and maximal fixpoint of guarded formulas are equal.

Theorem 3.1. *If ϕ is monotonic and guarded in X then $\nu X.\phi = \mu X.\phi$.*

Proof. It is enough to prove that $\nu\mathrm{X}.\phi \vdash \mu\mathrm{X}.\phi$, that is, $[\![\nu\mathrm{X}.\phi - \mu\mathrm{X}.\phi]\!]_v = \emptyset$. Let $\psi_k \triangleq (\phi^k(tt) - \phi^k(\mathit{ff}))$. Since ϕ is monotonic, we have $[\![\phi^k(\mathit{ff})]\!]_v \subseteq [\![\phi^{k+1}(\mathit{ff})]\!]_v \subseteq$

$[\![\phi^{k+1}(tt)]\!]_v \subseteq [\![\phi^k(tt)]\!]_v$, and therefore $\psi_{k+1} \vdash \psi_k$ for all k. Moreover, by a direct corollary of Knaster-Tarski theorem, see (2.1), we have: $[\![\nu X.\phi - \mu X.\phi]\!]_v = \bigcap_{k\in\mathbb{N}} [\![\psi_k]\!]_v \quad (3.1)$.

Next, we prove that if $P \models \psi_k$ then $\mathrm{d}(P) \geq k$. The proof is by induction on k. If $k = 0$ then $\psi_0 \triangleq tt$ and therefore $\mathrm{d}(\psi_0) = 0$. Assume $k \geq 1$ and $P \models \psi_k$. Then $P \models (\phi(\phi^{k-1}(tt)) - \phi(\phi^{k-1}(\mathit{ff})))$ and, by Lemma 3.1, $\mathrm{d}(P) \geq 1 + \mathrm{d}(\psi_{k-1})$, as required. Since every process has a bounded depth, it must be the case that, for all process $P \in \Pi$, there exists an integer k_0 such that $P \not\models \psi_{k_0}$, and therefore, by (3.1) and antimonotonicity of $([\![\psi_k]\!]_v)_{k\in\mathbb{N}}$, we have that for all process $P \in \Pi$, $P \notin [\![\nu X.\phi - \mu X.\phi]\!]_v$, which implies $[\![\nu X.\phi - \mu X.\phi]\!]_v = \emptyset$, as required.

4 Somewhere and Everywhere

We define a new operator, $\diamond\phi$, or somewhere ϕ, along the lines of [3]:

$$\diamond\phi \triangleq \mu X.(\phi \vee \exists y.(y[X] \mid tt)) \qquad \text{(where X does not occurs free in } \phi.)$$

We also consider its DeMorgan's dual, the everywhere modality: $\boxtimes\phi \triangleq \neg\diamond\neg\phi$. Note that, since $\exists y.(y[X] \mid tt)$ is monotonic and guarded in X, Theorem 3.1 allows us to deduce that:

Theorem 4.1. *We have:* $\boxtimes\phi = \mu X.(\phi \wedge \forall y.\neg(y[\neg X] \mid \mathrm{tt}))$*, where* X *does not occurs free in* ϕ*.*

We define the spatial reduction relation, $P \downarrow Q$, to mean that Q resides inside an ambient of P. More formally, $P \downarrow Q$ if there exists n, R such that $P \equiv n[Q] \mid R$. The relation $\Downarrow$ is the reflexive and transitive closure of $\downarrow$. Just like the spatial operator, $n[\phi]$, and the spatial reduction relation, $\downarrow$, can be interpreted as analogues of the operator $\langle n\rangle\phi$ and relation, $\rightarrow^*$, often found in semantics of the μ-calculus. It is possible to draw a parallel between the (temporal logic) sometimes modality, $\Diamond\phi$, and its spatial counterpart, $\diamond\phi$. Some differences exist, though, like the use of the logical operator, $\mathbf{0}$, which can be interpreted as the equivalent of a "time-stop" modality, and the presence of quantification over names, $\exists n.\phi$.

We prove that the set of processes satisfying $\diamond\phi$ correspond to the definition given in [3].

Theorem 4.2. *We have* $[\![\diamond\phi]\!]_v = \{P \in \Pi \mid \exists P' \in [\![\phi]\!]_v . P \Downarrow P'\}$.

Proof. Let $\mathcal{S}_{\diamond}$ be the set $\{P \in \Pi \mid \exists P' \in [\![\phi]\!]_v . P \Downarrow P'\}$ and F denotes the function $\lambda\mathcal{S}.([\![\phi]\!]_v \cup \bigcup_{n\in\Lambda} (n[\mathcal{S}] \mid \Pi))$. It is enough to prove that $\mathcal{S}_{\diamond}$ is a fixpoint of F (for all v.) Then, since the minimal and maximal fixpoint of F are equal, it must be the case that $\mu\mathcal{S}.F(\mathcal{S}) = \mathcal{S}_{\diamond}$, and therefore: $[\![\diamond\phi]\!]_v = \mathcal{S}_{\diamond}$.

An interesting property of this new characterization of the modalities used in [3], is that it becomes possible to prove some theorems (of the ambient logic), which where proved directly previously, using traditional induction and co-induction principles. For example, we can prove that $\diamond$ obeys the rule of S4 modalities, like: $\boxtimes(\phi \Rightarrow \psi) \vdash (\boxtimes\phi) \Rightarrow (\boxtimes\psi)$; $\boxtimes\phi \vdash \phi$; $\boxtimes\phi \vdash \boxtimes\boxtimes\phi$; or $\phi \vdash \psi \Rightarrow \boxtimes\phi \vdash \boxtimes\psi$.

Another interesting proof method is based on our result on the equivalence of fixpoints (Theorem 3.1). Indeed, it is enough to prove that $\psi \vdash \phi \wedge \forall y.\neg(y[\neg\psi] \mid tt)$, to obtain $\psi \vdash \boxtimes\phi$ and $\boxtimes\phi \vdash \psi$.

A combination of these two methods can be used to prove more "exotic" axioms, like: $\diamond\phi \mid \psi \vdash \diamond(\phi \mid tt)$; $\diamond\diamond\phi \vdash \diamond\phi$; and $n[\diamond\phi] \vdash \diamond\phi$.

References

1. L. Cardelli and L. Caires. A spatial logic for concurrency. In *Proc. of TACS '01*, Lecture Notes in Computer Science. Springer-Verlag, 2001. to appear.
2. L. Cardelli and G. Ghelli. A query language based on the ambient logic. In *Proc. of ESOP '01*, volume 2028 of *Lecture Notes in Computer Science*, pages 1–22. Springer-Verlag, Apr. 2001.
3. L. Cardelli and A. D. Gordon. Anytime, anywhere: Modal logics for mobile ambients. In *Proc. of POPL '00 – 27th Annual ACM Symposium on Principles of Programming Languages*, pages 365–377. ACM Press, Jan. 2000.
4. L. Cardelli and A. D. Gordon. Mobile ambients. *Theoretical Computer Science*, 240:177–213, 2000.
5. U. Engberg and G. Winskel. Linear logic on petri nets. Technical Report RS-94-3, BRICS, 1994.
6. D. Kozen. Results on the propositional μ-calculus. *Theoretical Computer Science*, 27(3):333–354, 1983.