Programming Research Group

THE HYPERFINE SEMANTICS OF NON-INTERFERENCE

Dan R. Ghica

PRG-RR-02-14

Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford OX1 3QD

Abstract

We are presenting a semantic analysis of Reynolds's specification logic of Idealised ALGOL using the operationally-based techniques developed by Pitts. We hope that this more elementary account will make the important insights of Tennent and O'Hearn, originally formulated in a functor-category denotational semantics, more accessible to a wider audience. In addition, the operational model gives simple proofs to new axioms of specification logic as well as an interesting non-decidability result.

1 Introduction

The specification logic of Idealised ALGOL (IA) [Rey81a, Rey81b] is perhaps the best attempt to extend Hoare-style programming logic to a language with procedures. It is quite general and its usability has been clearly demonstrated. The semantics initially proposed by Reynolds is classical, with models of specifications consisting of environments of meanings for its free identifiers (universal specifications). Subsequently, Reynolds realized that making specifications stateful, i.e. including environment and state in the model, would lead to more powerful and more useful programming axioms.

The soundness of specification logic with stateful specifications has been the object of important semantic research. Tennent [Ten90] had the first important insight that this logic is intuitionistic and requires a Kripke-style possible worlds model, with sets of states functioning as worlds. The principal semantic innovation of his approach was the restriction of the behaviour of IA commands so that no states outside of the current world are visited in the course of the command's execution. The way this restriction is imposed mathematically in the denotational setting is also innovative, adapting a functor-categorical construction initially developed by Reynolds and Oles for a denotational semantics of IA [Rey81c, Ole97]. This mathematical construction is remarkable because the restriction it imposes seems, prima facie, incompatible with denotational semantics, which is extensional rather than intensional; in addition, the semantic model of the specification logic connects seamlessly with that of the programming language. This semantic model was further refined by Tennent and O'Hearn, allowing the validation of several new axioms [OT93].

The semantic ideas of the research mentioned before carried over into further work on the semantics of IA, leading to several improved models. Much of this work is collected in [OT97]. One trait this line of research shares is the technical reliance on the functor-categorical construction pioneered by Reynolds and Oles. The presentation therefore demands a rather high level of mathematical sophistication from the reader. In addition, the denotational model of IA it leads to is not fully abstract, which is, to some extent, unsatisfactory.

A more elementary account of the semantic properties of IA is given by Pitts, using operational techniques [Pit96]. The mathematical apparatus of this model is elementary, yet the model is powerful enough to prove various non-trivial properties of IA. In this paper we further develop Pitts's model to deal with specification logic. We hope that this will make the important and interesting ideas used to prove the soundness of specification logic accessible in the same way as Pitts's work made accessible the semantic properties of the programming language. To illustrate the strength of the model we prove two additional new axioms of specification logic. One of the axioms has been proposed before by O'Hearn [O'H90], but without a soundness proof. The other axiom is interesting because it relates Hoare triples and equivalence.

Finally, the operational model of specification logic allows a straightforward proof of undecidability for specification logic. What is remarkable about this undecidability result is that it occurs in a very restricted fragment of specification logic: first-order recursion-free boolean ALGOL with first-order quantifiers. Indeed, this is the bare minimum fragment in which procedures can be specified. This is despite the fact that observational equivalence of IA terms of first [GM00] and second [Ong02] order IA (with active expressions) is decidable.

2 Operational Semantics of IA

In this section we briefly present Pitts's operational model of IA [Pit96].

IA is simply-typed lambda calculus over booleans, integers, variables, expressions and commands. Variables, storing integers, form the state while commands can change the state. In addition to abstraction ($\lambda x{:}\sigma.M$) and application (FA), other terms of the language are conditionals, uniformly applied to any type, ($\mathbf{if}\ B\ \mathbf{then}\ M\ \mathbf{else}\ N$), fix-point recursion ($\mathbf{fix}\,x{:}\sigma.M$), constants (integers, booleans) and arithmetic-logic operators ($M * N$); we also have command-type terms which are the standard imperative operators: dereferencing (explicit in the syntax, $!V$), assignment ($V := N$), sequencing ($C; C'$), no-op (**skip**) and local variable block ($\mathbf{new}\,x := N\,\mathbf{in}\,C$). We write $M : \sigma$ to indicate that term M has type σ; if $\sigma = \sigma_1 \to \cdots \to \sigma_k \to \sigma'$ with σ' a ground type we say M is σ'-like.

The terms for abstraction, fix-point and local-variable block are identifier binders; IA terms are identified up to α-conversion. For any term M we denote the set of free identifiers and their type assignment $\mathit{fi}(M)$. By

$$\mathit{IA}_\sigma(w) = \{M : \sigma \mid \mathit{fi}(M) = \emptyset \text{ and } \mathit{gv}(M) \subseteq w\},$$

we denote the set of closed IA terms of type σ with global variables in the set w.

The operational semantics of IA is defined inductively on the syntax of terms by an evaluation relation of the form

$$w \vdash s; M \Downarrow_\sigma s'; R.$$

We call the set of global variables w *the world*. Terms $M, R \in \mathit{IA}_\sigma(w)$ and states $s, s' \in \mathit{States}(w) = \{f \mid f : w \to \mathbb{N}\}$. The interpretation of the rules is the following: term M executed in state s evaluates to term R and changes the state to s'. The evaluation relation is defined in Fig. 2.

The following notations are used: wv denotes the set w with a new element v added; $s \otimes (v \mapsto n) \in \mathit{States}(wv)$ denotes the state properly extending s by mapping v to n; $(s \mid v \mapsto n)$ denotes the state mapping v to n and otherwise acting like s.

The evaluation rules are more general than really necessary. It is straightforward to show that the evaluation of non-command terms does not change the state. Conversely,

$$w \vdash s; R \Downarrow_\sigma s; R, \qquad \text{where } R ::= \mathit{tt} \mid \mathit{ff} \mid v \mid n \mid \mathbf{skip} \mid \lambda x{:}\sigma.M$$

$$\frac{w \vdash s; B \Downarrow_{\mathbf{bool}} s'; b \qquad w \vdash s'; M_b \Downarrow_\sigma s''; R}{w \vdash s; (\mathbf{if}\ B\ \mathbf{then}\ M_{\mathit{tt}}\ \mathbf{else}\ M_{\mathit{ff}}) \Downarrow_\sigma s''; R}$$

$$\frac{w \vdash s; N_1 \Downarrow_{\mathbf{int}} s'; n_1 \qquad w \vdash s'; N_2 \Downarrow_{\mathbf{int}} s''; n_2}{w \vdash s; (N_1 * N_2) \Downarrow_{\mathbf{int}} s''; n}\ n = n_1 * n_2$$

$$\frac{w \vdash s; F \Downarrow_{\sigma \to \sigma'} s'; \lambda x{:}\sigma.M \qquad w \vdash s'; M[A/x] \Downarrow_{\sigma'} s''; R}{w \vdash s; FA \Downarrow_{\sigma'} s''; R}$$

$$\frac{w \vdash s; M[\mathbf{fix}\, x{:}\sigma.M/x] \Downarrow_\sigma s'; R}{w \vdash s; \mathbf{fix}\, x{:}\sigma.M \Downarrow_\sigma s'; R}$$

$$\frac{w \vdash s; V \Downarrow_{\mathbf{var}} s'; v}{w \vdash s; !V \Downarrow_{\mathbf{int}} s'; n}\ s'(v) = n$$

$$\frac{w \vdash s; V \Downarrow_{\mathbf{var}} s'; v \qquad w \vdash s'; N \Downarrow_{\mathbf{int}} s''; n}{w \vdash s; V := N \Downarrow_{\mathbf{comm}} (s'' \mid v \mapsto n); \mathbf{skip}}$$

$$\frac{w \vdash s; C \Downarrow_{\mathbf{comm}} s'; \mathbf{skip} \qquad w \vdash s'; C' \Downarrow_{\mathbf{comm}} s''; \mathbf{skip}}{w \vdash s; (C; C') \Downarrow_{\mathbf{comm}} s''; \mathbf{skip}}$$

$$\frac{w \vdash s; N \Downarrow_{\mathbf{int}} s'; n \qquad wv \vdash s' \otimes (v \mapsto n); C[v/x] \Downarrow_{\mathbf{comm}} s'' \otimes (v \mapsto n'); \mathbf{skip}}{w \vdash s; (\mathbf{new}\, x := N\, \mathbf{in}\, C) \Downarrow_{\mathbf{comm}} s''; \mathbf{skip}}$$

Figure 1: IA evaluation relation

command terms can only evaluate to **skip**. Therefore, the evaluation relation can be abbreviated to $w \vdash s; M \Downarrow_\sigma R$ if $\sigma \neq \mathbf{comm}$ and to $w \vdash s; C \Downarrow s'$, if $C : \mathbf{comm}$. If $w \vdash s; M \Downarrow_\sigma s'; R$ does not hold for any R and s' we write $w \vdash s; M \Uparrow_\sigma$.

A context $\mathcal{C}[-_\sigma]$ is an IA term in which a sub-term of type σ is replaced by a "hole" $-_\sigma$. The term resulting from filling the hole with term $M{:}\sigma$ is denoted by $\mathcal{C}[M]$. We write $\mathit{traps}(\mathcal{C}[-_\sigma])$ for the set of bound identifiers the scope of which includes the hole of $\mathcal{C}[-_\sigma]$, and their type assignments.

Terms or contexts without free identifiers are called *closed*. It is important to point out that a key distinction is being made between *global variables* and *free identifiers of type* **var**. A closed term may have zero, one or more global variables.

Definition 1 (Contextual equivalence) *If $M_i : \sigma$, with $\mathit{fi}(M_i) \subseteq \Gamma$ and $\mathit{gv}(M_i) \subseteq w$ for $i = 1, 2$, we write $w, \Gamma \vdash M_1 \cong_\sigma M_2$ to indicated that the terms are* contextually equivalent. *By definition, this means that for all worlds $w' \supseteq w$, all closed contexts $\mathcal{C}[-_\sigma]$:* **comm** *with $\mathit{gv}\big(\mathcal{C}[-_\sigma]\big) \subseteq w'$ and $\Gamma \subseteq \mathit{traps}\big(\mathcal{C}[-_\sigma]\big)$, and all states $s, s' \in \mathit{States}(w')$ we have*

$$w' \vdash \mathcal{C}[M_1]; s \Downarrow s' \quad \text{iff} \quad w' \vdash \mathcal{C}[M_2]; s \Downarrow s'.$$

Two terms are contextually equivalent if their occurrences can be interchanged in any closed command without affecting the meaning of the command, as a partial function from states to states.

The quantification over contexts in the definition of contextual equivalence makes the definition unwieldy for the proof of program properties. A more usable form of equivalence is *extensional equivalence* (OE).

Definition 2 (Extensional equivalence) *If $M_i \in IA_\sigma(w)$, $i = 1, 2$, we write $w \vdash M_1 \equiv_\sigma M_2$ to indicate that the terms are* extensionally equivalent*, which is defined inductively on the structure of σ as follows:*

- *If $\sigma = \mathbf{bool}, \mathbf{int}$ then $w \vdash M_1 \equiv_\sigma M_2$ if for all $s \in States(w)$ and all constants c, $w \vdash M_1; s \Downarrow_\sigma c$ iff $w \vdash M_2; s \Downarrow_\sigma c$;*
- *$w \vdash M_1 \equiv_{\mathbf{comm}} M_2$ if for all $s, s' \in States(w)$, $w \vdash M_1; s \Downarrow s'$ iff $w \vdash M_2; s \Downarrow s'$;*
- *$w \vdash M_1 \equiv_{\mathbf{var}} M_2$ if $w \vdash M_1 := n \equiv_{\mathbf{comm}} M_2 := n$ for all $n \in \mathbb{N}$;*
- *$w \vdash M_1 \equiv_{\sigma_1 \to \sigma_2} M_2$ if for all $w' \supseteq w$ and $A \in IA_{\sigma_1}(w')$, $w' \vdash M_1 A \equiv_{\sigma_2} M_2 A$.*

Extensional equivalence is extended to open terms via closed instantiations. If $M_i{:}\sigma_i$ with $fi(M_i) \subseteq \Gamma = \{x_1{:}\sigma_1, \ldots, x_n{:}\sigma_n\}$, $gv(M_i) \subseteq w$, $i = 1, 2$, we define $w, \Gamma \vdash M_1 \equiv_\sigma M_2$ as $w' \vdash M_1[\vec{A}/\vec{x}] \equiv_\sigma M_2[\vec{A}/\vec{x}]$ for all $w' \supseteq w$ and all $A_j \in IA_{\sigma_j}(w')$, $j = 1, \ldots, n$.

The key result of [Pit96] is the following:

Theorem 1 (Operational Extensionality) IA *contextual equivalence coincides with extensional equivalence:*

$$w, \Gamma \vdash M_1 \cong_\sigma M_2 \quad \text{iff} \quad w, \Gamma \vdash M_1 \equiv_\sigma M_2.$$

The proof technique used in [Pit96] is perhaps as important as the result itself, involving an operational version of parametric logical relations for IA. Using this technique Pitts is able to prove several challenging, and historically significant, properties of IA.

A useful ancillary property of IA proved in the same paper is Weakening and Strengthening (WS).

Lemma 1 (Weakening and Strengthening) *Suppose $w = w_1 w_2$, $s_i \in States(w_i)$, $i = 1, 2$. Given $M \in IA_\sigma(w_1)$, then $w \vdash s_1 \otimes s_2; M \Downarrow_\sigma s'; R$ if and only if $R \in IA_\sigma(w_1)$ and $s' = s'_1 \otimes s_2$ for some $s'_1 \in States(w_1)$ with $w \vdash s_1; M \Downarrow_\sigma s'_1; R$.*

2.1 Identity Logic of IA

One important direct consequence of the OE Theorem, pointed out by Pitts, is that it allows one to establish familiar functional extensionality properties such as:

$$F \cong_{\sigma \to \sigma'} F' \quad \text{iff} \quad \forall A{:}\sigma.\, F A \cong_{\sigma'} F' A.$$

It is important to point out that extensionality is not an universal property of programming languages. In call-by-value languages with more complex computational features such as references or exceptions, such as SCHEME or ML, this property fails.

IA, which is a conservative extension of PCF [O'H95], inherits extensionality as a generalised version of Milner's Context Lemma [Mil77] for PCF. Indeed, the denotational models of IA and its specification logic rest on the implicit assumption that the language is extensional. For example, the denotation typically given to equivalence in the specification logic is that of extensional equivalence, not that of observational equivalence. However, Pitts was the first to make this assumption explicit and formal.

We take this point further and we notice that the definitions of extensional equivalence for λ-abstraction and for terms with free identifiers is strongly suggestive of the interpretation of the universal quantifier in an intuitionistic logic, with a Kripke structure of worlds w and domains $IA_\sigma(w)$, cf. [vD94, Chap. 5].

Let us define the intuitionistic identity logic of IA as its many-sorted predicate logic with identity.

$$\phi ::= \phi \wedge \phi \mid \phi \vee \phi \mid \phi \to \phi \mid \forall x{:}\sigma.\, \phi \mid \exists x{:}\sigma.\, \phi \mid M = M'.$$

We can give a standard Kripke-semantics to this logic as follows.

Definition 3 (Kripke model) *For any world w and formula ϕ we define $w \Vdash \phi$, read "w forces ϕ," inductively on the structure of ϕ:*

- $w \Vdash \phi_1 \vee \phi_2$ *if* $w \Vdash \phi_1$ *or* $w \Vdash \phi_2$;
- $w \Vdash \phi_1 \wedge \phi_2$ *if* $w \Vdash \phi_1$ *and* $w \Vdash \phi_2$;
- $w \Vdash \phi_1 \to \phi_2$ *if for all* $w' \supseteq w$, *if* $w' \Vdash \phi_1$ *then* $w' \Vdash \phi_2$;
- $w \Vdash \forall x{:}\sigma.\, \phi$ *if for all* $w' \supseteq w$ *and for all* $A \in IA_\sigma(w')$, $w' \Vdash \phi[A/x]$;
- $w \Vdash \exists x{:}\sigma.\, \phi$ *if there is* $A \in IA_\sigma(w)$ *such that* $w \Vdash \phi[A/x]$;
- $w \Vdash M_1 = M_2$ *if* $w, \Gamma \vdash M_1 \cong_\sigma M_2$.

The Kripke-semantics of the intuitionistic identity logic of IA is sound. For connectives and quantifiers the interpretation is standard, and it is sound, so we will focus on the properties of identity.

Proposition 1 (Universal Closure of Identity) $w \Vdash M_1 = M_2$ *iff* $w \Vdash \forall x_1{:}\sigma_1 \cdots \forall x_k{:}\sigma_k.\, M_1 = M_2$, *where* $fi(M_i) \subseteq \{x_1{:}\sigma_1, \ldots x_k{:}\sigma_k\}$.

PROOF: $w \Vdash M_1 = M_2$ iff $w, \Gamma \vdash M_1 \cong_\sigma M_2$ iff $ww' \vdash M_1[\vec{A}/\vec{x}] = M_2[\vec{A}/\vec{x}]$ for all w' and $A_j \in IA_{\sigma_j}(ww')$ (by definition of OE), which is true iff $w \Vdash \forall x_1{:}\sigma_1 \cdots \forall x_k{:}\sigma_k.\, M_1 = M_2$ by definition of the universal quantifier. ∎

Proposition 2 (Monotonicity of Identity) *If* $w \Vdash M_1 = M_2$, *then for all worlds* $w' \supseteq w$, $w' \Vdash M_1 = M_2$.

PROOF: Using Prop. 1 and the definition of universal quantifier, it is enough to prove that the property holds for closed terms at any world $w'' \supseteq w$:

$$w'' \Vdash M_1 = M_2,\ M_i \in IA(w'') \text{ then for all worlds } w' \supseteq w'',\ w' \Vdash M_1 = M_2.$$

But this is an immediate consequence of the WS Lemma. ∎

Lemma 2 (Monotonicity) *If $w \Vdash \phi$ then for all $w' \supseteq w$, $w' \Vdash \phi$.*

PROOF: For connectives and quantifiers we have a standard Kripke semantics, and the monotoniciy proof is standard. For identity we use monotonicity of identity (Prop. 2). ∎

Definition 4 (Validity) *We say that ϕ is* valid*, denoted by $\Vdash \phi$, if for all worlds w, $w \Vdash \forall \vec{x}. \phi$, where $\vec{x} = \{x_1{:}\sigma_1, \cdots, x_k{:}\sigma_k\} \supseteq fi(\phi)$.*

Theorem 2 (Soundness) *If ϕ is a closed formula of the identity logic of* IA *derivable using the (standard) axioms of intuitionistic logic and identity then $\Vdash \phi$.*

PROOF: A standard induction on the length of derivation, for the intuitionistic logic and identity axioms and inference rules.

The most interesting case is one of the identity axioms:

$$w \Vdash \forall \vec{x}. \forall \vec{y}. \left(\bigwedge_i x_i = y_i \to \big(\phi(\vec{x}) \to \phi(\vec{y})\big) \right),$$

which in turn requires a lengthy but trivial induction on the structure of ϕ, with the only interesting case being the base case:

$$w \Vdash \forall \vec{x}. \forall \vec{y}. \left(\bigwedge_i x_i = y_i \to \big((M_1 = M_2)[\vec{x}/\vec{z}] \to (M_1 = M_2)[\vec{y}/\vec{z}]\big) \right).$$

Using the definitions, we need to prove that for all $w' \supseteq w$, $X_i \in IA_{\sigma_i}(w')$, for all $Y_j \in IA_{\sigma'_j}(w')$,

$$w' \Vdash \bigwedge_i X_i = Y_i \to \big((M_1 = M_2)[\vec{X}/\vec{z}] \to (M_1 = M_2)[\vec{Y}/\vec{z}]\big),$$

which follows directly from the OE Theorem, with M_i the contexts, with 'holes' z_i. ∎

2.2 Undecidability of the Intuitionistic Identity Logic of IA

The identity logic of full IA is obviously undecidable, as the language is Turing-complete. What may come as a surprise is that even if we restrict IA to its boolean, first-order, recursion-free subset, which is decidable [GM00], the intuitionistic identity logic is still undecidable. The language fragment also is assumed to contain a diverging term denoted by **diverge**.

The proof is quite straightforward. We show that Diophantine equations can be encoded in this language. It is well known that solving Diophantine equations, Hilbert's Tenth Problem, is undecidable (see [Mat93] for a comprehensive survey).

A Diophantine equation is an equation of the form $P(X_1, \ldots, X_N) = 0$ where P is a polynomial with integer coefficients. Hilbert's Tenth Problem concerns the existence of integer solutions for the equation. A similar undecidable problem can be posed for the existence of natural number solutions for equations of the form $P(X_1,\dots,X_N) = P'(X_1,\dots,X_N)$ and polynomials with natural coefficients:

$$\exists\vec{X}\in\mathbb{N}.P(X_1,\dots,X_N) = P'(X_1,\dots,X_N).$$

We show that there is an encoding $\ulcorner - \urcorner : \mathbb{N}[X] \to IA$ of polynomials with natural coefficients into IA terms then we show that the encoding is faithful, in the following sense.

Definition 5 (Faithful encoding) *We say that $\ulcorner - \urcorner : \mathbb{N}[X] \to IA$ is faithful if for all $P \in \mathbb{N}[X]$ and all $n', \vec{n} \in \mathbb{N}$, $P(\vec{n}) = n'$ iff $\ulcorner P(\vec{n})\urcorner = \ulcorner n'\urcorner$. If an encoding is faithful we write $\ulcorner - \urcorner : \mathbb{N}[X] \cong IA$.*

We define the encoding as follows:

- $\ulcorner 0\urcorner = \lambda c{:}\mathbf{comm}.\mathbf{skip}$
- $\ulcorner n+1\urcorner = \lambda c{:}\mathbf{comm}.\ulcorner n\urcorner(c); c = \lambda c{:}\mathbf{comm}.\underbrace{c;\cdots;c}_{n+1\text{ times}} = \lambda c{:}\mathbf{comm}.c^{n+1}$
- $\ulcorner X_i\urcorner = x_i{:}\mathbf{comm}\to\mathbf{comm}$
- $\ulcorner P_1 + P_2\urcorner = \lambda c{:}\mathbf{comm}.\ulcorner P_1\urcorner(c);\ulcorner P_2\urcorner(c)$
- $\ulcorner P_1 \times P_2\urcorner = \lambda c{:}\mathbf{comm}.\ulcorner P_1\urcorner\big(\ulcorner P_2\urcorner(c)\big)$

Proposition 3 (Faithfulness of encoding) $\ulcorner - \urcorner : \mathbb{N}[X] \cong IA$.

PROOF: Straightforward, by induction on the structure of the polynomial P. The only non-trivial step, albeit the most obvious, is the inductive hypothesis basis, $n = n'$ iff $\ulcorner n\urcorner = \ulcorner n'\urcorner$ for all $n, n' \in \mathbb{N}$. One direction is trivial; the second direction is $\ulcorner n\urcorner = \ulcorner n'\urcorner$ implies $n = n'$. Assume $n' \neq n$, then it follows that:

$$\lambda c{:}\mathbf{comm}.c^n = \lambda c{:}\mathbf{comm}.c^{n'}, \quad n \neq n'.$$

Using the semantics of equality from the previous section it follows that at any world w, $w \vdash \lambda c{:}\mathbf{comm}.c^n = \lambda c{:}\mathbf{comm}.c^{n'}$. Assume w.l.o.g. $n \le n'$ and consider the term $C \in IA_{\mathbf{comm}}(wv_1\cdots v_n)$ defined as follows:

$$\mathbf{if}\ !v_1\ \mathbf{then}\ v_1 := \mathbf{false}\ \mathbf{else}\ \cdots\mathbf{if}\ !v_n\ \mathbf{then}\ v_n := \mathbf{false}\ \mathbf{else}\ \mathbf{diverge}$$

It is quite obvious that $wv_1\cdots v_n \vdash s\otimes(v_i \mapsto tt); (\lambda c{:}\mathbf{comm}.c^n)C \Downarrow s\otimes(v_i\mapsto ff)$ but $wv_1\cdots v_n \vdash s\otimes(v_i\mapsto tt);(\lambda c{:}\mathbf{comm}.c^{n'})C \Uparrow_{\mathbf{comm}}$. Therefore, according to the OE Theorem the two terms are not equivalent, which is a contradiction. So $n = n'$. ∎

Given that the encoding is faithful, Hilbert's tenth problem can be formulated in the intuitionistic identity logic of first-order, recursion-free, boolean IA as follows:

$$\exists x_1{:}\mathbf{comm}\to\mathbf{comm}\cdots\exists x_n{:}\mathbf{comm}\to\mathbf{comm}.\ulcorner P_1\urcorner = \ulcorner P_2\urcorner, \quad P_1, P_2 \in \mathbb{N}[X]. \qquad (1)$$

As immediate consequence it follows that

Theorem 3 (Undecidability) *The intuitionistic identity logic of first-order, recursion-free, boolean IA is undecidable.*

3 Specification Logic

The logic of the previous section can be augmented with two more predicate symbols, Hoare-triples and non-interference:

$$\phi ::= \cdots \mid \{P\}\ C\ \{Q\} \mid M \# N,$$

where P, Q are *assertions*, C a command and M, N arbitrary IA terms. The language of assertions is the language of boolean phrases augmented with universal and existential quantifiers, but to keep the current presentation focused we will only consider a reduced assertion language which coincides with boolean phrases. The introduction of assertion quantifiers raises some technical complications, surveyed in [Ben86].

A straightforward interpretation of the new predicate symbols

- $w \Vdash \{P\}\ C\ \{Q\}$ if for all $s \in \mathit{States}(w)$, $w \vdash s; P \Downarrow_{\mathbf{assert}} \mathit{tt}$ and $w \vdash s; C \Downarrow s'$ implies $w \vdash s'; Q \Downarrow_{\mathbf{assert}} \mathit{tt}$
- $w \Vdash M \# N$ if for all $s_0, s_1, s_2, s_3 \in \mathit{States}(w)$, if $w \vdash s_0; M \Downarrow_{\sigma'} s_1; R$ then $w \vdash s_0; N \Downarrow_\sigma s_2; R'$ iff $w \vdash s_1; N \Downarrow_\sigma s_2; R'$

is enough to show the soundness of much of Reynolds's original, universal, specification logic [Rey81a].

The stateful specification logic requires a more sophisticated approach. The reason we want to make specifications stateful is to "factor out" assumptions about the state in judgements of the form

$$\{R\} \to \{P\}\ C\ \{Q\},$$

to be interpreted as "specification $\{P\}\ C\ \{Q\}$ is true in all states in which assertion {R} is true." Reynolds shows several examples where this is useful. Clearly, the role of the world must be now played by a set of states, which we shall call W. The interpretation of the logical connectives is now given by:

Definition 6 (Stateful Kripke semantics)

- *$W \Vdash \phi_1 \wedge \phi_2$ if $W \Vdash \phi_1$ and $W \Vdash \phi_2$*
- *$W \Vdash \phi_1 \vee \phi_2$ if $W \Vdash \phi_1$ or $W \Vdash \phi_2$*
- *$W \Vdash \phi_1 \to \phi_2$ if for all $W' \succsim W$, $W' \Vdash \phi_1$ implies $W' \Vdash \phi_2$*
- *$W \Vdash \forall x{:}\sigma.\,\phi$ if for all $W' \succsim W$, $W' \in \mathit{States}(ww')$, for all $A \in \mathit{IA}_\sigma(ww')$, $W' \Vdash \phi[A/x]$*
- *$W \Vdash \exists x{:}\sigma.\,\phi$ if there is $A \in \mathit{IA}_\sigma(w)$, $W \Vdash \phi[A/x]$*

The accessibility relation on worlds $\precsim$ reflects the fact that worlds, as set of states, can change in two ways: they can expand through the introduction of new variables or they can shrink because of implication.

Definition 7 (World accessibility) *We define the relation $W_1 \precsim W_2$, for $W_i \subseteq States(w_i)$, as the transitive and reflexive closure of:*

- $W_1 \precsim W_2$ *if* $W_2 = W_1 \times States(w_2 \setminus w_1)$
- $W_1 \precsim W_2$ *if* $W_2 \subseteq W_1$

It is straightforward to show that $\precsim$ is a partial order on sets of states.

The straightforward interpretation of the Hoare triple is no longer satisfactory in this context, because the axiom of command composition is no longer valid. We need to apply Tennent's key idea [Ten90] that execution of commands must be restricted to the current world, not only in terms of its final state but also in terms of all the intermediary states that are visited.

If a command C is allowed to visit states outside of W *even temporarily* then the axiom of sequential composition fails. Here is a simple example; we assume x is a global variable. Then,

$$\{!x = 0\} \to \{!x = 0\}\ x := 1\ \{!x = 1\} \tag{2}$$
$$\{!x = 0\} \to \{!x = 1\}\ x := 0\ \{!x = 2\} \tag{3}$$
$$\{!x = 0\} \to \{!x = 0\}\ x := 1\ \{!x = 1\} \wedge \{!x = 1\}\ x := 0\ \{!x = 2\} \tag{4}$$
$$\{!x = 0\} \to \{!x = 0\}\ x := 1; x := 0\ \{!x = 2\}. \tag{5}$$

Spec. 2 is true by virtue of the command leaving permanently the set of states to which it is restricted by the previous implication. (Note that if we use a semantics that does not restrict execution at all, this specification is also true.) Spec. 3 is true because the precondition cannot be met in the set of states for which the precedent holds. Spec. 4 is just predicate logic. Finally, spec. 5 is the consequence of the sequential composition axiom—and it is clearly a contradiction if the command completes successfully. Only the semantics which restricts even temporary excursions outside of the prescribed set of worlds causes the composed command to diverge.

We do this by introducing a more refined evaluation relation for IA, which we shall call *confined execution* and denote by $w, W \vdash s; M \Downarrow_\sigma s'; R$.

This relation is defined just like the normal evaluation (Fig. 2) with the exception of assignment and local variable definition.

Definition 8 (Confined evaluation)

$$w, W \vdash s; R \Downarrow_\sigma R;, \qquad \textit{where } R ::= tt \mid ff \mid v \mid n \mid \mathbf{skip} \mid \lambda x{:}\sigma.M$$

$$\frac{w, W \vdash s; B \Downarrow_{\mathbf{bool}} s'; b \qquad w, W \vdash s'; M_b \Downarrow_\sigma s''; R}{w, W \vdash s; \mathbf{if}\ B\ \mathbf{then}\ M_{tt}\ \mathbf{else}\ M_{ff} \Downarrow_\sigma s''; R}$$

$$\frac{w, W \vdash s; N_1 \Downarrow_{\mathbf{int}} s'; n_1 \qquad w, W \vdash s'; N_2 \Downarrow_{\mathbf{int}} s''; n_2}{w, W \vdash s; N_1 * N_2 \Downarrow_{\mathbf{int}} s''; n}\ n = n_1 * n_2$$

$$\frac{w, W \vdash s; F \Downarrow_{\sigma \to \sigma'} s'; \lambda x{:}\sigma.M \qquad w, W \vdash s'; M[A/x] \Downarrow_{\sigma'} s''; R}{w, W \vdash s; FA \Downarrow_{\sigma'} s''; R}$$

$$\frac{w, W \vdash s; M[\mathbf{fix}\, x{:}\sigma.M/x] \Downarrow_\sigma s'; R}{w, W \vdash s; \mathbf{fix}\, x{:}\sigma.M \Downarrow_\sigma s'; R}$$

$$\frac{w, W \vdash s; V \Downarrow_{\mathbf{var}} s'; v}{w, W \vdash s; !V \Downarrow_{\mathbf{int}} s'; n}\; s'(v) = n$$

$$\frac{w, W \vdash s; V \Downarrow_{\mathbf{var}} s'; v \qquad w, W \vdash s'; N \Downarrow_{\mathbf{int}} s''; n}{w, W \vdash s; V := N \Downarrow_{\mathbf{comm}} (s'' \mid v \mapsto n); \mathbf{skip}}\; (s'' \mid v \mapsto n) \in W$$

$$\frac{w, W \vdash s; N \Downarrow_{\mathbf{int}} s'; n \quad wv, W \times \mathit{States}(v) \vdash s' \otimes (v \mapsto n); C[v/x] \Downarrow_{\mathbf{comm}} s'' \otimes (v \mapsto n'); \mathbf{skip}}{w, W \vdash s; (\mathbf{new}\, x := N \,\mathbf{in}\, C) \Downarrow_{\mathbf{comm}} s''; \mathbf{skip}}$$

The only way a command can stray outside the current world is through assignment, but such an assignment is prevented by confined execution. If an illegal assignment is attempted the command cannot be executed. The world of a local variable block is expanded by all possible states involving the newly allocated variable.

Confined evaluation can be notationally simplified, similarly to standard evaluation, considering that only commands can change the state. We will adapt the old notation in the straightforward way.

The interpretation of the Hoare-triple predicate is:

Definition 9 (Hoare triple) $W \Vdash \{P\}\ C\ \{Q\}$ iff $w, W \vdash s; P \Downarrow_{\mathbf{assert}} \mathit{tt}$ *and* $w, W \vdash s; C \Downarrow s'$ *implies* $w, W \vdash s'; Q \Downarrow_{\mathbf{assert}} \mathit{tt}$.

Using confined evaluation we can define stronger notions of contextual and extensional equivalence in the obvious way.

Definition 10 (Hyperfine contextual equivalence) *If* $M_i : \sigma$, *with* $\mathit{fi}(M_i) \subseteq \Gamma$, $W \subseteq \mathit{States}(w)$ *and* $\mathit{gv}(M_i) \subseteq w$ *for* $i = 1, 2$, *we write* $W, \Gamma \vdash M_1 \cong_\sigma M_2$ *to indicated that the terms are* contextually hyperfine equivalent. *By definition, this means that for all worlds* ww', *all closed contexts* $\mathcal{C}[-_\sigma] : \mathbf{comm}$ *with* $\mathit{gv}(\mathcal{C}[-_\sigma]) \subseteq ww'$ *and* $\Gamma \subseteq \mathit{traps}(\mathcal{C}[-_\sigma])$, *set of states* $W' \subseteq \mathit{States}(w')$ *and states* $s, s' \in W \times W'$ *we have*

$$ww', W \times W' \vdash \mathcal{C}[M_1]; s \Downarrow s' \quad \text{iff} \quad ww', W \times W' \vdash \mathcal{C}[M_2]; s \Downarrow s'.$$

Definition 11 (Hyperfine extensional equivalence) *If* $M_i \in \mathit{IA}_\sigma(w)$, $i = 1, 2$, *we write* $w, W \vdash M_1 \equiv_\sigma M_2$ *to indicate that the terms are* extensionally hyperfine equivalent, *which is defined inductively on the structure of* σ *as follows:*

- *If* $\sigma = \mathbf{bool}, \mathbf{int}$ *then* $w, W \vdash M_1 \equiv_\sigma M_2$ *if for all* $s \in W$ *and all constants* c, $w, W \vdash M_1; s \Downarrow_\sigma c$ iff $w, W \vdash M_2; s \Downarrow_\sigma c$;
- $w, W \vdash M_1 \equiv_{\mathbf{comm}} M_2$ *if for all* $s, s' \in W$, $w, W \vdash M_1; s \Downarrow s'$ iff $w, W \vdash M_2; s \Downarrow s'$;
- $w, W \vdash M_1 \equiv_{\mathbf{var}} M_2$ *if* $w, W \vdash M_1 := n \equiv_{\mathbf{comm}} M_2 := n$ *for all* $n \in \mathbb{N}$;
- $w, W \vdash M_1 \equiv_{\sigma_1 \to \sigma_2} M_2$ *if for all worlds* ww', *all* $W' \subseteq \mathit{States}(w')$ *and* $A \in \mathit{IA}_{\sigma_1}(ww')$, *we have* $ww', W \times W' \vdash M_1 A \equiv_{\sigma_2} M_2 A$.

Extensional equivalence is extended to open terms via closed instantiations. If $M_i{:}\sigma_i$ *with* $fi(M_i) \subseteq \Gamma = \{x_1{:}\sigma_1, \ldots, x_n{:}\sigma_n\}$, $gv(M_i) \subseteq w$, $i = 1, 2$, *we define* $W, \Gamma \vdash M_1 \equiv_\sigma M_2$ *as* $ww', W \times W' \vdash M_1[\vec{A}/\vec{x}] \equiv_\sigma M_2[\vec{A}/\vec{x}]$ *for all* ww', *all* $W' \subseteq \mathit{States}(w')$ *and all* $A_j \in IA_{\sigma_j}(ww')$, $j = 1, \ldots, n$.

It is easy to show, by induction on derivation of evaluation, that confined evaluation also satisfies the WS Lemma.

Lemma 3 (Confined Weakening and Strengthening) *Suppose* $w = w_1 w_2$, $W_i \subseteq \mathit{States}(w_i)$, $s_i \in W_i$, $i = 1, 2$. *Given* $M \in IA_\sigma(w_1)$, *then*

$$w, W_1 \times W_2 \vdash s_1 \otimes s_2; M \Downarrow_\sigma s_1' \otimes s_2; R$$

iff $R \in IA_\sigma(w_1)$ *and* $s_1' \in W_1$ *with* $w_1, W_1 \vdash s_1; M \Downarrow_\sigma s_1'; R$.

Using exactly the same proof method as Pitts we can show that hyperfine equivalence is also extensional.

Theorem 4 (Hyperfine Operational Extensionality) IA *hyperfine contextual equivalence coincides with hyperfine extensional equivalence:*

$$W, \Gamma \vdash M_1 \cong_\sigma M_2 \quad \text{iff} \quad W, \Gamma \vdash M_1 \equiv_\sigma M_2.$$

Obviously, confined evaluation is a conservative extension of IA evaluation, and hyperfine equivalence is strictly stronger than contextual equivalence, which corresponds to equivalence 'confined' to the set of all states.

We give the following interpretation for identity:

Definition 12 (Identity) $W \Vdash M_1 = M_2$ iff *for all* $W' \subseteq W$, $\quad W', \Gamma \vdash M_1 \cong_\sigma M_2$.

3.1 Non-interference

Finally, we have come to the interpretation of the non-interference predicate, $M \# N$. As in the previous section, our approach is to implement the denotational concepts in the operational setting.

Intuitively, non-interference is interpreted as follows. The term on the right-hand-side, typically an expression, is used to partition the world into smaller worlds in which the term evaluates to the same result. Then, we require any evaluation of the term on the left-hand-side to be confined to any such equivalence class. In other words, any execution of M must not change the value of N *even temporarily.*

Definition 13 (State partitioning) *For any* IA *term* $E \in IA_\sigma(w)$ *we define the relation* $[M]_W \subseteq W^2$, $W \subseteq \mathit{States}(w)$, *inductively on the structure of* σ*:*

- *if* $\sigma =$ **int** *(or* **bool***) then* $s_1[E]_W s_2$ *if and only if there exists* $n \in \mathbb{N}$ *(or* $\{tt, ff\}$*) such that* $w, W \vdash s_1; E \Downarrow_\sigma n$ *iff* $w, W \vdash s_2; E \Downarrow_\sigma n$*;*
- *if* $\sigma =$ **var** *then* $s_1[V]_W s_2$ *if and only if* $s_1[!V]_W s_2$*;*

- *if* $\sigma = \mathbf{comm}$ *then* $s_1[C]_W s_2$ *if and only if* $w, W \vdash s_1; C \Downarrow$ *iff* $w, W \vdash s_2; C \Downarrow$*;*

- *if* $\sigma = \sigma_1 \to \sigma_2$ *then* $s_1[F]_W s_2$ *if and only if for all* $A \in IA_{\sigma_1}(w)$ *such that* $s_1[A]_W s_2$*,* $s_1[FA]_W s_2$*.*

The interpretation of the non-interference predicate $M \# N$ is also inductive, on the structure of M's type. For ground types, the definition is straightforward and it illustrates quite well the intuition above:

Definition 14 (Command non-interference) *If* $C \in IA_{\mathbf{comm}}(w)$ *then* $W \Vdash C \# N$ *if and only if, for all* $W_0 \in W/[N]$*, for all* $s \in W_0$*,* $w, W \vdash s; C \Downarrow s'$ *implies* $w, W_0 \vdash s; C \Downarrow s'$*.*

By $W/[N]$ we denote the set of equivalence classes of W under $[N]_W$. For variables, the definition is:

Definition 15 (Variable non-interference) *If* $V \in IA_{\mathbf{var}}(w)$ *then* $W \Vdash V \# N$ *if and only if for all* $n \in \mathbb{N}$ $w, W \Vdash V := n \# N$*.*

Since expressions do not change state, expression non-interference is always true. Expressions and expression-returning functions can never cause interference; O'Hearn and Tennent call such types *passive* types [OT93].

The definition of higher-order non-interference is subtler. Reynolds initially defined it extensionally:

$$\begin{aligned} F \# E &\leftrightarrow \big(\forall c{:}\sigma.\, c \# E \to F(c) \# E\big) \\ C \# F &\leftrightarrow \big(\forall e{:}\sigma.\, C \# e \to C \# F(e)\big), \end{aligned}$$

but Tennent showed that this definition is incompatible with a desirable axiom concerning non-interference decomposition [Ten90]. A sound model was given in [OT93].

An important technical role will be played by the property of *hyperfine termination*, which is a generalisation of the usual notion of termination to confined evaluation.

Definition 16 (Hyperfine termination) *We say that* $M \in IA(w)$ hyperfinely terminates*, denoted by* $w, W \vdash M \Downarrow_\sigma$ *if*

- $\sigma = \mathbf{comm}, \mathbf{int}, \mathbf{bool}$*: for all* $s \in W$*,* $w, W \vdash s; M \Downarrow_\sigma s'; R$

- $\sigma = \mathbf{var}$*: for all* $n \in \mathbb{N}$*,* $w, W \vdash M := n \Downarrow_{\mathbf{comm}}$

- $\sigma = \sigma_1 \to \sigma_2$ *and for all* $M' \in IA_{\sigma_1}(w)$*, if* $w, W \vdash M' \Downarrow_{\sigma_1}$ *then* $w, W \vdash MM' \Downarrow_{\sigma_2}$*.*

We can now define higher-order non-interference, which can be easily seen as a generalisation of the command non-interference, introduced earlier.

Definition 17 (Higher-order non-interference) *If* $F \in IA_\sigma(w)$*, then* $W \Vdash F \# M$ *if and only if,* $w, W \vdash F \Downarrow_\sigma$ *implies that for all* $W_0 \subseteq W$ *such that* $W_0 = \bigcup_{W' \in A} W'$*, where* $A \subseteq \mathbb{P}\big(W/[M]\big)$*, we have that* $w, W_0 \vdash F \Downarrow_\sigma$*.*

By $\mathbb{P}(-)$ we denote the powerset.

In words, restricting the current world to any smaller world which is a union of equivalence classes $W/[M]$, should not change the hyperfine termination status of F.

We can see how this definition works by examining a classic example:

$$\mathit{States}(i) \nVdash \lambda c{:}\mathbf{comm}.\,\mathbf{if}\ !i = 1\,\mathbf{then}\,(c; \mathbf{if}\ !i > 1\,\mathbf{then}\,i := 0) \mathbin{\#} i.$$

Let us call the procedure above F. Consider $M \stackrel{\text{def}}{=} \mathbf{if}\,i > 0\,\mathbf{then}\,i := !i + 1$. If we take $W_0 = \{(i \mapsto n) \mid n > 0\}$ it can be easily seen that $w, W_0 \vdash M \Downarrow_{\mathbf{comm}}$ but it is not the case that $w, W_0 \vdash FM \Downarrow_{\mathbf{comm}}$, since for $s = (i \mapsto 1)$, FM cannot be confinedly evaluated. W_0 is indeed a union of equivalences clases of $W/[i]$: $\bigcup_{k>0}\{(i \mapsto k)\}$.

3.2 Soundness

For the logical connectives and quantifiers we have a standard Kripke-semantics, which is sound. Using the Hyperfine OE Theorem we can also show that the interpretation of identity satisfies the standard axioms.

For identity, it is important to point out that the "hyperfine" semantics is truly required, because contextually equivalent IA phrases are not necessarily hyperfine equivalent. Consider for example the simple case $x \vdash x := 0; x := 1 \equiv_{\mathbf{comm}} x := 1$. Although contextually equivalent, when confined to world $(x \mapsto 1)$ the LHS diverges but the RHS does not, so they are not logically identical.

The Hoare-like axioms are proved in a standard way, and we have already showed the interesting bit regarding command composition for stateful specifications.

Technically, the only non-trivial part is showing that the non-interference predicate is monotonic. First we show that the confined evaluation relation is monotonic in the following sense

Lemma 4 (Monotonicity of Confined Evaluation) *If $w, W \vdash s; M \Downarrow_\sigma s'; R$ then for all $W' \supseteq W$, $w, W' \vdash s; M \Downarrow_\sigma s'; R$.*

Proof: Immediate, by induction on confined evaluation relation. ∎

Lemma 5 (Closure under Intersection for Confined Evaluation) *If $w, W_1 \vdash s; M \Downarrow_\sigma s'; R$ and $w, W_2 \vdash s; M \Downarrow_\sigma s'; R$ then $w, W_1 \cap W_2 \vdash s; M \Downarrow_\sigma s'; R$.*

Proof: Immediate, by induction on confined evaluation relation. ∎

Lemma 6 (Monotonicity of Confined Evaluation)

$$\text{If } W \Vdash F \mathbin{\#} M \text{ then } W' \Vdash F \mathbin{\#} M, \text{ for all } W' \gtrsim W.$$

Proof: The relation $\gtrsim$ is the transitive and reflexive closure of $\subseteq$ and $- \times \mathit{States}(w)$, so we need to prove that if $W \Vdash F \mathbin{\#} M$ then $W' \Vdash F \mathbin{\#} M$

- for all $W' = W \times \mathit{States}(w')$: that is immediate from the WS Lemma.

- for all $W' \subseteq W$:

  We need to prove that if $w, W \vdash F \Downarrow_\sigma$ implies that for all $W_0 \subseteq W$ such that $W_0 = \bigcup_{X \in A} X$, where $A \subseteq \mathbb{P}\big(W/[M]\big)$, we have that $w, W_0 \vdash F \Downarrow_\sigma$ then $w, W' \vdash F \Downarrow_\sigma$ implies that for all $W'_0 \subseteq W'$ such that $W'_0 = \bigcup_{X \in A'} X$, where $A' \subseteq \mathbb{P}\big(W'/[M]\big)$, we have that $w, W'_0 \vdash F \Downarrow_\sigma$.

  We use structural induction on the type of σ.

  If σ is a ground type we need to show that $w, W'_0 \vdash s; F \Downarrow_\sigma s'; R$ for all $s \in W'_0$. But $W'_0 = \bigcup_{X \in A'} X$, where $A' \subseteq \mathbb{P}\big(W'/[M]\big)$, so $W'_0 = W_0 \cap W'$ for some $W_0 = \bigcup_{X \in A} X$, where $A \subseteq \mathbb{P}\big(W/[M]\big)$. So we need to prove that $w, W_0 \cap W' \vdash s; F \Downarrow_\sigma s'; R$ for all $s \in W'_0$. This follows from Lem. 5 and the assumption that $w, W_0 \vdash F \Downarrow_\sigma$, $w, W' \vdash F \Downarrow_\sigma$.

  The inductive step is similar. ∎

We now show the soundness of the key axioms of Specification Logic.

3.2.1 Strong constancy

The proof for the constancy axiom:

$$\forall c{:}\mathbf{comm}.\forall pqr{:}\mathbf{assert}.\; c \,\#\, r \wedge (\{r\} \rightarrow \{p\}\; c\; \{q\}) \rightarrow \{p \;\mathbf{and}\; r\}\; c\; \{q \;\mathbf{and}\; r\},$$

is straightforward. The non-interference condition ensures that command c does not satisfy $\{p\}\; c\; \{q\}$ trivially, by (even temporarily) breaking assertion $\{r\}$ and causing a hyperfine divergence.

3.2.2 Left-side non-interference decomposition

We give a slightly different version of this axiom, which is equivalent with the traditional one but easier to deal with:

- if $C \in IA_\sigma(\emptyset)$ then $\forall e{:}\sigma'.\, C \,\#\, e$;
- $\forall f{:}\sigma{\rightarrow}\sigma'.\forall c{:}\sigma.\forall e{:}\sigma''.\, f \,\#\, e \wedge c \,\#\, e \rightarrow f(c) \,\#\, e$.

Closed terms without global variables cannot cause interference. Also, non-interference is compositional to the left.

For the first item, we need to prove that $W \Vdash C \,\#\, E$ for all $E \in IA_{\sigma'}(w)$. Using the WS Lemma we can show that for any $W_0 \subseteq W$, $w, W_0 \vdash C \Downarrow_\sigma$ if and only if $w, \mathit{States}(\emptyset) \vdash C \Downarrow_\sigma$, because C is a closed term. In this case, it is not even required that W_0 is a union of equivalence classes of $W/[E]$.

The second item reduces to $W \Vdash F \,\#\, E, C \,\#\, E$ implies $W \Vdash FC \,\#\, E$, which follows directly from the definition of hyperfine termination at function types.

3.2.3 Right-side non-interference decomposition

Again, we give a different but equivalent formulation for the axioms:

- if $E \in IA_\sigma(\emptyset)$ then $\forall c{:}\sigma'.\, c \# E$;
- $\forall f{:}\sigma \to \sigma'.\forall e{:}\sigma.\forall c{:}\sigma''.\, c \# f \wedge c \# e \to c \# f(e)$.

A closed term without global variables cannot be interfered with. Non-interference is also compositional to the right.

For the first item we can show using induction on the structure of σ and the WS Lemma that for any two states $s, s' \in W$, $s[E]_W s'$, i.e., the state-set is 'partitioned' in just one large partition.

The second item is proved by noticing that $s[E]_W s'$, and $s[F]_W s'$ implies $s[F(E)]_W s'$, i.e. the partitions generated by $F(E)$ include the partitions formed by F and E. Any execution of C confined to the smaller partitions will also be properly confined to the larger partitions.

3.2.4 Local variable

The local variable axiom scheme is

$$\big(\forall x{:}\mathbf{var}.\forall n{:}\mathbf{int}.\, \mathbf{gv}(x) \wedge \cdots x \# E_i \cdots \wedge \cdots C_j \# x \cdots \to \{P\}\ x := n; C\ \{Q\}\big) \\ \to \{P\}\ \mathbf{new}\, x := n\, \mathbf{in}\, C\ \{Q\}, \qquad x \notin \mathit{fi}(E_i, C_j, P, Q),$$

where the good variable predicate $\mathbf{gv}$[1] is defined as:

$$\mathbf{gv}(x) \stackrel{\text{def}}{=} \forall p{:}\mathbf{int} \to \mathbf{assert}.\forall e{:}\mathbf{int}.\, x \# p \to \{p(e)\}\ x := e\ \{p(!v)\}.$$

We first show that for any global variable v and world W, $W \Vdash \mathbf{gv}(v)$. For any P, we can show that $v \notin gv(P)$ implies $W \vdash v \# P$. Then we apply the WS Lemma and the OE Theorem to show that $P(E)$ and $P(!v)$ evaluate the same value.

The second part is to show that local variable v cannot interfere or be interfered with. This also follows directly from the WS Lemma, since v does not occur in any other phrases other than the block of the command, $C[v/x]$.

4 New Axioms and Undecidability

In this section we will prove two new axioms of specification logic.

The first one is

$$\forall pq{:}\mathbf{assert}.\forall c_1 c_2{:}\mathbf{comm}.\, \{p\}\ c_1; c_2\ \{q\} \leftrightarrow \exists r{:}\mathbf{assert}.\, \{p\}\ c_1\ \{r\} \wedge \{r\}\ c_2\ \{q\},$$

and it was suggested in [O'H90], as a stronger tool necessary for the proof of IA equivalences.

[1]NB. not to be confused with the global variable set gv.

PROOF (SOUNDNESS): The right-to-left direction is trivial and is simply the Hoare axiom for sequential composition.

The left-to-right direction requires us to prove that for all W,

$$W \Vdash \{P\}\ C_1;C_2\ \{Q\} \text{ implies } W \Vdash \exists r{:}\mathbf{assert}.\,\{P\}\ C_1\ \{r\} \wedge \{r\}\ C_2\ \{Q\},$$

with $P, Q \in IA_{\mathbf{assert}}(w)$, $C_1, C_2 \in IA_{\mathbf{comm}}(w)$.

Let

$$\begin{aligned} R \stackrel{\text{def}}{=} & \big(!v_1 = n_{1,1} \textbf{ and } \cdots \textbf{ and } !v_{k,1} = n_k\big) \textbf{ or} \\ & \vdots \\ & \textbf{or } \big(!v_1 = n_{1,l} \textbf{ and } \cdots \textbf{ and } !v_k = n_{k,l}\big), \end{aligned}$$

where $w = v_1 \cdots v_k$ and $n_{i,j} = s_j(v_i)$ and $W = \{s_1, s_2, \cdots, s_l\}$.

It can be easily seen that $R \in IA_{\mathbf{assert}}(w)$ and

$$W \Vdash \{P\}\ C_1;C_2\ \{Q\} \text{ implies } W \Vdash \{P\}\ C_1\ \{R\} \wedge \{R\}\ C_2\ \{Q\}.$$

∎

The second new axiom we will prove is

$$\forall c_1, c_2{:}\mathbf{comm}.\ \big(\forall p{:}\mathbf{assert}.\,\{\mathbf{true}\}\ c\ \{p\} = \{\mathbf{true}\}\ c_2\ \{p\}\big) \leftrightarrow c_1 = c_2.$$

PROOF (SOUNDNESS): The right-to-left implication is trivial. The left-to-right is proved by contradiction. Assume that there is world W, and $C_1, C_2 \in IA_{\mathbf{comm}}(w)$ such that $W \nVdash C_1 = C_2$. Let $s \in W$; we have three possible cases: C_1 terminates, C_2 diverges; C_2 terminates, C_1 diverges; both terminate but with different final states.

In the first case, let $s, s' \in W$ such that $w, W \vdash s; C_1 \Downarrow s'$ and $w, W \vdash s; C_2 \Uparrow_{\mathbf{comm}}$. Let $P \stackrel{\text{def}}{=} !v = n$ for some $v \in w$, where $n \neq s'(v)$. It can be easily seen that $W \Vdash \{\mathbf{true}\}\ C_2\ \{P\}$, through divergence, but $W \nVdash \{\mathbf{true}\}\ C_2\ \{P\}$. The other cases are similar. This is a contradiction. ∎

The reason for this axiom is technical. Our non-decidability result is based on the identity logic of IA. However, in specification logic term equality is not considered an essential connective, yet it plays the critical role in the proof of undecidability.

But the axiom above shows that term equality can be encoded in specification logic using just Hoare triples and predicate logic. Our main result follows from it:

Theorem 5 (Undecidability of Specification Logic) *Specification logic of recursion-free, first-order boolean* IA *without term equality, is undecidable in the presence of quantifiers over first-order types.*

PROOF: We know from Subsec. 2.2 that equations of this form:

$$\exists \vec{x}{:}\mathbf{comm} \to \mathbf{comm}.\,F =_{\mathbf{comm}\to\mathbf{comm}} G$$

are undecidable. Using the OE Theorem, this is equivalent to

$$\exists\vec{x}{:}\mathbf{comm} \to \mathbf{comm}.\forall c{:}\mathbf{comm}.\, Fc =_{\mathbf{comm}} Gc$$

being undecidable. Using the axiom above, this is equivalent to

$$\exists\vec{x}{:}\mathbf{comm} \to \mathbf{comm}.\forall c{:}\mathbf{comm}.\forall p{:}\mathbf{assert}.\, \{\mathbf{true}\}\ Fc\ \{p\} \leftrightarrow \{\mathbf{true}\}\ Gc\ \{p\}$$

being undecidable. So we can formulate undecidable propositions without using term equality. ∎

5 Semantics of Absurdity and Negation

The functor-category denotational semantics of specification logic [Ten90, OT93] introduces the the logical constant of **absurd** defined as false in all possible worlds, which is the standard Kripke-semantics of falsity.

However, this definition raises technical problems because specifications such as

$$\{\mathbf{false}\} \to \mathbf{absurd}, \tag{6}$$

which we might expect to be true, are in fact invalidated in the O'Hearn-Tennent models. The reason is that in the functor-category semantics, as in the semantics presented here, all Hoare triples are trivially true at the empty world. The definition of the Hoare triple is universally quantified over all states in the current world; having an empty world makes the Hoare triple trivially true. The hyperfine explanation is that in the empty world all IA phrases diverge, so all basic predicates (Hoare triples, non-interference, identity) are trivially true. The same can be seen to happen in the functor-category, but the calculations are a little more involved. Additionally, the empty world is accessible from any current world through inclusion.

So the *falsity* of specifications is not monotonic, therefore we can have neither Kripke-style negation nor Kripke-style falsity in our semantics. However, this does not have serious consequences at the logical level. We can simply define **absurd** as the following abbreviation:

$$\mathbf{absurd} \stackrel{\text{def}}{=} \{\mathbf{false}\}.$$

This validates (6) above, and in general has all the properties we expect of falsity. Negation can be defined then as

$$\neg\phi \stackrel{\text{def}}{=} \phi \to \mathbf{absurd}.$$

However, for the reasons discussed above **absurd** and $\neg$ are not genuine falsity and negation. Specification logic is, semantically, a strictly positive logic.

A semantic solution to this problem is to restrict the set of possible worlds to non-empty sets, since it is the empty set of worlds which forces the truth of these questionable specifications. Although this restriction introduces an unpleasant singularity in the semantics, it does not seem to raise additional technical problems.

Acknowledgements

I would like to thank Andrzej Murawski for helpful technical discussions, and to Bob Tennent and Peter O'Hearn for patiently answering my numerous questions.

References

[Ben86] E. Bencivenga. Free logics. In D. Gabbay and F. Guenthner, editors, *Handbook of Philosophical Logic, vol. III: Alternatives in Classical Logic*, number 166 in Synthese Library, pages 373–426. D. Reidel, Dordrecht, Holland, 1986.

[GM00] D. R. Ghica and G. McCusker. Reasoning about Idealized ALGOL using regular languages. In *Proceedings of 27th International Colloquium on Automata, Languages and Programming ICALP 2000*, volume 1853 of *LNCS*, pages 103–116. Springer-Verlag, 2000.

[Mat93] Y. V. Matiyasevich. *Hilbert's tenth Problem.* Nauka Publishers, Fizmalit, 1993. English translation: MIT Press, Cambridge, MA, 1993.

[Mil77] R. Milner. Fully abstract models of typed λ-calculi. *Theoretical Computer Science*, 4:1–22, 1977.

[MS88] A. R. Meyer and K. Sieber. Towards fully abstract semantics for local variables: preliminary report. In *Conference Record of the Fifteenth Annual ACM Symposium on Principles of Programming Languages*, pages 191–203, San Diego, California, 1988. ACM, New York. Reprinted as Chapter 7 of [OT97].

[O'H90] P. W. O'Hearn. *The Semantics of Non-Interference: A Natural Approach.* Ph.D. thesis, Queen's University, Kingston, Canada, 1990.

[O'H95] P. W. O'Hearn. Note on ALGOL and conservatively extending functional programming. *Journal of Functional Programming*, 6(1):171–180, 1995. A version also published as Chapter 4 of [OT97].

[Ole97] F. J. Oles. Functor categories and store shapes. In O'Hearn and Tennent [OT97], chapter 11, pages 3–12.

[Ong02] C.-H. L. Ong. Observational equivalence of third-order Idealized Algol is decidable. In *Proceedings of IEEE Symposium on Logic in Computer Science, 2002*, July 2002.

[OT93] P. W. O'Hearn and R. D. Tennent. Semantical analysis of specification logic, 2. *Information and Computation*, 107(1):25–57, 1993. Published also as Chapter 19 of [OT97].

[OT97] P. W. O'Hearn and R. D. Tennent, editors. ALGOL*-like Languages.* Progress in Theoretical Computer Science. Birkhäuser, Boston, 1997. Two volumes.

[Pit96] A. M. Pitts. Reasoning about local variables with operationally-based logical relations. In *11th Annual Symposium on Logic in Computer Science*, pages 152–163. IEEE Computer Society Press, Washington, 1996. A version also published as Chapter 17 of [OT97].

[Rey81a] J. C. Reynolds. *The Craft of Programming.* Prentice-Hall International, London, 1981.

[Rey81b] J. C. Reynolds. IDEALIZED ALGOL and its specification logic. In D. Néel, editor, *Tools and Notions for Program Construction*, pages 121–161, Nice, France, December 1981. Cambridge University Press, Cambridge, 1982.

[Rey81c] J. C. Reynolds. The essence of ALGOL. In J. W. de Bakker and J. C. van Vliet, editors, *Algorithmic Languages,* Proceedings of the International Symposium on Algorithmic Languages, pages 345–372, Amsterdam, October 1981. North-Holland, Amsterdam. Reprinted as Chapter 3 of [OT97].

[Ten90] R. D. Tennent. Semantical analysis of specification logic. *Information and Computation*, 85(2):135–162, 1990. A version also published as Chapter 13 of [OT97].

[vD94] D. van Dalen. *Logic and Structure.* Springer, Berlin, third edition, 1994.