On the Completeness of Propositional Hoare Logic

Dexter Kozen[1] and Jerzy Tiuryn[2]

[1] Computer Science Department, Cornell University, Ithaca NY 14853-7501, USA.
Email: kozen@cs.cornell.edu
[2] Institute of Informatics, Warsaw University, ul. Banacha 2, 02-097 Warsaw, Poland.
Email: tiuryn@mimuw.edu.pl

Abstract. We investigate the completeness of Hoare Logic on the propositional level. In particular, the expressiveness requirements of Cook's proof are characterized propositionally. We give a completeness result for Propositional Hoare Logic (PHL): all relationally valid rules

$$\frac{\{b_1\}\,p_1\,\{c_1\},\ \ldots\ ,\ \{b_n\}\,p_n\,\{c_n\}}{\{b\}\,p\,\{c\}}$$

are derivable in PHL, provided the propositional expressiveness conditions are met. Moreover, if the programs p_i in the premises are atomic, no expressiveness assumptions are needed.

1 Introduction

As shown by Cook [5], Hoare logic is relatively complete for partial correctness assertions (PCAs) over **while** programs whenever the underlying assertion language is sufficiently expressive. The expressiveness conditions in Cook's formulation provide for the expression of weakest preconditions. These conditions holds for first-order logic over $\mathbb{N}$, for example, because of the coding power of first-order number theory. Cook's proof essentially shows that in any sufficiently expressive context, the Hoare rules suffice to eliminate partial correctness assertions by reducing them to the first-order theory of the underlying domain.

Gurevich and Blass [3] separate Cook's construction into two steps: existential fixpoint logic gives sufficient expressibility for weakest preconditions; and if the domain is expressive, then first-order logic reduces to existential fixpoint logic.

Cook's and Gurevich and Blass's investigations in Hoare Logic, like most, are carried out in a first-order (Tarskian) context [1, 2, 6]. However, one can formulate a propositional version, appropriately named propositional Hoare logic (PHL) [10, 12], and ask about the derivation of relationally valid rules of the form

$$\frac{\{b_1\}\,p_1\,\{c_1\},\ \ldots\ ,\ \{b_n\}\,p_n\,\{c_n\}}{\{b\}\,p\,\{c\}}. \tag{1}$$

PHL is subsumed by other propositional program logics such as Propositional Dynamic Logic (PDL) [7] and Kleene algebra with tests (KAT) [9], whose semantics is derived from relational algebra. In PDL, expressiveness is not an issue because weakest preconditions are explicit in the language: the weakest precondition for program p with respect to postcondition c is expressed as $[p]\,c$. The Hoare partial correctness assertion $\{b\}\,p\,\{c\}$ becomes $b \to [p]\,c$ in PDL and $bp\overline{c} = 0$ in KAT. As shown in [11], KAT subsumes PHL, is of no greater complexity, and is complete for all relationally valid Horn formulas of the form $(\bigwedge_i p_i = 0) \to p = q$ (which include all rules of the form (1)), so for practical purposes the completeness of PHL is moot.

Nevertheless, there is interest in determining the deductive strength of the original Hoare rules in a propositional context in order to delineate the boundary between Hoare logic proper and the expressiveness assumptions on the underlying domain. We attempt here to characterize in a purely propositional way the necessary expressiveness properties used in Cook's proof. In doing so, we are led to the conclusion that in essence, expressiveness is a matter of axiomatization of the properties of weakest preconditions. We are able to show the following results concerning the derivation of relationally valid rules of the form (1):

(i) Under the assumption that the programs p_i in the premises of (1) are atomic, no expressiveness assumptions are necessary. Note that in the traditional formulation of Cook's theorem [5], this assumption is in force. The usual formulation of Hoare logic, as given for example in [2], is trivially incomplete, but a simple extension is complete for all relationally valid rules (1).

(ii) Without the atomicity assumption of (i), and even with the extensions of (i), Hoare logic is incomplete. We give a finite propositional axiomatization of weakest preconditions that essentially captures on a propositional level the expressiveness requirements of Cook's proof. Under these assumptions, PHL is complete.

To our knowledge, neither of these results follows from any previous result in propositional logics of programs. PDL is more expressive than KAT or PHL, and is apparently more complex (it is *EXPTIME*-complete as opposed to *PSPACE*-complete). However, the completeness results for PDL (see [13]) do not allow premises; in fact, the entailment problem for PDL is known to be Π_1^1-complete [15]. The Horn theory of KAT for equational implications involving premises of the form $p = 0$ is *PSPACE*-complete, but the relationship between PHL with the extra expressiveness assumptions and KAT is not known.

2 Propositional Hoare Logic

We denote programs by $p, q, r, \ldots$, atomic programs by a, and propositions by $b, c, d, \ldots$. As in KAT, we overload the symbols $+$ and $\cdot$ to denote choice and sequential composition, respectively, when applied to programs and disjunction and conjunction, respectively, when applied to propositions. We take $\to$ and $\mathbf{0}$ as a basis for the Boolean connectives. We denote the negation $b \to \mathbf{0}$ by $\overline{b}$ or $\neg b$. A *test* is a Boolean combination of atomic propositions. A PCA $\{b\}\, p\, \{c\}$ is called *atomic* if p is an atomic program.

The traditional Hoare rules for **while** programs are

$$\frac{\{bc\}\, p\, \{d\}, \quad \{\overline{b}c\}\, q\, \{d\}}{\{c\}\ \textbf{if}\ b\ \textbf{then}\ p\ \textbf{else}\ q\ \{d\}} \qquad \text{(conditional rule)}$$

$$\frac{\{b\}\, p\, \{c\}, \quad \{c\}\, q\, \{d\}}{\{b\}\, pq\, \{d\}} \qquad \text{(composition rule)}$$

$$\frac{\{bc\}\, p\, \{c\}}{\{c\}\ \textbf{while}\ b\ \textbf{do}\ p\ \{\overline{b}c\}} \qquad (\textbf{while}\ \text{rule})$$

$$\frac{b' \to b, \quad \{b\}\, p\, \{c\}, \quad c \to c'}{\{b'\}\, p\, \{c'\}} \qquad \text{(weakening rule).}$$

For simplicity, we formulate PHL over regular programs instead. We take the composition and weakening rules as in the traditional formulation, but replace the conditional and **while** rules with the simpler rules

$$\frac{\{b\}\, p\, \{c\}, \quad \{b\}\, q\, \{c\}}{\{b\}\, p + q\, \{c\}} \qquad \text{(choice rule)}$$

$$\frac{\{b\}\, p\, \{b\}}{\{b\}\, p^*\, \{b\}} \qquad \text{(iteration rule)}$$

$$\{b\}\, c\, \{bc\} \qquad \text{(test rule).}$$

Defining **if** b **then** p **else** q as $bp + \overline{b}q$ and **while** b **do** p as $(bp)^*\overline{b}$ as in PDL, the traditional formulation is subsumed [12].

We will also consider the following rules for incorporating propositional tautologies into PCAs: for any finite set C of tests,

$$\frac{\{c\}\,p\,\{d\}, \quad c \in C}{\{\bigvee C\}\,p\,\{d\}} \qquad \text{(or-rule)}$$

$$\frac{\{b\}\,p\,\{c\}, \quad c \in C}{\{b\}\,p\,\{\bigwedge C\}} \qquad \text{(and-rule).}$$

These rules are not needed in the traditional formulation because they can be viewed as properties of weakest preconditions.

We interpret PHL in Kripke frames. A Kripke frame $\mathfrak{K}$ consists of a set of states K and a map $\mathfrak{m}_{\mathfrak{K}}$ associating a subset of K with each atomic proposition and a binary relation on K with each atomic program. The map $\mathfrak{m}_{\mathfrak{K}}$ is extended inductively to compound programs and propositions according to standard rules (see [13]). We write $\mathfrak{K}, s \vDash b$ for $s \in \mathfrak{m}_{\mathfrak{K}}(b)$ and $s \xrightarrow[\mathfrak{K}]{p} t$ for $(s,t) \in \mathfrak{m}_{\mathfrak{K}}(p)$, and omit the $\mathfrak{K}$ when it is clear from context.

The PCA $\{b\}\,p\,\{c\}$ says intuitively that if b holds before executing p, then c must hold after. Formally, the meaning in PHL is the same as the meaning of $b \to [p]\,c$ in PDL: in a state s of a Kripke frame $\mathfrak{K}$,

$$\mathfrak{K}, s \vDash \{b\}\,p\,\{c\} \overset{\text{def}}{\Longleftrightarrow} (\mathfrak{K}, s \vDash b \;\Rightarrow\; \forall t\,(s \xrightarrow[\mathfrak{K}]{p} t \;\Rightarrow\; \mathfrak{K}, t \vDash c)).$$

For φ a PCA and Φ a set of PCAs, we write

$$\begin{aligned}
\mathfrak{K} \vDash \varphi &\overset{\text{def}}{\Longleftrightarrow} \forall s \in \mathfrak{K} \quad \mathfrak{K}, s \vDash \varphi \\
\mathfrak{K} \vDash \Phi &\overset{\text{def}}{\Longleftrightarrow} \forall \varphi \in \Phi \quad \mathfrak{K} \vDash \varphi \\
\Phi \vDash \varphi &\overset{\text{def}}{\Longleftrightarrow} \forall \mathfrak{K} \quad \mathfrak{K} \vDash \Phi \Rightarrow \mathfrak{K} \vDash \varphi.
\end{aligned}$$

A rule of the form (1) is *relationally valid* if $\{\{b_i\}\,p_i\,\{c_i\} \mid 1 \le i \le n\} \vDash \{b\}\,p\,\{c\}$. All the rules of PHL over **while** or regular programs mentioned above are relationally valid.

3 Weakest Preconditions

To formulate our assumptions concerning weakest preconditions, we extend our assertion language with formulas of the form either

$$[p_1]\,[p_2]\cdots[p_n]\,c \quad \text{or} \quad b \to [p_1]\,[p_2]\cdots[p_n]\,c.$$

Here b and c are tests and the p_i are regular programs. We call such formulas *extended PCAs*. Ordinary PCAs correspond to the case $n = 1$. We assume that there exists an interpretation of these formulas in the underlying domain such that the following properties are satisfied:

$$[p+q]\,\psi \leftrightarrow [p]\,\psi \wedge [q]\,\psi \tag{2}$$

$$[pq]\,\psi \leftrightarrow [p]\,[q]\,\psi \tag{3}$$

$$[p^*]\,\psi \leftrightarrow \psi \wedge [p]\,[p^*]\,\psi \tag{4}$$

$$[b]\,\psi \leftrightarrow (b \to \psi). \tag{5}$$

These properties are axioms of PDL (see [13]) and are related to properties of weakest preconditions for **while** programs [2]. Additionally, when reasoning in the presence of assumptions Φ, we will also postulate

$$b \to [p]\,c \tag{6}$$

for each $\{b\}\,p\,\{c\}$ in Φ, as well as certain atomic PCAs of the form

$$\{[a]\,c\}\,a\,\{c\}. \tag{7}$$

We use $\varphi, \psi, \ldots$ to denote PCAs or extended PCAs.

4 Main Results

The standard Hoare system consisting of the choice, composition, iteration, test, and weakening rules is trivially incomplete, even for relationally valid rules with atomic premises. For example, the and- and or-rules are not derivable, since it follows by induction on the length of proofs that without the or-rule, only atomic PCAs with stronger preconditions than those of the premises can be derived; similarly, without the and-rule, only atomic PCAs with weaker postconditions than those of the premises can be derived. However, if we add the and- and or-rules, we obtain completeness:

Theorem 1. *The Hoare system consisting of the choice, composition, iteration, test, weakening, and-, and or-rules is complete for relationally valid rules of the form* (1) *with atomic premises. Nothing is assumed about the underlying assertion language beyond propositional completeness.*

Proof. For this proof only, we write $\Phi \vdash \varphi$ if the conclusion φ is derivable from the premises Φ in the deductive system specified in the statement of the theorem. Suppose Φ is a set of atomic PCAs and φ a PCA such that $\Phi \nvdash \varphi$. We will construct a Kripke frame $\mathfrak{K}$ such that $\mathfrak{K} \vDash \Phi$ but $\mathfrak{K} \nvDash \varphi$.

A *literal* is an atomic proposition occurring in Φ or φ or its negation. For this proof only, an *atom* is a maximal propositionally consistent conjunction of literals. Atoms are denoted $\alpha, \beta, \gamma, \ldots$. Let K be the set of all atoms. For any formulas b and c, write $b \leq c$ if $b \to c$ is a propositional tautology.

The states of $\mathfrak{K}$ are the atoms. For atomic programs a and atomic propositions b, define

$$\begin{aligned}\mathfrak{m}_{\mathfrak{K}}(a) &\stackrel{\text{def}}{=} \{(\alpha, \beta) \mid \Phi \nvdash \{\alpha\}\, a\, \{\overline{\beta}\}\}\\ \mathfrak{m}_{\mathfrak{K}}(b) &\stackrel{\text{def}}{=} \{\alpha \mid \alpha \leq b\}.\end{aligned}$$

Thus

$$\begin{aligned}\alpha \xrightarrow{a} \beta &\iff \Phi \nvdash \{\alpha\}\, a\, \{\overline{\beta}\}\\ \alpha \vDash b &\iff \alpha \leq b.\end{aligned}$$

Extend $\mathfrak{m}_{\mathfrak{K}}$ to compound programs and propositions according to the usual inductive rules.

First we show that $\mathfrak{K} \vDash \Phi$. Let $\{b\}\, a\, \{c\}$ be a PCA in Φ. By assumption, a is atomic. If $\alpha \vDash b$ and $\beta \vDash \overline{c}$, then $\alpha \leq b$, $\beta \leq \overline{c}$, and $\Phi \vdash \{b\}\, a\, \{c\}$, so by weakening, $\Phi \vdash \{\alpha\}\, a\, \{\overline{\beta}\}$. By definition of $\mathfrak{m}_{\mathfrak{K}}(a)$, it is not the case that $\alpha \xrightarrow{a} \beta$.

Now we show that if $\Phi \nvdash \{b\}\, p\, \{c\}$, then there exist states α and β of $\mathfrak{K}$ such that $\alpha \xrightarrow{p} \beta$, $\alpha \vDash b$, and $\beta \vDash \overline{c}$, thus $\mathfrak{K} \nvDash \{b\}\, p\, \{c\}$.

Suppose $\Phi \nvdash \{b\}\, p\, \{c\}$. By the and- and or-rules, there must exist $\alpha \leq b$ and $\beta \leq \overline{c}$ such that $\Phi \nvdash \{\alpha\}\, p\, \{\overline{\beta}\}$, and it suffices to show that

$$\Phi \nvdash \{\alpha\}\, p\, \{\overline{\beta}\} \Rightarrow \alpha \xrightarrow{p} \beta.$$

We show the contrapositive by induction on the structure of p.

Suppose it is not the case that $\alpha \xrightarrow{p} \beta$. The case for atomic programs a is just the definition of $\mathfrak{m}_{\mathfrak{K}}(a)$. For p a test b, we have by definition of $\mathfrak{K}$ that either $\alpha \neq \beta$ or $\alpha = \beta \leq \overline{b}$. For the former, since $\Phi \vdash \{\overline{\beta}\}\, b\, \{b\overline{\beta}\}$ by the test rule,

$$\begin{aligned}\alpha \neq \beta &\Rightarrow \alpha \leq \overline{\beta} \text{ and } b\overline{\beta} \leq \overline{\beta}\\ &\Rightarrow \Phi \vdash \{\alpha\}\, b\, \{\overline{\beta}\} \qquad \text{by weakening.}\end{aligned}$$

For the latter, since $\Phi \vdash \{\alpha\}\, b\, \{b\alpha\}$ by the test rule,

$$\begin{aligned}\alpha = \beta \text{ and } \beta \leq \overline{b} &\Rightarrow b\alpha = \mathbf{0}\\ &\Rightarrow \Phi \vdash \{\alpha\}\, b\, \{\mathbf{0}\}\\ &\Rightarrow \Phi \vdash \{\alpha\}\, b\, \{\overline{\beta}\}.\end{aligned}$$

For the case of a choice $p+q$, if not $\alpha \xrightarrow{p+q} \beta$, then by the semantics of $\mathfrak{K}$ neither $\alpha \xrightarrow{p} \beta$ nor $\alpha \xrightarrow{q} \beta$. By the induction hypothesis, $\Phi \vdash \{\alpha\}\, p\, \{\overline{\beta}\}$ and $\Phi \vdash \{\alpha\}\, q\, \{\overline{\beta}\}$. By the choice rule, $\Phi \vdash \{\alpha\}\, p+q\, \{\overline{\beta}\}$.

For the case of a composition pq, if not $\alpha \xrightarrow{pq} \beta$, then by the semantics of $\mathfrak{K}$, no γ exists such that $\alpha \xrightarrow{p} \gamma \xrightarrow{q} \beta$. By the induction hypothesis, for all γ, either $\Phi \vdash \{\alpha\}\, p\, \{\overline{\gamma}\}$ or $\Phi \vdash \{\gamma\}\, q\, \{\overline{\beta}\}$. Defining

$$A = \{\gamma \mid \Phi \vdash \{\alpha\}\, p\, \{\overline{\gamma}\}\}$$
$$B = \{\gamma \mid \Phi \vdash \{\gamma\}\, q\, \{\overline{\beta}\}\},$$

we have that $A \cup B$ contains all atoms, therefore $(\neg \bigvee A) \to \bigvee B$ is a propositional tautology. But then

$$\begin{array}{ll} \Phi \vdash \{\alpha\}\, p\, \{\bigwedge_{\gamma \in A} \overline{\gamma}\} & \text{by the and-rule} \\ \Rightarrow \Phi \vdash \{\alpha\}\, p\, \{\neg \bigvee A\} & \text{by propositional logic} \\ \Rightarrow \Phi \vdash \{\alpha\}\, p\, \{\bigvee B\} & \text{by weakening,} \end{array}$$

and $\Phi \vdash \{\bigvee B\}\, q\, \{\overline{\beta}\}$ by the or-rule, therefore $\Phi \vdash \{\alpha\}\, pq\, \{\overline{\beta}\}$ by the composition rule.

Finally, for the case of iteration p^*, suppose $\beta \notin C$, where

$$C = \{\gamma \mid \alpha \xrightarrow{p^*} \gamma\}.$$

For $\gamma \in C$ and $\delta \notin C$, it is not the case that $\gamma \xrightarrow{p} \delta$, therefore by the induction hypothesis, $\Phi \vdash \{\gamma\}\, p\, \{\overline{\delta}\}$. It follows from the and- and or-rules that $\Phi \vdash \{\bigvee C\}\, p\, \{\bigwedge_{\delta \notin C} \overline{\delta}\}$. Since $\alpha \in C$ and $\beta \notin C$, we have $\alpha \le \bigvee C$ and $\bigvee C \le \overline{\beta}$, therefore

$$\begin{array}{ll} \Phi \vdash \{\bigvee C\}\, p\, \{\bigwedge_{\delta \notin C} \overline{\delta}\} & \\ \Rightarrow \Phi \vdash \{\bigvee C\}\, p\, \{\bigvee C\} & \text{by propositional logic} \\ \Rightarrow \Phi \vdash \{\bigvee C\}\, p^*\, \{\bigvee C\} & \text{by the iteration rule} \\ \Rightarrow \Phi \vdash \{\alpha\}\, p^*\, \{\overline{\beta}\} & \text{by weakening.} \end{array}$$

□

For rules of the form (1) whose premises are not necessarily atomic, the system of Theorem 1 is trivially incomplete. For example, the relationally valid rule

$$\frac{\{b\}\, p^*\, \{c\}}{\{b\}\, p\, \{c\}}$$

is not derivable, since it follows by induction on the length of proofs that no atomic PCA can be deduced from non-atomic premises unless it is a test. However, we will be able to obtain completeness under certain assumptions on the expressiveness of the underlying assertion language.

To formulate this result, we define the *Fischer–Ladner closure* for extended PCAs as in PDL (see [13]). A set X of extended PCAs is (*Fischer–Ladner*) *closed* if it satisfies the following closure rules:

- $b \to \psi \in X \quad \Rightarrow \quad b \in X$ and $\psi \in X$
- $\mathbf{0} \in X$
- $[p+q]\psi \in X \quad \Rightarrow \quad [p]\psi \in X$ and $[q]\psi \in X$
- $[pq]\psi \in X \quad \Rightarrow \quad [p]\,[q]\psi \in X$ and $[q]\psi \in X$
- $[p^*]\psi \in X \quad \Rightarrow \quad \psi \in X$ and $[p]\,[p^*]\psi \in X$
- $[b]\psi \in X \quad \Rightarrow \quad b \to \psi \in X$
- $[a]\psi \in X \quad \Rightarrow \quad \psi \in X$.

The smallest closed set containing a set Φ of extended PCAs is called the *Fischer–Ladner closure* of Φ and is denoted $FL\,\Phi$. Note that every element of $FL\,\Phi$ is an extended PCA.

The following theorem establishes completeness for all relationally valid rules of the form (1).

Theorem 2. *For a given relationally valid rule of the form* (1) *with premises Φ and conclusion φ, suppose that the underlying assertion language has formulas corresponding to all elements of $FL\Phi$ such that* (2)–(5) *hold for those formulas, as well as* (6) *for all elements of Φ. Then $\Phi \vdash \varphi$ in the Hoare system consisting of the choice, composition, iteration, test, weakening, and-, and or-rules, and* (7) *for all atomic PCAs in $FL\,\varphi$.*

Proof. For this proof, we write $\Phi \vdash \varphi$ if φ is deducible from the premises Φ in the system specified in the statement of the theorem.

Suppose $\Phi \nvdash \varphi$. As in Theorem 1, we build a Kripke frame $\mathfrak{K}$ such that $\mathfrak{K} \vDash \Phi$ but $\mathfrak{K} \nvDash \varphi$. The states of $\mathfrak{K}$ will be the maximal consistent conjunctions of elements of $FL\,\Phi$ and their negations; but in this case, *consistent* takes into account not only propositional logic, but also the properties (2)–(6).

Formally, define an *atom* to be a set α of formulas of $FL\,\Phi$ and their negations satisfying the following properties:

(i) for each $\psi \in FL\,\Phi$, exactly one of $\psi, \overline{\psi} \in \alpha$
(ii) for $b \to \psi \in FL\,\Phi$, $b \to \psi \in \alpha \iff (b \in \alpha \Rightarrow \psi \in \alpha)$
(iii) $\mathbf{0} \notin \alpha$
(iv) for $[p+q]\psi \in FL\,\Phi$, $[p+q]\psi \in \alpha \iff [p]\psi \in \alpha$ and $[q]\psi \in \alpha$
(v) for $[pq]\psi \in FL\,\Phi$, $[pq]\psi \in \alpha \iff [p][q]\psi \in \alpha$
(vi) for $[p^*]\psi \in FL\,\Phi$, $[p^*]\psi \in \alpha \iff \psi \in \alpha$ and $[p][p^*]\psi \in \alpha$
(vii) for $[b]\psi \in FL\,\Phi$, $[b]\psi \in \alpha \iff b \to \psi \in \alpha$
(viii) if $\{b\}\,p\,\{c\} \in \Phi$, then $b \to [p]\,c \in \alpha$.

We regard such an α variously as a set or as a formula corresponding to the conjunction of its elements. The properties (iv)–(viii) ensure consistency with respect to (2)–(6), respectively. The properties (i)–(iii) ensure propositional consistency. Our expressiveness assumption amounts to the assertion that if K is the set of all atoms, then $\bigvee K$ is true in the underlying model.

As in the proof of Theorem 1, we construct a model $\mathfrak{K}$ with states K. We define

$$\begin{aligned}
\mathfrak{m}_{\mathfrak{K}}(a) &\stackrel{\text{def}}{=} \{(\alpha,\beta) \mid \forall\,[a]\psi \in FL\,\Phi\,([a]\psi \in \alpha \Rightarrow \psi \in \beta)\}\\
\mathfrak{m}_{\mathfrak{K}}(b) &\stackrel{\text{def}}{=} \{\alpha \mid b \in \alpha\}\\
\mathfrak{m}_{\mathfrak{K}}([p]\psi) &\stackrel{\text{def}}{=} \{\alpha \mid [p]\psi \in \alpha\}
\end{aligned}$$

for atomic programs a, atomic propositions b, and extended PCAs of the form $[p]\psi$. The meaning function $\mathfrak{m}_{\mathfrak{K}}$ is lifted to compound programs and propositions according to the usual inductive rules.

For the purposes of this definition, formulas $[p]\psi$ occurring in $FL\,\Phi$ are treated as atomic propositions, since Hoare logic has no mechanism for breaking them down further. However, our subsequent arguments will establish a relationship between the meaning of such formulas as defined here and their meaning in PDL. Let us write $\vDash_{\mathsf{PDL}}$ for the latter; thus

$$\begin{aligned}
\alpha \vDash_{\mathsf{PDL}} [p]\psi &\iff \forall\beta\,(\alpha \xrightarrow{p} \beta \Rightarrow \beta \vDash_{\mathsf{PDL}} \psi)\\
\alpha \vDash_{\mathsf{PDL}} b &\iff \alpha \vDash b.
\end{aligned}$$

First we show by induction on the structure of p that for an extended PCA $[p]\psi \in FL\,\Phi$ and atoms α, β,

$$[p]\psi \in \alpha \text{ and } \alpha \xrightarrow{p} \beta \Rightarrow \psi \in \beta.$$

For an atomic program a, the conclusion is immediate from the definition of $\mathfrak{m}_{\mathfrak{K}}(a)$.

For a test b, if $[b]\psi \in \alpha$ and $\alpha \xrightarrow{b} \beta$, then $\alpha = \beta$ and $b \in \alpha$. By clauses (vii) and (ii) in the definition of atom, $\psi \in \alpha$.

If $[pq]\psi \in \alpha$, then by clause (v) in the definition of atom, $[p][q]\psi \in \alpha$. Suppose $\alpha \xrightarrow{pq} \beta$. Then there exists γ such that $\alpha \xrightarrow{p} \gamma \xrightarrow{q} \beta$. By the induction hypothesis on p, $[q]\psi \in \gamma$, and by the induction hypothesis on q, $\psi \in \beta$.

The case of a choice $p + q$ is similar, using clause (iv) in the definition of atom.

Finally, suppose $[p^*]\psi \in \alpha$ and $\alpha \xrightarrow{p^*} \beta$. There exist atoms $\gamma_0, \ldots, \gamma_n$ such that $\alpha = \gamma_0$, $\beta = \gamma_n$, and $\gamma_i \xrightarrow{p} \gamma_{i+1}$, $0 \leq i < n$. We have $[p^*]\psi \in \alpha = \gamma_0$. Now suppose $[p^*]\psi \in \gamma_i$, $i < n$. By clause (vi) in the definition of atom, $[p][p^*]\psi \in \gamma_i$. By the induction hypothesis on p, $[p^*]\psi \in \gamma_{i+1}$. Continuing in this fashion, we eventually have $[p^*]\psi \in \gamma_n = \beta$. Again by clause (vi) in the definition of atom, $\psi \in \beta$.

Now we show inductively that for $\psi \in FL\,\Phi$,

$$\psi \in \alpha \Rightarrow \alpha \models_{\mathsf{PDL}} \psi.$$

For tests b, we have

$$b \in \alpha \iff \alpha \models_{\mathsf{PDL}} b$$

by a simple induction on the structure of b.

For extended PCAs of the form $[p]\psi$ in $FL\,\Phi$, we have

$$\begin{aligned}
[p]\psi \in \alpha &\Rightarrow \forall \beta\,(\alpha \xrightarrow{p} \beta \Rightarrow \psi \in \beta) && \text{by the argument above}\\
&\Rightarrow \forall \beta\,(\alpha \xrightarrow{p} \beta \Rightarrow \beta \models_{\mathsf{PDL}} \psi) && \text{induction hypothesis}\\
&\Rightarrow \alpha \models_{\mathsf{PDL}} [p]\psi.
\end{aligned}$$

Finally, for extended PCAs of the form $b \to [p]\psi$ in $FL\,\Phi$, we have

$$\begin{aligned}
b \to [p]\psi \in \alpha &\Rightarrow (b \in \alpha \Rightarrow [p]\psi \in \alpha) && \text{definition of atom}\\
&\Rightarrow (\alpha \models_{\mathsf{PDL}} b \Rightarrow \alpha \models_{\mathsf{PDL}} [p]\psi) && \text{induction hypothesis}\\
&\Rightarrow (\alpha \models_{\mathsf{PDL}} b \to [p]\psi).
\end{aligned}$$

Now we can conclude that $\mathfrak{K} \models \Phi$. For any PCA $\{b\}\,p\,\{c\}$ in Φ, all atoms contain $b \to [p]c$ by clause (viii) in the definition of atom. By the argument above, $\alpha \models_{\mathsf{PDL}} b \to [p]c$ for all α. But this is just the semantics of the PCA $\{b\}\,p\,\{c\}$; thus $\mathfrak{K} \models \{b\}\,p\,\{c\}$.

To finish the completeness proof, we show that if $\Phi \nvdash \{b\}\,p\,\{c\}$, then there exist α and β such that $\alpha \xrightarrow{p} \beta$, $\alpha \models b$, and $\beta \models \overline{c}$, therefore $\mathfrak{K} \not\models \{b\}\,p\,\{c\}$. As in the proof of Theorem 1, it suffices to show that

$$\Phi \nvdash \{\alpha\}\,p\,\{\overline{\beta}\} \Rightarrow \alpha \xrightarrow{p} \beta.$$

We show the contrapositive by induction on the structure of p. All cases are identical to the corresponding cases in the proof of Theorem 1 except for the cases of atomic programs and composition.

For composition, the only difference is that the join of all atoms is not a propositional tautology when formulas $[p]\psi$ are regarded as atomic propositions because every atom must respect (2)–(6). For example, no atom can contain both $[p^*]c$ and $\overline{c}$. Because of this, we cannot conclude that the formula $(\neg \bigvee A) \to \bigvee B$ is a propositional tautology as in the proof of Theorem 1. However, although it is not a tautology, it is deducible from the postulated assumptions (2)–(6) and propositional logic.

For the case of an atomic program a, if it is not the case that $\alpha \xrightarrow{a} \beta$, then there must exist $[a]\psi \in \alpha$ such that $\overline{\psi} \in \beta$. Then $\alpha \leq [a]\psi$ and $\psi \leq \overline{\beta}$. By (7), $\Phi \vdash \{[a]\psi\}\,a\,\{\psi\}$, therefore by weakening, $\Phi \vdash \{\alpha\}\,a\,\{\overline{\beta}\}$. □

References

1. K. R. Apt. Ten years of Hoare's logic, a survey, part I. *ACM Trans. Programming Languages and Systems*, 3:431–483, 1981.
2. K. R. Apt and E.-R. Olderog. *Verification of Sequential and Concurrent Programs*. Springer-Verlag, 1991.
3. A. Blass and Y. Gurevich. Existential fixed-point logic. In E. Börger, editor, *Computation Theory and Logic. Lecture Notes in Computer Science 270*, pages 20–36, 1987.
4. E. M. Clarke. Programming language constructs for which it is impossible to obtain good Hoare axiom systems. *J. Assoc. Comput. Mach.*, 26:129–147, 1979.
5. S. A. Cook. Soundness and completeness of an axiom system for program verification. *SIAM J. Comput.*, 7:70–80, 1978.
6. Patrick Cousot. Methods and logics for proving programs. In J. van Leeuwen, editor, *Handbood of Theoretical Computer Science*, volume B, pages 841–993. Elsevier, Amsterdam, 1990.
7. M. J. Fischer and R. E. Ladner. Propositional dynamic logic of regular programs. *J. Comput. Syst. Sci.*, 18(2):194–211, 1979.
8. C. A. R. Hoare. An axiomatic basis for computer programming. *Comm. Assoc. Comput. Mach.*, 12:576–580, 583, 1969.
9. Dexter Kozen. Kleene algebra with tests. *Transactions on Programming Languages and Systems*, pages 427–443, May 1997.
10. Dexter Kozen. On Hoare logic and Kleene algebra with tests. In *Proc. Conf. Logic in Computer Science (LICS'99)*, pages 167–172. IEEE, July 1999.
11. Dexter Kozen. On Hoare logic and Kleene algebra with tests. *Trans. Computational Logic*, 1999. Submitted.
12. Dexter Kozen. On Hoare logic, Kleene algebra, and types. Technical Report 99-1760, Computer Science Department, Cornell University, July 1999.
13. Dexter Kozen and Jerzy Tiuryn. Logics of programs. In van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, pages 789–840. North Holland, Amsterdam, 1990.
14. R. J. Lipton. A necessary and sufficient condition for the existence of Hoare logics. In *Proc. 18th Symp. Found. Comput. Sci.*, pages 1–6. IEEE, 1977.
15. A. R. Meyer, R. S. Streett, and G. Mirkowska. The deducibility problem in propositional dynamic logic. In E. Engeler, editor, *Proc. Workshop Logic of Programs*, volume 125 of *Lect. Notes in Comput. Sci.*, pages 12–22. Springer-Verlag, 1981.
16. M. Wand. A new incompleteness result for Hoare's system. *J. Assoc. Comput. Mach.*, 25:168–175, 1978.