ELSEVIER

Information Sciences 139 (2001) 187–195

INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL

www.elsevier.com/locate/ins

On the completeness of propositional Hoare logic

Dexter Kozen [a,*,1], Jerzy Tiuryn [b,2]

[a] Computer Science Department, Cornell University, Ithaca, NY 14853-7501, USA
[b] Institute of Informatics, Warsaw University, ul. Banacha 2, 02-097 Warsaw, Poland

Received 9 January 2000; received in revised form 17 March 2001; accepted 25 June 2001

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. © 2001 Elsevier Science Inc. All rights reserved.

1. Introduction

As shown by Cook [6], 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

[*] Corresponding author. Tel.: +607-255-9209; fax: +607-255-4428.
E-mail addresses: kozen@cs.cornell.edu (D. Kozen), Tiuryn@mimuw.edu.pl (J. Tiuryn).

[1] Supported by NSF grants CCR-9708915 and CCR-0105586 and by ONR Grant N00014-01-1-0968.

[2] Supported by Polish KBN Grant 8 T11C 035 14.

PII: S0020-0255(01)00164-5

Cook's formulation provide for the expression of weakest preconditions. These conditions hold 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.

Several authors have undertaken to explicate the role of the expressiveness conditions in Cook's proof. Apt and Olderog [2] regard them as properties of weakest preconditions. 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 existential fixpoint logic reduces to first-order logic. Bloom and Ésik [4,5] give necessary and sufficient expressiveness conditions for the completeness of Hoare logic in the context of iteration theories.

Most investigations in Hoare logic are carried out in a context in which the symbols are interpreted over a fixed domain, usually a first-order (Tarskian) structure [1,2,7]. However, one can formulate a more abstract propositional version, appropriately named propositional Hoare logic (PHL) [10,11], 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) [8] 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 $bp\bar{c} = 0$ in KAT. As shown in [10], 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. Although motivated by the properties of weakest preconditions, we find that it is not necessary to characterize them completely. In this paper we 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 [6], 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 characterization of weakest preconditions that 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 [12]) do not allow premises; in fact, the entailment problem for PDL is known to be Π^1_1-complete [13]. 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 $\rightarrow$ and $\mathbf{0}$ as a basis for the Boolean connectives. We denote the negation $b \rightarrow \mathbf{0}$ by $\bar{b}$ or $\neg b$. A *test* is just a proposition, but we call it a test when we use it as a program. A PCA $\{b\}p\{c\}$ is called *simple* if p is either an atomic program or a test.

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

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

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

$$\frac{\{bc\}\ p\ \{c\}}{\{c\}\ \mathbf{while}\ b\ \mathbf{do}\ \{\bar{b}c\}} \quad (\textbf{while}\ \text{rule}),$$

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

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

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

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

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

Defining **if** b **then** p **else** q as $bp+\bar{b}q$ and **while** b **do** p as $(bp)^*\bar{b}$ as in PDL, the traditional formulation is subsumed [11].

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

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

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

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 all programs and propositions according to standard rules (see [12]). We write $\mathfrak{K},s\models b$ for $s\in\mathfrak{m}_{\mathfrak{K}}(b)$ and $s\underset{\mathfrak{K}}{\xrightarrow{p}}t$ for $(s,t)\in\mathfrak{m}_{\mathfrak{K}}(p)$, and omit the $\mathfrak{K}$ when it is clear from the 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 $\mathfrak{K}$, $\mathfrak{K},s\models\{b\}p\{c\}$ iff for all $t\in K$, if $\mathfrak{K},s\models b$ and $s\underset{\mathfrak{K}}{\xrightarrow{p}}t$, then $\mathfrak{K},t\models c$. For φ a PCA and Φ a set of PCAs, we write $\mathfrak{K}\models\varphi$ if for all $s\in K$, $\mathfrak{K},s\models\varphi$; $\mathfrak{K}\models\Phi$ if for all $\varphi\in\Phi$, $\mathfrak{K}\models\varphi$; and $\Phi\models\varphi$ if for all $\mathfrak{K}$, if $\mathfrak{K}\models\Phi$, then $\mathfrak{K}\models\varphi$. A rule of the form (1) is *relationally valid* if $\{\{b_i\}p_i\{c_i\}\mid 1\leqslant i\leqslant n\}\models\{b\}p\{c\}$. All the rules of PHL over **while** or regular programs mentioned above are relationally valid.

We tacitly assume a complete propositional deductive system for tests. All our completeness results hold in the presence of extra propositional assumptions of the form $b=0$, which we can encode as the PCA $\{true\}b\{false\}$.

3. Weakest preconditions

Theorem 4.1 will hold without any expressiveness assumptions concerning weakest preconditions. To formulate Theorem 4.2, however, we will need to extend our assertion language with formulas of the form either $[p_1][p_2]\cdots[p_n]c$

or $b \to [p_1][p_2]\cdots[p_n]c$. 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 will assume that there exists an interpretation of these formulas in the underlying domain such that the following properties are satisfied:

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

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

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

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

$$b \to [p]c \text{ for each } \{b\}p\{c\} \text{ in } \Phi \tag{6}$$

where Φ is the set of premises. Properties (2)–(5) are axioms of PDL (see [12]) 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 (6), as well as certain simple PCAs of the form $\{[a]\psi\}a\{\psi\}$. 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 simple 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 simple PCAs with stronger preconditions than those of the premises can be derived; similarly, without the and-rule, only simple 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 4.1. *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 simple premises.*

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 simple PCAs and φ a PCA such that $\Phi \nvdash \varphi$. We will construct a Kripke frame $\mathfrak{K}$ such that $\mathfrak{K} \models \Phi$ but $\mathfrak{K} \nvDash \varphi$.

A *literal* is an atomic proposition occurring in Φ or φ or its negation. Let Ψ be the set of propositional assumptions $bc \to d$ appearing in Φ in the form $\{b\}c\{d\}$. For this proof only, an *atom* is a maximal conjunction of literals propositionally consistent with Ψ. Atoms are denoted $\alpha, \beta, \gamma, \ldots$ Note that $\overline{\beta}$ is propositionally equivalent to the disjunction of all atoms different from β. Let

K be the set of all atoms. For propositions b and c, write $b \leqslant c$ if $b \to c$ is a propositional consequence of Ψ.

The states of $\mathfrak{K}$ are the atoms. For atomic programs a and atomic propositions b, define $\mathfrak{m}_{\mathfrak{K}}(a) \overset{\text{def}}{=} \{(\alpha, \beta) \mid \Phi \nvdash \{\alpha\}a\{\overline{\beta}\}\}$ and $\mathfrak{m}_{\mathfrak{K}}(b) \overset{\text{def}}{=} \{\alpha \mid \alpha \leqslant b\}$. Thus $\alpha \xrightarrow{a} \beta$ iff $\Phi \nvdash \{\alpha\}a\{\overline{\beta}\}$, and $\alpha \models b$ iff $\alpha \leqslant b$. Extend $\mathfrak{m}_{\mathfrak{K}}$ to all programs and propositions according to the usual inductive rules.

First we show that $\mathfrak{K} \models \Phi$. Let $\{b\}a\{c\}$ be a PCA in Φ. If a is a test, then $ba \leqslant c$, and $\mathfrak{K} \models ba \to c$ by purely propositional considerations. Otherwise, by assumption, a is an atomic program. If $\alpha \models b$ and $\beta \models \bar{c}$, then $\alpha \leqslant b$, $\beta \leqslant \bar{c}$, 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 suppose $\Phi \nvdash \{b\}p\{c\}$. We show that there must exist states α and β of $\mathfrak{K}$ such that $\alpha \xrightarrow{p} \beta$, $\alpha \models b$, and $\beta \models \bar{c}$, thus $\mathfrak{K} \nvDash \{b\}p\{c\}$. By the and- and or-rules, there exist $\alpha \leqslant b$ and $\beta \leqslant \bar{c}$ such that $\Phi \nvdash \{\alpha\}p\{\overline{\beta}\}$, so it suffices to show that if $\Phi \nvdash \{\alpha\}p\{\overline{\beta}\}$, then $\alpha \xrightarrow{p} \beta$. 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 $\alpha = \beta \leqslant \bar{b}$. For the former, since $\Phi \vdash \{\overline{\beta}\}b\{b\overline{\beta}\}$ by the test rule, if $\alpha \neq \beta$, then $\alpha \leqslant \overline{\beta}$ and $b\overline{\beta} \leqslant \overline{\beta}$, therefore $\Phi \vdash \{\alpha\}b\{\overline{\beta}\}$ by weakening. For the latter, since $\Phi \vdash \{\alpha\}b\{b\alpha\}$ by the test rule, if $\alpha = \beta$ and $\beta \leqslant \bar{b}$, then $b\alpha = \mathbf{0}$, therefore $\Phi \vdash \{\alpha\}b\{\mathbf{0}\}$ and $\Phi \vdash \{\alpha\}b\{\overline{\beta}\}$.

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 $p + q$, if not $\alpha \xrightarrow{p+q} \beta$, 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 $\Phi \vdash \{\alpha\}p\{\bar{\gamma}\}$ or $\Phi \vdash \{\gamma\}q\{\overline{\beta}\}$. Defining $A = \{\gamma \mid \Phi \vdash \{\alpha\}p\{\bar{\gamma}\}\}$ and $B = \{\gamma \mid \Phi \vdash \{\gamma\}q\{\overline{\beta}\}\}$, we have that $A \cup B$ contains all atoms, therefore $(\neg \vee A) \to \vee B$ is a consequence of Ψ. Then $\Phi \vdash \{\alpha\}p\{\bigwedge_{\gamma \in A} \bar{\gamma}\}$ by the and-rule, $\Phi \vdash \{\alpha\}p\{\neg \vee A\}$ by propositional logic, $\Phi \vdash \{\alpha\}p\{\vee B\}$ by weakening, $\Phi \vdash \{\vee B\}q\{\overline{\beta}\}$ by the or-rule, and $\Phi \vdash \{\alpha\}p + q\{\overline{\beta}\}$ 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, $\Phi \vdash \{\gamma\}p\{\bar{\delta}\}$. It follows from the and- and or-rules that $\Phi \vdash \{\vee C\}p\{\bigwedge_{\delta \notin C} \bar{\delta}\}$. Since $\alpha \in C$ and $\beta \notin C$, we have $\alpha \leqslant \vee C$ and $\vee C \leqslant \overline{\beta}$, therefore $\Phi \vdash \{\vee C\}p\{\vee C\}$ by propositional logic, $\Phi \vdash \{\vee C\}p^*\{\vee C\}$ by the iteration rule, and $\Phi \vdash \{\alpha\}p^*\{\overline{\beta}\}$ by weakening. □

For rules of the form (1) whose premises are not necessarily simple, the system of Theorem 4.1 is trivially incomplete. For example, the relationally valid rule that infers $\{b\}p\{c\}$ from $\{b\}p^*\{c\}$ is not derivable, since it follows by induction on the length of proofs that no simple PCA can be deduced from non-simple premises unless its program 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 [12]). A set X of extended PCAs is (*Fischer–Ladner*) *closed* if it satisfies the following closure rules:

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

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 4.2. *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 all simple PCAs* $\{[a]\psi\}a\{\psi\}$ *for* $[a]\psi \in FL\varphi$.

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 4.1, we build a Kripke frame $\mathfrak{K}$ such that $\mathfrak{K} \models \Phi$ but $\mathfrak{K} \not\models \varphi$. 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 the propositional consequences of Φ, 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 ψ, $\overline{\psi} \in \alpha$;
(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. Properties (iv)–(viii) ensure consistency with respect to (2)–(6), respectively. Properties (i)–(iii) ensure propositional consistency. Our expressiveness assumption amounts to the assertion that if K is the set of all atoms, then $\vee K$ is true in the underlying model.

As in the proof of Theorem 4.1, we construct a model $\mathfrak{K}$ with states K. We define $\mathfrak{m}_{\mathfrak{K}}(a) \overset{\text{def}}{=} \{(\alpha,\beta) \mid \forall [a]\psi \in FL\Phi\ ([a]\psi \in \alpha \Rightarrow \psi \in \beta)\}$ for atomic programs a, $\mathfrak{m}_{\mathfrak{K}}(b) \overset{\text{def}}{=} \{\alpha \mid b \in \alpha\}$ for atomic propositions b, and $\mathfrak{m}_{\mathfrak{K}}([p]\psi) \overset{\text{def}}{=} \{\alpha \mid [p]\psi \in \alpha\}$ for extended PCAs $[p]\psi$. The meaning function $\mathfrak{m}_{\mathfrak{K}}$ is extended to all 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 $\models_{\mathsf{PDL}}$ for the latter. Thus $\alpha \models_{\mathsf{PDL}} [p]\psi$ iff for all β, if $\alpha \xrightarrow{p} \beta$, then $\beta \models_{\mathsf{PDL}} \psi$; and $\alpha \models_{\mathsf{PDL}} b$ iff $\alpha \models b$.

First we show by induction on the structure of p that for an extended PCA $[p]\psi \in FL\Phi$ and atoms α, β, if $[p]\psi \in \alpha$ and $\alpha \xrightarrow{p} \beta$, then $\psi \in \beta$.

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 $\gamma_i \xrightarrow{p} \gamma_{i+1}$, $0 \leqslant i < n$. 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 $\psi \in FL\Phi$, if $\psi \in \alpha$, then $\alpha \models_{\mathsf{PDL}} \psi$. 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 $FL\Phi$, if $[p]\psi \in \alpha$, then for all β, if $\alpha \xrightarrow{p} \beta$, then $\psi \in \beta$ by the argument above. By the induction hypothesis, for all β, if $\alpha \xrightarrow{p} \beta$, then $\beta \models_{\mathsf{PDL}} \psi$, therefore $\alpha \models_{\mathsf{PDL}} [p]\psi$.

Finally, for extended PCAs of the form $b \to [p]\psi$ in $FL\Phi$, if $b \to [p]\psi \in \alpha$ and $b \in \alpha$, then $[p]\psi \in \alpha$ by the definition of atom. By the induction hypothesis, if $\alpha \models_{\mathsf{PDL}} b$, then $\alpha \models_{\mathsf{PDL}} [p]\psi$, therefore $\alpha \models_{\mathsf{PDL}} b \to [p]\psi$.

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 $\beta \models \bar{c}$, therefore $\mathfrak{K} \nvDash \{b\}p\{c\}$. As in the proof of Theorem 4.1, it suffices to show that if $\Phi \nvdash \{\alpha\}p\{\overline{\beta}\}$, then $\alpha \xrightarrow{p} \beta$. We show the contrapositive by induction on the structure of p. All cases are identical to the corresponding cases in the proof of Theorem 4.1 except for the case of atomic programs.

For an atomic program a, if not $\alpha \xrightarrow{a} \beta$, then there must exist $[a]\psi \in \alpha$ such that $\overline{\psi} \in \beta$. Then $\alpha \leqslant [a]\psi$ and $\psi \leqslant \overline{\beta}$. Since $[a]\psi \in FL\Phi$, we have $\Phi \vdash \{[a]\psi\}a$ $\{\psi\}$, 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 Syst. 3 (1981) 431–483.

[2] K.R. Apt, E.-R. Olderog, Verification of Sequential and Concurrent Programs, Springer, Berlin, 1991.

[3] A. Blass, Y. Gurevich, Existential fixed-point logic, in: E. Börger (Ed.), Computation Theory and Logic, Lecture Notes in Computer Science, vol. 270, Springer, Berlin, 1987, pp. 20–36.

[4] S.L. Bloom, Z. Ésik, Floyd–Hoare logic in iteration theories, J. Assoc. Comput. Mach. 38 (1991) 887–934.

[5] S.L. Bloom, Z. Ésik, Program correctness and matricial iteration theories, in: Proceedings of the 7th International Conference on Mathematical Foundations of Programming Semantics, Lecture Notes in Computer Science, vol. 598, Springer, Berlin, 1992, pp. 457–476.

[6] S.A. Cook, Soundness and completeness of an axiom system for program verification, SIAM J. Comput. 7 (1978) 70–80.

[7] P. Cousot, Methods and logics for proving programs, in: J. van Leeuwen (Ed.), Handbood of Theoretical Computer Science, vol. B, Elsevier, Amsterdam, 1990, pp. 841–993.

[8] M.J. Fischer, R.E. Ladner, Propositional dynamic logic of regular programs, J. Comput. Syst. Sci. 18 (1979) 194–211.

[9] D. Kozen, Kleene algebra with tests, Trans. Programming Languages Syst. 19 (1997) 427–443.

[10] D. Kozen, On Hoare logic and Kleene algebra with tests, in: Proceedings of the Conference on Logic in Computer Science (LICS'99), IEEE, New York, July 1999, pp. 167–172.

[11] D. Kozen, On Hoare logic, Kleene algebra, and types, Technical Report 99-1760, Computer Science Department, Cornell University, July 1999; Abstract, in: J. Cachro, K. Kijania-Placek (Eds.), Abstracts of 11th International Congress on Logic, Methodology and Philosophy of Science, Krakow, Poland, August 1999, p. 15; in: P. Gardenfors, K. Kijania-Placek, J. Wolenski (Eds.), Proceedings of the 11th International Congress on Logic, Methodology and Philosophy of Science, Kluwer Academic Publishers, Dordrecht (to appear).

[12] D. Kozen, J. Tiuryn, Logics of programs, in: J. van Leeuwen (Ed.), Handbook of Theoretical Computer Science, vol. B, North-Holland, Amsterdam, 1990, pp. 789–840.

[13] A.R. Meyer, R.S. Streett, G. Mirkowska, The deducibility problem in propositional dynamic logic, in: E. Engeler (Ed.), Proceedings of the Workshop Logic of Programs, Lecture Notes in Computer Science, vol. 125, Springer, Berlin, 1981, pp. 12–22.