PC-compactness, a necessary condition for the existence of sound and complete logics of partial correctness

by

J.A. Bergstra

Mathematical Center, Amsterdam, The Netherlands

J.Tiuryn

Institute of Mathematics, University of Warsaw, Poland

ABSTRACT

A first order theory is called PC-compact if each asserted program which is true in all models of the theory is true in all models of a finite subset of the theory. If a structure has a complete Hoare's logic then its first order theory must be PC-compact; moreover, its partial correctness theory must be decidable relative to this first order theory.

This identifies two necessary conditions that a structure must satisfy if Hoare's logic (or any sound logic of partial correctness extending Hoare's logic) is to be complete on the given structure. We provide an example of a structure that satisfies both conditions, on which Hoare's logic is incomplete but which does possess a sound and complete logic of partial correctness. This logic is obtained by adding a proof rule which incorporates aprogram transformation. The concept of PC-compactness is further studied in detail by means of an examination of various example structures.

KEY WORDS & PHRASES: Hoare's logic, logic of partial correctness, soundness, completeness, PC-compactness.

1. INTRODUCTION

This paper studies general and natural necessary conditions that are true of structures A which happen to have a complete Hoare's Logic for their while-programs. Especially we consider the following conditions:

(I) $Th(A)$ is PC-compact

(II) $PC(A)$ is recursive in $Th(A)$.

These conditions (to be explained in detail below) are quite natural and interesting for themselves.

We show that $HL(A)$ may be incomplete even if I and II are satisfied for A. The new concept of PC-compactness is investigated by evaluating it on various interesting example structures where it will show an unexpectedly irregular behaviour.

If $HL(A)$ is incomplete it is conceivable that some sound proof system $HL'(A)$, properly extending $HL(A)$, can be found which is complete. If so then we observe that also in this more general case the conditions I and II must necessarily be satisfied. (At this stage it will be essential to have a convincing concept of a sound proof system at hand). We infer that given A satisfying conditions I and II but having HL incomplete it is worthwhile to search for a sound and complete extension of $HL(A)$. Applying this on the example mentioned before we succeed in finding such an extension. It is not clear whether conditions I and II imply the existence of a sound and complete logic.

Before discussing connections with the litterature we will briefly consider some technical and definitional matters. Let Σ be a single or many-sorted signature. $Mod(\Sigma)$ denotes the class of all Σ-structures, $L(\Sigma)$ the corresponding first order language. For $A \in Mod(\Sigma)$, $Th(A) = \{p \in L(\Sigma) \mid A \models p\}$, the first order theory of A. For an asserted triple $\{p\}\ S\ \{q\}$ over Σ we write $T \models \{p\}\ S\ \{q\}$ if for all $A \in Mod(\Sigma)$, $A \models T$ implies $A \models \{p\}\ S\ \{q\}$.

$PC(T)$, the partial correctness theory of T consists of all asserted triples $\{p\}\ R\ \{q\}$ with $T \models \{p\}\ S\ \{q\}$. For $A \in Mod(\Sigma)$, $PC(A)$ denotes $PC(Th(A))$ and coincides with the set of all asserted programs true in A.

1.1. DEFINITION. T is PC-compact if for all $\{p\}\ S\ \{q\} \in PC(T)$ there is a finite subtheory $T' \subseteq T$ with $\{p\}\ S\ \{q\} \in PC(T')$.

On the syntactic side we have for each theory $T \subseteq L(\Sigma)$ a proof system HL(T), Hoare's Logic, proving asserted programs over Σ. HL is sound in the sense that HL(T) $\vdash \{p\}\ S\ \{q\}$ implies $T \models \{p\}\ S\ \{q\}$, for all T and $\{p\}\ S\ \{q\}$. For a fixed structure A, HL(A) is an abbreviation of HL(Th(A)), it is complete if it proves all of PC(A). We summarize some facts of prime importance in a proposition.

1.2. PROPOSITION.

(i) *If* HL(A) *is complete then* Th(A) *is* PC*-compact.*

(ii) Th(A) *is* PC*-compact if and only if for each* $\{p\}\ S\ \{q\}$ *true in* A *there is a sentence* $\phi \in$ Th(A) *such that* $\phi \models \{p\}\ S\ \{q\}$.

(iii) *If* A *and* B *are elementary equivalent* (Th(A)=Th(B)) *then* PC(A) = PC(B).

(iv) *If* HL(A) *is complete then* PC(A) *is recursive in* Th(A).

PROOF. (i) follows from the finitary nature of HL. (ii) is obvious, (iii) follows from the fact that $\{p\}\ S\ \{q\}$ can be written as an infinite conjunction $\bigwedge_{i=1}^{\infty} \{p\}\ S^n\ \{q\}$, where S^n denotes a program running n steps of S; $\{p\}\ S^n\ \{q\}$ moreover is a formula in $L(\Sigma)$. (iv) if HL(A) is complete then HL(A) = PC(A); as HL(A) is recursively enumerable in Th(A) by the nature of a proof system, on the other hand $\{p\}\ S\ \{q\} \notin$ PC(A) iff $\exists n\ A \models \{p\}\ S^n\ \{q\}$ iff $\exists n\ \{p\}\ S^n\ \{q\} \in$ Th(A) which shows that PC(A) is also co-recursively enumerable in Th(A). Combining both facts PC(A) is recursive in Th(A).

From this proposition we find that conditions I and II are necessary for the completeness of HL(A). It can easily be seen that both conditions are independent. For instance the structure A = $(\omega,S,0)$ satisfies condition I but not condition II whereas the structure [N,N] satisfies condition II but not condition I (see 3.1.). Consequently the conjunction I $\wedge$ II is a meaningful stronger necessary condition for completeness of HL(A).

We will now briefly discuss results from previous work connected with our topic. WAND [9] presents a nice example of a structure A with HL(A) incomplete. One can show that Wand's example violates condition II. COOK [5] introduces the now familiar concept of expressiveness which constitutes a condition on a structure A sufficient for the completeness of HL(A). In BERGSTRA & TUCKER [3] it is shown that expressiveness is not a necessary cocdition however. Condition II studied in BERGSTRA, CHMIELIENSKA & TIURYN [1]; it is

shown that condition II is not sufficient for completeness of HL. Using two-sorted structures this fact is derived more easily in BERGSTRA & TUCKER [2]. Essentially [1] show how to transform examples using two-sorted structures into similar examples using single sorted structures. We take that as a justification for freely using two-sorted structures in this paper.

Four concrete structures will be considered more closely. These examples all are two sorted structures $[M_1,M_2]$ resulting from combining two disjoint (and disconnected) single sorted structures M_1 and M_2 into a two-sorted structure.

[N,B] with $N = (\omega,S,t,\cdot,<,0)$ and
$B = (\{t,f\}, \vee,\neg,T,F)$, the booleans.

[N,A] with $A = (\omega,S,0)$, in LAMBEK [7]
A is called Abacus arithmetic.

[N,A0] with $A0 = (\omega,S,<,0)$, Abacus arithmetic with ordering.

[N,N] two copies of N.

The only essential point of two-sorted structures is that we may use separate variables for both sorts. For clarity it may be useful to have different names S',t',·',<',0' in connection with the second sort.

Each of these structures satisfies condition II. This follows from the following simple fact that can serve as a test for condition II in most (practical) cases:

1.3. PROPOSITION. *Suppose* A *is computable and* Th(N) *is recursive in* Th(A), *then* PC(A) *is recursive in* Th(A).

Concerning condition I, PC-compactness, we will prove the following theorem.

1.4. THEOREM.

(i) Th([N,B]) *is* PC-*compact.* (3)
(ii) Th([N,A]) *is not* PC-*compact.* (3.3)
(iii) Th([N,A0]) *is* PC-*compact.* (3.5)
(iv) Th([N,N]) *is not* PC-*compact.* (3.1)

This behaviour of PC-compactness is rather surprising and the proof of (iii) suggests that [N,A0], though not a pathological structure, might be a rather isolated example of a PC-compact structure of such complexity. Relating these results to proof systems we obtain the following theorem.

1.5. THEOREM.

(i) [N,A0] *satisfies both conditions I and II but* HL([N,A0]) *is incomplete.* (3.7)

(ii) There exists a sound logic of partial correctness HL'([N,A0]) *properly extending* HL([N,A0]) *which is complete.* (3.6)

We will conclude the paper with a listing of four open questions that naturally arise from our results.

2. PRELIMINARIES ON LOGIC

First of all we will need logical information about the structures A,A0 and N. The following proposition contains all nontrivial facts that will play a rôle in the proofs of both theorems 1.4 and 1.5.

2.1. PROPOSITION.

(i) Th(A) *has no finite axiomatisation.*

(ii) Each finite $T \subseteq$ Th(A) *has a model that contains a finite S-cycle as a substructure.*

(iii) Th(A0) *is finitely axiomatizable.*

(iv) There is a formula $\phi(x) \in L(N)$ *such that* $\{n \mid N \models \phi(\underline{n})\}$ *is not recursively enumerable.*

PROOF. (i), (ii) and (iii) follow from various results in CHANG & KEISLER [4]; (iv) follows from the fact that all arithmetical relations are definable in N (see SHOENFIELD [8] for more details).

Then we need a simple fact about two-sorted structures of the form [M,M'].

2.2. SEPARATION OF VARIABLES LEMMA. For each $\phi \in L([M,M'])$ there exists a formula ψ equivalent to ϕ which is a propositional combination of formulae in $L(M_1) \cup L(M_2)$.

PROOF. A proof is given in [2]. Note here that $L(M_1)$ and $L(M_2)$ are supposed to use different variables.

In particular ψ can be written in the form $\bigvee_{i=1}^{n} (\psi_1^i \wedge \psi_2^i)$ with $\psi_1^i \in L(M_1)$ and $\psi_2^i \in L(M_2)$.

Thirdly we must explain what exactly will be meant by a (sound) proof system for partial correctness. Given a signature Σ a logic of partial correctness L_Σ for Σ is a recursively enumerable set of pairs:

$$\{(\phi_i, \{p_i\} S_i \{q_i\}) \mid i \in \omega\}$$

with $\phi_i \in L(\Sigma)$ and $\{p_i\}\ S_i\ \{q_i\}$ an asserted triple over Σ. We write for $T \subseteq L(\Sigma)$

$$L_\Sigma(T) \vdash \{p\}\ S\ \{q\}$$

if for some ϕ, $T \vdash \phi$ and $(\phi, \{p\}S\{q\}) \in L_\Sigma$. L_Σ is sound if for all T and $\{p\}\ S\ \{q\}$

$$L_\Sigma(T) \vdash \{p\}\ S\ \{q\} \text{ implies } T \models \{p\}\ S\ \{q\}.$$

Note that soundness of L_Σ is a notion not related to any particular interpretation $A \in \mathrm{Mod}(\Sigma)$.
We put

$$L_\Sigma(A) = L_\Sigma(\mathrm{Th}(A)).$$

$L_\Sigma(A)$ is sound if L_Σ is sound, and complete if $L_\Sigma(A) = \mathrm{PC}(A)$.

HL_Σ can be considered as an L_Σ as follows: Let $(\phi, \{p\}S\{q\}) \in L_\Sigma^{HL}$ if ϕ is of the form $\phi_0 \wedge \ldots \wedge \phi_{2(k-1)}$ with k the smallest number of applications of the rule of consequence necessary in a HL-proof of $\{p\}\ S\ \{q\}$ and with ϕ_{2n}, ϕ_{2n+1} the logical information required to pass the n-th application

of the rule of consequence in a proof of {p} S {q}.

3. PROOFS OF THE THEOREMS

We will prove the various parts of both theorems 1.4 and 1.5 in the form of a series of propositions that cover individual parts. Th 1.4. (i), however, follows from the results in [2]; as a mather of fact for any finite structure F, [N,F] is expressive and therefore satisfies conditions I and II. All remaining parts require some argument and have a special proposition devoted to them.

3.1. PROPOSITION. Th([N,N]) *is not* PC-*compact*.

PROOF. We will destinguish both copies of N by writing [N,N'] and using the superscript prime on all symbols of its signature.

Now let $\phi(x)$ be a formula in $L(N)$ such that $\{n \mid N \models \phi(n)\}$ is not recursively enumerable (see 2.1. (iv)). Let $\phi'(y)$ be a version of ϕ for $L(N')$, and let z be one more variable for N. Consider the program R:

z := 0; y := 0;

while $z \neq x$ do z := S(z); y := S'(y) od

It is clear by inspection that

$$[N,N'] \models \{\phi(x)\}\ R\ \{\phi'(y)\}.$$

We will then show that there is no sentence θ true of [N,N'] such that $\theta \models \{\phi(x)\}\ R\ \{\phi'(y)\}$. Indeed suppose such a θ exists. Using the separation of variables lemma θ can equivalently be written as follow:

$$\vdash \theta \leftrightarrow \bigvee_{i=1}^{k} (\theta_i \wedge \theta_i') \text{ with } \theta_i \in L(N),\ \theta_i' \in L(N).$$

Because $[N,N'] \models \theta$ we may choose an i such that $[N,N'] \models \theta_i \wedge \theta_i'$. Clearly $\theta_i \wedge \theta_i' \models \{\phi(x)\}\ R\ \{\phi'(y)\}$. We will derive a contradiction from this fact.

Let $\underline{0} = \underline{0}$, $\underline{n+1} = S(\underline{n})$, $\underline{0}' = \underline{0}'$, $\underline{n+1}' = S'(\underline{n}')$ and write

$$A = \{n \in \omega \mid N \models \phi(\underline{n})\}$$

$$B = \{n \in \omega \mid \theta_i' \models \phi(\underline{n}')\}$$

B is recursively enumerable (by construction) and due to the choice of ϕ, A is not recursively enumerable so $A \neq B$. Taking into account that $N \models \theta_i'$ we see that $A \supseteq B$. So we may choose $n \in A - B$. Then by the completeness theorem there is a model N" of θ_i' in which $N'' \models \neg\phi(\underline{n}')$. On the other hand $[N,N''] \not\models \{\phi(x)\}\ R\ \{\phi'(y)\}$ which follows by giving x the initial value n. Indeed because $n \in A$, $[N,N''] \models \phi(\underline{n})$ but after termination of S,y equals $\underline{n}'$ and $[N,N''] \not\models \phi'(\underline{n}')$. This gives the required contradiction.

3.2. PROPOSITION. *If* $[M_1,M_2]$ *satisfies condition I then so do* M_1 *and* M_2.

PROOF. Supppose $M_1 \models \{p\}\ S\ \{q\}$, then $[M_1,M_2] \models \{p\}\ S\ \{q\}$. Choose $\theta \in L([M_1,M_2])$ such that $\theta \models \{p\}\ S\ \{q\}$. Write $\theta \leftrightarrow \bigvee_{i=1}^{n} (\theta_i^1 \wedge \theta_i^2)$ with $\theta_i^j \in L(M_j)$. Choose i such that $[M_1,M_2] \models \theta_i^1 \wedge \theta_i^2$; then $\theta_i^1 \wedge \theta_i^2 \models \{p\}\ R\ \{q\}$ and obviously $\theta_i^1 \models \{p\}\ R\ \{q\}$ which state of affairs we were looking for.

3.3. PROPOSITION. $[N,A]$ *does not satisfy condition I.*

PROOF. In view of the previous proposition it suffices to show that Th(A) is not PC-compact. To see this consider the asserted program

$$\{\underline{\text{true}}\}\ R\ \{\underline{\text{false}}\}$$

with R: $z := S(x)$

$$\underline{\text{while}}\ z \neq x\ \underline{\text{do}}\ z := S(z)\ \underline{\text{od}}$$

Clearly $A \models \{\underline{\text{true}}\}\ R\ \{\underline{\text{false}}\}$; assume that $A \models \phi$ and $\phi \models \{\underline{\text{true}}\}\ R\ \{\underline{\text{false}}\}$. Using 2.1. (ii) ϕ has a model A^* in which a finite S-cycle exists. Choosing as an initial value of x some element in such a cycle one finds that $A' \not\models \{\underline{\text{true}}\}\ R\ \{\underline{\text{false}}\}$ thus contradicting the assumption on ϕ. It follows that A and $[N,A]$ do not meet condition I.

3.4. PROPOSITION. *If* T *is finitely axiomatizable then* T *is* PC*-compact.*

PROOF. Obvious.

3.5. PROPOSITION. Th([N,AO]) *is* PC*-compact.*

PROOF. From proposition 2.1. (iii) we obtain a sentence $\phi \in L(AO)$ which finitely axiomatizes Th(AO) i.e. for each $\psi \in L(AO)$, $\psi \in Th(AO) \iff \phi \vdash \psi$. So Th(AO) is PC-compact, a promising fact in view of 3.2. We will now use the rather accidental fact that there is an easy interpretation of $L(AO)$ in $L(N)$. Let $L(N) = (S, +, \cdot, <, 0)$ and $L(AO) = (S', <', 0')$ and use variables x_i for N and x_i' for AO. Omitting the superscripts yields a mapping $\Delta: L(AO) \to L(N)$. Now suppose that $[N,AO] \models \{p\}\ R\ \{q\}$; in several steps θ will be constructed such that $[N,AO] \models \theta$ and $\theta \models \{p\}\ R\ \{q\}$.

Step 1. Transform the asserted program $\{p\}\ R\ \{q\}$ to an equivalent one, $\{p^*\}\ R^*\ \{q^*\}$ by changing the free and bound variables in such a way that variables x_i ranging over N have even indices and variables x_i' ranging over AO will have odd indices. Observe:

$$[N,AO] \models \{p^*\}\ R^*\ \{q^*\}$$

and even

$$\{p^*\}\ R^*\ \{q^*\} \models \{p\}\ R\ \{q\}.$$

Step 2. The interpretation Δ can be extended to asserted programs. Write $\Delta(\{p^*\}\ R^*\ \{q^*\})$ for $\{\Delta(p^*)\}\ \Delta(R^*)\ \{\Delta(q^*)\}$; this is an asserted triple over $\Sigma(N)$ true in N. Because N is expressive, HL(N) is complete and N is PC-compact; so choose $\psi \in Th(N)$ with $\psi \models \Delta(\{p^*\}R^*\{q^*\})$ and put $\theta \equiv \psi \wedge \Delta(\phi) \wedge \phi$ (here ϕ is the sentence that axiomatises Th(AO)).

By construction $[N,AO] \models \theta$. In order to prove $\theta \models \{p\}\ R\ \{q\}$ it suffices to show $\theta \models \{p^*\}\ R^*\ \{q^*\}$. Suppose $[\overline{N},\overline{AO}]$ is some model of θ, then $\overline{N} \models \psi \wedge \Delta(\phi)$ and $\overline{AO} \models \phi$. Let Σ be the signature of AO and denote with $\overline{N}_\Sigma$ the Σ-reduct of $\overline{N}$. Because $\psi \models \Delta(\{p^*\}R^*\{q^*\})$, $\overline{N} \models \Delta(\{p^*\}R^*\{q^*\})$ and thus $[\overline{N},\overline{N}_\Sigma] \models \{p^*\}\ R^*\ \{q^*\}$ (this uses the fact that Δ will map AO-variables in $\{p^*\}\ R^*\ \{q^*\}$ to variables different from the N-variables occurring in it).

Because $\overline{N} \models \Delta(\phi)$, $\overline{N}_\Sigma \models \phi$ and consequently $\overline{N}_\Sigma$ and $\overline{AO}$ are elementary equivalent. Using the separation of variables lemma also $[\overline{N},\overline{N}_\Sigma]$ and $[\overline{N},\overline{AO}]$ are elementary equivalent. Consequently $PC([\overline{N},\overline{N}_\Sigma]) = PC([\overline{N},\overline{AO}])$ and a fortiori $\{p^*\}\ R^*\ \{q^*\} \in PC([\overline{N},\overline{AO}])$ which had to be shown.

3.6. PROPOSITION. *There is a sound logic* L_Σ, *with* Σ *the signature of* [N,AO], *such that* $L_\Sigma([N,AO])$ *proves all asserted programs true in* [N,AO]. *(I.e.* $L_\Sigma([N,AO])$ *is complete).*

PROOF. Using definitions and notations from the preceding proof we can explicitly define L_Σ as follow:

$$L_\Sigma = \{(\psi \wedge \Delta(\phi) \wedge \phi, \{p\}R\{q\}) \mid HL_\Sigma(\psi) \vdash \Delta(\{p^*\}R^*\{q^*\})\}.$$

The completeness as well as soundness are now an immediate corollary to the previous proof.

3.7. PROPOSITION. HL([N,AO]) *is incomplete.*

PROOF. Let $\underline{n} = S^n(\underline{0})$, $\underline{n} = S'^n(\underline{0}')$ where again we use superscripts to distinguish the symbols of $\Sigma(AO)$ from those in $\Sigma(N)$. The diagonal of [N,AO] is the set $\{(\underline{n},\underline{n}') \mid n \in \omega\}$. Using the separation of variables lemma one finds that the diagonal is not definable in [N,AO].

Let x_1, x_2 be variables for N and y_1, y_2 be variables for AO. Consider the following programs R_1 and R_2.

R_1:

$x_2 := \underline{0}$
$y_1 := \underline{0}'$
$y_2 := \underline{0}$
while $x_2 \neq x_1$
do $x_2 := S(x_2)$
$y_2 := S'(y_2)$
od
$x_1 := \underline{0}$

R_2:

$x_2 := \underline{0}$
$y_1 := \underline{0}$
while $y_2 \neq y_1$
do $y_1 := S'(y_1)$
$x_1 := S(x_1)$
od

It follows that $[N,AO] \models \{\underline{true}\}R_1;R_2\{x_1 = x_2 \wedge y_1 = y_2\}$. In order to prove this fact in HL([N,AO]) we need an intermediate assertion between R_1 and R_2 equivalent to the predicate

$$x_1 = 0 \wedge y_1 = 0 \wedge \exists n(x_2 = \underline{n} \wedge y_2 = \underline{n}').$$

Definability of this predicate entails definability of the diagonal in [N,AO] thus leading to a contradiction.

4. CONCLUDING REMARKS AND OPEN QUESTIONS

We have shown that for some fixed datatype A, HL(A) is incomplete but nevertheless a sound and complete proof system $L_\Sigma(A)$ can be found. Searching for a complete special purpose logic in this fashion competes with more rigorous options like adding extra functions or relations in order to obtain an expressive structure, or with adding second order features to assertion language or proof system.

Various problems remains unsettled, we mention four of these:

(i) Let PRA = $(\omega,S,+,0)$. Is Th([N,PRA]) PC-compact?

(ii) If A satisfies conditions I and II, does there exists a sound logic L_Σ with $L_\Sigma(A)$ complete?

(iii) If A is computable and HL(A) is complete, must A be expressive?

(iv) Let K be the class of all Σ-structures A for which there exists a sound and complete $L_\Sigma(A)$. Can one find a single logic L_Σ which is uniformly complete for all $A \in K$? (If so this would be <u>the</u> logic of partial correctness for Σ).

REFERENCES

[1] BERGSTRA, J.A., A. CHMIELIENSKA & J. TIURYN, *Hoare's logic is incomplete when it does not have to be,* in Logics of Programs Ed. D. Kozen Spr. L.N.C.S. 131 (1981), 9-23.

[2] BERGSTRA, J.A. & J.V. TUCKER, *Hoare's logic for programming languages with two datatypes,* Math. Centre Department of Computer Science Technical Report IW 207 Amsterdam 1982.

[3] BERGSTRA, J.A. & J.V. TUCKER, *Expressiveness and the completeness of Hoare's logic*, JCSS, vol. 25, Nr. 3 (1983), p. 267-284.

[4] CHANG, C.C. & H.J. KEISLER, *Model Theory*, North Holland, Studies in logic vol. 73.

[5] COOK, S.A., *Soundness and completeness of an axiom system for program verification*, SIAM J. Computing 7 (1978), 70-90.

[6] HOARE, C.A.R., *An axiomatic basis for computer programming*, Communications ACM 12 (1967), 567-580.

[7] LAMBEK, J., *How to program an infinite abacus*, Canadian Mathematical Bulletin 4 (1961), 295-302.

[8] SHOENFIELD, J., *Mathematical logic*, Reading, Addison-Wesley (1967).

[9] WAND, M., *A new incompleteness result for Hoare's system*, J. Association Computing Machinary, 25 (1978), 168-175.