Publ. RIMS, Kyoto Univ.
17 (1981), 297-309

Arithmetical Completeness in First-Order Dynamic Logic for Concurrent Programs

By

Hirokazu NISHIMURA*

Abstract

We extend Harel's [4] arithmetical axiomatization $\boldsymbol{P}$ of regular first-order dynamic logic so as to include concurrent programs $\alpha /\!/ \beta$, and then establish its arithmetical completeness.

§ 1. Introduction

Following Floyd's [3] invariant assertion method, Hoare [4] provided a finitary axiom system for proving the partial correctness of simple sequential, iterative programs. Cook [2] introduced the notion of relative completeness as a certain kind of measure of the adequacy of such systems. Cook's approach was to add the valid formulas of the underlying assertion language to the system as axioms, and then to check whether in each universe of discourse for which the assertion language is expressive, the resulting axiom system can prove any true partial correctness assertion.

Among many approaches which followed Cook, it is Owicki's [7, 8] system for the partial correctness of concurrent programs and Harel's [4] first-order dynamic logic that are most relevant to this paper. Owicki extended Hoare's system to concurrent programs, while Harel extended Hoare's system so that programs themselves are syntactical entities and so we can express the equivalence of two apparently distinct programs formally.

In this paper we generalize Harel's system $\boldsymbol{P}$ to concurrent programs directly rather than incorporate Owicki's system into Harel's one. In our opinion, Owicki's system, though being popular and interesting, fails

Received May 12, 1980.
* Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606, Japan.

to understand concurrency in its most aesthetic and structured level. Among many axioms and inference rules of ***P***, the most central ones are (I*) and (C*), which deal with programs of the form α^* (i.e., iteration programs). Similarly, any worthwhile extension of ***P*** to concurrent programs must contain inference rules which deal with programs of the form $\alpha^*/\!/\beta$ (i.e., combination of iteration and concurrency) in a structured manner. However it is such rules that are almost lacking in Owicki's system.

After presenting the exact syntax and semantics for concurrent dynamic logic in Section 2, our axiomatization ***CP*** for concurrent dynamic logic is given in Section 3. The arithmetical soundness and completeness of ***CP*** will be established in Sections 4 and 5 repectively. Throughout this paper we assume the reader to be familiar with Harel [4].

§ 2. Concurrent Dynamic Logic

Roughly speaking, concurrent dynamic logic (CDL) can be obtained from regular first-order dynamic logic (DL) simply by admitting $\alpha/\!/\beta$ (*cobegin⋯coend*) to be also a program. Specifically we define by simultaneous induction the set CRG of *first-order concurrent regular programs* and the set of CDL-*wffs*:

(1) For any variable x and any term e, $x\leftarrow e$ is in CRG.

(2) For any program-free (see below) CDL-wff P, P? is in CRG.

(3) For any α and β in CRG, $(\alpha;\beta)$, $(\alpha\cup\beta)$, $(\alpha/\!/\beta)$ and α^* are also in CRG.

(4) Any atomic formula is a CDL-wff.

(5) For any CDL-wffs P and Q, α in CRG and variable x, $\neg P$, $(P\vee Q)$, $\exists xP$ and $\langle\alpha\rangle P$ are CDL-wffs.

A CDL-wff which contains no occurrence of a program in CRG is called *program-free*, a *first-order formula*, or simply an L-*wff*. Programs of the form indicated in (1) and (2) are called *indivisible programs*. We shall use most of the conventions of Harel (4) freely (e.g., $[\alpha]P$ for $\neg\langle\alpha\rangle\neg P$). CDL-wffs $P_0/\backslash\cdots/\backslash P_n$ and $P_0\vee\cdots\vee P_n$ are often

abbreviated to $\bigwedge_{i=0}^{n} P_i$ and $\bigvee_{i=0}^{n} P_i$ respectively.

Let N be the set of all nonnegative integers. We define a function φ from $N\times N$ to N as follows:

$$\varphi(i, j) = \frac{(i+j+1)(i+j)}{2} + j \text{ for each } (i, j) \in N\times N.$$

We know well in elementary mathematics that φ is a one-to-one correspondence of $N\times N$ onto N and if $i+j<i'+j'$, then $\varphi(i, j) < \varphi(i', j')$. We denote by ψ and χ the functions from N to N satisfying the following conditions:

$$\varphi(\psi(i), \chi(i)) = i \quad \text{for any } i\in N.$$

We define a function d from CRG to N as follows:

(1) $d(\alpha) = 1$ for any indivisible program α.
(2) $d(\alpha; \beta) = d(\alpha \cup \beta) = 2(\max\{d(\alpha), d(\beta)\} + 1)$.
(3) $d(\alpha^*) = d(\alpha) + 1$.
(4) $d(\alpha /\!/ \beta) = \varphi(d(\alpha), d(\beta)) + 1$.

We denote by θ the program $(\forall x(x=x))?$ (a program for "do nothings"). We define two functions init and rest from $N\times$CRG to CRG as follows:

(0) $\text{init}(0, \alpha) = \theta$ and $\text{rest}(0, \alpha) = \alpha$ for any $\alpha\in$CRG.
(1) $\text{init}(i+1, \alpha) = \alpha$ and $\text{rest}(i+1, \alpha) = \theta$ for any indivisible program α.
(2a) $\text{init}(2i+1, \alpha; \beta) = \text{init}(i, \alpha)$ and
$\text{rest}(2i+1, \alpha; \beta) = \text{rest}(i, \alpha); \beta$.
(2b) $\text{init}(2(i+1), \alpha; \beta) = \alpha; \text{init}(i, \beta)$ and
$\text{rest}(2(i+1), \alpha; \beta) = \text{rest}(i, \beta)$.
(3a) $\text{init}(2i+1, \alpha \cup \beta) = \text{init}(i, \alpha)$ and
$\text{rest}(2i+1, \alpha \cup \beta) = \text{rest}(i, \alpha)$.
(3b) $\text{init}(2(i+1), \alpha \cup \beta) = \text{init}(i, \beta)$ and
$\text{rest}(2(i+1), \alpha \cup \beta) = \text{rest}(i, \beta)$.

(4) $\mathrm{init}(i+1, \alpha /\!/ \beta) = \mathrm{init}(\psi(i), \alpha) /\!/ \mathrm{init}(\chi(i), \beta)$ and
$\mathrm{rest}(i+1, \alpha /\!/ \beta) = \mathrm{rest}(\psi(i), \alpha) /\!/ \mathrm{rest}(\chi(i), \beta)$.

(5) $\mathrm{init}(i+1, \alpha^*) = \alpha^*; \mathrm{init}(i, \alpha)$ and
$\mathrm{rest}(i+1, \alpha^*) = \mathrm{rest}(i, \alpha) ; \alpha^*$.

Our notations φ, ψ, χ, d, init and rest are slightly modified versions of Nishimura's [6] J_2, $(\ )_1$, $(\ )_2$, lw, comp and lete respectively. We define the rest-*closure* of a program α in CRG, written rest-cl(α), as the set

$$\{\mathrm{rest}(i, \alpha) \mid 0 \leq i \leq \mathrm{d}(\alpha)\}.$$

The following proposition justifies the name.

Proposition 2. 1. *For any* $\alpha \in$ CRG, *any* $\beta \in$ rest-cl(α) *and any* $i \in \boldsymbol{N}$, *we have* $\mathrm{rest}(i, \beta) \in$ rest-cl(α). *I.e.,* rest-cl(α) *is closed with respect to the operation* rest.

Proof. By induction on the construction of α.

Some examples of rest-cl(α) may be helpful to the reader.

(1) rest-cl$(\alpha) = \{\alpha, \theta\}$.
(2) rest-cl$(\alpha; \beta) = \{\alpha; \beta, \theta; \beta, \beta, \theta\}$.
(3) rest-cl$(\alpha /\!/ \beta) = \{\alpha /\!/ \beta, \theta /\!/ \beta, \alpha /\!/ \theta, \theta /\!/ \theta\}$.

In the above examples, α and β are assumed to be indivisible.

We now turn our attention to semantics. In the rest of this paper, an arithmetical universe A shall be fixed. An ordered pair (I, J) of states I and J in A is called a *move*. A finite sequence $(I_1, J_1) \cdots (I_n, J_n)$ of moves is called a *path*, while I_1 and J_n are called the *initial* and *final states* of the path respectively. The number n is called the *length* of the path. We denote by H(A) the set of all paths. For any $h \in H(A)$, we denote the initial state, final state and the lenght of h by is(h), fs(h) and lh(h) respectively. A path $(I_1, J_1) \cdots (I_n, J_n)$ is called *legal* if $J_i = I_{i+1}$ for any $1 \leq i \leq n-1$. We denote by $H_r(A)$ the set of all legal paths. Given two subsets S and T of H(A), we define:

(1) S; T is the set of all concatenations of $h_1 \in S$ and $h_2 \in T$.

(2) S^* is the least subset of H(A) which contains S and $\{(I, I) \mid I \in A\}$ and which is closed under concatenation.

(3) $S /\!/ T$ is the set of all interleaving sequences of $h_1 \in S$ and $h_2 \in T$.

We now define a subset $\rho(\alpha) \subseteq H(A)$ for each $\alpha \in CRG$ and a relation $I \models P$ between $I \in A$ and a CDL-wff P by simultaneous induction.

(1) For any variable x and term e,
$\rho(x \leftarrow e) = \{(I, J) \mid J = [e_I/x]I\}$.

(2) For any program-free CDL-wff P,
$\rho(P?) = \{(I, I) \mid I \models P\}$.

(3) For any α and β in CRG,
$\rho(\alpha; \beta) = \rho(\alpha) ; \rho(\beta)$,
$\rho(\alpha \cup \beta) = \rho(\alpha) \cup \rho(\beta)$,
$\rho(\alpha^*) = (\rho(\alpha))^*$, and
$\rho(\alpha /\!/ \beta) = \rho(\alpha) /\!/ \rho(\beta)$.

(4) For any atomic fomula $p(e_1, \cdots, e_k)$,
$I \models p(e_1, \cdots, e_k)$ whenever $p_I(e_{1_I}, \cdots, e_{k_I})$ is true.

(5) For any CDL-wffs P and Q, α in CRG and variable x,
$I \models \neg P$ iff it is not the case that $I \models P$,
$I \models (P \vee Q)$ iff either $I \models P$ or $I \models Q$,
$I \models \exists x P$ iff there exists an element d in D_I such that $[d/x]I \models P$,
$I \models \langle\alpha\rangle P$ iff there exists a path $h \in \rho(\alpha)$ such that $is(h) = I$, h is legal and $fs(h) \models P$.

We say that a CDL-wff P is A-*valid*, notation: $\models_A P$, if for every $I \in A$, we have $I \models P$.

§ 3. Axiomatization of CDL

The main objective of this section is to present our formal system ***CP*** for CDL, which is an extension of Harel's [4] ***P*** for DL. First of all, we recall the formal system ***P***, which consists of the following axioms and inference rules:

Axioms:

(T) All tautologies of propositional calculus.

(←R) $[x \leftarrow e]P \equiv P^{e}_{x}$, where P is an L-wff.

(?R) $[Q?]P \equiv (Q \supset P)$.

(; R) $[\alpha; \beta]P \equiv [\alpha][\beta]P$.

($\cup$ R) $[\alpha \cup \beta]P \equiv ([\alpha]P \wedge [\beta]P)$.

Inference rules:

(MP) $\dfrac{P,\ P \supset Q}{Q}$

(G) $\dfrac{P \supset Q}{[\alpha]P \supset [\alpha]Q}$ and $\dfrac{P \supset Q}{\exists x P \supset \exists x Q}$

(I*) $\dfrac{R \supset P,\ P \supset [\alpha]P,\ P \supset Q}{R \supset [\alpha^*]Q}$

(C*) $\dfrac{R \supset \exists n P(n),\ P(n+1) \supset \langle\alpha\rangle P(n),\ P(0) \supset Q}{R \supset \langle\alpha^*\rangle Q}$, where P is an L-wff with free n such that $n \notin var(\alpha)$.

Rules (I*) and (C*) are called the rules of *invariance* and *convergence* respectively. Strictly speaking, rules (I*) and (C*) of this paper are introduced as derived ones in Harel [4], but we prefer to regard them as fundamental ones so as to stress the strong analogy between them and our new rules which are to be introduced soon.

Our formal system ***CP*** for CDL is obtained from ***P*** by adding the following axioms and inference rules:

Axioms:

(//R) $[\alpha // \beta]P \equiv \bigwedge_{i=0}^{d(\beta)} [\mathrm{init}(i, \beta)][\alpha][\mathrm{rest}(i, \beta)]P$, where α is an indivisible program.

(; CR) $[(\alpha; \beta) // \gamma]P \equiv \bigwedge\!\!\!/_{i=0}^{d(\gamma)} [\alpha // \mathrm{init}(i, \gamma)][\beta // \mathrm{rest}(i, \gamma)]P$.

($\cup$ CR) $[(\alpha \cup \beta) // \gamma]P \equiv ([\alpha // \gamma]P \wedge [\beta // \gamma]P)$.

(//CR) $[(\alpha // \beta) // \gamma]P \equiv [\alpha // (\beta // \gamma)]P$.

Inference rules:

(CI*) $\dfrac{R\supset P_{\beta},\ T_1,\ T_2}{R\supset[\alpha^*/\!/\beta]Q}$, where

(1) P_γ is a CDL-wff for each $\gamma\in$rest-cl(β),

(2) $T_1=\{P_\gamma\supset[\alpha/\!/\text{init}(i,\gamma)]P_{\text{rest}(i,\gamma)}\mid\gamma\in\text{rest-cl}(\beta)$ and $0\leq i\leq d(\gamma)\}$, and

(3) $T_2=\{P_\gamma\supset[\gamma]Q\mid\gamma\in\text{rest-cl}(\beta)\}$.

(CC*) $\dfrac{R\supset\exists nP_\beta(n),\ T_1,\ T_2}{R\supset\langle\alpha^*/\!/\beta\rangle Q}$, where

(1) P_γ is an L-wff with free n such that $n\notin var(\alpha^*/\!/\beta)$ for each $\gamma\in$rest-cl(β),

(2) $T_1=\{P_\gamma(n+1)\supset\bigvee_{i=0}^{d(\gamma)}\langle\alpha/\!/\text{init}(i,\gamma)\rangle P_{\text{rest}(i,\gamma)}(n)\mid$ $\gamma\in\text{rest-cl}(\beta)$ and $0\leq i\leq d(\gamma)\}$, and

(3) $T_2=\{P_\gamma(0)\supset\langle\gamma\rangle Q\mid\gamma\in\text{rest-cl}(\beta)\}$.

Axioms (/\!/R) and (;CR) are borrowed from Nishimura [6]. Rules (CI*) and (CC*) are called the rules of *concurrent invariance* and *concurrent convergence* respectively.

CP(A) is ***CP*** with the set $\{P\mid P$ is an L-wff and $\models_A P\}$ taken as additional axioms. A CDL-wff P is said to be *provable* in ***CP***(A), written $\vdash_{\boldsymbol{CP}(A)}P$, if there exists a finite sequences S of CDL-wffs, the last one being P, and such that each formula in S is an axiom or is obtained from previous formulas of S by one of the rules of inference.

§ 4. Soundness

The main purpose of this section is to establish the following theorem:

Theorem 4.1 (A-soundness of CP(A)). *For any* ***CD***L-*wff* P, *if* $\vdash_{\boldsymbol{CP}(A)}P$, *then* $\models_A P$.

Since the A-soundness of $\boldsymbol{P}(\mathrm{A})$ is already established in Harel (4) and it is rather straightforward to see that axioms ($/\!/\mathrm{R}$), ($;\mathrm{CR}$), ($\cup\mathrm{CR}$) and ($/\!/\mathrm{CR}$) are A-valid, it is sufficient to show that rules (CI*) and (CC*) preserve A-validity.

Lemma 4. 2. *For any* $\alpha, \beta \in \mathrm{CRG}$ *and any* CDL-*wffs* R, Q *and* $\mathrm{P}_\gamma(\gamma \in \text{rest-cl}(\beta))$, *if* $\models_{\mathrm{A}}(R \supset \mathrm{P}_\beta)$, $\models_{\mathrm{A}}(\mathrm{P}_\gamma \supset [\alpha /\!/ \text{init}(\mathrm{i}, \gamma)]\mathrm{P}_{\text{rest}(\mathrm{i},\gamma)})$ *for each* $0 \leq \mathrm{i} \leq \mathrm{d}(\gamma)$ *and* $\models_{\mathrm{A}}(\mathrm{P}_\gamma \supset [\gamma]\mathrm{Q})$, *then* $\models_{\mathrm{A}}(\mathrm{R} \supset [\alpha^* /\!/ \beta]\mathrm{Q})$.

Proof. It is sufficient to show that $\models_{\mathrm{A}}(R \supset [\alpha^n /\!/ \beta]\mathrm{Q})$ for any $\mathrm{n} \in \mathrm{N}$. It is easy to see that $[\alpha^n /\!/ \beta]\mathrm{Q}$ is equivalent to the conjunction of all formulas of the form

$$[\alpha /\!/ \lambda_1][\alpha /\!/ \lambda_2] \cdots [\alpha /\!/ \lambda_n][\lambda_{n+1}]\mathrm{Q},$$

where for some $\sigma_1, \cdots, \sigma_{n-1}$ in CRG and some $\mathrm{i}_1, \cdots, \mathrm{i}_n \in \boldsymbol{N}$ such that $0 \leq \mathrm{i}_1 \leq \mathrm{d}(\beta), 0 \leq \mathrm{i}_2 \leq \mathrm{d}(\sigma_1), \cdots, 0 \leq \mathrm{i}_n \leq \mathrm{d}(\sigma_{n-1})$,

(1) $\lambda_1 = \text{init}(\mathrm{i}_1, \beta)$ and $\sigma_1 = \text{rest}(\mathrm{i}_1, \beta)$;
(2) $\lambda_2 = \text{init}(\mathrm{i}_2, \sigma_1)$ and $\sigma_2 = \text{rest}(\mathrm{i}_2, \sigma_1)$;
$\vdots$
($\mathrm{n}-1$) $\lambda_{n-1} = \text{init}(\mathrm{i}_{n-1}, \sigma_{n-2})$ and $\sigma_{n-1} = \text{rest}(\mathrm{i}_{n-1}, \sigma_{n-2})$;
(n) $\lambda_n = \text{init}(\mathrm{i}_n, \sigma_{n-1})$ and $\lambda_{n+1} = \text{rest}(\mathrm{i}_n, \sigma_{n-1})$.

Since $\models_{\mathrm{A}}(\mathrm{R} \supset \mathrm{P}_\beta)$, $\models_{\mathrm{A}}(\mathrm{P}_\beta \supset [\alpha /\!/ \lambda_1]\mathrm{P}_{\sigma_1})$, $\models_{\mathrm{A}}(\mathrm{P}_{\sigma_i} \supset [\alpha /\!/ \lambda_{i+1}]\mathrm{P}_{\sigma_{i+1}})$ $(1 \leq \mathrm{i} \leq \mathrm{n}-2)$, $\models_{\mathrm{A}}(\mathrm{P}_{\sigma_{n-1}} \supset [\alpha /\!/ \lambda_n]\mathrm{P}_{\lambda_{n+1}})$ and $\models_{\mathrm{A}}(\mathrm{P}_{\lambda_{n+1}} \supset [\lambda_{n+1}]\mathrm{Q})$ by assumption, $\models_{\mathrm{A}}(\mathrm{R} \supset [\alpha /\!/ \lambda_1][\alpha /\!/ \lambda_2] \cdots [\alpha /\!/ \lambda_n][\alpha /\!/ \lambda_{n+1}]\mathrm{Q})$. Thus the desired conclusion follows readily.

Lemma 4. 3. *For any* $\alpha, \beta \in \mathrm{CRG}$, *any* CDL-*wffs* R *and* Q, *and any* L-*wffs* P_γ $(\gamma \in \text{rest-cl}(\beta))$ with free $\mathrm{n} \notin var(\alpha^* /\!/ \beta)$, *if* $\models_{\mathrm{A}}(\mathrm{R} \supset \exists \mathrm{n} \mathrm{P}_\beta(\mathrm{n}))$, $\models_{\mathrm{A}}(\mathrm{P}_\gamma(\mathrm{n}+1) \supset \bigvee_{\mathrm{i}=0}^{\mathrm{d}(\gamma)} \langle \alpha /\!/ \text{init}(\mathrm{i}, \gamma) \rangle \mathrm{P}_{\text{rest}(\mathrm{i},\gamma)}(\mathrm{n}))$ *and* $\models_{\mathrm{A}}(\mathrm{P}_\gamma(0) \supset \langle \gamma \rangle \mathrm{Q})$, *then* $\models_{\mathrm{A}}(\mathrm{R} \supset \langle \alpha^* /\!/ \beta \rangle \mathrm{Q})$.

Proof. Similar to that of Lemma 4. 2.

§ 5. Completeness

The main purpose of this section is to establish the arithmetical completeness of ***CP***. Owing to Theorem 3.1 of Harel [4], it is sufficient to show that:

(C1) L is A-expressive for CDL. I.e., for any CDL-wff P, there exists an L-wff Q such that $\models_A P \equiv Q$.

(C2) The following inference rule has to be derivable in ***CP***(A):

$$\frac{R \supset Q}{\langle\alpha\rangle R \supset \langle\alpha\rangle Q}$$

(C3) We can prove completeness for formulas of the simple forms $R \supset [\alpha]Q$ and $R \supset \langle\alpha\rangle Q$ with L-wffs R and Q.

Theorem 5.1. *For any arithmetical universe* A, L *is* A*-expressive for* CDL.

Proof. This follows from the closure of regular sets under shuffling and the A-expressiveness of L for DL established in Theorem 3.2 of Harel [4].

Corollary 5.2. *For any* CDL*-wff of the form* $\langle\alpha^*\rangle Q$, *there exists an* L*-wff* P(n) *with free* $n \notin var(\alpha)$ *such that* $\models_A \forall n(\langle\alpha^n\rangle Q \equiv P(n))$.

Corollary 5.3. *For any* CDL*-wffs of the form* $\langle\alpha^* /\!/ \beta\rangle Q$, *there exists an* L*-wff* P(n) *with free* $n \notin var(\alpha^* /\!/ \beta)$ *such that* $\models_A \forall n(\langle\alpha^n /\!/ \beta\rangle Q \equiv P(n))$.

The following two lemmas are borrowed form Harel [4].

Lemma 5.4. The following is a derived rule of ***CP***.

$$\frac{P \supset Q}{\langle\alpha\rangle P \supset \langle\alpha\rangle Q}$$

Lemma 5.5 (Invariance Lemma). *For any* CDL-*wff of the form* $R \supset [\alpha^*]Q$, *if* $\models_A (R \supset [\alpha^*]Q)$, *then there exists an* L-*wff* P *such that* $\models_A (R \supset P)$, $\models_A (P \supset [\alpha]P)$ *and* $\models_A (P \supset Q)$.

The following lemma is the concurrent analog of Lemma 5.6.

Lemma 5.6 (Concurrent Invariance Lemma). *For any* CDL-*wff of the form* $R \supset [\alpha^* /\!/ \beta]Q$, *if* $\models_A (R \supset [\alpha^* /\!/ \beta]Q)$, *then there exists an* L-*wff* P_γ *for each* $\gamma \in \text{rest-cl}(\beta)$ *such that* $\models_A (R \supset P_\beta)$, $\models_A (P_\gamma \supset [\alpha /\!/ \text{init}(i, \gamma)]P_{\text{rest}(i,\gamma)})$ *for each* $0 \leq i \leq d(\gamma)$ *and* $\models_A (P_\gamma \supset [\gamma]Q)$.

Proof. By Theorem 4.1, there exists an L-wff P_γ for each $\gamma \in \text{rest-cl}(\beta)$ such that $\models_A (P_\gamma \equiv [\alpha^* /\!/ \gamma]Q)$. Since $\models_A (R \supset [\alpha^* /\!/ \beta]Q)$ and $\models_A (P_\beta \equiv [\alpha^* /\!/ \beta]Q)$, we have $\models_A (R \supset P_\beta)$. It is easy to see that $\models_A ([\alpha^* /\!/ \gamma]Q \supset [\alpha /\!/ \text{init}(i, \gamma)][\alpha^* /\!/ \text{rest}(i, \gamma)]Q)$ for each $0 \leq i \leq d(\gamma)$. Since $\models_A (P_\gamma \equiv [\alpha^* /\!/ \gamma]Q)$ and $\models_A (P_{\text{rest}(i,\gamma)} \equiv [\alpha^* /\!/ \text{rest}(i, \gamma)]Q)$, $\models_A (P_\gamma \supset [\alpha /\!/ \text{init}(i, \gamma)]P_{\text{rest}(i,\gamma)})$. It is easy to see that $\models_A ([\alpha^* /\!/ \gamma]Q \supset [\gamma]Q)$. Since $\models_A (P_\gamma \equiv [\alpha^* /\!/ \gamma]Q)$, we have $\models_A (P_\gamma \supset [\gamma]Q)$. This completes the proof.

We define two functions ω_1 and ω_2 from CRG to $\boldsymbol{N}$ as follows:

(1) $\omega_1(\alpha) = 1$ for any indivisible program α.
(2) $\omega_1(\alpha; \beta) = \omega_1(\alpha \cup \beta) = \omega_1(\alpha) + \omega_1(\beta) + 1$.
(3) $\omega_1(\alpha^*) = \omega_1(\alpha /\!/ \beta) = \omega_1(\alpha) + 1$.
(4) $\omega_2(\alpha) = 0$ for any indivisible program α.
(5) $\omega_2(\alpha; \beta) = \omega_2(\alpha \cup \beta) = \max\{\omega_2(\alpha), \omega_2(\beta)\}$.
(6) $\omega_2(\alpha^*) = \omega_2(\alpha)$.
(7) $\omega_2(\alpha /\!/ \beta) = \omega_2(\alpha) + \omega_2(\beta) + 1$.

We denote by $<$ the usual lexicographic order on $\boldsymbol{N} \times \boldsymbol{N}$. I.e., for any $(i_1, i_2), (j_1, j_2) \in \boldsymbol{N} \times \boldsymbol{N}$, $(i_1, i_2) < (j_1, j_2)$ iff one of the following conditions holds:

(1) $i_2 < j_2$.
(2) $i_2 = j_2$ and $i_1 < j_1$.

We decree that $\Omega(\alpha) = (\omega_1(\alpha), \omega_2(\alpha))$ for any $\alpha \in$ CRG. To establish the box-completeness and diamond-completeness, we need the following lemma.

Lemma 5.7.

(1) $\Omega(\alpha) < \Omega(\alpha; \beta)$ *and* $\Omega(\beta) < \Omega(\alpha; \beta)$.

(2) $\Omega(\alpha) < \Omega(\alpha \cup \beta)$ *and* $\Omega(\beta) < \Omega(\alpha \cup \beta)$.

(3) $\Omega(\alpha) < \Omega(\alpha^*)$.

(4) $\Omega(\alpha) < \Omega(\alpha /\!/ \beta)$, $\Omega(\text{init}(\text{i}, \beta)) < \Omega(\alpha /\!/ \beta)$ *and* $\Omega(\text{rest}(\text{i}, \beta)) < \Omega(\alpha /\!/ \beta)$ *for any* $\text{i} \in \mathbf{N}$.

(5) $\Omega(\alpha /\!/ \text{init}(\text{i}, \gamma)) < \Omega((\alpha; \beta) /\!/ \gamma)$ *and* $\Omega(\beta /\!/ \text{rest}(\text{i}, \gamma)) < \Omega((\alpha; \beta) /\!/ \gamma)$ *for any* $\text{i} \in \mathbf{N}$.

(6) $\Omega(\alpha /\!/ \gamma) < \Omega((\alpha \cup \beta) /\!/ \gamma)$ *and* $\Omega(\beta /\!/ \gamma) < \Omega((\alpha \cup \beta) /\!/ \gamma)$.

(7) $\Omega(\alpha /\!/ \text{init}(\text{i}, \gamma)) < \Omega(\alpha^* /\!/ \beta)$ *and* $\Omega(\gamma) < \Omega(\alpha^* /\!/ \beta)$ *for any* $\gamma \in \text{rest-cl}(\beta)$ *and any* $0 \leq \text{i} \leq \text{d}(\gamma)$.

(8) $\Omega(\alpha /\!/ (\beta /\!/ \gamma)) < \Omega((\alpha /\!/ \beta) /\!/ \gamma)$.

The above lemma follows immediately from a simple inspection and the following lemma.

Lemma 5.8. *For any* $\alpha \in$ CRG *and any* $\text{i} \in \mathbf{N}$, $\omega_2(\text{init}(\text{i}, \alpha)) \leq \omega_2(\alpha)$ *and* $\omega_2(\text{rest}(\text{i}, \alpha)) \leq \omega_2(\alpha)$.

Proof. By induction on the construction of α.

Now we are ready to establish the box-completeness theorem for $\boldsymbol{CP}(\text{A})$.

Theorem 5.9 (Box-completeness Theorem). *For any* $\alpha \in$ CRG *and any* L-*wffs* R *and* Q, *if* $\models_{\text{A}} (\text{R} \supset [\alpha]\text{Q})$, *then* $\vdash_{\overline{\boldsymbol{CP}(\text{A})}} (\text{R} \supset [\alpha]\text{Q})$.

Proof. We proceed by induction on $\Omega(\alpha)$. Since the proof is similar to that of Theorem 3.9 of Harel [4], we deal only with the case that α is of the form $\beta^* /\!/ \gamma$, leaving other cases to the reader. By Lemma 5.6, there exists an L-wff P_δ for each $\delta \in \text{rest-cl}(\gamma)$ such that

$\models_A(R \supset P_\gamma)$, $\models_A(P_\delta \supset [\beta /\!/ \text{init}(i, \delta)]P_{\text{rest}(i,\delta)})$ for each $0 \leq i \leq d(\delta)$ and $\models_A(P_\delta \supset [\delta]Q)$. By Lemma 5.7, we can apply induction hypothesis to these formulas, so that $\vdash_{\overline{CP(A)}}(R \supset P_\gamma)$, $\vdash_{\overline{CP(A)}}(P_\delta \supset [\beta /\!/ \text{init}(i, \delta)]P_{\text{rest}(i,\delta)})$ and $\vdash_{\overline{CP(A)}}(P_\delta \supset [\delta]Q)$ for each $\delta \in \text{rest-cl}(\gamma)$ and each $0 \leq i \leq d(\delta)$. Hence by rule (CI*), we have $\vdash_{\overline{CP(A)}}(R \supset [\alpha]Q)$.

The following lemma is borrowed from Harel [4].

Lemma 5.10 (Convergence Lemma). *For every* CDL-*wff of the form* $R \supset \langle \alpha^* \rangle Q$, *if* $\models_A(R \supset \langle \alpha^* \rangle Q)$, *then there exists an* L-*wff* $P(n)$ *with free* $n \notin var(\alpha)$, *such that* $\models_A(R \supset \exists n P(n))$, $\models_A(P(n+1) \supset \langle \alpha \rangle P(n))$ *and* $\models_A(P(0) \supset Q)$.

The following lemma is the concurrent analog of Lemma 5.10.

Lemma 5.11 (Concurrent Convergence Lemma). *For every* CDL-*wff of the form* $R \supset \langle \alpha^* /\!/ \beta \rangle Q$, *if* $\models_A(R \supset \langle \alpha^* /\!/ \beta \rangle Q)$, *then there exists an* L-*wff* $P_\gamma(n)$ *with free* $n \notin var(\alpha^* /\!/ \beta)$ *for each* $\gamma \in \text{rest-cl}(\beta)$, *such that* $\models_A(R \supset \exists n P_\beta(n))$, $\models_A(P_\gamma(n+1) \supset \bigvee_{i=0}^{d(\gamma)} \langle \alpha /\!/ \text{init}(i, \gamma) \rangle P_{\text{rest}(i,\gamma)}(n))$ and $\models_A(P_\gamma(0) \supset \langle \gamma \rangle Q)$ *for each* $\gamma \in \text{rest-cl}(\beta)$.

Proof. By Corollary 5.3, there exists an L-wff $P_\gamma(n)$ with free $n \notin var(\alpha^* /\!/ \beta)$ for each $\gamma \in \text{rest-cl}(\beta)$ such that $\models_A \forall n(P_\gamma(n) \equiv \langle \alpha /\!/ \gamma \rangle Q)$. Since $\models_A(R \supset \langle \alpha^* /\!/ \beta \rangle Q)$ by assumption, $\models_A(R \supset \exists n P_\beta(n))$. Similarly, it is easy to see that the other A-validities hold too.

Theorem 5.12 (Diamond-Completeness Theorem). *For any* $\alpha \in$ CRG *and any* L-*wffs* R *and* Q, *if* $\models_A(R \supset \langle \alpha \rangle Q)$, *then* $\vdash_{\overline{CP(A)}}(R \supset \langle \alpha \rangle Q)$.

Proof. Similar to that of Theorem 5.9.

Thus we have just established the following.

Theorem 5.13 (Arithmetical Soundness and Completeness for CDL). *For any* CDL-*wff* P, $\models_A P$ *iff* $\vdash_{\overline{CP(A)}} P$.

References

[1] Abrahamson, K., Modal logic of concurrent nondeterministic programs, *Semantics of concurrent computation, Lecture Notes in Computer Science*, **70**, Springer, Berlin-Heidelberg-New York. 1979, 21-33.

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

[3] Floyd, R. W., Assigning meaning to programs, Schwartz, J. T., ed., *Mathematical Aspects of Computer Science*, American Math. Soc., Providence, R. I., 1967.

[4] Harel, D., *First-order dynamic logic, Lecture Notes in Computer Science*, **68**, Springer, Berlin-Heidelberg-New York, 1979.

[5] Hoare, C. A. R., An axiomatic basis for computer programming, *Comm. of the ACM*, **12** (1969), 576-580.

[6] Nishimura, T., Formalization of concurrent processes, Gilchrist, B. ed., *Information Processing 77*, North-Holland, Amsterdam, 1977.

[7] Owicki, S., A consistent and complete deductive system for the verification of parallel programs, *Proc. 8th Ann. ACM Symp. on Theory of Computing*, 1976.

[8] Owicki, S. and Gries, D., An axiomatic proof technique for parallel programs I. *Acta Informatica*, **6** (1976), 319-340.

[9] Shoenfield, J. R., *Mathematical logic*, Addison-Wesley, Massachussetts, 1967.