数理解析研究所講究録
458巻 1982年 103-112

非決定性プログラムの全面的正当性

名大 工　村上 昌己　稲垣 康善
豊橋技科大　本多 波雄

1 まえがき　並行プログラムの正当性の検証システムとしては，Hoare流の公理系の拡張や，並行プログラムを一種の非決定性プログラムとみなして議論する方法が報告されている．後者の方法では並行プログラムの様々な性質がそれに対応する非決定性プログラムの性質として記述，証明できることが必要である．本報告では，並行プログラムの全面的正当性に対応する非決定性プログラムの性質である，D-全面的正当性について，記述，証明できるような体系を2通り提案する．これらの体系はいずれもHarel[1](1979)が提案した非決定性プログラムの証明体系であるDynamic Logic(DL)の拡張である．

2 Dynamic Logic(DL)　最初にHarelの提案したDLについて述べる．Harelは非決定プログラムを記述する言語として，正規プログラム(RG)を導入している．

2.1 RGのシンタックス

定義2.1　変数記号$x, y, \ldots$，関数記号$f, g, \ldots$からつくられる項ならびに変数xについて，$x \leftarrow t$の形の式を代入文という．また，述語記号$p, q, \ldots$からつくられる量記号なしの述語Pについて$P?$を判定文という．代入文と判定文を基本命令という．

定義2.2　基本命令の集合の上の正規表現を正規プログラム(RG)と呼ぶ．

2.2 RGのセマンティクス(1)

プログラムのセマンティクスを記述するために，状態の概念を導入する．状態とは各論理式に対して，その真偽を決定する情報をもつものと考えられる．

定義2.3　空でない領域Dが指定されているものとする．このとき状態iは，各関数，述語，定数のDでの解釈および，変数のD上での値からなる．

定義2.4　ユニバースUは全状態の集合である．ここではUに含まれるすべてのiについて各関数，述語，定数の解釈は同じであるものとする．

定義2.5　プログラムαに対してU上の二項関係$m(\alpha)$を次のように定義する．

i) $m(x \leftarrow t) = \{(i, j) \mid j$は，$i$でのtの値を$x$に代入して得られる状態.$\}$.

ii) $m(Q?) = \{(i, i) \mid i \models Q\}$.

iii) $m(\alpha \cup \beta) = m(\alpha) \cup m(\beta)$.

$m(\alpha\beta) = \{(i,j) \mid \exists k\, (i,k) \in m(\alpha) \wedge (k,j) \in m(\beta)\}$.

$m(\alpha^*) = \{(i,j) \mid (\exists n \geq 0)(\exists i_0, \cdots, i_n)(i_0 = i \wedge i_n = j \wedge n \geq \forall \ell > 0$

$((i_{\ell-1}, i_\ell) \in m(\alpha))\}$.

2.3 DL の論理式

定義 2.6 (シンタックス) DL の論理式を次のように定義する.

i) 述語記号 p と項 $\tau_1, \cdots, \tau_n$ から作られる素命題 $p(\tau_1, \cdots, \tau_n)$ は論理式である.

ii) P, Q が論理式, かつ α が RG, α を変数とするとき,

$\neg P$, $P \vee Q$, $\exists x P$, $[\alpha]P$ は論理式.

$\neg[\alpha]\neg P$ を $\langle\alpha\rangle P$ と略記する. その他 $\supset$, $\wedge$, $\forall$ 等の記号も通常のように使用する.

定義 2.7 (セマンティクス) DL の論理式の真偽は次のようにして決定される.

i) $p(\tau_1, \cdots, \tau_n)$ が素命題のとき

$i \Vdash p(\tau_1, \cdots, \tau_n) \Leftrightarrow$「$p(\tau_1, \cdots, \tau_n)$ の状態 i での解釈の結果が真」

ii) $\vee, \exists, \neg$ は通常どうりに解釈する.

iii) P が論理式, α が RG のとき.

$i \Vdash [\alpha]P \Leftrightarrow$「$\forall j\, (i,j) \in m(\alpha) \supset j \Vdash P$」

公理系 以上のセマンティクスのもとで完全かつ無矛盾な公理系が Harel[1] によって次のように与えられた.

公理系DL

公理　T) All tautologies of propositional calculus.

←R) $[x \leftarrow \tau]P \equiv P_x^\tau$　：Pは述語論理式

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

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

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

推論規則

MP) $\dfrac{P,\ P \supset Q}{Q}$　　G) $\dfrac{P \supset Q}{[\alpha]P \supset [\alpha]Q}$　　$\dfrac{P \supset Q}{\exists x P \supset \exists x Q}$

I*) $\dfrac{P \supset [\alpha]P}{P \supset [\alpha^*]P}$　　C*) $\dfrac{P(n+1) \supset \langle\alpha\rangle P(n)}{P(n) \supset \langle\alpha^*\rangle P(0)}$

2.4 RGのセマンティクス(2)

定義2.8　次のような形の系列$\langle \varepsilon, i_0\rangle\langle e_1, i_1\rangle \cdots \langle e_n, i_n\rangle$を計算履歴という．ただし，$e_k$は基本命令，$\varepsilon$は空な命令，$i_k$は状態で，$0<k\leq n$について$(i_{k-1}, i_k) \in m(e_k)$．

定義2.9　計算履歴u, vの連接uvを次のように定義する．

$u=\langle \varepsilon, i_0\rangle \cdots \langle e_n, i_n\rangle$　$v=\langle \varepsilon, i'_0\rangle\langle e'_1, i'_1\rangle \cdots \langle e'_m, i'_m\rangle$で$i_n=i'_0$のとき，

$uv=\langle \varepsilon, i_0\rangle \cdots \langle e_n, i_n\rangle\langle e'_1, i'_1\rangle \cdots \langle e'_m, i'_m\rangle$．

定義2.10　αをRG，$I(\subset U)$を状態の集合とするとき，計算履歴集合$H(\alpha, I)$を次のように定義する．

$H(x \leftarrow \tau, I) = \{\langle \varepsilon, i\rangle\langle \perp\rangle \mid i \in I \wedge \neg\exists j : (i,j) \in m(x \leftarrow \tau)\}$

$$\cup\{\langle\varepsilon,i\rangle\langle x\leftarrow\tau,i\rangle \mid (i,i')\in m(x\leftarrow\tau)\wedge i\in I\}\cup\{\langle\varepsilon,i\rangle \mid i\in I\}.$$

$$H(Q?,I)=\{\langle\varepsilon,i\rangle\langle\perp\rangle \mid i\in I\wedge i\not\models Q\}$$

$$\cup\{\langle\varepsilon,i\rangle\langle Q?,i\rangle \mid i\in I\wedge i\models Q\}\cup\{\langle\varepsilon,i\rangle \mid i\in I\}.$$

$$H(\alpha\cup\beta,I)=H(\alpha,I)\cup H(\beta,I).$$

$$H(\alpha\beta,I)=H(\alpha,I)H(\beta,\{j \mid i\in I,(i,j)\in m(\alpha)\})\cup H(\alpha,I).$$

$$H(\alpha^*,I)=H(\alpha^*,I)H(\alpha,U)\cup H(\alpha,I).$$

ここで，$H(\alpha,I)H(\beta,I)$は履歴の連接を集合の上に拡張したもの．$\langle\perp\rangle$は計算がそれ以上その方向に進めなくなったことを表わす記号である．

$H(\alpha,I)$はIに含まれる状態からαを実行したときにたどる履歴の集合を定義している．

<u>3 非決定性プログラムの全面的正当性</u>．Harel[1]は非決定性プログラムの全面的正当性の定義は，その実行方法に依存するとして，4種類の実行方法について入力条件Rと出力条件Qについての全面的正当性を次のように定義している．

<u>定義3.1</u>　$R\,G.\alpha$が計算の途中で先へ進めなくなる可能性があることを$fail\alpha$，計算が発散して停止しなくなる可能性があることを$loop\alpha$で表わすことにするとき，αが入力条件Rと出力条件Qについて，

1. D-全面的正当 $\Leftrightarrow R\supset(\langle\alpha\rangle true\wedge[\alpha]Q\wedge\neg loop\alpha\wedge\neg fail\alpha)$.
2. DT-全面的正当 $\Leftrightarrow R\supset(\langle\alpha\rangle true\wedge[\alpha]Q\wedge\neg loop\alpha)$.

3. B-全面的正当 $\Leftrightarrow R \supset (\langle\alpha\rangle true \wedge [\alpha]Q \wedge \neg fail\,\alpha)$.

4. BI-全面的正当 $\Leftrightarrow R \supset (\langle\alpha\rangle true \wedge [\alpha]Q)$.

Harel[1]はDLのひとつの拡張としてDT-全面的正当性を証明する体系DL^+を与えている．本稿では並行プログラムの全面的正当性に対応するD-全面的正当性についての証明体系を二通り与える．

3.1 DL^+. IL　D-全面的正当性の定義より「αがRとQについてD-全面的正当」=「αがRとQについてDT-全面的正当 $\wedge$ B-全面的正当」となる．ゆえにB-全面的正当性あるいは$\neg fail\,\alpha$を記述・証明する体系を導入しDL^+と合わせることによって，D-全面的正当性を証明する体系とすることができる．そこでまず，Harel[1]によって与えられたDL^+について述べる．DL^+の論理式はDLの論理式に以下の定義をつけ加えたものである．

定義3.2　αがRG，Pが論理式であるとき，$[\alpha]^+P$は論理式である．

定義3.3　$i \models [\alpha]^+P \Leftrightarrow$「$H(\alpha, i)$は有限集合 $\wedge$ $i \models [\alpha]P$」

$\neg[\alpha]^+\neg P$を$\langle\alpha\rangle^+P$と略記する．

文献1)にDL^+の完全かつ無矛盾な公理系が，DLの公理系に次の公理と推論規則をつけ加えることによって与えられている．

公理　$([]^+)\ [\alpha]^+P \equiv ([\alpha]P \wedge [\alpha]^+true)$.

$(\leftarrow^+R)\ [x \leftarrow \tau]^+true$　　$(?^+R)\ [Q?]^+true$

$(;^{+}R)[\alpha\beta]^{+}true \equiv [\alpha]^{+}[\beta]^{+}true$.

$(\cup^{+}R)[\alpha\cup\beta]^{+}true \equiv ([\alpha]^{+}true \wedge [\beta]^{+}true)$

推論規則 (C^{+*}) $\dfrac{P(n+1)\supset[\alpha]^{+}P(n) \qquad \neg P(0)}{P(n)\supset[\alpha^{*}]^{+}true}$

(I^{+*}) $\dfrac{P\supset\langle\alpha\rangle^{+}P}{P\supset\langle\alpha^{*}\rangle^{+}true}$.

DL^{+} の記法を導入すると入力条件 R と出力条件 Q についての D-全面的正当性は $R\supset([\alpha]^{+}Q\wedge\neg fail(\alpha))$ のように表わせる．$\neg fail\alpha$ を表現する論理として，本稿では新たに invariance logic (IL) を導入する．ILの論理式は，DLの論理式に次の定義をつけ加えたものである．

定義 3.4 α が RG，P が論理式のとき $\boxed{\alpha}P$ は論理式である．

定義 3.5 $i\models\boxed{\alpha}P \Leftrightarrow$「$H(\alpha,\{i\})\ni^{\forall}u$ について $Last(u)=\perp \vee Last(u)\models P$」

ただし $u=\langle\varepsilon,i\rangle\cdots\langle r,j\rangle$ のとき $Last(u)=j$.

$u=\langle\varepsilon,i\rangle\cdots\langle\perp\rangle$ のとき $Last(u)=\perp$.

$\neg fail\alpha$ は $\boxed{\alpha}P$ の表現を使えば次のように表わせる．α に含まれる命令を $r_1,r_2\cdots r_n$，停止に至ったことを halt で表わすと，

$$\neg fail\alpha \equiv \boxed{\alpha}\left(\bigvee_{i=1}^{n}\langle r\rangle true \vee halt\right).$$

ILの公理系として，DLの公理系に加えて次の公理を与える．

公理 I1) $\boxed{x\leftarrow\tau}P\equiv[x\leftarrow\tau]P\wedge P$ I1)' $\boxed{Q?}P\equiv[Q?]P\wedge P$

I2) $\boxed{\alpha\cup\beta}P\equiv\boxed{\alpha}P\wedge\boxed{\beta}P$

I3) $[\alpha\beta]P \equiv [\alpha]P \wedge [\alpha][\beta]P$

I4) $[\alpha^*]P \equiv [\alpha^*][\alpha]P$

以上の公理系について次の結果を得る.

定理 IL は完全かつ無矛盾である.

3.3 DL^I 以下では, D-全面的正当性をより直接的に記述・証明する体系 DL^I を提案する. DL^I の論理式の定義は, DL の論理式に次の定義をつけ加えることによって得られる.

定義 3.6 α を RG, P を論理式とするとき, $\langle\langle\alpha\rangle\rangle P$ は論理式である.

定義 3.7 $i \models \langle\langle\alpha\rangle\rangle P \Leftrightarrow$「$H(\alpha, fi3)$ が有限集合で, $\forall u \in H(\alpha, fi3)$ について, $u = u'\langle 1\rangle$ ならば $\exists u'\{u'u'' \in H(\alpha, fi3) \wedge (i, \mathcal{L}ast(u')) \in m(\alpha)\}$, かつ $(i, \mathcal{L}ast(u)) \in m(\alpha)$ ならば $\mathcal{L}ast(u) \models P$」.

$\neg\langle\langle\alpha\rangle\rangle\neg P$ を $[\![\alpha]\!]P$ と略記する.

この記法を使うと, α の入力条件 Q と出力条件 R についての D-全面的正当性は, $Q \supset \langle\langle\alpha\rangle\rangle R$ のように表現できる.

DL^I の公理系は DL の公理系に以下の公理および推論規則を加えることにより得られる.

公理 D1) $\langle\langle x \leftarrow \tau\rangle\rangle P(x) \equiv P(\tau) \wedge \langle x \leftarrow \tau\rangle true$ D2) $\langle\langle Q?\rangle\rangle P(x) \equiv P(x) \wedge Q$

DU1) $[\![\alpha]\!]P \vee [\![\beta]\!]P \supset [\![\alpha \cup \beta]\!]P$ D;1) $\langle\langle\alpha\rangle\rangle\langle\langle\beta\rangle\rangle P \supset \langle\langle\alpha\beta\rangle\rangle P$

D;2) α がプレフィクスフリーな正規表現のとき.

$\langle\langle\alpha\beta\rangle\rangle P \supset \langle\langle\alpha\rangle\rangle\langle\langle\beta\rangle\rangle P$

D《》) $[\alpha]P \wedge \langle\langle\alpha\rangle\rangle true \equiv \langle\langle\alpha\rangle\rangle P$

推論規則 DU2) $\dfrac{Q \supset \langle\langle\alpha\rangle\rangle P \quad R \supset \langle\langle\beta\rangle\rangle P \quad Q \wedge \neg R \supset Ne(\beta) \quad R \wedge \neg Q \supset Ne(\alpha)}{(Q \vee R) \supset \langle\langle\alpha \cup \beta\rangle\rangle P}$

D*;) $\dfrac{\langle\langle\alpha^*\rangle\rangle true \quad P \supset \langle\langle\alpha\rangle\rangle((P \wedge Ne(\beta)) \vee \langle\langle\beta\rangle\rangle true)}{P \supset \langle\langle\alpha^*\beta\rangle\rangle true}$

D*ε) $P \supset Ne(\alpha) \Rightarrow P \supset \langle\langle\alpha^*\rangle\rangle P$

D*2) $\dfrac{P(n+1) \supset \langle\langle\alpha\rangle\rangle P(n) \quad P(0) \supset Ne(\alpha)}{P(n) \supset \langle\langle\alpha^*\rangle\rangle true}$

Dc) i) $\dfrac{\langle\langle\alpha\rangle\rangle Q \quad Q \supset P}{\langle\langle\alpha\rangle\rangle P}$ ii) $\dfrac{[\![\alpha]\!] Q \quad Q \supset P}{[\![\alpha]\!] P}$

iii) $\dfrac{P \supset Q \quad Q \supset \langle\langle\alpha\rangle\rangle R}{P \supset \langle\langle\alpha\rangle\rangle R}$ iv) $\dfrac{P \supset Q \quad Q \supset [\![\alpha]\!] R}{P \supset [\![\alpha]\!] R}$

ただし $Ne(\alpha)$ は α の実行が開始できないことを表わす述語で，形式的には次のようにして得られる．RG α の最初に実行されうる命令を $e_1, e_2, \cdots, e_n$ とするとき，

$$Ne(\alpha) \equiv \bigwedge_{i=1}^{n} [e_i] false$$

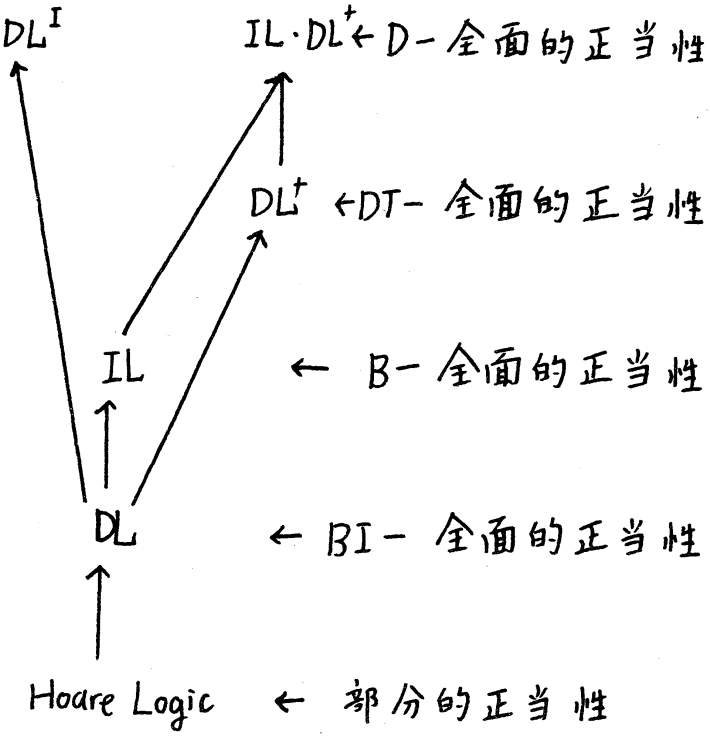
以上のような公理系について次のような結果を得る．

定理 DL^I は無矛盾である．

あとがき 本稿では非決定性プログラムの D-全面的正当性を，いずれも DL の拡張として二通り与えた．ここで扱った論理体系の互いの関係と，それらで記述・証明できる性質は次の

図に示すようになる．

最後に日頃，御指導頂く本学福村教授並びに御討論頂く研究室の皆様に感謝いたします．



参考文献

1) D. Harel "First-Order Dynamic Logic" Lecture Note in Computer Science 68 (1979)

2) S. Owicki and D. Gries "Verifying Properties of Parallel Program: An Axiomatic Approach" CACM 19,5 (1976) pp 279-284.

3) K. Apt "Recursive Assertions and Parallel Program" Acta Informatica 15 219-232 (1981).

4) L. Flon and N. Suzuki "The Total Correctness of Parallel Programs" SAIAM. J. COMPUT. Vol. 10 No 2. pp 227-246 (1981).

5) Z. Manna "Logic of Programs" Proc. of IFIP 80 (1980).

6) D. Harel "On the Total Correctness of Nondeterministic Programs" Theoret. Comput. Sci. 13,2 pp 175~192 (1981).