命令的指称语义在谓词域上的一种表示*)

丁志义[1,2] 李全德[2] 宋国新[1] 邵志清[1]

(华东理工大学计算机科学与工程系 上海 200237)[1] (宁夏大学数学计算机学院 银川 750021)[2]

摘 要 文中讨论了谓词转换器和状态转换器之间的对应关系,将谓词转换器作为命令的指称,刻画了 IMP 语言命令的指称语义,并证明与状态转换器形式的指称语义是等价的。

关键词 谓词转换器,状态转换器,指称语义

Description to the Denotational Semantics of IMP in Predicates Domain

DING Zhi-yi[1,2] LI Quan-de[2] SONG Guo-xin[1] SHAO Zhi-qing[1]

(Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China)[1]

(School of Mathematics and Computer Science, Ningxia University, Yinchuan 750021, China)[2]

Abstract The corresponding relation between predicate transformers and state transformers has been studied. We treat the imperative denotations as predicate transformers to specify the denotational semantics of programming language IMP, and predicate transformers semantics has been demonstrated to agree with state transformers semantics.

Keywords Predicate transformers, State transformers, Denotational semantics

1 引言

形式语义学的研究大致可分为 4 个分支:操作语义、指称语义、公理语义和代数语义。指称语义学以域论为核心,具有坚实的数学基础,被公认为标准的形式语义学,在域论的研究方面成果显著[1-3]。与此同时,形式语义学各分支的研究是相互融合的,不同的语义类型往往是高度依赖的。例如,正确地实现一个程序设计语言的主要依据是指称语义的描述,其次需要证明其操作语义与指称语义是一致的,这称之为完全抽象问题[4];另一方面,论证公理语义证明系统的正确性必须依靠基本的指称语义或操作语义。公理语义以程序逻辑为基础,Hoare 逻辑是经典的程序逻辑,利用最弱(宽容)前置条件(wp, weakest precondition; wlp, weakest liberal precondition)[5]可以证明 Hoare 逻辑的相对完备性[6]。最弱(宽容)前置条件以及谓词转换器语义的进一步研究还应用了拓扑方法[3,7,8]。最常见命令的指称语义表示是状态转换器形式。而采用外延描述方法,一个最弱(宽容)前置条件就是满足某一性质的状态集合。本文的主要目的是以 IMP 为对象语言,将谓词转换器作为命令的指称,并证明它与状态转换器对语义的刻画是一致的,表明公理语义与指称语义具有一种紧密的内在联系。

2 基本数学概念

定义 1.1 若集合 P 上的二元关系$\sqsubseteq$满足:

(ⅰ) 自反性:$\forall p\in P.\ p\sqsubseteq p$,

(ⅱ) 传递性:$\forall p,q,r\in P.\ p\sqsubseteq q\&q\sqsubseteq r\Rightarrow p\sqsubseteq r$,

(ⅲ) 反对称性:$\forall p,q\in P.\ p\sqsubseteq q\&q\sqsubseteq p\Rightarrow p=q$,

则称集合$(P,\sqsubseteq)$是一个偏序(PO)。

定义 1.2 对偏序$(P,\sqsubseteq)$和子集 $X\subseteq P$,称 p 是 X 的上界当且仅当 $q\in X.\ q\sqsubseteq p$;称 p 是 X 的最小上界当且仅当

(ⅰ) p 是 X 的上界,且

(ⅱ) 对 X 的所有上界 q,有 $p\sqsubseteq q$。

最小上界也记为$\sqcup X$。

定义 1.3 设$(P,\sqsubseteq)$是 PO,$(P,\sqsubseteq)$是一个全序当且仅当$\forall x,y\in P.\ x\sqsubseteq y$ 或 $y\sqsubseteq x$。全序也称线序。

定义 1.4 设$(P,\sqsubseteq)$是 PO,子集 $X\subseteq P$,若 X 是关系$\sqsubseteq$下的一个全序,则称 X 是集合 P 中的一个链。设 $X=\{d_n\mid n\in\omega\}$,ω 为自然数集,则 X 是一个 ω 递增链 $d_0\sqsubseteq d_1\sqsubseteq\cdots\sqsubseteq d_n\sqsubseteq\cdots$,简称为 ω 链。

定义 1.5 设$(P,\sqsubseteq_P)$是 PO。若 P 的所有的 ω 链$\{d_n\mid n\in\omega\}$在 P 中都有最小上界$\sqcup\{d_n\mid n\in\omega\}$,记为$\sqcup_{n\in\omega}d_n$,则称$(P,\sqsubseteq_P)$是完全偏序(CPO)。

如果$(P,\sqsubseteq_P)$有最小元$\perp_P$(称为底),则$(P,\sqsubseteq_P)$是含底的 CPO,也称为域。

在上下文清楚时,有时把完全偏序$(P,\sqsubseteq_P)$简记为 P 或$\sqsubseteq$;把底元素简记为$\perp$。

定义 1.6 设 X 是一个集合,以恒等关系 Id_X 为偏序的集合(X,Id_X)是一个 CPO,称为离散 CPO,该集合的每一个元素构成一个链,称为常链,每一元素本身也是链的最小上界。

定义 1.7 设$(D,\sqsubseteq_D)$和$(E,\sqsubseteq_E)$是 CPO,函数 $f:D\to E$ 是单调的当且仅当

$$\forall d,d'\in D.\ d\sqsubseteq_D d'\Rightarrow f(d)\sqsubseteq_E f(d')$$

函数 f 是连续的当且仅当 f 是单调的且对$(D,\sqsubseteq_D)$中所有 ω 链 $d_0\sqsubseteq_D d_1\sqsubseteq_D\cdots\sqsubseteq_D d_n\sqsubseteq_D\cdots$有

$$\bigsqcup_{n\in\omega}f(d_n)=f(\bigsqcup_{n\in\omega}d_n)$$

*)国家自然科学基金资助项目(60373075);教育部科学技术研究重点基金资助项目(01077);中科院计算机科学重点实验室基金资助项目(SYSKF0305);上海市科学技术委员会科研计划项目资助(045115006);宁夏自然科学基金项目(NZ0725)。丁志义 副教授,博士生,主要研究方向为软件形式化方法和形式语言理论;李全德 硕士研究生,主要研究方向为软件验证方法;宋国新 教授,博士生导师,主要研究方向为软件形式化方法;邵志清 教授,博士生导师,主要研究领域为软件开发与验证方法。

定义 1.8 设$(D,\sqsubseteq)$是 CPO，$f:D\to D$是连续函数，D中满足函数方程$f(d)=d$的元素d称为f的一个不动点。若对f的任一不动点x均有$d\sqsubseteq x$，则d是f的最小不动点。

定理 1.1[6]（Tarski 最小不动点定理） 设函数$f:D\to D$是含底完全偏序$(D,\sqsubseteq)$上的连续函数，定义$fix(f)=\bigsqcup_{n\in\omega}f^n(\bot)$，则$fix(f)$是$f$的最小不动点。

3 状态转换器

3.1 IMP 语言的语法

IMP 语言[6]有 3 个语法范畴：

1）算术表达式 AExp，其元素为$a,a_0,a_1,\cdots$

2）布尔表达式 BExp，其元素为$b,b_0,b_1,\cdots$

3）命令 Com，其元素为$c,c_0,c_1,\cdots$

一个 IMP 程序就是 Com 中的一个命令。设 Var 是变量的可数集，其元素为$x,x_0,x_1\cdots$；设$\mathbb{Z}$为整数集，用$n,n_0,n_1\cdots$表示$\mathbb{Z}$的元素；用整数常量符号$\hat{n}$表示整数n。

IMP 的语法用 BNF 表示为

AExp::$=\hat{n}\mid x\mid(a_0\oplus a_1)$

BExp::$=$true$\mid$false$\mid(a_0\odot a_1)\mid(b_0\otimes b_1)\mid\neg b$

Com::$=$skip$\mid x:=a\mid(c_0;c_1)\mid$(if b then c_0 else c_1)$\mid$(while b do c)

$\oplus$::$=+\mid-\mid\times$

$\odot$::$=\leqslant\mid=$

$\otimes$::$=\wedge\mid\vee$

3.2 状态转换器的一些性质

IMP 的一个命令指称状态集$\Sigma\equiv$Var$\to\mathbb{Z}$上的一个部分函数$f:\Sigma\rightharpoonup\Sigma$，即$C(c)\triangleq\lambda\sigma.\ f(\sigma)$，状态集$\Sigma$在恒等关系$Id_\Sigma\triangleq\lambda\sigma\in\Sigma.\ \sigma$下构成一个离散完全偏序。若在$(\Sigma_\bot,\mathrm{Id}_{\Sigma_\bot})$中加入底元素$\bot(\bot\notin\Sigma)$，使得$\forall\sigma\in\Sigma.\ \bot\sqsubseteq\sigma$，则$(\Sigma_\bot,Id_{\Sigma_\bot})$是一个含底的离散 CPO，也称为平坦域。从计算的直观角度看，$\bot$表示$f(\sigma)$无定义的状态，即信息为空的状态。

给一个 CPO 加入底元素$\bot$后得到一个含底的 CPO，这种构造方法称为提升，可用多种方法定义一个提升函数$\lfloor\text{-}\rfloor:\Sigma\to\Sigma_\bot$，只要求底元素$\bot$和函数$\lfloor\text{-}\rfloor$满足以下性质：

$\forall\sigma,\sigma_0,\sigma_1\in\Sigma.\lfloor\sigma_0\rfloor=\lfloor\sigma_1\rfloor\Rightarrow\sigma_0=\sigma_1$，且$\bot\neq\lfloor\sigma\rfloor$

因此，提升后的完全偏序为$\Sigma_\bot=\{\lfloor\sigma\rfloor\mid\sigma\in\Sigma\}\cup\{\bot\}$。

定义 2.1 设Σ是一个 CPO，则提升后的完全偏序$\Sigma_\bot$可定义为：$\sigma'_0\sqsubseteq\sigma'_1$当且仅当

$(\sigma'_0=\bot)$或$(\exists\sigma_0,\sigma_1\in\Sigma.\ \sigma'_0=\lfloor\sigma_0\rfloor\ \&\ \sigma'_1=\lfloor\sigma_1\rfloor\ \&\ \sigma_0\sqsubseteq\sigma_1)$

显然，函数$\lfloor\text{-}\rfloor:\Sigma\to\Sigma_\bot$是连续的。

定理 2.1 部分函数集合$\Sigma\rightharpoonup\Sigma$与全函数集合$\Sigma\to\Sigma_\bot$是一一对应的。

证明：首先定义映射$\Phi:(\Sigma\rightharpoonup\Sigma)\to(\Sigma\to\Sigma_\bot)$为

$$\Phi(f)(\sigma)=\begin{cases}\lfloor f(\sigma)\rfloor,\text{对某一}\sigma\in\Sigma,f(\sigma)\text{有定义}\\ \bot,\text{否则}\end{cases}$$

然后证明Φ是双射的。

先证Φ是单射的。设$f_1,f_2:\Sigma\rightharpoonup\Sigma$是两个部分函数，且$f_1\neq f_2$，则必存在某个$\sigma\in\Sigma$，使得$f_1(\sigma)\neq f_2(\sigma)$。再由函数的性质得$\lfloor f_1(\sigma)\rfloor\neq\lfloor f_2(\sigma)\rfloor$，故$\Phi(f_1)\neq\Phi(f_2)$。

再证Φ是满射的。对任一全函数$g:\Sigma\to\Sigma_\bot$，可构造f如下：

$$f(\sigma)=\begin{cases}\sigma',&\text{若 }g(\sigma)=\lfloor\sigma'\rfloor,\text{其中}\sigma'\in\Sigma\\ \text{未定义},&\text{若 }g(\sigma)=\bot\end{cases}$$

显然，f是$\Sigma\rightharpoonup\Sigma$的一个部分函数，且$\Phi(f)=g$，故$\Phi$是满射的。

定义 2.2 设$f,g:\Sigma\to\Sigma_\bot$，定义$f\sqsubseteq g$当且仅当$\forall\sigma\in\Sigma.\ f(\sigma)\sqsubseteq g(\sigma)$，即函数$f$和$g$具有点式序。

定理 2.2 函数$f,g:\Sigma\to\Sigma_\bot$的点式序对应着相应部分函数$f',g':\Sigma\rightharpoonup\Sigma$的包含次序，即$f\sqsubseteq g$当且仅当$f'\subseteq g'$当且仅当$\mathrm{Dom}(f')\subseteq\mathrm{Dom}(g')\ \&\ \forall\sigma\in\mathrm{Dom}(f').\ f'(\sigma)=g'(\sigma)$。其中$\mathrm{Dom}(f')$和$\mathrm{Dom}(g')$分别是部分函数$f'$和$g'$的定义域。

证明：根据定义 2.2 和定理 2.1 可证。

点式序刻画了函数的“全性”，若$f\sqsubseteq g$，则说明函数g比f更“全”。点式序下函数链的最小上界即是一个完全函数。部分函数集$\Sigma\rightharpoonup\Sigma$上的包含关系$\subseteq$构成一个 CPO，完全函数集$\Sigma\to\Sigma_\bot$的点式序也构成一个 CPO，其函数链$f_0\sqsubseteq f_1\sqsubseteq\cdots f_n\sqsubseteq\cdots$的最小上界$\bigsqcup_{n\in\omega}f_n$与$(\Sigma\rightharpoonup\Sigma,\subseteq)$上的最小上界$\bigcup_{n\in\omega}f'_n$相对应。

定理 2.3 $f:\Sigma\to\Sigma_\bot$是连续函数，即$f(\bigsqcup_{n\in\omega}\sigma)=\bigsqcup_{n\in\omega}f(\sigma)$，其中$\sigma\in\Sigma$。

证明：$(\Sigma,\mathrm{Id}_\Sigma)$是离散 CPO，故有$\forall\sigma\in\Sigma$。$\bigsqcup\sigma=\sigma$，所以$f(\bigsqcup\sigma)=\bigsqcup f(\sigma)$。

若$f(\sigma)=\bot$，则$\bigsqcup f(\sigma)=\bot=f(\sigma)=f(\bigsqcup\sigma)$；

若$f(\sigma)=\lfloor\sigma\rfloor$，则$\bigsqcup f(\sigma)=\lfloor\sigma\rfloor=\lfloor\sigma\rfloor=f(\sigma)=f(\bigsqcup\sigma)$，故$f$是连续的。

定义 2.3 设$f:\Sigma\to\Sigma_\bot$是连续函数，定义函数$(f)^*:\Sigma_\bot\to_\bot\Sigma_\bot$如下：

$$(f)^*(\sigma')=\begin{cases}f(\sigma),&\text{若}\exists\sigma\in\Sigma,\sigma'=\lfloor\sigma\rfloor\\ \bot,&\text{其它}\end{cases}$$

即$(f)^*$是f的一个扩充，是严格连续的，$(f)^*$也记作$f_\bot$。

$f_\bot$是严格函数是因为$f_\bot(\bot)=\bot$。不难证明$f_\bot$也是连续函数。这样，$\Sigma_\bot\to_\bot\Sigma_\bot$就是$\Sigma_\bot\to\Sigma_\bot$中的所有严格连续函数构成的集合，同时$\Sigma_\bot\to_\bot\Sigma_\bot$仍具有点式序。

定义 2.4 $\Sigma_\bot\to_\bot\Sigma_\bot$的所有函数按点式序可构成一个完全偏序，称为函数空间，记作$[\Sigma_\bot\to_\bot\Sigma_\bot]$，其底元素为$\bot_{[\Sigma_\bot\to_\bot\Sigma_\bot]}$，即值恒为$\bot$的常函数，对任一$\sigma\in\Sigma_\bot$均有$\bot_{[\Sigma_\bot\to_\bot\Sigma_\bot]}(\sigma)=\bot$。$[\Sigma_\bot\to_\bot\Sigma_\bot]$中的函数链$f_0\sqsubseteq f_1\sqsubseteq\cdots\sqsubseteq f_n\sqsubseteq\cdots(n\in\omega)$按点式序排列，链的最小上界$\bigsqcup_{n\in\omega}f_n$在点式序下是存在的，即对任一$\sigma\in\Sigma_\bot$，有

$$(\bigsqcup_{n\in\omega}f_n)(\sigma)=\bigsqcup_{n\in\omega}(f_n(\sigma))$$

为证明$\bigsqcup_{n\in\omega}f_n$的连续性，需要以下引理：

引理[5] 设$e_{n,m}(n,m\in\omega)$是完全偏序E的元素，当$n\leqslant n'\ \&\ m\leqslant m'$时有$e_{n,m}\sqsubseteq e_{n',m'}$，则集合$\{e_{n,m}\mid n,m\in\omega\}$的最小上界$\bigsqcup_{n,m\in\omega}e_{n,m}=\bigsqcup_{n\in\omega}(\bigsqcup_{m\in\omega}e_{n,m})=\bigsqcup_{m\in\omega}(\bigsqcup_{n\in\omega}e_{n,m})=\bigsqcup_{n\in\omega}e_{n,n}$。

定理 2.4 函数空间$[\Sigma_\bot\to_\bot\Sigma_\bot]$中点式序下的函数链$\{f_n\mid n\in\omega\}$的最小上界$\bigsqcup_{n\in\omega}f_n$是连续函数。

证明：对任一$\sigma\in\Sigma_\bot$，有

$$\begin{aligned}(\bigsqcup_{n\in\omega}f_n)(\bigsqcup_{m\in\omega}\sigma_m)&=\bigsqcup_{n\in\omega}(f_n(\bigsqcup_{m\in\omega}\sigma_m))=\bigsqcup_{n\in\omega}(\bigsqcup_{m\in\omega}f_n(\sigma_m))\\&=\bigsqcup_{m\in\omega}(\bigsqcup_{n\in\omega}f_n(\sigma_m))=\bigsqcup_{m\in\omega}((\bigsqcup_{n\in\omega}f_n)(\sigma_m))\end{aligned}$$

IMP 语言的命令可抽象地表示为一个函数$f:\Sigma\to_\bot\Sigma_\bot$，因为$\Sigma\rightharpoonup\Sigma$，$\Sigma\to\Sigma_\bot$和$\Sigma_\bot\to_\bot\Sigma_\bot$是一一对应的。这样的函数称为状态转换器，所有的状态转换器按点式序可构成含底的 CPO，与状态集合上的部分函数按点式序下的 CPO 同构。

3.3 IMP 语言的指称语义

IMP 语言指称语义的定义要用到状态集$\Sigma\equiv$Var$\to\mathbb{Z}$，各语法范畴对象的指称为

$A[\![a]\!]\in\Sigma\to\mathbb{Z}$

$B[\![b]\!]\in\Sigma\to\{\mathrm{TRUE},\mathrm{FALSE}\}$

$C[\![c]\!]\in\Sigma\to\Sigma_\perp$

IMP 语言的指称语义是归纳定义的。对算术表达式

$A[\![\hat{n}]\!]\triangleq\lambda\sigma\in\Sigma\cdot n$

$A[\![x]\!]\sigma\triangleq\sigma(x)$

$A[\![a_0\oplus a_1]\!]\sigma\triangleq A[\![a_0]\!]\sigma\oplus A[\![a_1]\!]\sigma$

对布尔表达式

$B[\![\mathrm{true}]\!]\sigma\triangleq\mathrm{TRUE}$

$B[\![\mathrm{false}]\!]\sigma\triangleq\mathrm{FALSE}$

$B[\![a_0\odot a_1]\!]\sigma\triangleq A[\![a_0]\!]\sigma\subseteq\triangleq\odot A[\![a_1]\!]\sigma$

$B[\![b_0\otimes b_1]\!]\sigma\triangleq B[\![b_0]\!]\sigma\otimes B[\![b_1]\!]\sigma$

$B[\![\neg b]\!]\sigma\triangleq$ if $B[\![b]\!]\sigma$ then FALSE else TRUE

对命令

$C[\![\mathrm{skip}]\!]\sigma\triangleq\sigma$

$C[\![x:\alpha]\!]\sigma\triangleq[A[\![\alpha]\!]\sigma/x]$

$$C[\![\text{if } b \text{ then } c_0 \text{ else } c_1]\!]\sigma\triangleq\begin{cases}C[\![c_0]\!]\sigma, & \text{if } B[\![b]\!]\sigma=\mathrm{TPUE}\\ C[\![c_1]\!]\sigma, & \text{if } B[\![b]\!]\sigma=\mathrm{FALSE}\end{cases}$$

$$C[\![c_0;c_1]\!]\sigma\triangleq\begin{cases}C[\![c_1]\!](C[\![c_0]\!]\sigma), & \text{if } C[\![c_0]\!]\sigma\neq\perp\\ \perp, & \text{if } C[\![c_0]\!]\sigma=\perp\end{cases}$$

函数 $f_\perp:(D\to E_\perp)\to(D\to E_\perp)$ 定义为

$f_\perp\triangleq\lambda x.$ if $x=\perp$ then $\perp$ else $f(x)$

则

$C[\![c_0;c_1]\!]\sigma\triangleq C[\![c_1]\!]_\perp(C[\![c_0]\!]\sigma)$

$C[\![\text{while } b \text{ do } c]\!]\sigma\triangleq$ if $B[\![b]\!]\sigma$ then $C[\![c;\text{ while } b \text{ do } c]\!]\sigma$ else σ

$=$ if $B[\![b]\!]\sigma$ then $C[\![\text{while } b \text{ do } c]\!]_\perp(C[\![c]\!]\sigma)$ else σ

定义连续函数

$\Gamma\triangleq\lambda w\in\Sigma\to\Sigma_\perp.\lambda\sigma\in\Sigma.$ if $B[\![b]\!]\sigma$ then $w_\perp(C[\![c]\!]\sigma)$ else σ

取命令 while b do c 的指称为 Γ 的最小不动点，即

$C[\![\text{while } b \text{ do } c]\!]=fix(\Gamma)$

其中 $fix:[(\Sigma\to\Sigma_\perp)\to(\Sigma\to\Sigma_\perp)]\to(\Sigma\to\Sigma_\perp)$ 是求取最小不动点的算子。

4 谓词转换器

Dijkstra 把命令的语义规定为谓词转换器[5]，认为满足一个命令的后置谓词当且仅当满足该命令关于其后置条件的最弱宽容前置条件，最弱宽容前置条件可定义为

$wlp^I(c,B)=\{\sigma\in\Sigma_\perp\mid C[\![c]\!]\sigma\vdash^I B\}$

其中 $c\in\mathrm{Com}$，B 为断言语句表示的谓词，I 是解释。对于 Hoare 部分正确性断言 $\{A\}c\{B\}$ 有

$\vdash^I\{A\}c\{B\}$ 当且仅当 $\vdash^I A\Rightarrow wlp^I(c,B)$

按照这一概念，一个部分正确性谓词就可表示为 $\Sigma_\perp$ 的一个子集。$\mathrm{Pred}(\Sigma)$ 定义如下：

$\mathrm{Pred}(\Sigma)=\{Q\subseteq\Sigma_\perp\ \&\perp\in Q\}$

从信息处理的直观角度来看，当命令执行能够终止，则由命令的格局给出的更多的终态信息包含在一个更小的集合里。因此，谓词集合上的反包含关系 $\supseteq$ 就构成一个部分正确性谓词的完全偏序 $(\mathrm{Pred}(\Sigma),\supseteq)$。其中，对应信息量最小的为底元素 $\perp_{\mathrm{Pred}}=\Sigma\cup\{\perp\}$。对任意部分正确性谓词 B，均有 $\perp\vdash B$。这样，就可以定义 $(\mathrm{Pred}(\Sigma),\supseteq)$ 上的连续函数——谓词转换器。

定义 3.1 对 $Q_1,Q_2\in\mathrm{Pred}(\Sigma)$，定义偏序关系 $\sqsubseteq$ 为：$Q_1\sqsubseteq Q_2$ 当且仅当 $Q_1\supseteq Q_2$，这样 $\bigsqcup_{n\in\omega}Q_n=\bigcap_{n\in\omega}Q_n$。

定义 3.2 设 $f:\Sigma\to\Sigma_\perp$ 是状态转换器。函数 $Wf:\mathrm{Pred}(\Sigma)\to\mathrm{Pred}(\Sigma)$ 定义为

$(Wf)(Q)=\{\sigma\in\Sigma\mid f(\sigma)\in Q\}\cup\{\perp\}=(f^{-1}Q)\cup\{\perp\}$

由指称语义可知命令 c 的指称 $C[\![c]\!]:\Sigma\to\Sigma_\perp$ 是一个状态转换器，根据最弱前置条件的结构，由定义 3.2 容易确定下式是成立的：

$(W(C[\![c]\!]))(B^I)=wlp^I(c,B)$

其中 B 是任一断言，I 是解释。

定理 3.1 设 $ST\equiv[\Sigma_\perp\to_\perp\Sigma_\perp]$，$PT\equiv[\mathrm{Pred}(\Sigma)\to\mathrm{Pred}(\Sigma)]$，则

(ⅰ) $W:ST\to_\perp PT$ 且 W 是连续的；

(ⅱ) $W(Id_{\Sigma_\perp})=Id_{\mathrm{Pred}(\Sigma)}$；

(ⅲ) $W(f\circ g)=(Wg)\circ(Wf)$；

(ⅳ) $Wf=Wf'\Rightarrow f=f'$。

证明：由前面的论述可知 $[\Sigma\to\Sigma_\perp]$ 与 $[\Sigma_\perp\to_\perp\Sigma_\perp]$ 同构，其中的任意函数都连续且一一对应。

(ⅰ) 由定义 3.2，$(Wf)Q=\{\sigma\in\Sigma\mid f(\sigma)\in Q\}\cup\{\perp\}=\{\sigma\in\Sigma_\perp\mid f_\perp(\sigma)\in Q\}$，故 $W\in ST\to_\perp PT$。

$(W(\perp_{\Sigma_\perp\to_\perp\Sigma_\perp}))(Q)=\{\sigma\in\Sigma_\perp\mid\perp_{[\Sigma_\perp\to_\perp\Sigma_\perp]}(\sigma)=\perp\in Q\}=\Sigma\cup\{\perp\}=\perp_{\mathrm{Pred}}$，故 W 是严格函数。

对任一 $Q\in\mathrm{Pred}(\Sigma)$，由连续函数的定义，以及点式序刻画的函数的“全性”和谓词递增链刻画的状态集合的反包含关系，有下式成立：

$$\begin{aligned}(W(\bigsqcup_n f_n))(Q)&=\{\sigma\in\Sigma_\perp\mid(\bigsqcup_n f_n)(\sigma)\in Q\}\\&=\bigcap_{n\in\omega}\{\sigma\in\Sigma_\perp\mid f_n(\sigma)\in Q\}\\&=\bigsqcup_{n\in\omega}\{\sigma\in\Sigma_\perp\mid f_n(\sigma)\in Q\}\\&=\bigsqcup_{n\in\omega}((Wf_n)Q)\\&=(\bigsqcup_{n\in\omega}(Wf_n))Q\end{aligned}$$

即 $W(\bigsqcup_{n\in\omega}f_n)=\bigsqcup_{n\in\omega}W(f_n)$，$W$ 是连续的。

(ⅱ) 对任一 $Q\in\mathrm{Pred}(\Sigma)$，有

$$\begin{aligned}W(Id_{\Sigma_\perp})(Q)&=\{\sigma\in\Sigma\mid Id_{\Sigma_\perp}(\sigma)\in Q\}\cup\{\perp\}\\&=Q=Id_{\mathrm{Pred}(\Sigma)}(Q)\end{aligned}$$

(ⅲ) 因为 f 是严格连续函数，对任一 $Q\in\mathrm{Pred}(\Sigma)$，有

$$\begin{aligned}(W(f\circ g))(Q)&=((f\circ g)^{-1}Q)\cup\{\perp\}\\&=((g^{-1}\circ f^{-1})Q)\cup\{\perp\}\\&=(g^{-1}(f^{-1}Q))\cup\{\perp\}\\&=Wg((f^{-1}Q))\\&=(Wg\circ Wf)(Q)\end{aligned}$$

(ⅳ) 已知 f,f' 是 $\Sigma_\perp$ 上的两个严格连续函数，且 $Wf=Wf'$，即对任一 $Q\in\mathrm{Pred}(\Sigma)$，有

$$\{\sigma\in\Sigma_\perp\mid f(\sigma)\in Q\}=\{\sigma\in\Sigma_\perp\mid f'(\sigma)\in Q\}\qquad(1)$$

采用反证法。假设 $f\neq f'$，即对某一 $\sigma'\in\Sigma_\perp$ 有 $f(\sigma')\neq f'(\sigma')$。由于 f,f' 均为严格函数，即 $f(\perp)=f'(\perp)=\perp$，故必有 $\sigma'\neq\perp$。现令 $Q=\{\perp\}$，则(1)式为

$\{\sigma\in\Sigma_\perp\mid f(\sigma)=\perp\}=\{\sigma\in\Sigma_\perp\mid f'(\sigma)=\perp\}=S$

若 $\sigma'\in S$，则立即有 $f'(\sigma')=\perp=f(\sigma')$，与 $f'(\sigma')\neq f(\sigma')$ 矛盾。

若 $\sigma'\notin S$，则 $f(\sigma')=\sigma_1\neq\perp$，$f'(\sigma')=\sigma_2\neq\perp$，且 $\sigma_1\neq\sigma_2$。令 $Q'=\{\sigma_1,\perp\}$ 则

$\{\sigma\in\Sigma_\perp\mid f(\sigma)\in Q'\}=(Wf)Q'=\{\sigma\in\Sigma_\perp\mid f'(\sigma)\in Q'\}$

显然，$\sigma'\in\{\sigma\in\Sigma_\perp\mid f(\sigma)\in Q'\}$，而 $\sigma'\notin\{\sigma\in\Sigma_\perp\mid f'(\sigma)\in Q'\}$，与 $Wf\neq Wf'$ 矛盾。

由以上两方面，$f=f'$ 得证。

5 谓词转换器作为命令的指称

上面讨论了谓词的完全偏序 $(\mathrm{Pred}(\Sigma),\supseteq)$ 和谓词转换

器的完全偏序[Pred(Σ)→Pred(Σ)]。

为了用谓词转换器来表示 IMP 命令的指称语义，首先需要定义语义函数 $\mathscr{P}t$:Com→PT。

定义 4.1 语义函数 $\mathscr{P}t$:Com→PT 定义为

$\mathscr{P}t[\![\text{skip}]\!]Q=Q$

$\mathscr{P}t[\![X:=a]\!]Q=\{\sigma\in A\Sigma_\perp \mid \sigma[A[\![a]\!]\sigma/X]\in Q\}$

$\mathscr{P}t[\![c_0;c_1]\!]Q=\mathscr{P}t[\![c_0]\!](\mathscr{P}t[\![c_1]\!]Q)$

$\mathscr{P}t[\![\text{if } b \text{ then } c_0 \text{ else } c_1]\!]Q=(\bar{b}\cap\mathscr{P}t[\![c_0]\!]Q)\cup(\overline{\neg b}\cap\mathscr{P}t[\![c_1]\!]Q)$

其中，对任意的布尔表达式 b，有 $\bar{b}=\{\sigma\mid\sigma=\perp or\ \beta[\![b]\!]\sigma=\text{true}\}$

$\mathscr{P}t[\![\text{while } b \text{ do } c]\!]=fix(G)$

其中，函数 $G:PT\to PT$ 定义为 $G(p)(Q)=(\bar{b}\cap Pt[\![c]\!](p(Q)))\cup(\overline{\neg b}\cap Q)$。由定理 1.1 和谓词的逆包含关系，有

$$fix(G)=\bigsqcup_{n\in\omega}G^n(\perp_{\text{pred}(\Sigma)})=\bigcap_{n\in\omega}G^n(\perp_{\text{pred}(\Sigma)})$$

定理 4.1 令 $G:PT\to PT$，且 $G(p)(Q)=(\bar{b}\cap\mathscr{P}t[\![c]\!](p(Q)))\cup(\overline{\neg b}\cap Q)$，则有以下性质成立：

(ⅰ) G 是连续的；

(ⅱ) 对任意的命令 c，有 $W(c[\![c]\!]_\perp)=\mathscr{P}t[\![c]\!]$；

(ⅲ) $C[\![c]\!]=C[\![c']\!]$ 当且仅当 $Pt[\![c]\!]=\mathscr{P}t[\![c']\!]$。

证明：(ⅰ) 对任一 $Q\in\text{Pred}(\Sigma)$，有

$$\begin{aligned}G(\sqcup p_i)(Q)&=(\bar{b}\cap\mathscr{P}t[\![c]\!]((\bigsqcup_{i\in\omega}p_i)(Q)))\cup(\overline{\neg b}\cap Q)\\&=(\bar{b}\cap\mathscr{P}t[\![c]\!](\bigsqcup_{i\in\omega}(p_i(Q))))\cup(\overline{\neg b}\cap Q)\\&=(\bar{b}\cap(\bigsqcup_{i\in\omega}\mathscr{P}t[\![c]\!](p_i(Q))))\cup(\overline{\neg b}\cap Q)\\&=(\bar{b}\cap(\bigcap_{i\in\omega}\mathscr{P}t[\![c]\!](p_i(Q))))\cup(\overline{\neg b}\cap Q)\\&=\bigcap_{i\in\omega}(G(p_i)(Q))\\&=\bigsqcup_{i\in\omega}(G(p_i)(Q))\end{aligned}$$

所以，G 是连续的。

(ⅱ) 由 $\mathscr{P}t$ 和 W 的定义，施结构归纳于命令 c 证明如下：

$c\equiv$skip：对任一 $Q\in\text{Pred}(\Sigma)$，有

$W(c[\![\text{skip}]\!]_\perp)Q=\{\sigma\in\Sigma_\perp\mid\sigma\in Q\}=Q=\mathscr{P}t[\![\text{skip}]\!]Q$

$c\equiv X:a$：对任一 $Q\in\text{Pred}(\Sigma)$，有

$$\begin{aligned}W(c[\![X:=a]\!]_\perp)Q&=\{\sigma\in\Sigma_\perp\mid C[\![X:=a]\!]_\perp\sigma\in Q\}\\&=\{\sigma\in\Sigma_\perp\mid\sigma[A[\![a]\!]\sigma/X]\in Q\}\\&=\mathscr{P}t[\![X:=a]\!]Q\end{aligned}$$

$c\equiv c_0;c_1$：归纳假设为 $W(c[\![c_0]\!]\mathscr{P}t[\![c_0]\!])$ 且 $W(C[\![c_1]\!]_\perp)=\mathscr{P}t[\![c_1]\!]$。对任一 $Q\in\text{Pred}(\Sigma)$，有

$$\begin{aligned}W(C[\![c_0;c_1]\!]_\perp)Q&=W(C[\![c_1]\!]_\perp\circ C[\![c_0]\!]_\perp)Q\\&=(W(C[\![c_0]\!]_\perp)\circ W(C[\![c_1]\!]_\perp))Q\\&=(\mathscr{P}t[\![c_0]\!]\circ\mathscr{P}t[\![c_1]\!])Q\\&=\mathscr{P}t[\![c_0;c_1]\!]Q\end{aligned}$$

$c\equiv$if b then c_0 else c_1：归纳假设为：$W(C[\![c_0]\!]_\perp)=\mathscr{P}t[\![c_0]\!]$ 且 $W(C[\![c_1]\!]_\perp)=\mathscr{P}t[\![c_1]\!]$。对任一状态 $\sigma\in\Sigma$ 有

$$C[\![\text{if } b \text{ then } c_0 \text{ else } c_1]\!]_\perp\sigma=\begin{cases}C[\![c_0]\!]\sigma, & \text{if } \mathscr{B}[\![b]\!]\sigma=\text{TRUE}\\C[\![c_1]\!]\sigma, & \text{if } \mathscr{B}[\![b]\!]\sigma=\text{FALSE}\\\perp, & \text{if } \sigma=\perp\end{cases}$$

此时，对任一 $Q\in\text{Pred}(\Sigma)$，有

$$\begin{aligned}&W(C[\![\text{ if } b \text{ then } c_0 \text{ else } c_1]\!]_\perp)Q=\{\sigma\in\Sigma\mid C[\![\text{ if } b \text{ then } c_0\\&\quad\text{else } c_1]\!]\sigma\in Q\}\cup\{\perp\}\\&=\{\sigma\in\Sigma\mid\mathscr{B}[\![b]\!]\sigma=\text{TPUE}\ \&\ C[\![c_0]\!]\sigma\in Q\}\cup\{\perp\}\cup\\&\quad\{\sigma\in\Sigma\mid\mathscr{B}[\![b]\!]\sigma=\text{FALSE}\ \&\ C[\![c_1]\!]\sigma\in Q\}\cup\{\perp\}\\&=(\bar{b}\cap(\{\sigma\in\Sigma\mid C[\![c_0]\!]\sigma\in Q\}\cup\{\perp\}))\cup\\&\quad(\overline{\neg b}\cap(\{\sigma\in\Sigma\mid C[\![c_1]\!]\sigma\in Q\}\cup\{\perp\}))\\&=(\bar{b}\cap(W(C[\![c_0]\!]_\perp\sigma)Q))\cup(\overline{\neg b}\cap(W(c[\![c_1]\!]_\perp\sigma)Q))\\&=(\bar{b}\cap\mathscr{P}t[\![c_0]\!]Q)\cup(\overline{\neg b}\cap\mathscr{P}t[\![c_1]\!]Q)\\&=\mathscr{P}t[\![\text{if } b \text{ then } c_0 \text{else } c_1]\!]Q\end{aligned}$$

$c\equiv$while b do c：将命令 while b do c 简记为 w。由于 $C[\![w]\!]=C[\![\text{if } b \text{ then } c;w \text{ else skip}]\!]$，因此，对任一 $Q\in\text{Pred}(\Sigma)$，有

$$\begin{aligned}W(C[\![w]\!]_\perp)Q&=W(C[\![\text{if } b \text{ then } c;w \text{ else skip}]\!]_\perp)Q\\&=\mathscr{P}t[\![\text{if } b \text{ then } c;w \text{ else skip}]\!]Q\\&=(\bar{b}\cap\mathscr{P}t[\![c;w]\!]Q)\cup(\overline{\neg b}\cap\mathscr{P}t[\![\text{skip}]\!]Q)\\&=(\bar{b}\cap\mathscr{P}t[\![c]\!](\mathscr{P}t[\![w]\!]Q))\cup(\overline{\neg b}\cap Q)\\&=G(\mathscr{P}t[\![w]\!])(Q)\\&=\mathscr{P}t[\![w]\!]Q\end{aligned}$$

(ⅲ) 注意到

$$C[\![c]\!]\sigma=\begin{cases}C[\![c]\!]_\perp\sigma, & \text{if } C[\![c]\!]_\perp\sigma\neq\perp\\\perp, & \text{if } C[\![c]\!]_\perp\sigma=\perp\end{cases}$$

充分性：由定理 3.1，有

$$\mathscr{P}t[\![c]\!]=\mathscr{P}t[\![c']\!]\Rightarrow W(C[\![c]\!]_\perp\Rightarrow W(C[\![c']\!]_\perp)\Rightarrow C[\![c]\!]_\perp\Rightarrow C[\![c']\!]_\perp\Rightarrow C[\![c]\!]=C[\![c']\!]$$

必要性：

$$\begin{aligned}&\mathscr{P}t[\![c]\!]\neq\mathscr{P}t[\![c']\!]\Rightarrow W(C[\![c]\!]_\perp)\neq W(C[\![c']\!])\\&\Rightarrow\exists Q\in\text{Pred}(\Sigma).\ W(C[\![c]\!]_\perp)(Q)\neq W(C[\![c']\!]_\perp)(Q)\\&\Rightarrow\sigma'\in\Sigma.\ C[\![c]\!]\sigma'\neq C[\![c]\!]\sigma'\\&\Rightarrow\exists\sigma'\in\Sigma_\perp.\ C[\![c]\!]_\perp\sigma'\neq C[\![c']\!]\sigma'\\&\Rightarrow C[\![c]\!]\neq C[\![c']\!]\end{aligned}$$

结束语 本文对传统的表示命令指称的状态转换器进行了较深入的讨论。在此基础上，以 IMP 语言的对象语言，在 IMP 语言的指称语义描述方面引入了一类 wlp 域上的连续函数——谓词转换器以及谓词转换器空间，采用域论的一些研究方法，论证了状态转换器和谓词转换器的对应关系。研究结果表明，谓词转换器和状态转换器所刻画的对象语言的指称语义是等价的，从而揭示了公理语义和指称语义之间存在的一种紧密的联系。尽管更常用的指称语义是状态转换器形式的，而在另一角度上，以上论证的结果可看作是为状态转换语义者提供的谓词转换语义。

参 考 文 献

[1] Amadio R, Curien P L. Domains and Lambda-Calculus [M]. Cambridge: Cambridge University Press, 1998

[2] Stoltenberg-Hansen V, Lindstrom I, Griffor E R. Mathematical Theory of Domains [J]. Cambridge Tracts in Theoretical Computer Science, Cambridge: Cambridge University Press, 1994 (22)

[3] 陈仪香. 形式语义学的稳定论域理论[M]. 北京：科学出版社，2003

[4] Abramsky S, Jagadeesan R, Malacaria P. Full abstraction for PCF [J]. Information and Computation, 2000, 163: 409-470

[5] Dijkstra E W. A discipline of programming [M]. Englewood Cliffs, NJ: Prentice-Hall, 1976

[6] Winskel G. The Formal Semantics of Programming Languages: An Introduction [M]. The MIT Press, 1993

[7] 陈仪香. 最弱前置谓词的稳定语义[J]. 软件学报，2003, 14(专集)：161-167

[8] 陈仪香. 谓词转换器的拓扑语义[J]. 数学进展，2003, 32(2)：221-229