数理解析研究所講究録
666巻 1988年 1-7

初等トポスでの プログラムの公理的意味論

(Axiomatic Semantics in Elementary Toposes)

河原　康雄　（九州大学・理学部）
溝口　佳寛　（九州大学・理学部）

§0. はじめに

プログラムの意味の特徴付けの1つとして、プログラムの前後に表明を挿入し実行前後の状態を特徴付ける公理的方法がある。p, q を表明、f をプログラムとして、Hoareの記法を用いると {p}f{q} によって、前提条件 p のもとで、プログラム f を実行すると後置条件 q を満足することを表す。この表明とプログラムの関係を考察し意味を特徴つけるのが公理的方法である。

また、プログラム意味論には、プログラムを状態の集合（領域）間の関数と考え、その性質を考察する表示的方法がある。

Arbib らは、この2つの方法を融合し、各表明を状態の集合の部分集合に対応する防御関数、プログラムを表示的意味論に基づく状態集合間の関数へ対応させた。すなわち Hoare 記法の表明、プログラムともに集合上の関係の圏の射として解釈し、表明とプログラムに関する様々な性質を考察した。

しかし、一般には表示的意味論において、プログラムの意味を考える圏としては、集合上の関係の圏では不十分である。また、プログラム中の論理式等の解釈は、部分集合によるブール代数よりは、直観論理に基づく Heyting代数で

の解釈の方が一般的である。そこで我々は Arbib らの方法を一般化し、トポス上の関係の圏で Hoare記法を解釈する方法を導入した。さらに、Dijkstra の最弱前置条件をトポス上での防御関数として考え直した。プログラムと表明に関する諸性質の証明は、トポス上での関係の理論を利用して、関係式の計算を用いて明解に示される。これは、トポス上の関係の圏での解釈の正当性を示すだけではなく、プログラムの等価性等の諸性質の証明に関係計算（Relational Calculus）が有効であることを示している。

§1. 準備

E を初等トポスとする。E の対象X,Yに対して、X×Y の部分対象 α をXからYへの関係といい $\alpha:X\to Y$ と書く。XからYへの関係の全体をRel(X,Y)で表す。トポスの対象X×Yの部分対象全体であるRel(X,Y)は、Heyting代数の構造を持つ。関係 $\alpha:X\to Y$, $\beta:X\to Y$ に対して、$\alpha\sqcap\beta$ で下限、$\alpha\sqcup\beta$ で上限、$\neg\alpha$ で否定を表す。関係 $\alpha:X\to Y$, $\beta:Y\to Z$ に対して、$\alpha\cdot\beta:X\to Z$ で α, β の結合、$\alpha^{\#}:Y\to X$ で α の逆関係を表す。1をEの終対象とする。Xから1への最大関係を Ω_X と書く。XからYへの最小関係を 0_{XY} と書く。必要に応じて添え字のX,Yは省略する。関係 $f:X\to Y$ が $f^{\#}f\sqsubseteq id_Y$ を満たすとき、f を部分関数という。本論文では、E の対象と関係の圏 Rel 及び、その射を部分関数に制限した部分圏 Pfn を考える。

<u>補題1.</u> 関係 $\alpha,\beta:X\to Y$ に対して、

(1) $\alpha^{\#}\beta=0$ かつ $\alpha\Omega_Y\sqsubseteq\beta\Omega_Y$ ならば、$\alpha=0$ である。

(2) $\alpha\Omega_Y=0$ ならば、$\alpha=0$ である。

E の対象 X に対して、X 上の恒等射を $id_X:X\to X$ で表す。関係 $p:X\to X$ が $p\sqsubseteq id_X$ を満たすとき、p を X 上の防御関数(guard function)という。X 上の防御関数全体をG(X)と書く。G(X)はRel(X,X)の部分集合として自然にHeyting代数の構造が入る。

補題２．防御関数 p, p':$X \to X$ に対して、

(1) $pp = p$

(2) $pp' = p'p = p \sqcap p'$

(3) $p^{\sharp} = p$

(4) $p\Omega_X \sqsubseteq p'\Omega_X$ ならば、$p \sqsubseteq p'$

(5) $p\Omega_X = p'\Omega_X$ ならば、$p = p'$

補題３．　関係 α:$X \to Y$ 及び、防御関数 p:$Y \to Y$ に対して、次の (1),(2),(3) は同値である。

(1) $\alpha p = 0$

(2) $(\alpha^{\sharp}\alpha \sqcap id_Y) \sqsubseteq \neg p$

(3) $\alpha \cdot (\neg p) = \alpha$

命題４．任意の関係 α:$X \to Y$ に対して、Eの単射 i:$D \to X$ が存在して、$i^{\sharp}\Omega_D = \alpha\Omega_Y$ が成り立つ。

命題４．で定まる i を α の定義域単射という。この i に対して、α の核を $k(\alpha) = \neg(i^{\sharp}i)$、$\alpha$ の定義域を $d(\alpha) = \neg k(\alpha)$ で定める。

（注）定義域と核の定義は、定義域単射の取り方に依存しない。

命題５．　関係 α, β:$X \to Y$ に対して、$\alpha \sqsubseteq \beta$ の時、

(1) $k(\beta) \sqsubseteq k(\alpha)$

(2) $d(\alpha) \sqsubseteq d(\beta)$

補題６．関係 α:$X \to Y$, 防御関数 p:$X \to X$ に対して、

(1) $p\alpha = 0 \quad \leftrightarrow \quad p \sqsubseteq k(\alpha)$

(2) $p \sqsubseteq k(\alpha) \leftrightarrow \neg\neg p \sqsubseteq k(\alpha)$

(3) $p\alpha = 0 \quad \leftrightarrow \quad (\neg\neg p)\alpha = 0$

命題７．関係 $\alpha : X \rightharpoonup Y$ に対して、

(1) $k(\alpha)\cdot\alpha = 0$ 従って、$k(\alpha)$ は $\{p \in G(X) \mid p\cdot\alpha = 0\}$ の最大元である。

(2) 関係 $\tau : W \rightharpoonup X$ に対して、

$$\tau\,\alpha = 0 \quad \leftrightarrow \quad \tau\cdot k(\alpha) = \tau$$

(3) $d(\alpha)\cdot\alpha\cdot\Omega_Y = \alpha\cdot\Omega_Y$

(4) $k(\alpha) = id_X \quad \leftrightarrow \quad d(\alpha) = 0 \quad \leftrightarrow \quad \alpha = 0$

命題８．関係 $\alpha : X \rightharpoonup Y$, 防御関数 $p : X \rightharpoonup X$, $q : Y \rightharpoonup Y$ に対して、以下の(1)…(5)は、同値である。

(1) $p\,\alpha(\neg q) = 0$

(2) $p\,\alpha(\neg\neg q) = p\,\alpha$

(3) $(\neg\neg p)\,\alpha(\neg q) = 0$

(4) $(\neg\neg p)\,\alpha(\neg\neg q) = (\neg\neg p)\,\alpha$

(5) $p \sqsubset k(\alpha\cdot(\neg q))$

命題８．の条件の１つ、従って全てが成り立つ時、$\{p\}\alpha\{q\}$ と書く。また、

最弱自由前置条件(weakest leberal precondition)を

$wlp(\alpha, q) = k(\alpha\cdot(\neg q))$、

最弱前置条件(weakest precondition)を

$wp(\alpha, q) = wlp(\alpha, q) \sqcap d(\alpha)$

で定義する。

§ ２．公理的意味論

以下 p, q は防御関数、α, β は関係を表すとする。また、分脈から明かなときは、これらがどこからどこへの関数（関係）であるかは明記しない。

プログラムにおける基本文が、状態対象間の関係に対応付けられているとき、基本制御構造を次のように解釈する。

(1) $(\alpha ; \beta)$ を $\alpha\cdot\beta$ で解釈する。

(2) (if p then α else β) を $(q\cdot\alpha) \sqcup ((\neg q)\cdot\beta)$ で解釈する。

(3) (while p do α) を $\sqcup(p\cdot\alpha)^n(\neg p)$ で解釈する。

(注. $\sqcup\{(p\cdot\alpha)^n \mid 0\leqq n\}$ を $\sqcup(p\cdot\alpha)^n$ で略記する。)

命題9. (Consequence Rule)

$p\sqsubset p_1$, $q_1\sqsubset q$, $\{p_1\}\alpha\{q_1\}$ の時、$\{p\}\alpha\{q\}$ が成り立つ。

命題10. (Composition Rule)

$\{p\}\alpha\{q\}$, $\{q\}\beta\{r\}$ の時、$\{p\}(\alpha;\beta)\{r\}$ が成り立つ。

命題11. (Conditional Rule)

$\{p\sqcap q\}\alpha\{r\}$, $\{p\sqcap\neg q\}\beta\{r\}$ の時、$\{p\}$(if q then α else β)$\{r\}$ が成り立つ。

命題12. (Iteration Rule)

$\{p\sqcap q\}\alpha\{q\}$ の時、$\{q\}$(while p do α)$\{(\neg p)\sqcap q\}$ が成り立つ。

命題13. 命題10. の条件と以下の条件は同値である。

$wlp(\alpha, wlp(\beta,r)) \sqsubset wlp(\alpha\beta,r)$

定理14. (Partial Correctness)

任意の関係 $\alpha:X\rightarrow Y$, $\beta:Y\rightarrow Z$ 及び、防御関数 $r:Z\rightarrow Z$ に対して、$wlp(\alpha, wlp(\beta,r)) = wlp(\alpha\beta,r)$ が成り立つ。

命題15. 関係 $\alpha:X\rightarrow Y$ に対して、

(1) $wlp(\alpha,id_Y) = id_X$

(2) $wp(\alpha,id_Y) = d(\alpha)$

(3) $wp(\alpha, 0) = 0$

命題16. 関係 $\alpha:X\rightarrow Y$, 防御関数 $q_1,q_2:Y\rightarrow Y$ に対して、$q_1=\neg\neg q_1$, $q_2=\neg\neg q_2$ ならば、$wlp(\alpha,(q_1\sqcap q_2)) = wlp(\alpha,q_1)\sqcap wlp(\alpha,q_2)$ が成り立つ。

関係$\alpha:X\to Y$が、任意の関係$\tau:U\to X$に対して、$\tau\alpha=0$ならば$\tau=0$が成り立つときに、αを全関係(total)という。関係$\alpha:X\to Y$, $\tau:T\to X$に対して、$\tau\alpha$が全関係となり、さらに任意の関係$\upsilon:U\to X$に対して、$\upsilon\alpha$が全関係となるとき、$\upsilon=\sigma\tau$となる関係$\sigma:U\to T$が唯一存在するときに、τをαの全化射(totalizer)という。

補題16. 関係$\alpha:X\to Y$に対して、

(1) $d(\alpha)=0 \leftrightarrow k(\alpha)=id_X \leftrightarrow \alpha$:全関係

(2) $\alpha\Omega_Y=\Omega_X$ ならばαは全関係である。

定理17. 部分関数$f:X\to Y$が全関係であるとき、任意の関係$\beta:Y\to Z$に対して、$k(f\cdot k(\beta))=d(f\beta)$が成り立つ。

系 18. (Total Correctness)
部分関数$f:X\to Y$が全関係であるとき、任意の関係$\beta:Y\to Z$及び防御関数$q:Z\to Z$に対して、$wp(f\beta,q)=wp(f,wp(\beta,q))$が成り立つ。

系 19. 部分関数$f:X\to Y$に対して、$d(f):X\to X$の定義域単射を$t:E\to X$とすると、tはfの全化射である。すなわち、任意の部分関数は全化射を持つ。

§3. おわりに

プログラムを初等トポス上の関係、表明を防御関数と解釈しプログラムとその前置、後置条件を関係の圏の射の性質によって考察する方法を導入した。その解釈の正当性が関係計算によって示された。また、最弱自由前置条件、最弱前置条件も関係射によって定義され、それらが満たすべきプログラム結合による正当性が圏Relにおける部分正当性、圏Pfnにおける全正当性として証明された。さらに、圏Pfnでの全化射の存在も示された。

[参考文献]

[1] E. W. Dijkstra, A discipline of programming, Prentice-Hall, 1976.

[2] R. Goldblatt, Topoi, The categorial analysis of logic, North-Holland, 1979.

[3] C. A. R. Hoare, An axiomatic basis for computer programming, CACM 12, 1969.

[3] Y. Kawahara, Pushout-complements in the category of graphs, RMC 62-02, Dept. Math. Kyushu Univ., Fukuoka, JAPAN, 1987.

[4] J. Lambek and P. J. Scott, Introduction to higher order categorical logic, Cambridge University Press, 1986.

[5] E. G. Manes and M. A. Arbib, Algebraic approaches to program semantics, Springer-Verlag, 1986.

[6] E. G. Manes, Weakest preconditions: categorial insights, LNCS 240, 1986.

[7] E. G. Wagner, A categorical view of weakest liberal preconditions, LNCS 240, 1986.