# 第5章

# 抽象解释的两个理论模型

第4章比较详细地介绍了模型检验方法。我们知道，抽象解释首先由 Cousot 等于1977年提出，它作为程序设计和程序静态分析的统一框架，现在已经成为描述具体系统近似语义的一个基本方法理论，应用到许多计算机科学领域，其中包括程序检验。

经典抽象解释理论是在 Galois 连接或与之等价的闭包算子的关于抽象论域的框架下进行的，许多学者在这方面做了大量工作。本章将给出抽象解释的两个新的理论模型。因为这两个新模型是基于经典的全总域模型[69]和部分等价模型[70]的理论构造的，所以我们也把它们分别称为抽象解释全总域模型和抽象解释部分等价逻辑关系模型。但为了简便，常把“抽象解释”几个字省略，从上下文看，并不会引起混淆。

全总域模型也是在经典抽象解释理论方向上的工作，但是作为一个综合统一模型，它是对经典抽象解释的总结。就我们所知，它与目前现存的一切有关抽象解释文献所采取的框架是相容和等价的。全总域模型的主要作用如下。

(1) 作为经典抽象解释理论的统一模型，使我们可以进一步讨论一些有关抽象解释理论需要解决的几个基本问题，如完备性问题。

(2) 模型深化了经典抽象理论的一些概念。例如，我们提出了本质函数和亚本质函数概念，对泛型概念进行广义表述，它们在模型检验理论中都是有用的理念。

(3) 模型可以启发我们把抽象解释理论应用到软件工程领域(从设计到实现的过程)，即从抽象设计到具体论域的实践。

如果说，我们提出的抽象解释全总域模型仍然符合传统抽象解释模型范式，是“抽象即简化”思维的发展，那么我们提出的抽象解释部分等价逻辑关系模型却和传统抽象解释模型根本不同，是“抽象即本质”思维的发展。

部分等价逻辑关系模型不像全总域模型那样是对原系统在“近似”意义上的抽象，而是对原系统上的一切关系(包括逻辑关系)在“本质”意义上的抽象。因此，它不是原系统的“简化”，而是原系统的一个“深化”。部分等价逻辑关系模型的主要作用如下。

(1) 模型认为，抽象论域是“部分等价关系”的集聚，而语义操作算子是“逻辑部分等价关系”的集聚。因此，除了要求具体或抽象语义算子具有一定的逻辑关系以外，该模型并不

要求它们具有什么特殊性质，如单调性。

(2) 模型没有从“近似”意义上对具体域进行抽象，而是从“本质”上深化原系统。它分离出原系统的“性质”单元，比原系统可能更复杂。因此，该模型从另外角度深化了我们对抽象解释理论的理解。

(3) 它可以启发我们讨论与传统模型不同的问题，如复杂性和多态性问题。

## 5.1　抽象解释全总域模型

### 5.1.1　构造全总域模型

**1. 具体语义论域**

用 $S$ 表示一个具体系统，其中元素可以是无限的。例如，在经典模型检验中，$S$ 是一个(具体的)Kripke 结构，$S$ 中的元素表示系统的状态。下面我们用状态指称 $S$ 中的元素，假设 $S$ 是可数无限的，并称它为状态空间。我们用 $\wp(S)$ 表示 $S$ 的幂集，用它表示系统 $S$ 的语义论域。$\wp(S)$ 中的元素是 $S$ 的子集，它是 $S$ 中状态组成的集合。对于任意 $a\in\wp(S)$，它可以是 $S$ 中有限子集合或是 $S$ 中无限子集合。即

$$a=\{s_1,s_2,\cdots,s_n\}\text{ 或 }a=\{s_1,s_2,\cdots,s_n,\cdots\}$$

其中，$s_i\in S$ 是 $S$ 中的状态，$i=1,2,\cdots,n,\cdots$。关于 $a$ 的意义叙述如下。

(1) $a$ 可以表示一个(成员关系)谓词 $P$，即每个 $s_i$ 使该谓词 $P$ 为真。如果适当扩展 $\wp(S)$ 和/或 $S$(扩展后仍记为 $\wp(S)$)，则 $a$ 还可以表示一个(任意元)的谓词。

(2) $a$ 可以表示某一属性(性质)$\varphi$，即每个 $s_i$ 具有该属性(或该性质)$\varphi$。为了简单叙述下面引进的语义操作算子的单调性，在考虑属性 $\varphi$ 时，我们限制“否定性质”到基本原子层次上，这和(模型检验)讨论 LTL 逻辑公式时所作的限制一样。

(3) $a$ 可以表示状态空间 $S$ 的某些轨道可达到的状态集合。例如，在考虑程序“不变式”属性时，我们常常是这样做的[64]。当然，$a$ 也可以表示状态空间 $S$ 中的一条(具有某性质)轨道，即 $s_1,s_2,\cdots$ 是从 $s_1$ 出发的一条轨道的顺序出现的状态集合。不过为了表示循环轨道，必须扩展语义域 $\wp(S)$ 和/或 $S$，仍记为 $\wp(S)$，则 $a$ 也可以表示状态空间中的循环轨道。

(4) $a$ 可以表示一个类型 $T$，准确地说，它是类型 $T$ 的值域，即 $a$ 中所有元素 $s_i$ 都属于类型 $T$。

总之，我们在非常广泛的意义上，理解 $\wp(S)$ 中的元素的语义特征，如果需要，还可以扩展 $S$ 和/或 $\wp(S)$ 使它们可以表达更多的内容，如文献[64]的时序模型(Temporal Models)。为了确定起见，我们称 $\wp(S)$ 中的元素为属性，这样也较直观些。同样，我们也可以在 $\wp(S)$ 上建立(一般)格结构。例如，在集合包含的自然序下，$\wp(S)$ 的任意子集都有最小上界和最大下界，所以 $\wp(S)$ 是一个完备格。为了确定起见，不妨认为 $\wp(S)$ 是一个完备

格，且沿用集合论包含符号$\subseteq$，作为格中序关系，并在直观上也把它作为集合包含关系理解。也就是说，$\wp(S)$是权当作在集合论包含自然序下组成的格。但这时，若$a,b\in\wp(S)$，$a\subseteq b$，则认为$a$较$b$更精确，即$b$是$a$的近似。

**2. 抽象语义总域**

在经典抽象解释框架中，依据具体状态幂集的抽象解释，Golois连接和闭包操作是等价的。闭包操作具有独立于抽象元素表示法的优点，如果推理不涉及抽象表示内涵，用闭包操作作为抽象语义领域是比较方便的。因此，我们用$\mathrm{uco}(\wp(S))$表示系统$S$的抽象语义全总域，其中任意元素$\mu\in\mathrm{uco}(\wp(S))$是一个闭包，即$\mu$是具体语义域$\wp(S)$的一个抽象语义域，而全总域$\mathrm{uco}(\wp(S))$是所有抽象语义域的集合。对于闭包$\mu\in\mathrm{uco}(\wp(S))$，它可以从以下两个等价角度定义。

(1) $\mu$是$\wp(S)$上单调、幂等、扩展的操作，因此可以把$\mu$看作函数。即设$a$和$b$是$\wp(S)$中任意两个元素，若$a\subseteq b$，则$\mu(a)\subseteq\mu(b)$(单调性)；$\mu\circ\mu(a)\triangleq\mu(\mu(a))=\mu(a)$(幂等性)；$\mu(a)\supseteq a$(扩展性)。

(2) $\mu$是由它的不动点唯一确定的，且$\mu$在$\wp(S)$上操作的所有不动点组成的集合与$\mu$的像集$\mu(\wp(S))$一致。因此，可以把$\mu$看作$\wp(S)$中的子集合，即

$$\mu(\wp(S))=\{a\in\wp(S)\mid\mu(a)=a\}$$

今后称任意闭包$\mu\in\mathrm{uco}(\wp(S))$，我们互用它的函数和集合两种表示。值得注意的是，$a\in\wp(S)$表示系统$S$某个属性$\varphi$，于是由$\mu\in\mathrm{uco}(\wp(S))$的扩展性$\mu(a)\supseteq a$，就可以认为一个闭包是将一个任意的$a\in\wp(S)$到$a$的满足某个性质的最小超集的映射，而那个最小超集可以看作属性$\varphi$的从上面的一个最“精确”近似。实质上，关于$\mu$的两种等价定义，我们有：$\forall a\in\wp(S),\forall\mu\in\mathrm{uco}(\wp(S)),\mu(a)=\bigcap\{b\mid a\subseteq b\text{ 且 }b\in\mu\}$。

所以，若$\mu(a)=b'$，$b'$就是最接近$a$的一个近似表示。

在经典抽象解释框架下，这种近似就称为抽象。这也是我们称任意闭包$\mu\in\mathrm{uco}(\wp(S))$为具体语义域$\wp(S)$的一个抽象语义域的原因，而$\mathrm{uco}(\wp(S))$就是所有抽象语义域的全总域。

对于任意闭包$\mu\in\mathrm{uco}(\wp(S))$，$\mu$由$S$的子集合组成，按照集合的包含自然序，$\mu$可以构成一个完备格，虽然它未必是$\wp(S)$上的完备子格。若$a,b\in\mu$，$a\subseteq b$，则称$a$较$b$精确，即$b$是$a$的一个近似。对于全总域$\mathrm{uco}(\wp(S))$，我们在抽象域之间规定一个序$\sqsubseteq$，它就是通用的函数之间的逐点序。这样任意两个闭包$\rho,\eta\in\mathrm{uco}(\wp(S))$，$\rho\sqsubseteq\eta$，即$\forall a\in\wp(S)$，都有$\rho(a)\subseteq\eta(a)$(等价地，$\eta(\wp(S))\subseteq\rho(\wp(S))$)，它表示在$\mathrm{uco}(\wp(S))$全总域，$\rho$较$\eta$精确，$\eta$较$\rho$抽象。于是，$\mathrm{uco}(\wp(S))$在逐点序$\sqsubseteq$下也构成一个完备格。

**3. 具体语义操作和抽象语义操作**

我们用$f$表示$\wp(S)$具体语义域上的一个语义操作，为了简单起见，只考虑$f:\wp(S)\to\wp(S)$是$\wp(S)$上的一元单调函数情形。因为对一般情况的单调函数可以类似处理，例如，当我们考虑完备性问题时，文献[46]指出，可以把$n$元函数的完备性问题划归为一组一元函数的完备性问题。更复杂一些，回忆前面说过的扩充$\wp(S)$和/或$S$，可以使$\wp(S)$具有需

要的语义属性，同样能使用递归配对函数或参数分离处理多元函数，甚至利用并行系统还可以处理不确定的语义操作，因此只考虑一元单调函数并不丧失一般性。下面互用语义操作和语义函数两个术语。

对于任意语义函数 $f$，若 $\rho,\eta\in \mathrm{uco}(\wp(S))$ 是两个任意闭包，令

$$f^{\rho,\eta}\triangleq\eta\circ f\circ\rho \tag{5.1}$$

为 $f$ 的关于$\langle\rho,\eta\rangle$的抽象语义操作。在经典抽象解释框架中，$f^{\rho,\eta}$ 为 $f$ 在抽象域 $\rho,\eta$ 上的最正确近似抽象语义操作。注意 $\rho$ 和 $\eta$ 也可以是同一个闭包。

合理性和完备性是经典抽象解释理论里最基本的两个概念[45-47]。

$f$ 是任意具体的语义函数，$\rho$ 和 $\eta$ 是任意两个闭包，$f^{\sharp}:\rho\to\eta$ 是对应的在$\langle\rho,\eta\rangle$上的抽象语义函数，若

$$\eta\circ f\sqsubseteq f^{\sharp}\circ\rho \tag{5.2}$$

则称 $f^{\sharp}$ 为合理抽象语义函数。注意，合理性与近似性等价。由此观之，最正确近似 $f^{\rho,\eta}$ 自动满足式(5.2)，这是由于 $\rho,\eta$ 都是单调函数且满足幂等性的缘故。若 $f^{\sharp}$ 是$\langle\rho,\eta\rangle$上的任意一个合理抽象函数，因为 $\eta\circ f\sqsubseteq f^{\sharp}\circ\rho$，于是 $\eta\circ f\circ\rho\sqsubseteq f^{\sharp}\circ\rho\circ\rho$，根据 $\rho$ 的幂等性，可得 $\eta\circ f\circ\rho\sqsubseteq f^{\sharp}\circ\rho$，再根据 $f^{\rho,\eta}$ 的定义和 $f^{\sharp}$ 的定义域，所以 $f^{\rho,\eta}\sqsubseteq f^{\sharp}$ 关系成立，这也是我们称 $f^{\rho,\eta}$ 是最正确近似的原因。

沿用上面的术语，如果式(5.2)成立，即

$$\eta\circ f=f^{\sharp}\circ\rho \tag{5.3}$$

则称抽象解释 $f^{\sharp}$ 关于 $f$ 在$\langle\rho,\eta\rangle$上是完备的。下面我们将证明这时 $f^{\rho,\eta}$ 关于 $f$ 在$\langle\rho,\eta\rangle$上也是完备的。所以，为了方便，这时也称$\langle\rho,\eta\rangle$关于 $f$ 是完备的。上下文不会混淆，我们互用 $f^{\sharp}$($f^{\rho,\eta}$)完备或$\langle\rho,\eta\rangle$完备两个术语。

更进一步，如果给定$\langle\rho,\eta\rangle$，$f^{\sharp}$ 关于 $f$ 是完备的，则 $f^{\rho,\eta}$ 也是完备的，并且 $f^{\rho,\eta}$ 与 $f^{\sharp}$ 一致。实际上

$f^{\sharp}=$(因为 $\rho,\eta$ 的幂等性)

$f^{\sharp}\circ\rho=$(由 $f^{\sharp}$ 完备性定义：式(5.3))

$\eta\circ f\sqsubseteq$(由 $f^{\rho,\eta}$ 的合理性：式(5.2))

$\eta\circ f\circ\rho\sqsubseteq$(由近似性：$f^{\rho,\eta}\sqsubseteq f^{\sharp}$)

$f^{\sharp}$

鉴于此，式(5.3)也可以改写为 $\eta\circ f=\eta\circ f\circ\rho$(今后将此式也记为式(5.3))。

所以这里只讨论最正确近似抽象 $f^{\rho,\eta}$，除非特殊声明，我们把 $f^{\rho,\eta}$ 简记为 $f^{\sharp}$，即在定义抽象语义操作时，只用式(5.1)。因为 $f^{\sharp}=f^{\rho,\eta}=\eta\circ f\circ\rho$，它是 $\rho\to\eta$ 上相应于 $f$ 的抽象语义函数，所以直观上它是这样的抽象语义函数：首先强制实参 $x\in\wp(S)$为闭包 $\rho$ 中的元素，接着应用 $f$，然后强制结果为闭包 $\eta$ 中的元素。可以看出，若 $x\in\rho$，则 $f^{\rho,\eta}(x)=\eta\circ f\circ\rho(x)\in\eta$，因此，$f^{\rho,\eta}$ 实质上是一个特殊的“具体”语义函数，限制它的定义域和值域分别到 $\rho$ 闭包集合和 $\eta$ 闭包集合上，即 $f^{\rho,\eta}$ 是 $\rho\to\eta$ 函数，是在$\langle\rho,\eta\rangle$上关于 $f$ 的抽象语义

操作。

令$\mathcal{F}=\{f\mid f:\wp(S)\to\wp(S),$(单调)具体语义函数$\}$是所有具体语义函数的集合，用$F\subset\mathcal{F}$表示$\mathcal{F}$的子集合，它是若干个语义操作的集聚。并用$\mathcal{F}^{\#}=\{f^{\#}\mid\exists f\in\mathcal{F},\exists\rho,\eta\in\mathrm{uco}(\wp(S))$，使$f^{\#}=\eta\circ f\circ\rho\}$表示所有抽象语义函数的集合，同样记$F^{\#}\subset\mathcal{F}^{\#}$为相应于具体语义函数集聚$F$的抽象语义函数集聚。

**4. 全总域模型**

按照前面的叙述，实际上我们已经为抽象解释框架构造了一个模型，称为全总域模型，它是一个5元组

$$\mathcal{A}=\{S,\wp(S),\mathrm{uco}(\wp(S)),\mathcal{F},\mathcal{F}^{\#}\}\tag{5.4}$$

其中，每个符号的解释如上所述。

**例5.1** 闭包示例[45,46,71]

$Z$表示整数集合，$\wp(Z)$是$Z$中所有子集合组成的集合。用集合包含关系，$(Z,\wp(Z))$构成具体语义论域体系，它是一个完备格。现在考查经典符号关系，令$0+=\{x\mid x\in Z,x\geqslant 0\}$，$-0=\{x\mid x\in Z,x\leqslant 0\}$，$0=\{0\}$；$\varnothing$表示空集，$Z$表示全集。使用上述符号可以定义$\wp(Z)$上的一个闭包$\rho_s=\{Z,-0,0+,0,\varnothing\}$。

考虑具体逐点乘法运算$*:\wp(Z)^2\to\wp(Z)$，其定义为：$\forall X\in\wp(Z),\forall Y\in\wp(Z)$，$X*Y=\{x\cdot y\mid x\in X,y\in Y\}$，以及抽象乘法运算$*^{\#}:{\rho_s}^2\to\rho_s$。按通常乘法符号法则定义，有$-0*^{\#}0+=-0$；$0*^{\#}0+=0$；$-0*^{\#}-0=0+$，等等。

下面证明，$*^{\#}$关于$*$在$\langle\rho_s^2,\rho_s\rangle$上是完备的。因为，对于$\forall Z_1,Z_2\in\wp(Z)$，有

$$\rho_s(Z_1*Z_2)=\rho_s(Z_1)*^{\#}\rho_s(Z_2)$$

若记$f=*$，则$f^{\#}=*^{\#}$，且把$Z_1*Z_2$写成$*(Z_1,Z_2)$形式，类似地，$\rho_s(Z_1)*^{\#}\rho_s(Z_2)$写成$*^{\#}(\rho_s(Z_1),\rho_s(Z_2))$形式，则上式即为$\rho_s\circ f=f^{\#}\circ\rho_s^2$。它符合完备性定义(式(5.3))，只要在式(5.3)中令$\eta=\rho_s,\rho=\rho_s\times\rho_s=\rho_s^2$即可得到。例如，$\rho_s(\{-1\}*\{-2\})=\rho_s(\{2\})=0+=-0*^{\#}-0=\rho_s(\{-1\})*^{\#}\rho_s(\{-2\})$。于是，用闭包$\rho_s^2$和$\rho_s$描述具体乘法符号规则是适宜的。严格地说，这里所说的$f$和$f^{\#}$的定义域分别是前面定义中情况的扩充。前面只是为了叙述简便，才做了一些简化，并不失一般性。

**例5.2** 全总域示例[45,46,71]

沿用例5.1中的符号，定义$\mathrm{sign}=\{Z,-0,0+,0,\varnothing\}$，现在把sign当作具体域，我们可以考虑sign所有可能的抽象闭包如下。

$\rho_1=\{Z\}$，$\rho_2=\{Z,0+\}$，$\rho_3=\{Z,0\}$，$\rho_4=\{Z,\varnothing\}$，$\rho_5=\{Z,-0\}$，$\rho_6=\{Z,0+,\varnothing\}$

$\rho_7=\{Z,0+,0\}$，$\rho_8=\{Z,0,\varnothing\}$，$\rho_9=\{Z,-0,0\}$，$\rho_{10}=\{Z,-0,\varnothing\}$

$\rho_{11}=\{Z,0+,0,\varnothing\}$，$\rho_{12}=\{Z,-0,+0,0\}$，$\rho_{13}=\{Z,-0,0,\varnothing\}$，$\rho_s=\mathrm{sign}$

于是，uco(sign)在逐点序$\sqsubseteq$下也构成一个完备格。所有可能抽象闭包构成的完备格如图5.1所示。

从上述模型的构造流程中可以看出现今文献关于经典抽象解释所采用的框架，在隐蔽

形式或等价形式下，都与式(5.4)的框架相容。利用式(5.4)模型，至少可以讨论有关抽象解释的大部分重要问题。

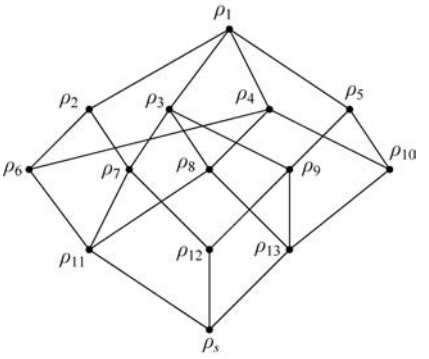


图 5.1　uco(sign)完备格

(转摘于文献[46]图 2)

## 5.1.2　理论性问题

**1. 最优完备存在性**

在式(5.4)框架中，对任意具体语义函数 $f$，无论 $\eta$ 如何确定，只要令 $\rho=\wp(S)$，则式(5.3)成立，即

$$\eta\circ f=\eta\circ f\circ\rho$$

也就是说，只要选择 $\rho=\wp(S)$，对任意的 $f$ 和 $\eta$，抽象语义函数 $f^{\rho,\eta}$ 关于 $f$ 是平凡完备的。

同样，若选择 $\eta=\{S\}$，即 $\eta$ 映射 $\wp(S)$ 任意子集为基本集合 $S$，对于任意 $f\in\mathcal{F}$，任意 $\rho\in\mathrm{uco}(\wp(S))$，式(5.3)也成立，即

$$\eta\circ f=\eta\circ f\circ\rho=\{S\}$$

也就是说，只要选择 $\eta=\{S\}$，$\forall f\in\mathcal{F}$，$\forall\rho\in\mathrm{uco}(\wp(S))$，抽象语义函数 $f^{\rho,\eta}$ 关于 $f$ 是平凡完备的。

根据文献[46]，若$\langle\rho,\eta\rangle$关于 $f$ 完备，$\rho\sqsupseteq\delta\in\mathrm{uco}(\wp(S))$和 $\eta\sqsubseteq\beta\in\mathrm{uco}(\wp(S))$，则$\langle\delta,\beta\rangle$也关于 $f$ 完备。也就是说，若$\langle\rho,\eta\rangle$关于 $f$ 完备，将 $\rho$“精确化”到 $\delta(\delta(\wp(S))\supseteq\rho(\wp(S)))$，将 $\eta$“抽象化”到 $\beta(\beta(\wp(S))\subseteq\eta(\wp(S)))$，则$\langle\delta,\beta\rangle$也关于 $f$ 完备。注意 $\delta$ 和 $\beta$ 是从两个不同方向分别对 $\rho$ 和 $\eta$ 的“改良”，$\rho\rightarrowtail\delta$ 是延展，$\eta\rightarrowtail\beta$ 是简化。

鉴于上述考虑，我们提出最优完备的定义。

**定义 5.1**(最优完备)　设$\langle\rho,\eta\rangle$关于 $f$ 完备，如果对任意关于 $f$ 的完备抽象$\langle\rho',\eta'\rangle$，都有

$$\rho\sqsupseteq\rho',\quad\eta\sqsubseteq\eta'\tag{5.5}$$

则称 $\eta\circ f\circ\rho$ 是 $f$ 的最优完备抽象语义函数，也称$\langle\rho,\eta\rangle$是 $f$ 的最优完备抽象语义域。

根据文献[46]，对于最优完备$\langle\rho,\eta\rangle$，无须进一步对 $\rho$ 在精确化方向和对 $\eta$ 在抽象化方

向分别加以改进。同样，也无法进一步对 $\rho$ 在抽象化方向和对 $\eta$ 在精确化方向分别加以改进，若存在这样的改进$\langle\delta,\beta\rangle$，由于 $\delta$ 是 $\rho$ 的抽象化，即 $\rho\sqsubseteq\delta$，由最优完备定义，$\rho\sqsupseteq\delta$，所以 $\rho=\delta$；由于 $\beta$ 是 $\eta$ 的精确化，即 $\beta\sqsubseteq\eta$，由最优完备定义，$\eta\sqsubseteq\beta$，所以 $\beta=\eta$。

因此，提出以下问题。

**问题 1** 对于具体语义函数 $f$，是否存在它的最优完备抽象语义函数 $f^{\sharp}$，或者它的最优完备抽象语义域？

对于函数族 $F$，若$\langle\rho,\eta\rangle$对于 $F$ 中的每个函数都完备，则称$\langle\rho,\eta\rangle$关于 $F$ 完备。同样，也可以对于函数族 $F$ 定义最优完备问题，即若存在$\langle\rho,\eta\rangle$关于 $F$ 完备，且对任意关于 $F$ 的完备$\langle\rho',\eta'\rangle$，式(5.5)条件成立，则称$\langle\rho,\eta\rangle$是 $F$ 的最优完备抽象语义域。

**问题 2** 对于语义函数族 $F=\{f_1,f_2,\cdots,f_n\}$，是否存在它的最优完备抽象语义域？如果 $\forall i=1,2,\cdots,n$，$\langle\rho_i,\eta_i\rangle$关于 $f_i$ 最优完备，那么 $F$ 的最优完备抽象语义域(如果存在)与$\langle\rho_i,\eta_i\rangle$之间有什么样关系？即能否从$\langle\rho_i,\eta_i\rangle(i=1,2,\cdots,n)$构造 $F$ 的最优完备？

根据文献[46]，设 $F$ 为具体语义函数族，$\rho,\eta\in\mathrm{uco}(\wp(S))$，定义算子 $C_F^{\rho}$ 和 $S_F^{\eta}$ 如下。

$$C_F^{\rho}:\ \mathrm{uco}(\wp(S))\to\mathrm{uco}(\wp(S))$$

其中，$C_F^{\rho}(\eta)\triangleq\sqcap\{\beta\in\mathrm{uco}(\wp(S))\mid\mu\sqsubseteq\beta,\langle\rho,\beta\rangle\text{关于 }F\text{ 完备}\}$。

$$S_F^{\eta}:\ \mathrm{uco}(\wp(S))\to\mathrm{uco}(\wp(S))$$

其中，$S_F^{\eta}(\rho)\triangleq\sqcup\{\delta\in\mathrm{uco}(\wp(S))\mid\delta\sqsubseteq\rho,\langle\delta,\eta\rangle\text{关于 }F\text{ 完备}\}$。

再根据文献[46]，设 $F$ 为具体语义函数族，$\rho,\eta\in\mathrm{uco}(\wp(S))$，若$\langle\rho,C_F^{\rho}(\eta)\rangle$关于 $F$ 完备，则称 $C_F^{\rho}(\eta)$是关于 $F$ 相对于 $\rho$ 的 $\eta$ 完备核；若$\langle S_F^{\eta}(\rho),\eta\rangle$关于 $F$ 完备，则称 $S_F^{\eta}(\rho)$是关于 $F$ 相对于 $\eta$ 的 $\rho$ 的完备壳。

根据 $S_F^{\eta}(\rho)$的定义，可知 $S_F^{\eta}(\rho)$是一切满足定义的 $\delta(\delta\sqsubseteq\rho)$的上确界，于是 $S_F^{\eta}(\rho)\sqsubseteq\rho$，若它是(相对于 $\eta$ 关于 $F$)$\rho$ 的完备壳，则$\langle S_F^{\eta}(\rho),\eta\rangle$是$\langle\rho,\eta\rangle$在 $\rho$ 上向精确化方向的一次改良。

同样，$C_F^{\rho}(\eta)\sqsupseteq\eta$，若它是(相对于 $\rho$ 关于 $F$)$\eta$ 的完备核，则$\langle\rho,C_F^{\rho}(\eta)\rangle$是$\langle\rho,\eta\rangle$在 $\eta$ 上向抽象化方向的一次改良。

**问题 3** 给定具体语义函数族 $F$，其最优完备(如果存在的话)$\langle\rho,\eta\rangle$能否通过初始化 $\rho=\{S\}$，$\eta=\wp(S)$递归运用 $S_F^{\eta}(\rho)$、$C_F^{\rho}(\eta)$算子分别对 $\rho$ 在精确化方向、对 $\eta$ 在抽象化方向进行改良而得？

**2. 最优函数存在性**

回忆前面关于抽象语义函数 $f^{\sharp}=\eta\circ f\circ\rho$ 的解释，对于给定的闭包 $\rho,\eta\in\mathrm{uco}(\wp(S))$，仿照 $\lambda$ 演算，定义

$$\rho\to\eta\triangleq\lambda f:\mathcal{F}.\,\eta\circ f\circ\rho \tag{5.6}$$

其中，$f:\mathcal{F}$，表示 $f\in\mathcal{F}$，其直观意义是所有的关于闭包$\langle\rho,\eta\rangle$上的抽象语义函数的集合。现在我们证明 $\rho\to\eta$ 中的元素是外延的。

$\rho\to\eta$ 的任务是取任意具体语义函数 $f$，并产生这样的函数 $\eta\circ f\circ\rho$，即它把每个函数 $f$

强制为从$\rho$的值域到$\eta$的值域的抽象函数。因此，若对所有$x\in\rho$，有

$$(\eta\circ f_1\circ\rho)x=(\eta\circ f_2\circ\rho)x$$

又注意到限制$x\in\rho$是无关紧要的，所以$\forall x\in\wp(S)$，都有$(\eta\circ f_1\circ\rho)x=(\eta\circ f_2\circ\rho)x$，于是

$$\lambda x.(\eta\circ f_1\circ\rho)x=\lambda x.(\eta\circ f_2\circ\rho)x \tag{5.7}$$

根据复合的意义，在式(5.7)成立的意义上，应该有$\eta\circ f_1\circ\rho=\eta\circ f_2\circ\rho$，这意味着$\rho\to\eta$的值域对于每个在$\wp(S)$上入射$\rho$到$\eta$的单调函数恰好包含一个代表，这说明$\rho\to\eta$模型是外延的。下面的讨论就是基于上面叙述的直观意义，把$\rho\to\eta$看作关于闭包$\langle\rho,\eta\rangle$上的抽象语义函数的集合。

可以看出，若$f$已经是一个从$\rho$到$\eta$的(具体)语义函数，也就是说，一旦$x\in\rho$，就有$f(x)\in\eta$，那么对所有的$x\in\rho$，有$f^{\#}(x)=\eta\circ f\circ\rho(x)=f(x)$，基于这样的观察，我们引入下面的定义。

**定义 5.2**(本质函数和亚本质函数)

(1) 若对任意$\forall x\in\rho$，$f(x)=f^{\#}(x)\in\eta$，则称$f$是$\rho\to\eta$中的本质(具体)函数。换言之，把$f$的定义域限制到$\rho$闭包上，记为$f_{\downarrow\rho}$，则$f_{\downarrow\rho}\equiv f^{\#}$。

(2) 若对任意$\forall x\in\wp(S)$，$\eta\circ f=f^{\#}=\eta\circ f\circ\rho$，则称$f$是$\rho\to\eta$中的亚本质(具体)函数。对于亚本质函数$f$，$\langle\rho,\eta\rangle$是完备的抽象语义域。

因此，(亚)本质函数是$\rho\to\eta$类中的特殊函数族。直观意义是，设计一个系统(检验一个系统也一样)时，我们对系统的特性、功能和行为都应有一个预先的设想，这些设想就是抽象语义域及其在抽象域上的操作。当我们实现系统时，具体的语义域及其上的操作受到技术及其环境的限制，自然要复杂迂回得多。所以，本质函数和亚本质函数反映了理想操作的忠实可靠的实现。在这个意义上，它们都是最优函数族。

**问题 4**　如果$\rho$和$\eta$抽象语义域构想完美，能否解决技术上的问题，使实现$\rho$和$\eta$的具体语义域上的操作都是本质函数或亚本质函数？或者说，能否改进具体语义操作到至多是只用亚本质函数就能解决的实际问题(如完备性)？

在一般意义上，$\langle\rho,\eta\rangle$抽象域比具体语义域$\wp(S)$简单，而$\rho\to\eta$上的抽象语义函数也比$\wp(S)\to\wp(S)$上的具体语义函数少。所以在模型检验应用中，我们从两方面(域和操作)做了简化，只要解决了完备性问题，那么模型检验中的高期望强保留特性就能满足。

可惜的是，从问题1到问题4，至今仍然没有“彻底”解决。文献[46]指出：以可能最好的方式，即最小化延展或简化正在考虑的抽象域和操作算子，使抽象解释完备，仍然是一个开放问题。甚至，寻找某些合理的很强的条件施加于具体语义域和/或具体操作算子，使抽象域的不动点完备壳存在，一般来说都是不能保证的。因此，对于上述问题，是否能够定义某种“近似”标准和“近似”计算，寻找相关问题的某种意义上的“最优”解决，这些都是值得探讨的。

**3. 与不可预知多态模型类比**

简写$\mathcal{V}=\mathrm{uco}(\wp(S))$，并用记号$\rho:\mathcal{V}$表示$\rho\in\mathrm{uco}(\wp(S))$，定义

$$\to^{\#}\triangleq\lambda\rho:\mathcal{V}.\lambda\eta:\mathcal{V}.(\lambda f:\mathcal{F}.\eta\circ f\circ\rho) \tag{5.8}$$

表示所有的抽象函数的集合。式(5.8)表明它可以看作式(5.4)全总域模型$\mathcal{A}$中的元素$\mathcal{F}^{\sharp}$，即$\rightarrow^{\sharp}=\mathcal{F}^{\sharp}$。

改写$\rightarrow^{\sharp}$为$\forall$，即

$$\forall=\lambda f:\mathcal{F}.(\lambda\rho:\mathcal{V}.\lambda\eta:\mathcal{V}.\eta\circ f\circ\rho)=\lambda f:\mathcal{F}.(\lambda\langle\rho,\eta\rangle:\mathcal{V}\times\mathcal{V}.\eta\circ f\circ\rho) \tag{5.9}$$

于是，$\forall f$的定义域为$\mathcal{V}\times\mathcal{V}=\mathrm{uco}(\wp(S))\times\mathrm{uco}(\wp(S))$，值域为$\{\eta\circ f\circ\rho\}$，即

$$\forall f=\lambda\langle\rho,\eta\rangle:\mathcal{V}\times\mathcal{V}.\eta\circ f\circ\rho:\mathcal{V}\times\mathcal{V}\rightarrow\eta\circ f\circ\rho \tag{5.10}$$

直观上，$\forall f$是抽象函数族，它是具体操作$f$的泛化，在不同的$\langle\rho,\eta\rangle$上呈现出不同的特性，具有多态特征。在某种意义上，它体现了多态性或泛型性。

现在扩展式(5.4)的全总域模型$\mathcal{A}$如下，扩展后记为$\mathcal{A}'$。

$$\mathcal{A}'=\{S,\wp(S),\mathrm{uco}(\wp(S)),\mathcal{F},\mathcal{F}\sharp,\{\rho\rightarrow\eta\},\{\forall f\}\} \tag{5.11}$$

$\mathcal{A}'$是7元组，其中符号是自明的。例如，$\{\rho\rightarrow\eta\}$是一切形如式(5.6)定义的函数族的集聚，其中$\rho\rightarrow\eta$是在固定的闭包对$\langle\rho,\eta\rangle$上讨论每个具体操作相应的抽象操作，重点是具体操作和抽象操作之间的对应关系；$\{\forall f\}$是一切形如式(5.10)定义的函数族的集合，其中$\forall f$是讨论具体操作$f$的在每对$\langle\rho,\eta\rangle$闭包上的多态表现，即$\forall f$是$f$的泛型。

式(5.11)模型总的想法是：一个多态函数是一种可以作用在多种“类型”实参上的函数。在某种意义上，该多态函数在各个类型上使用了“本质同样的算法”。例如，对于具体语义函数$f$，式(5.10)定义的$\forall f$，它可以作用在所有“类型”的$\langle\rho,\eta\rangle$上，因为在每个$\langle\rho,\eta\rangle$上，它都是相应于$f$的抽象语义函数$\eta\circ f\circ\rho$，所以它们的算法在本质上具有“共性”。关于它的具体实例可以参考文献[39]中的$\mathcal{P}_{\omega}$模型。

随着网络技术的发展，现代社会已经处于一个信息爆炸的时代。为了能够从大量数据中寻找有意义的新的关系和模式，数据挖掘技术从而诞生。事实上，人类研究自然现象、社会现象，大都采用一般途径。根据大量经验数据，通过各种定性分析或定量分析，对数据加以整理，归纳产生抽象解释，进一步将这种抽象解释总结成理论，甚至上升到“定律”高度。如果从这个角度考虑问题，式(5.4)和式(5.11)所示的模型还具有方法论意义。

数据挖掘是指从大型数据库中提取潜在有用的知识，将这些知识表达为概念、规则、规律和模式等形式。抽象解释也和人类认知思维类似，从大量的数据中提取感兴趣的知识，加以抽象，上升为模型。

前面提出的问题1到问题3，都是立足在$\{\rho\rightarrow\eta\}$上讨论，怎样改良$\langle\rho,\eta\rangle$使具体语义函数和抽象语义函数之间满足(例如)完备性关系；而问题4立足于$\{\forall f\}$，讨论怎样设计良好操作，使它具有“安全”的泛型，即它一切泛化都具有完备特性。再把$\mathcal{A}'$与文献[39]相比较，$\mathcal{A}'$与其使用$\mathcal{P}_{\omega}$的闭包构造出来的模型在许多方面都是类似的。实际上，$\mathcal{A}$和$\mathcal{A}'$模型都是受到文献[39]的启发构造出来的。文献[39]构造的模型是$\lambda^{\rightarrow,\forall}$(不可预知多态)模型，因此有以下问题。

**问题5** 基于$\mathcal{A}'$，能否构造一个有关抽象解释的计算理论？

综上所述，针对现有的抽象解释理论构造了一个统一模型，并把它称为抽象解释全总域模型。在该模型上，可以很方便地讨论经典抽象理论的一些问题，如完备性问题等。并且在

该模型的基础上，提出了本质函数和亚本质函数的概念，以及对泛型概念给出了其广义表达方式。这个模型一方面可以深化我们对经典抽象理论概念的理解，另一方面可以作为抽象解释理论的基础。如果以上提出的开放性问题能够得到解决，那么通用性模型将有助于人们处理各个应用领域中存在的复杂结构及特性等问题。

## 5.2　抽象解释部分等价逻辑关系模型

现在采取另外的观点，认为抽象论域是“部分等价关系”的集聚，而语义操作算子是“逻辑部分等价关系”的集聚，提出一个新模型-部分等价逻辑关系模型。这个模型除了要求具体或抽象语义算子具有一定的逻辑关系以外，并不要求它们具有什么特殊性质，如单调性，因此它与传统模型不同，同样也与全总域模型不同。尤为重要的是，该模型并没有从“近似”意义上对具体域进行简化，反而是从“性质”上深化原系统，在某种意义上，它分离出原系统的“性质”单元，比原系统可能要复杂些。因此，基于这样的模型，可以讨论与传统模型不同的问题，如复杂性和多态性问题，从而深化我们对抽象解释理论的理解。

### 5.2.1　具体语义域和语义函数

用 $S$ 表示一个(可能是无限)的具体系统，例如在模型检验中，经典的方式通常将系统 $S$ 表达为一个 Kripke 结构，$S$ 中的元素表示具体系统的状态。以下称 $S$ 中的元素为状态，并认为 $S$ 是可数无限的，称 $S$ 为(具体)状态空间。

通常，系统 $S$ 由许多组件组成，各个组件内部和各个组件之间都存在着一定的关系，下面用部分等价关系和逻辑部分等价关系分别概括组件内部的元素性质和组件内部元素之间以及组件和组件之间的相互作用。首先引入几个概念。

(1) 部分等价关系 per 的含义就是一个成员关系谓词和一个等价关系[39]。具体地说，系统 $S$ 上的一个部分等价关系是 $S$ 的某个子集上的等价关系。例如，序偶$\langle S', R\rangle$，其中 $S' \subseteq S$，且 $R \subseteq S' \times S'$是一个等价关系。然而，由于只通过 $S' = \{a \mid aRa\}$就可以决定 $S'$，所以子集 $S'$在技术上是多余的。注意到，$R$ 是子集 $S'$上的等价关系，当且仅当 $R$ 在(全域)$S$ 上是对称和传递的。因此，一个部分等价关系是一个 $S$ 上的对称和传递关系。部分等价关系的一个直接有用的事实是：对于任意 per $R$，若 $aRb$，则 $aRa$[39]。今后当我们说 $R$ 是一个部分等价关系时，用$|R| \triangleq \{a \mid aRa\}$指代 $R$ 在其上是一个等价关系的子集 $S'$。

(2) 若 $S$ 上的一个部分等价关系是逻辑关系时，则称此部分等价关系为逻辑部分等价关系。逻辑关系和逻辑部分等价关系的定义可以参阅文献[39]。粗略地说，文献[39]认为，逻辑关系 $R$ 在本质上是类型化关系的集聚$\{R^{\sigma} \mid \sigma$ 是一个类型$\}$，使类型 $\sigma \to \tau$ 的关系 $R^{\sigma \to \tau}$ 以保证在作用和 $\lambda$ 抽象下闭合的方法意义上由关系 $R^{\sigma}$ 和 $R^{\tau}$ 确定。类似部分等价关系 per 的定义，逻辑部分等价关系(逻辑 per)$R$ 是指它使每个 $R^{\sigma}$ 是对称和传递的。我们的模型主要是在思想原理上借用上述概念阐述的理念。

下面举例阐述本章用到的有关函数之间的逻辑关系的含义。设 $f, g: A \to B$ 是映射 $A$

到 $B$ 上的两个函数，如 $A$ 内和 $B$ 内元素之间分别存在关系 $R$，$T$，若 $\forall x, y \in A$，$xRy$，都有 $f(x), g(y) \in B$ 且 $f(x)Tg(y)$，则称 $f$，$g$ 满足 $A \to B$ 上关于函数的逻辑关系。注意，在函数的逻辑关系定义中，并没有考虑 $R$ 和 $T$ 的 per 性。但在下面我们将看到，当考虑系统所有部分等价关系“对”上的函数逻辑关系时，如果上述函数逻辑关系是所讨论的系统中的一个对称和传递关系，则称它为（函数）逻辑部分等价关系，这里只用到此类型的逻辑 per。

下面构造具体语义域及其上的语义操作算子。

用 $\{R\}$ 表示 $S$ 上所有部分等价关系集聚，更直观些，$\{R\} = \{\langle S', R\rangle\}$，其中序偶 $\langle S', R\rangle$，表示 $R$ 是 $S$ 的子集 $S'$ 上的等价关系，即 $|R| = S'$。下面互用 $\{R\}$、$\{\langle S', R\rangle\}$ 和 $\{\langle |R|, R\rangle\}$ 等记号。$\{R\}$ 就是我们在 $S$ 上构造出来的具体语义域，简记为 $\mathcal{U}$，即 $\mathcal{U} = \{R\} = \{\langle S', R\rangle\} = \{\langle |R|, R\rangle\}$。需要强调的是，也有可能在一个子集 $S'$ 上存在不同的等价关系。例如，有两个等价关系 $R_1$ 和 $R_2$，则 $\langle S', R_1\rangle$ 和 $\langle S', R_2\rangle$ 应视为是 $\mathcal{U}$ 中的不同元素。当把部分等价关系看作全域上的一个对称和传递关系时，更容易理解上述规定。

设 $\langle S_1, R_1\rangle$ 和 $\langle S_2, R_2\rangle \in \mathcal{U}$，只讨论从 $S_1$ 到 $S_2$ 满足以下性质的函数，$f: S_1 \to S_2$，即对任意 $x, y \in S_1$，且 $xR_1y$，有 $f(x), f(y) \in S_2$ 且 $f(x)R_2f(y)$。直观上看，$f$ 和它自身满足 $S_1 \to S_2$ 上的函数逻辑关系。为了强调此种类型逻辑关系，特别用符号 $f: \langle S_1, R_1\rangle \to \langle S_2, R_2\rangle$ 表示满足上述性质的函数，并称 $f$ 为从 $\langle S_1, R_1\rangle$ 到 $\langle S_2, R_2\rangle$ 上的语义函数（或语义算子），有时简称它为从 $S_1$ 到 $S_2$ 的语义函数（操作），如果不会产生歧义，简称 $f$ 为函数。注意在上述定义中，也有可能 $\langle S_1, R_1\rangle = \langle S_2, R_2\rangle$，即它们是同一个部分等价关系，这时 $f$ 就是一个部分等价关系内部的语义操作。也就是说，部分等价关系内部以及部分等价关系之间的操作，我们都视为满足函数逻辑关系的操作。

用符号 $[\langle S_1, R_1\rangle \to \langle S_2, R_2\rangle]$（或简记为 $[R_1 \to R_2]$）表示从 $\langle S_1, R_1\rangle$ 到 $\langle S_2, R_2\rangle$ 所有语义操作的集合，在 $[\langle S_1, R_1\rangle \to \langle S_2, R_2\rangle]$ 集合上定义一个等价关系如下：即若 $f, g \in [\langle S_1, R_1\rangle \to \langle S_2, R_2\rangle]$，对 $\forall x, y \in S_1$，$xR_1y$，有 $f(x), g(y) \in S_2$，且 $f(x)R_2g(y)$，也就是我们前面所说的 $f$，$g$ 满足 $S_1$ 到 $S_2$ 上函数逻辑关系，显然如此定义的关系是等价关系。

用符号 $\mathcal{U} \to \mathcal{U} = \{[\langle S_1, R_1\rangle \to \langle S_2, R_2\rangle]\}$ 表示系统 $S$ 所有的语义操作的集合，则上面在 $[\langle S_1, R_1\rangle \to \langle S_2, R_2\rangle]$ 上定义的等价关系（即 $S_1 \to S_2$ 的函数逻辑关系）就是整个讨论的 $\mathcal{U} \to \mathcal{U}$ 上的一个逻辑部分等价关系。今后记语义操作集合 $\mathcal{U} \to \mathcal{U}$ 上的一个部分等价关系为 $R \to T$，它是 $[R \to T] = [\langle |R|, R\rangle \to \langle |T|, T\rangle]$ 上的等价关系。因此，$\mathcal{U} \to \mathcal{U}$ 上的部分等价关系详细写出来应是一个序偶 $\langle [R \to T], R \to T\rangle$，但我们简写它为 $R \to T$，因为对这个序偶的成员关系谓词，有

$$[R \to T] = \{f \mid f(R \to T)f\}$$

它也可以通过 $R \to T$ 唯一确定。

鉴于我们的目的是“关注”（部分）逻辑关系，所以常常局限语义操作算子集合 $\mathcal{U} \to \mathcal{U}$ 为其上的部分等价关系的集聚。即使这样，为了节省符号，仍然用 $\mathcal{U} \to \mathcal{U}$ 符号表示。总之，对于具体系统，在其状态空间上规定了语义域 $\mathcal{U} = \{R\} = \{\langle |R|, R\rangle\}$ 以及语义操作算子集合 $\mathcal{U} \to \mathcal{U} = \{(R \to T)\} = \{\langle [R \to T], R \to T\rangle\}$。直观上，$\mathcal{U}$ 中的每个 per 表示系统中一些元素间

的某个固有性质关系，而$\mathcal{U}\to\mathcal{U}$中的每个 per 表示系统中一些元素之间的动态联系或相互作用的关系。注意，这里的符号虽然有点混用，即现在仍用$\mathcal{U}\to\mathcal{U}$表示所有函数逻辑部分等价关系的集合，通过上下文应不至于混淆。

### 5.2.2　抽象解释

首先引入几个概念和符号。

(1) 因为一个 per $R\subseteq S\times S$ 是一个子集$|R|=\{s\mid sRs\}$上的等价关系，这样的 per $R$ 的“元素”就是等价类$[s]_R=\{t\mid sRt\}$，对于 $s\in|R|$[39]。

(2) 因为一个逻辑 per $R\to T\in\mathcal{U}\times\mathcal{U}$是一个函数子集$[R\to T]$上的等价关系，因此 $R\to T$ 中的“元素”就是等价类$[f]_{R\to T}=\{g\mid f(R\to T)g\}$，对于 $f\in[R\to T]$。

下面构造抽象语义域和抽象语义操作。

对每个 per $R\subseteq S\times S$，它的成员关系谓词成立的集合为$|R|$，令$|R|^*$由$|R|$中元素的等价类组成，即$|R|^*=\{[s]_R\mid s\in|R|\}$。于是，如果 $R^*$ 为 $R$ 的抽象，它也应为$|R|^*$上的等价关系，显然，$R^*$ 应是$|R|^*$上的恒等关系。直观上，在抽象层次上，$R^*$ 与$|R|^*$应视为等同，即原先在$|R|$上的等价关系 $R$ 已经转变为$|R|^*$上恒等关系 $R^*$。于是令$\mathcal{U}^*=\{R^*\}=\{\langle|R|^*,R^*\rangle\}$，$R^*$ 就是$\mathcal{U}^*$上的一个部分等价关系，它相应于$\mathcal{U}=\{R\}$中具体的 per $R$。特别地，若 $R_1$ 与 $R_2$ 都具有相同的成员关系谓词 $S'$，则$|R_1|^*$和$|R_2|^*$应视为两个不同的集合，前者为$\{[s]_{R_1}\mid s\in S'\}$，后者为$\{[s]_{R_2}\mid s\in S'\}$。对于元素 $s\in S'$，$[s]_{R_1}$ 和$[s]_{R_2}$是 $s$ 在 $S$ 中不同的两个副本。

类似地，若记$[R\to T]^*$为$[R\to T]$上(函数)元素等价类的集合，$[R\to T]^*=\{[f]_{R\to T}\mid f\in[R\to T]\}$，则应定义 $R\to T$ 的抽象$(R\to T)^*$是$[R\to T]^*$上的恒等关系。在抽象层次上，$(R\to T)^*$与其成员关系谓词成立的集合$[R\to T]^*$等同。若记$(\mathcal{U}\to\mathcal{U})^*=\{(R\to T)^*\mid(R\to T)^*$是$[R\to T]^*$上的恒等关系$\}$，则$(R\to T)^*$就是$(\mathcal{U}\to\mathcal{U})^*$论域上的一个部分等价逻辑关系。今后称$(R\to T)^*$中的元素$[f]_{R\to T}$是抽象语义操作算子，$(\mathcal{U}\to\mathcal{U})^*$是相应于所有具体语义操作算子的抽象语义操作算子集合。特别要强调的是，$[f]_{R\to T}$实际上是$|R|^*\to|T|^*$上的函数，即把原先定义在$|R|\to|T|$上的函数转化为该函数所属等价类$[f]_{R\to T}$表达的一个从$|R|^*$到$|T|^*$的函数，而且与等价类$[f]_{R\to T}$的代表无关。

总结如下：对应于具体状态空间 $S=\{s\}$，具体语义域$\mathcal{U}=\{R\}$，具体语义操作算子集聚$\mathcal{U}\to\mathcal{U}=\{R\to T\}$，我们定义抽象状态空间 $S^*=\{[s]_R\mid\exists R,s\in|R|\}$，抽象语义域$\mathcal{U}^*=\{R^*\mid$视$R^*=\{[s]_R\mid s\in|R|\}\}$，抽象语义算子集聚$(\mathcal{U}\to\mathcal{U})^*=\{(R\to T)^*\mid$视$(R\to T)^*=\{[f]_{R\to T}\mid f\in[R\to T]\}\}$。这样，便构造了抽象解释的一个部分等价关系模型，它是一个六元组

$$\mathcal{A}=\{S,\mathcal{U},\mathcal{U}\to\mathcal{U},S^*,\mathcal{U}^*,(\mathcal{U}\to\mathcal{U})^*\}$$

这个模型的优点是它并不要求具体的或抽象的语义操作算子有特殊的性质(如单调性)，它只反映系统功能上的逻辑关系。所以，这里的抽象并不是经典意义上的抽象，经典处

理方法大致把对具体状态的某种近似称为抽象，并要求具体语义域和抽象语义域是特殊的数学结构，如是格或 cpo，这是由“近似”作为抽象的基本内涵所致。而这个模型利用部分等价关系和逻辑部分等价关系，把具体系统 $S$ 从语义域和语义操作两个方面结构化，即把它们的组件一一析取出来，最后形成在$\{[s]_R\}$集合上讨论语义域和语义算子，其中语义域$\mathcal{U}^*$由$\{[s]_R\}$上的一些子集组成，即$\mathcal{U}^* \subseteq \wp(\{[s]_R\})$，而语义算子便是定义在$\mathcal{U}^*$上的一些(部分)函数。

### 5.2.3 理论问题

**1. 复杂性问题**

从前面的叙述不难看出，$\forall f \in [R \to T]$，$[f]_{R\to T}$ 在功能上与 $f$ 完全一致，所以在我们的模型中并不存在经典抽象框架中遇到的完备性问题。然而，我们的模型却存在另一个问题。表面上抽象状态$[s]_R$是具体状态的一个等价类，似乎把状态空间 $S=\{s\}$换成抽象状态空间 $S^*=\{[s]_R\}$时，已经对具体状态空间进行了压缩。但事实并非如此，当 $S' \subset S$ 上存在不同的(部分)等价关系，或者 $s \in S$ 使不同的部分等价关系成员关系谓词成立时，则 $S^*$ 中便存在许多形如$[s]_{R_1}$，$[s]_{R_2}$，…的副本。同样，对于操作函数也有类似的情况。例如，$f: S \to S$ 是这样的函数，当它局限到$|R_1| \to |T_1|$时，$f \in [R_1 \to T_1]$，也许它能局限到$|R_2| \to |T_2|$成为$[R_2 \to T_2]$中的一个函数，即 $f \in [R_2 \to T_2]$，于是在抽象结构中，也有$[f]_{R_1\to T_1}$，$[f]_{R_2\to T_2}$，…等副本。特别地，在全域 $S$ 上，因恒等关系 $I$ 是一个等价关系，所以可以视$\langle S, I\rangle$为一个特殊的部分等价关系，这样抽象结构也可能有$[f]_{I\to I}$这个副本。前面已经说过，部分等价关系模型是非常细致地把原系统的组件按照特征析取出来，当考虑不同特征时，“同一”实体往往分离成“不同”的实体，因此，我们提出如下问题。

能否选取适当的部分等价关系和逻辑部分等价关系，使抽象结构不至于太庞杂？更进一步，能否在此抽象结构上，再使用基于“近似”意义的抽象解释手段，进行传统上的分析？

**2. 与多态的关系**

固定某一操作算子 $f: |R| \to |T|$，能否将它扩展使之成为$\mathcal{U} \to \mathcal{U}$中不同元素中的成员，即在抽象结构中，应该有 $f$ 的不同版本：$[f]_{R\to T}$，$[f]_{R'\to T'}$，$[f]_{R''\to T''}$，…。这与程序设计语言多态理论有点相似。实际上，我们的模型就是受到$\lambda^{\to,\forall}$的部分等价关系模型[39]的启发构造的(尽管与它在许多地方不同)。另外，文献[72]也提出了基于特殊定义的 per 发展的抽象解释的框架，但是它与我们模型的立足点是不同的。现在把上面的叙述总结为如下问题。

对任意的 $f$，能否将它的逻辑功能泛化，使之在系统中不同的满足一定性质(表达为部分等价关系)的组件上都发挥相应的功能？

抽象解释的部分等价逻辑关系模型是基于部分等价关系和逻辑部分等价关系的一个模型。该模型认为抽象领域是“部分等价关系”的集聚，语义操作算子是“逻辑部分等价关系”的集聚。在该模型上，可以很方便地讨论经典抽象理论的一些问题，如复杂性和多态性问题等。这个模型一方面可以深化我们对经典抽象理论概念的理解，另一方面可以作为抽象解释理论的基础。