$[\alpha_1,\alpha_2]$1-概率拟 Hoare 逻辑及其可靠性证明

吴新星[1] 胡国胜[1] 陈仪香[2]
(上海电子信息职业技术学院计算机应用系 上海 201411)[1]
(华东师范大学教育部软硬件协同设计技术与应用工程研究中心 上海 200062)[2]

摘 要 基于 C. A. R. Hoare 提出的 Hoare 逻辑,给出了$[\alpha_1,\alpha_2]$1-概率拟 Hoare 逻辑,并证明了其可靠性。

关键词 Hoare 逻辑,Hoare 三元组,正确度,概率测度
中图法分类号 TP3-0 **文献标识码** A

$[\alpha_1,\alpha_2]$1-Probabilistic Quasi-Hoare Logic and its Reliability

WU Xin-xing[1] HU Guo-sheng[1] CHEN Yi-xiang[2]
(Department of Computer, Shanghai Technical Institute of Electronics & Information, Shanghai 201411, China)[1]
(Soft/Hardware Co-design Engineering Research Center MoE, East China Normal University, Shanghai 200062, China)[2]

Abstract A Hoare logic-baesed $[\alpha_1,\alpha_2]$1-probabilistic quasi-Hoare logic was presented, and its reliability was proved.

Keywords Hoare logic, Hoare triple, Correctness degree, Probability measure

1 引言

C. A. R. Hoare 基于 R. W. Floyd 在 1967 年发表的工作"给程序赋义(Assigning Meanings to Programs)"[1,2],提出了一种形式化处理程序的方法——Hoare 逻辑[3-5]。它不仅能够证明程序的性质,而且还能用于解释程序结构的含义[3-5]。Hoare 的这种"以公理或是规则来表示程序结构的含义,并说明如何证明程序性质"[6]的方法被称为公理语义。

Hoare 提出的逻辑,是一种可以对程序正确性进行证明的形式化方法。如下面的程序 $x:=x+1$ 可以通过 Hoare 逻辑证明理论上是正确的:

$$\{x\geqslant 0\}x:=x+1\{x\geqslant 1\} \tag{1}$$

但是,我们说实际程序的实现还需要借助于一定的硬件设备或物理条件,而在程序的执行过程中这些相关设备或条件未必能保证完全可靠。因此,如果将上面的程序例子(1)放到实际环境中执行,就有可能会出错。如,将 $x:=x+1$ 在计算机上执行,运行 $x:=32767+1$(x 的数据类型为 signed short int),我们发现由于数据溢出等原因,实际的执行结果可能为 -32767,是错误的。又如:

$$\{0\leqslant x\leqslant 1000\}x:=x^2\{0\leqslant x\leqslant 1000000\} \tag{2}$$

表 1 所列的程序 Square. c 100%实现了上面的(2)吗?事实上,我们说一个程序的运行依赖于环境,很可能在有些环境下程序的运行是正确的,但在其它的环境就未必正确。根据不同的实际运行环境,如,在 16 位、32 位或是 64 位计算机上,程序 Square. c 被实现程度可能会不一样。再如下面的例子:

例 1 在 32 位计算机上的程序满足:

$$\{0\leqslant x\leqslant 192\}x:=x^2\{0\leqslant x\leqslant 32767\} \tag{3}$$

表 1 程序 Square. c

```
int main(void)
{
    int x;
    printf("Enter the number x\n");
    scanf("\%d",\&x);
    x=x*x;
    printf("\%d",x);
    return 0;
}
```

将上面的(3)移植到 64 位计算机上,实现情况会怎么样?

还有,使用 C 语言在计算机(数据类型是 long double)计算 25! 时,实际往往可能因数据溢出等原因而出现问题,导致结果是不正确的。

出现这些情况的根本原因是 Hoare 逻辑是不考虑环境的。因此我们说,对具体的实际执行而言,Hoare 逻辑是理想化的,它描述程序正确性的方法本质上是绝对的。在 Hoare 逻辑框架下,程序本身只有两种属性:正确或者是错误。

注意到 Hoare 逻辑理论上证明是正确的程序,实际执行时却可能会出现错误以及 Hoare 逻辑不考虑环境等情况。接下来,基于经典 Hoare 逻辑,我们先研究、讨论如下的问题:

(1)若所给的条件比最弱前置还要弱

程序的执行局限于一定的物理设备和条件等,而这些相关的物理设备和条件未必完全可信。注意到这种情况,我们考虑如下的理论问题:

假定有经典的 Hoare 三元组 $\{A\}c\{B\}$,其中,A 是 $c\{B\}$ 的最弱前置,且有 $A\Rightarrow A'$。如果以 A' 替换 $\{A\}c\{B\}$ 中的 A,那么程序 c 就会出现虽然当前状态满足 A,但是 c 未必能正确执行的情况。此时,被修改后的"三元组" $\{A'\}c\{B\}$ 的语义如何来描述?

吴新星(1981—),男,博士,工程师,CCF 会员,主要研究方向为形式化方法、随机过程,E-mail: xinxingwu@yeah. net;**胡国胜**(1965—),男,博士,教授,主要研究方向为机器学习、负荷预测;**陈仪香**(1961—),男,博士,教授,主要研究方向为物联网、实时协同规范语言设计、程序语义模型、软件可信度量与评估理论。

(2)若所给的条件比最强后置还要强

从程序的使用者(或是说用户)角度出发,程序的执行结果不满足其使用者的要求(出现这种现象有两种原因:1)程序执行的结果出错了;2)程序虽然执行没有出错,但是程序的这种功能是使用者所不需要的或是不要求的)。注意到这种情况,便有如下的理论问题:

假定有经典的 Hoare 三元组$\{A\}c\{B\}$,B 是$\{A\}c$ 的最强后置,有 $B'\Rightarrow B$。如果以 B'替换$\{A\}c\{B\}$中的 B,那么程序 c 即使是成功执行并且终止,回状态也可能不满足 B'。此时,被修改后的"三元组"$\{A\}c\{B'\}$的语义如何来描述?

基于前面的问题和讨论,本文主要基于 Hoare 逻辑提出了一种概率拟 Hoare 逻辑,用于刻画程序执行的正确度,将经典 Hoare 逻辑框架下程序属性的两种取值状态(0 和 1)推广到整个[0,1]区间。具体的工作如下:

• 首先,给出 α 正确蕴含、α 正确包含和程序诱导分布等定义和命题,并进一步地给出概率拟 Hoare 三元组等定义。

• 然后,在 Hoare 逻辑的基础上,针对 IMP 语言[6]给出一种$[\alpha_1,\alpha_2]$1-概率拟 Hoare 逻辑并证明了其可靠性。

在本文的讨论中,若非特别说明,有如下假设:

(i)Σ 表示可数状态集,*Assn* 表示扩充的布尔表达式集,*Com* 表示命令集,*Loc* 表示存储单元的集合,$\bar{N}$表示正整数、负整数和零的集合,*Index* 表示任意指标集,是 I_c 程序 c 的关系语义或说明,$\{A\}c\{B\}$表示部分正确性断言,$[A]c[B]$表示完全正确性断言。

(ii)若称 *Prob* 是 $A(\subseteq\Sigma)$上的概率测度,实际上是指 *Prob* 是可测空间$(A,\sigma(A))$上的概率测度,而所构成的三元组$(A,\sigma(A),Prob)$称为概率测度空间。在不引起混淆的情况下,A 上的概率测度 $Prob_A$(或 $Probs_A$)简记为 *Prob*。其中 $\sigma(A)$表示由状态空间 A 的一切子集所生成的 σ-代数。

(iii)如果 *Prob* 是 $A(\subseteq\Sigma)$上的一个概率测度,那么有 $\forall\sigma\in A, Prob(\{\sigma\})>0$。

(iv)程序运行环境为 Intel(R) Core(TM)2 Duo CPU E8400 @3.00GHz,2.99GHz,2.00GB,Windows XP SP3,采用 Win-TC 编译器;

(v)另外,考虑到程序实际运行中数据溢出等物理环境问题,认为指称函数是概率意义下成立的。为了区别文献[6]中的符号,我们分别记 $\mathscr{A},\mathscr{B}$ 和 $\mathscr{C}$ 为 $\mathscr{A}_{env},\mathscr{B}_{env}$ 和 $\mathscr{C}_{env}$。

2 预备知识

这一节中将给出 α 正确蕴含、α 正确包含、程序诱导分布以及程序正确度 α 规则等定义和命题。

下面首先给出一些本节后面讨论要用到的约定和定义。

在本节中约定:

设 $A\in A_{ssn}$,所有满足 A 的状态的集合记为

$S_A=\{\sigma\in\Sigma\mid\sigma\vdash A\}$

定义 1(状态)[7] 一个状态是一个以 *Loc* 作为定义域,集合$\bar{N}$作为值域的函数,即 $X\in Loc,\sigma(X)$表示在状态 δ 下存储单元 X 的求值结果。

定义 2(程序说明)[7] 程序的关系语义或说明(用 *Ic* 表示)是状态空间 Σ 上的二元关系$\langle\sigma,\sigma'\rangle\in Ic$,当且仅当存在一个可执行的程序 c,它以初始状态 σ 开始,以终结状态 σ'结束。

定义 3(定义域)[7] 给定一个关系 $R\subset\Sigma\times\Sigma$,$R$ 的定义域表示为 *Dom*. R,即 $Dom.R=\{x\mid x\in\Sigma\wedge\exists x'(x'\in\Sigma\wedge\langle x,x'\rangle\in R)\}$。

定义 4(值域) 给定一个关系 $R\subset\Sigma\times\Sigma$,$R$ 的值域表示为 *Range*. R,即 $Range.R=\{x'\mid x'\in\Sigma\wedge\exists x(x\in\Sigma\wedge\langle x,x'\rangle\in R)\}$。

定义 5(定义域限制)[7] 给定一个关系 $R\subset\Sigma\times\Sigma$ 和一个集合 $Y\subset\Sigma$,关系 R 的定义域由 Y 限制,记为 $Y\upharpoonright R$,即 $Y\upharpoonright R=\{\langle x,x'\rangle\mid x\in Y\wedge\langle x,x'\rangle\in R\}$。

定义 6(值域限制)[7] 给定一个关系 $R\subset\Sigma\times\Sigma$ 和一个集合 $Z\subset\Sigma$,关系 R 的值域由 Z 限制,记为 $R\downarrow Z$,即 $R\downarrow Z=\{\langle x,x'\rangle\mid x\in Z\wedge\langle x,x'\rangle\in R\}$。

定义 7(σ-代数)[8] 称集合 Ω 的子集类$\mathfrak{A}$为 Ω 中的 σ-代数,如果它满足下列条件:

(a)$\Omega\in\mathfrak{A}$;

(b)若 $A\in\mathfrak{A}$,则 $A^c\in\mathfrak{A}$;

(c)若 $A_n\in\mathfrak{A},n=1,2,\cdots$,则$\bigcup_{n=1}^{+\infty}A_n\in\mathfrak{A}$。

定义 8[8,9] 设$\mathfrak{A}$为 Ω 的子集类,$\emptyset\in\mathfrak{A}$。集函数 $\mu:\mathfrak{A}\to\bar{R}$,如果

(a)非负性:$\forall A\in\mathfrak{A},\mu(A)\geqslant\mu(\emptyset)=0$;

(b)σ-可加性:设 $A_n(n=1,2,\cdots)$两两不交(即 $A_i\cap A_j=\emptyset,i\neq j$),且$\sum_{n=1}^{+\infty}A_n\in\mathfrak{A}$,则

$$\mu\left(\sum_{n=1}^{+\infty}A_n\right)=\sum_{n=1}^{+\infty}\mu(A_n)$$

称 μ 为测度。如果 $\forall A\in\mathfrak{A}$,有 $\mu(A)<+\infty$,则称 μ 为有限测度;如果存在一列 $A_i\in\mathfrak{A},n\geqslant1$,使得$\bigcup_{i=1}^{+\infty}A_i=\Omega$ 且 $\mu(A_n)<+\infty,n\geqslant1$,则称 μ 为 σ-有限测度。具有性质 $\mu(\Omega)=1$ 的测度称为正规测度,亦称概率测度,一般用 *Prob* 表示。

注 1[9]:从上面测度的定义可知,测度的自然定义域应当是 σ-代数。

定义 9[10] 设$\mathfrak{A}$为 Ω 上一 σ-代数,称序偶$(\Omega,\mathfrak{A})$为可测空间,$\mathfrak{A}$中的元素称为$\mathfrak{A}$-可测集。设 μ 为可测空间$(\Omega,\mathfrak{A})$上的测度,则称三元组$(\Omega,\mathfrak{A},\mu)$为测度空间。若 μ 是有限测度,则称$(\Omega,\mathfrak{A},\mu)$为有限测度空间;若 μ 是概率测度,则称$(\Omega,\mathfrak{A},\mu)$为概率测度空间。

定义 10[10] 设$(\Omega,\mathfrak{A})$为可测空间,E 是 Ω 的一个子集,f 是定义在 E 上的有限实函数。如果对于一切实数 c,集合 $E(c\leqslant f)$都是 $E(c\leqslant f)$上的可测集(即 $E(c\leqslant f)\in\mathfrak{A}$),那么则称 f 是 E 上关于$(\Omega,\mathfrak{A})$的可测函数,简称是 E 上可测函数。

定义 11[10] 设$(\Omega,\mathfrak{A},\mu)$为一测度空间。若 $A\in\mathfrak{A}$,且 $\mu(A)=0$,则称 A 为 μ-零测集。

定理 1(积分变换定理)[9] 设 f 是测度空间$(\Omega,\mathfrak{A},\mu)$到可测空间$(\prod,\mathfrak{A}')$上的可测映射,$\mu_f$ 为由 f 导出的测度。又设 g 是$(\prod,\mathfrak{A}')$到$(R,\mathscr{B}(R))$的可测函数,则 $\forall B\in\mathfrak{A}'$,

$$\int_{f^{-1}(B)}g(f)\mathrm{d}\mu=\int_B g\mathrm{d}\mu_f$$

上式的意义是一方有意义,则另一方也有意义,且两者相等。

命题 1[11] $\mathfrak{A}$上的任何测度 μ 的原子是一个使$\mu(\{x\})>0$ 的单元。σ-有限测度的原子个数是可数的。

文献[12,13]中讨论了布尔表达式(公式)真度的概念。在这里,我们也引入类似的概念。

定义 12(α 正确蕴含) 我们说 A_1 以正确度 α 蕴含 A_2,

如果有

$$\int_{S_{A_1}} (\llbracket A_1 \wedge A_2 \rrbracket)(\omega) Prob_{A_1}(d\omega) = \alpha \tag{4}$$

记为 $A_1 \overset{\alpha}{\infty} A_2$。其中，$A_1, A_2 \in Assn$，$Prob_{A_1}$ 是 S_{A_1} 上的概率测度或分布。若 $A_1 \wedge A_2$ 为真，那么 $\llbracket A_1 \wedge A_2 \rrbracket = 1$，否则 $\llbracket A_1 \wedge A_2 \rrbracket = 0$。

注 2：(i)在式(4)中，若 $A_1 \equiv$ false，则 $\alpha = 0$；(ii)在式(4)中，若 $A_1 \equiv$ true，我们称 α 为 A_2 的正确度(类似于文献[13]的真度定义)；(iii)在式(4)中，$\alpha = 1$ 蕴含 $A_1 \Rightarrow A_2$，但是注意到 false$\Rightarrow A_2$，因此，若 $A_1 \Rightarrow A_2$，未必会有 $A_1 \overset{1}{\infty} A_2$；(iv)$A_1 \overset{\alpha\leqslant}{\infty} A_2$ 表示 A_1 以大于等于 α 的正确度蕴含 A_2，于是有 $\int_{S_{A_1}} (\llbracket A_1 \wedge A_2 \rrbracket(\omega) Prob_{A_1}(d\omega) \geqslant \alpha)$；(v)$A_1 \overset{\alpha}{\infty} A_2$ 表示 $A_1 \overset{\alpha}{\infty} A_2$ 且 $A_2 \overset{\alpha}{\infty} A_1$。

定义 13(α 正确包含)　我们说 S_{A_1} 以正确度 α 包含于 S_{A_2}，如果有

$$\int_{S_{A_1}} \chi(S_{A_1} \cap S_{A_2})(\omega) Prob_{A_1}(d\omega) = \alpha \tag{5}$$

记为 $S_{A_1} \sqsubseteq_\alpha S_{A_2}$。其中，$A_1 A_2 \in Assn$，$Prob_{A_1}$ 是 S_{A_1} 上的概率测度或分布。

注 3：(i)在式(5)中，若 $S_{A_1} = \emptyset$，则 $\alpha = 0$；(ii)在式(5)中，$\alpha = 1$ 蕴含 $S_{A_1} \subseteq S_{A_2}$。但是，注意到 $\emptyset \subseteq S_{A_2}$，因此，若 $S_{A_1} \subseteq S_{A_2}$，未必会有 $S_{A_1} \sqsubseteq_1 S_{A_2}$；(iii)若 $\int_{S_{A_1}} \chi(S_{A_1} \cap S_{A_2})(\omega) Prob_{A_1}(d\omega) \geqslant \alpha$，则记为 $S_{A_1} \sqsubseteq_{\alpha\leqslant} S_{A_2}$。

命题 2　$A_1 \overset{\alpha\leqslant}{\infty} A_2 \Leftrightarrow S_{A_1} \sqsubseteq_{\alpha\leqslant} S_{A_2}$。证明：由定义 12、定义 13、注 2 和注 3 可知

$$A_1 \overset{\alpha\leqslant}{\infty} A_2 \Leftrightarrow Prob_{A_1}(S_{A_1} \cap S_{A_2}) \geqslant \alpha \tag{6}$$

及

$$S_{A_1} \sqsubseteq_{\alpha\leqslant} S_{A_2} \Leftrightarrow Prob_{A_1}(S_{A_1} \cap S_{A_2}) \geqslant \alpha \tag{7}$$

从而由式(6)和式(7)易知结论成立。

3　概率拟 Hoare 三元组

在这一节中将给出一种概率拟 Hoare 三元组，来用于量化程序执行的正确性，刻画程序的正确度或是理论被实际程序实现的程度。

下面给出概率拟 Hoare 三元组的定义。这里主要介绍了概率拟 Hoare 三元组以及其 6 种特殊情况，我们统称这些为概率拟 Hoare 三元组。

定义 14(区间拟 Hoare 三元组)　设 $A', B' \in Assn$，$c \in Com$. $\{A'\}_{[\alpha_1,\alpha_2]}(c)_{[\beta_1,\beta_2]}\{\beta'\}$ 为区间拟 Hoare 三元组。其中，$0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant 1$，$0 \leqslant \beta_1 \leqslant \beta_2 \leqslant 1$，$A'$ 是程序 c 的区间拟前置条件，B' 是程序 c 的区间拟后置条件。其意思是说：程序 c 的当前状态满足 A'。那么程序段 c 以 $\alpha \in [\alpha_1, \alpha_2]$ 的概率执行并能正常终止，且返回值以 $\beta \in [\beta_1, \beta_2]$ 的概率满足 B'[1]。

注 4：特别地，(i)$[\alpha_1, \alpha_2]$1-拟 Hoare 三元组

$\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$

其中，A' 是程序 c 的 $[\alpha_1, \alpha_2]$-拟前置条件，B' 是程序 c 的 1-拟后置条件。其意思是说：程序 c 的当前状态满足 A'。那么程序段 c 以 $a \in [\alpha_1, \alpha_2]$ 的概率执行并能正常终止，且返回值以 1 的概率满足 B'。

(ii)$1[\beta_1, \beta_2]$-拟 Hoare 三元组

$\{A'\}_1(c)_{[\beta_1,\beta_2]}\{B'\}$

其中，A' 是程序 c 的 1-拟前置条件，B' 是程序 c 的 $[\beta_1, \beta_2]$-拟后置条件。其意思是说：程序 c 的当前状态满足 A'。那么程序段 c 以 1 的概率执行并能正常终止，且返回值以 $\beta \in [\beta_1, \beta_2]$ 的概率满足 B'。

(iii)$\alpha\beta$-拟 *Hoare* 三元组

$\{A'\}_\alpha(c)_\beta\{B'\}$

其中，A' 是程序 c 的 α-拟前置条件，B' 是程序 c 的 β-拟后置条件。其意思是说：程序 A 的当前状态满足 A'。那么程序段 c 以 α 的概率执行并能正常终止，且返回值以 β 的概率满足 B'。

(iv)α1-拟 Hoare 三元组

$\{A'\}_\alpha(c)_1\{B'\}$

其中，A' 是程序 c 的 α-拟前置条件，B' 是程序 c 的 1-拟后置条件。其意思是说：程序 c 的当前状态满足 A'。那么程序段 c 以 α 的概率执行并能正常终止，且返回值以 1 的概率满足 B'。

(v)1β-拟 Hoare 三元组

$\{A'\}_1(c)_\beta\{B'\}$

其中，A' 是程序 c 的 1-拟前置条件，B' 是程序 c 的 β-拟后置条件。其意思是说：程序 c 的当前状态满足 A'。那么程序段 c 以 1 的概率执行并能正常终止，且返回值以 β 的概率满足 B'。

(vi)$\{A'\}_{\alpha\leqslant}(c)_{\leqslant\beta}\{B'\}$ 表示程序 c 的当前状态满足 A'。那么程序段 c 以大于等于 α 的概率执行并能正常终止，且返回值以小于等于 β 的概率满足 B'。

定义 15(程序正确度(或称实现度)α 规则)　概率拟 Hoare 三元组正确度 α 规则有如下说明：

$$I[\{A'\}_{[\alpha_1,\alpha_2]}(c)_{[\beta_1,\beta_2]}\{B'\}] = (S_{A'} \sqsubseteq_{[\alpha_1,\alpha_2]} Dom.\ I_c) \wedge (Range.\ (S_{A'} \uparrow I_c) \sqsubseteq_{[\beta_1,\beta_2]} S_{B'}) \tag{8}$$

其中，$\alpha = \tau_1 \times \tau_2$，$\tau_1 \in [\alpha_1, \alpha_2]$，$\tau_2 \in [\beta_1, \beta_2]$，$0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant 1$，$0 \leqslant \beta_1 \leqslant \beta_2 \leqslant 1$。

4　$[\alpha_1, \alpha_2]$1-概率拟 Hoare 三元组

第 3 节中给出了概率拟 Hoare 三元组的定义，这一节中将讨论 $[\alpha_1, \alpha_2]$1-拟 Hoare 三元组。首先给出其形式化语义，然后再进一步地给出其概率拟 Hoare 规则——$[\alpha_1, \alpha_2]$1-拟 Hoare 规则，最后证明 $[\alpha_1, \alpha_2]$1-拟 Hoare 规则的可靠性。

· α-拟 Hoare 规则

为了便于下面的讨论，首先给出一些约定和定义。

在本节中约定：

设 $A' \in Assn$，I 是一个解释。在解释 I 下所有满足 A' 的状态的集合记为 $S^I_{A'} = \{\sigma \in \Sigma \mid \sigma \models^I A'\}$。

定义 16(有效性)　(i)设 I 是一个解释。如果对应于解释 I，有

$$\forall \sigma \in \Sigma.\ \sigma \models^I \{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$$

则称，对应于解释 I，$\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$ 是有效的，记为 $\models^I \{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$。

---

[1] 为了避免与 c 下标的混淆，将 $\{A'\}_{[\alpha_1,\alpha_2]}c_{[\beta_1,\beta_2]}\{B'\}$ 写成 $\{A'\}_{[\alpha_1,\alpha_2]}(c)_{[\beta_1,\beta_2]}\{B'\}$

(ii)若对于一切解释 I,有

$\models^I\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$

则称$\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$是有效的,记为$\models\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$。特别地,若对于一切解释 I,有$\forall\sigma\in\Sigma.\sigma\models^I A'$,则称 A'是有效的,记为$\models A'$。

由上面的定义可知,$\models\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$(其中,$A',B'\in Assn,c\in Com$),当且仅当对于所有的解释 I',在满足 A'的状态下执行程序段 c,那么 c 以$\alpha\in[\alpha_1,\alpha_2]$的概率执行并能正常终止,且返回值以 1 的概率满足 B'。其形式化语义表示如下:对于所有的解释 I

$$Prob\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\}=\alpha(\in[\alpha_1,\alpha_2]) \tag{9}$$

且

$$\mathscr{C}_{env}[\![c]\!](S^I_{A'}\cap Dom.I_c)\sqsubseteq_1 S^I_{B'} \tag{10}$$

其中,$Prob$ 是$\{\sigma\mid\sigma\models^I A'\}$上的概率测度。如果 $\mathscr{C}_{env}[\![c]\!]\sigma$ 没有定义,则记 $\mathscr{C}_{env}[\![c]\!]=\perp$。约定对于所有的断言 B,有$\perp\models\neq B$,这表示将不终止的计算指称到$\perp$,并且不满足任一后置条件。换而言之,如果程序 c 的执行是不终止的,那么我们认为 c 不能正确被执行或是说 c 不是我们所需要的,是不可信的。

注 5:显然地,若$\forall\sigma\in\Sigma.\sigma\models\neq^I A'$,则有

$Prob(\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\})=Prob(\emptyset)=0$

于是,有如下命题:

命题 3 设 $Prob$ 是 Ω 上的概率测度。$\forall A_y\in\Omega,y\in Index$,有

$Prob(A_y)=1\Leftrightarrow Prob(\bigcap\limits_{y\in Index}A_y)=1$

证明:"⇒"。假设 $Prob(\bigcap\limits_{y\in Index}A_y)\neq 1$,于是有 $\exists A_{y_0}\subseteq\Omega(y_0\in Index)$,使得 $Prob(A_{y_0}>0)$。于是,有 $Prob(A_y\backslash A_{y_0})=Prob(A_y)-Prob(A_{y_0})<1$。

与假设矛盾,故结论成立。

"⇐"。注意到 $\forall y\in Index$,有 $\bigcap\limits_{y'\in Index}A_{y'}\subseteq A_y$,易知结论成立。

命题 4 I 是解释,(i)若 $Prob_{A'}(\bigcap\limits_I\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\})\leqslant\inf\limits_I Prob_{A'}(\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\})\leqslant Prob_{A'}(\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\})$

(ii)特别地,$Prob_{A'}(\bigcap\limits_I\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\})=1$,当且仅当$\inf\limits_I Prob_{A'}(\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\})=1$;当且仅当,对于所有的解释 I

$Prob_{A'}(\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\})=1$

证明:(i)注意到

$$\bigcap\limits_I\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\}\subseteq\{\sigma\models A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\} \tag{11}$$

故有

$$\bigcap\limits_I\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\}\subseteq\inf\limits_I\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\} \tag{12}$$

于是,由式(11)、式(12)以及概率测度 $Prob_{A'}$ 的单调性可知,结论成立。

(ii)由命题 3 和(i)可知,结论成立。

命题 5 对于任意的解释 I,假定 $Range.(S^I_{A'}\uparrow I_c)\sqsubseteq_1 S^I_{B'}$,且 $Dom.I_c\sqsubseteq_1 S^I_{A'}$。那么有 $Dom.I_c=Dom.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}))$。

证明:显然 $Dom.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}))\subseteq Dom.I_c$。

下证 $Dom.I_c\subseteq Dom.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}))$。

使用反证法。假设 $Dom.I_c\nsubseteq Dom.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}))$,即有 $\exists\sigma_0\in Dom.I_c$,但

$$\sigma_0\notin Dom.(I_c\downarrow(S^I_{B'})\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\})) \tag{13}$$

于是,由式(13)可知,$\exists\sigma_0'$,有

$$\langle\sigma_0,\sigma_0'\rangle\in I_c \tag{14}$$

但

$$\sigma_0'\notin S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\} \tag{15}$$

故由式(15)可以知道,有以下两种情况:

(i)$\sigma_0'\notin S^I_{B'}$

由假设及定义 12 可知 $\sigma_0'\notin Range.(S^I_{A'}\uparrow I_c)$,又由式(14)可知 $\sigma_0\notin S^I_{A'}$。于是,由题设 $Dom.I_c\sqsubseteq_1 S^I_{A'}$ 可知 $\sigma_0\notin Dom.I_c$,与假设矛盾。

(ii)$\sigma_0'\notin\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}$

由假设以及式(14)可知 $\sigma_0\notin S^I_{A'}$,于是,由(i)中的证明可知,显然地,亦得到与假设矛盾。

综合(i)和(ii),结论成立。

命题 6 对于任意的解释 I,假定 $Range.(S^I_{A'}\uparrow I_c)\sqsubseteq_1 S^I_{B'}$,且 $Dom.I_c\sqsubseteq_1 S^I_{A'}$。那么有 $Range.(I_c)=Range.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}))$。

证明:显然 $Range.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}))\subseteq Range.(I_c)$。

下证 $Range.(I_c)\subseteq Range.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}))$。

使用反证法。假设 $Range.(I_c)\nsubseteq Range.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}))$,即有 $\exists\sigma_0'\in Range.(I_c)$,但

$$\sigma_0'\notin Range.(I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\})) \tag{16}$$

于是,由式(16)可知,$\exists\sigma_0$,有

$$\langle\sigma_0,\sigma_0'\rangle\in I_c \tag{17}$$

但

$$\sigma_0'\notin S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\} \tag{18}$$

故由式(18)可以知道,有以下两种情况:

(i)$\sigma_0'\notin S^I_{B'}$

由假设及定义 12 可知 $\sigma_0'\notin Range.(S^I_{A'}\uparrow I_c)$,又由式(17)可知 $\sigma_0\notin S^I_{A'}$。于是由题设 $Dom.I_c\sqsubseteq_1 S^I_{A'}$ 可知 $\sigma_0'\notin Range.(I_c)$,与假设矛盾。

(ii)$\sigma_0'\notin\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\}$

由假设以及(17)可知 $\sigma_0\notin S^I_{A'}$,于是,由(i)中的证明可知,显然地,亦得到与假设矛盾。

综合(i)和(ii),结论成立。

推论 1 对于任意的解释 I,假定 $Range.(S^I_{A'}\uparrow I_c)\sqsubseteq_1 S^I_{A'}$,且 $Dom.I_c\sqsubseteq_1 S^I_{A'}$。那么有 $I_c=I_c\downarrow(S^I_{B'}\cap\{\mathscr{C}_{env}[\![c]\!]\sigma\mid\sigma\in S^I_{A'}\})$。

证明:由命题 5 和命题 6 可知,结论成立。

定理 2 对于任意的解释 I，设 $Prob$ 是 $\{\sigma \mid \sigma \models {}^{I}A'\}$ 上的概率测度，并且假设 $Range.(S^{I}_{A'} \upharpoonright I_c) \sqsubseteq_1 S^{I}_{B'}$ 以及 $Dom.\ I_c \sqsubseteq_1 S^{I}_{A'}$。于是有

$$S^{I}_{A'} \sqsubseteq_{[\alpha_1,\alpha_2]} Dom.\ I_c \tag{19}$$

当且仅当

$$Prob(Dom.(I_c \downarrow (S^{I}_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\}))) = \alpha(\in [\alpha_1,\alpha_2]) \tag{20}$$

当且仅当

$$S^{I}_{A'} \sqsubseteq_{[\alpha_1,\alpha_2]} Dom.(I_c \downarrow (S^{I}_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\})) \tag{21}$$

当且仅当

$$Prob(\sigma \models {}^{I}A' \mid \forall \sigma \in \Sigma.\ \sigma \models {}^{I}A' \Rightarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \models {}^{I}B'\}) = \alpha(\in [\alpha_1,\alpha_2]) \tag{22}$$

证明："式(19)⇒式(20)"。由定义 12 可知 $Prob(S^{I}_{A'} \cap Dom.\ I_c) = \alpha(\in [\alpha_1,\alpha_2])$。

于是，由命题 5 可以得到

$$Prob(Dom.(I_c \downarrow (S_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\}))) = \alpha(\in [\alpha_1,\alpha_2])$$

"式(20)⇒式(21)"。由命题 5 显然可知结论成立。

"式(21)⇒式(22)"。显然地，有 $S^{I}_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\}) \subseteq Range.(I_c)$。于是，有 $S^{I}_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\} = Range.(I_c) \cap S^{I}_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\})$。故有

$$\begin{aligned} &Dom.(I_c \downarrow (S^{I}_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\})) \\ &= \{\sigma \in \Sigma \mid \sigma \in S^{I}_{A'} \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{B'}\} \\ &= \{\sigma \models {}^{I}A' \mid \forall \sigma \in \Sigma.\ \sigma \models {}^{I}A' \Rightarrow \mathscr{C}_{env} \llbracket c \rrbracket \sigma \models {}^{I}B'\} \end{aligned} \tag{23}$$

于是得到 $Prob(\{\sigma \models {}^{I}A' \mid \forall \sigma \in \Sigma.\ \sigma \models {}^{I}A' \Rightarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \models {}^{I}B'\}) = \alpha(\in [\alpha_1,\alpha_2])$。

"式(22)⇒式(19)"。注意到命题 5 和式(23)，显然地，结论成立。

注 6：注意到 $\perp \notin \Sigma$，显然地 $S_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\} \setminus \perp) = S_{B'} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\}$。

定理 3 对于任意的解释 I，设 $Prob$ 是 $\{\sigma \mid \sigma \models {}^{I}A'\}$ 上的概率测度，并且 $Dom.\ I_c \sqsubseteq_1 S^{I}_{A'}$。于是有

$$Range.(S^{I}_{A'} \upharpoonright I_c) \sqsubseteq_1 S^{I}_{B'} \tag{24}$$

当且仅当

$$Range.(I_c \downarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\}) \sqsubseteq_1 S^{I}_{B'} \tag{25}$$

当且仅当

$$Prob(\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'} \cap Dom.\ I_c\} \cap S^{I}_{B'}) = 1 \tag{26}$$

当且仅当

$$\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'} \cap Dom.\ I_c\} \sqsubseteq_1 S^{I}_{B'} \tag{27}$$

当且仅当

$$Prob(\{\mathscr{C}_{env} \llbracket c \rrbracket \mid \forall \sigma \in \Sigma.\ \sigma \models {}^{I}A' \Rightarrow \mathscr{C}_{env} \llbracket c \rrbracket \sigma \models {}^{I}B' \text{ 且 } \sigma \models {}^{I}A'\}) = 1 \tag{28}$$

证明："式(24)⇒式(25)"。只需证明如下等式成立：

$$Range.(S^{I}_{A'} \upharpoonright I_c) = Range.(I_c \downarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\}) \tag{29}$$

先证 $Range.(S^{I}_{A'} \upharpoonright I_c) \subseteq Range.(I_c \downarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\})$。

设 $\sigma' \in Range.(S^{I}_{A'} \upharpoonright I_c)$。于是有，$\exists \sigma$，使得

$$\sigma \in S^{I}_{A'} \text{ 且 } \langle \sigma,\sigma' \rangle \in I_c \tag{30}$$

由式(30)可知 $\sigma'(=\mathscr{C}_{env} \llbracket c \rrbracket \sigma) \in Range.(I_c)$，故有 $\sigma' \in Range.(I_c \downarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\})$。

再证 $Range.(I_c \downarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\}) \subseteq Range.(S^{I}_{A'} \upharpoonright I_c)$。设 $\sigma' \in Range.(I_c \downarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\})$。于是有，$\exists \sigma$，使得

$$\sigma' \in \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\} \text{ 且 } \langle \sigma,\sigma' \rangle \in I_c \tag{31}$$

注意到 $Dom.\ I_c \sqsubseteq_1 S^{I}_{A'}$，于是有

$$\sigma \in S^{I}_{A'} \tag{32}$$

由式(31)和式(32)可知结论成立。

"式(25)⇒式(26)"。只需证明如下关系成立：

$$\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'} \cup Dom.\ I_c\} \sqsubseteq_1 S^{I}_{B'}$$

由假设可知 $Range.(I_c \downarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\}) \sqsubseteq_1 S^{I}_{B'}$。

因此，只需证明

$$\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'} \cap Dom.\ I_c\} \subseteq Range.(I_c \downarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\})$$

设 $\sigma' \in \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'} \cap Dom.\ I_c\}$。于是 $\exists \sigma$ 和 σ'，使得 $\sigma \in S^{I}_{A'}$ 且 $\langle \sigma,\sigma' \rangle \in I_c$。

故有 $\sigma' = \mathscr{C}_{env} \llbracket c \rrbracket \sigma \in \subseteq Range.(I_c)$。因此，结论成立。

"式(26)⇒式(27)"。由定义 12 可知，结论显然成立。

"式(26)⇒式(27)"。由假设以及式(27)可知

$$\begin{aligned} &\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'} \cap Dom.\ I_c\} \cap S^{I}_{B'} \\ &= \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in Dom.\ I_c\} \cap S^{I}_{B'} \\ &= \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in Dom.\ I_c \mathscr{C}_{env} \llbracket c \rrbracket \sigma \in S^{I}_{B'}\} \\ &= \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in Dom.\ I_c\} \end{aligned} \tag{33}$$

于是，由式(33)有 $\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}$，且 $\mathscr{C}_{env} \llbracket c \rrbracket \sigma \in S^{I}_{B'}\} \cap \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}\} \cap Dom.\ I_c\} = \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid Dom.\ I_c$ 且 $\mathscr{C}_{env} \llbracket c \rrbracket \sigma \in S^{I}_{B'}\} = \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid Dom.\ I_c\}$。

故得结论成立。

"式(28)⇒式(24)"。设 $\sigma' \in Range.(S^{I}_{A'} \upharpoonright I_c)$，于是有 $\exists \sigma$，使得 $\sigma \in S^{I}_{A'}$ 且 $\langle \sigma,\sigma' \rangle \in I_c$。

注意到式(28)，有 $\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'} \cap Dom.\ I_c\} \subseteq \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'}$ 且 $\mathscr{C}_{env} \llbracket c \rrbracket \sigma \in S^{I}_{B'}\}$，于是便有 $\sigma'(=\mathscr{C}_{env} \llbracket c \rrbracket \sigma) \in S^{I}_{B'}$。故得结论成立。

注 7：定理 2 和定理 3 说明了，对于 $\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$ 形式化语义的描述至少可以有 20 种，并且它们都是等价的。

推论 2 对于任意解释 I，设 $Prob$ 是 $\{\sigma \mid \sigma \models {}^{I}A'\}$ 上的概率测度，$Prob'$ 是 $\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \sigma \in S^{I}_{A'} \cap Dom.\ I_c\}$ 上的概率测度。则有 $(S^{I}_{A'} \sqsubseteq_{\alpha_1,\alpha_2} Dom.\ I_c) \wedge (Range.\ S^{I}_{A'} \upharpoonright I_c \sqsubseteq_1 S^{I}_{B'})$，当且仅当 $Prob(\{\sigma \models {}^{I}A' \mid \forall \sigma \in \Sigma.\ \sigma \models {}^{I}A' \Rightarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \models {}^{I}B'\}) = \alpha(\in [\alpha_1,\alpha_2]) \wedge Prob'(\{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \mid \forall \sigma \in \Sigma.\ \sigma \models {}^{I}A' \Rightarrow \{\mathscr{C}_{env} \llbracket c \rrbracket \sigma \models {}^{I}B'$ 且 $\sigma \models {}^{I}A'$ 且 $\sigma \in Dom.\ I_c\}) = 1$。

证明：由定理 2 和定理 3 易得结论。

注 8：推论 2 是上面定理 2 和定理 3 揭示形式化语义描述的一种情况。它的意义在于，说明了 $\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$ 的形式化，以集合的可信包含关系刻画(式(8))与以状态集上的概率测度刻画(式(9)和式(10))本质上是一致的。

给出 $[\alpha_1,\alpha_2]$1-拟 Hoare 规则如下。

拟(Skip)规则：

$$\{A'\}_1 Skip_1 \{A'\}$$

拟赋值规则：

若 $Prob(\sigma \models A'[\alpha/X] \mid \sigma \models A'[a/X] \Rightarrow \sigma[\mathscr{A}_{env}\llbracket c \rrbracket \sigma/X] \models A') = \alpha$，则 $A'[\alpha/X]_a(X:=a)_1\{A\}', \alpha(\in[\alpha_1,\alpha_2])$。其中，$Prob$ 是 $\{\sigma \mid \sigma \models A'[\alpha/X]\}$ 上的概率测度。而条件 $Prob(\sigma) \models A'[a/X] \mid \forall \sigma \in \Sigma.\ \sigma \models A'[a/X] \Rightarrow \sigma[\mathscr{A}_{env}\llbracket c \rrbracket \sigma/X] \models A') = \alpha(\in[\alpha_1,\alpha_2])$ 是为了表示因为局限于一定的物理设备和条件，赋值可能会因为溢出或是强制类型转换等原因而出错。

拟顺序规则：

$$\frac{\{A'\}_{[a_1,a_2]}(c_0)_1\{D'\}\{D'\}_{[a_1',a_2']}(c_1)_1\{B'\}}{\{A'\}_{[0,a_2\cdot a_2']}(c_0;c_1)_1\{B'\}}$$

拟选择规则：

$$\frac{\{A'\wedge b\}_{[a_1,a_2]}(c_0)_1\{B'\}\{A'\wedge\neg b\}_{[a_1',a_2']}(c_1)_1\{B'\}\Phi}{\{A'\}_{[0,(a_2\vee a_2')]}(\text{if } b \text{ then } c_0 \text{ else } c_1)_1\{B'\}}$$

拟循环规则：

$$\frac{\{A'\wedge b\}_{[a_1,a_2]}(c)_1\{A'\}\Phi}{\{A'\}_{[0,1]}(\text{while } b \text{ do } c)_1\{A'\wedge\neg b\}}$$

其中，$Prob$ 是 $\{\sigma \mid \sigma \models b\}$ 上的概率测度，$Prob'$ 是 $\{\sigma \mid \sigma \models\!\!\!\neq b\}$ 上的概率测度；并记 Φ 为条件 $Prob(\{\sigma \models b \mid \forall \sigma \in \Sigma.\ \sigma \models b \Rightarrow \mathscr{B}_{env}\llbracket c \rrbracket \sigma = \text{true}\}) \leqslant 1$ 且 $Prob'(\{\sigma \models\!\!\!\neq b \mid \forall \sigma \in \Sigma.\ \sigma \models b \Rightarrow \mathscr{B}_{env}\llbracket c \rrbracket \sigma = \text{false}\}) \leqslant 1$，表示布尔条件 b 从(拟)前置条件到程序中布尔条件的过程中，由于程序实际的执行可能会遇到内存溢出等问题，而使得其正确性降低。

拟推理规则 1：

$$\frac{\{A\}_{[a_1,a_2]}(c)_1\{B'\}B'\overset{1}{\propto}B}{\{A\}_{[a_1,a_2]}(c)_1\{B\}}$$

拟推理规则 2：

$$\frac{A\overset{1}{\propto}A'\{A'\}_{[a_1,a_2]}(c)_1\{B\}}{\{A\}_{[0,1]}(c)_1\{B\}}$$

5 $[\alpha_1,\alpha_2]$1-拟 Hoare 规则可靠性

在上一节中，给出了概率拟 Hoare 规则——$[\alpha_1,\alpha_2]$1-Hoare 规则，在这一节中我们将证明 $[\alpha_1,\alpha_2]$1-拟 Hoare 规则的可靠性。

定理 4 给出 $[\alpha_1,\alpha_2]$1-拟 Hoare 三元组 $\{A'\}_{[a_1,a_2]}(c)_1\{B'\}$。如果 $\vdash\{A'\}_{[a_1,a_2]}(c)_1\{B'\}$，那么 $\models\{A'\}_{[a_1,a_2]}(c)_1\{B'\}$。

证明：显然地，如果能证明上面的 $[\alpha_1,\alpha_2]$1-拟 Hoare 规则每条规则是可靠的，那么由规则归纳法知道，每条定理都是有效的。

拟 Skip 规则：显然地 $\models\{A'\}_1(c)_1\{A'\}$ 成立，因此拟 Skip 规则是可靠的。

拟赋值规则：记 $c \overset{\triangle}{=} (X:=a)$，设 I 是一个解释，显然地，有

$$\mathscr{C}_{env}\llbracket X:=a \rrbracket (S^I_{A'[a/X]} \cap Dom.\ I(X:=a)) \sqsubseteq_1 S^I_{A'} \tag{34}$$

由假设

$$Prob(\sigma \models A'[a/X] \mid \forall \sigma \in \Sigma.\ \sigma \models A'[a/X] \Rightarrow \sigma[\mathscr{A}_{env}\llbracket a \rrbracket \sigma/X] \models A) = \alpha(\in[\alpha_1,\alpha_2]) \tag{35}$$

从而由式(34)和式(35)得到 $\models\{A'[a/X]\}_{[a_1,a_2]}(X:=a)_1\{A'\}$

因此拟赋值规则是可靠的。

拟顺序规则：设 $\models\{A'\}_{[a_1,a_2]}(c_0)_1\{D'\}$ 且 $\models\{D'\}_{[a_1',a_2']}(c_1)_1\{B'\}$，$I$ 是一个解释。于是由 $\models^I\{A'\}_{[a_1,a_2]}(c_0)_1\{D'\}$ 可得

$$Prob_{S^I_{A'}}(\{\sigma \models^I A' \mid \forall \sigma \in \Sigma \cdot \sigma \models^I A' \Rightarrow \mathscr{C}_{env}\llbracket c_0 \rrbracket \sigma \models^I D'\}) = \alpha(\in[\alpha_1,\alpha_2]) \tag{36}$$

且

$$\mathscr{C}_{env}\llbracket c_0 \rrbracket (S^I_{A'} \cap Dom.\ I_{c_0}) \sqsubseteq_1 S^I_{D'} \tag{37}$$

而由 $\models^I\{D\}'_{[a_1',a_2']}(c_1)_1\{B'\}$ 得到

$$Prob_{S^I_{D'}}(\{\sigma \models^I D' \mid \forall \sigma \in \Sigma.\ \sigma \models^I D' \Rightarrow \mathscr{C}_{env}\llbracket c_1 \rrbracket \sigma \models^I B'\}) = \alpha'(\in[\alpha_1',\alpha_2']) \tag{38}$$

且

$$\mathscr{C}_{env}\llbracket c_1 \rrbracket (S^I_{D'} \cap Dom.\ I_{c_1}) \sqsubseteq_1 S^I_{B'} \tag{39}$$

于是，由式(36)和式(38)得到 $Prob_{S^I_{A'}}(\{\sigma \models^I A' \mid \forall \sigma \in \Sigma.\ \sigma \models^I A' \Rightarrow \mathscr{C}_{env}\llbracket c_1 \rrbracket (\mathscr{C}_{env}\llbracket c_0 \rrbracket \sigma) \models^I D'\}) \leqslant \alpha_2 \cdot \alpha_2'$。

故有 $Prob_{S^I_{A'}}(\{\sigma \models^I A' \mid \forall \sigma \in \Sigma.\ \sigma \models^I A' \Rightarrow \mathscr{C}_{env}\llbracket c_0;c_1 \rrbracket \sigma \models^I D'\}) \leqslant \alpha_2 \cdot \alpha_2'$。

又由式(37)和式(39)得到 $\mathscr{C}_{env}\llbracket c_1;c_2 \rrbracket (S^I_{A'} \cap Dom.\ I_{(c_1;c_2)}) \sqsubseteq_1 S^I_{B'}$。

因此拟顺序规则是可靠的。

拟选择规则：设 $\models\{A'\wedge b\}_{[a_1,a_2]}(c_0)_1\{B'\}$ 且 $\models\{A'\wedge\neg b\}_{[a_1',a_2']}(c_1)_1\{B'\}$，$I$ 是一个解释。假定 $\sigma \models^I A'$：

(a) $\sigma \models^I b$

显然地，有 $\sigma \models^I A' \wedge b$。由于 $\models^I\{A'\wedge b\}_{[a_1,a_2]}(c_0)_1\{B'\}$，故有 $Prob_{S^I_{A'\wedge b}}(\{\sigma \models^I A'\wedge b \mid \forall \sigma \in \Sigma.\ \sigma \models^I A'\wedge b \Rightarrow \mathscr{C}_{env}\llbracket c_0 \rrbracket \sigma \models^I B') = \alpha(\in[\alpha_1,\alpha_2])$，且 $\mathscr{C}_{env}\llbracket c_0 \rrbracket (S^I_{A'\wedge b} \cap Dom.\ I_{c_0}) \sqsubseteq_1 S^I_{B'}$。

(b) $\sigma \models^I \neg b$

显然地，有 $\sigma \models^I A' \wedge \neg b$。由于 $\models^I\{A'\wedge b\}_{[a_1',a_2']}(c_1)_1\{B'\}$，故有 $Prob_{S^I_{A'\wedge\neg b}}(\{\sigma \models^I A'\wedge\neg b \mid \forall \sigma \in \Sigma \cdot \sigma \models^I A'\wedge\neg b \Rightarrow \mathscr{C}_{env}\llbracket c_1 \rrbracket \sigma \models^I B'\}) = \alpha'(\in[\alpha_1',\alpha_2'])$，且 $\mathscr{C}_{env}\llbracket c_1 \rrbracket (S^I_{A'\wedge\neg b} \cap Dom.\ I_{c_1}) \sqsubseteq_1 S^I_{B'}$。

注意到 $Prob(\{\sigma \models b \mid \forall \sigma \in \Sigma.\ \sigma \models b \Rightarrow \mathscr{B}_{env}\llbracket b \rrbracket \sigma = \text{true}\}) \leqslant 1$ 和 $Prob'(\{\sigma \models\!\!\!\neq b \mid \forall \sigma \in \Sigma.\ \sigma \models\!\!\!\neq b \Rightarrow \mathscr{B}_{env}\llbracket b \rrbracket \sigma = \text{false}\}) \leqslant 1$。

综合(a)和(b)得到 $Prob_{S^I_{A'}}(\sigma \models A' \mid \forall \sigma \in \Sigma.\ \sigma \models^I A' \Rightarrow \mathscr{C}_{env}\llbracket \text{if } b \text{ then } c_0 \text{ else } c_1 \rrbracket \sigma \models^I B') \leqslant \alpha_2 \vee \alpha_2'$，且 $\mathscr{C}_{env}\llbracket \text{if } b \text{ then } c_0 \text{ else } c_1 \rrbracket (S^I_{A'} \cap Dom.\ \text{if } b \text{ then } c_0 \text{ else } c_1) \sqsubseteq_1 S^I_{B'}$。

因此拟选择规则是可靠的。

拟循环规则：假定 $\models(A'\wedge b)_{[a_1,a_2]}(c)_1\{A'\}$，即 A' 是循环语句 $w=\text{while } b \text{ do } c$ 的一个不变式。设 I 是一个解释。因为 $\mathscr{C}_{env}\llbracket \text{while } b \text{ do } c \rrbracket = fix(\Gamma)$，所以用 θ_n 表示 $\Gamma^n(\theta)$，就有 $\mathscr{C}_{env}\llbracket w \rrbracket = \bigcup_{n\in\mathbf{N}} \theta_n$，其中，$\theta_0=\varnothing$，$\theta_{n+1}=\{(\sigma,\sigma') \mid \mathscr{B}_{env}\llbracket b \rrbracket \sigma = \text{true}(\sigma,\sigma') \in \sigma_n \circ \mathscr{C}_{env}\llbracket c \rrbracket\} \cup \{(\sigma,\sigma) \mid \mathscr{B}_{env}\llbracket b \rrbracket \sigma = \text{false}\}$。

显然地，有 $\mathscr{C}_{env}\llbracket \text{while } b \text{ do } c \rrbracket (S^I_{A'} \cap Dom.\ I_{(\text{while } b \text{ do } c)}) \sqsubseteq_1 S^I_{B'}$。

定义 $P(n)$ 为：对所有的 $n\in\mathbf{N}$，$P(n) \Leftrightarrow_{def} Prob_{S^I_{A'}}(\{\sigma \models^I A' \mid \forall \sigma,\sigma' \in \Sigma.\ (\sigma,\sigma') \in \theta_n \text{ 且 } \sigma \models^I A' \Rightarrow \sigma' \models^I A' \wedge \neg b\}) \leqslant 1$。

若能证得 $P(n)$，$\forall n\in\mathbf{N}$ 成立。那么就有 $Prob_{S^I_{A'}}(\{\sigma \models A' \mid \forall \sigma' \in \Sigma.\ \sigma \models^I A' \Rightarrow \mathscr{C}_{env}\llbracket w \rrbracket \sigma \models^I A' \wedge \neg b\}) \leqslant 1$。于是，有 $\models\{A'\}_{[0,1]}(\text{while } b \text{ do } c)_1\{A'\wedge\neg b\}$。

下面采用数学归纳法证明 $P(n)$，$\forall n\in\mathbf{N}$ 成立。

奠基步：令 $n=0$，则 $\theta_0=\varnothing$，故 $P(0)$ 为真。

归纳步骤：假设 $n\geqslant 0$，$P(n)$为真，下面证明 $P(n+1)$亦为真。设$(\sigma,\sigma')\in\theta_{n+1}$，且$\sigma\models^I A'$，则

(a)$\sigma\models^I A'\wedge b$

对某个状态σ''使得$(\sigma,\sigma'')\in\mathscr{C}_{env}[\![c]\!]$，且$(\sigma'',\sigma')\in\theta_n$。由于$\vdash\{A'\wedge b\}_{[\alpha_1,\alpha_2]}(c)_1\{A'\}$，故有

$$Prob_{S^I_{A'\wedge b}}(\{\sigma\models^I A'\wedge b\mid\forall\sigma'\in\Sigma.\ \sigma\models^I A'\wedge b\Rightarrow\sigma''\models^I A'\})=\alpha(\in[\alpha_1,\alpha_2]) \tag{40}$$

而由假设 $P(n)$为真，可以得到

$$Prob_{S^I_{A'\wedge b}}(\{\sigma''\models^I A'\wedge b\mid\forall\sigma'\in\Sigma\cdot\sigma''\models^I A'\wedge b\Rightarrow\sigma'\models^I A'\wedge\neg b\})=\alpha(\in[\alpha_1,\alpha_2]) \tag{41}$$

从而由 $Prob(\{\sigma\models b\mid\forall\sigma\in\Sigma.\ \sigma\models b\Rightarrow\mathscr{B}_{env}[\![b]\!]\sigma=\text{true}\})\leqslant 1$ 以及式(40)和式(41)可得

$$Prob_{S^I_{A'\wedge b}}(\{\sigma\models^I A'\mid\forall\sigma'\in\Sigma.\ \sigma\models^I A'\Rightarrow\sigma'\models^I A'\wedge\neg b\})\leqslant\alpha\leqslant 1$$

(b)$\sigma\models^I A'\wedge\neg b$

显然地，$\sigma=\sigma'$。从而由 $\sigma\models^I A'\wedge\neg b$ 得到$\sigma'\models^I A'\wedge\neg b$。

注意到 $Prob^I(\{\sigma\not\models b\mid\forall\sigma\in\Sigma.\ \sigma\not\models b\Rightarrow\mathscr{B}_{env}[\![b]\!]\sigma=\text{false}\})\leqslant 1$，故有 $Prob_{S^I_{A'\wedge b}}(\{\sigma\models^I A'\mid\forall\sigma'\in\Sigma.\ \sigma\models^I A'\Rightarrow\sigma'\models^I A'\wedge\neg b\})\leqslant 1$。

这样，就证明了 $P(n+1)$为真。从而$\forall n\in\mathbb{N}$，$P(n)$为真，因此拟循环规则是可靠的。

拟推理规则 1：设$\vdash B'\overset{1}{\propto}B$且$\vdash\{A\}_{[\alpha_1,\alpha_2]}(c)_1\{B'\}$。$I$是一个解释。假定$\sigma\models^I A'$，于是 $Prob_{S^I_A}(\{\sigma\models^I A\mid\forall\sigma\in\Sigma.\ \sigma\models^I A\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B'\})=\alpha(\in[\alpha_1,\alpha_2])$且$\mathscr{C}_{env}[\![c]\!](S^I_A\cap Dom.\ I_c)\sqsubseteq_1 S^I_{B'}$。

从而再由定义 12 可知 $Prob_{S^I_A}(\{\sigma\models^I A\mid\forall\sigma\in\Sigma.\ \sigma\models^I A\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B\})=\alpha(\in[\alpha_1,\alpha_2])$且$\mathscr{C}_{env}[\![c]\!](S^I_A\cap Dom.\ I_c)\sqsubseteq_1 S^I_B$。

于是$\vdash\{A\}_{[\alpha_1,\alpha_2]}(c)_1\{B\}$。故拟推理规则 1 是可靠的。

拟推理规则 2：设$\vdash A\overset{1}{\propto}A'$且$\vdash\{A'\}_{[\alpha_1,\alpha_2]}(c)_1\{B\}$。$I$是一个解释。假定$\sigma\models^I A'$，于是 $Prob_{S^I_{A'}}(\{\sigma\models^I A'\mid\forall\sigma\in\Sigma.\ \sigma\models^I A'\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B\})=\alpha(\in[\alpha_1,\alpha_2])$且$\mathscr{C}_{env}[\![c]\!](S^I_{A'}\cap Dom.\ I_c)\sqsubseteq_1 S^I_B$。

从而再由定义 12 可知 $Prob_{S^I_A}(\{\sigma\models^I A\mid\forall\sigma\in\Sigma.\ \sigma\models^I A\Rightarrow\mathscr{C}_{env}[\![c]\!]\sigma\models^I B\})\leqslant 1$且$\mathscr{C}_{env}[\![c]\!](S^I_A\cap Dom.\ I_c)\sqsubseteq_1 S^I_B$。

于是$\vdash\{A\}_{[0,1]}(c)_1\{B\}$。故拟推理规则 2 是可靠的。

根据规则归纳原理便有，每一条定理都是有效的。

结束语 鉴于 Hoare 逻辑理论上证明是正确的程序，实际执行时却可能会出错等现象，同时为了对此现象进行刻画，本文基于经典 Hoare 逻辑提出了一种$[\alpha_1,\alpha_2]$1-概率拟 Hoare 逻辑用于量化程序的正确执行情况，度量程序实际执行与理论之间的差距，反映理论被实际程序实现的程度，进一步地，证明了该逻辑的可靠性。在接下来的工作中，我们会深入研究更复杂的概率拟 Hoare 逻辑形式，同时，考虑如何将本文所提出的$[\alpha_1,\alpha_2]$1-概率拟 Hoare 逻辑理论应用到软件工程的实际中，并基于该理论开发相应的工具。

参 考 文 献

[1] Floyd R W. Assigning Meanings to Programs[M]// Schwartz J T, A M S, eds. Proceedings of Symposium on Applied Mathematics. 1967:19-32

[2] 周巢尘. 形式语义学引论[M]. 长沙：湖南科学技术出版社，1985

[3] Hoare C A R. An Axiomatic Basis for Computer Programming [J]. Communications of The ACM, 1969, 12(10):576-580, 583

[4] Apt K R. Ten Years of Hoare's Logic: A Survey Part-I[J]. ACM Transactions on Programming Languages and Systems, 1981, 3(4):431-483

[5] Jones C B, Roscoe A W, Wood K R, et al. Reflections on the Work of C. A. R. Hoare[M]. Springer-Verlag, 2010

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

[7] 王志坚，费玉奎，娄渊清. 软件构件技术及其应用[M]. 北京：科学出版社，2005

[8] 严士健，王隽骧，刘秀英. 概率论基础(第二版)[M]. 北京：科学出版社，2009

[9] 丁万鼎. 测度论概要[M]. 合肥：安徽人民出版社，2005

[10] 严加安. 测度论讲义(第二版)[M]. 北京：科学出版社，2004

[11] Chung K L. A Course in Probability Theory (Third Edition) [M]. Academic Press, 2001

[12] Hailperin T. Probability Logic[J]. Notre Dame Journal of Formal Logic, 1984, 25(3):198-212

[13] 王国俊，王伟. 逻辑度量空间[J]. 数学学报，2001，44(1)：159-168

[14] Wu Xin-xing, Hu Guo-sheng. Trustworthiness Measurements of Real-time Web Services[C]// 2014 International Conference on E-Commerce, E-Business and E-Service (EEE 2014). 2014, 5

[15] 吴新星，胡国胜，陈仪香. 构件近似匹配的度量研究[J]. 计算机科学，2014，41(5)：190-195

[16] 吴新星，胡国胜，陈仪香. Web 服务降级替换的一致性问题及量化研究[J]. 计算机科学，2015，42(2)：81-85，94

[17] 吴新星，李俊燕. 系统可信性度量可视化软件 v2.0[P]. 2014，8

(上接第 85 页)

[12] 郝国生，巩敦卫，史有群，等. 交互式遗传算法的机器代替用户方法[J]. 模式识别与人工智能，2006，19(1)：111-115

[13] 蒋培. 基于共同进化遗传算法的机器学习[J]. 湖南师范大学学报，2004，27(3)：33-38

[14] 崔嘉，刘弘. 遗传算法在计算机辅助创新作曲中的应用[J]. 计算机工程与应用，2007，43(3)：198-206

[15] 陈群，宴克非. 考虑公交优先的城市交叉口遗传算法信号配时研究[J]. 系统工程理论与实践，2005，11：133-138

[16] 刘伯鸿，李国宁，洪玲娇. 基于遗传算法的信号联锁故障处理中风险问题[J]. 兰州交通大学学报，2005，24(4)：103-105

[17] 梁旭，黄明. 基于学习机制的退火并行遗传算法应用研究[J]. 系统工程学报，2006，21(6)：663-66

[18] 王鼎，吴瑛. 基于改进遗传算法的矩阵联合对角化[J]. 电子与信息学报，2007，29(3)：578-581

[19] 邵克勇，李飞，等. 基于改进遗传算法的双向 BP 神经网络控制[J]. 化工自动化及仪表，2010，37(10)：18-21

[20] 玄光男，程润伟. 遗传算法与工程设计[M]. 北京：科学出版社，2000