ISSN 1000-1239/CN 11-1777/TP
50(3): 626-635, 2013

软件动态正确性的形式化描述

马艳芳[1,2] 张 敏[2] 陈仪香[2]
[1](淮北师范大学计算机科学与技术学院 安徽淮北 235000)
[2](上海市高可信计算重点实验室(华东师范大学软件学院) 上海 200062)
(yfma@sei.ecnu.edu.cn)

Formal Description of Software Dynamic Correctness

Ma Yanfang[1,2], Zhang Min[2], and Chen Yixiang[2]
[1](*School of Computer Science and Technology, Huaibei Normal University, Huaibei, Anhui* 235000)
[2](*Shanghai Key Laboratory of Trustworthy Computing* (*Software Engineering Institute, East China Normal University*), *Shanghai* 200062)

Abstract Correctness is a key attribute of software trustworthiness. Abstractly, software correctness can be represented as whether or not the implementation of software satisfies its specification. However, in the real world, it is difficult to get the satisfaction absolutely. In the course of developing and designing software, implementation is often modified in order to satisfy its specification. This means that the software is more and more close to correctness, i.e. software correctness is a dynamic course. In order to describe the dynamic correctness of software, in this paper, the abstract characterization and the limit theory of dynamic correctness based on parameterized bisimulation are proposed. Firstly, the infinite evolution mechanism of parameterized bisimulation is established. Parameterized limit bisimulation is defined in order to characterize the relation between a series of software implementations obtained in the real design and its specification, and some special examples are shown. Secondly, parameterized bisimulation limit is given, and the recursive characterization of parameterized bisimulation limit is stated. Finally, some algebraic properties are proved, such as the uniqueness of parameterized bisimulation limit and the consistence between parameterized bisimulation limit and parameterized bisimulation.

Key words correctness of software; parameterized bisimulation; formalization; limit; topology

摘 要 软件正确性是一个逐渐改进的过程.通过不断地修改,软件越来越接近于正确.同时软件的执行依赖于环境.为了刻画软件的动态正确性并考虑环境的因素,以参数化互模拟为基础,利用极限的观点,建立软件动态正确性的形式化描述.首先建立参数化互模拟的无限演化理论,给出参数化极限互模拟的定义,并给出几个特殊的参数化极限互模拟实例.其次,建立参数化互模拟极限,给出参数化互模拟极限的规约刻画.最后,证明参数化互模拟极限的唯一性、与参数化互模拟的相容性等代数性质.

关键词 软件正确性;参数化互模拟;形式化;极限;拓扑

中图法分类号 TP301.2

收稿日期:2011-01-18;**修回日期**:2012-03-27

基金项目:国家自然科学基金项目(91118007);中央高校基本科研业务费专项基金项目(78210045);安徽省高等学校省级自然科学研究项目(KJ2011A248,KJ2012Z347);上海市高可信计算重点实验室开放课题项目(07dz22304201004);安徽省淮北师范大学青年科学基金项目(700583)

随着人们对软件功能要求的不断增加,软件系统变得日趋庞大和难以控制,很多时候不以人们预期的方式工作.软件并不总是让人信任的,从而软件可信性问题越来越得到人们的关注[1].软件的可信性是在软件的正确性、可靠性、安全性等众多属性基础上发展起来的一个新概念.软件正确性是软件可信研究中一个重要内容.软件的正确与否直接关系到软件的运行效果.软件正确性主要体现在软件的执行结果能否符合人们的预期.在抽象层次上,可以把软件的执行结果抽象为软件的实现,而人们的预期抽象为软件的规范,由此软件的正确性抽象为软件的实现能否符合其规范.这种抽象表示可以借助于进程代数理论中的各种等价关系来刻画.

在实际中交互和并发是非常必要的,为了讨论这种复杂系统的行为特征,发展了很多进程代数理论,如通信系统演算(calculus of communication system, CCS)[2-5],CSP[6-7],ACP[8]和 Petri 网[9]等.而 CCS 更加侧重于从数学角度来建立并发理论的语义描述,其中最重要的内容是提出了互模拟等价和观测等价概念,这些概念为刻画一个系统的实现与其规范之间的关系提供了抽象描述.若系统的实现与其规范之间存在互模拟等价或观测等价关系,则在一定程度上认为这个系统是正确的.

在实际的软件开发和设计过程中,软件实现都是在一定物理设备(如计算机)下运行的,而物理设备不能保证其运行是完全可靠的,软件实现很难达到完全满足其规范,在很大程度上,软件的实现近似于其规范,即软件是近似正确的.这种近似性可以从两个方面来考虑.一方面,从静态的观点看,给定一个实现,其与规范之间可能会存在一定的误差,但这种误差是被允许的.由此实现可以看成是规范的近似版本.而实现在多大程度上近似规范是需要进行描述和度量的.对于这种近似正确性的抽象描述,基于不同的进程演算理论,如 CCS,CSP,概率进程演算、自动机、Petri 网等已经产生了很多的结果.在概率进程代数基础上,已经提出了概率的 ε-互模拟等价关系[10],并以进程所执行相同动作的概率差为基础,提出了一种进程之间的度量模型.在概率 CSP 的基础上,根据进程所执行动作,引入折扣因子,建立了另一种度量模型[11],这种度量与文献[10]中的相比较,更加全面合理地描述了进程之间的近似性.基于自动机理论,研究者提出了一种动作标号量化转换系统(action-labeled quantitative transition system)[12],根据进程执行的状态定义了一种度量,作为从非量化系统到量化系统的一种延拓.基于 Petri 网,根据进程的观测动作建立了进程之间的度量关系[13].基于 CCS,建立了 λ-强(弱)互模拟关系[14-15],用来比较进程之间的关系.根据进程与执行环境的拒绝关系,在 2/3 模拟的基础上,建立进程之间的度量关系[16].这些度量模型,都从不同的角度建立进程之间的度量.在实际应用中,可以根据不同的需要,选择不同的度量模型.近似正确性的另一方面可以从动态的观点来考虑实现与规范的近似性.假定一系列实现被给定,这些实现都越来越近似规范,这样实现序列的趋势是越来越满足规范,也就说软件越来越接近于正确.对于这种近似趋势的抽象描述,在强(弱)互模拟的基础上,已建立其抽象描述[17].然而,软件的运行依赖于环境,在从动态的观点来考虑实现与规范的近似性描述时,需要考虑环境的因素.

软件对环境的依赖主要体现在软件与环境的交互,最基本的交互是软件与环境之间的接受和拒绝关系[18].基于软件与环境的拒绝关系,以 2/3 互模拟为基础,从动态的角度已经建立了实现与规范的近似性描述[19].而由 Larsen 提出的参数化互模拟[20]在一定程度上更加适合描述软件与环境之间的接受关系.与文献[11-17]的工作相比较,文献[11-17]中所建立的各种度量模型,使用的互模拟关系主要是基于不同的进程代数理论,对强或弱互模拟关系的一种改进.这些互模拟可以用来描述软件实现与规范之间的近似度量关系,但是这些互模拟关系没有反映软件实现和规范与其所处的环境之间的关系.为了描述软件与环境之间的关系,一个主要的问题是如何来描述环境,同时还需要考虑其与软件规范和实现的关系,故从最基本的互模拟关系出发.参数化互模拟虽然其提出的时间较早,但其以一个标号转换系统为参数一般化了强互模拟.作为参数的标号转换系统反映了软件规范和实现的上下文环境.而软件实现满足其规范也需要在任意的上下文环境下保持.如,可以把软件的一些物理设备或软件支持等环境抽象为实现和规范的上下文环境.当上下文环境的信息发生变化时,相应的实现和规范也要做出相应的变化.由此,可以把与上下文有关的信息抽象为一个标号转换系统.这个转换系统显示地给出了环境之间的转换关系.当使用参数化互模拟来验证软件的近似正确性时,只能静态描述实现与规范之间的关系,而对于动态近似正确的描述,还没有得到考虑.本文将以参数化互模拟为基础,建立参数化互模拟的无限演化理论和极限理论.提出参

数化极限互模拟和参数化互模拟极限的概念,它们在一定程度上刻画了在参数化互模拟下,软件规范是其实现的极限形式.

1 进程通信演算(CCS)基础

1.1 CCS 的语法和语义

令 Δ 表示动作名集合,其元素用小写字母 $a,b,c\cdots$ 表示. $\bar{\Delta}=\{\bar{a}:a\in\Delta\}$ 表示补动作名集合. 规定 $\bar{a}$ 表示 a. 令 $\Gamma=\Delta\cup\bar{\Delta}$,称为标号集合(也称可观测动作集),其元素用 $l,\bar{l},k,\bar{k},h,\bar{h}\cdots$ 表示. τ 作为内部动作,即不可观测动作,$\bar{\tau}=\tau$. 所有动作的集合用 Act 表示,即 $Act=\Gamma\cup\{\tau\}$,其元素用 $\alpha,\beta\cdots$ 表示. 集合 Γ 上的映射 $f:\Gamma\to\Gamma$,如果满足任意 $l\in\Gamma$ 有 $f(\bar{l})=\overline{f(l)}$,则称 f 为重新标号函数. 如果增加 $f(\tau)=\tau$,则 f 可延拓到集合 Act 上. 对于 Γ 的任何一个子集 X,定义 $\bar{X}\overset{\text{def}}{=}\{\bar{l}:l\in X\}$,$X^{\tau}\overset{\text{def}}{=}X\cup\{\tau\}$. 进一步,令 $\mathcal{S}$ 表示进程变量集合,K 表示进程常量集合,用 I 或 J 表示索引集合. 下面定义进程表达式的集合.

定义 1. 进程表达式[2]. 进程表达式集合 $\mathcal{E}$ 是包含 $\mathcal{S}$,K 和下列表达式的最小集合,其中 $E,E_i\in\mathcal{E}$:

$$E::=\alpha.E\mid E_1\mid E_2\mid\sum_{i\in I}E_i\mid E\backslash L\mid E[f].$$

若进程表达式 E 中的变量 Y 只在其形如 $l.F$ 的子表达式中出现,则称变量 Y 在 E 中是 Guarded. 如果一个进程表达式中不含有变量,称这个表达式是一个进程. 把所有进程构成的集合记为 $\mathcal{P}$,其中的元素用 $P,Q,W\cdots$ 表示. 令 $B\in K$,一般地 B 有如下的定义方程:$B\overset{\text{def}}{=}P_B$,其中 $P_B\in\mathcal{P}$,如 $B\overset{\text{def}}{=}a.B'$,$B'\overset{\text{def}}{=}c.B$. 常量在进程演算中提供了一种归约机制. 接下来只讨论形如 $B=\sum_{i\in I}l_i.P_i$ 的常量定义,其中 P_i 可以包含 B,$l_i\in\Gamma$.

下面给出 CCS 的操作语义.

定义 2. 标号转换系统[2]. 在 Act 集合上的标号转换系统是一个三元组$(\mathcal{E},Act,\{\overset{\alpha}{\to}:\alpha\in Act\})$,转换关系 $\overset{\alpha}{\to}(\alpha\in Act)$ 由下面规则给出:

$$Act:\frac{}{\alpha.E\overset{\alpha}{\to}E}.$$

$$Sum_j:\frac{E_j\overset{\alpha}{\to}E_j'}{\sum_{i\in I}E_i\overset{\alpha}{\to}E_j'}(j\in I).$$

$$Com_1:\frac{E\overset{\alpha}{\to}E'}{E\mid F\overset{\alpha}{\to}E'\mid F}.$$

$$Com_2:\frac{F\overset{\alpha}{\to}F'}{E\mid F\overset{\alpha}{\to}E\mid F'}.$$

$$Com_3:\frac{E\overset{l}{\to}E'F\overset{\bar{l}}{\to}F'}{E\mid F\overset{\tau}{\to}E'\mid F'}.$$

$$Res:\frac{E\overset{\alpha}{\to}E'}{E\backslash L\overset{\alpha}{\to}E'\backslash L}(\alpha,\bar{\alpha}\notin L).$$

$$Rel:\frac{E\overset{\alpha}{\to}E'}{E[f]\overset{f(\alpha)}{\to}E'[f]}.$$

$$Con:\frac{P_B\overset{\alpha}{\to}P'}{B\overset{\alpha}{\to}P'}(B\overset{\text{def}}{=}P_B).$$

自然地,根据转换规则可以定义含有一串标号的转换. 如果 $t=\alpha_1,\cdots,\alpha_n\in Act^*=\bigcup_{n=0}^{\infty}Act^n$,且存在 $E_1,\cdots,E_{n-1},E'\in\mathcal{E}$,使得:

$$E\overset{\alpha_1}{\to}E_1\overset{\alpha_2}{\to}\cdots\overset{\alpha_{n-1}}{\to}E_{n-1}\overset{\alpha_n}{\to}E',$$

则称 t 是 E 的一个动作序列,E' 是 E 的一个 t 阶导出,记为 $E\overset{t}{\to}E'$.

接下来主要考虑标号转换系统$(\mathcal{E},Act,\{\overset{\alpha}{\to}:\alpha\in Act\})$在 $\mathcal{P}$ 上的限制$(\mathcal{P},Act,\{\overset{\alpha}{\to}|_{\mathcal{P}}:\alpha\in Act\})$,其中对每一个 α,$\overset{\alpha}{\to}|_{\mathcal{P}}=\overset{\alpha}{\to}\cap(\mathcal{P}\times\mathcal{P})$. 在不引起混淆的情况下,用 $\overset{\alpha}{\to}$ 来表示 $\overset{\alpha}{\to}|_{\mathcal{P}}$.

1.2 参数化互模拟

Larsen 在 1986 年首次提出参数化互模拟[20],把与上下文环境 $\mathcal{C}$ 有关的信息抽象为一个标号转换系统,在这个系统中,每个状态都是一个环境对象,这个环境对象消耗进程产生的动作. 类似于进程,一个环境对象在消耗一个动作以后可以达到另一个环境对象. 由此看出这个环境实际上是一个进程. 但是给定一个环境的转换系统,其消耗能力是有限的. 如果进程 P 存在转换 $P\overset{\alpha}{\to}P'$,但是环境对象 e 不能消耗这个动作 α,则当进程 P 在环境 e 下执行时,导出 $P\overset{\alpha}{\to}P'$ 将从来不会发生. 在参数化互模拟中把内部动作 τ 认为和其他动作一样,这样就产生了一个非常严格的环境转换系统和参数化互模拟. 参数化互模拟可以用来从接受环境角度验证软件实现与规范之间的关系. 下面回顾一下参数化互摸拟的相关定义,详细内容可参考文献[20].

定义 3. 环境转换系统. 如果 Es 是环境对象集合,A 是动作集合(与 Act 相同),$\to_{\varepsilon}\subseteq Es\times A\times Es$,

则标号转换系统 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 称为环境转换系统,其中 $\rightarrow_\varepsilon$ 称为消耗关系,$e\xrightarrow{\alpha}_\varepsilon e'$ 称为环境 e 可以消耗动作 α 且消耗此动作后变为环境 e'.

定义 4. ε-参数化互模拟. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统. 一个 ε-参数化互模拟 R 是进程集合 $\mathcal{P}$ 上二元关系 Es-索引族,即任意 $e\in Es$,$R_e\subseteq\mathcal{P}\times\mathcal{P}$ 且满足只要 $(P,Q)\in R_e$,$e\xrightarrow{\alpha}_\varepsilon f$ 就有下面的条件成立:

1) 若 $P\xrightarrow{\alpha}P'$,则存在 $Q'\in\mathcal{P}$,使得 $Q\xrightarrow{\alpha}Q'$ 且 $(P',Q')\in R_f$;

2) 若 $Q\xrightarrow{\alpha}Q'$,则存在 $P'\in\mathcal{P}$,使得 $P\xrightarrow{\alpha}P'$ 且 $(P',Q')\in R_f$.

两个进程 P 和 Q 被称为在环境 e 下是互模拟等价当且仅当存在一个 ε-参数化互模拟 R,使得 $(P,Q)\in R_e$,$P\sim_e Q$.

命题 1. 设 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统. 任意环境 $e\in Es$,$P,Q\in\mathcal{P}$,如果 $P\sim Q$,则 $P\sim_e Q$.

命题 1 表明参数化互模拟一般化了强互模拟.

命题 2. 设 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统,$e\xrightarrow{\alpha}_\varepsilon f$ 当且仅当:

1) 若 $P\xrightarrow{\alpha}P'$,则存在 $Q'\in\mathcal{P}$,使得 $Q\xrightarrow{\alpha}Q'$ 且 $P'\sim_f Q'$;

2) 若 $Q\xrightarrow{\alpha}Q'$,则存在 $P'\in\mathcal{P}$,使得 $P\xrightarrow{\alpha}P'$ 且 $P'\sim_f Q'$.

命题 3. 设 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统,Id 表示进程集合上恒等关系的 Es-索引族,即任意 $e\in Es$,$Id_e=\{(P,P):P\in\mathcal{P}\}$,则 Id 是 ε-参数化互模拟.

由于考虑的是 Es-索引族,为了以后讨论方便,给出下面的定义. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是环境转换系统. 任意 Es-索引族 R 和 S:

1) $R\subseteq S$ 当且仅当任意 $e\in Es$,$R_e\subseteq S_e$;

2) $R\cap S$ 是一个 Es-索引族且 $(R\cap S)_e=R_e\cap S_e$;

3) $R\cup S$ 是一个 Es-索引族且 $(R\cup S)_e=R_e\cup S_e$.

2 参数化极限互模拟

为了保证软件的正确性,软件在实际开发设计时,需要对软件实现与规范之间的关系作一些验证,以便进一步完善和修改软件的实现版本. 在不断修改过程中得到一系列软件实现,这些实现越来越近似于规范. 抽象地,这些实现版本可以通过拓扑学中的网来刻画. 如一个软件有几个模块组成,每个模块由一个开发团队完成. 不妨设一个软件由两个模块 B_1,B_2 组成,若对 B_1 进行修改后,再与 B_2 合成,得到实现 A_1,若对 B_2 进行修改,再与 B_1 合成得到实现 A_2. 但若在某一个时刻,同时修改了 B_1 和 B_2,此时将无法比较 A_1 与规范之间的近似程度和 A_2 与规范之间的近似程度哪个更好. 但若将同时修改 B_1 和 B_2 后得到的实现记为 A_3,总有 A_3 与规范之间的近似程度比 A_2 和 A_1 都要好. 由此,这种对软件实现进行修改的过程,用序列可能不足以描述,为了达到数学上的严格性,可以借助于拓扑学中的网来刻画.

2.1 定向集

定义 5. 定向集[21]. 令 D 是非空集合,$\leqslant$ 是 D 上的二元关系. 如果 $\leqslant$ 满足下面的条件,则称 $(D,\leqslant)$ 为定向的:

1) $\leqslant$ 是自反的:每一个 $m\in D$,有 $m\leqslant m$;

2) $\leqslant$ 是传递的:若 $m,n,p\in D$ 且 $m\leqslant n$,$n\leqslant p$,则 $m\leqslant p$;

3) 若 $m,n\in D$,则存在 $p\in D$,使得 $m\leqslant p$,$n\leqslant p$.

定义 6. 共尾[21]. 令 C,D 是定向集合. 如果 $N:C\rightarrow D$ 是一个映射,使得对任意 $n\in D$,存在 $m\in C$,$p\geqslant m$,都有 $N_p=N(p)\geqslant n$,则称 (C,N) 为 D 的共尾.

定义 7. 共尾子集[21]. 令 $(D,\leqslant)$ 是定向集,$C\subseteq D$ 也是定向集. 如果对任何 $n\in D$,存在 $m\in C$,使得 $n\leqslant m$,即 (C,in_C) 是 D 的共尾,则称 C 为 D 的共尾子集.

定义 8. 网[21]. 令 $(D,\leqslant)$ 是定向集合,U 是非空集合. 从 D 到 U 的映射 S 称为 U 在 D 上一个网,通常用 $\{S_n:n\in D\}$ 来表示,其中每一个 $n\in D$,有 $S_n=S(n)\in U$.

定义 9. 子网[21]. 令 $\{S_n:n\in D\}$ 和 $\{T_m:m\in C\}$ 是网. 如果存在映射 $N:C\rightarrow D$,满足下面的条件,则称 $\{T_m:m\in C\}$ 是 $\{S_n:n\in D\}$ 的子网:

1) $T_m=S_{N_m}$,$\forall m\in C$;

2) (C,N) 是 D 的共尾.

定义 10. 最终[22]. 设 D 是定向集,$\{Q_n:n\in D\}$ 是网. 如果存在 $n_0\in D$,使得 $n\geqslant n_0$,Q_n 具有某个性质 pro,则称这个网最终具有性质 pro.

把进程集合 $\mathcal{P}$ 上的所有进程网构成的集合记为 $\mathcal{P}_N$. 若 $\{P_n:n\in D\}\in\mathcal{P}_N$,则 D 是一个定向集,任

意 $n\in D, P_n\in \mathcal{P}$.

2.2 参数化极限互模拟

在本节中,试图将定义 4 推广到进程集合和进程网集合上的关系,并且为了讨论进程集合和进程网集合上的恒等关系,提出在环境转换系统下进程的确定性描述.

定义 11. 参数化极限互模拟. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$是环境转换系统. 一个 ε-参数化极限互模拟 R 是进程集合和进程网集合上二元关系的 Es-索引族,即任意 $e\in Es, R_e\subseteq \mathcal{P}\times \mathcal{P}_N$ 且满足下面的条件,任意$(P,\{Q_n:n\in D\})\in R_e, e\xrightarrow{\alpha}_\varepsilon f$:

1) 如果 $P\xrightarrow{\alpha}P'$,则存在进程网$\{Q'_n:n\in D\}\in \mathcal{P}_N$ 和 $n_0\in D$,使得每一个 $n\geqslant n_0, Q_n\xrightarrow{\alpha}Q'_n$ 且$(P',\{Q'_n:n\in D\})\in R_f$;

2) 如果 C 是 D 的共尾子集且任意 $m\in C$, $Q_m\xrightarrow{\alpha}Q'_m$,则存在 $P'\in\mathcal{P}$ 和 C 的共尾子集 B,使得 $P\xrightarrow{\alpha}P'$且$(P',\{Q'_k:k\in B\})\in R_f$.

从定义 11 可以看出,ε-参数化极限互模拟是ε-参数化互模拟的动态形式. 这种动态性体现在参数化极限互模拟可以用来描述一系列进程与另一进程之间的关系. 进而可以用来描述软件在修改过程中得到的一系列实现与规范之间是否能够满足参数化互模拟. 语句 1)表示如果 P 在环境 e 下执行动作 α,则$\{Q_n:n\in D\}$在环境 e 下也能执行此动作 α. 语句 2)说明如果$\{Q_n:n\in D\}$在环境 e 下经常能够执行动作 α,则进程 P 在环境 e 下也能执行动作 α.

在参数化互模拟中一个重要的性质是恒等关系的 Es-索引族 Id 是参数化互模拟. 自然地,想把 Id 推广到参数化极限互模拟的情况. 一个通常的想法是:在每个环境 e 下,进程集合和进程网集合上的二元关系是每个进程和它的常量网有关系,但是当进程是非确定的,这个关系未必是参数化极限互模拟的. 因此,需要在相关的进程上定义一定的确定性. 由于进程是依赖于环境的,故需引入进程在 ε-环境转换系统下的确定性.

定义 12. 在环境 e 下的基. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$是一个环境转换系统,$e\in Es, \Omega\subseteq\mathcal{P}, \Theta\subseteq\Omega$. 如果对任意 $P\in\Omega$,存在 $Q\in\Theta$ 使得 $P\sim_e Q$,则称 Θ 是 Ω 在环境 e 下的基.

定义 13. 在环境 e 下的 t-导出(derivative). 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$是一个环境转换系统,$e$ 是进程 P 的环境且存在 $t\in Act^*$,使得 $e\xrightarrow{t}_\varepsilon f$. 如果存在 $P'\in\mathcal{P}$,使得 $P\xrightarrow{t}P'$,则称 P'是进程 P 在环境 e 下的 t-导出且 P'的环境为 f.

定义 14. 在环境 e 下的 λ-确定. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$是一个环境转换系统,$P\in\mathcal{P}$,$\lambda$ 是一个基数(cardinal number). 对进程 P 在环境 e 下的每个导出 Q,假设 Q 的环境为 f,且有转换 $f\xrightarrow{\beta}_\varepsilon h$,如果集合$\{Q':Q\xrightarrow{\beta}Q'\}$在环境 h 下有一个基 Θ,且$|\Theta|<\lambda$,则称 P 在环境 e 下是 λ-确定的.

定义 15. 在环境下的强确定. 设 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$是一个环境转换系统,$P\in\mathcal{P}$是一个进程,且 P 的环境为 e. 若 P 在环境 e 下的每个导出 Q,不妨设 Q 的环境为 f,只要 $f\xrightarrow{\alpha}_\varepsilon h, \alpha\in Act$ 且 $Q\xrightarrow{\alpha}Q', Q\xrightarrow{\alpha}Q''$就有 $Q'\sim_h Q''$,则称 P 在环境 e 下是强确定的.

定义 15 表明在 CCS 中进程的强确定性可以推广到在环境转换系统下的强确定性.

命题 4 说明进程在环境下的 λ-确定性关于其导出是封闭的.

命题 4. 如果 P 在环境 e 下是 λ-确定的,P'是 P 的 t 阶导出,P'的环境为 f,则 P'在环境 f 下也是 λ-确定的.

证明. 令 V 是 P'在环境 f 下的导出,且 g 是 V 所在的环境. 则存在 $t'\in Act^*$,使得 $f\xrightarrow{t'}_\varepsilon g$ 且 $P'\xrightarrow{t'}V$. 假设 $g\xrightarrow{\beta}_\varepsilon h$,需要证明集合$\{V':V\xrightarrow{\beta}V'\}$在环境 h 下存在基 Θ 且$|\Theta|<\lambda$. 事实上,V 也是 P 在环境 e 下的导出,由于 P 在环境 e 下是 λ-确定的,所以集合$\{V':V\xrightarrow{\beta}V'\}$在环境 h 下有基 Θ 且$|\Theta|<\lambda$. 因此 P'在环境 f 下也是 λ-确定的. 证毕.

命题 5 陈述了在环境下的 λ-确定保持ε-参数化互模拟等价.

命题 5. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$是一个环境转换系统,$P$ 在环境 e 下是 λ-确定的,且 $P\sim_e Q$. 则 Q 在环境 e 下也是 λ-确定的.

证明. 令 V 是 Q 在环境 e 下的 t 阶导出,即存在 $t\in Act^*, f\in Es$,使得 $e\xrightarrow{t}_\varepsilon f$ 且 $Q\xrightarrow{t}V$,V 的环境为 f. 由于 $P\sim_e Q$,所以存在 $U\in\mathcal{P}$,使得 $P\xrightarrow{t}U$ 且 $V\sim_f U$. 又因为 P 在环境 e 下是 λ-确定的,令 $f\xrightarrow{\alpha}_\varepsilon h$,因此集合$\{U':U\xrightarrow{\alpha}U'\}$在环境 h 下有基 Θ 且$|\Theta|<\lambda$.

由于 $V\sim_f U$,对任意 $U'\in\Theta$,存在 $V(U')\in\mathcal{P}$,使得 $V\xrightarrow{\alpha}V(U')\sim_h U'$. 令:

$$\Lambda = \{V(U'):U' \in \Theta\},$$

则 $\Lambda \subseteq \{V':V \xrightarrow{\alpha} V'\}$ 且 $|\Lambda| \leqslant |\Theta| < \lambda$. 同时对任意 $V' \in \mathcal{P}$, 如果 $V \xrightarrow{\alpha} V'$, 则存在 $U' \in \mathcal{P}$, 使得 $U \xrightarrow{\alpha} U' \sim_h V'$. 更进一步, 因为 Θ 是集合 $\{U':U \xrightarrow{\alpha} U'\}$ 的基, 所以存在 $U'' \in \mathcal{P}$, 使得 $U'' \sim_k U'$, 这样 $V(U'') \sim_k U'' \sim_k U' \sim_k V'$, 因此 Λ 是集合 $\{V':V \xrightarrow{\alpha} V'\}$ 的基. 故 Q 在环境 e 下也是 λ-确定的. 证毕.

接下来讨论将参数化互模拟 Id 推广到参数化极限互模拟的情况. 令 D 是定向集合, $cf(D) = \inf\{|D'|:D' \text{是 } D \text{ 的共尾子集}\}$, 其中 $|D'|$ 表示集合 D' 中元素的个数.

定理 1. 令 $\varepsilon = (Es, A, \rightarrow_\varepsilon)$ 是一个环境转换系统. $Ilim$ 是进程集合和进程网集合上的二元关系的 Es-索引族, 任意 $e \in Es$, $Ilim_e = \{(P, \{Q_n:n \in D\}):P \in \mathcal{P}$, 且在 e 下是 $cf(D)$-确定的, $\{Q_n:n \in D\} \in \mathcal{P}_N$, 存在 $n_0 \in D$, 使得任意 $n \geqslant n_0, Q_n \sim_e P\}$, 则 $Ilim$ 是 ε-参数化极限互模拟.

证明. 令 $e \in Es$ 且 $e \xrightarrow{\alpha}_\varepsilon f$, $(P, \{Q_n:n \in D\}) \in Ilim_e$. 则 P 在环境 e 下是 $cf(D)$-确定的, 且存在 $n_0 \in D$, 使得任意 $n \geqslant n_0, Q_n \sim_e P$. 假设 $P \xrightarrow{\alpha} P'$, 由命题 2 可知, 对每一个 $n \geqslant n_0$, 存在 $Q'_n \in \mathcal{P}$, 使得 $Q_n \xrightarrow{\alpha} Q'_n$ 且 $Q'_n \sim_f P'$. 对 $n \not\geqslant n_0$, 选择 $\mathcal{P}$ 中的任意元素作为 Q'_n. 这样得到一个进程网 $\{Q'_n:n \in D\}$. 由命题 4 可知 P' 在环境 f 下是 $cf(D)$-确定的. 因此 $(P', \{Q'_n:n \in D\}) \in Ilim_f$.

另一方面, 设 C 是 D 的共尾子集, 且任意 $m \in C, Q_m \xrightarrow{\alpha} Q'_m$. 因为 $n_0 \in D$, 根据共尾子集的定义, 存在 $m_0 \in C$, 使得 $m_0 \geqslant n_0$. 由此根据 $Ilim$ 的定义可知, 每一个 $m \geqslant m_0, Q_m \sim_e P$. 又由于 $Q_m \xrightarrow{\alpha} Q'_m$, 所以每一个 $m \geqslant m_0$, 存在 $P'_m \in \mathcal{P}$, 使得 $P \xrightarrow{\alpha} P'_m \sim_f Q'_m$. 因为 P 在环境 e 下是 $cf(D)$-确定的, 所以存在 $M \subseteq C[m_0) = \{m \in C:m \geqslant m_0\}$ 且 $|M| < cf(D)$, 对每一个 $m \in C[m_0)$, 存在 $k \in M$, 使得 $P'_m \sim_f P'_k$. 每一个 $k \in M$, 定义 $C_k = \{m \in C[m_0):P'_m \sim_f P'_k\}$, 则 $\bigcup_{k \in M} C_k = C[m_0)$. 因为 C 是 D 的共尾子集且 $cf(C[m_0)) = cf(C) = cf(D) > |M|$, 故存在 $k_0 \in M$, 使得 C_{k_0} 是 $C[m_0)$ 的共尾子集. 这样对每一个 $m \in C_{k_0}$ 有 $Q'_m \sim_f P'_m \sim_f P'_{k_0}$ 成立并且 $(P'_{k_0}, \{Q'_m:m \in C_{k_0}\}) \in Ilim_f$. 注意到 C_{k_0} 是 C 的共尾子集, 进而完成了证明. 证毕.

令 $\varepsilon = (Es, A, \rightarrow_\varepsilon)$ 是一个环境转换系统, R 是进程集合和进程网集合上的二元关系的 Es-索引族, 即每一个 $e \in Es, R_e \subseteq \mathcal{P} \times \mathcal{P}_N$, 定义 $sub(R)$ 也是二元关系的 Es-索引族, 每一个 $e \in Es, sub(R)_e = \{(P, \{Q_n:n \in D\}):$ 存在 $(P, \{W_m:m \in C\}) \in R_e$, 使得 $\{Q_n:n \in D\}$ 是 $\{W_m:m \in C\}$ 的子网$\}$.

定理 2. 令 $\varepsilon = (Es, A, \rightarrow_\varepsilon)$ 是一个环境转换系统, R 是进程集合和进程网集合上的二元关系的 Es-索引族, 即每一个 $e \in Es, R_e \subseteq \mathcal{P} \times \mathcal{P}_N$. $sub(R)$ 是 ε-参数化极限互模拟当且仅当每一个 $e \in Es, e \xrightarrow{\alpha}_\varepsilon f$, $(P, \{Q_n:n \in D\}) \in R_e$ 下面条件成立:

1) 如果 $P \xrightarrow{\alpha} P'$, 则存在进程网 $\{Q_n:n \in D\} \in \mathcal{P}_N$ 和 $n_0 \in D$, 使得每一个 $n \geqslant n_0$, 都有进程 $Q_n \xrightarrow{\alpha} Q'_n$ 且 $(P', \{Q'_n:n \in D\}) \in sub(R)_f$.

2) 如果 C 是 D 的共尾子集, 且任意 $m \in C$, $Q_m \xrightarrow{\alpha} Q'_m$, 则存在 $P' \in \mathcal{P}$ 和 C 的共尾子集 B, 使得 $P \xrightarrow{\alpha} P'$ 且 $(P', \{Q_k':k \in B\}) \in sub(R)_f$.

证明. ($\Rightarrow$) 如果 $sub(R)$ 是 ε-参数化极限互模拟, 则每一个 $e \in Es, e \xrightarrow{\alpha}_\varepsilon f$, $(P, \{Q_n:n \in D\}) \in R_e$, $(P, \{Q_n:n \in D\}) \in sub(R)_e$, 所以由定义 11 可知命题成立.

($\Leftarrow$) 假设 $e \in Es, e \xrightarrow{\alpha}_\varepsilon f$, $(P, \{W_m:m \in C\}) \in sub(R)_e$ 且定理 2 中的条件 1) 和 2) 成立, 下面需要证明 $sub(R)$ 是 ε-参数化极限互模拟. 由 $sub(R)_e$ 的定义可知存在 $(P, \{Q_n:n \in D\}) \in R_e$, 使得 $\{W_m:m \in C\}$ 是 $\{Q_n:n \in D\}$ 的子网, 因此存在映射 $N:C \to D$ 使得 (C, N) 是 D 的共尾且每一个 $m \in C, W_m = Q_{N_m}$. 我们不妨假设 N 是增加的, 即 $p_1 \leqslant p_2$ 蕴含 $N(p_1) \leqslant N(p_2)$.

如果 $P \xrightarrow{\alpha} P'$, 因为 $(P, \{Q_n:n \in D\}) \in R_e$, 由假设存在进程网 $\{Q'_n:n \in D\} \in \mathcal{P}_N$ 和 $n_0 \in D$, 使得每一个 $n \geqslant n_0, Q_n \xrightarrow{\alpha} Q'_n$ 且 $(P', \{Q'_n:n \in D\}) \in sub(R)_f$. 因为 (C, N) 是 D 的共尾, 所以存在 $p_0 \in C$, 使得每一个 $p \geqslant p_0, N_p \geqslant n_0$. 对每一个 $p \in C$, 令 $W'_p = Q'_{N_p}$. 则对每一个 $p \geqslant p_0, W_p = Q_{N_p} \xrightarrow{\alpha} Q'_{N_p} = W'_p$, 且 $\{W_p':p \in C\}$ 是 $\{Q'_n:n \in D\}$ 的子网. 因此由 $(P', \{Q'_n:n \in D\}) \in sub(R)_f$ 可以得到 $(P', \{W'_p:p \in C\}) \in sub(R)_f$.

如果 F 是 C 的共尾子集, 每一个 $q \in F, W_q \xrightarrow{\alpha} W'_q$, 则 $N(F)$ 是 D 的共尾子集, 每一个 $q \in F$, 令 $Q'_{N_q} =$

W'_q. 则所有 $q\in F, Q_{N_q}=W_q\xrightarrow{a}W'_q=Q'_{N_q}$. 这样存在 $P'\in\mathcal{P}$ 和 $N(F)$ 的共尾子集 G, 使得 $P\xrightarrow{a}P'$ 且 $(P',\{Q'_r:r\in G\})\in sub(R)_f$. 因为 N 是单调增加的, 所以 $N^{-1}(G)$ 是 F 的共尾子集, 更进一步的 $\{Q'_r:r\in G\}=\{W'_q:q\in N^{-1}(G)\}$ 且 $(P',\{W'_q:q\in N^{-1}(G)\})\in sub(R)_f$, 进而完成了证明. 证毕.

推论 1. 如果 R 是 ε-参数化极限互模拟, 则 $sub(R)$ 是 ε-参数化极限互模拟.

推论 2. 如果对每一个 $i\in I$, S_i 是参数化极限互模拟, 则 $\bigcup_{i\in I}S_i$ 也是参数化极限互模拟.

3 参数化互模拟极限

在 2.2 节中我们主要给出参数化互模拟的无限演化理论, 这个无限演化理论为在参数化互模拟下建立软件实现与规范之间的动态近似性提供了工具. 本节提出参数化互模拟极限的概念, 这个极限描述了在参数化互模拟下软件规范是其实现的极限形式. 在这个极限定义中, 用一个进程网来刻画软件在修改过程中所得到的那些实现, 而软件规范定义为这个进程网的参数化互模拟极限.

3.1 参数化互模拟极限的定义

定义 16. 参数化互模拟极限. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是环境转换系统. 如果存在参数化极限互模拟 R 和环境 $e\in Es$, 使得 $(P,\{Q_n:n\in D\})\in R_e\subseteq\mathcal{P}\times\mathcal{P}_N$, 则称 P 为 $\{Q_n:n\in D\}$ 在环境 e 下的参数化互模拟极限, 记为 $P\sim_e\lim\limits_{n\in D}Q_n$. 令 $\sim_e\lim\limits_{n\in D}=\{(P,\{Q_n:n\in D\}):P\sim_e\lim\limits_{n\in D}Q_n\}$. 由推论 2 知 $\sim_e\lim\limits_{n\in D}=\bigcup\{$所有参数化极限互模$\}$ 是最大的参数化极限互模拟.

例 1. 令环境转换系统 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$. 其中 $Es=\{e\}$, $A=\{a\}$, $e\xrightarrow{a}_\varepsilon e$. 进程 $P\overset{\text{def}}{=}a.P$. 则在环境 e 下有 $P\sim_e\lim\limits_{n\in\omega}a.a.\cdots a.0$, 其中 a 出现 n 次, 且 $\sum\limits_{i\in\varnothing}E_i=0$.

事实上, 由于环境对象只有一个, 可以构造二元关系 $R_e=\{(P,\{a^{k_n}:n\in\omega\})$, 任意 $n\in\omega$, $k_n\in\omega$ 且 $\lim\limits_{n\to\infty}k_n=\infty\}$, 其中, 把任意 $n\in\omega$, $a.a.\cdots a.0$ 中 a 出现 n 次记为 a^n, 则 $(P,\{a^n:n\in\omega\})\in R_e$. 任取 $(P,\{a^{k_n}:n\in\omega\})\in R_e$, $\lim\limits_{n\to\infty}k_n=\infty$. 如果 $P\xrightarrow{a}P$, 需要证明存在 $\{Q'_n:n\in\omega\}$ 和 $n_0\in\omega$, 使得任意 $n\geqslant n_0$, $a^{k_n}\xrightarrow{a}Q'_n$ 且 $(P,\{Q'_n:n\in\omega\})\in R_e$. 由于任意 $n\in\omega$, $k_n\in\omega$ 都有 $\lim\limits_{n\to\infty}k_n=\infty$ 和 $\lim\limits_{n\to\infty}\max\{0,k_n-1\}=\infty$, 故 R_e 的定义知, $(P,\{a^{(\max\{0,k_n-1\})}:n\in\omega\})\in R_e$ 且存在 $n_0\in\omega$, 使得 $k_n\geqslant1$ 且任意 $n\geqslant n_0$, $a^{k_n}\xrightarrow{a}a^{(\max\{0,k_n-1\})}$, 这样存在 $\{Q'_n:n\in\omega\}=\{a^{(\max\{0,k_n-1\})}:n\in\omega\}$ 和 n_0, 使得任意 $n\geqslant n_0$, 有 $a^{k_n}\xrightarrow{a}Q'_n$ 且 $(P,\{Q'_n:n\in\omega\})\in R_e$. 另一方面, 若 C 是 ω 的共尾子集, 且任意 $m\in C$, $a^{k_m}\xrightarrow{a}A'_m$, 则根据共尾子集的定义, 我们可以假设 $C=\{n_l:l\in\omega\}$ 且 $\lim\limits_{l\to\infty}n_l=\infty$, 故对每一个 $m\in C$, 令 $A'_m=a^{(k_m-1)}$, 则 $\{A'_m:m\in C\}=\{a^{(k_{n_l}-1)}:l\in\omega\}$, 因为 $\lim\limits_{l\to\infty}n_l=\infty$, 所以 $(P,\{A'_m:m\in C\})\in R_e$. 由此证明了 R 是参数化极限互模拟. 证毕.

例 2. 令环境转换系统 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$. 如图 1 所示 $Es=\{e,f\}$, $e\xrightarrow{a}_\varepsilon f$, 进程 $P,Q\in\mathcal{P}$. 如图 2 所示, 且令每一个 $n\in D$, $Q_n=Q$, $Q'_n=Q_1$. 由此可以构造一个 Es-索引族 R, $R_e=\{(P,\{Q_n:n\in D\})\}$, $R_f=\{(P_1,\{Q'_n:n\in C\}):C$ 是 D 的共尾子集$\}$. 则 R 是 ε-参数化极限互模拟且 $P\sim_e\lim\limits_{n\in D}Q_n$.

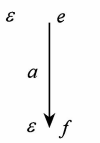
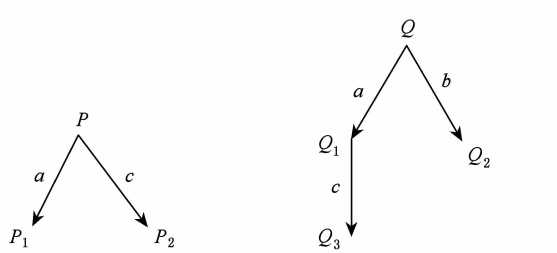


Fig. 1 Environment transitive system.

图 1 环境转换系统



(a) Process P. (b) Process Q.

Fig. 2 Process P and Q.

图 2 进程 P 和 Q

命题 6. 归约刻画. 若 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统, $e\in Es$ 且 $e\xrightarrow{a}_\varepsilon f$, 则 $P\sim_e\lim\limits_{n\in D}Q_n$ 当且仅当:

1) 如果 $P\xrightarrow{a}P'$, 则存在 $\{Q'_n:n\in D\}\in\mathcal{P}_N$ 和 $n_0\in D$, 使得每一个 $n\geqslant n_0$, $Q_n\xrightarrow{a}Q'_n$ 且 $P'\sim_e\lim\limits_{n\in D}Q'_n$;

2) 如果 C 是 D 的共尾子集, 对每一个 $m\in C$, $Q_m\xrightarrow{a}Q'_m$, 则存在 $P'\in\mathcal{P}$ 和 C 的共尾子集 B, 使得

$P \xrightarrow{\alpha} P'$ 且 $P' \sim_f \lim_{k\in B} Q_k'$.

证明. 由 $\sim_e \lim_{n\in D}$ 的定义及命题 6 可证. 证毕.

3.2 参数化互模拟极限的性质

命题 7 刻画了参数化互模拟极限与参数化互模拟是相容的,也就是说如果进程 P 和 Q 在环境 e 下是参数化互模拟的,则它们是同一个进程网在环境 e 下的极限.

命题 7. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统,$e\in Es$. 如果 $P\sim_e Q$ 且 $P\sim_e \lim_{n\in D} P_n$,则 $Q\sim_e \lim_{n\in D} P_n$.

证明. 需要找到一个 ε-参数化极限互模拟 R',使得 $(Q,\{P_n:n\in D\})\in R'_e$. 因为 $P\sim_e \lim_{n\in D} P_n$,因此存在 ε-参数化极限互模拟 R,使得 $(Q,\{P_n:n\in D\})\in R_e$. 构造 R' 是一个进程集合和进程网集合上二元关系的 Es-索引族. 对每一个 $f\in Es$,定义

$R'_f=\{(W,\{V_m:m\in C\}):$存在进程 $V\in\mathcal{P}$,使得 $W\sim_f V$ 且满足 $(V,\{V_m:m\in C\})\in R_f\}$.

下面证明 R' 是 ε-参数化极限互模拟. 令 $(W,\{V_m:m\in C\})\in R'_f$ 且 $f\xrightarrow{\alpha}_\varepsilon g$. 由 R' 的定义,存在 $V\in\mathcal{P}$,使得 $W\sim_f V$ 且 $(V,\{V_m:m\in C\})\in R_f$.

1) 如果 $W\xrightarrow{\alpha} W'$,则存在 $V'\in\mathcal{P}$,使得 $V\xrightarrow{\alpha} V'$ 且 $W'\sim_g V'$. 因为 $V\xrightarrow{\alpha} V'$ 且 $(V,\{V_m:m\in C\})\in R_f$,故存在进程网 $\{V'_m:m\in C\}\in\mathcal{P}_N$ 和 $m_0\in C$,使得任意 $m\geqslant m_0$,都有 $V_m\xrightarrow{\alpha} V'_m$ 且 $(V',\{V'_m:m\in C\})\in R_g$. 所以由 R' 的定义知 $(W',\{V'_m:m\in C\})\in R'_g$.

2) 如果 U 是 C 的共尾子集且对每一个 $u\in U$,都有 $V_u\xrightarrow{\alpha} V'_u$,则由 $(V,\{V_m:m\in C\})\in R_f$ 可知,存在 $V'\in\mathcal{P}$ 和 U 的共尾子集 B,使得 $V\xrightarrow{\alpha} V'$ 且 $(V',\{V'_k:k\in B\})\in R_g$. 因为 $W\sim_f V$,故存在 $W'\in\mathcal{P}$,使得 $W\xrightarrow{\alpha} W'$ 且 $W'\sim_g V'$. 这样由 R' 的定义可得 $(W',\{V'_k:k\in B\})\in R'_g$.

因此 R' 是 ε-参数化极限互模拟且 $(Q,\{P_n:n\in D\})\in R'_e$,且 $Q\sim_e \lim_{n\in D} P_n$.

命题 8 说明如果两个进程网 $\{P_n:n\in D\}$ 和 $\{Q_n:n\in D\}$ 在环境 e 下最终是参数化互模拟的,即存在 $n_0\in D$,使得任意 $n\geqslant n_0$,$P_n\sim_e Q_n$,则这两个进程网在环境 e 下具有相同的参数化互模拟极限.

命题 8. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统,$e\in Es$. 如果存在 $n_0\in D$,使得任意 $n\geqslant n_0$,$P_n\sim_e Q_n$ 且 $P\sim_e \lim_{n\in D} P_n$,则 $P\sim_e \lim_{n\in D} Q_n$.

证明. 类似命题 7 可证. 证毕.

命题 9 说明在环境转换系统下,参数化互模拟极限是唯一的.

命题 9. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统,$e\in Es$. 如果 $P\sim_e \lim_{n\in D} P_n$ 且 $Q\sim_e \lim_{n\in D} P_n$,则 $P\sim_e Q$.

证明. 因为 $P\sim_e \lim_{n\in D} P_n$ 和 $Q\sim_e \lim_{n\in D} P_n$,故存在 R^1 和 R^2 是 ε-参数化极限互模拟使得 $(P,\{P_n:n\in D\})\in R^1$,$(Q,\{P_n:n\in D\})\in R^2$.

令 $sub(R^1)\circ sub(R^2)$ 是进程和进程网上的二元关系的 Es-索引族,即对每一个 $e\in Es$ 定义

$$(sub(R^1)\circ sub(R^2))_e = sub(R^1)_e \circ sub(R^2)_e,$$

其中 $sub(R^1)_e\circ sub(R^2)_e=\{(U,W):$存在 $\{V_n:n\in D\}\in\mathcal{P}_N$,$(U,\{V_n:n\in D\})\in sub(R^1)_e$,$(W,\{V_n:n\in D\})\in sub(R^2)_e\}$.

需要证明 $sub(R^1)\circ sub(R^2)$ 是 ε-参数化互模拟. 假设 $e\xrightarrow{\alpha}_\varepsilon f$,$(U,\{V_n:n\in D\})\in sub(R^1)_e$ 并且 $(W,\{V_n:n\in D\})\in sub(R^2)_e$. 因为 R^1 和 R^2 是 ε-参数化极限互模拟,因此由推论 1 知 $sub(R^1)$ 和 $sub(R^2)$ 也是 ε-参数化极限互模拟.

1) 如果 $U\xrightarrow{\alpha} U'$,则存在 $\{V'_n:n\in D\}\in\mathcal{P}_N$ 和 $n_0\in D$,使得每一个 $n\geqslant n_0$,都有进程 $V_n\xrightarrow{\alpha} V'_n$ 且二元组 $(U',\{V_n:n\in D\})\in sub(R^1)_f$. 注意到 $D\lceil n_0$ 是 D 的共尾子集,因此存在 $W'\in\mathcal{P}$ 和 $D\lceil n_0$ 的共尾子集 B,使得 $W\xrightarrow{\alpha} W'$ 且 $(W',\{V'_k:k\in B\})\in sub(R^2)_f$. 因为 B 也是 D 的共尾子集,故 $\{V'_k:k\in B\}$ 是 $\{V'_n:n\in D\}$ 的子网,所以 $(U',\{V'_k:k\in B\})\in sub(R^1)_f$ 且 $(U',W')\in sub(R^1)_f\circ sub(R^2)_f$.

2) 如果 $W\xrightarrow{\alpha} W'$,则类似于 1)的方法可以证明存在 $U'\in\mathcal{P}$,使得 $U\xrightarrow{\alpha} U'$ 且 $(U',W')\in sub(R^1)_f\circ sub(R^2)_f$. 因此,$sub(R^1)\circ sub(R^2)$ 是 ε-参数化极限互模拟且 $(P,Q)\in(sub(R^1)\circ sub(R^2))_e$. 故,$P\sim_e Q$.

证毕.

命题 10. 令 $\varepsilon=(Es,A,\rightarrow_\varepsilon)$ 是一个环境转换系统. 如果存在 n_0,对每一个 $n\geqslant n_0$,P_n 在环境 e 下是强确定的且 $P\sim_e \lim_{n\in D} P_n$,则 P 在环境 e 下也是强确定的.

证明. 设 P 在环境 e 下的导出 Q,Q 的环境为 f,则 $e\xrightarrow{t}_\varepsilon f$,$P\xrightarrow{t} Q$. 若 $f\xrightarrow{\alpha}_\varepsilon h$ 且 $Q\xrightarrow{\alpha} Q'$,$Q\xrightarrow{\alpha} Q''$,则可以利用命题 6 $|t|+1$ 次,其中 $|t|$ 表示 t 的长度,得到存在进程网 $\{Q_n:n\in D\}$,$\{Q'_n:n\in D\}$ 和 $\{Q''_n:n\in$

$D\}\in\mathcal{P}_N$ 以及 $n_1,n_2\in D$,使得任意 $n\geqslant n_1$,$P_n\xrightarrow{t}Q_n\xrightarrow{\alpha}Q'_n$ 成立且 $Q'\sim_h\lim\limits_{n\in D}Q'_n$,同样地,任意 $n\geqslant n_2$,$P_n\xrightarrow{t}Q_n\xrightarrow{\alpha}Q''_n$ 成立且 $Q''\sim_h\lim\limits_{n\in D}Q''_n$. 因为 D 是定向集合,所以存在 $n_3\in D$,使得 $n_3\geqslant n_0,n_1,n_2$,因为任意 $n\geqslant n_3$,P_n 是强确定的,所以任意 $n\geqslant n_3$,$Q'\sim_h Q''_n$,再由命题 8 和命题 9 得 $Q'\sim_h Q''$. 证毕.

4 结 论

在本文中主要以 CCS 语言为基础,形式化描述了软件实现与其规范之间的动态关系. 利用拓扑学中的网极限理论,基于参数化互模拟,形式化描述了软件规范是其实现的极限形式.

在本文中,我们从接受环境角度描述了软件实现与规范之间的逐渐接近关系,然而,软件与环境在多大程度上能够接受环境或多大程度上能够拒绝环境直接影响到软件在环境下的运行. 在接下来的工作中,我们将采用一些方法建立软件与环境之间交互程度的度量模型,以便更好地考察软件的性质.

参 考 文 献

[1] Liu Ke, Shan Zhiguang, Wang Ji, et al. Overview on major research plan of trustworthy software [J]. Science Foundation in China, 2008(3): 145-151 (in Chinese)
(刘克, 单志广, 王戟, 等. 可信软件基础研究重大研究计划综述[J]. 中国科学基金, 2008(3): 145-151)

[2] Milner R. A Calculus of Communicating Systems [M]. Berlin: Springer, 1982

[3] Milner R. A complete inference system for a class of regular behaviors [J]. Journal of Computer and System Sciences, 1984, 28(3): 439-466

[4] Hennessy M, Milner R. Algebraic laws for nondeterminism and concurrency [J]. Journal of the ACM, 1985, 32(1): 137-161

[5] Milner R. Communicating and Mobile Systems: The π-Calculus [M]. Cambridge: Cambridge University Press, 1999

[6] Hoare C A R. Communicating Sequential Processes [M]. New York: Prentice Hall, 1985

[7] Brookes S D, Hoare C A R, Roscoe A W. A theory of communicating sequential processes [J]. Journal of the ACM, 1984, 31(3): 560-599

[8] Berstra J A, Klop J W. Algebra of communicating processes with abstraction [J]. Theoretical Computer Science, 1985, 37: 77-121

[9] Reusug W. Petri Nets: An Introduction [M]. New York: Springer, 1985

[10] Giacalone A, Jou C C, Smolka S A. Algebraic reasoning for probabilistic concurrent systems [C] //Proc IFIP TC2 Working Conf on Programming Concepts and Methods. Amsterdam: Elsevier, 1990: 443-458

[11] Song L, Deng Y X, Cai X J. Towards automatic measurement of probabilistic processes [C] //Proc of the 7th Int Conf on Quality Software. Los Alamitos, CA: IEEE Computer Society, 2007: 50-59

[12] Deng Y X, Chothia T, Palamidessi C, et al. Metrics for action-labeled quantitative transition systems [C] //Proc of the 3rd Workshop on Quantitative Aspects of Programming Languages. Amsterdam: Elsevier, 2005: 79-96

[13] De Medeiros A K A, Van der Aalst W M P, Weijters A J M M. Quantifying process equivalence based on observed behavior [J]. Data & Knowledge Engineering, 2008, 64(1): 55-74

[14] Ying M S. Bisimulation indexes and their applications [J]. Theoretical Computer Science, 2002, 275(1/2): 1-68

[15] Zhang J J, Zhu Z H. A modal characterization of λ-bisimilarity [J]. International Journal of Software Informatics, 2007, 1(1): 85-99

[16] Ma Y F, Chen Y X, Zhang M, et al. Two-thirds simulation indexes and modal logic characterization [J]. Frontier of Computer Science in China, 2011, 5(4): 454-471

[17] Ying M S. Topology in Process Calculus: Approximate Correctness and Infinite Evolution of Concurrency Programs [M]. Berlin: Springer, 2001

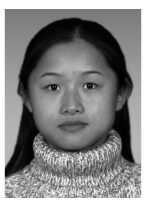
[18] He J F, Hoare T. Equating bisimulation with refinement [R]. Tokyo: United Nations University Centre, 2003

[19] Ma Yanfang, Zhang Min, Chen Yixiang. The formal description of software correctness based on the environment [J]. Journal of Shandong University: Natural Science, 2011, 46(9): 22-27 (in Chinese)
(马艳芳, 张敏, 陈仪香. 基于环境的软件正确性形式化描述[J]. 山东大学学报: 理学版, 2011, 46(9): 22-27)

[20] Larsen K G. Context-dependent bisimulation between pocess [D]. Edinburgh: Aalborg University Centre Strandvejen, 1986

[21] Chen Yixiang. The Stable Domains Theory of Formal Semantics [M]. Beijing: Science Press, 2003 (in Chinese)
(陈仪香. 形式语义学的稳定论域理论[M]. 北京: 科学出版社, 2003)

[22] Engelking R. General Topology [M]. Warszawa: Polish Scientific, 1977



Ma Yanfang, born in 1978. Received her PhD degree in the East China Normal University in 2010. Her main research interests include formalization of software, semantics of program and trustworthiness measure.

Zhang Min, born in 1976. Received her PhD degree in the Shanghai Jiaotong University and Université Paris Diderot-Paris Ⅶ in 2007. Her main research interests include formalization methods and trustworthiness computation.

Chen Yixiang, born in 1961. Professor and PhD supervisor of the East China Normal University. Senior member of China Computer Federation. His main research interests include formalization methods, internet of things and cloud computing.