关于并发系统分支互模拟关系发散性保持的研究①

廖文琪 [1,2]，柳欣欣 [1]

[1](中国科学院 软件研究所计算机科学国家重点实验室，北京 100190)
[2](中国科学院大学，北京 100190)

摘 要：带发散性说明的分支互模拟是 van Glabbeek 和 Weijland 提出的一个概念，并被用来定义等价关系 $\approx_b^\Delta$. 该等价关系应该是最弱的一个发散性保持的并且满足分支互模拟性质的等价关系. 然而在概念提出时并没有提供这些重要性质的证明，并且我们认为在原定义的基础上这个证明是不显然的. 本文通过 co-induction 的手段利用染色迹的概念定义了着色完全迹等价，并证明该等价关系是最弱的一个保持发散的并且满足分支互模拟性质的等价关系. 然后我们证明了着色完全迹等价关系和 $\approx_b^\Delta$ 是相同的，因而补充了 van Glabbeek 和 Weijland 的工作，即证明了 $\approx_b^\Delta$ 是最弱的一个保持发散的并且是满足分支互模拟性质的等价关系.

关键词：分支互模拟等价关系；发散性；发散性保持；co-induction 定义；染色迹

Branching Bisimulation with Explicit Divergence in Concurrent Systems

LIAO Wen-Qi[1,2], LIU Xin-Xin[1]

[1](State Key Laboratory of Computer Science Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)
[2](University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract: The notion of branching bisimulation with explicit divergence was introduced by van Glabbeek and Weijland. It is used to define an equivalence relation $\approx_b^\Delta$, which means to be the weakest equivalence with the property of branching bisimulation and divergence preservation. However, in that paper it only claims that $\approx_b^\Delta$ is an equivalence with such properties without proofs, and as it turns out that the proving is not obvious. In this paper we introduce an equivalence relation called coloured complete trace equivalence, and prove that it is the weakest equivalence which has the property of branching bisimulation equivalence and is also divergence preserving. We then prove that the coloured complete trace equivalence coincides with $\approx_b^\Delta$, thus supplementing the work of van Glabbeek and Weijland.

Key words: branching bisimulation; divergence; divergence preserving; co-induction; colour trace

软件系统对社会的各个方面起着重要的作用. 很多软件有着非常复杂的结构. 因而软件的生产需要理论上的支持以构建可靠的软件系统[1]. 通过建立给定程序以及程序的计算环境所组成的软件系统抽象模型和程序的性质规约之间的某种等价关系比如互模拟是验证程序正确性的有效方法[2,3].

并发理论的基本问题是两个并发系统在什么时候可以看作是相等. 在提出通信系统演算(CCS)[4]的时候，Robin Milner 就提出了所谓的观察等价，之后 Park 在对标号迁移系统的研究中采用 co-induction 的方式定义了互模拟等价关系[5]，Park 不但给出了互模拟关系的严格定义，而且为证明互模拟等价关系提供了重要的方法.

在并发系统中，发散性是一个重要的性质，它通常涉及的是一个进程有无穷多个内部动作，不能同外界环境交互. 对于一个等价关系≡，如果 P 和 Q 具有 $P \equiv Q$ 时，P 是发散的当且仅当 Q 也是发散的，则称≡是发散性保持的[6]. 发散性是对进程内部性质的约束，涉及到程序的终止性和进程的前进属性，因此利用等价关系验证程序正确性时，等价关系的发散性保持是

① 基金项目:国家自然科学基金(NSFC-91418204)
收稿时间:2016-03-21;收到修改稿时间:2016-04-05 [doi: 10.15888/j.cnki.csa.005431]

非常重要的性质.

互模拟等价关系是一种观察理论, 侧重于系统与外部环境的交互, 着重研究的是可见的外部性质, 而对内部动作进行抽象处理. 经过内部动作抽象出来的互模拟等价关系常常不保持发散性, 需要添加额外的约束. 分支互模拟(branching bisimulation)[7]是由 van Glabbeek 和 Weijlang 提出的一种进程等价关系. 研究发现分支互模拟关系不是发散性保持的. 因此 van Glabbeek 和 Weijland 对分支互模拟作了额外约束, 提出了带发散性说明的分支互模拟关系(branching bisimulation with explicit divergence)[7]. 然而, 利用该概念在证明相关性质时不够直接, 等价关系传递性上的证明太过复杂[8]. 主要原因是:

① 该概念不能用单个单调函数的不动点来表示;

② 需要对无限运行序列的相关状态的发散性进行分类讨论, 然后归纳证明.

为了解决上述问题, 我们首先使用 co-induction 思想同时借用染色迹概念定义了着色完全迹等价关系(coloured complete trace equivalence), 该等价关系能通过一个单调函数的不动点刻画, 之后利用刻画函数的最大不动点理论在概念的定义上证明其等价关系和发散性保持性质, 最后我们说明着色完成迹等价和带发散性说明的分支互模拟关系是相同的. 从新概念出发, 利用不动点理论大大降低了证明的复杂程度.

1 基本概念和符号说明

文章中主要涉及到如下几个概念: 标号迁移系统(labeled transition systems), 着色(colouring), 带发散性说明的分支互模拟关系(branching bisimulation with explicit divergence). 本文中在证明中对分支互模拟概念没有细节上的涉及而是通过不同进程和系统状态有同一颜色来体现其等价关系, 因此在这里就不给出定义, 后文中作者提出的定义也在后续的证明中给出. 我们所有的研究都是在标号迁移系统上进行的, 首先给出标号迁移系统[1]的定义和一些符号说明.

定义 1. 标号迁移系统(labeled transition systems): 一个标号迁移系统是一个三元组 M=<S, A, →>, 其中

① S 为状态集合;

② A 为标号集合;

③ $\rightarrow \subseteq S \times (A \cup \tau) \times S$ 是一个有标号的迁移关系. 其中 τ 是内部动作, 通常假设其不在集合 A 中, → 中的一个元素 (s, α, t) 表示一次迁移, 记为 $s \xrightarrow{\alpha} t$;

④ M 的一个有限运行系列是指由状态和动作交替组成的非空有限迁移系列, 记为 $\rho = s_0\alpha_0 s_1\alpha_1 \Lambda\ s_{n-1}\alpha_{n-1}s_n$, 其中 first(ρ)= s_0, last(ρ)= s_n, length(ρ) =n;

⑤ M 的一个无限运行系列是指由状态和动作交替组成的非空无限迁移系列, 记为 $\rho = s_0\alpha_0 s_1\alpha_1 \Lambda$ 其中 first(ρ)= s_0.

一般情况下, 我们可以通过连接已有的运行系列, 状态和动作形成新的运行系列.

存在多步 τ 迁移时, 可以通过一些标准符号进行简略表示: $s \Rightarrow s'$ 表示存在一个以 s, s' 分别作为起始状态和结束状态的有穷运行系列, 其中所有的动作均为 τ.

结束了对标号迁移系统的定义和相关符号的说明之后, 接下来给出 van Glabbeek 在刻画发散性保持性质中使用到的染色迹概念[8], 从定义着色(Colouring)开始.

定义 2. 着色(Colouring): M=<S, A, →>是一个标号迁移系统(LTS), M 的着色是一个在状态集合 S 上的等价关系; 给定一个着色 C 和一个状态 $s \in S$, s 的一个颜色 $C(s)$ 是一个包含 s 的等价类. 其中

① 一个 C -coloured 运行是指由颜色和动作交替组成的一个非空有限系列, 以一种颜色起始, 终止于一种颜色;

② 一个着色 C 导出一个从 M 的有限运行系列集合到 C -coloured 运行系列集合的映射, 记为 $\hat{C}$, 在运行系列长度上的归纳定义如下:

$\hat{C}(\sigma) = C(s)$, 当 $\sigma = s$;

$\hat{C}(s\alpha\sigma) = C(s)\alpha\hat{C}(\sigma)$, 当 $\alpha \neq \tau$;

$\hat{C}(s\tau\sigma) = C(s)\tau\hat{C}(\sigma)$, 当 $C(s) \neq C(first(\sigma))$;

$\hat{C}(s\tau\sigma) = \hat{C}(\sigma)$, 当 $C(s) = C(first(\sigma))$.

记 $\hat{C}(\sigma)$ 为有限运行系列 σ 的 C -coloured 运行系列;

③ ρ 是标号迁移系统 M 的一个无限运行系列, $\tilde{C}(\rho)$ 为 ρ 的所有有限运行前缀的 C -coloured 运行系列组成的集合, 记为 $\tilde{C}(\rho)$={ $\hat{C}(\rho')$| ρ' 为 ρ 的一个有限运行前缀};

④ 对 $s \in S$, 称 s 关于着色 C 发散, 若存在一个以 s 为起始状态的无限运行系列 ρ 且 $\tilde{C}(\rho)$={ $C(s)$}, 记

为 $s \Uparrow_C$; 我们称 ρ 是一个发散运行系列, 当 ρ 中所有的动作均为 τ 且 ρ 所有的状态均为颜色 $C(s)$ 时.

引理 1. M=<S, A, →>是一个标号迁移系统(LTS), C 为 M 的一个着色, ρ 是一个有穷运行.

① 对 $s \in S$, 若 $\hat{C}(\rho)=C(s)$, 则 ρ 中的所有动作均为 τ 且 ρ 所有状态的颜色为 $C(s)$;

② 对 $t, t' \in S$, 若 $\hat{C}(\rho)=C(t)\alpha C(t')$, 则存在 $\rho = s_0\tau \Lambda\ \tau s_{k-1}\alpha s_k \Lambda\ \tau s_n$ 且 i=0,...,k-1 时有 $C(s_i)=C(t)$, i=k,...,n 时有 $C(s_i)=C(t')$.

证明: 使用归纳法证明, 在 ρ 长度上进行归纳证明可完成①的证明. 在证明①为真的基础上, ρ 长度上进行归纳证明可得到②.

在完成对基本概念的准备和记号的说明后, 我们给出 van Glabbeek 提出的带发散性说明的分支互模拟关系[7].

定义 3. 带发散性说明的分支互模拟关系(branching bisimultiaon with explicit divergence): M=<S, A, →>是一个标号迁移系统(LTS), C 为 M 的一个着色.

① 着色 C 是一致的(consistent), 如果对任意 $C(s)=C(t)$, 其中 $s, t \in S$, 若存在一个以 s 为起始的有穷运行系列 σ, 则必然存在一个以 t 为起始的有穷运行 ρ 且有 $\hat{C}(\sigma)=\hat{C}(\rho)$;

② 着色 C 是发散性保持的(divergence preserving), 如果对任意 $C(s)=C(t)$, 其中 $s, t \in S$, 若 $s \Uparrow_C$, 则 $t \Uparrow_C$.

对 $s, t \in S$, 如果存在一个一致的且是发散性保持的着色 C, 使得 $C(s)=C(t)$, 则称 s 和 t 是带发散性说明的分支互模拟等价关系, 记为 $s \approx_b^{\Delta} t$.

我们希望定义 4 给出的关系是一个等价关系, 并且具有分支互模拟性质, 并且是保持发散性, 并且是具备所有以上性质的最弱的那个等价关系. 但在概念提出时[7]并没有提供这些事实的证明, 后续的研究[8]也只有部分证明(证明了它是一种等价关系). 在下面章节中, 我们将定义一个等价关系, 并且证明这个等价关系具有上述性质, 最后证明这个等价关系和定义 4 给出的是相同的.

2 概念的提出及性质证明

2.1 染色迹完全等价

本节我们将定义一个新的等价关系, 该等价关系利用染色迹(colour trace)概念使用 co-induction 的方式完成对一致性和发散性保持的刻画, 定义着色完全迹等价关系, 并证明这个关系是最弱的同时发散性保持和分支互模拟性质的等价关系.

定义 4. 着色完全迹等价关系(coloured complete trace equivalence): M=<S ,A, →>是一个标号迁移系统(LTS), C 为 M 的一个着色. C 是完全迹一致的(complete trace consistent), 如果对任意 $C(s)=C(t)$, 其中 $s, t \in S$, 蕴含着

① 若存在一个以 s 为起始的有穷运行系列 σ, 则必然存在一个以 t 为起始的有穷运行 ρ 且有 $\hat{C}(\sigma)=\hat{C}(\rho)$;

② 若存在一个以 s 为起始的无穷运行系列 σ, 则必然存在一个以 t 为起始的无穷运行 ρ 且有 $\tilde{C}(\sigma)=\tilde{C}(\rho)$.

对 $s, t \in S$, 如存在一个完全迹一致的着色 C, 使得 $C(s)=C(t)$, 则称 s 和 t 是着色完全迹等价关系, 记为 $s \approx_{cc} t$.

2.2 $\approx_{cc}$ 的性质说明

为帮助完成对 $\approx_{cc}$ 性质的研究, 引入函数ℵ, 其定义如下:

定义 5. M=<S, A, →>是一个标号迁移系统(LTS), C 为 M 的一个着色. 函数ℵ(C)是定义在状态集合 S 上的二元关系, 对 $s, t \in S$, $(s,t) \in \aleph(C)$ 当且仅当满足下列两个性质:

① { $\hat{C}(\sigma)$ | σ 是以 s 为起始的有限运行系列}={ $\hat{C}(\rho)$ | ρ 是以 t 为起始的有限运行系列};

② { $\tilde{C}(\sigma)$ | σ 是以 s 为起始的无限运行系列}={ $\tilde{C}(\rho)$ | ρ 是以 t 为起始的无限运行系列}.

引理 2.

① $\aleph(C)$ 是一个在状态集合 S 上等价关系.

② C 是完全迹一致的当且仅当{ (s,t) | $s, t \in S$, $C(s)=C(t)$ } $\subseteq \aleph(C)$ 成立

③ 函数ℵ是一个关于 M 的着色集合的单调函数

证明: 引理中①和②的证明可以在定义 4 和定义 5 中直接推导获得. ③的证明可以转化为证明: 存在在状态集合 S 上的两个等价关系 $\equiv_1$, $\equiv_2$ 且有 $\equiv_1 \subseteq \equiv_2$, 则有 $\aleph(\equiv_1) \subseteq \aleph(\equiv_2)$. 该单调性的证明从函数ℵ定义出发不难获得.

上述引理给出了函数ℵ的性质, ℵ是着色完全迹等价关系 $\approx_{cc}$ 的一个刻画, 完成对函数ℵ性质说明后, 接下来对 $\approx_{cc}$ 的性质进行阐述.

定理 1. M=<S, A, →>是一个标号迁移系统(LTS), 则$\approx_{cc}$是在状态集合 S 上的等价关系, 同时$\approx_{cc}$是一个完全迹一致的着色并且是M中完全迹一致着色刻画的等价关系中最粗粒度的那个.

证明: 令$\{\equiv_i\}_{i\in I}$为在状态集合 S 上的等价关系的集合, 根据集合知识我们可以得到下面几个事实:

① $\cap\{\equiv_i \mid i\in I\}$是在集合$S$上的等价关系;

② 对所有$i\in I$, $\cap\{\equiv_i \mid i\in I\}\subseteq\equiv_i$均成立;

③ 如果$\equiv$是状态集合 S 上的等价关系且对所有$i\in I$, 均有$\equiv\subseteq\equiv_i$, 则$\equiv\subseteq\cap\{\equiv_i \mid i\in I\}$;

④ $(\cup\{\equiv_i \mid i\in I\})^*$是$\cup\{\equiv_i \mid i\in I\}$的传递闭包, 同时也是一个在集合 S 上的等价关系;

⑤ $\equiv_i\subseteq(\cup\{\equiv_i \mid i\in I\})^*$对所有$i\in I$成立;

⑥ 如果$\equiv$是在状态集合S上的等价关系并且对所有$i\in I$均有$\equiv_i\subseteq\equiv$, 则有$(\cup\{\equiv_i \mid i\in I\})^*\subseteq\equiv$.

令ε为状态集合 S 上的等价关系的集合, 则由上述事实可知ε的任意子集在关系$\subseteq$中既有最大下确界也有最小上确界, 因此$(\varepsilon,\subseteq)$是一个完全格. 又由引理 2 可知函数$\aleph$是在该完全格中的单调函数, 则根据 Knaster-Tarski 不动点理论[9]可知函数$\aleph$有最大不动点$FIX(\aleph)\in\varepsilon$, 该不动点有如下性质:

① $FIX(\aleph)=\aleph(FIX(\aleph))$;

② 对任意$\equiv\in\varepsilon$, 当$\equiv\subseteq\aleph(\equiv)$时, 有$\equiv\subseteq FIX(\aleph)$.

由引理 2 可知, $\equiv$是完全迹一致的当且仅当$\equiv\subseteq\aleph(\equiv)$. 根据上述不动点性质可知$FIX(\aleph)$是一个完全迹一致的着色, 并且是标号迁移系统 M 中所有完全迹一致的着色刻画的等价关系中最弱的那个. 因此欲证定理 1 成立, 只需要证明$\approx_{cc}=FIX(\aleph)$. 对任意$(s,t)\in FIX(\aleph)$, 因为$FIX(\aleph)$是完全迹一致的, 所以有$s\approx_{cc}t$, 从而$FIX(\aleph)\subseteq\approx_{cc}$; $s\approx_{cc}t$, 则存在完全迹一致的等价关系$\equiv$, 使得$s\equiv t$, 根据引理 2 可得$\equiv\subseteq\aleph(\equiv)$, 因此有$\equiv\subseteq FIX(\aleph)$, 故$(s,t)\in FIX(\aleph)$, 从而$\approx_{cc}\subseteq FIX(\aleph)$. 即有$\approx_{cc}=FIX(\aleph)$得证.

综上所得定理 1 得证.

定理1的证明应用到了Knaster-Tarski不动点理论, 证明了$\approx_{cc}$是一个单调函数$\aleph$刻画的最大不动点. 这使得定理 1 的证明清晰而且规整. 相比较而言, $\approx_b^\Delta$因为不能由单个单调函数的最大不动点进行刻画获得, 使得等价关系的证明不明显, 性质的说明也不充分. 接下来通过一个例子来对刻画$\approx_b^\Delta$的函数的单调性加以说明.

同样, 我们需引入一个在ε上的函数$\wp$, 定义如下:

$\equiv$是状态集合 S 上的一个二元等价关系, $(s,t)\in\wp(\equiv)$当且仅当对$(s,t)\in S\times S$, 满足下面两个条件:

① $\{\hat{C}(\sigma)\mid\sigma$是以 s 为起始的有限运行系列$\}=\{\hat{C}(\rho)\mid\rho$是以$t$为起始的有限运行系列$\}$;

② $s\Uparrow_C$当且仅当$t\Uparrow_C$.

文献[8]对$\approx_b^\Delta$的性质进行了说明, 并证明了其为一个等价性关系, 且具有发散性保持的性质, 这些结论不是通过对函数$\wp$应用 Knaster-Tarski 定理得到的, 因为函数$\wp$不具有单调性, 下面我们给出一个反例(如图 1 所示).

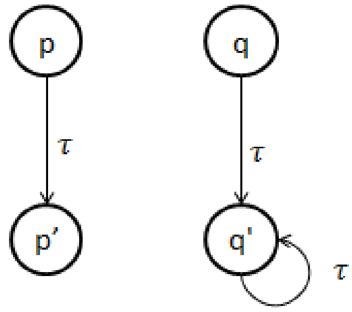

图 1　函数$\wp$单调性反例

$\equiv_1$和$\equiv_2$是定义在状态集合 S 上的等价关系且有$\equiv_1\subseteq\equiv_2$, 其中有$p\equiv_1 q$, $p'\equiv_1 q'$, 且p和p', q和q'不具有关系$\equiv_1$; p,q,p',q'之间均有关系$\equiv_2$; 根据定义可知p和q在$\equiv_1$中均不发散, 有$(p,q)\in\wp(\equiv_1)$; 但 p 在$\equiv_2$中不发散, q 在$\equiv_2$中发散, 有$(p,q)\notin\wp(\equiv_2)$, 故$\wp$不具有单调性.

定理 2. 如果二元等价关系$\equiv$是完全迹一致的着色, 则$\equiv$是发散性保持的.

证明: $\equiv$是一个完全迹一致的着色, 则可假设$s\equiv t$且有$s\Uparrow_C$; 根据发散的定义, 则存在一个以 s 为起始的无限运行系列σ且$\tilde{C}_\equiv(\sigma)=\{C_\equiv(s)\}$; 又$\equiv$是一个完全迹一致的着色, 故存在一个以 t 为起始的无限运行系列 ρ 且$\tilde{C}_\equiv(\rho)=\tilde{C}_\equiv(\sigma)=\{C_\equiv(s)\}$, 又因为 $s\equiv t$, 所以$C_\equiv(s)=C_\equiv(t)$, 进而得到$\tilde{C}_\equiv(\rho)=C_\equiv(s)$, 即$t\Uparrow_C$; 所以$\equiv$是发散性保持的.

推论 1. $\approx_{cc}$是发散性保持的.

证明: 由定理 1 可知$\approx_{cc}$是一个完全迹一致的着色, 结合定理 2 可知$\approx_{cc}$是发散性保持的.

至此, 我们对 $\approx_{cc}$ 的性质进行了全面的说明, 证明了 $\approx_{cc}$ 是一个等价关系, 当着色时使用的是分支互模拟关系时, $\approx_{cc}$ 是分支互模拟等价关系, 具有发散性保持的特性, 同时也是具备所有以上性质的最弱的那个等价关系.

2.3 $\approx_{cc}$ 和 $\approx_b^\Delta$ 关系

由上节对 $\approx_{cc}$ 性质的描述我们知道, $\approx_{cc}$ 是最粗粒度的具有发散性保持的分支互模拟等价关系. $\approx_b^\Delta$ 同样是最弱的带发散性保持的分支互模拟等价关系[7-8]. 那么 $\approx_b^\Delta$ 和 $\approx_{cc}$ 之间的有什么关系, 本节将对其进行完整的阐述.

定理 3. M=<S, A, $\rightarrow$>是一个标号迁移系统(LTS), $\equiv$ 是在状态集合 S 上的二元等价关系, 则 $\equiv\subseteq\aleph(\equiv)$ 当且仅当 $\equiv$ 是一致的且是发散性保持的.

证明:

① $\Rightarrow$: 当 $\equiv\subseteq\aleph(\equiv)$ 时, $\equiv$ 是一致的且是发散性保持的. $\equiv\subseteq\aleph(\equiv)$, 由引理 2 可知 $\equiv$ 是完全迹一致的, 根据定义 3 中的第一个条件可知 $\equiv$ 是一致的, 同时运用定理 2 可知 $\equiv$ 是发散性保持的, $\Rightarrow$ 方向得证.

② $\Leftarrow$: 当 $\equiv$ 是一致的且是发散性保持的时, 有 $\equiv\subseteq\aleph(\equiv)$. $\equiv$ 是一致的, 根据一致性的定义(定义 3), 结合定义 4 可得在有限运行系列中 $\equiv$ 是完全迹一致, 故可根据引理 2 得 $\equiv\subseteq\aleph(\equiv)$. 在无限运行系列中, $\equiv$ 是发散性保持的. 假设 $(s,t)\in S\times S$ 且有 $s\equiv t$, 一个以 s 为起始的无穷运行系列 $\sigma = s_0\alpha_1 s_1 \Lambda\ s_{k-1}\alpha_k s_k\ \Lambda$, 则存在一个以 t 为起始的无穷运行系列 ρ 且有 $\tilde{C}_{\equiv}(\rho)=\tilde{C}_{\equiv}(\sigma)$. 此时需要分两种情况讨论: 第一种情况是 σ 只存在一种颜色, 此时可以假设存在状态 s_m 将 σ 分隔成两段一段是 $\sigma_1 = s_0\alpha_1 s_1\ \Lambda\ s_m$ 和一段从 s_m 起始的发散系列, 因为 $\equiv$ 是一致的所以可以在 ρ 找到相应的一段有限运行系列 ρ_1, 使得 $\hat{C}_{\equiv}(\rho_1)=\hat{C}_{\equiv}(\sigma_1)$, 且有 last($\rho_1$)=$t'$, $t'\equiv s_m$, 又 $\equiv$ 是发散性保持的, 故 t' 也是发散的, 在这种情况下 ρ 是由 ρ_1 这个有限运行系列和以 t' 开始的发散系列连接而成. 第二种情况是存在 $\alpha_k\neq\tau$ 或者 $s_{k-1}\neq s_k$, 此时 σ 这一无穷运行系列的 C-coloured 运行有多个颜色, σ 被分割成多个有限系列 σ_i, 根据 $\equiv$ 的一致性可以找到相应的 ρ_i, 使得 $\hat{C}_{\equiv}(\rho_i)=\hat{C}_{\equiv}(\sigma_i)$, 最后连接所有的 ρ_i 得到所需的从 t 起始的无穷运行系列 ρ. 完成上述论述后能保证在无穷运行系列中的有穷子系列同样也是一致的, 进而证明了 $\equiv$ 是染色迹完全一致的, 有 $\equiv\subseteq\aleph(\equiv)$.

上述定理告诉我们定义 3 和定义 4 中获得的两个关系的条件是相同的, 得到的等价应该也是相同的, 即 $\approx_b^\Delta=\approx_{cc}$, 将在定理 4 中给出完善的证明. 这不禁让人疑问: 两个定义给定的条件是可以互推得到的, 关系也是相同的, 为什么刻画该关系的函数会在单调性上有不同的表现. 比较两个定义的条件发现, 两种定义都分为两个部分, 第一部分是对有限运行系列的一致性的要求, 两种定义此部分完全相同, 区别在第二部分对无限系列的发散性保持上的约束. 定义 3 只对无限系列相关状态的发散性保持做了要求, 对其有限子系列的一致性并没有说明, 而定义 4 对无穷运行系列中的相关状态的发散性和一致性都给出了明确的说明. 从这个角度上看定义4的条件比定义3更强, 这个说法没有问题, 但事实是对发散性保持的说明本身其实蕴含着从相关状态起始的无限系列的有限子系列具有一致性, 但需要进一步的说明. 定义 4 不能使用单个单调函数进行刻画获得最大不动点性质, 但使用两个函数可以完成对其该性质的阐述.

定理 4. M=<S, A, $\rightarrow$>是一个标号迁移系统(LTS). 则

① $\approx_b^\Delta=\approx_{cc}$;

② $\approx_b^\Delta$ 是在状态集合 S 上的二元等价关系, 同时 $\approx_b^\Delta$ 具有一致性和发散性保持特性, 并且 $\approx_b^\Delta$ 是标号迁移系统 M 中最弱的带发散性保持的等价关系.

证明:

① 由定理 2 可知 $\approx_{cc}$ 是发散性保持的, 并且是一致的, 根据定义 3, 有 $\approx_{cc}\subseteq\approx_b^\Delta$; 任意 $s,t\in S$, 如果 $s\approx_b^\Delta t$, 则存在一个等价关系 $\equiv$, $\equiv$ 是一致的并且是发散性保持的且有 $s\equiv t$, 由定理 3 可知 $\equiv\subseteq\aleph(\equiv)$, 运用引理 2 可知 $\equiv$ 是完全迹一致的, 故 $s\approx_{cc} t$, 即 $\approx_b^\Delta\subseteq\approx_{cc}$; 综上 $\approx_b^\Delta=\approx_{cc}$.

② 由定理 1 可知 $\approx_{cc}$ 是在状态集合 S 上的等价关系, 由于 $\approx_b^\Delta=\approx_{cc}$, 所以 $\approx_b^\Delta$ 也是在状态集合 S 上的等价关系, 同时在定理 8 中我们对 $\approx_{cc}$ 的最弱等价性进行了证明, 同样也可以迁移到 $\approx_b^\Delta$ 上.

3 结语

分支互模拟关系发散性保持的研究对并发系统理论发展和并发程序的验证具有重要的意义. 尽管 van Glabbeek 等提出了带发散性说明的分支互模拟概念并对其性质进行了一定的说明, 但我们提出了着色完全

迹等价关系对分支互模拟关系的发散性保持问题进行了研究, 从另一个角度证明了带发散性说明的分支互模拟概念的性质, 完善了其工作. 本文的研究有以下贡献和创新性:

① 使用 co-induction 方式定义了着色完全迹等价关系, 并证明了其为最弱的发散性保持的分支互模拟等价关系.

② 对刻画带发散性说明的分支互模拟关系的函数的单调性进行了说明.

③ 建立了着色完全迹等价关系和带发散性说明的分支互模拟等价关系之间的联系, 完善带发散性说明的分支互模拟关系的研究工作.

④ 研究了发散性保持的分支互模拟等价关系, 为应用该关系验证程序的正确性提供帮助.

参考文献

1 张文辉.软件系统行为与程序正确性.http://lcs.ios.ac.cn/~zwh/pv/pv13.pdf.

2 Liang H, Feng X, Fu M. A rely-guarantee-based simulation for verifying concurrent program transformations. ACM SIGPLAN Notices, ACM, 2012, 47(1): 455–468.

3 Liang H, Hoffmann J, Feng X, et al. Characterizing progress properties of concurrent objects via contextual refinements . CONCUR 2013–Concurrency Theory. Springer Berlin Heidelberg, 2013: 227–241.

4 Milner R. Communication and Concurrency. Prentice-Hall, Inc., 1989.

5 Park D. Concurrency and automata on infinite sequences. Gi-Conference on Theoretical Computer Science. Springer-Verlag. 1981. 167–183.

6 何超栋.CCS 的基本问题研究[博士学位论文].上海:上海交通大学,2011.

7 Van Glabbeek R, Weijland W. Branching time and abstraction in bisimulation semantics. Journal of the ACM, 1996.

8 Van Glabbeek R, Luttik B, Trcka N. Branching bisimilarity with explicit divergence. Fundamenta Informaticae, 2009, 93(4): 371–392.

9 Paulson LC. A Fixedpoint Approach to Implementing (co) Inductive Definitions. Springer Berlin Heidelberg, 1994.