软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(1):16−26 [doi: 10.13328/j.cnki.jos.004408]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于余归纳的最小 Kripke 结构的求解*

高建华[1,2], 蒋 颖[1]

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

[2](中国科学院大学,北京 100190)

通讯作者: 高建华, E-mail: gaojh@ios.ac.cn

摘 要: 状态空间爆炸问题是模型检测的最大障碍.从余归纳(特别是余代数)的角度研究了这个问题.用余归纳的方法证明:(1) 对于任意给定的一类 Kripke 结构(记为$\mathcal{K}$),在互模拟等价意义下$\mathcal{K}$中最小 Kripke 结构(记为K_0)的存在唯一性.K_0描述了$\mathcal{K}$中所有 Kripke 结构的行为而且没有冗余的状态;(2) 对于任意的$M\in\mathcal{K}$(M可能包含无穷多个状态),在互模拟等价意义下的相对于(M 且基于 K_0)的最小 Kripke 结构(记为 K_M)的存在唯一性.由此提出一种求解 K_M 的算法,并用 Ocaml 予以简单实现.其应用之一在于可以用状态空间更小的 K_M 代替 M 进行模型检测.该方法可自然地推广到基于其他类型函子的余代数结构.

关键词: 模型检测;互模拟;函子;终余代数;最小 Kripke 结构

中图法分类号: TP301 **文献标识码**: A

中文引用格式: 高建华,蒋颖.基于余归纳的最小 Kripke 结构的求解.软件学报,2014,25(1):16−26. http://www.jos.org.cn/1000-9825/4408.htm

英文引用格式: Gao JH, Jiang Y. Coinduction-Based solution for minimization of Kripke structures. Ruan Jian Xue Bao/Journal of Software, 2014,25(1):16−26 (in Chinese). http://www.jos.org.cn/1000-9825/4408.htm

Coinduction-Based Solution for Minimization of Kripke Structures

GAO Jian-Hua[1,2], JIANG Ying[1]

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

[2](University of Chinese Academy of Sciences, Beijing 100190, China)

Corresponding author: GAO Jian-Hua, E-mail: gaojh@ios.ac.cn

Abstract: State explosion problem is the main obstacle of model checking. This problem is addressed in the paper from a coalgebraic point of view. By coninduction principle, the paper proves that: (1) Given any class of Kripke Structures (denoted by $\mathcal{K}$), there exists a unique smallest Kripke structure (denoted by K_0) with respect to bisimilarity which describes all behaviors of the Kripke structures with no redundancy. (2) For any Kripke Structure $M\in\mathcal{K}$ (the state space of M may be infinite), there exists a unique concrete smallest Kripke structure K_M. Base on this idea, an algorithm is established for minimization of Kripke Structures. A naive implementation of this algorithm is developed in Ocaml. One of its applications is that instead of M, K_M can be used with a smaller state space to verify properties for M in the process of Model Checking.

Key words: model checking; bisimulation; functor; final coalgebra; minimal Kripke structure

状态空间爆炸问题是模型检测的最大障碍.本文从余归纳定义(特别是余代数)和余归纳证明的角度来研究这个问题.众所周知,余代数是代数的对偶概念,通常用其来描述无穷状态的动态的结构,进而从观察的角度来考察结构的性质.粗略地说,不同于基于构造算子(constructor operations)的代数结构及其归纳法则,余代数结构

* 基金项目: 国家自然科学基金(60833001); 中法 NSFC-ANR 共同资助合作研究项目(61161130530)
本文初始工作 Model Cheking: A Co-Algebraic Approach 已在国际会议 TASE 2011 上宣读,本文是其拓展工作.
收稿时间: 2012-11-06; 修改时间: 2013-01-25; 定稿时间: 2013-03-29

则依赖于其观察算子(observer operations),其相应的证明法则是余归纳法则.Jacobs 和 Rutten 详细描述了代数和余代数的对偶性[1].Sangiorgi 用函子、推演规则和不动点这 3 种方式描述了余归纳的定义和余归纳证明法则,并证明了 3 种定义的等价性[2].Aczel 和 Mendler 提出并证明了一个一般的终余代数定理[3]:每个基于范畴 *Set* 的函子都有一个终余代数.Rutten 和 Turi 提出了一种能行(efficient)的方法,并由此证明了基于范畴 *Set* 的标号迁移系统函子的终余代数的存在性[4].

互模拟概念是一个余归纳定义的典型实例,互模拟等价的证明是一个余归纳证明法则的典型应用,求解互模拟等价是构造最小模型的一种有效方法.对于有穷状态系统而言,求解互模拟等价的算法已很成熟[5,6].对于无穷状态系统而言,Bonchi 和 Montanari 研究了符号互模拟关系的求法[7],Burkart 等人研究了进程重写系统(process rewrite system)的互模拟关系的求解方法[8].

本文从余归纳的角度来研究模型检测中的状态空间爆炸问题.基于余归纳的方法,我们证明了:

(1) 对任给原子命题集合 AP,对于由基于 AP 的所有 Kripke 结构所构成的类$\mathcal{K}$,在互模拟等价意义下的最小 Kripke 结构 K_0 的存在唯一性.K_0 描述了$\mathcal{K}$中所有 Kripke 结构的行为且 K_0 没有冗余的状态,即:对任意的 $M\in\mathcal{K}$,都存在唯一的同态 $f:M\to K_0$,使得对 M 的任意两个状态 s 和 s'互模拟等价当且仅当 $f(s)=f(s')$;

(2) 对任意 $M\in\mathcal{K}$(M 可能包含无穷多个状态),相对于 M 的最小 Kripke 结构 K_M 的存在唯一性,即:M 和 K_M 互模拟等价且 K_M 是 K_0 中 M 的像.由此提出一种求解 K_M 的算法,并用 Ocaml 予以简单实现.

本文的工作基于终余代数的存在唯一性[3].我们所提出的求解终余代数的方法是受文献[4]的启发,与其不同之处在于:首先,文献[4]中所构造的是相对于标号迁移系统函子,即:$\mathcal{P}_f(A\times\cdot)$的终余代数,而我们所构造的是相对于 Kripke 结构函子,即:$\mathcal{P}_f(AP)\times\mathcal{P}_f(\cdot)$的终余代数;其次,文献[4]旨在研究标号迁移系统的始代数和终余代数语义(initial algebra and final coalgebra semantics),而我们的工作在于求解在互模拟等价意义下的最小模型.Joost 等人用划分等价类的方法对 Markov Chain 进行极小化[9].而用等价类的方法只是本文的一个特例,本文的方法可以应用于 Markov Chain 的极小化.值得指出的是,对于某些无穷状态的 Kripke 结构 M,其最小 Kripke 结构 K_M 的状态空间是有穷的.事实上,对于每一个 CTL^*公式φ,$M\models\varphi$当且仅当 $K_M\models\varphi$,即:M 和 K_M 满足相同的可用 CTL^*公式表达的性质[5].因此,我们可以用状态空间更小的 K_M 来代替 M 进行模型检测.该方法可自然地推广到基于其他函子的余代数结构.

本文第 1 节简单介绍本研究所需要的范畴论和模型检测的基础知识.第 2 节给出 Kripke 结构的余代数表述并证明了其相关性质.第 3 节构造 Kripke 结构函子的终余代数及由此所产生的最小 Kripke 结构 K_0.第 4 节对任意给定的 Kripke 结构 M,构造其相应的最小 Kripke 结构 K_M,给出计算 K_M 的算法并举例说明.第 5 节是总结.

1 基础知识

本节简单介绍余代数和模型检测的基础知识,其中的定义、定理出自文献[4,5],更详细的内容见文献[1,10].分别用 $A\times B=\{(a,b)|a\in A,b\in B\}$和 $A+B=\{(a,0)|a\in A\}\cup\{(b,1)|b\in B\}$表示集合 A,B 的笛卡尔积(Cartesian product)和不相交并(disjoint union).

1.1 余代数

定义 1(函子). 令 C 和 D 为两个范畴.函子 $F:C\to D$ 是一个映射,它将 C 中的每一个对象 A 映射到 D 中的对象 $F(A)$,并且将 C 中的每一个态射 $f:A\to B$ 映射到 D 中的态射 $F(f):F(A)\to F(B)$,使得对于 C 中的每一个对象 A 以及可复合的态射 f 和 g,满足:(1) $F(id_A)=id_{F(A)}$;(2) $F(f\circ g)=F(f)\circ F(g)$.

若不特别说明,以下函子均指范畴 *Set* 上的自函子,即:范畴 *Set* 到 *Set* 的函子.

定义 2(F-余代数,F-同态,终余代数). 令 F 为范畴 C 上的一个函子.对于 C 中的对象 A,如果存在映射$\alpha:A\to F(A)$,则称二元组(A,α)是一个 F-余代数.给定 F-余代数(A,α)和(B,β),如果存在映射 $h:A\to B$ 使得$\beta\circ h=F(h)\circ\alpha$,则称 h 为从(A,α)到(B,β)的 F-同态(简称同态,记为 $h:(A,\alpha)\to(B,\beta)$);若 h 为双射,则称其为 F-同构(简称同构).F-余代数

(A,α)是终结的,如果对任意 F-余代数(B,β)都存在唯一的同态 $h:(B,\beta)\to(A,\alpha)$.F-余代数(A,α)是弱终结的,如果对任意 F-余代数(B,β)都存在至少一个同态 $h:(B,\beta)\to(A,\alpha)$.

定理 1. 若函子 F 的终余代数存在,则在同构意义下是唯一的;F 的终余代数(A,α)是 F 的不动点,即:A 和 $F(A)$是等势的[1].

定义 3(互模拟). 令(A,α)和(B,β)为 F-余代数,我们称 $A\times B$ 的子集 R 为(A,α)和(B,β)的互模拟,如果存在函数 $\gamma:R\to F(R)$,使得投影函数$\pi_1:R\to A$ 是从(R,γ)到(A,α)的 F-同态,投影函数$\pi_2:R\to B$ 是从(R,γ)到(B,β)的 F-同态.特别地,当$(A,\alpha)\to(B,\beta)$时,我们称 R 为(A,α)上的互模拟.

事实上,给定函子 F,所有 F-余代数形成一个以 F-余代数为对象、以余代数之间的互模拟为态射的范畴.

定义 4(互模拟等价). F-余代数(A,α)上的互模拟等价(记为$\sim_A$)是指(A,α)上的所有互模拟的并:

$$\sim_A=\{R\subseteq A\times A\mid R \text{ 是}(A,\alpha)\text{上的互模拟}\}.$$

在不引起歧义的情况下,我们把$\sim_A$ 简写为$\sim$.

定理 2. 函子 F 的终余代数(A,α)是强外延的,即:对于所有的 $a,a'\in A$,如果 $a\sim a'$,那么 $a=a'$[4].

定义 5(核,弱保核). 函数 $f:A\to B$ 的核是指$\{(a,a')\mid f(a)=f(a')\}$(记为 K_f).令 F 为函子,如果对范畴 Set 中的每一个映射 f,都存在一个单射 $i:K_{F(f)}\to F(K_f)$,则称 F 是弱保核的.

定理 3. 令(A,α)为弱保核函子 F 的终余代数,h 为 F-余代数(B,β)到终余代数(A,α)的 F-同态,对于任意的 $b,b'\in B,b\sim b'\Leftrightarrow h(b)=h(b')$[4].

定义 6(链). 在范畴 Set 中,我们称 $\Delta=X_0\xleftarrow{f_0}X_1\xleftarrow{f_1}X_2\xleftarrow{f_2}\cdots$ 为链.

定义 7(极限). 在范畴 Set 中,链 $\Delta=X_0\xleftarrow{f_0}X_1\xleftarrow{f_1}X_2\xleftarrow{f_2}\cdots$ 的极限是指满足以下两个性质的对象 Z 以及映射类 $(Z\xrightarrow{\zeta_n}X_n)_{n\in N}$:(1) $f_n\circ\zeta_{n+1}=\zeta_n$;(2) 对每个使得 $f_n\circ g_{n+1}=g_n$ 成立的对象 Y 以及映射类 $(Y\xrightarrow{\zeta_n}X_n)_{n\in N}$,都存在唯一的映射 $h:Y\to Z$ 使得 $\zeta_n\circ h=g_n$.

定义 8(ω-连续). 令 F 为函子,若对任意链 $\Delta=X_0\xleftarrow{f_0}X_1\xleftarrow{f_1}X_2\xleftarrow{f_2}\cdots$ 及其极限 Z 和 $(Z\xrightarrow{\zeta_n}X_n)_{n\in N}$ 有 Z 和 $F(Z)$是等势的,则称 F 是 ω-连续的.

定理 4. 在范畴 Set 中,链 $\Delta=D_0\xleftarrow{f_0}D_1\xleftarrow{f_1}D_2\xleftarrow{f_2}\cdots$ 的极限是无穷笛卡尔积 $\prod_{n\in N}D_n$ 的子集:

$$Z=\{(d_0,d_1,\ldots)\mid\forall n\in N.d_n\in D_n\wedge f_n(d_{n+1})=d_n\}.$$

定理 5. ω-连续函子 F 存在终余代数$(Z,\alpha:Z\to F(Z))$,其中,Z 是链 $(F^{n+1}\xrightarrow{F^n(!)}F^n(1))_{n\in N}$ 的极限,1 为范畴 Set 的终对象,!为 $F(1)$到 1 的映射.

定义 9(自然转换). 函子 F 到函子 G 的自然转换(记为 $F\xrightarrow{\cdot}G$)是一个映射:把集合 X 映射到函数 $\pi_X:F(X)\to G(X)$,使得对每一个函数 $f:X\to Y,\pi_Y\circ F(f)=G(f)\circ\pi_X$.

定理 6. 令 $F\xrightarrow{\cdot}G$ 为函子 F 到函子 G 的自然转换.如果对每一个集合 X,π_X 都是满射,并且 F 有终余代数,那么 G 也有终余代数[4].

1.2 模型检测

定义 10(Kripke 结构). 令 AP 为原子命题集合.一个基于 AP 的 Kripke 结构是一个四元组(S,S_0,R,L),其中,S 为有穷状态集合;$S_0\subseteq S$ 为初始状态集合;$R\subseteq S\times S$ 为一个完全的迁移关系,即:对每个 $s\in S$ 存在 s'使得 $R(s,s')$;$L:S\to 2^{AP}$ 为标号函数.

以下我们用$\mathcal{K}$表示由基于 AP 的所有 Kripke 结构所构成的类.

定义 11(互模拟关系). 令 $M=(S,S_0,R,L)$和 $M'=(S',S_0',R',L')$ 为基于 AP 的 Kripke 结构.令 B 为 $S\times S$ 的子集,如果对任意的 $s\in S,s'\in S',B(s,s')$有:

(1) $L(s)=L(s')$;

(2) 对于任意的状态 s_1 使得 $R(s,s_1)$存在 $s_1'\in S'$ 使得 $R'(s',s_1')$ 并且 $B(s_1,s_1')$;

(3) 对于任意的状态 $s_1'\in S'$ 使得 $R'(s',s_1')$ 存在 $s_1\in S$ 使得 $R(s,s_1)$并且 $B(s_1,s_1')$,

则称 B 为互模拟关系.特别地,当 $M'=M$ 时,我们称 B 为 M 上的互模拟.

我们把 $\bigcup\{B\subseteq S\times S\mid B$是$M$上的互模拟关系$\}$ 记为$\approx_M$,在不引起歧义的情况下,把$\approx_M$简写为$\approx$.

定义 12(互模拟等价). 我们称 Kripke 结构 M,M'是互模拟等价的(记为 $M\equiv M'$),如果存在一个互模拟关系 B 使得:对 M 的每个初始状态 s_0,都存在一个 M'的初始状态 s_0 使得 $B(s_0,s_0')$; 对 M'的每个初始状态 s_0',都存在一个 M 的初始状态 s_0 使得 $B(s_0,s_0')$.

定理 7. $M\equiv M'$当且仅当对于任意的 CTL^*公式φ,$M\vDash\varphi\Leftrightarrow M'\vDash\varphi$[5].

2 Kripke 结构的函子及其性质

令 AP 为原子命题集合,我们将定义能够描述基于 AP 的所有 Kripke 结构的函子,并研究其性质.

2.1 Kripke结构的函子

在本节中,我们引入函子$\mathcal{P}(AP)\times\mathcal{P}(\cdot)$,其形式定义如下:

- 对任意的集合 S,$\mathcal{P}(AP)\times\mathcal{P}(S)=\{(B,V)\mid B\subseteq AP,V\subseteq S,V\neq\varnothing\}$($V\neq\varnothing$是因为 Kripke 结构的迁移关系是完全关系);
- 对任意的函数 $f:S\to T$,$\mathcal{P}(AP)\times\mathcal{P}(f):\mathcal{P}(AP)\times\mathcal{P}(S)\to\mathcal{P}(AP)\times\mathcal{P}(T)$,即:$(B,V)\mapsto(B,\{f(s)\mid s\in V\})$.

定义 13(余代数 Kripke 结构). 给定原子命题集合 AP,一个基于 AP 的余代数 Kripke 结构是一个二元组$(\mathcal{A},I)$,其中,$\mathcal{A}$为$\mathcal{P}(AP)\times\mathcal{P}(\cdot)$-余代数$(A,\alpha)$,$I\subseteq A$.

以下我们用$\mathcal{C}$表示由所有基于 AP 的余代数 Kripke 结构所构成的类.

命题 1. $\mathcal{K}$和$\mathcal{C}$是等势的.

证明:我们只需证明存在两个函数 $f:\mathcal{K}\to\mathcal{C}$,$g:\mathcal{C}\to\mathcal{K}$使得 $f\circ g=id_{\mathcal{C}}$ 且 $g\circ f=id_{\mathcal{K}}$.事实上,我们定义:

- $f((S,S_0,R,L))=((S,\gamma),S_0)$,其中,$\gamma(s)=(L(s),\{s'\mid(s,s')\in R\})$;
- $g(((S,\gamma),S_0))=(S,S_0,R,L)$,其中,$L(s)=\pi_1(\gamma(s))$且 $R=\{(s_1,s_2)\mid s_2\in\pi_2(\gamma(s_1))\}$. □

根据函数 f 和 g 定义,我们可以证明 $f\circ g=id_{\mathcal{C}}$ 以及 $g\circ f=id_{\mathcal{K}}$.

以下我们用$(\mathcal{A}_M,I_M)$表示与 Kripke 结构 M 对应的余代数 Kripke 结构.

函子$\mathcal{P}(AP)\times\mathcal{P}(\cdot)$可表示所有基于 AP 的 Kripke 结构,但该函子不存在终余代数(定理 1).为此,我们将函子$\mathcal{P}(AP)\times\mathcal{P}(\cdot)$修正为函子$\mathcal{P}_f(AP)\times\mathcal{P}_f(\cdot)$,其不同之处在于,$\mathcal{P}_f(AP)\times\mathcal{P}_f(\cdot)=\{(B,V)\in\mathcal{P}(AP)\times\mathcal{P}(S)\mid B,V$是有穷集合$\}$.为了简便起见,我们把$\mathcal{P}_f(AP)\times\mathcal{P}_f(\cdot)$记为$\mathcal{G}(\cdot)$,其描述了基于 AP 的有穷分支的所有 Kripke 结构,即:Kripke 结构的每一个状态有有穷多个直接后继.

引理 1. 函子$\mathcal{G}(\cdot)$是弱保核的.

证明:根据定义 5,我们需要证明对任意的函数 $f:A\to B$,都存在一个单射 $i:K_{\mathcal{G}(f)}\to\mathcal{G}(K_f)$.

令 $i:((S,V_1),(S,V_2))\mapsto(S,\{(v_1,v_2)\mid v_1\in V_1,v_2\in V_2,f(v_1)=f(v_2)\})$,显然,$i$ 是一个单射,所以函子$\mathcal{G}(\cdot)$是弱保核的. □

2.2 互模拟等价

我们证明:基于 AP 的 Kripke 结构之间的互模拟关系和$\mathcal{G}(\cdot)$-余代数之间的互模拟是相互吻合的.为此,我们引入余代数 Kripke 结构之间的互模拟等价.

定义 14(余代数 Kripke 结构的互模拟等价). 我们称余代数 Kripke 结构$(\mathcal{A},I)$和$(\mathcal{A}',I')$是互模拟等价的(记为$(\mathcal{A},I)\doteq(\mathcal{A}',I')$)如果存在$\mathcal{A}$和$\mathcal{A}'$的互模拟 B,使得:(1) 对每个 $s\in I$ 存在 $s'\in I'$使得 $B(s,s')$;(2) 对每个 $s'\in I'$存在 $s\in I$ 使得 $B(s,s')$.

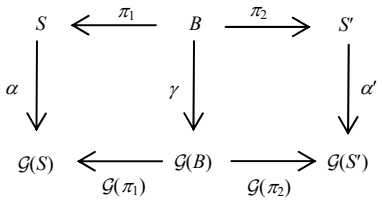
命题 2. 令 $M,M'\in\mathcal{K}$,则 $M\equiv M'\Leftrightarrow(\mathcal{A}_M,I_M)\doteq(\mathcal{A}_{M'},I_{M'})$.

证明:假设 $M=(S,S_0,R,L)$, $M'=(S',S_0',R',L')$.根据命题 1 的证明,存在α,α'使得$\mathcal{A}_M=(S,\alpha)$,$\mathcal{A}_{M'}=(S',\alpha')$.

我们只需证明:对任意的 $B\subseteq S\times S'$,B 是 M 和 M'的互模拟关系当且仅当 B 是$\mathcal{A}_M$和$\mathcal{A}_{M'}$的互模拟.

充分性:

令$\gamma:B\to\mathcal{G}(\cdot)$,使得$\gamma(s_1,s_2)=(L(s_1),\{(s_1',s_2')\in B\mid(s_1,s_1')\in R,(s_2,s_2')\in R'\})$.证明下图中左子图是可交换的:



对任意$(s_1,s_2)\in B$,我们有:

$$\begin{aligned}\alpha\circ\pi_1(s_1,s_2)&=\alpha(s_1)(\pi_1\text{的定义})\\&=(L_1(s_1),\{s_1'\mid(s_1,s_1')\in R\})(\text{命题1的证明})\\&=(L_1(s_1),\{s_1'\mid\exists s_2'.(s_1',s_2')\in B,(s_1,s_1')\in R,(s_2,s_1')\in R'\})(B\text{是互模拟关系})\\&=\mathcal{G}(\pi_1)(L_1(s_1),\{(s_1',s_2')\mid(s_1,s_1')\in R,(s_2,s_1')\in R'\})\\&=\mathcal{G}(\pi_1)\circ\gamma(s_1,s_2),\end{aligned}$$

故$\alpha\circ\pi_1=\mathcal{G}(\pi_1)\circ\gamma$,即:左子图是可交换的.同理可证右子图是可交换的.

必要性:

对任意的$(s_1,s_2)\in B$:

1. $L(s_1)=L'(s_2)$:

$$\begin{aligned}L(s_1)&=\pi_1(\alpha(s_1))(\text{命题1的证明})\\&=\pi_1(\alpha\circ\pi_1(s_1,s_2))(\pi_1\text{的定义})\\&=\pi_1(\mathcal{G}(\pi_1)\circ\gamma(s_1,s_2))(\text{左子图的可交换性})\\&=\pi_1(\mathcal{G}(\pi_2)\circ\gamma(s_1,s_2))(\mathcal{G}(\cdot)\text{的定义})\\&=\pi_1(\beta\circ\pi_2(s_1,s_2))(\text{右子图的可交换性})\\&=\pi_1(\beta(s_2))(\pi_2\text{的定义})\\&=L'(s_2)(\text{命题1的证明});\end{aligned}$$

2. 对于任意的$s_1'\in S$使得$R(s_1,s_1')$,存在$s_2'\in S'$使得$R'(s_2,s_2')$且$B(s_1',s_2')$:

$$\begin{aligned}R(s_1)&=\pi_2(\alpha(s_1))(\text{命题1的证明})\\&=\pi_2(\alpha\circ\pi_1(s_1,s_2))(\pi_2\text{的定义})\\&=\pi_2(\mathcal{G}(\pi_1)\circ\gamma(s_1,s_2))(\text{左子图的可交换性})\\&=\{s_1'\mid\exists s_2'.(s_1',s_2')\in\pi_2(\gamma(s_1,s_2))\}(\mathcal{G}(\cdot)\text{的定义})\\&=\{s_1'\mid\exists s_2'.(s_1',s_2')\in\pi_2(\beta\circ\pi_2(s_1,s_2)),(s_1',s_2')\in B\}(\text{右子图的可交换性})\\&=\{s_1'\mid\exists s_2'.s_2'\in\pi_2(\beta(s_2)),(s_1',s_2')\in B\}(\pi_2\text{的定义})\\&=\{s_1'\mid\exists s_2'.s_2'\in R'(s_2),(s_1',s_2')\in B\}(\text{命题1的证明});\end{aligned}$$

3. 对于任意的$s_2'\in S'$使得$R'(s_2,s_2')$,存在$s_1'\in S$使得$R(s_1,s_1')$且$B(s_1',s_2')$:证明同上. □

3 K_0的求解

本节首先证明函子$\mathcal{G}(\cdot)$的终余代数的存在唯一性,在此基础上,我们构造类$\mathcal{K}$的最小 Kripke 结构K_0.

3.1 函子$\mathcal{G}(\cdot)$的终余代数的存在唯一性

根据定理 1,我们只需证明函子$\mathcal{G}(\cdot)$的终余代数的存在性.根据定理 6,我们需要构造一个具有终余代数的函子$\mathcal{F}$和一个自然转换$\pi:\mathcal{F}\stackrel{\cdot}{\longrightarrow}\mathcal{G}$,使得对每一个集合$X$,$\pi_X$是一个满射.

首先,我们构造函子$\mathcal{F}$,其形式定义如下:

- 对任意的集合X,$\mathcal{F}(X)=\sum_{1\leqslant n\leqslant\omega}X^n+(AP\times X)^n$;

- 对任意的函数 $f:X\to Y$,$\mathcal{F}(f):\mathcal{F}(X)\to\mathcal{F}(Y)$:

$$\mathcal{F}(f)(Z)=\begin{cases}(f(x_1),f(x_2),...,f(x_n)), & \text{若}Z=(x_1,x_2,...,x_n)\\((a_1,f(x_1)),(a_2,f(x_2)),...,(a_m,f(x_m)), & \text{若}Z=((a_1,x_1),(a_2,x_2),...,(a_m,x_m))\end{cases}.$$

其次,我们证明函子$\mathcal{F}$具有终余代数.为此,我们首先证明函子$\mathcal{F}$是ω-连续的.

根据定理 4,链 $\Delta=D_0\xleftarrow{f_0}D_1\xleftarrow{f_1}D_2\xleftarrow{f_2}...$ 的极限是 $Z=\{(d_0,d_1,\ldots)|\forall n\in\mathbb{N}.d_n\in D_n\wedge f_n(d_{n+1})=d_n\}$.将链$\Delta$输入$\mathcal{F}$得到链 $\mathcal{F}(\Delta)=\mathcal{F}(D_0)\xleftarrow{\mathcal{F}(f_0)}\mathcal{F}(D_1)\xleftarrow{\mathcal{F}(f_1)}\mathcal{F}(D_2)\xleftarrow{\mathcal{F}(f_2)}...$

同样地,链$\mathcal{F}(\Delta)$的极限是 $Z'=\{(d'_0,d'_1,...)\mid\forall n\in\mathbb{N}.d'_n\in\mathcal{F}(D_n)\wedge\mathcal{F}(f_n)(d'_{n+1})=d'_n\}$.根据定义 8,我们只需证明$\mathcal{F}(Z)$和 Z'是等势的,即:存在函数$\gamma:\mathcal{F}(Z)\to Z'$,$\theta:Z'\to\mathcal{F}(Z)$使得 $\theta\circ\gamma=id_{\mathcal{F}(Z)}$ 且$\gamma\circ\theta=id_{Z'}$.函数$\gamma:\mathcal{F}(Z)\to Z'$的构造如下:

$$\gamma(x)=\begin{cases}((d_0^0,d_0^1,...,d_0^n),(d_1^0,d_1^1,...,d_1^n),...), & \text{若}x=((d_0^0,d_1^0,...),...,(d_1^n,d_1^n,...))\\(((a_0,d_0^0),...,(a_n,d_0^n)),((a_0,d_1^0),...,(a_n,d_1^n)),...), & \text{若}x=((a_0,(d_0^0,d_1^0,...)),...,(a_n,(d_1^n,d_1^n,...)))\end{cases}.$$

函数$\theta:Z'\to\mathcal{F}(Z)$的构造如下所示:

$$\theta(x)=\begin{cases}((d_0^0,d_1^0,...),...,(d_1^n,d_1^n,...)), & \text{若}x=((d_0^0,d_0^1,...,d_0^n),(d_1^0,d_1^1,...,d_1^n),...)\\((a_0,(d_0^0,d_1^0,...)),...,(a_n,(d_1^n,d_1^n,...))), & \text{若}x=(((a_0,d_0^0),...,(a_n,d_0^n)),((a_0,d_1^0),...,(a_n,d_1^n)),...)\end{cases}.$$

显然, $\theta\circ\gamma=id_{\mathcal{F}(Z)}$,$\gamma\circ\theta=id_{Z'}$.

根据定理 5,函子$\mathcal{F}$的终余代数为(T,τ),其状态空间 T 是链 $1\xleftarrow{!}\mathcal{F}(1)\xleftarrow{\mathcal{F}(!)}\mathcal{F}^2(1)\xleftarrow{\mathcal{F}^2(f_1)}...$ 的极限.T 的元素是标号属于 $\sum_{0\leqslant n\leqslant\omega}AP^n$ 的所有有穷分支的有序有穷树;其结构$\tau:T\to\mathcal{F}(T)$把根为$(a_1,a_2,\ldots,a_n)$、直接子树(immediate sub-tree)为$(t_1,t_2,\ldots,t_n)$的树 $t\in T$ 映射到$((a_1,t_1),(a_2,t_2),\ldots,(a_n,t_n))$.

最后,我们构造映射 $\pi:\mathcal{F}\dot{\longrightarrow}\mathcal{G}$,对于每个集合 X,我们定义$\pi_X:\mathcal{F}(X)\to\mathcal{G}(X)$:

$$\pi_X(x)=\begin{cases}(\varnothing,\{x_0,x_1,...,x_n\}), & \text{若}x=(x_0,x_1,...,x_n)\\(\{a_1,a_2,...,a_n\},\{x_0,x_1,...,x_n\}), & \text{若}x=((a_0,x_0),...,(a_n,x_n))\end{cases}.$$

容易证明:π是从$\mathcal{F}$到$\mathcal{G}$的自然转换,并且每一个π_X都是满射的.根据定理 6,函子$\mathcal{G}$有一个终余代数.

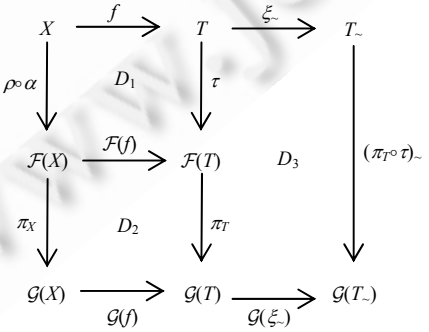
3.2 函子$\mathcal{G}$的终余代数

我们在上节证明了函子$\mathcal{G}$的终余代数的存在性,本节我们将给出该终余代数的具体构造.首先,我们引入一些基础知识:给定$\mathcal{G}$-余代数(S,α),对(S,α)上的任意互模拟 R 及任意 $s\in S$,我们定义:$[s]_R=\{s'\in S|(s,s')\in R\}$;$S_R=\{[s]_R|s\in S\}$;$\xi_R:S\to S_R$,使得$\xi_R(s)=[s]_R$;$\alpha_R:S_R\to\mathcal{G}(S_R)$,使得$\alpha_R([s]_R)=(\pi_1(\alpha(s)),\{[s']_R|s'\in\pi_2(\alpha(s))\})$:$S_R\to\mathcal{G}(S_R)$.容易证明:对于互模拟等价关系~而言,$\xi_{\sim}$是一个同态函数;$(S_{\sim},\alpha_{\sim})$是强外延的(见定理 2);对于任意的$\mathcal{G}$-余代数$(A,\alpha)$,若$f,g:(A,\alpha)\to(S_{\sim},\alpha_{\sim})$是两个同态,则$f=g$.

命题 3. $(T_{\sim},(\pi_T\circ\tau)_{\sim})$是$\mathcal{G}$的终余代数,其中,$(T,\tau)$是$\mathcal{F}$的终余代数.

证明:根据定义2,我们只需证明: (1) $(T_{\sim},(\pi_T\circ\tau)_{\sim})$是一个$\mathcal{G}$-余代数;(2) 对任意的$\mathcal{G}$-余代数$(X,\alpha)$,都存在一个$\mathcal{G}$-同态 $h:X\to T_{\sim}$;(3) 对任意的$\mathcal{G}$-余代数(X,α),若有两个$\mathcal{G}$-同态 $f,g:X\to T_{\sim}$,则 $f=g$.

我们仅证明第 2 点,即:下图中的 D_1,D_2,D_3 分别是可交换子图.



- D_1 是可交换的:任给$\mathcal{G}$-余代数(X,α),因为π_X是满射,故存在函数$\rho:\mathcal{G}(X)\to\mathcal{F}(X)$使得$\pi_X\circ\rho=id_{\mathcal{G}(X)}$,且$(X,\rho\circ\alpha)$是一个$\mathcal{F}$-余代数.由定义 2 可知,存在唯一一个从$(X,\rho\circ\alpha)$到$(T,\tau)$的$\mathcal{F}$-同态,即:子图 D_1 是可交换的;
- D_2 是可交换的:由定义 9 可得;
- D_3 是可交换的:因为$\xi_{\sim}$是从$(T,(\pi_T\circ\tau))$到$(T_{\sim},(\pi_T\circ\tau)_{\sim})$的$\mathcal{G}$-同态,根据定义 2,我们有:子图 D_3 是可交换的.

由上可知,$\xi_{\sim}\circ f:X\to T_{\sim}$是从$(X,\alpha)$到$(T_{\sim},(\pi_T\circ\tau)_{\sim})$的$\mathcal{G}$-同态. □

3.3 K_0的定义、性质及求解

定义 15(Kripke 结构的同态). 我们称函数$h:S\to S'$是从 Kripke 结构(S,S_0,R,L)到 Kripke 结构(S',S_0',R',L')的同态,如果对任意$s\in S$,$s\in S_0\Rightarrow h(s)\in S_0'$;$h(R(s))=R'(h(s))$;$L(s)=L'(h(s))$,若 h 为双射,则称其为同构.

定义 16(基于 *AP* 的最小 Kripke 结构). $\mathcal{K}$中的元素 M 被称为基于 AP 的最小 Kripke 结构(记为$K_0=(S^0,S_0^0,R^0,L^0)$),若其满足下述条件:对任意$M'\in\mathcal{K}$,存在唯一一个从 M'到 M 的同态 h,使得对 M'的任意两个状态 s,s'而言,$s\approx s'\Leftrightarrow h(s)=h(s')$.

命题 4. 令 K 为对应于余代数 Kripke 结构$((T_{\sim},(\pi_T\circ\tau)_{\sim}),T_{\sim})$的 Kripke 结构,则 K 是基于 AP 的最小 Kripke 结构.

证明:任给 Kripke 结构$M=(S,S_0,R,L)$,我们需要证明:存在唯一一个从 M 到 K 的同态 h,使得对任意的$s,s'\in S$,$s\approx s'\Leftrightarrow h(s)=h(s')$.根据命题 1 的证明,$((S,\alpha),S_0)$为 M 的余代数 Kripke 结构,其中,$\alpha(s)=(L(s),\{s'|(s,s')\in R\})$.同样地,我们有$K=(S^K,S_0^K,R^K,L^K)$,其中,$S^K=S_0^K=T_{\sim}$,$R^K=\{(s_1,s_2)|s_2\in\pi_2((\pi_T\circ\tau)_{\sim})(s_1)\}$,$L^K(s)=\pi_1((\pi_T\circ\tau)_{\sim})(s)$.

根据定义 2,存在唯一一个从$\mathcal{G}$-余代数(S,α)到$(T_{\sim},(\pi_T\circ\tau)_{\sim})$的同态 $h:S\to T_{\sim}$.

首先我们证明:h 是从 M 到 K 的同态(存在性).根据定义 15,需证:对任意的 $s\in S$:(1) $s\in S_0\Rightarrow h(s)\in S_0^K$;(2) $L(s)=L^K(h(s))$;(3) $h(R(s))=R^K(h(s))$.

1. $s\in S_0\Rightarrow h(s)\in T_{\sim}=S_0^K$;
2. $L(s)=\pi_1(\alpha(s))=\pi_1(\mathcal{G}(h)\circ\alpha(s))=\pi_1((\pi_T\circ\tau)_{\sim})\circ h(s)=L^K(h(s))$;
3. $h(R(s))=h(\{s'|(s,s')\in R\})=h(\pi_2(\alpha(s)))=\pi_2(\mathcal{G}(h)\circ\alpha(s))=\pi_2((\pi_T\circ\tau)_{\sim})\circ h(s)=R^K(h(s))$.

其次我们证明:若 h 是从 M 到 K 的同态,则 h 是从(S,α)到$(T_{\sim},(\pi_T\circ\tau)_{\sim})$的同态(唯一性);若$h:S\to S^K$是从 M 到 K 的同态,则对任意的 $s\in S$,我们有$\mathcal{G}(h)\circ\alpha(s)=\mathcal{G}(h)((L(s),R(s)))=(L(s),h(R(s)))=(L(s),R^K(h(s)))=(\pi_T\circ\tau)_{\sim}\circ h(s)$.因此,$h:S\to S^K$是一个从$(S,\alpha)$到$(T_{\sim},(\pi_T\circ\tau)_{\sim})$的同态,从而可得 h 是唯一的.

最后我们证明:对任意两个状态 s,s'而言,$s\approx s'\Leftrightarrow h(s)=h(s')$:由定理 3、引理 1 及命题 2 的证明可得. □

定理 8. 存在唯一一个基于 AP 的最小 Kripke 结构.

证明:由定理 1 和命题 4 的证明可得. □

4 K_M的求解

本节我们证明:对任意$M\in\mathcal{K}$,在互模拟等价的意义下,存在唯一一个相对于 M 的最小 Kripke 结构(记为 K_M).

4.1 K_M的定义及性质

定义 17(相对于 *M* 的最小 Kripke 结构). 令 $M\in\mathcal{K}$,我们称$\mathcal{K}$中的元素(S^M,S_0^M,R^M,L^M)为相对于 M 的最小 Kripke 结构(记为 K_M),若其满足下述性质:

- $M\equiv K_M$;
- $s\approx_{K_M}s'\Leftrightarrow s=s'$;
- 对任意的$s\in S^M$,s 是可达的,即:存在$s_0,s_1,\ldots,s_n\in S^M$使得$s_0\in S_0^M$,$R^M(s_i,s_{i+1})$,$s_n=s$.

定理 9. 对任意的$M\in\mathcal{K}$,在同构意义下,存在唯一一个 K_M.

证明:我们首先证明 K_M 的存在性,然后证明其唯一性.

存在性:

令 $M=(S,S_0,R,L)$,$h:S\to S^0$ 为 M 到 K 的同态.令 $K=(S^K,S_0^K,R^K,L^K)$,其中,

- $S^K=\{s^0\in S^0|$存在可达的状态 $s\in S$ 使得 $h(s)=s^0\}$;
- $S_0^K=\{s_0^K\in S^K\mid$存在$s_0\in S_0$使得$h(s_0)=s_K^0\}$;
- $R^K=\{(s^K,t^K)\in S^K\times S^K|$存在 $s,t\in S,R(s,t),h(s)=s^K,h(t)=t^K\}$;
- $L^K:s\mapsto L^0(s)$.

容易验证 $K\in\mathcal{K}$.下面证明 K 是 M 的最小 Kripke 结构:

(a) $K\equiv M$:容易证明 $B=\{(s,h(s))|s\in S\}$ 是 K 和 M 的互模拟关系.根据 K 的构造,对任意 $s_0\in S_0$,我们有 $B=(s_0,h(s_0))$,反之亦然;

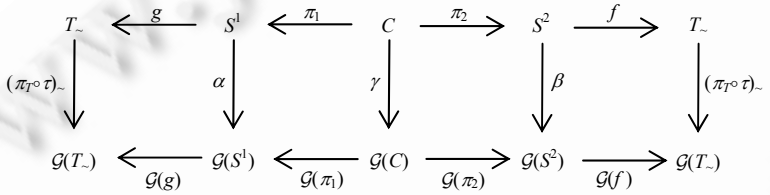
(b) $s_K\approx_K t_K\Leftrightarrow s_K=t_K$:由 K 的构造可知,存在 $s,t\in S$ 使得 $h(s)=s_K,h(t)=t_K$.根据定义 15,我们有 $s_K\approx_K t_K\Leftrightarrow s_K=t_K$;

(c) 对任意的 $s_K\in S^K$,s_K 是可达的:由 K 的构造可知,存在 $s\in S$ 使得 $h(s)=s_K$.由于 s 是可达的,则存在 $s_0,\ldots,s_n\in S$ 使得 $s_0\in S_0,R(s_i,s_{i+1}),s_n=s$,且 $h(s_0)\in S_0^K$,$R^K(h(s_i),h(s_{i+1})),h(s_n)=s_K$.

唯一性:

假设相对于 M 存在两个最小的 Kripke 结构 $M_1=(S^1,S_0^1,R^1,L^1),M_2=(S^2,S_0^2,R^2,L^2)$,我们只需证明 S^1 和 S^2 是等势的.为此,只需证明在 S^1 和 S^2 之间存在一个一一对应.

根据命题 1,存在函数 α,β 使得 $((S^1,\alpha),S_0^1),((S^2,\beta),S_0^2)$ 分别为 M_1,M_2 的余代数 Kripke 结构.根据定义 17,我们有 $M_1\equiv M_2\equiv M_3$.根据命题 2,我们有 $((S^1,\alpha),S_0^1)\doteq((S^2,\beta),S_0^2)$.根据定义 14,存在$(S^1,\alpha)$和$(S^2,\beta)$之间的互模拟关系 C 以及映射 γ,g,f 使得下图是可交换的,即:$\alpha\circ\pi_1=\mathcal{G}(\pi_1)\circ\gamma,\beta\circ\pi_2=\mathcal{G}(\pi_2)\circ\gamma,(\pi_T\circ\tau)_\sim\circ g=\mathcal{G}(g)\circ\alpha,(\pi_T\circ\tau)_\sim\circ f=\mathcal{G}(f)\circ\beta$.



下面证明 C 是 S^1 和 S^2 之间的一一对应.根据定义 14,$S_0^1\subseteq\pi_1(C)$.因为 M_1 是 M 的最小的 Kripke 结构,对任意 $s\in S^1$ 而言,s 是可达的,所以 $S^1\subseteq\pi_1(C)$.同理,$S^2\subseteq\pi_2(C)$.由于 $g\circ\pi_1$ 和 $f\circ\pi_2$ 都是从(C,γ)到$(T_\sim,(\pi_T\circ\tau)_\sim)$的同态,根据定义 2,$g\circ\pi_1=f\circ\pi_2$.假设存在 $s\in S^1,s',s''\in S^2$ 使得 $C(s,s')$和 $C(s,s'')$且 $s'=s''$,我们有 $g(s)=g\circ\pi_1(s,s')=f\circ\pi_2(s,s')=f(s')$.同理,我们有 $g(s)=f(s'')$.因此,$f(s'')=f(s')$.根据定理 3,我们有 $s'\sim_{M^2}s''$;又因为 M_2 是最小的,所以 $s'=s''$,与假设矛盾.因此,对于任意 $s\in S^1$ 都存在唯一的 $s'\in S^2$ 使得 $C(s,s')$;同理,对于任意 $s\in S^2$ 都存在唯一的 $s'\in S^1$ 使得 $C(s',s)$. □

4.2 求解K_M的算法

令 h 为 M 到 K_0 的同态,根据定理 9 的证明,K_M 为 M 在 h 下的像.根据定义 16,我们有 $s\approx s'\Leftrightarrow h(s)=h(s')$,因此,$S^M=\{[s]_\approx|s\in S\}$,$S^M=\{[s]_\approx|s\in S\}$,$S_0^M=\{[s]_\approx\mid s\in S_0\}$,$R^M=\{([s]_\approx,[t]_\approx|R(s,t)\}$,$L^M([s]_\approx)=L(s)$,其中,$[s]_\approx=\{s'|s\approx s'\}$.由此,我们给出求解 K_M 的算法,详见算法 1.

算法 1 的输入是一个由简单图文法(SGG)所表示的 Kripke 结构.这里,我们仅简单介绍 SGG,详细内容请见文献[11].一个 SGG 为一个二元组$\mathcal{G}_0=(G_0,A)$,其中,$G_0=(S_{G_0},S_0^{G_0},R_{G_0},L_{G_0})$ 为$\mathcal{K}$的一个元素,G_0 有 N 个接口状态 $(ex_i)_1^N$;$A=(S_A,\varnothing,R_A,L_A)$为$\mathcal{K}$的一个元素,$A$ 有 $2N$ 个接口状态 $(in_i)_1^N$ 和 $(out_i)_1^N$;并且 $L_{G_0}(ex_i)=L_A(in_i)=L_A(out_i)$.$\mathcal{G}_0$ 所表示的 Kripke 结构为$\mathcal{G}_0$ 和 A 叠加所得到的 Kripke 结构(将 $(ex_i)_1^N$ 与 $(in_i)_1^N$ 重叠,将 $(in_i)_1^N$ 与 $(out_i)_1^N$ 重叠).其中,$S_{G_0}/(ex_i)_1^N$ 和 $S_A/(out_i)_1^N$ 分别相对于 $(in_i)_1^N$ 和 $(out_i)_1^N$ 是不可达的,否则,K_M 是无穷状态的 Kripke 结构.特别地,

若 G_0 表示一个有穷状态的 Kripke 结构,则 $S_A=\varnothing$.

在算法 1 中,由(G_0,A)转化得到的 Kripke 结构 M 的状态空间 $|S|=|\overline{G_0}|+|\overline{A}|$.虽然算法 1 循环层次很多,但是只有第 26 行~第 35 行的代码用了两层状态级别的循环(其中一个是$\forall G((R(s')\cap G==\varnothing)==(R(S)\cap G==\varnothing))$).所以,算法 1 的时间复杂度为 $O((|\overline{G_0}|+|A|)^2)$.

算法 1. Kripke 结构的最小化.

Minimize*Inf*(G_0,A) /*the input is an $SGG(G_0,A)$*/

1. $S=S_{G_0}\cup\left(S_A/(in_i)_1^N\right)/(out_i)_1^N$; /*transform $SGG(G_0,A)$ to M*/
2. $S_0=S_0^{G_0}$;
3. $R=R_{G_0}\cup\{(s_1,s_2)\in R_A\mid s_1,s_2\notin(in_i)_1^N)\cup(out_i)_1^N\}\cup$
   $\{(s_1,ex_i)\mid(s_1,in_i)\in R_A\vee(s_1,out_i)\in R_A,i\in[1,N]\}\cup\{(ex_i,s_1)\mid(in_i,s_1)\in R_A\}$
4. **if** $s\in G_0$ **then**
5. $L(s)=L_{G_0}(s)$;
6. else
7. $L(s)=L_A(s)$;
8. **end if**
9. $M=(S,S_0,R,L)$; /*minimize M*/
10. initialize a set $\Pi=\varnothing$;
11. **for** $s\in S$ **do** /*allocate states with same label in the same set*/
12. initialize a new state set $G_{new}=\{s\}$, where $s\in S$;
13. **for** each $s'\in S$ **do**
14. **if** $L(s')=L(s)$ **then**
15. $G_{new}=G_{new}\cup\{s\}$;
16. $S=S-\{s'\}$;
17. **end if**
18. **end for**
19. $\Pi=\Pi\cup G_{new}$;
20. **end for**
21. initialize a new set $\Pi_{new}=\varnothing$;
22. **while** $\Pi_{new}!=\Pi$ **do**
23. $\Pi_{new}=\Pi$;
24. **for** $G\in\Pi$ **do**
25. **for** $s\in G$ **do**
26. initialize a new state set $G_{new}=\{s\}$, where $s\in G$;
27. **for** $s'\in G$ **do**
28. **if** $\forall G((R(s')\cap G==\varnothing)==(R(S)\cap G==\varnothing))$ **then**
29. $G_{new}=G_{new}\cup\{s\}$;
30. $G=G-\{s\}$;
31. **end if**
32. **end for**
33. $\Pi=\Pi\cup G_{new}$;
34. **end for**

35. **end for**

36. **end while**

37. $S^M=\Pi$;

38. $S_0^M=\{\pi\in\Pi\mid\pi\cap S_0\neq\varnothing\}$;

39. $R^M=\{(\pi_1,\pi_2)\in\Pi\times\Pi\mid\exists s_1,s_2(s_1\in\pi_1\wedge s_2\in\pi_2\wedge R(s_1,s_2))\}$;

40. $L_M:\Pi\to 2^{AP},\pi\mapsto L(s)$ with $s\in\pi$;

41. $K_M=(S_M,S_0^M,R_M,L_M)$;

42. **return** K_M;

4.3 例 子

本节简单介绍两个求解 K_M 的例子.

例 1:对于图 1 中的 Kripke 结构 M,应用算法 1 可获得其最小 Kripke 结构 K_M.

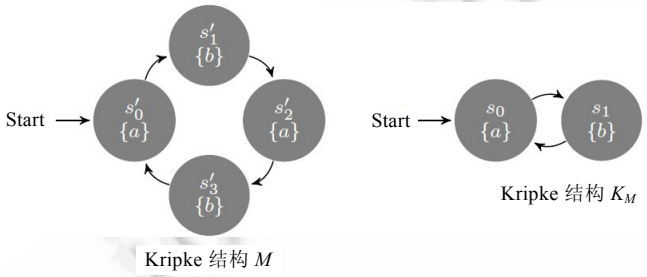


Fig.1 An example of finite Kripke structure

图 1 有穷状态 Kripke 结构的例子

例 2:令 $M=(\omega,I,R,L)$为基于 $AP=\{p_0,p_1,p_2,p_3,p_4\}$的无穷状态 Kripke 结构,其中,$\omega$为自然数集,$I=\{0\}$,$R=\{(n,n+1)\mid n\in\omega\}$,$L(n)=\{p_i\mid i=n\%5\}$.应用算法 1,$K_M$ 为有穷状态的 Kripke 结构 (S^M,S_0^M,R^M,L^M),其中,$S^M=\{s_0,s_1,s_2,s_3,s_4\}$, $S_0^M=\{s_0\}$,$R^M=\{(s_0,s_1),(s_1,s_2),(s_2,s_3),(s_3,s_4),(s_4,s_0)\}$,$L^M(s_i)=\{p_i\}$.

5 总 结

我们为由基于 AP 的所有 Kripke 结构所构成的类$\mathcal{K}$构造了函子$\mathcal{P}_f(AP)\times\mathcal{P}_f(\cdot)$,并且求出其终余代数.对$\mathcal{K}$而言,我们证明了在互模拟等价意义下的最小 Kripke 结构(记为 K_0)的存在唯一性.进而,对于任意的 $M\in\mathcal{K}$,我们证明了其最小 Kripke 结构 K_M 的存在唯一性,提出了一种求解 K_M 的算法,并用 Ocaml 予以简单实现.该算法可以应用于一些 Rational Kripke 模型的最小化,但不适用于无穷分支的 Rational Kripke 模型(其状态可能有无穷多个直接后继)[12],这是由于我们的算法是基于函子$\mathcal{P}_f(AP)\times\mathcal{P}_f(\cdot)$的终余代数的存在唯一性.本文的应用之一在于:可以用状态空间更小的 K_M 代替 M 进行模型检测(见定理 7).该方法可自然地推广到基于其他类型函子的余代数结构,比如 Markov Chain 等.

References:

[1] Jacobs B, Rutten J. A tutorial on (CO) algebras and (CO) induction. Theoretical Computer Science, 1997,182(1-2):222−259.

[2] Sangiorgi D. Introduction to Bisimulation and Coinduction. New York: Cambridge University Press, 2012.

[3] Aczel P, Mendler P. A final coalgebra theorem. In: Pitt D, Rydeheard D, Dybjer P, Pitts A, Poigné A, eds. Proc. of the Category Theory and Computer Science. LNCS 389, Heidelberg: Springer-Verlag, 1989. 357−365. [doi: 10.1007/BFb0018361]

[4] Rutten J, Turi D. Initial algebra and final coalgebra semantics for concurrency. In: Bakker J, Roever W, Rozenberg G, eds. Proc. of the Decade of Concurrency, Reflections and Perspectives. LNCS 803, Heidelberg: Springer-Verlag, 1994. 530−582. [doi: 10.1007/3-540-58043-3_28]

[5] Clarke EM, Grumberg O, Peled DA. Model Checking. Cambridge: MIT Press, 1999.

[6] Dovier A, Piazza C, Policriti A. An efficient algorithm for computing bisimulation equivalence. Theoretical Computer Science, 2004,311(1-3):221−256. [doi: 10.1016/S0304-3975(03)00361-X]

[7] Bonchi F, Montanari U. Minimization algorithm for symbolic bisimilarity. In: Castagna G, ed. Proc. of the ESOP 2009. LNCS 5502, Heidelberg: Springer-Verlag, 2009. 267−284. [doi: 10.1007/978-3-642-00590-9_20]

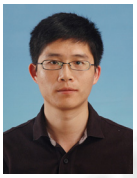
[8] Burkart O, Caucal D, Moller F, Steffen B. Verification on Infinite Structures. Bergstra J, Ponse A, Smolka S, eds. Handbook of Process Algebra. New York: Elsevier Science, 2000. 545−623.

[9] Katoen JP, Kemna T, Zapreev I, Jansen DN. Bisimulation minimisation mostly speeds up probabilistic model checking. In: Grumberg O, Huth M, eds. Proc. of the Tools and Algorithms for the Construction and Analysis of Systems. LNCS 4424, Heidelberg: Springer-Verlag, 2007. 87−101. [doi: 10.1007/978-3-540-71209-1_9]

[10] Pierce B. Basic Category Theory for Computer Scientists. Cambridge: MIT Press, 1991.

[11] Quemener YM, Jéron T. Model-Checking of infinite Kripke structures defined by simple graph grammars. Electronic Notes in Theoretical Computer Science, 1995,2:222−229. http://www.sciencedirect.com/science/journal/15710661/2 [doi: 10.1016/S1571-0661(05)80200-2]

[12] Bekker W, Goranko V. Symbolic model checking of tense logics on rational Kripke models. In: Archibald M, Brattka V, Goranko V, Löwe B, eds. Proc. of the ILC 2007. LNCS 5489, Heidelberg: Springer-Verlag, 2009. 2−20. [doi: 10.1007/978-3-642-03092-5_2]



高建华(1986－),男,河南新乡人,博士生,CCF 学生会员,主要研究领域为定理证明,模型检测.
E-mail: gaojh@ios.ac.cn

蒋颖(1958－),女,博士,研究员,博士生导师,CCF 高级会员,主要研究领域为λ演算,共代数,自动推理与模型检测,进程演算与树自动机,程序设计语义学,网络建模.
E-mail: jy@ios.ac.cn