中国科学院大学2022春季学期

形式化方法

中国科学院软件研究所
张文辉

前言

随着计算机科学和应用的发展，软件产品经历了从简单计算程序到分布式系统和移动计算等越来越复杂的软件结构和功能。软件在尖端领域的应用更加需要软件设计理论上的支持以构建正确可靠的软件系统。

形式化方法的目标是开发满足给定需求的程序与软件，即具有正确性保证的程序与软件。形式化方法依赖的理论与技术是软件系统行为的数学模型、逻辑描述、以及形式化的分析验证方法。

软件正确性问题就是在程序与软件基础上建立的计算机软件系统的行为是否合乎行为规范的问题。软件系统行为的基本组成部分可以理解为系统状态变化的无穷序列或者是可表示状态的若干可能后继的计算树。软件系统行为通常可抽象地用具有状态变化的动态系统来描述而软件系统行为的规范通常用较为简单的容易理解的方式如逻辑和自动机等。正确性问题涉及三个方面：软件系统行为、行为规范、软件系统行为是否符合行为规范的分析验证。

计算机科学界在形式验证的理论和算法方面做了长期的研究。基础的程序分析和程序验证的理论工作在六十、七十年代取得了奠基性的成果。进入七十年代后期和八十年代，由于分布式系统和计算机网络的发展，并发理论研究成为计算机领域的前沿课题。由于计算机软件变得更为复杂和难于验证分析，基于演绎推理的分析和验证方法，从实际应用的角度有着一定的局限性。演绎推理只能证明系统满足给定的性质。对于不能证明的性质，演绎推理在一般情况下，并不能确定是性质不满足或是证明的思路不对或证明的过程过于复杂。八十年代兴起的模型检测研究试图寻求有效的算法来验证系统和系统性质的关系。对于有穷状态模型，这种方法从理论上能够验证性质是否满足，并能在性质不满足的情况下举例说明。模型检测方法主要针对有穷状态模型，与演绎推理形成一种互补关系。

本书主要介绍形式化方法的基本概念和动态系统及其行为规范的描述方法与分析验证方法。动态系统的描述方法以离散迁移系统为主。相关行为规范的描述语言包括用于描述顺序计算系统性质的一阶逻辑和描述并发系统性质的时序逻辑。相关分析验证方法包括基于推理规则的演绎推理和基于状态搜索的模型检测。本书内容的章节划分如下。第1章介绍预备知识，第2-4章介绍不同类型的迁移系统，第5-6章介绍时序逻辑，第7-8章分别介绍演绎推理和模型检测方法，第9章介绍实例分析。附录A介绍第9章的实例分析中用到的模块化迁移系统建模语言。附录B为参考文献。若本书应用于研究生教学，由于学生的基础知识可能存在一定的差别，预备知识部分可先略过，其后章节内容中若有用到学生可能缺乏的相关预备知识时再稍加回顾；实例分析的部分内容可在介绍理论与方法时一并介绍且可进行适当简化裁剪以服务于这些方法的应用举例并对不同方法在同一个验证问题上的应用进行对照比较。

形式化方法虽然在理论上具有保证程序与软件系统在模型层次上的正确性的优越性，但对于实际应用而言，由于形式描述和验证的复杂性，其使用范围十分受限。众多的相关研究试图为形式化方法理论和应用中的一些问题提供解决方案，本书涉及基本的概念和方法，希望其内容能够帮助读者在形式化方法的研究和应用方面提供相关基础知识和基本方法。

目录

§1 预备知识

本章介绍逻辑、集合、关系和有向图方面的知识。

§1.1 命题逻辑

命题是具有确定真假意义的陈述句，是逻辑推理的基本元素。真假值用1和0表示。简单命题是不可分解的命题。复合命题由简单命题和联结词组成。通常我们有一元联结词$\neg$（非）和二元联结词$\wedge$（合取）,$\vee$（析取）, $\rightarrow$（蕴涵）,$\leftrightarrow$（等价）等。n-元联结词可以看成是$\{0,1\}^n$到$\{0,1\}$的函数。我们有$\neg 1 = 0$和$\neg 0 = 1$。用A,B,C等字母表示命题变元，以下是$\wedge, \vee, \rightarrow, \leftrightarrow$的真值表。

A	B		$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$
0	0		0	0	1	1
0	1		0	1	1	0
1	0		0	1	0	0
1	1		1	1	1	1

命题变元称为原子公式。公式集合由归纳定义生成。设S是联结词的集合。由S生成的公式如下。（1）命题变元（原子公式）是由S生成的公式; （2）若φ是S中的0元联结词，则φ是由S生成的公式; （3）若f是S中的n元$(n \geq 1)$联结词，$\varphi_1, ..., \varphi_n$是由$S$ 生成的公式，则$f(\varphi_1, ..., \varphi_n)$是由$S$生成的公式。这里用的是前缀记法。对于二元联结词，我们习惯使用中缀记法。我们规定联结词的优先级以省略括号。联结词的优先级按顺序排列如下：$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$。

由全体命题变元组成的集合到$\{0,1\}$的函数称为真值赋值。设v是真值函数。记A^v为v赋给A的值。由S生成的公式φ在v下的值定义如下。（1）若φ是命题变元A，则$v(\varphi) = A^v$; （2）若φ是S中的0元联结词c，则$v(\varphi) = c$; （3）若$\varphi = f(\varphi_1, ..., \varphi_n)$，其中$f$是$S$中的n元$(n \geq 1)$联结词，则$v(\varphi) = f(v(\varphi_1), ..., v(\varphi_n))$。

如果真值赋值v使得$v(\varphi) = 1$，则称v满足φ，记作$v \models \varphi$。

如果有真值赋值v，使得$v \models \varphi$，则称φ为可满足式。否则称φ为永假式（不可满足式）。如果对于每个真值赋值v，都有$v \models \varphi$，则称φ为永真式（重言式）。

如果对于每个真值赋值v，都有$v(\varphi) = v(\psi)$，则称φ与ψ逻辑等价，记作$\varphi \Leftrightarrow \psi$。$\varphi \Leftrightarrow \psi$当且仅当$\varphi \leftrightarrow \psi$是永真式。

修改真值赋值v中$A_1, ..., A_n$的赋值为$a_1, ..., a_n$得到的赋值记作$v[A_1/a_1, ..., A_n/a_n]$。设$v' = v[A_1/a_1, ..., A_n/a_n]$。我们有

$$v'(A) = \begin{cases} a_i & if \quad A = A_i, i \in \{1, ..., n\} \\ A^v & if \quad A \notin \{A_1, ..., A_n\} \end{cases}$$

用公式$\varphi_1, ..., \varphi_n$分别替换公式$\varphi$中的不同命题变元$A_1, ..., A_n$ 得到的公式记作$\varphi^{\varphi_1,...,\varphi_n}_{A_1,...,A_n}$. 我们有

$$v(\varphi^{\varphi_1,...,\varphi_n}_{A_1,...,A_n}) = v[A_1/v(\varphi_1), ..., A_n/v(\varphi_n)](\varphi)$$

设φ是由$\{0, 1, \neg, \wedge, \vee\}$生成的公式。将$\varphi$中的$\wedge$ 与$\vee$互换、0与1互换等到的公式φ^*，称为φ的对偶式。对于真值赋值v和其相反的真值赋值v'，我们有$v(\varphi) = \neg v'(\varphi^*)$。设$\varphi$与$\varphi^*$互为对偶式，$\psi$与$\psi^*$互为对偶式。如果$\varphi \Leftrightarrow \psi$，则$\varphi^* \Leftrightarrow \psi^*$。

逻辑公式的合取、析取和否运算满足幂等律、结合律、交换律、分配律、吸收律，德摩根律（对偶关系）。

$A \wedge A$	$=$	A	$A \vee A$	$=$	A
$A \wedge (B \wedge C)$	$=$	$(A \wedge B) \wedge C$	$A \vee (B \vee C)$	$=$	$(A \vee B) \vee C$
$A \wedge B$	$=$	$B \wedge A$	$A \vee B$	$=$	$B \vee A$
$A \wedge (B \vee C)$	$=$	$A \wedge B \vee A \wedge C$	$A \vee (B \wedge C)$	$=$	$A \vee B \wedge A \vee C$
$A \wedge (A \vee B)$	$=$	A	$A \vee (A \wedge B)$	$=$	A
$\neg(A \wedge B)$	$=$	$\neg A \vee \neg B$	$\neg(A \vee B)$	$=$	$\neg A \wedge \neg B$

设f是n元联结词，$A_1, ..., A_n$是不同的命题变元。如果公式φ中不出现除$A_1, ..., A_n$之外的的命题变元，且$\varphi = f(A_1, ..., A_n)$，则称$\varphi$定义$f$。如果存在由$S$生成的公式定义$f$，则称$f$可由$S$定义。

设S是联结词集合。若每个n元$(n \geq 1)$联结词都可由S定义，则称S为完全集。若S的任何真子集都不是完全集，则称S为极小完全集。$\{\neg, \wedge, \vee\}$是完全集，$\{\neg, \wedge\}$是极小完全集。

设Γ为公式集合，如果真值赋值v满足Γ中的每个公式，则称v满足Γ。如果有真值赋值v满足Γ，则称Γ是可满足的。否则称Γ是不可满足的。

设Γ为公式集合，φ为公式。如果每个满足公式集合Γ的真值赋值都满足φ，则称φ是Γ的逻辑推论，记作$\Gamma \models \varphi$。$\Gamma \models \varphi$不成立记作$\Gamma \not\models \varphi$。若$\Gamma = \{\varphi_1, ..., \varphi_n\}$，则将$\Gamma \models \varphi$ 写作$\varphi_1, ..., \varphi_n \models \varphi$。

设$\varphi_1, ..., \varphi_n, \varphi, \psi$为公式。$\models \varphi$当且仅当$\varphi$是永真式。$\varphi_1, ..., \varphi_n \models \varphi$ 当且仅当$\varphi_1 \wedge \cdots \wedge \varphi_n \to \varphi$是永真式。$\varphi \Leftrightarrow \psi$ 当且仅当$\varphi \models \psi$且$\psi \models \varphi$。$\Gamma \cup \{\varphi\} \models \psi$当且仅当$\Gamma \models \varphi \to \psi$。$\Gamma = \{\varphi_1, ..., \varphi_n\}$ 是可满足的当且仅当$\varphi_1 \wedge \cdots \wedge \varphi_n$是可满足的。设$\Gamma$是公式集合。则$\Gamma$是不可满足的当且仅当每个公式都是$\Gamma$的逻辑推论。

§1.2 谓词逻辑

谓词逻辑可以对所考察的命题加以细化，分清主词和谓词，考虑一般和个别情况。谓词逻辑中使用的符号有以下几组：(1) 个体变元，简称变元，有无穷多个，用x, y, z, u, v, w表示。(2) 个体常元，简称常元，用a, b, c表示。(3) 函数符号，每个符号都有与之相联系的正整数n，并称该符号为n元函数符号，用f, g, h表示。(4) 谓词符号，每个符号都有与之相联系的正整数n，并称该符号为n元谓词符号，用A, B, C表示。(5) 量词符号$\forall$和$\exists$。(6) 联结词符号$\neg, \wedge, \vee, \to, \leftrightarrow$。(7) 左括号（，右括号），点。和逗号，。

设F是常元和函数符号的集合。由F生成的项定义如下。（1）变元是由F生成的项；（2）F中的常元是由F生成的项；（3）若f是F中的n元$(n \geq 1)$函数符号，$t_1, ..., t_n$是由F生成的项，则$f(t_1, ..., t_n)$是由F生成的项。

设G是谓词符号的集合。若$t_1, ..., t_n$是由F生成的项，A是P中的n元谓词符号，则$A(t_1, ..., t_n)$是由(F, G)生成的原子公式。

$B = (F, G)$上的公式集合，记作$\mathcal{L}^B$，定义如下。（1）由(F, G)生成的原子公式是$\mathcal{L}^B$的公式；(2) 若f是$\{\neg, \wedge, \vee, \to, \leftrightarrow\}$中的n元$(n \geq 1)$联结词，$\varphi_1, ..., \varphi_n$是$\mathcal{L}^B$的公式，则$f(\varphi_1, ..., \varphi_n)$是$\mathcal{L}^B$的公式；(3) 若$\varphi$是$\mathcal{L}^B$的公式，$x$是变元，则$\forall x\varphi$和$\exists x\varphi$是$\mathcal{L}^B$的公式。

一个解释I由两个部分组成。其一是一个非空集合，称为论域，其二是B中符号到论域中的元素、函数、谓词的解释（映射）。设$I = (D, I_0)$。对于每个常元a，$I_0(a)$为D中的一个元素；

对于每个n元函数符号f，$I_0(f)$为D中的一个n元函数；对于每个n元谓词符号P，$I_0(P)$为D中的一个n元谓词。

设I是一个解释。从所有变元组成的集合到论域D的函数称为I中的赋值。修改赋值σ中$x_1,...,x_n$的赋值为$a_1,...,a_n$得到的赋值记作$\sigma[x_1/a_1,...,x_n/a_n]$。我们有

$$\sigma[x_1/a_1,...,x_n/a_n](x) = \begin{cases} a_i & if \quad x = x_i, i \in \{1,...,n\} \\ \sigma(x) & if \quad x \notin \{x_1,...,x_n\} \end{cases}$$

解释和赋值共同规定了项和公式的意义。设σ是I中的赋值。项t在解释I和赋值σ下的意义$I(t)\sigma$定义如下。(1) 若t是变元x，则$I(t)\sigma = \sigma(x)$；(2) 若t是常元a，则$I(t)\sigma = I_0(a)$；(3) 若t是$f(t_1,...,t_n)$，其中f是n元函数符号，$t_1,...,t_n$是项，则$I(t)\sigma = I_0(f)(I(t_1)\sigma,...,I(t_n)\sigma)$。

设σ是I中的赋值。公式φ在解释I和赋值σ下的意义$I(\varphi)\sigma$定义如下。(1) 若φ是$P(t_1,...,t_n)$，其中P是n元谓词符号，$t_1,...,t_n$ 是项，则$I(\varphi)\sigma = I_0(P)(I(t_1)\sigma,...,I(t_n)\sigma)$； (2) 若$\varphi$是$\neg\psi$，$\psi$是公式，则$I(\varphi)\sigma = \neg I(\psi)\sigma$； (3) 若$\varphi$是$\varphi_0 \wedge \varphi_1$，则$I(\varphi)\sigma = I(\varphi_0)\sigma \wedge I(\varphi_1)\sigma$； (4) 若$\varphi$是$\varphi_0 \vee \varphi_1$，则$I(\varphi)\sigma = I(\varphi_0)\sigma \vee I(\varphi_1)\sigma$；(5) 若$\varphi$是$\varphi_0 \to \varphi_1$，则$I(\varphi)\sigma = I(\varphi_0)\sigma \to I(\varphi_1)\sigma$；(6) 若$\varphi$是$\varphi_0 \leftrightarrow \varphi_1$，则$I(\varphi)\sigma = I(\varphi_0)\sigma \leftrightarrow I(\varphi_1)\sigma$；(7) 若$\varphi$是$\forall x\psi$，则$I(\varphi)\sigma = 1$当且仅当对于所有$d \in D$，$I(\psi)\sigma[x/d] = 1$；(8) 若$\varphi$是$\exists x\psi$，则$I(\varphi)\sigma = 1$当且仅当存在$d \in D$使得$I(\psi)\sigma[x/d] = 1$。

如果公式ψ在公式φ中出现，则称ψ为φ的子公式。变元x在$\forall x\varphi$或$\exists x\varphi$中的出现为约束出现，并称$\forall x$或$\exists x$的该次出现的辖域为φ。如果变元x在φ中的某次出现是在φ的一个子公式中的约束出现，则称x的该次出现为在φ中的约束出现。如果变元x在φ中的某次出现不是约束出现，则称该出现为在φ中的自由出现。在公式φ中有自由出现的变元称为φ的自由变元，在公式φ中有约束出现的变元称为φ的约束变元。φ中自由变元的集合记为$Var(\varphi)$。

不出现变元的项称为基项。没有自由变元的公式称为语句。没有约束变元的公式称为开公式。若$Var(\varphi) = \{x_1,...,x_n\}$，则称公式$\forall x_1 \cdots \forall x_n\varphi$ 为φ的闭包。每个公式的闭包是一个语句，每个语句的闭包是它自己。

若t是基项，则对任意σ, σ'有$I(t)\sigma = I(t)\sigma'$，即基项的意义与赋值无关。因此对于基项我们可将$I(t)\sigma$简记为$I(t)$。若φ是语句，则对任意σ, σ'有$I(\varphi)\sigma = I(\varphi)\sigma'$。因此对于语句我们可将$I(\varphi)\sigma$简记为$I(\varphi)$。

若$x_1,...,x_n$是不同的变元，$t_1,...,t_n$是项，则称$\{x_1/t_1,...,x_n/t_n\}$ 为代换。若t是项，则$t\{x_1/t_1,...,x_n/t_n\}$是用$t_1,...,t_n$分别替换t中$x_1,...,x_n$的所有出现得到的项，记为$t^{t_1,...,t_n}_{x_1,...,x_n}$。若$\varphi$是公式，则$\varphi\{x_1/t_1,...,x_n/t_n\}$是用$t_1,...,t_n$分别替换$t$中$x_1,...,x_n$的所有自由出现得到的公式，记为$\varphi^{t_1,...,t_n}_{x_1,...,x_n}$。如果在公式$\varphi$和$\varphi^{t_1,...,t_n}_{x_1,...,x_n}$ 中变元的约束出现次数相同，则称$t_1,...,t_n$对于φ中的$x_1,...,x_n$是可代入的。若$t_1,...,t_n$对于φ中的$x_1,...,x_n$是可代入的，则有

$$I(\varphi^{t_1,...,t_n}_{x_1,...,x_n})\sigma = I(\varphi)\sigma[x_1/I(t_1)\sigma,...,x_n/I(t_n)\sigma]$$

如果解释I和I中的赋值σ使得$I(\varphi)\sigma = 1$，则称解释I和赋值σ满足φ，记作$\sigma \models_I \varphi$。当解释给定时，简记为$\sigma \models \varphi$。

如果有解释I和I中的赋值σ使得$\sigma \models_I \varphi$，则称φ为可满足式。否则称φ为永假式（不可满足式）。如果φ在每个解释中为真，则称φ为永真式（逻辑有效式）。

用谓词逻辑公式$\varphi_1,...,\varphi_i$分别替换命题逻辑公式φ中的命题变元$A_1,...,A_n$得到的谓词逻辑公式记为$\varphi^{\varphi_1,...,\varphi_n}_{A_1,...,A_n}$，称为$\varphi$的替换实例。命题逻辑永真式的替换实例称为重言式。

设φ和ψ是公式。如果对于每个解释I和I中的赋值σ，$I(\varphi)\sigma = I(\psi)\sigma$，则称$\varphi$和$\psi$逻辑等价，记为$\varphi \Leftrightarrow \psi$。$\varphi \Leftrightarrow \psi$当且仅当$\varphi \leftrightarrow \psi$是永真式。对于$\forall$和$\exists$，我们有$\forall x\varphi \Leftrightarrow \neg\exists x\neg\varphi$。

设Γ为公式集合，解释I和I中的赋值σ满足Γ中的每个公式，则称I和σ满足Γ。如果有解释I和I中的赋值σ满足Γ，则称Γ是可满足的。否则称Γ是不可满足的。

设Γ为公式集合，φ为公式。如果每个满足公式集合Γ的解释I和I中的赋值σ都满足φ，则称φ是Γ的逻辑推论，记作$\Gamma \models \varphi$。$\Gamma \models \varphi$不成立记作$\Gamma \not\models \varphi$。若$\Gamma = \{\varphi_1, ..., \varphi_n\}$，则将$\Gamma \models \varphi$ 写作$\varphi_1, ..., \varphi_n \models \varphi$。

设$\varphi_1, ..., \varphi_n, \varphi, \psi$为公式。$\models \varphi$当且仅当$\varphi$是永真式。$\varphi_1, ..., \varphi_n \models \varphi$ 当且仅当$\varphi_1 \wedge \cdots \wedge \varphi_n \to \varphi$是永真式。$\varphi \Leftrightarrow \psi$ 当且仅当$\varphi \models \psi$且$\psi \models \varphi$。$\Gamma \cup \{\varphi\} \models \psi$当且仅当$\Gamma \models \varphi \to \psi$。$\Gamma = \{\varphi_1, ..., \varphi_n\}$ 是可满足的当且仅当$\varphi_1 \wedge \cdots \wedge \varphi_n$是可满足的。设$\Gamma$是公式集合。则$\Gamma$是不可满足的当且仅当每个公式都是$\Gamma$的逻辑推论。

§1.3 集合

集合是由一些个体组成的整体。这些个体称为集合的元素。集合的定义有两种：枚举定义和抽象定义。枚举定义即是列出所有属于集合的元素。如：$A = \{a, b, c\}$。抽象定义即是说明属于集合的元素所具有的性质特征。如：$A = \{x \in \mathbf{N} \mid x > 1\}$或$x \in A \Leftrightarrow x > 1$。

两个集合相等，记作$A = B$，当且仅当他们具有相同的元素。集合A是集合B的子集，或说集合A包含于集合B，记作$A \subseteq B$，当且仅当所有A的元素都是B的元素。

$$\boxed{\begin{array}{lcl} (A = B) & \Leftrightarrow & \forall x(x \in A \leftrightarrow x \in B) \\ (A \subseteq B) & \Leftrightarrow & \forall x(x \in A \to x \in B) \end{array}}$$

子集关系满足以下性质。

$$\boxed{\begin{array}{l} A \subseteq A \\ A \subseteq B \text{ 且} B \subseteq C \text{ 则} A \subseteq C \\ A \subseteq B \text{ 且} B \subseteq A \text{ 则} A = B \end{array}}$$

不含有任何元素的集合称为空集，记作$\emptyset$。空集是最小的集合，是唯一的，它包含于任何集合之中。由有限多个元素构成的集合称为有穷集。由无限多个元素构成的集合称为无穷集。集合A的全部子集的集合称为A的幂集，记作2^A，即$2^A = \{X \mid X \subseteq A\}$。若$a \in A$，则$\{a\} \subseteq A$。若$A \subseteq B$，则$A \in 2^B$。有穷集合$A$的元素个数称为基数，记作$|A|$。设$A$是有穷集合，则$|2^A| = 2^{|A|}$。

集合的运算有交、并、差。

$$\boxed{\begin{array}{ll} \text{交} & A \cap B = \{x \mid x \in A \wedge x \in B\} \\ \text{并} & A \cup B = \{x \mid x \in A \vee x \in B\} \\ \text{差} & A - B = \{x \mid x \in A \wedge x \notin B\} \end{array}}$$

若$A \cap B = \emptyset$，则称A和B是不相交的。集合A和B的差集$A - B$又称B关于A的相对补集。设U是全集或论域，即所有与讨论相关的集合都是该全集的子集。设A是U的子集，A关于U的相对补集$U - A$，称为A的绝对补集，通常就称补集，记作$\sim A$。

与逻辑公式的合取、析取和否运算类似，集合的交、并、补运算满足幂等律、结合律、交换律、分配律、吸收律，德摩根律。

$A \cap A$	$=$	A	$A \cup A$	$=$	A
$A \cap (B \cap C)$	$=$	$(A \cap B) \cap C$	$A \cup (B \cup C)$	$=$	$(A \cup B) \cup C$
$A \cap B$	$=$	$B \cap A$	$A \cup B$	$=$	$B \cup A$
$A \cap (B \cup C)$	$=$	$A \cap B \cup A \cap C$	$A \cup (B \cap C)$	$=$	$A \cup B \cap A \cup C$
$A \cap (A \cup B)$	$=$	A	$A \cup (A \cap B)$	$=$	A
$\sim (A \cap B)$	$=$	$\sim A \cup \sim B$	$\sim (A \cup B)$	$=$	$\sim A \cap \sim B$

任给两个对象x, y，将它们按规定的顺序构成的序列，称为有序偶，记为$\langle x, y\rangle$。有序偶有第一个元与第二个元之分，$\langle x, y\rangle$的第一个元是x，第二个元是y。有序偶可用集合表示。$\langle x, y\rangle$的集合表示为$\{\{x\}, \{x, y\}\}$。$\langle x, y\rangle = \langle u, v\rangle$当且仅当$x = u$且$y = v$。

有序偶可以推广到n重序偶。n重序偶定义为$\langle x_1, ..., x_{n-1}, x_n\rangle = \langle\langle x_1, ..., x_{n-1}\rangle, x_n\rangle$。$\langle x_1, ..., x_{n-1}, x_n\rangle = \langle y_1, ..., y_{n-1}, y_n\rangle$ 当且仅当$x_1 = y_1$，...，$x_{n-1} = y_{n-1}$且$x_n = y_n$。

集合$A_1, ..., A_n$的笛卡尔乘积$A_1 \times \cdots \times A_n$定义为$A_1 \times \cdots \times A_n = \{\langle a_1, ..., a_n\rangle \mid a_1 \in A_1, ..., a_n \in A_n\}$。对于任意有穷集合$A_1, ..., A_n$，$|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$。设$A = A_1 \times \cdots \times A_n$。则第$i$分量函数$pr_i : A \to A_i$定义如下。$pr_i(\langle a_1, ..., a_n\rangle) = a_i$。

§1.4 关系

任何有序偶的集合称为二元关系。从X到Y的关系R满足$R \subseteq X \times Y$。若$\langle x, y\rangle \in R$，则表示成$xRy$，读作$x$与$y$有关系$R$。若$\langle x, y\rangle \notin R$，则表示成$x\bar{R}y$。一个二元关系可以用一个二元谓词确定。定义$R = \{\langle x, y\rangle \mid P(x, y)\}$，即$xRy$当且仅当$P(x, y)$成立。

设R是一个关系。R中所有有序偶的第一个元的集合称为R的定义域，记作$dom(R)$。R中所有有序偶的第二个元的集合称为R的值域，记作$ran(R)$。集合X到X的关系称为X上的二元关系。关系的性质由关系中包含的所有有序偶所确定。记$\forall x_1 \cdots \forall x_n(x_1 \in X \wedge \cdots \wedge x_n \in X \to \varphi)$为$\forall x_1, ..., x_n \in X.\varphi$。设$R$是非空集合$X$上的关系。

自反性	$\forall x \in X.(xRx)$
反自反性	$\forall x \in X.(x\bar{R}x)$
对称性	$\forall x, y \in X.(xRy \to yRx)$
反对称性	$\forall x, y \in X.(xRy \wedge yRx \to x = y)$
传递性	$\forall x, y, z \in X.(xRy \wedge yRz \to xRz)$

如果R和S是X到Y的二元关系，则$R \cap S$，$R \cup S$，$R - S$，$\sim S$ 都是X到Y的二元关系，且

$x(R \cap S)y$	$\Leftrightarrow$	$xRy \wedge xSy$
$x(R \cup S)y$	$\Leftrightarrow$	$xRy \vee xSy$
$x(R - S)y$	$\Leftrightarrow$	$xRy \wedge x\bar{S}y$
$x(\sim S)y$	$\Leftrightarrow$	$x\bar{S}y$

设R是X到Y的关系。R的逆关系是Y到X的关系，记作R^{-1}，定义为$R^{-1} = \{\langle y, x\rangle \in Y \times X \mid \langle x, y\rangle \in R\}$。

设R是X到Y的关系，S是Y到Z的关系。$R \circ S$是X到Z的关系，称为R和S的复合关系，定义为$R \circ S = \{\langle x, z\rangle \in X \times Z \mid \exists y \in Y.(xRy \wedge ySz)\}$。$\circ$称为关系的复合运算。在不引起混淆的情况下，

复合关系的运算符常省略不写。关系的复合运算满足结合律。设R是X到Y的关系，S是Y到Z的关系。则有$(R \circ S)^{-1} = S^{-1} \circ R^{-1}$。

设R是X上的二元关系，$n \in \mathbf{N}$。R的n次幂，记作R^n，定义如下。$R^0 = I_X = \{\langle x, x\rangle \mid x \in X\}$是集合$X$上的恒等关系；$R^{n+1} = R^n \circ R$。

设R是X上的二元关系，关系R'是R的自反（对称、传递）闭包当且仅当（1）R'是自反（对称、传递）的；（2）$R \subseteq R'$；（3）对于任何自反（对称、传递）关系R''，如果$R \subseteq R''$，则$R' \subseteq R''$。用$r(R), s(R), t(R)$分别表示R的自反闭包、对称闭包、传递闭包。我们有

$$\boxed{\begin{array}{rcl} r(R) & = & R \cup I_X \\ s(R) & = & R \cup R^{-1} \\ t(R) & = & \bigcup_{i=1}^{\infty} R^i \end{array}}$$

为书写方便，关系R的传递闭包通常记为R^+。R的自反传递闭包通常记为R^*。

满足自反性、对称性和传递性的一个非空集合上的关系称为等价关系。设R是集合X上的等价关系。对于任意$x \in X$，集合$[x]_R$定义如下：$[x]_R = \{y \in X \mid yRx\}$。称$[x]_R$为由$x$所代表的等价类。用$X/R$表示$R$等价类的集合$\{[x]_R \mid x \in X\}$，称$X/R$为$X$模$R$的商集。

设A是非空集合S子集的聚合。对于每个集合$B \in A$，$B \neq \emptyset$且$\bigcup A = S$。则称集合A是S的一个覆盖。若A是S的一个覆盖，且对任意$B, C \in A$，$B \neq C$则$B \cap C = \emptyset$，则称A是S的一个划分。

任何一个X上的等价关系R都定义了X的一个划分，即X/R。任何X的一个划分$A = \{A_1, ..., A_n\}$都定义了一个等价关系R，即xRy当且仅当x, y同在一个A_i中。

满足自反性和传递性的非空集合上的关系称为预序关系。如果$\leq$是X上的预序关系，那么有序偶$\langle P, \leq\rangle$表示预序集合。

给定预序集合$\langle P, \leq\rangle$和$Q \subseteq P$。如果所有P的不包含Q元素的非空子集都有极小元且若$a \leq b \leq a$且$a \neq b$则$a, b \in Q$，则称$\langle P, \leq\rangle$为Q弱基集合。一个预序集合是Q弱基集合当且仅当无限严格递减序列中非Q元素只出现有限多次。

设$\langle P, \leq\rangle$为Q弱基集合。记$x \leq y$且$x \neq y$为$x < y$。记$\Delta(Q)(x)$为以x为出发点的只包含Q元素的无限严格递减序列的集合。以下为弱基归纳推理。

$$\text{若}\forall x' \in P.(\forall x \in P.(x < x' \to (\Delta(Q)(x) = \emptyset \to \varphi(x))) \to \varphi(x'))\ \text{则}\forall x \in P.\varphi(x)。$$

给定预序集合$\langle P, \leq\rangle$。若$\langle P, \leq\rangle$是$\emptyset$弱基集合，则称$\langle P, \leq\rangle$为良基（Well-Founded）集合。

满足自反性、反对称性和传递性的一个非空集合上的关系称为偏序关系。如果$\leq$是X上的偏序关系，那么有序偶$\langle P, \leq\rangle$表示偏序集合。

若$\langle P, \leq\rangle$是良基集合，则$\langle P, \leq\rangle$是偏序集合。

设$\langle P, \leq\rangle$是偏序集合。如果对于每一个$x, y \in P$都有$x \leq y$或$y \leq x$，则称$\leq$上为P上的全序或线序，称$\langle P, \leq\rangle$ 为全序集合或链。

设$\langle P, \leq\rangle$是偏序集合，并且$A \subseteq P$。设$a \in A, b \in P$。

a为A的最大元：	$\forall x \in A.(x \leq a)$
a为A的最小元：	$\forall x \in A.(a \leq x)$
a为A的极大元：	$\forall x \in A.(a \neq x \rightarrow a \nleq x)$
a为A的极小元：	$\forall x \in A.(a \neq x \rightarrow x \nleq a)$
b为A的上界：	$\forall x \in A.(x \leq b)$
b为A的下界：	$\forall x \in A.(b \leq x)$
b为A的最小上界：	b是A的上界，且对于每一个A的上界b'，有$b \leq b'$
b为A的最大下界：	b是A的下界，且对于每一个A的下界b'，有$b' \leq b$

一个偏序集合的最大元，最小元，最小上界，最大下界，如果存在，则是唯一的。最小上界，也称上确界，记作$\sqcup$，lub或sup，最大下界，也称下确界，记作$\sqcap$，glb或inf。

一个偏序集合$\langle P, \leq \rangle$，如果它的每一个非空子集都有一个最小元，则称$\leq$为良序的，称$\langle P, \leq \rangle$为良序集合。每一个良序集合都是全序集合，但全序集合未必都是良序集合，而每一个有限的全序集合都是良序集合。

设$\langle P_1, \leq_1 \rangle, ..., \langle P_n, \leq_n \rangle$为偏序，$P = P_1 \times \cdots \times P_n$。则偏序$\langle P_1, \leq_1 \rangle, ..., \langle P_n, \leq_n \rangle$的笛卡尔积$\langle P, \leq \rangle$是一个偏序，其中$\leq$定义如下。对所有$a, b \in P$，$a \leq b$当且仅当对所有$i \in \{1, ..., n\}$，有$pr_i(a) \leq_i pr_i(b)$。设$S \subseteq P_1 \times \cdots \times P_n$。则$\sqcup S$存在当且仅当对于所有$i \in \{1, ..., n\}$，$\sqcup pr_i(S)$存在，且$\sqcup S = \langle \sqcup pr_1(S), ..., \sqcup pr_n(S) \rangle$。

§1.5 函数

设f是集合X到集合Y的关系。如果对每一个$x \in X$存在唯一的$y \in Y$使得$\langle x, y \rangle \in f$，则称$f$为$X$到$Y$的一个函数。记为$f : X \rightarrow Y$。$X$称为$f$的定义域，$Y$称为$f$的值域。

对于函数$f : X \rightarrow Y$，如果$\langle x, y \rangle \in f$，则称$x$为自变量，$y$是函数$f$在$x$处的值，也称$y$为在$f$作用下$x$的象，而称$x$为$y$的一个象源。通常用$y = f(x)$表示$\langle x, y \rangle \in f$。

设函数$f : X \rightarrow Y$且$A \subseteq X$，则$f \cap (A \times Y)$是从A到Y的函数，称为f受限制于A，记为$f|A$。集合$\{f(x) \mid x \in A\}$称为A在f下的象，记为$f(A)$。

若$X' \subseteq X$，且$f : X' \rightarrow Y$是X'到Y的函数，则称f为X到Y的偏函数。为区别于偏函数，函数又称全函数。

设$f : X \rightarrow Y$和$g : Y \rightarrow Z$是两个函数，则f和g的复合函数$g \circ f$是一个从X到Z的函数，且对于所有的$x \in X$，$(g \circ f)(x) = g(f(x))$。函数的复合满足结合律。

若$f : X \rightarrow X$是一个函数，则f能够对自身复合任意多次。f对自身复合任意多次的定义如下。$f^0(x) = I_X(x)$；$f^{n+1}(x) = f(f^n(x))$。

记$\exists x_1 \cdots \exists x_n(x_1 \in X \wedge \cdots \wedge x_n \in X \wedge \varphi)$为$\exists x_1, ..., x_n \in X.\varphi$。设$f : X \rightarrow Y$是一个函数。

f是满射的	$\forall y \in Y.\exists x \in X.(f(x) = y)$
f是入射的	$\forall x_1, x_2 \in X.(f(x_1) = f(x_2) \rightarrow x_1 = x_2)$
f是双射的	f是满射的且是入射的

若$f : X \rightarrow Y, g : Y \rightarrow Z$都是满射函数，则$g \circ f$也是满射函数；若$f : X \rightarrow Y, g : Y \rightarrow Z$都是入射函数，则$g \circ f$也是入射函数；若$f : X \rightarrow Y, g : Y \rightarrow Z$都是双射函数，则$g \circ f$也是双射函数。

设f是双射的。它的反函数是f的逆关系，记作f^{-1}。若$f : X \to Y$是双射的，则其反函数$f^{-1} : Y \to X$也是双射的。若$f : X \to Y, g : Y \to Z$都是双射函数，则$(g \circ f)^{-1}$也是双射函数，且$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$。

设U是全集，$A \subseteq U$。A的特征函数$\Psi_A : U \to \{0, 1\}$定义如下。

$$\Psi_A(x) = \begin{cases} 1 & if \quad x \in A \\ 0 & if \quad x \notin A \end{cases}$$

设U是全集，$A, B \subseteq U$。则对所有$x \in U$，以下等式成立。

$$\boxed{\begin{array}{lcl} \Psi_{A\cap B}(x) & = & \Psi_A(x) \cdot \Psi_B(x) \\ \Psi_{A\cup B}(x) & = & \Psi_A(x) + \Psi_B(x) - \Psi_{A\cap B}(x) \\ \Psi_{\sim A}(x) & = & 1 - \Psi_A(x) \end{array}}$$

X到Y的所有全函数的集合记作$(X \to Y)$。设X是一个集合，$\langle Y, \leq\rangle$是一个偏序，$f, g : X \to Y$是两个函数。$f \leq g$当且仅当对于所有$x \in X$，$f(x) \leq g(x)$。$\langle (X \to Y), \leq\rangle$构成一个偏序。

设$S \subseteq (X \to Y)$是一个X到Y的函数的集合。设$x \in X$。Y的子集$\{f(x) \mid f \in S\}$记作$S(x)$。$\sqcup S$存在当且仅当对于所有$x \in X$，$\sqcup S(x)$存在，且对于所有$x \in X$，$(\sqcup S)(x) = \sqcup S(x)$。

设X是一个集合。记X的大小为n的子集的集合为$[X]^n$。一个$[X]^n$的k染色函数C是一个$[X]^n$到一个大小为k的集合的函数。称H为C的齐性集合当且仅当C作用在任意$[H]^n$中的元素所得的值是一样的。以下结论称为Ramsey定理。

设N是自然数集合。任意$[N]^n$的k染色函数都有一个无穷的齐性集合。

§1.6 完全偏序和格上的不动点

一个偏序$\langle X, \leq\rangle$，如果它X有最小元，且对于X上的每一条链$S \subseteq X$，$\sqcup S$都存在，则称$\langle X, \leq\rangle$为全偏序。X的最小元通常记作$\perp_X$或$\perp$。

任何有最小元且只包含有穷链的偏序是完全偏序。如果$\langle P_1, \leq_1\rangle, ..., \langle P_n, \leq_n\rangle$是完全偏序，则其笛卡尔积$\langle P_1 \times \cdots \times P_n, \leq\rangle$是完全偏序。如果$X$是一个集合，$\langle Y, \leq\rangle$是一个完全偏序，则$\langle (X \to Y), \leq\rangle$是完全偏序。

设$\langle X, \leq\rangle$是一个完全偏序，$Y \subseteq X$。$\langle Y, \leq\rangle$是$\langle X, \leq\rangle$的子完全偏序，当且仅当$\langle Y, \leq\rangle$是一个完全偏序，且对于Y上的每一条链S，都有$\sqcup_Y S = \sqcup_X S$。

设$\langle X, \leq_1\rangle$和$\langle Y, \leq_2\rangle$是偏序，$f : X \to Y$是函数。f是单调的当且仅当$\forall x_1, x_2 \in X.(x_1 \leq_1 x_2 \to f(x_1) \leq_2 f(x_2))$。

设$\langle X, \leq_1\rangle$是偏序，$\langle Y, \leq_2\rangle$是完全偏序。从X到Y的单调函数的集合构成$\langle (X \to Y), \leq_2\rangle$的一个子完全偏序。

设$\langle X, \leq_1\rangle$和$\langle Y, \leq_2\rangle$是完全偏序，$f : X \to Y$是函数。f是连续的(Scott-Continous)当且仅当对X的每一条链$S \subseteq X$，$\sqcup f(S)$都存在，且$\sqcup f(S) = f(\sqcup S)$。连续函数的集合记作$[X \to Y]$。

设$\langle X, \leq_1\rangle$和$\langle Y, \leq_2\rangle$是完全偏序。从X到Y的连续函数的集合$[X \to Y]$构成$\langle (X \to Y), \leq\rangle$的一个子完全偏序。

设$\langle X, \leq_1\rangle$和$\langle Y, \leq_2\rangle$是完全偏序，$f : X \to Y$是函数。f是连续的当且仅当f是单调的且对X的每一条链$S \subseteq X$，$f(\sqcup S) \leq \sqcup f(S)$。

设$\langle X, \leq \rangle$是偏序，$f : X \to X$是函数。若$f(x) = x$，则称x是f的不动点。若x是f的不动点，且对任意f的不动点y，都有$x \leq y$，则称x是f的最小不动点。f的最小不动点记作μf。若x是f的不动点，且对任意f的不动点y，都有$y \leq x$，则称x是f的最大不动点。f的最大不动点记作νf。

为了能够清楚地说明f的受不动点标记约束的自变量是x，μf有时写成$\mu x.f$，νf写成$\nu x.f$。

设$\langle X, \leq \rangle$是完全偏序，$f : X \to X$是连续函数。则f有最小不动点，且可表示如下(Kleene不动点定理)。

$$\mu f = \sqcup \{ f^i(\perp) \mid i \in \mathbf{N} \}$$

设$\langle X, \leq \rangle$是完全偏序，$f : X \to X$是连续函数，$x \in X$。若$f(x) \leq x$，则$\mu f \leq x$。

设$\langle X, \leq \rangle$是完全偏序，$\varphi : X \to \{0, 1\}$是一个谓词。φ是相容的当且仅当对X的每一条链S，若$\bigwedge_{x \in S} \varphi(x)$为真，则$\varphi(\sqcup S)$为真。

设$\langle X, \leq \rangle$是完全偏序，$\varphi : X \to \{0, 1\}$是一个相容谓词。以下为不动点归纳推理(Scott Induction)。

$$\text{若}\varphi(\perp)\text{且}\forall x \in X.(\varphi(x) \to \varphi(f(x)))\text{，则}\varphi(\mu f)\text{。}$$

一个偏序$\langle X, \leq \rangle$，如果X中的任意两个元素都有最小上界和最大下界，则称$\langle X, \leq \rangle$为格。

一个偏序$\langle X, \leq \rangle$，如果X中的任意子集都有最小上界，则称$\langle X, \leq \rangle$为完全格。对称地，一个偏序$\langle X, \leq \rangle$是完全格当且仅当其任意子集都有最大下界。

设$\langle X, \leq \rangle$是完全格，$f : X \to X$是单调函数。则f有非空的不动点集，且该集构成一个完全格，f有最小和最大不动点，且可表示如下(Knaster-Tarski不动点定理)。

$$\mu f = \sqcap \{ x \in X \mid f(x) \leq x \}$$
$$\nu f = \sqcup \{ x \in X \mid x \leq f(x) \}$$

§1.7 有向图

有向图D是一有序偶$\langle V, E \rangle$，其中V是一非空集合，E是V上的一个二元关系。分别称V和E为有向图D的顶点的集合和边的集合。为表示的直观性，边的集合E有时写成$\to$。关系$\to$的传递闭包和传递自反闭包分别记做$\xrightarrow{+}$和$\xrightarrow{*}$。

设有两个图$D = \langle V, E \rangle$和$D' = \langle V', E' \rangle$。若$V \subseteq V'$且$E \subset E'$，则称$D$为$D'$的子图，并表示为$D \subseteq D'$。若$V \subseteq V'$且$E = \{ \langle u, v \rangle \in E' \mid u, v \in V \}$，则称$D$为$D'$的导出子图。

在有向图$D = \langle V, E \rangle$中，把边的一个序列$(e_1, ..., e_n)$称为一条通路，其中$e_i = \langle v_i, v_{i+1} \rangle \in E$（$i = 1, ..., n$）。通路$(e_1, ..., e_n)$的长度为出现在通路中的边的次数，记作$|(e_1, ..., e_n)|$。通路$(e_1, ..., e_n)$通常也用顶点序列$(v_1, ..., v_{n+1})$表示。

对于有向图的一条通路，如果每条边的出现不超过一次，则称该通路为简单通路。如果每个顶点的出现不超过一次，则称该通路为基本通路。基本通路一定是简单通路。通过有向图中所有顶点的通路称为完备通路。

如果一条通路的开始和终结于同一顶点，则称该通路为回路。如果回路的长度为2，则称该回路为回路起点的顶点的自环。如果回路中每条边的出现不超过一次，则称该回路为简单回路。如果回路除去最后一个点的通路中每个顶点的出现不超过一次，则称该回路为基本回

路。通过有向图中所有顶点的回路称为完备回路。如果一条通路的终点与通路上的某个其它位置的顶点相同，则称该通路为套索。

如果存在从顶点u到顶点v的通路，则称顶点u可以到达顶点v，即u, v满足$u \xrightarrow{+} v$。如果存在从顶点u到顶点v的通路，则存在从顶点u到顶点v的基本通路。在一个有n个顶点的有向图中，任何基本通路的长度都不超过$n-1$，任何基本回路的长度都不超过n。

一个有向图$D = \langle V, E\rangle$，如果对它的每一对顶点u和v，可以从u到达v并且可以从v到达u，则称D为强连通图。有向图D是强连通的当且仅当D有完备回路。称强连通图为非平凡的，当且仅当该图至少有两个顶点或有一个有自环的顶点。

在有向图D中，$A \subseteq D$是D的一个极大强连通导出子图，当且仅当A是D的导出子图，A是强连通的，且对于任意的D的强连通的子图$B \subseteq D$，若$A \neq B$则$A \nsubseteq B$。在有向图D中，D的一个极大强连通导出子图，称为D的一个强连通分图。

设$D = \langle V, E\rangle$为有向图。设$A \subseteq V$。从集合A一步可达的顶点的集合为$\{b \mid a \rightarrow b, a \in A\}$，记为$E(A)$。从集合$A$可达的顶点的集合（包括$A$）为$\bigcup_{i\geq 0} E^i(A) = \{b \mid a \xrightarrow{*} b, a \in A\}$，记为$E^*(A)$。一步可达$A$的顶点的集合为$\bigcup_{i\geq 0}(E^{-1})^i(A) = \{b \mid b \rightarrow a, a \in A\}$，记为$E^{-1}(A)$。可达$A$的顶点的集合为$\{b \mid b \xrightarrow{*} a, a \in A\}$，记为$(E^{-1})^*(A)$。若$D$是强连通图且$A \subseteq V$非空，则$E^*(A) = (E^{-1})^*(A) = V$。

§1.8 练习

1. 设$N = \{0, 1, 2, ..., \}$为自然数集，$X = N \cup \{\omega, \omega'\}$为自然数集加两个无穷大量。$X$中元素的大小满足通常对整数大小和对无穷大量的理解且定义两个无穷大量满足$\omega < \omega'$。设$f_0, f_1 : X \rightarrow X$定义如下：$f_0(\omega) = \omega$，$f_0(\omega') = \omega'$且若$a \in N$则$f_0(a) = a + 1$；$f_1(\omega) = \omega'$，$f_1(\omega') = \omega'$且若$a \in N$则$f_1(a) = a + 1$。$f_0$和$f_1$是单调的。证明：$f_0$是连续的，$f_1$不是连续的。

2. 设$\langle X, \leq_1\rangle$和$\langle Y, \leq_2\rangle$是完全偏序。$f : X \rightarrow Y$是函数。证明：如果X只包含有穷链，则f是连续的当且仅当f是单调的。

3. 设$D = \langle V, E\rangle$为有向图。设$A \subseteq V$。将$A \cup E(Z)$和$A \cup E^{-1}(Z)$ 看成是自变量为Z的$(2^V \rightarrow 2^V)$中的函数，证明这两个函数在偏序$(2^V, \subseteq)$中是单调递增的，$E^*(A) = \mu Z.(A \cup E(Z))$且$(E^{-1})^*(A) = \mu Z.(A \cup E^{-1}(Z))$。

4. 设$D = \langle V, E\rangle$为有向图。证明：$E^{-1}(E(V)) = V$当且仅当E是完全关系，即任意顶点有后继。

§2　基于状态变迁的迁移系统

本章介绍以抽象状态的迁移为特点的模型。模型的基本要素为抽象状态和状态迁移关系以及初始状态。本章的算法仅限于有穷状态系统，而推理方法则不限于有穷状态系统。

基本符号：　设S是个集合。

S的幂集记作2^S。

无穷序列$s_0s_1s_2$......记作$[s_i]_{i\geq 0}$。

有穷序列$s_0s_1s_2...s_n$记作$[s_i]_{i=0}^n$。

S^ω表示S上的无穷序列的集合，即$S^\omega = \{[s_i]_{i\geq 0} \mid \forall i \geq 0, s_i \in S\}$。

依上下文关系，S^n可表示S上的n元组的集合$\{(s_1,...,s_n) \mid s_1,...,s_n \in S\}$或长度为$n$的有穷序列的集合$\{[s_i]_{i=0}^{n-1} \mid s_0,...,s_{n-1} \in S\}$。

若$\rightarrow\ \subseteq S \times S$为$S$上的二元关系，则$\stackrel{*}{\rightarrow}$表示$\rightarrow$的传递自反闭包。

集合的运算包括交、并、差，记作$\cap, \cup, \setminus$，为方便起见，有时写作$*, +, -$。

设S为全集。集合A的补为全集与A的差$S \setminus A$，亦记作$\neg A$。

若$Y \subseteq S \times S$且$X \subseteq S$，用$Y|X$表示$Y \cap (X \times X)$。

若$G = (V, E)$是有向图，依上下文关系，为方便起见，V的子集B亦可表示顶点集合为B的导出子图$(B, E|B)$。

用$e_1,...,e_k$分别替换φ中的$x_1,...,x_k$记作$\varphi(e_1/x_1,...,e_k/x_k)$，亦写作$\varphi_{x_1,...,x_k}^{e_1,...,e_k}$。

§2.1　Kripke模型

定义 2.1　*一个Kripke模型是一个三元组$\langle S, R, I\rangle$ 其中S为状态集合，$R \subseteq S \times S$为S上的完全迁移关系，$I \subseteq S$为初始状态集。*

$R \subseteq S \times S$是完全的，即$\forall s.\exists s'.(s, s') \in R$。

我们也称Kripke模型为系统。

用$s \rightarrow s'$ 表示存在从s到s'的迁移，即$(s, s') \in R$。

假定$K = \langle S, R, I\rangle$为给定模型。

后继状态：　若$s \rightarrow s'$，则称s'为s的后继状态。状态s的后继状态的集合为$\{s' \mid s \rightarrow s'\}$，记作$R(s)$。状态集合$A$的后继状态集合为$\bigcup_{s\in A} R(s)$，记作$R(A)$。

前驱状态：　若$s \rightarrow s'$，则称s为s'的前驱状态。状态s的前驱状态的集合为$\{s' \mid s' \rightarrow s\}$，记作$R^{-1}(s)$。状态集合$A$的前驱状态集合为$\bigcup_{s\in A} R^{-1}(s)$，记作$R^{-1}(A)$。

可达状态：　若$s \stackrel{*}{\rightarrow} s'$，则称$s'$为$s$的可达状态。状态$s$的可达状态的集合为$\{s' \mid s \stackrel{*}{\rightarrow} s'\}$，记作$R^*(s)$。状态集合$A$的可达状态集合为$\bigcup_{s\in A} R^*(s)$，记作$R^*(A)$。$K$的可达状态集合为$R^*(I)$，亦记作$Rh(K)$。

可达关系：　若B中有s的可达状态，则称B由s可达。若B中有A的可达状态，则称B由A可达，记作$A \stackrel{*}{\rightarrow} B$。

路径： K的有穷路径是S上的满足对任意$0 \le i \le n-1$都有$s_i \rightarrow s_{i+1}$的有穷序列$[s_i]_{i=0}^{n}$。K的无穷路径是S上的满足对任意$i \ge 0$都有$s_i \rightarrow s_{i+1}$的无穷序列$[s_i]_{i \ge 0}$。

计算与行为： K的计算序列(简称为计算)是K上的满足$s_0 \in I$的无穷路径$[s_i]_{i \ge 0}$。K的计算的集合称为K的行为，记作$[[K]]$。

状态的满足关系： 称状态s满足A，当且仅当$s \in A$。因而集合A中的状态都满足A，且满足A的状态都在A中。称集合B满足A，当且仅当B中的所有状态都满足A，即$B \subseteq A$。为方便叙述，满足A的状态称为A状态。若一条路径(或一个计算)上的所有状态都满足A，则称该路径(计算)为A路径(计算)。若一条路径(或一个计算)上有满足A的状态，则称该路径(计算)能到达A状态。

§2.1.1 可达性质分析

定义 2.2 (可达性质) 状态集合$A \subseteq S$称为K的可达性质，当且仅当$[[K]]$中有能到达A状态的计算。

命题 2.1 状态集合$A \subseteq S$是K的可达性质当且仅当$Rh(K) \cap A \neq \emptyset$。

给定Kripke模型$K = \langle S, R, I \rangle$和集合$A \subseteq S$。$A$是否是$K$的可达性质可通过对模型可达状态的检查来验证。

可达性质分析1： 首先介绍基于状态遍历的可达性质分析算法。为方便算法设计，我们定义集合类型结构的操作。我们记空集为{}。设w为集合。用$w.put(s)$，$w.get()$，$w.remove(s)$ 分别代表在集合w中添加元素s，从集合中读取元素，从集合中移除元素s。给定Kripke模型$K = \langle S, R, I \rangle$和集合$A \subseteq S$。设每个状态$s$有$s.visited$这个属性，其初始值为$false$。算法1是基于状态遍历的分析$A$是否为可达性质的算法。

Algorithm 1 ReachabilityAnalysis

Input: K, A;

Output: $true/false$;

$w := I$;
while $(w \neq \emptyset)$ **do**
    $s := w.get()$; if $(s \in A)$ return $true$;
    $s.visited := true$;
    for each $(s' \in R(s))$, if $(s'.visited = false)$ $w.put(s')$;
    $w.remove(s)$;
end while
return $false$;

命题 2.2 状态集合$A \subseteq S$是K的可达性质当且仅当$ReachabilityAnalysis(K, A)$为$true$。

可达性质分析2： 以下是基于不动点计算的可达性质分析。首先介绍有穷集合完全格上的单调函数的不动点算法如下。

最小和最大不动点的计算： 设X为有穷集合，$(X, \sqsubseteq)$ 为完全格，f为X上的单调函数。记最小元为$\perp$，最大元为$\top$。算法2计算f的以元素A为初始值的不动点。若A为$\perp$时，计算得到的为f的最小不动点，若A为$\top$时，计算得到的为f的最大不动点，即我们有f的最小不动点$\mu f = FNfp(f, \perp)$和f的最大不动点$\nu f = FNfp(f, \top)$。

Algorithm 2 FNfp

Input: 函数f和元素A;

Output: 函数f以A为初始值的不动点;

```
X := A; Y := f(A);
while X ≠ Y do
    X := Y; Y := f(X);
end while
return X;
```

基于最小不动点计算的可达性质分析的算法： 给定Kripke模型$K = \langle S, R, I\rangle$和集合$A \subseteq S$。设$S$为有穷状态集合。则$(2^S, \subseteq)$ 为完全偏序且空集为偏序的最小元。定义$f_K : 2^S \rightarrow 2^S$如下：$f_K(A) = I \cup R(A)$。则$f_K$为$(2^S, \subseteq)$上的单调函数且以下命题成立。

命题 2.3 $Rh(K) = \mu f_K$.

由命题2.3和命题2.1，知算法3是基于不动点计算的分析A是否为可达性质的算法。

Algorithm 3 ReachabilityAnalysisFP

Input: K, A;

Output: $true/false$;

```
w := FNfp(f_K, ∅);
return w ∩ A ≠ ∅;
```

命题 2.4 状态集合$A \subseteq S$是K的可达性质当且仅当$ReachabilityAnalysisFP(K, A)$为$true$。

§2.1.2 安全性质分析

定义 2.3 (安全性质) 状态集合$A \subseteq S$称为K的安全性质，当且仅当K的所有计算都是A计算。

命题 2.5 状态集合$A \subseteq S$是K的安全性质当且仅当$Rh(K) \subseteq A$。

推论 2.1 状态集合$A \subseteq S$是K的安全性质，当且仅当状态集合$\neg A$不是K的可达性质。

安全性质分析算法： 根据推论2.1知安全性质与可达性质是对偶性质。我们可以对可达性质分析算法做简单修改以分析安全性质。

安全性质分析算法1： 算法4是基于状态遍历的分析A是否为安全性质的算法。

命题 2.6 状态集合$A \subseteq S$是K的安全性质当且仅当$SafetyAnalysis(K, A)$为$true$。

Algorithm 4 SafetyAnalysis

Input: K, A;

Output: $true/false$;

```
w := I;
while (w ≠ ∅) do
    s := w.get(); if (s ∉ A) return false;
    s.visited := true;
    for each (s′ ∈ R(s)), if (s′.visited = false) w.put(s′);
    w.remove(s);
end while
return true;
```

Algorithm 5 SafetyAnalysisFP

Input: K, A;

Output: $true/false$;

```
w := FNfp(f_K, ∅);
return w ∩ ¬A = ∅;
```

安全性质分析算法2： 算法5是基于最小不动点计算的分析A是否为安全性质的算法。

命题 2.7 状态集合$A \subseteq S$是K的安全性质当且仅当$SafetyAnalysisFP(K, A)$为$true$。

由于安全性质与可达性质是对偶性质，我们有以下结论。

推论 2.2 $SafetyAnalysis(K, A)$为$true$当且仅当$ReachabilityAnalysis(K, \neg A)$为$false$。

安全性质的推理： 若$R(A) \subseteq A$，则称A为迁移不变。关于安全性质，我们有如下推理规则。设A', A为状态集合。

$$\frac{\begin{array}{l} I\text{满足}A' \\ A'\text{迁移不变} \\ A'\text{满足}A \end{array}}{A\text{是安全性质}}$$

可靠性与完备性： 以上推理规则是可靠的且完备的。假定前提成立，由前两条我们知道$R^*(I) \subseteq A'$，又由第三条我们知道$R^*(I) \subseteq A$，所以A 是安全性质，因而推理规则是可靠的。假定A是安全的，取$A' = R^*(I)$，我们就可保证前提条件的成立，由此可证A是安全性质，因而推理规则是完备的。

§2.1.3 可避免性质分析

定义 2.4 (可避免性质) 状态集合$A \subseteq S$称为K的可避免性质，当且仅当$[[K]]$中有$\neg A$ 计算。

命题 2.8 状态集合$A \subseteq S$是K的可避免性质当且仅当$\exists B \subseteq S.((B \cap I \neq \emptyset) \wedge (\forall s \in B.(\exists s' \in B.(s \rightarrow s'))) \wedge (B \cap A = \emptyset))$。

可避免性质分析1： 给定Kripke模型$K = \langle S, R, I\rangle$和集合$A \subseteq S$。$A$是否是$K$的可避免性质可通过对模型的强连通图的分析来验证，即考察模型是否可由$\neg A$有穷路径到达由$\neg A$状态组成的非平凡强连通图。

强连通分图的计算： 为方便算法设计，我们定义栈类型结构的操作。对于栈类型的变量，我们记空栈为[]。设w为栈。用$w.push(s)$，$w.top()$，$w.pop()$ 分别代表在栈w的栈顶添加元素s，从栈中读取栈顶元素，从栈中移除栈顶元素。给定一个有向图$G = (V, E)$。设每个顶点v有$v.index$和$v.lowlink$两个属性，其初始值为$undefined$。算法6是计算强连通分图的Tarjan算法。算法返回值$FNscc(G)$是G的强连通分图顶点集合的集合。

Algorithm 6 FNscc

Input: $G = (V, E)$;
Output: G的强连通分图顶点集合的集合;

$index := 0$; $S := []$; $scclist := \{\}$;
for each $v \in V$, if ($v.index = undefined$) strongconnect(v);
return $scclist$;
FUNCTION strongconnect(v)
$v.index := v.lowlink := index$; $index := index + 1$; $S.push(v)$;
for each $w \in E(v)$ **do**
  if ($w.index = undefined$) **then**
    $strongconnect(w)$; $v.lowlink := min(v.lowlink, w.lowlink)$;
  else if ($w \in S$)
    $v.lowlink := min(v.lowlink, w.index)$;
  end if
end for
if ($v.lowlink = v.index$) **then**
  $currentSCC := \{\}$;
  while $true$ **do**
    $w := S.top()$; $S.pop()$; $currentSCC.put(w)$; if ($w = v$) break;
  end while
  $scclist.put(currentSCC)$;
end if

可避免性质分析算法1： 假定$nontrivial(G, e)$为检查G的强连通分量e是否非平凡的函数。给定$K = \langle S, R, I\rangle$和集合$A \subseteq S$。定义$K|X = \langle S \cap X, R|X, I \cap X\rangle$。$A$是可避免性质当且仅当在$K|\neg A$中存在一条由初始状态出发的无穷路径。算法7是基于强连通分量计算的分析A是否为可避免性质的算法。

命题 2.9 状态集合$A \subseteq S$是K的可避免性质当且仅当$AvoidabilityAnalysis(K, A)$为$true$。

可避免性质分析2： 以下是基于不动点计算的可避免性质分析。给定有向图$G = (S, R)$且$A \subseteq S$。设S的为有穷集合。则$(2^S, \subseteq)$ 为完全偏序且S为偏序的最大元。定义$f_G : 2^S \to 2^S$ 如下：$f_G(A) =$

Algorithm 7 AvoidabilityAnalysis

Input: K, A;

Output: $true/false$;

$K' := (S', R', I') := K|\neg A$; $G := (S', R')$;

$scclist := FNscc(G)$;

$w := \emptyset$; for (each e in $scclist$) if ($nontrivial(G, e)$) $w := (w \cup e)$;

return $ReachbilityAnalysis(K', w)$;

$R^{-1}(A)$。则f_G为$(2^S, \subseteq)$上的单调函数且以下命题成立。

命题 2.10 νf为G中所有无穷路径起点状态组成的集合。

可避免性质分析算法2： 由命题2.10知算法8是基于最大不动点计算的分析A是否为可避免性质的算法。

Algorithm 8 AvoidabilityAnalysisFP

Input: K, A;

Output: $true/false$;

$G := (\neg A, R|\neg A)$;

$w := FNfp(f_G, \neg A)$;

return $w \cap I \neq \emptyset$;

命题 2.11 状态集合$A \subseteq S$是K的可避免性质当且仅当$AvoidabilityAnalysisFP(K, A)$为$true$。

§2.1.4 必达性质分析

定义 2.5 (必达性质) 状态集合$A \subseteq S$称为K的必达性质，当且仅当K的所有计算都能到达A 状态。

命题 2.12 状态集合$A \subseteq S$是K的必达性质当且仅当$\forall B \subseteq S.((B \cap I \neq \emptyset) \wedge (\forall s \in B.(\exists s' \in B.(s \rightarrow s'))) \rightarrow (B \cap A \neq \emptyset))$。

推论 2.3 状态集合$A \subseteq S$是K的必达性质，当且仅当状态集合A不是K的可避免性质。

必达性质分析算法： 根据推论2.3知必达性质与可避免性质是相反的关系。我们可以对可避免性质分析算法做简单修改以分析必达性质。给定$K = \langle S, R, I\rangle$和集合$A \subseteq S$。算法9是基于强连通分量计算的分析$A$是否为必达性质的算法。

命题 2.13 状态集合$A \subseteq S$是K的必达性质当且仅当$InevitabilityAnalysis(K, A)$为$true$。

推论 2.4 $InevitabilityAnalysis(K, A)$为$true$当且仅当$AvoidabilityAnalysis(K, A)$为$false$。

Algorithm 9 InevitabilityAnalysis

Input: K, A;

Output: $true/false$;

$K' := (S', R', I') := K|\neg A$; $G := (S', R')$;

$scclist := FNscc(G)$;

$w := \emptyset$; for (each e in $scclist$) if ($nontrivial(G, e)$) $w := (w \cup e)$;

return not $ReachbilityAnalysis(K', w)$;

必达性质的推理： 我们有如下推理规则。设$X_0, X_1, ..., X_n, A$为状态集合。

$$\frac{\begin{array}{l} I\text{满足}X_0 \\ \forall i \in \{0, ..., n-1\}\text{，}R(X_i \setminus A)\text{满足}X_{i+1} \\ X_n\text{满足}A \end{array}}{A\text{是必达性质}}$$

可靠性与完备性： 以上推理规则是可靠的且对于有穷状态系统是完备的。假定前提成立且结论不成立，那么由结论不成立，我们有一条由I状态出发的无穷$\neg A$路径，这条路径必然有状态出现在任一X_i中，与X_n满足A矛盾，所以前提成立则结论成立，因而推理规则是可靠的。假定A是必达性质，由于只考虑有穷状态系统，我们可以假定状态个数为n，那么取$X_0 = I$和$X_{i+1} = R(X_i \setminus A)$，则$X_n$为空(否则存在一条无限循环的$\neg A$ 路径)，由此可证A 是必达性质，因而推理规则是完备的。

§2.2 公平Kripke模型

对于Kripke模型而言，一个计算是以一个初始状态为起点的满足状态迁移关系的无穷状态序列。为了更精确地描述模型的计算，我们对计算做一定限制以排除部分满足状态转换关系的无穷状态序列。需要排除的部分称为不公平的无穷状态序列。为达到这个效果，我们在结构中加入新的成分，设置公平计算的条件。

定义 2.6 一个公平$Kripke$模型是一个四元组$\langle S, R, I, F\rangle$ 其中$\langle S, R, I\rangle$是一个$Kripke$模型，$F \subseteq 2^S$ 为公平性约束的有穷集合。

假定$K = \langle S, R, I, F\rangle$为给定模型。

可达状态： 标号Kripke模型K的可达状态即$K' = \langle S, R, I\rangle$的可达状态。

公平路径： 公平Kripke模型K上的路径即Kripke模型$\langle S, R, I\rangle$上的路径。定义$inf(\pi)$为无限多次出现在路径π中的状态的集合。路径$\pi = [s_i]_{i\geq 0}$ 是公平的，当且仅当对所有$f \in F$，

$$inf(\pi) \cap f \neq \emptyset$$

计算与行为： 公平Kripke模型K上的计算即Kripke模型$\langle S, R, I\rangle$上的计算。一个计算是公平的，当且仅当该计算是一条公平路径。K的公平计算的集合称为K的行为，记作$[[K]]$。

公平状态： 一个状态是公平的，当且仅当存在从该状态出发的公平路径。

公平状态集合： 记$\{s \mid s \to s', s' \in X\}$为$R^{-1}(X)$。

定义$S_F = \nu Z. \bigwedge_{f\in F} \mu Y.((f \cap R^{-1}(Z)) \cup R^{-1}(Y))$。

将$((X \cap R^{-1}(Z)) \cup R^{-1}(Y))$ 看成是自变量为Y的从2^S到2^S函数，我们知道这个函数在完备格$(2^S, \subseteq)$上是单调递增的，有最小不动点，因而$\bigwedge_{f\in F} \mu Y.((f \cap R^{-1}(Z)) \cup R^{-1}(Y))$是良定义。将$\bigwedge_{f\in F} \mu Y.((f \cap R^{-1}(Z)) \cup R^{-1}(Y))$ 看成是自变量为Z的函数，我们知道这个函数是单调递增的，有最大不动点，因而S_F是良定义。

命题 2.14 状态$s \in S$是K的公平状态，当且仅当$s \in S_F$。

可达公平状态集合： 记由A可达的公平状态集合为$Rh_F(A)$。

命题 2.15 $Rh_F(A) = Rh(A) \cap S_F$。

K的可达公平状态集合，记为$Rh_F(A)$，即由I可达的公平状态集合$Rh_F(I)$。

推论 2.5 $Rh_F(K) = Rh(I) \cap S_F$。

公平强连通分量： 考虑穷状态系统。给定$K = \langle S, R, I, F\rangle$。有向图$(S, R)$的强连通分量也称为$K$的强连通分量。$K$的强连通分量$e$是公平的，当且仅当$e$是非平凡的且$\forall f \in F.(e \cap f \neq \emptyset)$，其中$e \cap f$表示$f$中的元素和强连通分量$e$中的元素的交集。算法10是检查$e$是否为公平强连通分量的算法。

Algorithm 10 Fairscc

Input: K, e;

Output: $true/false$;

1: if ($nontrivial(K, e) = false$) return false;
2: for (each f in F) if ($e \cap f = \emptyset$) return false; ;
3: return true;

命题 2.16 K的强连通分量e是公平的，当且仅当$Fairscc(K, e)$为$true$。

公平状态判定： 在公平强连通分量检查算法的基础上，可以设计检查一个状态是否为公平状态和一个状态集中是否有公平状态的算法。算法11是检查A中是否是否有公平状态的算法。

命题 2.17 状态集$A \subseteq S$中有公平状态，当且仅当$ExistFairState(K, A)$为$true$。

推论 2.6 状态$s \in S$是K的公平状态，当且仅当$ExistFairState(K, \{s\})$为$true$。

Algorithm 11 ExistFairState

Input: K, A;

Output: $true/false$;

$G := (S, R)$; $scclist := FNscc(G)$;

$w := \emptyset$; for (each e in $scclist$) if ($fairscc(K, e)$) $w := w \cup e$;

$K' := (S, R, A)$;

return $ReachbilityAnalysis(K', w)$;

§2.2.1 公平可达性质分析

定义 2.7 (公平可达性质) 状态集合$A \subseteq S$称为K的公平可达性质，当且仅当$[[K]]$中有能到达A状态的公平计算。

命题 2.18 状态集合$A \subseteq S$是K的公平可达性质当且仅当$Rh_F(K) \cap A \neq \emptyset$。

推论 2.7 状态集合$A \subseteq S$是K的公平可达性质当且仅当$Rh(K) \cap A$中存在公平状态。

可达性分析1： 给定公平Kripke模型$K = \langle S, R, I, F \rangle$和集合$A \subseteq S$。$A$是否是$K$的公平可达性质的分析可通过首先看哪些$A$状态是公平状态，再结合可达性分析算法看这些公平状态中是否有由模型初始状态可达的。算法12是根据原来的可达性分析算法修改的公平可达性分析算法。

Algorithm 12 FairReachabilityAnalysis

Input: K, A;

Output: $true/false$;

$w := I$;

while ($w \neq \emptyset$) **do**

  $s := w.get()$; if ($s \in A$) and (ExistFairState(K,{s})=true) return $true$;

  $s.visited := true$;

  for each ($s' \in R(s)$), if ($s'.visited = false$) $w.put(s')$;

  $w.remove(s)$;

end while

return $false$;

命题 2.19 状态集合$A \subseteq S$是K的公平可达性质当且仅当$FairReachabilityAnalysisII(K, A)$为$true$。

可达性分析2： 由于$FairReachabilityAnalysis()$算法每次碰到一个$A$状态都要调用一次$ExistFairState()$，我们可以考虑收集这些可达的$A$状态，然后一次性地看其中是否有公平状态。算法13是根据这个结论和原来的可达性分析算法修改的公平可达性分析算法。

命题 2.20 状态集合$A \subseteq S$是K的公平可达性质当且仅当$FairReachabilityAnalysisII(K, A)$为$true$。

Algorithm 13 FairReachabilityAnalysisII

Input: K, A;

Output: $true/false$;

```
w := I; u := ∅;
while (w ≠ ∅) do
    s := w.get(); if (s ∈ A) u.put(s);
    s.visited := true;
    for each (s′ ∈ R(s)), if (s′.visited = false) w.put(s′);
    w.remove(s);
end while
return ExistFairState(K, u);
```

§2.2.2 公平安全性质分析

定义 2.8 (公平安全性质) 状态集合$A \subseteq S$称为K的公平安全性质，当且仅当K的所有公平计算都是A计算。

命题 2.21 状态集合$A \subseteq S$是K的公平安全性质，当且仅当以下之一成立。

- 状态集合$\neg A$不是K 的公平可达性质；
- $Rh_F(K) \subseteq A$；
- $FairReachabilityAnalysis(K, \neg A)$为$false$。

公平安全性质的推理： 给定$K = \langle S, R, I, F\rangle$且$F = \{f_1, ..., f_k\}$。设$X_0, X_1, ..., X_k, A$为状态集。我们有以下规则。

$$\frac{\begin{array}{l} A \cup X_0\text{是}\langle S, R, I\rangle\text{的安全性质} \\ \bigcup_{i=1}^{k} X_i\text{是}\langle S, R, X_0\rangle\text{的必达性质} \\ \forall i \in \{1, ..., k\}，\neg f_i\text{是}\langle S, R, X_i\rangle\text{的安全性质} \end{array}}{A\text{是}K\text{的公平安全性质}}$$

可靠性： 假定前提成立。由前提3知，对$i = 1, ..., k$，X_i状态以及X_i可达的状态都不是公平状态。由于X_0不能避开$X_1, ..., X_k$，因而X_0状态不是公平状态。由于$A \cup X_0$ 是$\langle S, R, I\rangle$ 的安全性质，因而所有K的公平计算都是A计算，即A是K的公平安全性质。由于在以X_0状态不是公平状态为前提条件的情况下，并不一定保证存在$X_1, ..., X_k$使得前提2和前题3成立，因而推理规则不具有完备性。

§2.2.3 公平可避免性质分析

定义 2.9 (公平可免性质) 状态集合$A \subseteq S$称为K的公平可免性质，当且仅当$[[K]]$中有公平$\neg A$计算。

考虑有穷状态系统。用$scc_F(B)$表示$B \subseteq S$为公平强连通图，即B是非平凡强连通的且$\forall f \in F.(B \cap f \neq \emptyset)$。

命题 2.22 状态集合$A \subseteq S$是K的公平可免性质当且仅当$\exists B \subseteq S.((B \cap I \neq \emptyset) \wedge \exists B' \subseteq B.(scc_F(B') \wedge \forall B'' \subseteq (B \setminus B').(\exists s \in B''.(B'' \neq \emptyset \rightarrow \exists s' \in (B \setminus B'').(s \rightarrow s')))) \wedge (B \cap A = \emptyset))$。

公平可避免性分析1： 给定公平Kripke模型$K = \langle S, R, I, F\rangle$和集合$A \subseteq S$。$A$是否是$K$的公平可免性分析类似于原先的可免性分析，只是将所用到的非平凡强连通分量加强为公平强连通分量即可。定义$\{f_1, ..., f_n\}|Y = \{f_1 \cap Y, ..., f_n \cap Y\}$和$\langle S, R, I, F\rangle|X = \langle S \cap X, R|X, I \cap X, F|X\rangle$。算法14是分析$A$是否为公平可避免性质的算法。

Algorithm 14 FairAvoidabilityAnalysis

Input: K, A;

Output: $true/false$;

1: $K' := (S', R', I', F') := K|\neg A$; $G := (S', R')$; $K'' := (S', R', I')$;

2: $scclist := FNscc(G)$;

3: $w := \emptyset$; for (each e in $scclist$) if $(Fairscc(K', e))$ $w := (w \cup e)$;

4: return $ReachbilityAnalysis(K'', w)$;

命题 2.23 状态集合$A \subseteq S$是K的公平可免性质当且仅当$FairAvoidabilityAnalysis(K, A)$为$true$。

公平可避免性分析2： 由于A是公平可免性质当且仅当$K|\neg A$有公平可达状态当且仅当$K|\neg A$的初始状态中有公平可达状态，使用$ExistFairState()$，则公平可免性分析可以更加简单。

命题 2.24 状态集合$A \subseteq S$是K的公平可免性质当且仅当$ExistFairState(K|\neg A, I \setminus A)$为$true$。

§2.2.4 公平必达性质分析

定义 2.10 (公平必达性质) 状态集合$A \subseteq S$称为K的公平必达性质，当且仅当K的所有公平计算都能到达A状态。

命题 2.25 状态集合$A \subseteq S$是K的公平必达性质，当且仅当以下之一成立。

- 状态集合A不是K的公平可避免性质；
- 对所有含有K的初始状态的S的子集B以下成立：

  $(\exists B' \subseteq B.(scc_F(B') \wedge \forall B'' \subseteq (B \setminus B').(B'' \neq \emptyset \rightarrow \exists s \in B''.(\exists s' \in (B \setminus B'').(s \rightarrow s')))) \rightarrow (B \cap A \neq \emptyset))$;

- $FairAvoidability(K, A)$为$false$；
- $ExistFairState(K|\neg A, I \setminus A)$为$false$。

公平必达性质的推理： 给定$K = \langle S, R, I, F\rangle$且$F = \{f_1, ..., f_k\}$。设$X_0, X_1, ..., X_k, A$为状态集。我们有以下规则。

$$\frac{\begin{array}{l} A \cup X_0\text{是}\langle S, R, I\rangle\text{的必达性质} \\ \bigcup_{i=1}^{k} X_i\text{是}\langle S, R, X_0\rangle\text{的必达性质} \\ \forall i \in \{1, ..., k\}, \neg f_i\text{是}\langle S, R, X_i\rangle\text{的安全性质} \end{array}}{A\text{是}K\text{的公平必达性质}}$$

可靠性： 假定前提成立，那么X_0状态不是公平状态。由于$A \cup X_0$ 是$\langle S, R, I\rangle$ 的必达性质，因而所有K 的公平计算都必然可达A状态，即A是K的公平必达性质。

§2.2.5 模型非空问题

由于对计算增加了限制，有可能使得所有计算都成了非公平的计算，这样，模型的行为就是一个空集。我们可以检查模型的行为是否为空。这个问题也称为模型非空问题。模型K非空记作$K \neq \emptyset$，当且仅当$[[K]] \neq \emptyset$。关于模型非空问题，我们有以下结论。

命题 2.26 给定$K = \langle S, R, I, F\rangle$。$K \neq \emptyset$当且仅当存在由$I$可达的公平强连通分量。

推论 2.8 给定$K = \langle S, R, I, F\rangle$。$K \neq \emptyset$当且仅当$I$中存在公平状态。

模型空性检查算法1： 检查模型是否为空的算法称为空性检查算法。给定$K = \langle S, R, I, F\rangle$。算法15是基于以上命题的空性检查算法。

Algorithm 15 EmpChecking

Input: K;

Output: $true/false$;

1: $G := (S, R)$; $scclist := FNscc(G)$;
2: $w := \emptyset$; for (each e in $scclist$) if ($fairscc(K, e)$) $w := w \cup e$;
3: $K' := (S, R, I)$;
4: return not $ReachbilityAnalysis(K', w)$;

命题 2.27 $K = \emptyset$当且仅当$EmpChecking(K)$为$true$。

又由于$K \neq \emptyset$当且仅当I中存在公平状态。我们由以下结论。

命题 2.28 $K = \emptyset$当且仅当$ExistFairState(K, I)$为$false$。

模型空性检查算法2： 若$|F| = 1$，即F中只有一个元素，则我们可以用一个双深度优先算法计算模型是否为空问题。给定$K = \langle S, R, I, \{f\}\rangle$。算法16是这样的一个算法。

命题 2.29 给定$K = \langle S, R, I, F\rangle$且$|F| = 1$。$K = \emptyset$当且仅当$EmpCheckingDDFS(K)$为$true$。

§2.2.6 非空问题的应用

非空问题是一个基本问题，可应用于解决其它的问题。

Algorithm 16 EmpCheckingDDFS

Input: K;

Output: $true/false$;

```
w:=[]; a:=b:={};
for each s ∈ I do
    if (s ∉ a) then
        a.put(s);
        w.push(s); if (empcheckingDFS1(s)=false) return false; w.pop();
    end if
end for
return true;
FUNCTION empcheckingDFS1(v)
for each s ∈ R(v) do
    if (s ∉ a) then
        a.put(s);
        w.push(s); if (empcheckingDFS1(s)=false) return false; w.pop();
    end if
end for
if (v in f) { b.put(s); if (empcheckingDFS2(s)=false) return false; }
return true;
FUNCTION empcheckingDFS2(v)
for each s ∈ R(v) do
    if (s in w) return false;
    if not (s in b) { b.put(s); if (empcheckingDFS2(s)=false) return false; };
end for
return true;
```

可达性问题 可达性问题可以转换到非空问题。给定Kripke模型$K = \langle S, R, I\rangle$和$A \subseteq S$。定义$K' = \langle S', R', I', F\rangle$其中$S', R', I', F$如下。

$$\boxed{\begin{aligned} &S' = S \cup \{t\} \\ &R' = R \cup \{(s,t) \mid s \in A\} \cup \{(t,t)\} \\ &I' = I \\ &F = \{\{t\}\} \end{aligned}}$$

命题 2.30 状态集合$A \subseteq S$是K的可达性质，当且仅当K'非空，当且仅当$EmpCheckingDDFS(K')$为$false$。

可避免性问题 可避免性问题可以转换到非空问题。给定Kripke模型$K = \langle S, R, I\rangle$和$A \subseteq S$。定义$K' = \langle S', R', I', F\rangle$其中$S', R', I', F$如下。

$$\boxed{\begin{aligned} &S' = S \cup \{t\} \\ &R' = \{(s,s') \mid (s,s') \in R, s \notin A\} \cup \{(s,t) \mid s \in A\} \cup \{(t,t)\} \\ &I' = I \\ &F = \{S\} \end{aligned}}$$

命题 2.31 状态集合$A \subseteq S$是K的可避免性质，当且仅当K'非空，当且仅当$EmpCheckingDDFS(K')$为$false$。

§2.2.7 强公平与弱公平条件

我们对公平Kripke模型，可以增强其公平条件。

强公平Kripke模型： 用$F \subseteq 2^S \times 2^S$取代原来$K = \langle S, R, I, F \rangle$的公平条件，并将公平路径定义如下。一条路径$\pi = [s_i]_{i \geq 0}$是公平的，当且仅当对所有$(f, g) \in F$，

$$inf(\pi) \cap f \neq \emptyset \rightarrow inf(\pi) \cap g \neq \emptyset$$

按照这样的公平路径的定义，我们有一个强公平Kripke模型。

强公平模型的表达能力： 强公平Kripke模型增强了原公平Kripke模型的表达能力。

- 给定公平Kripke模型$K = \langle S, R, I, \{g_1, ..., g_k\} \rangle$。定义$F' = \{(S, g_1), ..., (S, g_k)\}$。则强公平Kripke模型$K' = \langle S, R, I, F' \rangle$与$K$有相同的公平计算集合。
- 强公平Kripke模型对原公平Kripke模型的增强可以用如下例子作证。设$K_1 = \langle S, R, I, F \rangle$其中$S, R, I, F$定义如下。容易验证没有公平Kripke模型能够有与强公平Kripke模型K_1相同的公平计算集合。

$$\boxed{\begin{array}{l} S = \{s0, s1, s2\} \\ R = \{(s0, s0), (s1, s1), (s2, s2), (s0, s1), (s0, s2), (s1, s0), (s2, s0)\} \\ I = \{s0\} \\ F = \{(\{s0\}, \{s1\}), (\{s0\}, \{s2\})\} \end{array}}$$

弱公平Kripke模型： 弱公平Kripke模型的形式与强公平Kripke模型相同，即用$F \subseteq 2^S \times 2^S$取代原来$K = \langle S, R, I, F \rangle$的公平条件。不同的是对公平路径的定义。在这里，一条路径$\pi = [s_i]_{i \geq 0}$是公平的，当且仅当对所有$(f, g) \in F$，

$$inf(\pi) \subseteq f \rightarrow inf(\pi) \cap g \neq \emptyset$$

按照这样的公平路径的定义，我们有一个弱公平Kripke模型。

弱公平模型的表达能力： 弱公平Kripke模型在一些情况下与原公平Kripke模型相比较有表达的方便性，但与原公平Kripke模型的表达能力相同。

- 给定公平Kripke模型$K = \langle S, R, I, \{g_1, ..., g_k\} \rangle$。定义$F' = \{(S, g_1), ..., (S, g_k)\}$。则弱公平Kripke模型$K' = \langle S, R, I, F' \rangle$与$K$有相同的公平计算集合。
- 给定弱公平Kripke模型$K = \langle S, R, I, \{(f_1, g_1), ..., (f_k, g_k)\} \rangle$。定义$F' = \{g_1 \cup (S \setminus f_1), ..., g_k \cup (S \setminus f_k)\}$。则公平Kripke模型$K' = \langle S, R, I, F' \rangle$与$K$有相同的公平计算集合。

§2.3 标号Kripke模型

Kripke模型对于系统的描述过于简化，只使用状态集表示性质等。为了表达和计算的简便，可用命题表示性质。我们可将结构中的状态和命题建立联系，使得我们能知道每个状态上哪些命题是成立的。

定义 2.11 *给定原子命题的有穷集合AP。一个AP上的标号Kripke模型是一个四元组$\langle S, R, I, L\rangle$其中$\langle S, R, I\rangle$为Kripke模型，$L : S \to 2^{AP}$为状态集合到$AP$的幂集的映射。*

$L(s)$表示在s上成立的所有原子命题组成的集合，即原子命题p在s上成立当且仅当$p \in L(s)$。假定原子命题集合AP和AP上的标号Kripke模型$K = \langle S, R, I, L\rangle$为给定。

可达状态： 标号Kripke模型K的可达状态即$K' = \langle S, R, I\rangle$的可达状态。

计算与行为： 标号Kripke模型K上的路径即$K' = \langle S, R, I\rangle$上的路径。$K$的计算即$K'$的计算，其行为$[[K]] = [[K']]$。

模型语言： 将一个计算上的每个状态替换成这个状态所标的命题集合，我们得到一个命题集合的无穷串。与计算对应的这些无穷串的集合称为模型的语言，定义如下。设$\pi = [\pi_i]_{i\geq 0}$。定义$L(\pi) = [L(\pi_i)]_{i\geq 0}$。集合$\{L(\pi) \subseteq (2^{AP})^\omega \mid \pi \in [[K]]\}$称为$K$的语言，记作$\mathcal{L}(K)$。

可表达性质： 给定2^{AP}上的无穷串的集合$A \subseteq (2^{AP})^\omega$。称$A$是标号Kripke模型可表达的当且仅当存在$K$使得$\mathcal{L}(K) = A$。

状态与公式： 记原子命题集合AP上所有命题公式的集合为$\mathcal{L}_{AP}$。我们用命题逻辑的公式表示状态的性质。状态$s \in S$满足$\varphi \in \mathcal{L}_{AP}$记作$K, s \models \varphi$，定义如下。

$K, s \models p$	若$p \in AP$且$p \in L(s)$。
$K, s \models \neg\psi$	若$K, s \not\models \psi$。
$K, s \models \psi_0 \vee \psi_1$	若$K, s \models \psi_0$或$K, s \models \psi_1$。
$K, s \models \psi_0 \wedge \psi_1$	若$K, s \models \psi_0$且$K, s \models \psi_1$。
$K, s \models \psi_0 \rightarrow \psi_1$	若$K, s \models \psi_0$则$K, s \models \psi_1$。
$K, s \models \psi_0 \leftrightarrow \psi_1$	若$K, s \models \psi_0$当且仅当$K, s \models \psi_1$。

定义$K, X \models \varphi$，当且仅当对所有$s \in X$都有$K, s \models \varphi$。

定义 2.12 *设$m = \{x_1, ..., x_k\} \subseteq AP$且$\{y_1, ..., y_l\} = AP \setminus m$。$m \models \varphi$当且仅当$(\varphi^{1,...,1}_{x_1,...,x_k})^{0,...,0}_{y_1,...,y_l}$的值为1。*

为方便起见，在K为给定且不引起混淆的情况下，$K, s \models \varphi$和$K, X \models \varphi$亦可分别写做$s \models \varphi$和$X \models \varphi$。

命题 2.32 *$s \models \varphi$当且仅当$L(s) \models \varphi$。*

状态集合与公式的对应： 定义$[[s]] = (\bigwedge_{p \in L(s)} p) \wedge (\bigwedge_{p \in AP \setminus L(s)} \neg p)$。定义$[[X]] = \bigvee_{s \in X}[[s]]$。我们有以下相应性质。

- $X \models \varphi$ 当且仅当$[[X]] \to \varphi$。
- 若$X \subseteq Y$则$[[X]] \to [[Y]]$。
- 若L为单射函数，则以下成立。$[[X]] \to [[Y]]$则$X \subseteq Y$。

公式与状态集合的对应： 定义$[[\varphi]] = \{s \mid s \models \varphi\}$。$[[\varphi]]$即满足$\varphi$的状态的集合。称满足$\varphi$的状态为$\varphi$状态。若一条路径上的所有状态都满足$\varphi$，则称该路径为$\varphi$路径。若一个计算上的所有状态都满足$\varphi$，则称该计算为$\varphi$计算。我们有以下相应性质。

- $\varphi \to \psi$当且仅当$[[\varphi]] \subseteq [[\psi]]$。
- $\varphi \leftrightarrow [[([[\varphi]])]]$。
- 若L为单射函数，则$X = [[([[X]])]]$。

正确性性质： 我们可将原来用状态集合定义的可达性质、安全性质、可免性质、必达性质重新用公式定义。

- φ是$K = \langle S, R, I, L\rangle$的可达性质，当且仅当$[[\varphi]]$是$K' = \langle S, R, I\rangle$的可达性质，即$Rh(I) \cap [[\varphi]] \neq \emptyset$，即$\exists s \in Rh(I).(s \models \varphi)$。
- φ是$K = \langle S, R, I, L\rangle$的安全性质，当且仅当$[[\varphi]]$是$K' = \langle S, R, I\rangle$的安全性质，即$Rh(I) \subseteq [[\varphi]]$，即$Rh(I) \models \varphi$。
- φ是$K = \langle S, R, I, L\rangle$的可避免性质，当且仅当$[[\varphi]]$是$K' = \langle S, R, I\rangle$ 的可免性质，即$\exists B \subseteq S.((B \cap Rh(I) \neq \emptyset) \wedge (\forall s \in B.(\exists s' \in B.(s \to s')) \wedge (\forall s \in B.(s \not\models \varphi)))$。
- φ是$K = \langle S, R, I, L\rangle$的必达性质，当且仅当$[[\varphi]]$是$K' = \langle S, R, I\rangle$的必达性质，即$\forall B \subseteq S.((B \cap Rh(I) \neq \emptyset) \wedge (\forall s \in B.(\exists s' \in B.(s \to s'))) \to (\exists s \in B.(s \models \varphi)))$。

分析方法： 标号Kripke模型在原来Kripke模型之上建立了状态与命题逻辑公式的联系，原有的概念和分析方法可以经过相应改变后使用。以下仅讨论安全性质与必达性质的推理问题。

安全性质的推理： 定义$R(\varphi) = [[\{s' \mid s \to s', s \models \varphi\}]]$。若$R(\varphi) \to \varphi$，则称$\varphi$为迁移不变。关于安全性质，我们有如下推理规则。设$\varphi', \varphi$为公式。

$$\frac{\begin{array}{l}[[I]] \to \varphi' \\ R(\varphi') \to \varphi' \\ \varphi' \to \varphi\end{array}}{\varphi\text{是安全性质}}$$

可靠性与完备性： 以上推理规则是可靠的且若L为单射函数则推理规则是完备的。假定前提成立，由前两条我们知道$Rh(I) \models \varphi'$，又由第三条我们知道$Rh(I) \models \varphi$，所以φ是安全性质，因而推理规则是可靠的。假定φ是安全的，取$\varphi' = [[Rh(I)]]$，由L为单射函数知$s \models \varphi'$则$s \in Rh(I)$，所以前提条件成立，由此可证φ是安全性质，因而推理规则是完备的。

必达性质的推理： 关于必达性质，我们有如下推理规则。设$\psi_0, \psi_1, ..., \psi_n, \varphi$为公式。

$$\frac{\begin{array}{l}[[I]] \to \psi_0 \\ \forall i \in \{0, ..., n-1\}.(R(\psi_i \wedge \neg\varphi) \to \psi_{i+1}) \\ \psi_n \to \varphi\end{array}}{\varphi\text{是必达性质}}$$

可靠性与完备性： 以上推理规则是可靠且对于有穷状态系统若L是单射函数则推理规则是完备的。

§2.4 公平标号Kripke模型

我们可以结合标号Kripke模型和公平Kripke模型构造标号公平Kripke模型，这样我们可以使用公式描述性质，也可以对合理的计算设置条件。我们可以在公平Kripke模型加标号也可以在标号Kripke模型加公平条件。本节的选择是在标号Kripke模型上加公平条件。

定义 2.13 给定一个有穷命题集合AP。一个AP上的公平标号$Kripke$模型是一个五元组$\langle S, R, I, L, F\rangle$其中$\langle S, R, I, L\rangle$是一个$AP$上的标号$Kripke$模型，$F \subseteq \mathcal{L}_{AP}$为公平性约束的有穷集合。

计算与行为： 公平标号Kripke模型$K = \langle S, R, I, L, F\rangle$的计算就是Kripke模型$\langle S, R, I\rangle$的计算，设$F = \{\phi_1, ..., \phi_k\}$。$K$的公平计算就是公平Kripke模型$K' = \langle S, R, I, \{[[\phi_1]], ..., [[\phi_k]]\}\rangle$的公平计算，其行为$[[K]] = [[K']]$。

正确性性质及其分析方法： 由公式与状态集合的对应关系，我们可以相应地定义公平标号Kripke模型的公平安全和公平必达等性质，并将标号Kripke模型和公平Kripke 模型的概念和分析方法经过相应改变后使用。以下仅讨论语言及语言非空问题。

模型语言： 将一个计算上的每个状态替换成这个状态所标的命题集合，我们得到一个命题集合的无穷串。与公平计算对应的这些无穷串的集合称为模型的语言，定义如下。集合$\{L(\pi) \subseteq (2^{AP})^\omega \mid \pi \in [[K]]\}$称为$K$的语言，记作$\mathcal{L}(K)$。

语言非空问题： 语言非空问题可转化成模型非空问题。我们有以下结论。

命题 2.33 给定$K = \langle S, R, I, L, F\rangle$且$F = \{\phi_1, ..., \phi_k\}$。$\mathcal{L}(K) \neq \emptyset$，当且仅当$[[K]]$非空，当且仅当公平$Kripke$模型$K' = \langle S, R, I, \{[[\phi_1]], ..., [[\phi_k]]\}\rangle$非空，即$EmpChecking(K')$为$false$。

公平安全性质的推理： 给定$K = \langle S, R, I, L, F\rangle$且$F = \{\phi_1, ..., \phi_k\}$。设$\psi_0, \psi_1, ..., \psi_k, \varphi$为公式。我们有以下规则。

$$\frac{\begin{array}{l}\varphi \vee \psi_0\text{是}\langle S, R, I, L\rangle\text{的安全性质}\\ \bigvee_{i=1}^{k} \psi_i\text{是}\langle S, R, [[\psi_0]], L\rangle\text{的必达性质}\\ \forall i \in \{1, ..., k\}, \neg\phi_i\text{是}\langle S, R, [[\psi_i]], L\rangle\text{的安全性质}\end{array}}{\varphi\text{是}K\text{的公平安全性质}}$$

可靠性： 假定前提成立。由前提3知，对$i = 1, ..., k$，ψ_i状态以及其可达的状态都不是公平状态。由于ψ_0不能避开$\psi_1, ..., \psi_k$，因而ψ_0状态不是公平状态。由于$\varphi \vee \psi_0$ 是$\langle S, R, I, L\rangle$的安全性质，因而所有$K$的公平计算都是$\varphi$计算，即$\varphi$是$K$的公平安全性质。由于在以$\psi_0$状态不是公平状态为前提条件的情况下，并不一定保证存在$\psi_1, ..., \psi_k$使得前提2和前题3成立，因而推理规则不具有完备性。

公平必达性质的推理： 给定$K = \langle S, R, I, L, F\rangle$且$F = \{\phi_1, ..., \phi_k\}$。设$\psi_0, \psi_1, ..., \psi_k, \varphi$为公式。我们有以下规则。

$$\frac{\begin{array}{l}\varphi \vee \psi_0\text{是}\langle S, R, I, L\rangle\text{的必达性质}\\ \bigvee_{i=1}^{k} \psi_i\text{是}\langle S, R, [[\psi_0]], L\rangle\text{的必达性质}\\ \forall i \in \{1, ..., k\}, \neg\phi_i\text{是}\langle S, R, [[\psi_i]], L\rangle\text{的安全性质}\end{array}}{\varphi\text{是}K\text{的公平必达性质}}$$

可靠性： 假定前提成立，那么ψ_0状态不是公平状态。由于$\varphi \vee \psi_0$ 是$\langle S, R, I, L\rangle$ 的必达性质，因而所有K的公平计算都必然可达φ状态，即φ是K的公平必达性质。

§2.5 例子

例 2.1 （*1*）定义S, R, I如下。

$S = \{s_0, s_1, s_2, s_3, s_4, s_5, s_6\}$
$R = \{(s_0, s_1), (s_0, s_3), (s_1, s_2), (s_1, s_4), (s_2, s_1), (s_3, s_4), (s_4, s_4), (s_5, s_2), (s_5, s_4), (s_5, s_6), (s_6, s_5)\}$
$I = \{s_0, s_3\}$

则$K_1 = (S, R, I)$为$Kripke$模型。

K_1的可达状态集合为$\{s_0, s_1, s_2, s_3, s_4\}$。

定义A_1, A_2如下。

$$\begin{array}{rcl} A_1 &=& \{s_0, s_1, s_2, s_3, s_4\} \\ A_2 &=& \{s_0, s_1, s_2, s_3, s_4, s_5\} \end{array}$$

则A_1和A_2是模型的安全性质。

根据安全性质分析算法知$SafetyAnalysis(K_1, A_1)$为$true$且$SafetyAnalysis(K_1, A_2)$为$true$。

定义B_1, B_2如下。

$$\begin{array}{rcl} B_1 &=& \{s_2, s_4\} \\ B_2 &=& \{s_2, s_4, s_5\} \end{array}$$

则B_1和B_2是模型的必达性质。
根据必达性质分析算法知$InevitabilityAnalysis(K_1, B_1)$为$true$且$InevitabilityAnalysis(K_1, B_2)$为$true$。
（2）定义$F = \{\{s_1, s_4\}, \{s_2, s_5\}\}$
则$K_2 = (S, R, I, F)$为公平$Kripke$模型。
K_2的可达公平状态集合为$\{s_0, s_1, s_2\}$。
定义A_3, B_3如下。

$$\begin{aligned} A_3 &= \{s_0, s_1, s_2\} \\ B_3 &= \{s_2\} \end{aligned}$$

则A_3是模型的公平安全性质且B_3是模型的公平必达性质。
根据公平安全性质分析算法和公平必达性质分析算法知

$$FairSafetyAnalysis(K_2, A_3)\text{为}true\text{ 且}FairInevitabilityAnalysis(K_2, B_3)\text{为}true\text{。}$$

（3）设$AP = \{p, q, r\}$。定义$L : S \to 2^{AP}$如下。

$$\begin{array}{lllll} L(s_0) = \{p\} & L(s_1) = \{q\} & L(s_2) = \{p, q\} & L(s_3) = \{\} & L(s_4) = \{r\} \\ qL(s_5) = \{p, r\} & L(s_6) = \{q, r\} & & & \end{array}$$

则$K_3 = (S, R, I, L)$为AP上的标号$Kripke$模型。
定义$\varphi_1, \varphi_2, \psi_1, \psi_2$如下。

$$\begin{aligned} \varphi_1 &= (p \wedge \neg q \wedge \neg r) \vee (q \wedge \neg r) \vee (\neg p \wedge \neg q) \\ \varphi_2 &= (\neg p \vee \neg r) \\ \psi_1 &= (p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \\ \psi_2 &= (p \wedge q \wedge \neg r) \vee (\neg q \wedge r) \end{aligned}$$

则以下成立。

$$\begin{array}{lcllcl} [[\varphi_1]] & = & \{s_0, s_1, s_2, s_3, s_4\} & [[\varphi_2]] & = & \{s_0, s_1, s_2, s_3, s_4, s_5\} \\ [[\psi_1]] & = & \{s_2\} & [[\psi_2]] & = & \{s_2, s_4, s_5\} \end{array}$$

相应地，φ_1和φ_2是模型的安全性质且ψ_1和ψ_2是模型的必达性质。
(4) 定义$\Phi = \{\phi_1, \phi_2\}$其中$\phi_1, \phi_2$定义如下。

$$\begin{aligned} \phi_1 &= (\neg p \wedge (q \leftrightarrow \neg r)) \\ \phi_2 &= (p \wedge (q \leftrightarrow \neg r)) \end{aligned}$$

则$K_3 = (S, R, I, L, \Phi)$为AP上的标号公平$Kripke$模型。
定义φ_3, ψ_3如下。

$$\begin{aligned} \varphi_3 &= (p \vee q) \wedge \neg r \\ \psi_3 &= (p \wedge q) \wedge \neg r \end{aligned}$$

我们有

$$\begin{array}{lcllcl} [[\phi_1]] & = & \{s_1, s_4\} & [[\phi_2]] & = & \{s_2, s_5\} \\ [[\varphi_3]] & = & \{s_0, s_1, s_2\} & [[\psi_3]] & = & \{s_2\} \end{array}$$

相应地，φ_3是模型的公平安全性质且ψ_3是模型的公平必达性质。

例 2.2 设$K_1 = (S, R, I)$和A_1, A_2, B_1, B_2如例*2.1*中所定义。

（*1*）A_1是K_1的安全性质的推理证明如下。

定义$A'_1 = A_1$。则以下成立。

$$\begin{array}{l} I\text{满足}A'_1 \\ A'_1\text{是迁移不变量} \\ A'_1\text{满足}A_1 \end{array}$$

因而根据推理规则，A_1是K_1的安全性质。

A_2是K_1的安全性质的推理证明如下。

定义$A'_2 = A_1$。则以下成立。

$$\begin{array}{l} I\text{满足}A'_2 \\ A'_2\text{迁移不变} \\ A'_2\text{满足}A_2 \end{array}$$

因而根据推理规则，A_2是K_1的安全性质。

注意：由于A_2不是迁移不变，故不能取$A'_2 = A_2$。

（2）B_1是K_1的必达性质的推理证明如下。

定义X_i如下*:* $X_0 = \{s_0, s_3\}, X_1 = \{s_1, s_4\}, X_2 = \{s_2, s_4\}$。

则以下成立。

$$\begin{array}{l} I\text{满足}X_0 \\ \forall i \in \{0, 1\}, R(X_i \setminus B_1)\text{满足}X_{i+1} \\ X_2\text{满足}B_1 \end{array}$$

因而根据推理规则，B_1是K_1的必达性质。

类似地可以证明B_2是K_1的必达性质。

例 2.3 设$/, \%$分别为自然数上的整除和余数函数。设a, b, x, y, t为自然数上的函数定义如下。

$$\begin{array}{rclrcl} a(i) & = & i/24 & b(i) & = & (i\%24)/8 \\ x(i) & = & (i\%8)/4 & y(i) & = & (i\%4)/2 \\ t(i) & = & i\%2 & & & \end{array}$$

定义$t_1(k, j), ..., t_8(k, j)$如下。

$$\begin{array}{rcl} t_1(k, j) & = & a(k) = 0 \wedge a(j) = 1 \wedge b(j) = b(k) \wedge x(j) = x(k) \wedge y(j) = 1 \wedge t(j) = 1 \\ t_2(k, j) & = & a(k) = 1 \wedge \neg(x(k) = 0 \vee t(k) = 0) \wedge (j = k) \\ t_3(k, j) & = & a(k) = 1 \wedge (x(k) = 0 \vee t(k) = 0) \wedge a(j) = 2 \wedge b(j) = b(k) \wedge (j\%8 = k\%8) \\ t_4(k, j) & = & a(k) = 2 \wedge a(j) = a(k) \wedge b(j) = b(k) \wedge x(j) = x(k) \wedge y(j) = 0 \wedge t(j) = t(k) \\ t_5(k, j) & = & b(k) = 0 \wedge a(j) = a(k) \wedge b(j) = 1 \wedge x(j) = 1 \wedge y(j) = y(j) \wedge t(j) = 0 \\ t_6(k, j) & = & b(k) = 1 \wedge \neg(y(k) = 0 \vee t(k) = 1) \wedge (j = k) \\ t_7(k, j) & = & b(k) = 1 \wedge (y(k) = 0 \vee t(k) = 1) \wedge a(j) = a(k) \wedge b(j) = 2 \wedge (j\%8 = k\%8) \\ t_8(k, j) & = & b(k) = 2 \wedge a(j) = a(k) \wedge b(j) = b(k) \wedge x(j) = 0 \wedge y(j) = y(k) \wedge t(j) = t(k) \end{array}$$

（*1*）定义S, R, I如下。

$$\boxed{\begin{aligned} S &= \{s_0, s_1, ..., s_{71}\} \\ R &= \{(s_k, s_j) \mid t_1(k, j) \vee \cdots \vee t_8(k, j)\} \\ I &= \{s_0, s_1\} \end{aligned}}$$

则$K_1 = (S, R, I)$为$Kripke$模型。

定义A_1, B_1如下。

$$\begin{aligned} A_1 &= \{s_i \mid a(i) \neq 2 \vee b(i) \neq 2\} \\ B_1 &= \{s_i \mid a(i) = 2 \vee b(i) = 2\} \end{aligned}$$

则A_1为K_1的安全性质，B_1不是K_1的必达性质。

根据安全性质分析算法和必达性质分析算法知

$$SafetyAnalysis(K_1, A_1)\text{为}true\ \text{且}InevitabilityAnalysis(K_1, B_1)\text{为}false\text{。}$$

若该模型用以表示2个进程的互斥算法的运行模型，则模型具有以上意义的安全（互斥）性质。

设$R' = R \setminus \{(s, s) \mid s \in S\}$且$K'_1 = (S, R', I)$。

则K'_1为$Kripke$模型，A_1为K'_1的安全性质且B_1为K'_1的必达性质。

根据安全性质分析算法和必达性质分析算法知

$$SafetyAnalysis(K'_1, A_1)\text{为}true\ \text{且}InevitabilityAnalysis(K'_1, B_1)\text{为}true\text{。}$$

（2）定义F为以下集合的集合。

$$\begin{aligned} &\{s_i \mid \neg(a(i) = 0)\} \\ &\{s_i \mid \neg(a(i) = 1 \wedge (x(i) = 0 \vee t(i) = 0))\} \\ &\{s_i \mid \neg(a(i) = 2)\} \\ &\{s_i \mid \neg(b(i) = 0)\} \\ &\{s_i \mid \neg(b(i) = 1 \wedge (y(i) = 0 \vee t(i) = 1))\} \\ &\{s_i \mid \neg(b(i) = 2)\} \end{aligned}$$

定义$K_2 = (S, R, I, F)$。则A_1为K_2的公平安全性质且B_1为K_2的公平必达性质。

根据公平安全性质分析算法和公平必达性质分析算法知

$$FairSafetyAnalysis(K_2, A_1)\text{为}true\ \text{且}FairInevitabilityAnalysis(K_2, B_1)\text{为}true\text{。}$$

若该模型用以表示2个进程的互斥算法的带有公平约束的运行模型，则模型具有以上意义的安全和必达性质。

（*3*）设$AP = \{p_1, p_2, p_3, p_4, p_5, p_6\}$。定义$L : S \to 2^{AP}$如下。

$$\begin{aligned} p_1 \in L(s_i) &\quad \text{iff} \quad a(i) = 0 \\ p_2 \in L(s_i) &\quad \text{iff} \quad a(i) = 1 \\ p_3 \in L(s_i) &\quad \text{iff} \quad a(i) = 2 \\ p_4 \in L(s_i) &\quad \text{iff} \quad b(i) = 0 \\ p_5 \in L(s_i) &\quad \text{iff} \quad b(i) = 1 \\ p_6 \in L(s_i) &\quad \text{iff} \quad b(i) = 2 \end{aligned}$$

则$K_3 = (S, R, I, L)$为AP上的标号*Kripke*模型。
定义φ_1, ψ_1如下：$\varphi_1 = \neg(p_3 \wedge p_6), \psi_1 = (p_3 \vee p_6)$。
则φ_1是K_3的安全性质，ψ_1不是K_3的必达性质。
定义$K'_3 = (S, R, I, L)$。则φ_1是K'_3的安全性质且ψ_1是K'_3的必达性质。
（*4*）设$AP' = AP \cup \{q_1, q_2, q_3, q_4, q_5, q_6\}$。定义$L' : S \to 2^{AP}$如下。

$$
\begin{array}{lll}
p_i \in L'(s_i) & \text{iff} & p_i \in L(s_i) \\
q_1 \in L'(s_i) & \text{iff} & x(i) = 0 \\
q_2 \in L'(s_i) & \text{iff} & x(i) = 1 \\
q_3 \in L'(s_i) & \text{iff} & y(i) = 0 \\
q_4 \in L'(s_i) & \text{iff} & y(i) = 1 \\
q_5 \in L'(s_i) & \text{iff} & t(i) = 0 \\
q_6 \in L'(s_i) & \text{iff} & t(i) = 1
\end{array}
$$

设Φ为以下集合。

$$\{\neg(p_1), \neg(p_2 \wedge (q_1 \vee q_5)), \neg(p_3), \neg(p_4), \neg(p_5 \wedge (q_3 \vee q_6)), \neg(p_6)\}$$

则$K_4 = (S, R, I, L', \Phi)$为$AP'$上的公平标号*Kripke*模型，$\varphi_1$为$K_4$的公平安全（互斥）性质且$\psi_1$为$K_4$的公平必达（资源有机会得到使用）性质。

例 2.4 （*1*）设$K_1 = (S, R, I)$和A_1如例*2.3*中所定义。A_1是K_1的安全性质的推理证明如下。
定义A'_1为如下集合的并集。

$$
\begin{array}{l}
\{s_i \mid (a(i) = 0 \wedge b(i) = 0 \wedge x(i) = 0 \wedge y(i) = 0\} \\
\{s_i \mid (a(i) = 0 \wedge b(i) = 1 \wedge x(i) = 1 \wedge y(i) = 0\} \\
\{s_i \mid (a(i) = 0 \wedge b(i) = 2 \wedge x(i) = 1 \wedge y(i) = 0\} \\
\{s_i \mid (a(i) = 1 \wedge b(i) = 0 \wedge x(i) = 0 \wedge y(i) = 1\} \\
\{s_i \mid (a(i) = 1 \wedge b(i) = 1 \wedge x(i) = 1 \wedge y(i) = 1\} \\
\{s_i \mid (a(i) = 1 \wedge b(i) = 2 \wedge x(i) = 1 \wedge y(i) = 1 \wedge t(i) = 1\} \\
\{s_i \mid (a(i) = 2 \wedge b(i) = 0 \wedge x(i) = 0 \wedge y(i) = 1\} \\
\{s_i \mid (a(i) = 2 \wedge b(i) = 1 \wedge x(i) = 1 \wedge y(i) = 1 \wedge t(i) = 0\}
\end{array}
$$

则以下成立。

$$
\begin{array}{l}
I\text{满足}A'_1 \\
A'_1\text{是迁移不变量} \\
A'_1\text{满足}A_1
\end{array}
$$

因而根据推理规则，A_1是K_1的安全性质。
（2）设$K'_1 = (S, R', I)$和B_1如例*2.3*中所定义。B_1是K'_1的必达性质的推理证明如下。

定义$X_{i,j}$为如下。

$$
\begin{aligned}
X_{0,1} &= \{s_i \mid (a(i) = 0 \wedge b(i) = 0 \wedge x(i) = 0 \wedge y(i) = 0 \wedge t(i) = 0\} \\
X_{0,2} &= \{s_i \mid (a(i) = 0 \wedge b(i) = 0 \wedge x(i) = 0 \wedge y(i) = 0 \wedge t(i) = 1\} \\
X_{1,1} &= \{s_i \mid (a(i) = 1 \wedge b(i) = 0 \wedge x(i) = 0 \wedge y(i) = 1 \wedge t(i) = 1\} \\
X_{1,2} &= \{s_i \mid (a(i) = 0 \wedge b(i) = 1 \wedge x(i) = 1 \wedge y(i) = 0 \wedge t(i) = 0\} \\
X_{2,1} &= \{s_i \mid (a(i) = 1 \wedge b(i) = 1 \wedge x(i) = 1 \wedge y(i) = 0 \wedge t(i) = 0\} \\
X_{2,2} &= \{s_i \mid (a(i) = 1 \wedge b(i) = 1 \wedge x(i) = 1 \wedge y(i) = 1 \wedge t(i) = 1\} \\
X_{3,1} &= \{s_i \mid (a(i) = 2 \wedge b(i) = 1 \wedge x(i) = 1 \wedge y(i) = 1 \wedge t(i) = 0\} \\
X_{3,2} &= \{s_i \mid (a(i) = 1 \wedge b(i) = 2 \wedge x(i) = 1 \wedge y(i) = 1 \wedge t(i) = 1\}
\end{aligned}
$$

定义$X_0 = X_{0,1} \cup X_{0,2}$, $X_1 = X_{1,1} \cup X_{1,2}$,$X_2 = X_{2,1} \cup X_{2,2} \cup A_2$, $X_3 = X_{3,1} \cup X_{3,2}$。则以下成立。

$$
\begin{aligned}
&I\text{满足}X_0 \\
&\forall i \in \{0, 1, 2\},\ R'(X_i \setminus A_2)\text{满足}X_{i+1} \\
&X_3\text{满足}B_1
\end{aligned}
$$

因而根据推理规则，B_1是K_1'的必达性质。

§2.6 练习

1. 给定Kripke模型$K = \langle S, R, I\rangle$和$A \subseteq S$。判断以下说法的正确性：$A$是可避免性质，当且仅当$K$有一条由$I$出发可达非$A$非平凡强连通分量的非$A$路径。

2. 给定Kripke模型$K = \langle S, R, I\rangle$和$B, A \subseteq S$。结合安全与可达和必达概念，我们可定义系统的安全可达和安全必达性质如下：B为A安全可达性质当且仅当存在可达B的计算且该计算中第一个B状态前的所有状态都是A状态；B为A安全必达性质当且仅当B必达且在所有计算中第一个B状态前的所有状态都是A状态。设计算法分别检查B是否为A安全可达性质和B是否为A安全必达性质。

3. 给定Kripke模型$K = \langle S, R, I\rangle$和$B, A \subseteq S$。定义$(B, A)$路径为满足以下条件的路径：至少一个$B$状态出现在该路径中且同时或之后有$A$状态出现。设计基于不动点计算的算法以检查K中是否存在初始状态为起点的(B, A)路径。

4. 给定公平Kripke模型$K = \langle S, R, I, F\rangle$和$A \subseteq S$。通过对模型进行改造，用模型非空问题算法检查$A$是否是$K$的可达性质。

5. 给定公平Kripke模型$K = \langle S, R, I, F\rangle$和$A \subseteq S$。通过对模型进行改造，用模型非空问题算法检查$A$是否是$K$的可避免性质。

6. 设$S, R, R', I, AP', L', \varphi_1, \psi_1$如例2.3中所定义。则$K = (S, R, I, L')$和$K' = (S, R', I, L')$为$AP'$上的标号Kripke模型。用推理方法证明$\varphi_1$是$K$的安全性质且$\psi_1$是$K'$的必达性质。