中国科学院研究生院课程讲稿

§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。公式集合用归纳法定义。 设 S 是联结词的集合。由 S 生成的公式定义如下。 （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 φ 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 φ 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 φ 与 φ^* 互为对偶式， ψ 与 ψ^* 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 φ 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 φ 是永真式。$\varphi_1,...,\varphi_n\models\varphi$ 当且仅当 $\varphi_1\wedge\cdots\wedge\varphi_n\rightarrow\varphi$ 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 $\Gamma\models\varphi\rightarrow\psi$。 $\Gamma=\{\varphi_1,...,\varphi_n\}$ 是可满足的当且仅当 $\varphi_1\wedge\cdots\wedge\varphi_n$ 是可满足的。 Γ 是不可满足的当且仅当每个逻辑公式都是 Γ 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 $\neg,\wedge,\vee,\rightarrow,\leftrightarrow$。 （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 $\{\neg,\wedge,\vee,\rightarrow,\leftrightarrow\}$ 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 φ 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 φ 是 $\neg\psi$, ψ 是公式, 则 $I(\varphi)\sigma=\neg I(\psi)\sigma$; （3）若 φ 是 $\varphi_0\wedge\varphi_1$, 则 $I(\varphi)\sigma=I(\varphi_0)\sigma\wedge I(\varphi_1)\sigma$; （4）若 φ 是 $\varphi_0\vee\varphi_1$, 则 $I(\varphi)\sigma=I(\varphi_0)\sigma\vee I(\varphi_1)\sigma$; （5）若 φ 是 $\varphi_0\to\varphi_1$, 则 $I(\varphi)\sigma=I(\varphi_0)\sigma\to I(\varphi_1)\sigma$; （6）若 φ 是 $\varphi_0\leftrightarrow\varphi_1$ ，则 $I(\varphi)\sigma=I(\varphi_0)\sigma\leftrightarrow I(\varphi_1)\sigma$; （7）若 φ 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 φ 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 φ 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 φ 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 $\varphi_{A_1,...,A_n}^{\varphi_1,...,\varphi_n}$，称为 φ 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 φ 和 ψ 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 φ 是永真式。$\varphi_1, ..., \varphi_n \models \varphi$ 当且仅当 $\varphi_1 \wedge \cdots \wedge \varphi_n \rightarrow \varphi$ 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 $\Gamma \models \varphi \rightarrow \psi$。 $\Gamma = \{\varphi_1, ..., \varphi_n\}$ 是可满足的当且仅当 $\varphi_1 \wedge \cdots \wedge \varphi_n$ 是可满足的。 Γ 是不可满足的当且仅当每个逻辑公式都是 Γ 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。

$$\begin{array}{|ll|} \hline (A = B) & \Leftrightarrow \quad \forall x(x \in A \leftrightarrow x \in B) \\ (A \subseteq B) & \Leftrightarrow \quad \forall x(x \in A \rightarrow x \in B) \\ \hline \end{array}$$

子集关系满足以下性质。

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

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 $\rho(A)$。 $\rho(A) = \{X \mid X \subseteq A\}$。 若 $a \in A$，则 $\{a\} \subseteq A$。若 $A \subseteq B$，则 $A \in \rho(B)$。 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 $|\rho(A)| = 2^{|A|}$。

集合的运算有交、并、差。

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

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 $\sim A$。

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

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。

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

$r(R)$	$=$	$R\cup I_X$
$s(R)$	$=$	$R\cup R^{-1}$
$t(R)$	$=$	$\bigcup_{i=1}^{\infty}R^i$

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、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。

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：	$\forall x\in A.(a\not\leq x)$
a 为 A 的极小元：	$\forall x\in A.(x\not\leq a)$
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 。

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 $\sqcup S=\langle\sqcup pr_1(S),...,\sqcup pr_n(S)\rangle$ 。

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。

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极小元，则称 $\leq$ 为良基的 (Well Founded)，称 $\langle P,\leq\rangle$ 为良基集合。 一个集合是良基集合当且仅当该集合中不存在无限递减的序列。

设 $\langle P,\leq\rangle$ 为良基集合。记 $x\leq y$ 且 $x\neq y$ 为 $x<y$ 。以下推理规则为良基集合上的归纳法 (Noetherian Induction) 。

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

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。

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。 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。

§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 $f : X \to Y$。 X 称为 f 的定义域， Y 称为 f 的值域。

对于函数 $f : X \to Y$，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 $f : X \to Y$ 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 $f : X' \to Y$ 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 $f : X \to Y$ 和 $g : Y \to Z$ 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 $f : X \to X$ 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 $f : X \to Y$ 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	$\forall x_1, x_2 \in X.(f(x_1) = f(x_2) \to x_1 = x_2)$
f 是双射的	f 是满射的且是入射的

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

$\Psi_{A\cap B}(x)$	$=$	$\Psi_A(x) \cdot \Psi_B(x)$
$\Psi_{A\cup B}(x)$	$=$	$\Psi_A(x) + \Psi_B(x) - \Psi_{A\cap B}(x)$
$\Psi_{\sim A}(x)$	$=$	$1 - \Psi_A(x)$

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 $x \in X$ ，$(\sqcup S)(x) = \sqcup S(x)$ 。

§1.6 完全偏序和格上的不动点

一个偏序 $\langle X, \leq \rangle$ 是完全偏序当且仅当 X 有最小元，且对于 X 上的每一条链 $S \subseteq X$ ， $\sqcup S$ 都存在。 X 的最小元通常记作 $\bot_X$ 或 $\bot$ 。

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 $\sqcup_Y S = \sqcup_X S$ 。

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 $\langle X, \leq_1 \rangle$ 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 $S \subseteq X$ ， $f(\sqcup S) \leq \sqcup f(S)$ 。 如果 X 只包含有穷链，则 f 是连续的当且仅当 f 是单调的。

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 。

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

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

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。以下推理规则为不动点归纳法。

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

一个偏序 $\langle X, \leq \rangle$ 是格当且仅当任意两个 X 中的元素都有最小上界和最大下界。

一个偏序 $\langle X, \leq \rangle$ 是完全格当且仅当任意子集都有最小上界。同样，一个偏序 $\langle X, \leq \rangle$ 是完全格当且仅当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。

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

§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。

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。如果该回路中每条边的出现不超过一次，则称该回路为简单回路。如果该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 $u\to^+ v$。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。

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 $A\not\subseteq B$。 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 可达的顶点的集合（包括 A）为 $\{b\mid a\to^* b,a\in A\}$，记为 $rh(A)$。可达 A 的顶点的集合为 $\{b\mid b\to^* a,a\in A\}$，记为 $rh^b(A)$。

若 D 是强连通图，则 $rh(A)=rh^b(A)=V$。

定义 $E(a)=\{b\mid E(a,b)\},E(A)=\{b\mid E(a),a\in A\}$。若 V 是有穷集合，则

$$\begin{array}{ll} rh(A) & =\bigcup_{i=0}^{\infty}E^i(A) \qquad =\mu Z.(A\cup E(Z)).\\ rh^b(A) & =\bigcup_{i=0}^{\infty}(E^{-1})^i(A) \quad =\mu Z.(A\cup E^{-1}(Z)).\end{array}$$

设 $D_1=\langle V_1,E_1\rangle$ 和 $D_2=\langle V_2,E_2\rangle$ 为有向图。

$\sigma\subseteq V_1\times V_2$ 是一个 D_1 到 D_2 的模拟关系当且仅当对任意 $(u,v)\in\sigma$，对任意 $u'\in V_1$，如果 $E_1(u,u')$，则存在 $v'\in V_2$，$E_2(v,v')$ 且 $(u',v')\in\sigma$。σ 是模拟关系当且仅当 $\sigma^{-1}E_1\subseteq E_2\sigma^{-1}$。

$\sigma\subseteq V_1\times V_2$ 是互模拟关系当且仅当对任意 $(u,v)\in\sigma$，（1）对任意 $u'\in V_1$，如果 $E_1(u,u')$，则存在 $v'\in V_2$，$E_2(v,v')$ 且 $(u',v')\in\sigma$；（2）对任意 $v'\in V_2$，如果 $E_2(v,v')$，则存在 $u'\in V_1$，$E_1(u,u')$ 且 $(u',v')\in\sigma$。 σ 是互模拟关系当且仅当 $\sigma^{-1}E_1\subseteq E_2\sigma^{-1}$ 且 $\sigma E_2\subseteq E_1\sigma$。

设 $D=\langle V,E\rangle$ 为有向图。

$\sigma\subseteq V\times V$ 是 D 上的模拟等价关系当且仅当对任意 $(u,v)\in\sigma$，存在一个模拟关系 $\sigma'\subseteq V\times V$ 使得 $(u,v)\in\sigma'$ 且存在一个模拟关系 $\sigma''\subseteq V\times V$ 使得 $(v,u)\in\sigma''$。 $\sigma\subseteq V\times V$ 是互模拟等价关系当且仅当 σ 是 V 上的最大的互模拟关系。

§1.8 说明

本章的目的是让读者对离散数学中与程序验证相关的基础概念有所了解。离散数学的相关内容参考 [1, 2, 3]。

参考文献

[1] 尹宝林、何自强、许光汉、檀风琴。离散数学。高等教育出版社。 1998 。

[2] 左孝凌、李为镒、刘永才。离散数学。上海科学技术文献出版社。 2003 。

[3] J. Loeckx and K. Sieber. The foundation of program verification. John Wiley & Sons Ltd., 1984.