

# Contents

|          |                              |           |
|----------|------------------------------|-----------|
| <b>1</b> | <b>命题逻辑 Sentential logic</b> | <b>2</b>  |
| 1.1      | 合式公式 . . . . .               | 2         |
| 1.2      | 赋值 . . . . .                 | 4         |
| 1.3      | 真值表 . . . . .                | 5         |
| 1.4      | 布尔函数 . . . . .               | 5         |
| 1.5      | 等值 . . . . .                 | 6         |
| 1.6      | 表达能力 . . . . .               | 7         |
| 1.7      | 蕴涵 . . . . .                 | 9         |
| 1.8      | 推理理论 . . . . .               | 10        |
| 1.8.1    | 什么是证明 . . . . .              | 10        |
| 1.8.2    | 证明技巧 1: 演绎定理 . . . . .       | 11        |
| 1.8.3    | 证明技巧 2: 反证法 . . . . .        | 11        |
| 1.8.4    | 证明技巧 3: 利用等值式 . . . . .      | 12        |
| 1.9      | 习题 . . . . .                 | 13        |
| <b>2</b> | <b>一阶逻辑</b>                  | <b>14</b> |
| 2.1      | 语言 . . . . .                 | 14        |
| 2.2      | 一些翻译练习 . . . . .             | 16        |
| 2.3      | 结构 . . . . .                 | 16        |
| 2.4      | 真值 . . . . .                 | 17        |
| 2.4.1    | 赋值 . . . . .                 | 17        |
| 2.4.2    | 真假 . . . . .                 | 18        |
| 2.5      | 蕴涵 . . . . .                 | 18        |
| 2.6      | 习题 . . . . .                 | 22        |
| <b>3</b> | <b>集合</b>                    | <b>23</b> |
| 3.1      | 集合的概念 . . . . .              | 23        |
| 3.2      | 集合的基本运算 . . . . .            | 24        |
| 3.3      | 笛卡尔积 . . . . .               | 25        |
| 3.4      | 关系 . . . . .                 | 26        |
| 3.5      | 关系的性质 . . . . .              | 26        |
| 3.6      | 关系的运算 . . . . .              | 26        |
| 3.7      | 等价关系 . . . . .               | 27        |
| 3.8      | 偏序关系 . . . . .               | 29        |
| 3.9      | 哈斯图 . . . . .                | 29        |
| 3.10     | 习题 . . . . .                 | 30        |
|          | <b>习题提示</b>                  | <b>31</b> |

## § 1 命题逻辑 Sentential logic

本章目标：

1. 能凭借直观理解什么是命题，并能判断简单语句的真假。
2. 引入命题标识符、逻辑联词、括号，构建合式公式。
3. 给定赋值，会计算一个公式  $\alpha$  的真假。
4. 会找出成真赋值、成假赋值，并列成真值表。
5. 理解公式诱导的布尔函数  $B_\alpha$ ，并以  $B_\alpha = B_\beta$  理解等值。
6. 掌握全功能集，会求主析取范式、主合取范式。
7. 理解语义蕴涵  $\models$  与形式证明  $\vdash$ 。

本章先规定语言（合式公式），再规定语义（赋值、真值表、布尔函数），然后讨论等值、表达能力与范式，最后引入蕴涵与形式推理。

### 1.1 合式公式

**例 1.1** 下列哪些句子可以讨论“真”（“对”）或“假”（“错”）？2 是素数；雪是黑色的；你好；好你；晓庄真大！；晓庄是大的；方山真圆！；方山是圆的；我正在说谎；我是谁？； $x > 100$ ； $x = x$ ；如果这句话是真的，那么玉兔是存在的

如果把可以讨论真假的语句称为命题，上述例子中并非都可以讨论真假，有的句子看起来有真假，例如“我正在说谎”，但是它是一个悖论，无法评价它的真假。我们需要引入一种数学语言，作为数学叙述的载体。与中文、英文不同，我们要求这种语言没有歧义、足够简洁，并且表达能力足够丰富。

**定义 1.2** 用  $A_0, A_1, A_2, A_3, \dots$  表示命题标识符（sentence symbol）。

实际使用中，我们会自由地使用其他字母，例如  $A, B, C, \dots$ 。命题标识符是最基本的语言单元。我们可以给命题标识符赋予“意义”，使其表示命题。写作“A：我在读离散数学讲义。”。更多的例子如下。

**例 1.3**  $A_0$ ：我考上晓庄了； $A_1$ ：我毕业了； $A_2$ ：我没考上晓庄； $A_3$ ：如果我考上晓庄，我就能毕业； $A_4$ ：我考上晓庄了，但是我没有毕业； $A_5$ ：我既没有考上晓庄，也没有毕业。

其中  $A_0, A_1$  都比较“简单”，而后面的句子都比较“复杂”，包含一些简单的子句。直观上来看，只要知道前两条的真假，就能判断后面句子的真假。但我们需要说清楚，复杂句子都有哪些句式，复杂句子的真假是如何依赖于其简单子句的真假的。这是接下来的任务。

**定义 1.4** 真假已经确定的命题标识符称为命题常项；真假值尚未确定的命题标识符称为命题变元。

类比整数中的情形：我们用  $a$  表示常数（具体取值不必知道），用  $x$  表示变量。此时  $f(x) = x + a$  是一个一元函数。当然，常数和变量的分界不是绝对的： $g(x, a) = x + a$  是一个二元函数，此时  $a$  变成变量了。

**注 1.5** 具有唯一真假值，并不代表我们目前知道其真假。例如： $A_0$ ：小帅有 112003 根头发； $A_1$ ：哥德巴赫猜想； $A_2$ ：黎曼猜想； $A_3$ ：考拉兹猜想； $A_4$ ：昨天我生病了； $A_5$ ：明天我生病了。此时  $A_0, A_1, A_2, A_3, A_4$  都是命题常项，但具体是真还是假我们并不知道。 $A_5$  是命题变元：它可真可假，尚不能确定。

以后我们只处理命题变元，不处理命题常项。命题常项可以视为命题变元的特殊情形。

**定义 1.6 (逻辑联词)** 否定  $\neg$ ，合取  $\wedge$ ，析取  $\vee$ ，蕴涵  $\rightarrow$ ，等价  $\leftrightarrow$ 。

利用逻辑联词，我们可以表达更复杂的句子。

**定义 1.7** 用  $V$  表示由命题标识符、逻辑联词及括号（即（和））组成的所有有穷长字符串。 $V$  中的元素称为句子（这是一个临时称呼）。

$V$  中的句子可以是  $\wedge(A, B \rightarrow), )A \wedge B(), (B), A \wedge B, (A \vee B) \rightarrow C$ 。事实上，上述句子都不符合我们将要给出的语法规则。

**定义 1.8** 合式公式（well-formed formula, wff）由下列规则生成：

- (1) 命题变元是 wff；
- (2) 如果  $\alpha, \beta$  是 wff，则  $(\neg\alpha), (\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \rightarrow \beta), (\alpha \leftrightarrow \beta)$  是 wff。

经过有穷次规则 (1)、(2) 可以得到 wff；除此之外没有 wff。所有 wff 组成的集合记为  $WFF$ 。

换句话说，wff 是从命题变元出发，反复用逻辑联词（并配上括号）拼出来的有穷长句子。例如  $A, (A \wedge B), (A \rightarrow (B \wedge A))$  等。每应用一次规则 (2)，公式中恰好增加一个逻辑联词和一对括号。注意， $(A)$  不是 wff。

**定义 1.9** 称  $T \subseteq V$  对所有逻辑联词封闭，若对任意  $\alpha, \beta \in T$ ，都有  $(\neg\alpha), (\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \rightarrow \beta), (\alpha \leftrightarrow \beta) \in T$ 。

**定理 1.10**  $WFF$  是包含所有命题变元、且对所有逻辑联词封闭的最小集合。即：若  $T \subseteq V$  包含所有命题变元并对所有逻辑联词封闭，则  $WFF \subseteq T$ 。

**证明** 由定义 1.8 的规则 (1)， $WFF$  包含所有命题变元；由规则 (2)， $WFF$  对所有逻辑联词封闭。

设  $T \subseteq V$  包含所有命题变元并对所有逻辑联词封闭。若  $WFF \setminus T \neq \emptyset$ ，取  $\gamma \in WFF \setminus T$  使得  $\gamma$  中逻辑联词的个数最少。由于  $T$  已包含所有命题变元， $\gamma$  不是命题变元，从而至少含一个逻辑联词。由定义 1.8， $\gamma$  必具有形式  $(\neg\alpha)$  或  $(\alpha \square \beta)$ ，其中  $\square \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ ，且  $\alpha$ （以及二元情形下的  $\beta$ ）属于  $WFF$ 。这些子公式中逻辑联词的个数都严格小于  $\gamma$  中的个数，故由极小性它们都属于  $T$ 。再由  $T$  对逻辑联词封闭，得  $\gamma \in T$ ，矛盾。因此  $WFF \subseteq T$ 。□

**例 1.11** 若  $\alpha \in WFF$ ，则  $\alpha$  中左括号的个数等于右括号的个数。

**提示** 令  $T \subseteq V$  表示左右括号个数相等的句子（包括 “ $(A \rightarrow)$ ” 等病句）。可以验证（请验证！） $T$  包含所有命题变元，并且对所有逻辑联词封闭。由定理 1.10， $WFF \subseteq T$ 。□

**例 1.12** 若  $\alpha \in WFF$  并且  $\alpha$  不含  $\neg$  符号，则  $\alpha$  的长度为奇数。事实上， $\alpha$  的长度可以写成  $4k+1$  的形式，此时其中命题变元的个数为  $k+1$ 。因此  $(A)$  和  $(A \wedge B \wedge C)$  不是合式公式。

为便于阅读，许多括号可以省略<sup>1</sup>：

1. 最外层括号可以省略；
2.  $\neg\alpha$  总是被理解为  $(\neg\alpha)$ ；
3.  $A \square B \square C$ （其中两个  $\square$  相同）理解为  $(A \square (B \square C))$ ；
4.  $\wedge$  和  $\vee$  的优先级比  $\rightarrow, \leftrightarrow$  高： $\alpha \wedge \beta \rightarrow \gamma \vee \theta$  理解为  $(\alpha \wedge \beta) \rightarrow (\gamma \vee \theta)$ 。

例如： $A \rightarrow \neg B$  是  $(A \rightarrow (\neg B))$  的省略； $A \rightarrow B \rightarrow C$  是  $(A \rightarrow (B \rightarrow C))$  的省略<sup>2</sup>； $A \wedge B \wedge C$  是  $(A \wedge (B \wedge C))$  的省略；而  $A \wedge B \vee C$  应当添加括号。

**注 1.13** 根据直观可以初步判断， $A \wedge (B \vee C)$  与  $(A \wedge B) \vee C$  含义不同。更严格的验证需要等到引入赋值之后。（注意：严格验证也不应与直观矛盾太大。我们引入这些形式化工具，目的仍是刻画直观。）

<sup>1</sup>省略只是书写上的方便，并不修改定义 1.8：合式公式的标准写法仍须带齐括号。

<sup>2</sup>有的教材将  $A \rightarrow B \rightarrow C$  看作  $((A \rightarrow B) \rightarrow C)$  的省略，本讲义采用右结合。

## 1.2 赋值

合式公式只规定了句子的写法。要谈论真假，需要对命题变元赋值，再按联词的规则把真假传到整个公式。本节只回答：给定一个赋值  $v$ ，如何算出  $\bar{v}(\alpha)$ 。

本节  $S$  一般指有穷个命题变元的集合。

**定义 1.14** 称函数  $v : S \rightarrow \{0, 1\}$  是关于  $S$  的一个赋值 (truth assignment)。其中 1 表示真，0 表示假。

若  $|S| = n$ ，则一共有  $2^n$  个关于  $S$  的不同赋值。

**例 1.15** 一个赋值  $v : \{A_1, A_2, \dots, A_n\} \rightarrow \{0, 1\}$  也可以写作字符串  $v(A_1)v(A_2)\dots v(A_n)$ ，其中  $v(A_i)$  是 0 或 1。例如， $v(A_1) = 0, v(A_2) = 1, v(A_3) = 0$  可以写作 010。

**定义 1.16** 设  $S$  为部分或全部命题变元的集合。 $\bar{S}$  表示由  $S$  中的命题变元及逻辑联词按定义 1.8 生成的 wff 之集：规则 (1) 只取  $S$  中的命题变元，规则 (2) 不变。于是  $S \subseteq \bar{S} \subseteq WFF$ 。若  $S$  为全体命题变元，则  $\bar{S} = WFF$ ；若  $S = \{A_1, A_2, \dots, A_n\}$ ，则记  $\bar{S}$  为  $WFF(n)$ 。

**定义 1.17** 给定赋值  $v : S \rightarrow \{0, 1\}$ ，称  $\bar{v} : \bar{S} \rightarrow \{0, 1\}$  是  $v$  的一个扩张，如果它满足：

- 若  $A \in S$ ，则  $\bar{v}(A) = v(A)$ ；
- 若  $\alpha, \beta \in \bar{S}$ ，则
  - $\bar{v}(\neg\alpha) = 1 - \bar{v}(\alpha)$ ；
  - $\bar{v}(\alpha \wedge \beta) = \min\{\bar{v}(\alpha), \bar{v}(\beta)\}$ ；
  - $\bar{v}(\alpha \vee \beta) = \max\{\bar{v}(\alpha), \bar{v}(\beta)\}$ ；
  - $\bar{v}(\alpha \rightarrow \beta) = \begin{cases} 0 & \bar{v}(\alpha) = 1 \wedge \bar{v}(\beta) = 0 \\ 1 & \text{其他情况} \end{cases}$ ；
  - $\bar{v}(\alpha \leftrightarrow \beta) = \begin{cases} 1 & \bar{v}(\alpha) = \bar{v}(\beta) \\ 0 & \text{其他情况} \end{cases}$ 。

上述扩张条款是各联词的局部运算规则，可列成下表。这是联词本身怎么算；一个复合公式在所有赋值下的完整真值表，后文再引入。

| $A$ | $\neg A$ | $A$ | $B$ | $A \wedge B$ | $A \vee B$ | $A \rightarrow B$ | $A \leftrightarrow B$ |
|-----|----------|-----|-----|--------------|------------|-------------------|-----------------------|
| 0   | 1        | 0   | 0   | 0            | 0          | 1                 | 1                     |
| 1   | 0        | 0   | 1   | 0            | 1          | 1                 | 0                     |
|     |          | 1   | 0   | 0            | 1          | 0                 | 0                     |
|     |          | 1   | 1   | 1            | 1          | 1                 | 1                     |

Table 1: 基本联词的运算表

对着表中  $\rightarrow$  的一列，可以理解蕴涵的直观：当前提为假时蕴涵为真；仅当前提真而结论假时蕴涵为假。

**例 1.18**

- 若  $1 + 1 = 3$ ，则小帅考上了晓庄。(前提假，整句为真。)
- 若  $1 + 1 = 2$ ，则小帅考上了晓庄。(真假取决于小帅是否考上。)
- 若小帅考上了晓庄，则  $1 + 1 = 3$ 。(若小帅考上则为假。)
- 若小帅考上了晓庄，则  $1 + 1 = 2$ 。(结论真，整句为真。)

**定理 1.19** 任意赋值  $v : S \rightarrow \{0, 1\}$  都有唯一的一个扩张  $\bar{v} : \bar{S} \rightarrow \{0, 1\}$ 。

**证明** 略。

□

借助  $\bar{v}$ ，我们可以没有歧义地判断一个合式公式在给定赋值下的真假。

**例 1.20** 在赋值  $v(A_1) = 0, v(A_2) = 1$  下， $\bar{v}(A_1 \wedge A_2) = 0$ 。

为了叙述方便，我们会说：在赋值 01 下， $A_1 \wedge A_2$  为假，或取值为 0。

**例 1.21** 求在赋值 110 下， $(A_1 \rightarrow A_2 \rightarrow A_3) \leftrightarrow ((A_1 \wedge A_2) \rightarrow A_3)$  的真假。

以上是「给定  $v$ ，算出  $\bar{v}(\alpha)$ 」。反过来：固定  $\alpha$ ，找出使它为真（或为假）的赋值。

**定义 1.22** 若  $\bar{v}(\alpha) = 1$ ，则称  $v$  是  $\alpha$  的成真赋值，或者  $v$  满足  $\alpha$ 。若  $\bar{v}(\alpha) = 0$ ，则称  $v$  是  $\alpha$  的成假赋值，或者  $v$  不满足  $\alpha$ 。若  $\Sigma \subseteq WFF$ ，我们称  $\bar{v}(\Sigma) = 1$ ，如果对任意  $\alpha \in \Sigma$ ，都有  $\bar{v}(\alpha) = 1$ 。此时，我们说  $v$  满足  $\Sigma$ ，或者  $v$  是  $\Sigma$  的一个成真赋值。

**注 1.23** 若  $\Sigma$  涉及无穷个命题变元，我们需要将赋值的定义进行一些自然的改变。即，允许其定义域是无穷个命题标识符的集合。

**例 1.24** 找出  $A \wedge (B \vee \neg C)$  的所有成真赋值。

**例 1.25** 找出  $\neg(A \rightarrow B) \wedge C$  的所有成假赋值。

把全部成真赋值与全部成假赋值合在一起，就是下一节的真值表。

### 1.3 真值表

若  $\alpha$  的命题变元是  $A_1, \dots, A_n$ ，则共有  $2^n$  个赋值。把每个赋值下的  $\bar{v}(\alpha)$  列成表，称为  $\alpha$  的真值表。表 1 是五个联词的运算表；这里是复合公式的完整表。

**例 1.26 (真值表)** 列出  $(A_1 \rightarrow A_2 \rightarrow A_3) \leftrightarrow ((A_1 \wedge A_2) \rightarrow A_3)$  的真值表。赋值 110 那一行前面已经算过，现在补全其余 7 行。

**定义 1.27** 若  $\alpha$  在所有赋值下均为真，即真值表每一行都是 1，则称  $\alpha$  为永真式；若在所有赋值下均为假，则称  $\alpha$  为永假式。

$A \vee \neg A$  为永真式， $A \wedge \neg A$  为永假式。

**例 1.28**  $P \rightarrow Q$  和  $Q \rightarrow P$  都不是永真式，但  $(P \rightarrow Q) \vee (Q \rightarrow P)$  是永真式。

**例 1.29** 是否是永真式：

- $A \rightarrow B \rightarrow A$
- $(A \rightarrow B) \rightarrow (A \rightarrow B \rightarrow C) \rightarrow (A \rightarrow C)$
- $(\neg B \rightarrow A) \rightarrow (\neg B \rightarrow \neg A) \rightarrow B$

真值表把一个公式的全部语义收成一张有穷表。下一节把它看成一个函数。

### 1.4 布尔函数

真值表的每一行是一个输入  $(x_1, \dots, x_n) \in \{0, 1\}^n$ ，最后一列是输出。因此一张真值表就是一个从  $\{0, 1\}^n$  到  $\{0, 1\}$  的函数。

**定义 1.30** 函数  $B : \{0, 1\}^n \rightarrow \{0, 1\}$  称为  $n$  元布尔函数。 $BOOL_n$  表示所有的  $n$  元布尔函数， $BOOL$  表示所有布尔函数。

$$|BOOL_n| = 2^{2^n}.$$

**例 1.31** 表 1 中  $A \wedge B$  的那一列就是二元布尔函数  $B : \{0, 1\}^2 \rightarrow \{0, 1\}$ ，满足  $B(0, 0) = 0$ ， $B(0, 1) = 0$ ， $B(1, 0) = 0$ ，以及  $B(1, 1) = 1$ 。

**定义 1.32** 给定  $\alpha \in WFF(n)$ <sup>3</sup>。我们定义

$$B_\alpha(x_1, x_2, \dots, x_n) = \bar{v}(\alpha),$$

其中赋值  $v$  满足  $v(A_i) = x_i \in \{0, 1\}$  确定。称  $B_\alpha$  为  $\alpha$  诱导的布尔函数。

例 1.31 中的布尔函数可以记为  $B_{A \wedge B}$ 。

下面三件事是同一个对象： $\bar{v}(\alpha)$  随  $v$  的变化、 $\alpha$  的真值表、布尔函数  $B_\alpha$ 。永真式诱导常值函数 1，永假式诱导常值函数 0。

根据定义 1.17，联词在函数层面就是逐点运算：

**命题 1.33** 对任意  $\alpha, \beta \in WFF(n)$ ,

1.  $B_{\neg\alpha} = 1 - B_\alpha$ ;
2.  $B_{\alpha \wedge \beta} = \min\{B_\alpha, B_\beta\}$ ;
3.  $B_{\alpha \vee \beta} = \max\{B_\alpha, B_\beta\}$ ;
4.  $B_{\alpha \rightarrow \beta} = \begin{cases} 0 & B_\alpha = 1 \text{ 且 } B_\beta = 0 \\ 1 & \text{其他} \end{cases}$ ;
5.  $B_{\alpha \leftrightarrow \beta} = \begin{cases} 1 & B_\alpha = B_\beta \\ 0 & \text{其他} \end{cases}$ 。

**证明** 略。 □

公式作为字符串可以很长、写法可以很不同；语义上真正起作用的是  $B_\alpha$ 。后文把诱导相同布尔函数的公式视为可互换。

**例 1.34** 对比  $A \rightarrow B \rightarrow C$  与  $(A \wedge B) \rightarrow C$  诱导的布尔函数。

## 1.5 等值

既然语义由  $B_\alpha$  完全决定，两个公式若诱导同一函数，在赋值的眼光下就无法区分。

**定义 1.35** 称  $\alpha$  与  $\beta$  等值（或等价），如果  $B_\alpha = B_\beta$ 。

等值的公式作为字符串可以不同，但真值表相同。等值式就是保持  $B_\alpha$  不变的改写规则：下表每一行左右两边等值。

|         | 公式                                                | 等值于                              |
|---------|---------------------------------------------------|----------------------------------|
| 双重否定    | $\neg\neg A$                                      | $A$                              |
| 幂等律     | $A \wedge A$                                      | $A$                              |
|         | $A \vee A$                                        | $A$                              |
| 交换律     | $A \wedge B$                                      | $B \wedge A$                     |
|         | $A \vee B$                                        | $B \vee A$                       |
| 结合律     | $(A \vee B) \vee C$                               | $A \vee (B \vee C)$              |
|         | $(A \wedge B) \wedge C$                           | $A \wedge (B \wedge C)$          |
| 分配律     | $A \vee (B \wedge C)$                             | $(A \vee B) \wedge (A \vee C)$   |
|         | $A \wedge (B \vee C)$                             | $(A \wedge B) \vee (A \wedge C)$ |
| 德摩根律    | $\neg(A \vee B)$                                  | $\neg A \wedge \neg B$           |
|         | $\neg(A \wedge B)$                                | $\neg A \vee \neg B$             |
| 吸收律     | $A \vee (A \wedge B)$                             | $A$                              |
|         | $A \wedge (A \vee B)$                             | $A$                              |
| 蕴涵等值式   | $A \rightarrow B$                                 | $\neg A \vee B$                  |
| 等价等值式   | $(A \rightarrow B) \wedge (B \rightarrow A)$      | $A \leftrightarrow B$            |
| 假言易位    | $A \rightarrow B$                                 | $\neg B \rightarrow \neg A$      |
| 等价否定等值式 | $A \leftrightarrow B$                             | $\neg A \leftrightarrow \neg B$  |
| 归谬论     | $(A \rightarrow B) \wedge (A \rightarrow \neg B)$ | $\neg A$                         |

Table 2: 常见等值式

我们用 1 表示  $A \vee \neg A$ ，用 0 表示  $A \wedge \neg A$ ：它们分别是常值函数 1 与 0 的代表元。任意永真式都与 1 等值，任意永假式都与 0 等值。

<sup>3</sup>回顾定义 1.16。

|     | 公式                | 等值于 |
|-----|-------------------|-----|
| 排中律 | $A \vee \neg A$   | 1   |
| 矛盾律 | $A \wedge \neg A$ | 0   |
| 零律  | $A \vee 1$        | 1   |
|     | $A \wedge 0$      | 0   |
| 同一律 | $A \vee 0$        | $A$ |
|     | $A \wedge 1$      | $A$ |

Table 3: 含 0, 1 的等值式

表 2 中的  $A, B$  是命题变元。将它们整体换成任意公式后，等值关系仍然成立：两边的布尔函数只依赖于变元的取值，与变元写成哪个公式无关。下面的替换定理把这件事说清楚。

**定义 1.36**  $\alpha \in WFF$  为  $\beta \in WFF$  的子公式，如果  $\alpha$  作为连续子串出现在  $\beta$  中。

例如， $\neg A$  是  $B \rightarrow \neg A$  的子公式。 $A \vee B \rightarrow A \wedge B \rightarrow A \vee B$  的子公式有  $A \vee B, A \wedge B, A \wedge B \rightarrow A \vee B$ ，以及它自身  $A \vee B \rightarrow A \wedge B \rightarrow A \vee B$ 。

将子公式替换为等值的公式不改变原公式的真值表：

**引理 1.37** 若  $\alpha$  与  $\beta$  等值，则

1.  $\neg \alpha$  与  $\neg \beta$  等值；
2.  $\alpha \vee \gamma$  与  $\beta \vee \gamma$  等值；
3.  $\alpha \wedge \gamma$  与  $\beta \wedge \gamma$  等值；
4.  $\gamma \rightarrow \alpha$  与  $\gamma \rightarrow \beta$  等值；
5.  $\alpha \rightarrow \gamma$  与  $\beta \rightarrow \gamma$  等值；
6.  $\gamma \leftrightarrow \alpha$  与  $\gamma \leftrightarrow \beta$  等值。

**证明** 我们举一个例子： $B_{\neg \alpha} = 1 - B_{\alpha} = 1 - B_{\beta} = B_{\neg \beta}$ 。其他情况类似。  $\square$

实际上，我们可以运用递归证明下述更一般的叙述：

**定理 1.38** 如果  $\alpha$  是  $\sigma$  的子公式， $\sigma'$  是将其（部分或全部的）子公式  $\alpha$  替换为  $\beta$  形成的 wff。若  $\alpha$  与  $\beta$  等值，则  $\sigma$  与  $\sigma'$  等值。

**证明** 略。（严格证明需要用到递归严格的叙述，并非本节课程的重点）。  $\square$

## 1.6 表达能力

回顾：一个公式的写法不影响其语义，其语义由其诱导的布尔函数决定。那么，是否所有的布尔函数都能被一个公式诱导？换句话说，公式的表达能力是否足够强？

**例 1.39** 写出所有二元布尔函数对应的诱导公式。

通过这个例子，我们得到一个结论，任意  $G : \{0, 1\}^2 \rightarrow \{0, 1\}$  都存在  $\alpha \in WFF$  满足  $G = B_{\alpha}$ 。那么对一个三元布尔函数呢？

**问题 1.40** 一个布尔函数  $B(s_1, s_2, s_3)$  满足  $B(s_1, s_2, s_3) = 1$  当且仅当  $s_1, s_2, s_3$  中有两个或三个为 1。是否存在  $\alpha \in WFF$ ，使得  $B_{\alpha} = B$ ？

**主析取范式** 我们不妨先考虑最简单的布尔函数。常值函数 0 可以被公式诱导：

**引理 1.41** 若  $G = 0$ ，则  $G = B_{A_1 \wedge \neg A_1}$ 。  $\square$

再难一点，在 1 个点取值为 1：

**引理 1.42** 若  $G : \{0, 1\}^n \rightarrow \{0, 1\}$  只在  $(s_1, s_2, \dots, s_n)$  处取值为 1，则存在  $\alpha \in WFF$  满足  $G = B_{\alpha}$ 。

**定义 1.43** 给定  $s_1, s_2, \dots, s_n \in \{0, 1\}$ , 令  $\ell_i = A_i$  如果  $s_i = 1$ , 令  $\ell_i = \neg A_i$  如果  $s_i = 0$ 。用  $m_{s_1 s_2 \dots s_n}$  表示公式  $\ell_1 \wedge \ell_2 \wedge \dots \wedge \ell_n$ 。

注意到  $m_{s_1 s_2 \dots s_n}$  的成真赋值只有  $s_1 s_2 \dots s_n$ 。

引理 1.42 的证明  $G = B_{m_{s_1 s_2 \dots s_n}}$ 。

□

**定义 1.44**  $m_{s_1 s_2 \dots s_n}$  称为 (关于命题变元  $A_1, A_2, \dots, A_n$ ) 的极小项。

**例 1.45**  $m_{000}, m_{001}, m_{010}, m_{011}, m_{100}, m_{101}, m_{110}, m_{111}$  为关于  $A_1, A_2, A_3$  的所有极小项。请写出这些极小项的公式形式。

**定义 1.46** 若干个极小项的析取称为主析取范式。

**定理 1.47** 每个布尔函数都能被某个公式诱导: 给定非 0 布尔函数  $G: \{0, 1\}^n \rightarrow \{0, 1\}$ , 存在主析取范式  $\alpha$  满足  $G = B_\alpha$ 。

**证明** 假设  $G$  在  $(s_{i1}, s_{i2}, \dots, s_{in})$  处取值为 1,  $i = 1, \dots, k$ 。令  $\alpha_i$  为  $m_{s_{i1} s_{i2} \dots s_{in}}$ , 则  $G = B_{\alpha_1 \vee \alpha_2 \vee \dots \vee \alpha_k}$ 。

□

**注 1.48** 主析取范式就是真值表的另一种写法。应当学会如何相互解读真值表和范式。

**例 1.49** 回到问题 1.40, 由于其成真赋值为 011, 101, 110, 111, 因此,  $\alpha$  可取为  $m_{011} \vee m_{101} \vee m_{110} \vee m_{111}$ 。

**主合取范式.** 作为定义 1.43 的镜像, 我们定义极大项。

**定义 1.50** 给定  $s_1, s_2, \dots, s_n \in \{0, 1\}$ , 令  $\ell_i = A_i$  如果  $s_i = 0$ , 令  $\ell_i = \neg A_i$  如果  $s_i = 1$ 。用  $M_{s_1 s_2 \dots s_n}$  表示公式  $\ell_1 \vee \ell_2 \vee \dots \vee \ell_n$ , 称之为 (关于命题变元  $A_1, A_2, \dots, A_n$ ) 的极大项。若干个极大项的合取称为主合取范式。

注意到  $M_{s_1 s_2 \dots s_n}$  的成假赋值只有  $s_1 s_2 \dots s_n$ 。

**例 1.51**  $M_{000}, M_{001}, M_{010}, M_{011}, M_{100}, M_{101}, M_{110}, M_{111}$  为关于  $A_1, A_2, A_3$  的所有极大项。请写出这些极大项的公式形式。

**定理 1.52** 每个布尔函数都能被某个公式诱导: 给定非恒 1 布尔函数  $G: \{0, 1\}^n \rightarrow \{0, 1\}$ , 存在主合取范式  $\alpha$  满足  $G = B_\alpha$ 。

□

## 一些名词

这一节对主析取范式和主合取范式的名词由来进行展开。先有简单合取式, 由此构建析取范式, 析取范式中的重要特例被称为主析取范式。主合取范式的命名与之类似。

**定义 1.53** 简单析取式是指由有穷个命题变元及其否定构成的析取式; 简单合取式是指由有穷个命题变元及其否定构成的合取式。

例如,  $A, \neg A, A \vee B, A \vee \neg A, A \vee \neg B$  都是简单析取式。简单合取式不必出现全部变元, 因此一般可以有多个成真赋值。见习题 1.8。

**定义 1.54** 有穷个简单合取式构成的析取式称为析取范式; 有穷个简单析取式构成的合取式称为合取范式。

由于  $A$  和  $\neg A$  既是简单合取式, 也是简单析取式, 因此简单合 (析) 取式可以看作是合取范式, 也可以看作析取范式。

**例 1.55** 极小项是简单合取式, 极大项是简单析取式。两个不同极小项的合取是永假式; 两个不同极大项的析取是永真式。

### ★ 重要

极小项的下标是其成真赋值

### 💡 提示

主析取范式无法表达永假式。

### ★ 重要

极大项的下标是其成假赋值

### 💡 提示

请自行证明定理 1.52。

**全功能集.** 注意到主析取范式只使用逻辑联词  $\neg, \wedge, \vee$ , 不必动用全部五个联词。自然要问: 哪些联词的子集已经够用?

在定义 1.8 中, 若允许的逻辑联词集合为  $C$ , 则其生成的合式公式记为  $WFF_C$ 。

**定理 1.56** 仅用  $\wedge, \vee, \neg$  也足以诱导全部布尔函数: 对任意  $G : \{0, 1\}^n \rightarrow \{0, 1\}$ , 存在  $\alpha \in WFF_{\{\wedge, \vee, \neg\}}$  满足  $G = B_\alpha$ 。  $\square$

**定义 1.57** 设  $C$  是一些逻辑联词。如果每个布尔函数都能被  $WFF_C$  中某个公式诱导, 则称  $C$  为全功能集。

**例 1.58**  $\{\neg, \wedge, \vee\}, \{\neg, \wedge\}, \{\neg, \vee\}, \{\neg, \rightarrow\}$  都是全功能集。

**例 1.59** 定义联结词与非联结词  $p \uparrow q$  为  $\neg(p \wedge q)$ ; 或非联结词  $p \downarrow q$  为  $\neg(p \vee q)$ 。证明  $\{\uparrow\}$  和  $\{\downarrow\}$  为全功能集。或非部分见习题 1.5。

**例 1.60**  $\{\neg\}, \{\wedge\}, \{\vee\}$  都不是全功能集。见习题 1.6。

**证明** 先看  $\{\wedge\}$ 。直观上, 全 1 赋值下合取仍为 1, 故常值函数 0 不能被  $WFF_{\{\wedge\}}$  诱导。对  $\alpha \in WFF_{\{\wedge\}}$  的构造作归纳, 证明  $B_\alpha(1, \dots, 1) = 1$ :

1. 若  $\alpha$  为命题变元  $A_i$ , 则  $B_{A_i}(1, \dots, 1) = 1$ 。
2. 若  $\alpha$  为  $\alpha_1 \wedge \alpha_2$ , 且已有  $B_{\alpha_1}(1, \dots, 1) = B_{\alpha_2}(1, \dots, 1) = 1$ , 则由命题 1.33,  $B_\alpha(1, \dots, 1) = \min\{1, 1\} = 1$ 。

因此不存在  $\alpha \in WFF_{\{\wedge\}}$  使得  $B_\alpha$  为常值 0。

$\{\wedge, \vee\}$  同理: 全 1 赋值下  $\vee$  也保持为 1, 同样的归纳给出  $B_\alpha(1, \dots, 1) = 1$ 。

$\{\neg\}$  生成的公式都形如  $\neg \dots \neg A_i$ , 诱导函数只依赖一个变元, 不能诱导二元布尔函数。  $\square$

**定理 1.47** 只保证存在某个公式诱导给定的布尔函数。下一节给出从真值表直接读出的标准写法。

## 1.7 蕴涵

前面讨论的是单个公式的语义, 以及两个公式是否诱导同一布尔函数。本节引入语义蕴涵  $\models$ : 从一组前提  $\Sigma$  出发, 哪些结论必然成立。

**定义 1.61**  $\Sigma \subseteq WFF$ 。  $\Sigma \models \alpha$  如果所有满足  $\Sigma$  的赋值 (见定义 1.22) 也满足  $\alpha$ 。

为了方便, 我们将  $\Sigma \cup \{\alpha_1, \alpha_2, \dots, \alpha_n\} \models \beta$  写作

$$\Sigma, \alpha_1, \dots, \alpha_n \models \beta.$$

例如,  $\{\alpha, \beta\} \models \gamma$  可以写成  $\alpha, \beta \models \gamma$ 。特别地,  $\emptyset \models \alpha$  也写作  $\models \alpha$ , 这与“ $\alpha$  为永真式”一致。

**例 1.62** 下列哪些是对的?

1.  $A, B \models A \wedge B$
2. 对所有的  $\beta \in WFF$ ,  $\{A, \neg A\} \models \beta$
3.  $\neg(A \wedge B) \models \neg A \wedge \neg B$
4.  $A, A \rightarrow B \models B$
5.  $(A \wedge B) \rightarrow C \models (A \rightarrow C) \vee (B \rightarrow C)$

见习题 1.1。

**定理 1.63**  $\alpha \models \beta$  当且仅当对所有  $x_1, x_2, \dots, x_n \in \{0, 1\}$ ,  $B_\alpha(x_1, x_2, \dots, x_n) \leq B_\beta(x_1, x_2, \dots, x_n)$ 。

因此,  $\alpha \models \beta$  且  $\beta \models \alpha$  当且仅当  $B_\alpha = B_\beta$ , 即  $\alpha$  与  $\beta$  等值。记作  $\alpha \models \beta$ 。

**定理 1.64**  $\Sigma, \alpha \models \beta$  当且仅当  $\Sigma \models \alpha \rightarrow \beta$ 。

**证明**  $(\Rightarrow)$  若不然, 则存在一个赋值  $v$  满足  $\Sigma$ , 并且  $\bar{v}(\alpha \rightarrow \beta) = 0$ , 即  $\bar{v}(\alpha) = 1$  且  $\bar{v}(\beta) = 0$ 。注意到  $v$  满足  $\Sigma, \alpha$ , 由于  $\Sigma, \alpha \models \beta$ , 我们得到

$$\bar{v}(\beta) = 1,$$

矛盾。

$(\Leftarrow)$  任取  $v$  满足  $\Sigma, \alpha$ , 则  $\bar{v}(\alpha \rightarrow \beta) = 1$ 。由于  $\bar{v}(\alpha) = 1$ , 所以  $\bar{v}(\beta) = 1$ 。  $\square$

**推论 1.65**  $\alpha \models \beta$  当且仅当  $\alpha \leftrightarrow \beta$  为永真式。等价地,  $\alpha \models \beta$  当且仅当  $\models \alpha \leftrightarrow \beta$ 。  $\square$

**注 1.66** 当我们作为 wff 写下  $\alpha \leftrightarrow \beta$  时, 这是纯语法的, 和赋值没有关系。我们可以说  $\alpha$  和  $\beta$  等值当且仅当  $\models \alpha \leftrightarrow \beta$ , 但不能仅仅说当且仅当  $\alpha \leftrightarrow \beta$ 。

逐个检查赋值的工作量总是巨大的, 并且是机械的。下一节讨论如何用形式推理来「证明」 $\Sigma \models \sigma$ 。

## 1.8 推理理论

**什么是证明。** 本节在命题逻辑中探讨什么是“证明”：用有穷步形式推演代替穷尽赋值。由于  $\{\neg, \rightarrow\}$  是全功能集, 我们在本节中将公式限定为仅有  $\neg, \rightarrow$  构成的公式。这么约定是合理的, 因为我们最终关心的是语义而非公式本身。在第 1.8.4 节中, 我们将给出如何处理含有  $\vee, \wedge, \leftrightarrow$  的公式的证明技巧。

**定义 1.67** 令  $\Lambda$  表示下列形式的公式的集合：

$$\begin{aligned}\Lambda_1: & \alpha \rightarrow \beta \rightarrow \alpha \\ \Lambda_2: & (\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \gamma) \\ \Lambda_3: & (\neg\beta \rightarrow \alpha) \rightarrow (\neg\beta \rightarrow \neg\alpha) \rightarrow \beta\end{aligned}$$

称这些为逻辑公理。

根据例 1.29 及定理 1.38, 逻辑公理都是永真式。

**定义 1.68** 给定  $\Sigma \subseteq WFF$  和  $\alpha$ 。一个从  $\Sigma$  到  $\alpha$  的推理或证明是一个有穷序列

$$\alpha_0, \alpha_1, \dots, \alpha_n = \alpha$$

其中对任意  $i \leq n$ ,  $\alpha_i \in \Lambda \cup \Sigma$  或通过 *Modus Ponens* 规则得到, 即, 存在  $j, k < i$ , 其中  $\alpha_k$  为  $\alpha_j \rightarrow \alpha_i$ 。此时, 称  $\alpha$  为  $\Sigma$  的定理, 并记作  $\Sigma \vdash \alpha$ 。

**例 1.69** 证明  $\{A \rightarrow B \rightarrow C, A, B\} \vdash C$ 。

**证明** 我们有如下推理过程：

1.  $A \rightarrow B \rightarrow C$  (已知)
2.  $A$  (已知)
3.  $B \rightarrow C$  (1,2,MP)
4.  $B$  (已知)
5.  $C$  (3,4,MP)

$\square$

公理本身能否推出最简单的重言式？下面给出一个完全展开的推理。

**例 1.70**  $\vdash \alpha \rightarrow \alpha$ 。

**证明** 我们有如下推理过程：

1.  $(\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha) \rightarrow (\alpha \rightarrow (\alpha \rightarrow \alpha)) \rightarrow (\alpha \rightarrow \alpha)$  ( $\Lambda_2$ , 取  $\beta$  为  $\alpha \rightarrow \alpha$ ,  $\gamma$  为  $\alpha$ )

2.  $\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha$  ( $\Delta_1$ , 取  $\beta$  为  $\alpha \rightarrow \alpha$ )
3.  $(\alpha \rightarrow (\alpha \rightarrow \alpha)) \rightarrow (\alpha \rightarrow \alpha)$  (1,2,MP)
4.  $\alpha \rightarrow (\alpha \rightarrow \alpha)$  ( $\Delta_1$ , 取  $\beta$  为  $\alpha$ )
5.  $\alpha \rightarrow \alpha$  (3,4,MP)

□

若每条重言式都要如此展开，推理将难以书写。目前选取的公理并不直观，目的是公理尽量少、规则尽量少。后面给出符合直观的证明技巧。先记下  $\vdash$  的几条一般性质。

- 命题 1.71**
1. 如果  $\Gamma \subseteq \Delta$  且  $\Gamma \vdash \alpha$ ，那么  $\Delta \vdash \alpha$ 。
  2.  $\Gamma \vdash \alpha$  当且仅当存在  $\Gamma$  的一个有限子集  $\Gamma_0$ ，使得  $\Gamma_0 \vdash \alpha$ 。
  3. 如果  $\Delta \vdash \alpha$ ，并且对任意  $\beta \in \Delta$ ，都有  $\Gamma \vdash \beta$ ，那么  $\Gamma \vdash \alpha$ 。

能证的都是对的：

**定理 1.72 (Soundness)** 如果  $\Sigma \vdash \alpha$ ，则  $\Sigma \models \alpha$ 。

**证明** 设  $\alpha_0, \alpha_1, \dots, \alpha_n = \alpha$  为  $\Sigma$  推  $\alpha$  的序列。对  $i$  归纳证明：对所有  $i \leq n$ ， $\Sigma \models \alpha_i$ 。若  $\alpha_i \in \Sigma$ ，显然  $\Sigma \models \alpha_i$ 。若  $\alpha_i$  为逻辑公理，则  $\alpha_i$  永真，故  $\Sigma \models \alpha_i$ 。若  $\alpha_i$  由  $\alpha_j$  与  $\alpha_k = \alpha_j \rightarrow \alpha_i$  ( $j, k < i$ ) 经 MP 得到，则由归纳假设  $\Sigma \models \alpha_j$  且  $\Sigma \models \alpha_j \rightarrow \alpha_i$ ，从而  $\Sigma \models \alpha_i$ 。 □

- 引理 1.73**
- 如果  $\Sigma \vdash \alpha, \alpha \rightarrow \beta$ ，则  $\Sigma \vdash \beta$ 。
  - 如果  $\Sigma \vdash \alpha_1, \alpha_2, \dots, \alpha_n, \alpha_1 \rightarrow \alpha_2 \rightarrow \dots \rightarrow \alpha_n \rightarrow \beta$ ，则  $\Sigma \vdash \beta$ 。

**证明** 利用命题 1.71 中的第 3 条。 □

**证明技巧 1：演绎定理。** 演绎定理把「带前提的推理」改写成蕴涵式，与语义上的定理 1.64 平行。

**定理 1.74**  $\Sigma, \alpha \vdash \beta$  当且仅当  $\Sigma \vdash \alpha \rightarrow \beta$ 。

**证明** ( $\Leftarrow$ ) 由于  $\Sigma, \alpha \vdash \alpha, \alpha \rightarrow \beta$ ，由引理 1.73 知  $\Sigma, \alpha \vdash \beta$ 。

( $\Rightarrow$ ) 考虑  $\Sigma, \alpha$  到  $\beta$  的一个推理序列

$$\beta_0, \beta_1, \dots, \beta_n = \beta$$

我们对  $i$  作归纳证明  $\Sigma \vdash \alpha \rightarrow \beta_i$ 。

**情形 1：** 如果  $\beta_i$  属于  $\Lambda \cup \Sigma$ ，那么  $\Sigma \vdash \beta_i$ 。由  $\Delta_1, \vdash \beta_i \rightarrow \alpha \rightarrow \beta_i$ ，因此  $\Sigma \vdash \alpha \rightarrow \beta_i$ 。

**情形 2：** 如果  $\beta_i$  是  $\alpha$ ，由例 1.70， $\vdash \alpha \rightarrow \alpha$ ，因此  $\Sigma \vdash \alpha \rightarrow \alpha$ 。

**情形 3：** 如果存在  $j, k < i$  其中  $\beta_k$  为  $\beta_j \rightarrow \beta_i$ 。由归纳假设，

$$\Sigma \vdash \alpha \rightarrow \beta_j, \alpha \rightarrow \beta_j \rightarrow \beta_i$$

再由  $\Delta_2$  知  $\vdash (\alpha \rightarrow \beta_j) \rightarrow (\alpha \rightarrow \beta_j \rightarrow \beta_i) \rightarrow (\alpha \rightarrow \beta_i)$ ，故  $\Sigma \vdash \alpha \rightarrow \beta_i$ 。 □

- 例 1.75**
1.  $\{\alpha \rightarrow \beta, \beta \rightarrow \gamma\} \vdash \alpha \rightarrow \gamma$ 。
  2.  $\{\alpha \rightarrow (\beta \rightarrow \gamma), \beta\} \vdash \alpha \rightarrow \gamma$ 。

下面的反证法把“否定结论导致矛盾”改写成肯定结论。

**证明技巧 2：反证法。**

**定义 1.76**  $\Sigma$  是不相容的，如果存在某个  $\beta \in WFF$ ，满足  $\Sigma \vdash \beta, \neg \beta$ 。

**引理 1.77** 如果  $\Sigma$  不相容，则对任意  $\beta$ ， $\Sigma \vdash \beta$ 。

**证明**

1. 设  $\Sigma \vdash \alpha, \neg\alpha$ 。
2.  $\vdash \alpha \rightarrow \neg\beta \rightarrow \alpha$  ( $\Lambda_1$ )
3.  $\vdash \neg\alpha \rightarrow \neg\beta \rightarrow \neg\alpha$  ( $\Lambda_1$ )
4.  $\Sigma \vdash \neg\beta \rightarrow \alpha$  (1,2,MP)
5.  $\Sigma \vdash \neg\beta \rightarrow \neg\alpha$  (1,3,MP)
6.  $\vdash (\neg\beta \rightarrow \alpha) \rightarrow (\neg\beta \rightarrow \neg\alpha) \rightarrow \beta$  ( $\Lambda_3$ )
7.  $\Sigma \vdash \beta$  (4,5,6,MP)

□

**定理 1.78** 如果  $\Sigma, \neg\varphi$  不相容, 则  $\Sigma \vdash \varphi$ 。

证明

1.  $\Sigma, \neg\varphi \vdash \varphi$
2.  $\Sigma \vdash \neg\varphi \rightarrow \varphi$
3.  $\vdash \neg\varphi \rightarrow \neg\varphi$  (例 1.70)
4.  $\vdash (\neg\varphi \rightarrow \varphi) \rightarrow (\neg\varphi \rightarrow \neg\varphi) \rightarrow \varphi$  ( $\Lambda_3$ )
5.  $\Sigma \vdash \varphi$  (引理 1.73)

□

**例 1.79**  $\vdash \neg\neg\alpha \rightarrow \alpha$ 。这是因为  $\neg(\neg\alpha)$  和  $\neg\alpha$  不相容, 所以  $\neg\neg\alpha \vdash \alpha$ , 即  $\vdash \neg\neg\alpha \rightarrow \alpha$ 。

**例 1.80**  $\vdash \alpha \rightarrow \neg\neg\alpha$ 。

证明 由上一例,  $\vdash \neg\neg\neg\alpha \rightarrow \neg\alpha$ 。因此  $\{\alpha, \neg\neg\neg\alpha\}$  推出  $\alpha$  与  $\neg\alpha$ , 不相容。由定理 1.78,  $\alpha \vdash \neg\neg\alpha$ 。再由定理 1.74,  $\vdash \alpha \rightarrow \neg\neg\alpha$ 。 □

由这个例子, 我们得到定理 1.78 的另一个叙述。

**定理 1.81** 如果  $\Sigma, \varphi$  不相容, 则  $\Sigma \vdash \neg\varphi$ 。

证明 因为  $\Sigma, \varphi$  不相容, 所以  $\Sigma, \neg\neg\varphi$  也不相容 (你能证明吗?)。 □

**例 1.82**  $\alpha \rightarrow \beta \vdash \neg\beta \rightarrow \neg\alpha$ 。

证明 因为  $\alpha \rightarrow \beta, \neg\beta, \alpha$  不相容 (你能给出完整证明吗?)。 □

**证明技巧 3: 利用等值式**。前面的推理只使用  $\neg, \rightarrow$ 。完全性保证语义蕴涵可由形式证明得到, 因而可把容易验证的等值式当作推理中的合法改写, 从而处理含  $\vee, \wedge, \leftrightarrow$  的公式。

**定理 1.83 (Completeness)** 如果  $\Sigma \models \alpha$ , 则  $\Sigma \vdash \alpha$ 。

证明 不在本讲义范畴内。 □

据此有:

**定理 1.84** 若  $\alpha \models \beta$ ,  $\Sigma, \alpha \vdash \gamma$ , 当且仅当  $\Sigma, \beta \vdash \gamma$ 。

若  $\alpha \models \beta$ , 则  $\Sigma \vdash \alpha$  当且仅当  $\Sigma \vdash \beta$ 。

证明 我们只证明  $\Rightarrow$ 。由  $\beta \models \alpha$  得  $\vdash \beta \rightarrow \alpha$  (定理 1.64), 因此  $\vdash \beta \rightarrow \alpha$ 。因此  $\Sigma, \beta \vdash \alpha$ 。由于  $\Sigma, \alpha \vdash \gamma$ , 因此  $\Sigma, \beta \vdash \gamma$ 。

略。 □

如果我们有一个句子包含  $\vee, \wedge$ , 则我们可以用等值式将其转化为仅包含  $\rightarrow, \neg$  的句子。

**例 1.85** •  $P \rightarrow \neg(R \wedge S) \rightarrow \neg Q, P, \neg S \vdash \neg Q$   
 •  $A \rightarrow B, C \rightarrow D, A \vee C \vdash B \vee D$

**证明** (1) 令  $\Sigma = \{P \rightarrow \neg(R \wedge S) \rightarrow \neg Q, P, \neg S\}$ 。我们只需证明  $\Sigma \cup \{Q\}$  不相容:

1.  $P \rightarrow \neg(R \wedge S) \rightarrow \neg Q$  (已知)
2.  $P$  (已知)
3.  $\neg(R \wedge S) \rightarrow \neg Q$  (1, 2, MP)
4.  $Q \rightarrow R \wedge S$  (3, 等值式  $\alpha \rightarrow \beta \models \neg\beta \rightarrow \neg\alpha$ )
5.  $Q$  (已知)
6.  $R \wedge S$  (4,5,MP)
7.  $S$  (6)
8.  $\neg S$  (已知)

由 (7)(8) 得矛盾。

(2) 由于  $A \rightarrow B \models \neg B \rightarrow \neg A$ ,  $A \vee C \models \neg A \rightarrow C$  及  $B \vee D \models \neg B \rightarrow D$ , 由定理 1.84, 我们可以证明  $\neg B \rightarrow \neg A, C \rightarrow D, \neg A \rightarrow C, \neg B \vdash D$ : 而这只需要运用 3 次 MP 规则即可:

1.  $\neg B \rightarrow \neg A$  (已知)
2.  $\neg B$  (已知)
3.  $\neg A$  (1,2,MP)
4.  $\neg A \rightarrow C$  (已知)
5.  $C$  (3,4,MP)
6.  $C \rightarrow D$  (已知)
7.  $D$  (5,6,MP)

□

见习题 1.13。

## 1.9 习题

**习题 1.1** 以下是否正确?

1.  $A \vee C \leftrightarrow B \vee C \models A \leftrightarrow B$
2.  $A \wedge C \leftrightarrow B \wedge C \models A \leftrightarrow B$
3.  $\neg A \leftrightarrow \neg B \models A \leftrightarrow B$
4.  $\{A \rightarrow B, \neg B\} \models \neg A$
5.  $\{A \rightarrow B, B \rightarrow C\} \models A \rightarrow C$
6.  $(A \rightarrow B) \rightarrow B \models A \vee B$
7.  $(A \rightarrow B) \wedge (C \rightarrow D) \models A \wedge C \rightarrow B \wedge D$

**习题 1.2** 下面的陈述是否正确?

1. 若  $\Sigma \models \alpha$  或  $\Sigma \models \beta$ , 则  $\Sigma \models \alpha \vee \beta$
2. 若  $\Sigma \models \alpha \vee \beta$ , 则  $\Sigma \models \alpha$  或  $\Sigma \models \beta$ 。

**习题 1.3** 下面陈述是否正确?

1. 如果  $\Sigma \models \neg\alpha$ , 则  $\Sigma \not\models \alpha$ ;
2. 如果  $\Sigma \not\models \alpha$ , 则  $\Sigma \models \neg\alpha$ 。

**习题 1.4** 1. 已知  $\alpha \vee \gamma \models \beta \vee \gamma$ , 是否有  $\alpha \models \beta$ ?  
 2. 已知  $\alpha \wedge \gamma \models \beta \wedge \gamma$ , 是否有  $\alpha \models \beta$ ?

**习题 1.5** 或非联结词  $p \downarrow q$  为  $\neg(p \vee q)$ 。证明  $\{\downarrow\}$  为全功能集。

**习题 1.6** 证明  $\{\neg\}, \{\wedge\}, \{\vee\}$  都不是全功能集。

**习题 1.7** 引入逻辑联词  $+$ :  $A+B$  为真, 当且仅当  $A$  和  $B$  中有且仅有一个为真。证明  $\{\wedge, \leftrightarrow, +\}$  为全功能集, 但其中任意两个符号都不是全功能集。

**习题 1.8** 将公式 ①  $A \wedge \neg A$ , ②  $B$ , ③  $A \wedge B \wedge \neg C$ , ④  $A \vee B \vee \neg C$  填入下列类别:

- 简单合取式: \_\_\_\_\_
- 简单析取式: \_\_\_\_\_
- 合取范式: \_\_\_\_\_
- 析取范式: \_\_\_\_\_
- (关于  $A, B, C$  的) 极小项: \_\_\_\_\_
- (关于  $A, B, C$  的) 极大项: \_\_\_\_\_
- (关于  $A, B, C$  的) 主合取范式: \_\_\_\_\_
- (关于  $A, B, C$  的) 主析取范式: \_\_\_\_\_

**习题 1.9** 关于  $A, B, C$  的极大项  $M_{010}$  是 \_\_\_\_\_。

**习题 1.10** 关于  $A, B, C, D$  的极小项  $m_{13}$  是 \_\_\_\_\_。

**习题 1.11** 写出  $((A \wedge B) \rightarrow C) \rightarrow \neg A$  的主析取范式和主合取范式。(用极大(小)项表示即可)

**习题 1.12** 设  $E(A, B, C)$  为一个三元联词,  $E(A, B, C)$  为假当且仅当  $A, B, C$  中多数为假。写出  $E(A, B, C)$  的主析取范式和主合取范式(用极大(小)项表示即可)。

**习题 1.13** 证明(标注清楚理由):

1.  $\neg(P \wedge \neg Q), \neg Q \vee R, \neg R \vdash \neg P$
2.  $P \rightarrow Q \rightarrow S, Q, P \vee \neg R \vdash R \rightarrow S$
3.  $P \rightarrow Q \vdash P \rightarrow (P \wedge Q)$
4.  $Q \rightarrow P, Q \leftrightarrow S, S \leftrightarrow T, T \wedge R \vdash P \wedge Q \wedge S \wedge R$
5.  $(P \wedge Q) \rightarrow R, \neg R \vee S, \neg S, P \vdash \neg Q$

## §2 一阶逻辑

本章把命题逻辑的语义框架推广到带量词的语言: 先规定语言与公式, 再通过结构与赋值定义真假, 最后讨论蕴涵、等值与前束范式。本章目标:

1. 一阶逻辑的语言。
2. 真值、结构、模型。
3. 蕴涵、等值与前束范式。

### 2.1 语言

命题逻辑表达能力有限: 无法直接写出「存在无穷多素数」或「存在一个无穷集合」。讨论自然数与讨论集合时, 所需符号也不相同。因此对每种场景指定一套语言  $\mathcal{L}$ 。任何语言都包含下列逻辑符号:

- (1) 括号 (和), 逗号, ;
- (2) 逻辑联词  $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ ;
- (3) 全称量词  $\forall$ ;
- (4) 存在量词  $\exists$ ;
- (5) 变项  $v_0, v_1, v_2, \dots$ ;
- (6) 等号  $=$ 。

还可以包含下列非逻辑符号, 用来描述特定场景:

- (7) 对自然数  $n \geq 1$ , 有  $n$  元谓词符号  $P_0, P_1, P_2, \dots$ ;
- (8) 对自然数  $n \geq 1$ , 有  $n$  元函数符号  $f_0, f_1, f_2, \dots$ ;
- (9) 常数符号  $c_0, c_1, c_2, \dots$ 。

为了描述一个语言，只需给出它所含的谓词、函数、常数符号即可。例如  $\mathcal{L} = \{f_0, f_1, P_0, c_0, c_1, c_2\}$  表示这套语言有两个函数符号、一个谓词符号、三个常数符号。

**注 2.1** 由于习惯因素，我们有时用  $a, b, c, \dots$  或  $x, y, z, \dots$  或者其他形式表示变量；函数符号也可以用  $f, g, h, F, G, H, \varphi, \psi, \dots$  等等；谓词符号和常数符号也可以用其他符号取代。

**例 2.2** 讨论整数加法乘法时，我们需要的语言  $\mathcal{L} = \{+, \cdot, 0, 1\}$ 。事实上，我们的语言一开始写作  $\mathcal{L} = \{f_0, f_1, c_0, c_1\}$ 。其中  $f_0, f_1$  都是二元函数。我们准备用  $f_0(v_0, v_1)$  表示  $v_0$  加  $v_1$ ，因此我们将  $f_0(v_0, v_1)$  写成熟悉的  $v_0 + v_1$ 。同理，我们将  $f_1(v_0, v_1)$  写作  $v_0 \cdot v_1$ ，准备用这个符号表示乘法。我们准备用常数符号  $c_0$  表示 0，用  $c_1$  表示 1。

给定语言  $\mathcal{L}$  后，先规定项（指称个体的表达式），再规定公式。

**定义 2.3** 项（term）由下列规则递归定义：

1. 常数符号是项；
2. 变项符号是项；
3. 如果  $f \in \mathcal{L}$  是一个  $n$  元函数符号， $t_1, \dots, t_n$  是项，则  $f(t_1, \dots, t_n)$  也是项。

**注 2.4** 如果函数符号  $+$  意在表达加法，我们通常将  $+(x, y)$  写作  $x + y$ 。

**例 2.5** 在算术语言  $\mathcal{L}_{ar} = \{+, \cdot, 0, 1\}$  中， $1 + 1 + 1$  是项， $(1 + 1 + 1 + 1) \cdot (1 + 1)$  也是项。注意！

- 这里的 0 和 1 是常数符号，不是自然数——这两个常数符号通常会被解释为通常的自然数 0 和 1（见后文）。我们需要注意概念上的区别。
- 3 不是项。但我们通常可以认为 3 是  $1 + 1 + 1$  的缩写。

**定义 2.6** 如果  $P \in \mathcal{L}$  是一个  $n$  元谓词符号， $t_1, \dots, t_n$  是项，则  $P(t_1, \dots, t_n)$  是原子公式； $t_1 = t_2$  是原子公式。

**注 2.7** 若  $P$  是二元关系符号，则我们有时候会将  $P(x, y)$  写作  $xPy$ 。例如，在只含一个“小于”<sup>4</sup>号的语言  $\mathcal{L} = \{<\}$  中，我们不写  $<(x, y)$ ，而写  $x < y$ 。

**定义 2.8** 合式公式（wff）由下列规则递归定义：

1. 原子公式是 wff；
2. 如果  $\alpha, \beta$  是 wff，则  $(\neg \alpha)$ ， $(\alpha \wedge \beta)$ ， $(\alpha \vee \beta)$ ， $(\alpha \rightarrow \beta)$ ， $(\alpha \leftrightarrow \beta)$  也是 wff。
3. 如果  $\alpha$  是 wff，则  $(\forall v_i \alpha)$ 、 $(\exists v_i \alpha)$  也是 wff。

**注 2.9** 在不会造成歧义的情况下，我们会省略某些括号。

- 最外层的括号；
- $\neg, \forall, \exists$  优先级最高。 $\exists x \alpha \wedge \beta$  是  $((\exists x \alpha) \wedge \beta)$ 。
- $\wedge, \vee$  优先级其次。 $\neg \alpha \wedge \beta \rightarrow \gamma$  是  $((\neg \alpha) \wedge \beta) \rightarrow \gamma$ 。
- $\alpha \rightarrow \beta \rightarrow \gamma$  是  $\alpha \rightarrow (\beta \rightarrow \gamma)$ 。

**例 2.10** 在算术语言  $\mathcal{L} = \{+, \cdot, 0, 1\}$  中，

- $\forall n(n + 1 = 1 + 1 + 1 + 1)$  是 wff；
- $\forall n \exists m(n + m = 0)$  是 wff；
- $v + 1 = 0$  是 wff。

我们直观上知道，上述第一个公式在自然数的意义下是假的，第二个公式在讨论整数时是真的，讨论自然数时是假的，而第三个公式不管在什么意义下，我们都无法讨论其真假值。因为这里的  $v$  我们并不知道。如果一个句子包含自由的变量，通常<sup>5</sup>我们是无法判断真假的。

**定义 2.11** • 如果  $\alpha$  是原子公式，并且  $x$  出现，则  $x$  在  $\alpha$  自由出现，或称  $x$  是  $\alpha$  的自由变量；

<sup>4</sup>该符号暂时没有“小于”的意义，单纯作为符号引入。我们使用这个符号，当然是因为我们想用它来表示真正的小于。

<sup>5</sup> $v = v$  包含自由变量，但它是真的

- 如果  $x$  在  $\alpha$  中自由出现, 则  $x$  在  $\neg\alpha$  中自由出现。
- 如果  $x$  在  $\alpha$  或  $\beta$  中自由出现, 则  $x$  在  $\alpha \wedge \beta, \alpha \vee \beta, \alpha \rightarrow \beta, \alpha \leftrightarrow \beta$  中自由出现;
- 如果  $x$  在  $\alpha$  中自由出现, 并且  $v_i \neq x$ , 则  $x$  在  $\forall v_i \alpha$  中自由出现, 在  $\exists v_i \alpha$  中自由出现。

不包含自由变量的 wff 称为句子 (sentence) 或闭式。

**定义 2.12** 考虑  $\forall x\alpha$  或  $\exists x\alpha$ ,  $x$  被称为该全称量词或存在量词的指导变项,  $\alpha$  为  $x$  的辖域或作用域。若  $x$  为  $\alpha$  中的自由变项, 此时称  $x$  在  $\forall x\alpha$  或  $\exists x\alpha$  中约束出现。约束出现的变项称为约束变项。

例如,  $\exists x(A(x) \wedge B(x))$  是闭式。 $(\exists x A(x)) \wedge B(x)$  中  $B(x)$  中的  $x$  为自由变项,  $A(x)$  中的  $x$  为约束变项。(适当的省略括号后) 尽管是合理的, 但没有人愿意读  $\exists x A(x) \wedge B(x)$ 。为了可读性, 我们可以写  $\exists y A(y) \wedge B(x)$ :

**注 2.13 (换名规则)** 可以将一个指导变项  $x$  及其在辖域中的所有约束变项  $x$  同时替换成公式中没有出现的变项符号。**自由变项一般不换名。**

又例如, 我们会将  $\forall x(\exists x A(x) \wedge B(x))$  写成  $\forall x(\exists y A(y) \wedge B(x))$  或  $\forall y(\exists x A(x) \wedge B(y))$ 。见习题 2.4。

下面练习把自然语言译成公式。

## 2.2 一些翻译练习

**例 2.14** 集合论语言  $\mathcal{L} = \{\in\}$ 。

- 存在一个集合, 它不包含任何集合
- 不存在包含所有集合的集合
- 任何两个集合, 都有另一个恰好包含这些集合的集合
- $\forall z(z \in x \leftrightarrow z \in y) \rightarrow x = y$

**例 2.15** 算术语言  $\mathcal{L} = \{+, \cdot, 0, 1\}$

- 存在一个偶数
- 存在一对素数, 它们的差为 2
- 孪生素数猜想: 存在无穷多对差为 2 的素数
- $x$  小于  $y$
- $\exists x \exists y \exists z (x \neq 0 \wedge y \neq 0 \wedge z \neq 0 \wedge x \cdot x + y \cdot y = z \cdot z)$

**例 2.16** 日常生活  $\mathcal{L} = \{A, B\}$

- 所有苹果都是坏的;
- 有些苹果是坏的;
- 所有东西要么是坏的, 要么是苹果。
- $\exists x(A(x) \rightarrow B(x))$
- $\forall x(A(x) \wedge B(x))$

至此, 我们只谈翻译, 尚未谈及真假。但我们已经知道, 有些翻译的正确性依赖于考虑的情景: 例如, 存在一个偶数, 若使用  $\exists x \exists y (y + y = x)$ , 则这句话在有理数的情景下, 不能表达存在一个偶数。见习题 2.1、2.2。

## 2.3 结构

仅有语言和句子, 我们不足以判断一个公式的真假。例如, 给定语言  $\mathcal{L} = \{+, 0, 1\}$ , 我们考虑句子

$$\exists a(a + 1 = 0)$$

那么, 我们要如何判断这个句子的真假呢? 我们的情景究竟是如何的? 从直观上看,

- 如果我们讨论的是整数，则这个句子是真的；
- 如果我们讨论的是自然数，则这个句子是假的。

因此，一个句子的对错取决于我们讨论的情景：

**定义 2.17** 给定语言  $\mathcal{L} = \{f, P, c\}$ ，一个  $\mathcal{L}$  结构记为  $\mathcal{M} = (M, f^M, P^M, c^M)$ ，其中

- $M$  是一个集合，我们要求  $M \neq \emptyset$ ，称其为个体域， $M$  中的元素称为个体；
- 如果  $f$  是一个  $n$  元函数，则  $f^M : M^n \rightarrow M$  为一个函数；
- 如果  $P$  是一个  $n$  元谓词符号，则  $P^M \subseteq M^n$ 。
- $c^M \in M$ 。

若语言包含多个函数符号、谓词符号、常数符号，其定义类似。

$f^M$  是结构  $M$  对函数符号  $f$  的解释， $P^M$  是结构  $M$  对谓词符号  $P$  的解释， $c^M$  是结构  $M$  对常数符号  $c$  的解释。不同的结构有不同的解释。

**例 2.18** 考虑集合论语言  $\mathcal{L} = \{\in\}$ ，其中  $\in$  是一个二元关系符号。我们考虑结构  $\mathcal{M} = (\mathbb{N}, \in^M)$ ， $\in^M = \{\langle x, y \rangle \mid x < y\}$ 。下述句子

$$\exists x \forall y (\neg y \in x)$$

翻译成存在一个自然数，任何其他自然数都不比它小，其本意当然是存在一个最小的自然数。这句话在  $M$  中是真的。而

$$\forall x \exists y (y \in x)$$

翻译成对于任何自然数，都存在一个比它小的自然数，其本意当然是任何自然数都不是最小的自然数或者不存在一个最小的自然数。这句话的意思是前一句的否定——在  $M$  中为假。

**例 2.19** 考虑算术语言  $\mathcal{L} = \{+, \cdot, 0, 1\}$ ，及两个  $\mathcal{L}$  结构  $M_1 = (\mathbb{N}, +, \cdot, 0, 1)$  和  $M_2 = (\mathbb{Z}, +, \cdot, 0, 1)$ 。通过直观翻译，我们知道

$$\forall x \exists y (x + y = 0)$$

在  $M_1$  中是假的，在  $M_2$  中是真的。见习题 2.9。

## 2.4 真值

结构给出符号的解释。要判断含自由变项的公式的真假，还需把变项映射到个体。

**赋值.** 给定  $\mathcal{L} = \{f, P, c\}$  及一个  $\mathcal{L}$  结构  $\mathcal{M} = (M, f^M, P^M, c^M)$ 。为了讨论一个（可能含有自由变量的）公式  $\alpha$  在  $M$  中的真假，我们还需要引入赋值的概念：函数  $s : V \rightarrow M$  是结构  $M$  的一个赋值，其中  $V$  是变项的集合。 $s$  将一个变项指派给结构  $M$  中一个具体的元素。一个结构可以有很多赋值。我们想讨论一个公式  $\alpha$  在结构  $M$  及赋值  $s$  下的真假情况。

我们首先希望将  $s : V \rightarrow M$  进行扩展，使其能把所有项指派给结构  $M$  中的一个具体元素。令  $T$  表示所有的项。

**定义 2.20**  $\bar{s} : T \rightarrow M$  是  $s : V \rightarrow M$  的一个扩展，如果

- 对任意变项  $x$ ， $\bar{s}(x) = s(x)$ ；
- 对常数符号  $c$ ， $\bar{s}(c) = c^M$ ；
- 如果  $f$  是一个  $n$  元函数符号，并且  $t_1, \dots, t_n$  是项，则  $\bar{s}(f(t_1, \dots, t_n)) = f^M(\bar{s}(t_1), \dots, \bar{s}(t_n))$ 。

**定理 2.21** 赋值  $s : V \rightarrow M$  的扩展存在并且是唯一的。  $\square$

**例 2.22** 在算术语言  $\mathcal{L} = \{+, \cdot, 0, 1\}$  下， $M = \mathbb{N}$ ， $s(x) = 2024$ ， $s(y) = 2025$ ，则  $\bar{s}(x + y) = s(x) +^M s(y) = 4049$ ， $\bar{s}(x + 1) = 2025 = s(y)$ ， $\bar{s}(x \cdot (1 + 1)) = 4048$ 。所以，我们可以想象，公式  $x + 1 = y$  在  $M$  及赋值  $s$  下是真的。

**真假.** 给定  $\mathcal{L}$ , 一个  $\mathcal{L}$  结构  $M$ , 一个  $M$  上的赋值  $s$ , 我们用符号  $M \models \alpha[s]$  表示公式  $\alpha$  在  $M$  及赋值  $s$  下是真的。展开来说:

**定义 2.23** 原子公式情形:

1.  $M \models t_1 = t_2[s]$  如果  $\bar{s}(t_1) = \bar{s}(t_2)$ ;
2.  $M \models P(t_1, \dots, t_n)[s]$  如果  $\langle \bar{s}(t_1), \dots, \bar{s}(t_n) \rangle \in P^M$ 。

其他公式:

3.  $M \models \neg \alpha[s]$  如果  $M \not\models \alpha[s]$ 。
4.  $M \models \alpha \vee \beta[s]$  如果  $M \models \alpha[s]$  或  $M \models \beta[s]$ 。
5.  $M \models \alpha \wedge \beta[s]$  如果  $M \models \alpha[s]$  且  $M \models \beta[s]$ 。
6.  $M \models \alpha \rightarrow \beta[s]$  如果  $M \models \neg \alpha[s]$  或  $M \models \beta[s]$ 。
7.  $M \models \alpha \leftrightarrow \beta[s]$  如果  $M \models \alpha[s]$  当且仅当  $M \models \beta[s]$ 。
8.  $M \models \forall x \alpha[s]$  如果对所有  $m \in M$ ,  $M \models \alpha[s_x^m]$ 。
9.  $M \models \exists x \alpha[s]$  如果存在  $m \in M$ ,  $M \models \alpha[s_x^m]$ 。

这里  $s_x^m : V \rightarrow M$  和  $s : V \rightarrow M$  几乎一样:

$$s_x^m(y) = \begin{cases} s(y) & y \neq x \\ m & y = x \end{cases}$$

**定理 2.24**  $M \models \exists x \alpha[s]$  当且仅当  $M \models \neg \forall x \neg \alpha[s]$ 。

在讨论  $M$  及赋值  $s$  是否满足  $\alpha$  时, 我们实际上只关心  $s$  对自由变项的取值:

**定理 2.25** 如果对  $\alpha$  的任意自由变项  $x$  都有  $s_1(x) = s_2(x)$ , 则  $M \models \alpha[s_1]$  当且仅当  $M \models \alpha[s_2]$ 。

**证明** 对公式的构造作递归。先验证原子公式: 若  $s_1, s_2$  在  $\alpha$  的自由变项上取值相同, 则  $\bar{s}_1$  与  $\bar{s}_2$  在  $\alpha$  出现的项上取值相同, 从而  $M \models \alpha[s_1]$  当且仅当  $M \models \alpha[s_2]$ 。再对联词与量词逐条验证: 否定、合取、析取、蕴涵、等价以及  $\forall, \exists$  的真值只依赖于子公式在 (可能改动一个变项的) 赋值下的真值, 而归纳假设保证这些真值在  $s_1, s_2$  下一致。  $\square$

由该定理, 自由变项的取值已决定真假, 故可简写如下。

**定义 2.26** • 若  $\alpha$  自由变项依次为  $v_1, \dots, v_n$ , 我们用

$$M \models \alpha[s(v_1), \dots, s(v_n)]$$

表示  $M \models \alpha[s]$ 。

• 若  $\alpha$  不含自由变项, 我们用

$$M \models \alpha$$

表示  $M \models \alpha[s]$  (这里的  $s$  随便取一个即可)。

## 2.5 蕴涵

公式在结构中的真假已经定义。若一组公式  $\Sigma$  同时为真, 则称该结构为  $\Sigma$  的模型; 由此可定义语义蕴涵。

**定义 2.27** 若  $\Sigma \subseteq WFF$ , 我们称  $M$  及赋值  $s$  满足  $\Sigma$ , 记作  $M \models \Sigma[s]$ , 如果任意  $\alpha \in \Sigma$  都有  $M \models \alpha[s]$ 。若  $\Sigma$  只包含闭式, 我们记作  $M \models \Sigma$ , 此时, 我们称  $M$  是  $\Sigma$  的模型。

一组闭式  $\Sigma$  的模型, 就是满足这些公理的结构。下面用图、群、环、稠密线序以及有穷/无穷公理来说明。

**例 2.28** 令  $\mathcal{L} = \{E\}$ , 其中  $E$  为二元谓词 (将  $E(x, y)$  写作  $xEy$ )。任何一个  $\mathcal{L}$  结构都可以理解为一个图。令  $\Sigma_{graph}$  包含

- $\forall x(\neg xEx)$
- $\forall x\exists y(xEy)$
- $\forall x\forall y(xEy \rightarrow yEx)$

则  $\Sigma_{graph}$  的模型为没有孤立点的无向图。

**例 2.29 (群)** 令  $\mathcal{L} = \{\cdot, e\}$ , 其中  $\cdot$  为二元函数符号,  $e$  为常数符号。令  $\Sigma_{Group}$  包含

- (单位元)  $\forall x(x \cdot e = e \cdot x = x)$
- (结合律)  $\forall x\forall y\forall z(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
- (逆元)  $\forall x\exists y(x \cdot y = e)$

$\Sigma_{Group}$  的模型即为群。  $\Sigma_{Group} \cup \{\forall x\forall y(x \cdot y = y \cdot x)\}$  的模型为交换群, 即, 阿贝尔群。

**例 2.30**  $\mathcal{L} = \{+, \cdot, 0, 1\}$ , 其中  $+$  和  $\cdot$  为二元函数符号,  $0$  和  $1$  为常数符号。令  $\Sigma_{Ring}$  包含

- (加法单位元)  $\forall x(x + 0 = 0 + x = x)$
- (加法结合律)  $\forall x\forall y\forall z(x + (y + z) = (x + y) + z)$
- (加法逆元)  $\forall x\exists y(x + y = 0)$
- (加法交换律)  $\forall x\forall y(x + y = y + x)$
- (左分配律)  $\forall x\forall y\forall z(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
- (右分配律)  $\forall x\forall y\forall z((y + z) \cdot x = (y \cdot x) + (z \cdot x))$
- (乘法结合律)  $\forall x\forall y\forall z(x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
- (乘法单位元)  $\forall x(x \cdot 1 = 1 \cdot x = x)$

$\Sigma_{Ring}$  的模型即为环。例如, 模 2 整数环  $\mathbb{Z}/2\mathbb{Z}$  满足  $\Sigma_{Ring}$ 。

**例 2.31 (稠密线序)** 令  $\mathcal{L} = \{<\}$ ,  $\Sigma_{DLO}$  包含

- (反自反)  $\forall x(x < x)$
- (传递性)  $\forall x\forall y\forall z(x < y \rightarrow y < z \rightarrow x < z)$
- (完全线性序)  $\forall x\forall y(x < y \vee x = y \vee y < x)$
- (稠密)  $\forall x\forall y(x \neq y \rightarrow \exists z(x < z < y))$
- (无右端点)  $\forall x\exists y(x < y)$
- (无左端点)  $\forall x\exists y(y < x)$

$\Sigma_{DLO}$  的模型被称为稠密线序 (dense linear order), 例如  $\mathbb{Q}$ 、 $\mathbb{Q} \cap (0, 1)$  都是  $\Sigma_{DLO}$  的模型。见习题 2.8。

**例 2.32 (有穷模型)** 令  $\alpha_n$  为

$$\exists x_1\exists x_2 \cdots \exists x_n \left( \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \right)$$

则  $\alpha_n$  的模型至少包含  $n$  个个体。即,  $M \models \alpha_n$  当且仅当  $|M| \geq n$ 。例如  $n = 3$  时,  $\exists x_1\exists x_2\exists x_3 \bigwedge_{i \neq j} x_i \neq x_j$  即  $\exists x_1\exists x_2\exists x_3(x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3)$ 。恰有 3 个个体的句子见习题 2.7。

**例 2.33 (无穷模型)** 令  $\Sigma = \{\alpha_1, \alpha_2, \dots\}$ , 则  $\Sigma$  的模型包含无穷多个个体。即,  $M \models \Sigma$  当且仅当  $M$  为无穷集合。

**注 2.34** 不存在一个有穷的公式集  $\Sigma$ , 使得  $M \models \Sigma$  当且仅当  $M$  为无穷集合。

有了模型, 语义蕴涵与命题逻辑中的  $\models$  平行: 凡使前提为真的结构 (及赋值), 也使结论为真。

**定义 2.35** 给定  $\Sigma \subseteq WFF$ ,  $\alpha \in WFF$ , 我们定义  $\Sigma$  蕴涵  $\alpha$ , 记作  $\Sigma \models \alpha$ , 如果对任意  $M$  及所有赋值  $s$ , 若  $M \models \Sigma[s]$ , 则  $M \models \alpha[s]$ 。如果  $\Sigma = \{\alpha_1, \dots, \alpha_n\}$ , 我们也将  $\Sigma \models \alpha$  记为  $\alpha_1, \dots, \alpha_n \models \alpha$ 。

若  $\Sigma, \alpha$  都是闭式, 我们可将  $[s]$  省略。  $\Sigma \models \alpha$  可以理解为任何  $\Sigma$  的模型也是  $\alpha$  的模型。

**注 2.36** 我们立刻注意到, 对于命题逻辑, 验证  $\Sigma \models \alpha$  检查有穷多个赋值即可; 而对于一阶逻辑, 验证  $\Sigma \models \alpha$  则需要对任意  $\Sigma$  的模型  $M$ , 验证是否有  $M \models \alpha$ ——直观上来看, 验证  $\Sigma \models \alpha$  的工作似乎很难由计算机程序完成。

**例 2.37** 若  $M$  为稠密线序, 则  $M$  为无穷集合: 对任意  $n$ ,

$$\Sigma_{DLO} \models \exists x_1 \exists x_2 \cdots \exists x_n \left( \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \right)$$

**例 2.38** 若  $M$  为任意一个群, 则

$$\begin{aligned} M &\models \forall x \forall y \forall z (xy = xz \rightarrow y = z) \\ M &\models \forall x \forall y_1 \forall y_2 (xy_1 = e = xy_2 \rightarrow y_1 = y_2) \end{aligned}$$

即,  $M$  满足左消去律 (Left Cancellation Law), 及逆元唯一。由于  $M$  的任意性, 我们得到,

$$\begin{aligned} \Sigma_{Group} &\models \forall x \forall y \forall z (xy = xz \rightarrow y = z) \\ \Sigma_{Group} &\models \forall x \forall y_1 \forall y_2 (xy_1 = e = xy_2 \rightarrow y_1 = y_2) \end{aligned}$$

**例 2.39** 1.  $\forall x Qx \models Qy$   
 2.  $Qx \not\models \forall x Qx$   
 3.  $\forall x \alpha \models \exists x \alpha$   
 4.  $\exists x \forall y (xPy) \models \forall y \exists x (xPy)$   
 5.  $\forall y \exists x (xPy) \not\models \exists x \forall y (xPy)$   
 6.  $\models \exists x (Qx \rightarrow \forall x Qx)$

证明

1. 任取结构  $M$  及赋值  $s$  满足  $M \models \forall x Qx[s]$ 。令  $a = s(y)$ , 则

$$M \models Qx[s_x^a]$$

因此,  $s(y) = a \in Q^M$ 。由此得,

$$M \models Qy[s]$$

由于  $M, s$  的任意性, 我们得到  $\forall x Qx \models Qy$

2. 考虑结构  $M = (\{0, 1\}, Q^M = \{0\})$  及赋值  $s(x) = 0$ , 则有  $s(x) = 0 \in Q^M$ , 因此,

$$M \models Qx[s]$$

但由于

$$M \not\models Qx[s_x^1]$$

所以  $M \not\models \forall x Qx[s]$ 。由此可见,  $Qx \not\models \forall x Qx$ 。

3. 任取结构  $M$  及赋值  $s$  满足  $M \models \forall x \alpha[s]$ , 任取  $m \in M$ , 则

$$M \models \alpha[s_x^m]$$

因此,

$$M \models \exists x \alpha[s]$$

4. 任取结构  $M$  及赋值  $s$  满足  $M \models \exists x \forall y (xPy)[s]$ , 则存在  $a$  满足

$$M \models \forall y (xPy)[s_x^a]$$

则对任意  $b \in M$  有,

$$M \models xPy[(s_x^a)_y^b]$$

由于  $(s_x^a)_y^b = (s_y^b)_x^a$ , 则

$$M \models \exists x (xPy)[s_y^b]$$

由于  $b$  的任意性,

$$M \models \forall y \exists x (xPy)[s]$$

5. 考虑自然数结构  $\mathbb{N}$ , 其中  $P^{\mathbb{N}} = \{\langle m, n \rangle \mid m > n\}$ : 由于自然数中不存在最大数, 所以  $\mathbb{N} \models \forall y \exists x (xPy)$  但  $\mathbb{N} \not\models \exists x \forall y (xPy)$
6. 任取结构  $M$  和赋值  $s$ 。则
- 情况 1:**  $M \models \forall x Qx[s]$ 。此时, 我们任选一个 (任意性不重要)  $m \in M$ , 都有  $M \models \forall x Qx[s_x^m]$  ( $\forall x Qx$  不包含自由变项, 赋值不影响), 于是由定义 2.23(6) 知

$$M \models Qx \rightarrow \forall x Qx[s_x^m]$$

由定义 2.23(9) 知,  $M \models \exists x (Qx \rightarrow \forall x Qx)[s]$ 。

**情况 2:**  $M \not\models \forall x Qx[s]$ 。根据定义 2.23(8) 知存在  $m \in M$  满足  $M \not\models Qx[s_x^m]$ , 由定义 2.23(6) 知

$$M \models Qx \rightarrow \forall x Qx[s_x^m]$$

由定义 2.23(9) 知,  $M \models \exists x (Qx \rightarrow \forall x Qx)[s]$ 。

□

与命题逻辑一样, 全体结构上都为真的公式称为永真式。

**定义 2.40**  $\alpha$  为永真式, 记为  $\models \alpha$ , 如果  $\emptyset \models \alpha$ ; 永假式如果  $\neg \alpha$  为永真式。 $\alpha$  为可满足式, 如果  $\alpha$  不是永假式。

命题逻辑中的永真式, 把命题变元换成一阶公式后仍然永真:

**定理 2.41** 设包含命题变元  $A_1, A_2, \dots, A_n$  的命题公式  $\alpha$  为永真式 (命题逻辑意义下),  $\beta$  是将  $\alpha$  中的命题变元  $A_i$  替换成一阶公式  $\sigma_i$  的一阶公式, 则  $\beta$  为永真式 (一阶逻辑意义下)。

**例 2.42** 例如  $A \rightarrow B \rightarrow A$  为永真式, 则  $\forall x \alpha \rightarrow (y + y = z) \rightarrow \forall x \alpha$  为永真式: 考虑结构  $M$  和赋值  $s$ 。如果我们将  $M \models \forall x \alpha[s]$  记为  $A$ ,  $M \models y + y = z[s]$  记为  $B$ , 我们可以验证下列条件等价

- $M \models \forall x \alpha \rightarrow (y + y = z) \rightarrow \forall x \alpha[s]$
- $A \rightarrow B \rightarrow A$

而后句是永真式, 所以  $\forall x \alpha \rightarrow (y + y = z) \rightarrow \forall x \alpha$  为永真式 (一阶逻辑意义下)。

**例 2.43**  $\sigma, \tau \in WFF$

- $\models \neg \neg \sigma \leftrightarrow \sigma$
- $\models (\neg \sigma \vee \tau) \leftrightarrow (\sigma \rightarrow \tau)$

双向蕴涵即等值, 记法与命题逻辑相同。

**定义 2.44** 如果  $\alpha \models \beta$  并且  $\beta \models \alpha$ , 则称  $\alpha$  和  $\beta$  等值, 记为  $\alpha \models \beta$ 。

**引理 2.45**  $\alpha \models \beta$  当且仅当  $\models \alpha \leftrightarrow \beta$ 。

**例 2.46**

- $\neg \neg \alpha \models \alpha$
- $(\neg \alpha \vee \beta) \models (\alpha \rightarrow \beta)$
- $\alpha \models \beta$  当且仅当  $\neg \alpha \models \neg \beta$ 。

**引理 2.47 (传递性)** 若  $\alpha \models \beta, \beta \models \gamma$ , 则  $\alpha \models \gamma$ 。

**定理 2.48**

1.  $\neg \forall x \alpha \models \exists x \neg \alpha$
2.  $\neg \exists x \alpha \models \forall x \neg \alpha$
3.  $\forall x (\alpha \wedge \beta) \models \forall x \alpha \wedge \forall x \beta$
4.  $\exists x (\alpha \vee \beta) \models \exists x \alpha \vee \exists x \beta$
5.  $\forall x (\alpha \vee \beta) \models \alpha \vee \forall x \beta$ , 其中  $x$  不在  $\alpha$  中自由出现。
6.  $\exists x (\alpha \wedge \beta) \models \alpha \wedge \exists x \beta$ , 其中  $x$  不在  $\alpha$  中自由出现。
7. 若  $x$  不在  $\alpha$  中自由出现, 则  $\alpha \models \forall x \alpha$ , 且  $\alpha \models \exists x \alpha$ 。

$$8. \forall x \forall y \alpha \models \forall y \forall x \alpha$$

$$9. \exists x \exists y \alpha \models \exists y \exists x \alpha$$

证明

2 由 (1) 得  $\neg \neg \forall x \alpha \models \neg \exists x \neg \alpha$ , 由于  $\neg \neg \forall x \alpha \models \forall x \alpha$ , 再由传递性得证。

□

注意  $\forall x(\alpha \vee \beta)$  与  $\forall x \alpha \vee \forall x \beta$  一般不等值,  $\exists x(\alpha \wedge \beta)$  与  $\exists x \alpha \wedge \exists x \beta$  亦然, 见习题 2.10。第 (7) 条的蕴涵方向见习题 2.6。利用这些等值式, 我们可以把量词集中放在公式最左边:

**定义 2.49** 如果  $\alpha$  形如

$$Qv_1 Qv_2 Qv_3 \cdots Qv_n \beta$$

其中  $Q$  为  $\forall$  或者  $\exists$ , 且  $\beta$  不含有量词, 则称  $\alpha$  为前束范式。

**定理 2.50** 任意公式  $\alpha$  都与一个前束范式等值。

□

- 例 2.51**
- $\forall x F(x) \wedge \neg \exists x G(x)$
  - $\exists x F(x) \rightarrow \forall x G(x)$
  - $\neg \forall x [\exists y A(x, y) \rightarrow \exists x A(y, x)]$

证明

- 该公式等值于
  - $\forall x F(x) \wedge \forall x \neg G(x)$
  - $\forall x (F(x) \wedge \neg G(x))$
- 该公式等值于
  - $\neg \exists x F(x) \vee \forall x G(x)$
  - $\forall x \neg F(x) \vee \forall y G(y)$
  - $\forall x \forall y (\neg F(x) \vee G(y))$
- 该公式等值于
  - $\exists x \neg (\neg \exists y A(x, y) \vee \exists x A(y, x))$
  - $\exists x (\exists y A(x, y) \wedge \forall x \neg A(y, x))$
  - $\exists x (\exists u A(x, u) \wedge \forall z \neg A(y, z))$
  - $\exists x \exists u \forall z (A(x, u) \wedge \neg A(y, z))$

这里, 我们用到了定理 2.48 中  $x$  不自由出现时的条款, 以及换名。

□

见习题 2.11。

## 2.6 习题

**习题 2.1** 在语言  $\mathcal{L} = \{<\}$  下, 以实数为背景, 翻译下列句子:

- 存在一个最大的数 \_\_\_\_\_
- 存在一个最小的数 \_\_\_\_\_
- 存在两个不可比的数 \_\_\_\_\_

当然了, 这些句子在实数中都不成立。

**习题 2.2** 在语言  $\mathcal{L} = \{+, \times, 0, 1\}$  下, 以实数为背景, 翻译下列句子:

- 每个非零实数都存在乘法逆元 \_\_\_\_\_
- 每一个实数都有加法逆元 \_\_\_\_\_

- 0 是加法单位元 \_\_\_\_\_
- 1 是乘法单位元 \_\_\_\_\_
- 加法交换律 \_\_\_\_\_
- 加法结合律 \_\_\_\_\_
- 乘法交换律 \_\_\_\_\_
- 乘法结合律 \_\_\_\_\_
- 分配律 \_\_\_\_\_

实数满足这些性质，因此，实数是一个域。满足这些性质的也可以有其他数学对象，比如复数域。

**习题 2.3** 在语言  $\mathcal{L} = \{0, 1, +, \times\}$  下，是否存在  $\alpha$  满足  $\mathbb{C} \models \alpha$  但  $\mathbb{R} \models \neg \alpha$ 。

**习题 2.4** 下列语句中的变元哪些是自由变元？哪些不是？不是的变元分别都被哪个量词约束？其中  $P, Q$  是二元谓词符号。

$$\forall x(P(x, y) \wedge \exists y Q(x, y))$$

**习题 2.5** 证明  $\forall x(\alpha \rightarrow \beta), \forall x \alpha \models \forall x \beta$ 。

**习题 2.6** 若  $x$  不是  $\alpha$  的自由变量，则  $\alpha \models \forall x \alpha$ 。

**习题 2.7** 若  $M \models \alpha$  当且仅当  $|M| = 3$ ，写出  $\alpha$ 。

**习题 2.8** 考虑  $\mathcal{L} = \{<\}$ ，两个结构  $(\mathbb{N}, <)$  和  $(\mathbb{R}, <)$ 。写出一个句子  $\alpha$  使得  $\mathbb{R} \models \alpha$  但是  $\mathbb{N} \not\models \alpha$ 。

**习题 2.9**  $\mathcal{L} = \{+, \cdot, 0, 1\}$ ， $M_1 = (\mathbb{N}, +, \cdot, 0, 1)$  为标准自然数结构， $M_2 = (\mathbb{Z}, +, \cdot, 0, 1)$  为标准整数结构。下列 \_\_\_\_\_ 公式在  $M_1$  中为真；\_\_\_\_\_ 公式在  $M_2$  中为真：

1.  $\forall x \exists y(xy = 0)$
2.  $\forall x \exists y(xy = 1)$
3.  $\exists x \exists y(xy = 1 + 1)$
4.  $\forall x \forall y \exists z(x - y = z)$
5.  $\forall x \forall y(xy = y)$
6.  $\forall x(xy = x)$
7.  $\exists x \forall y(x + y = y + y)$

**习题 2.10** 证明

- $\forall x \alpha \vee \forall x \beta \models \forall x(\alpha \vee \beta)$ ，但不等值
- $\exists x(\alpha \wedge \beta) \models \exists x \alpha \wedge \exists x \beta$ ，但不等值

**习题 2.11** 写出下述句子的前束范式：

- $\neg \exists x F(x) \rightarrow \forall y G(x, y)$
- $\neg(\forall x F(x, y) \vee \exists y G(x, y))$
- $\forall x F(x) \vee \exists y G(x, y)$

## §3 集合

### 3.1 集合的概念

集合是一个抽象的、无法定义的概念。本章按朴素方式操作集合：用  $\in$  表示属于，用花括号列举或描述元素。

**定义 3.1** 集合  $A$  是集合  $B$  的子集，记作  $A \subseteq B$ ，如果  $\forall x(x \in A \rightarrow x \in B)$ 。

**定义 3.2**  $A = B$  当且仅当  $A \subseteq B$  并且  $B \subseteq A$ 。若  $A \subseteq B$  并且  $A \neq B$ ，则称  $A$  是  $B$  的真子集，记作  $A \subset B$ （或  $A \subsetneq B$ ）。

$\{1, 2, 5\} = \{5, 2, 1, 1\}$ 。由此可见，在集合内重复元素没有意义，顺序也不重要。

序对稍后要用到下述唯一性：

**命题 3.3** 令  $A = \{\{a\}, \{a, b\}\}$ ,  $C = \{\{c\}, \{c, d\}\}$ 。若  $A = C$ , 则  $a = c, b = d$ 。

**证明** 情形 1.  $a = b$ 。则  $A = \{\{a\}\}$ 。由于  $\{c, d\} \in A$ , 得  $\{c, d\} = \{a\}$ , 得  $c = d = a$ 。

情形 2.  $a \neq b$ 。则  $A$  恰有两个元素  $\{a\}$  与  $\{a, b\}$ 。由于  $\{a\} \in C$ , 要么  $\{a\} = \{c\}$ , 要么  $\{a\} = \{c, d\}$ 。后者推出  $c = d = a$ , 从而  $C = \{\{a\}\}$ , 与  $A$  有两个元素矛盾。故  $\{a\} = \{c\}$ , 得  $a = c$ 。再由  $\{a, b\} = \{c, d\}$  得  $b = d$ 。□

并非任意描述都能给出一个集合:

**定理 3.4 (罗素悖论)**  $\{x \mid x \notin x\}$  不是一个集合。

**证明** 假设是一个集合, 记作  $y$ 。若  $y \in y$ , 则  $y \notin y$ ; 若  $y \notin y$ , 则  $y \in y$ 。矛盾。□

我们约定: 从一个已有集合中分出满足某性质的元素, 得到的仍是集合, 记作  $\{z \in x \mid \varphi(z)\}$ 。

**定义 3.5** 集合  $A$  为空集, 如果  $\forall x (x \notin A)$ 。

**定理 3.6** 如果  $A$  为空集, 则  $\forall x (A \subseteq x)$ 。

**证明** 给定集合  $x$ , 我们只需要验证  $\forall z (z \in A \rightarrow z \in x)$ 。但  $z \in A$  不成立, 所以整个句子成立。□

**推论 3.7** 空集唯一。

**证明** 若  $A, B$  均为空集, 则由上一定理  $A \subseteq B$  且  $B \subseteq A$ , 故  $A = B$ 。□

由唯一性, 我们用  $\emptyset$  表示空集。

**例 3.8** 判断下列命题的真假: (1)  $\emptyset \in \emptyset$ ; (2)  $\emptyset \subseteq \emptyset$ ; (3)  $\emptyset \subset \emptyset$ ; (4)  $\emptyset \in \{\emptyset\}$ ; (5)  $\emptyset \subseteq \{\emptyset\}$ 。

**定义 3.9** 集合  $x$  的幂集为  $\mathcal{P}(x) = \{z \mid z \subseteq x\}$ 。

**例 3.10** •  $\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{1, 2, 3\}\}$ 。  
•  $\mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$

见习题 3.1。

## 3.2 集合的基本运算

有了集合, 即可定义交、并、差与对称差。

**定义 3.11** •  $A \cap B = \{x \mid x \in A \wedge x \in B\}$ ;  
•  $A \cup B = \{x \mid x \in A \vee x \in B\}$ ;  
•  $A \setminus B = \{x \in A \mid x \notin B\}$ ;  
•  $A \oplus B = (A \setminus B) \cup (B \setminus A)$ 。

**例 3.12** 令  $A = \{1, 2, 3\}$ ,  $B = \{1, 4\}$ , 则

$$\begin{aligned} A \cup B &= \{1, 2, 3, 4\} = B \cup A \\ A \cap B &= \{1\} = B \cap A \\ A \setminus B &= \{2, 3\} \\ B \setminus A &= \{4\} \\ A \oplus B &= \{2, 3, 4\} = B \oplus A \end{aligned}$$

**定义 3.13**  $A$  和  $B$  不相交, 如果  $A \cap B = \emptyset$ 。

例如,  $A \setminus B$  和  $A \cap B$  不相交, 而  $(A \setminus B) \cup (A \cap B) = A$ 。

固定全集  $\mathcal{U}$  后, 子集可用  $\{0, 1\}$  上的函数记录:

**定义 3.14** 给定一个集合  $\mathcal{U}$ ,  $A \subseteq \mathcal{U}$  的特征函数是函数  $\chi_A : \mathcal{U} \rightarrow \{0, 1\}$ , 满足

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

(相对于集合  $\mathcal{U}$ )  $A$  的补集为  $\mathcal{U} \setminus A$ , 记为  $A^c$ 。则  $\chi_{A^c}(x) = 1 - \chi_A(x)$ 。

**命题 3.15**

- 若  $A \subseteq B$ , 则  $\chi_A \leq \chi_B$ 。
- 若  $A = B$ , 则  $\chi_A = \chi_B$ 。

**命题 3.16**

- $\chi_{A \cap B} = \min\{\chi_A, \chi_B\} = \chi_A \cdot \chi_B \pmod 2$
- $\chi_{A \cup B} = \max\{\chi_A, \chi_B\} = \chi_A + \chi_B + \chi_A \cdot \chi_B \pmod 2$
- $\chi_{A \setminus B} = \chi_A \cdot (1 - \chi_B) \pmod 2$
- $\chi_{A \oplus B} = \chi_A + \chi_B \pmod 2$

**命题 3.17**

1.  $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
2.  $(A \oplus B) \oplus C = A \oplus (B \oplus C)$
3.  $A \oplus \emptyset = A$
4.  $A \oplus A = \emptyset$
5. 若  $A \oplus B = A \oplus C$ , 则  $B = C$

由特征函数的运算规则可见, 集合的  $\cap, \cup, ^c$  在每一点上的取值计算, 正是  $\{0, 1\}$  上的  $\wedge, \vee, \neg$ 。因此固定全集  $\mathcal{U}$  时,  $\mathcal{P}(\mathcal{U})$  上的交、并、补与命题逻辑共享同一套运算律。

### 3.3 笛卡尔积

集合的元素没有顺序。要记录有序信息, 先用无序对编码序对。

**定义 3.18** 序对  $\langle a, b \rangle = \{\{a\}, \{a, b\}\}$ 。

由命题 3.3, 若  $\langle a, b \rangle = \langle c, d \rangle$ , 则  $a = c, b = d$ 。

递归地, 我们可以定义

**定义 3.19** 有序  $n$  元组  $\langle x_1, x_2, \dots, x_n \rangle = \langle \langle x_1, x_2, \dots, x_{n-1} \rangle, x_n \rangle$

**命题 3.20** 若  $\langle x_1, x_2, \dots, x_n \rangle = \langle y_1, y_2, \dots, y_n \rangle$ , 则对任意  $i \leq n$ ,  $x_i = y_i$ 。

**证明** 对  $n$  做归纳法。当  $n = 2$  时, 命题显然成立。假设命题对  $n$  成立。我们考虑  $n + 1$  的情况。若

$$\langle x_1, x_2, \dots, x_{n+1} \rangle = \langle y_1, y_2, \dots, y_{n+1} \rangle$$

即

$$\langle \langle x_1, x_2, \dots, x_n \rangle, x_{n+1} \rangle = \langle \langle y_1, y_2, \dots, y_n \rangle, y_{n+1} \rangle$$

由定义 3.18, 我们得  $x_{n+1} = y_{n+1}$  以及  $\langle x_1, x_2, \dots, x_n \rangle = \langle y_1, y_2, \dots, y_n \rangle$ 。进一步由归纳假设得  $x_i = y_i$  对所有  $i \leq n$  成立。因此, 命题对  $n + 1$  成立。

由数学归纳法, 命题对所有  $n \geq 2$  都成立。□

**定义 3.21** 给定集合  $A, B$ , 定义  $A \times B = \{\langle a, b \rangle \mid a \in A \wedge b \in B\}$ 。

**命题 3.22**

- $\emptyset \times A = A \times \emptyset = \emptyset$ 。
- $A \times B = B \times A$  当且仅当  $A = B$  或  $A = \emptyset$  或  $B = \emptyset$ 。

**证明** 第一条由定义直接验证。第二条: ( $\Rightarrow$ ) 假设  $A, B$  非空, 证明  $A = B$ 。(请完成。) □

**例 3.23**  $A = \{1, 2\}$ , 求  $A \times \mathcal{P}(A)$ 。见习题 3.1。

**例 3.24**

- $A \times (B \cap C) = (A \times B) \cap (A \times C)$

$$\bullet A \times (B \cup C) = (A \times B) \cup (A \times C)$$

**例 3.25** 判断下列命题的真假：

- 若  $A \subseteq C$ ,  $B \subseteq D$ , 则  $A \times B \subseteq C \times D$ ;
- 若  $A \times B \subseteq C \times D$ , 则  $A \subseteq C$ ,  $B \subseteq D$ 。

笛卡尔积把两个集合的元素配成序对。其子集就是关系。

### 3.4 关系

**定义 3.26** 若  $R \subseteq A \times B$ , 则称  $R$  为从  $A$  到  $B$  的二元关系；若  $A = B$ , 则称  $R$  为  $A$  上的关系。

**定义 3.27**  $R$  为  $A$  上的一个关系。

- 若  $R = \emptyset$ , 则称  $R$  为空关系。
- 若  $R = A \times A$ , 则称  $R$  为全域关系, 记为  $E_A$ 。
- 若  $R = \{\langle a, a \rangle \mid a \in A\}$ , 则称  $R$  为恒等关系, 记为  $I_A$ 。

**例 3.28** 若  $A = \{1, 2, 3\}$ , 则

$$E_A = \{\langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 1, 3 \rangle, \langle 2, 1 \rangle, \langle 2, 2 \rangle, \langle 2, 3 \rangle, \langle 3, 1 \rangle, \langle 3, 2 \rangle, \langle 3, 3 \rangle\}$$

$$I_A = \{\langle 1, 1 \rangle, \langle 2, 2 \rangle, \langle 3, 3 \rangle\}$$

**定义 3.29** 若  $R \subseteq A \times B$ , 我们通常也用  $aRb$  表示  $\langle a, b \rangle \in R$ 。

**定义 3.30** 若  $A = \{x_1, \dots, x_n\}$ ,  $R \subseteq A \times A$ , 令

$$r_{ij} = \begin{cases} 1 & x_i R x_j \\ 0 & \neg x_i R x_j \end{cases}$$

我们称矩阵  $M_R = (r_{ij})$  为  $R$  的关系矩阵。 $G_R = (A, R)$  为  $R$  的关系图。

**注 3.31** 我们回顾有向图的定义：一个有向图  $G = (V, E)$  包含一个顶点集  $V$  及边集  $E$ , 其中  $E \subseteq V \times V$ 。

**例 3.32** 考虑  $[10]$  上的整除关系, 写出关系矩阵、画出关系图。

### 3.5 关系的性质

通常, 一个关系可以讨论以下性质：

**定义 3.33** 令  $R$  为  $A$  上的关系。

- (自反性)  $\forall x \in A (xRx)$ ;
- (反自反性)  $\forall x \in A \neg (xRx)$ ;
- (对称性)  $\forall x \in A \forall y \in A (xRy \rightarrow yRx)$ ;
- (反对称性)  $\forall x \in A \forall y \in A (x \neq y \wedge xRy \rightarrow \neg yRx)$ ;
- (传递性)  $\forall x \in A \forall y \in A \forall z \in A (xRy \rightarrow yRz \rightarrow xRz)$ 。

**例 3.34**  $I_A$ 、 $E_A$ 、整除关系, 小于关系, 小于等于关系, 幂集上的包含关系。

**例 3.35** 这些性质会有相互制约关系吗? 例如  $\{1, 2\}$  上的一个关系, 要么是对称的, 要么是反对称的。 $\{1, 2, 3\}$  上的关系呢?

### 3.6 关系的运算

关系作为集合, 可以谈定义域、值域; 有了传递性, 还可以生成包含它的最小传递关系。

**定义 3.36** 考虑  $R \subseteq A \times B$  是一个关系。其定义域  $\text{dom } R$ 、值域  $\text{ran } R$  为

$$\begin{aligned}\text{dom } R &= \{x \in A \mid \exists y(xRy)\} \\ \text{ran } R &= \{y \in B \mid \exists x(xRy)\}\end{aligned}$$

当  $A = B$  时, 关系的域为  $\text{fld } R = \text{dom } R \cup \text{ran } R$ 。

**定义 3.37** 若  $R$  为  $A$  上的一个关系,  $S$  为  $R$  的传递闭包, 如果

- $S$  是传递的;
- $R \subseteq S$ ;
- 若  $T \supseteq R$  是传递的, 则  $S \subseteq T$ 。

此时, 我们记  $t(R) = S$ 。

满足自反、对称、传递的关系特别重要: 它们把“在所关注的性质上无法区分”做成等价。

### 3.7 等价关系

**定义 3.38**  $R$  为  $A$  上的等价关系, 如果  $R$  是对称的、自反的、传递的。

**例 3.39** 1. 固定一个  $n \in \mathbb{N}$ , 定义  $\mathbb{Z}$  上的一个关系  $R$  满足

$$xRy \text{ 当且仅当 } n \mid (x - y)$$

则  $R$  为等价关系。我们通常将  $xRy$  记为

$$x \equiv y \pmod{n}$$

2. 在  $\mathcal{P}([3])$  上定义  $S \sim T$  当且仅当  $|S| = |T|$ 。
3. 非空集合  $A$  上的恒等关系  $I_A$  是等价关系。

等价关系抽取了等号  $=$  的一些重要性质。如果  $x = y$ , 我们认为  $x$  和  $y$  是完全相同的数学对象, 只是名称不同 (一个叫  $x$ 、另一个叫  $y$ )。如果  $xRy$ , 则  $x$  和  $y$  在我们所关注的性质上 (由  $R$  确定) 无法区分。

**定义 3.40**  $R$  为  $A$  上的等价关系, 对于  $a \in A$ ,  $a$  的等价类为集合

$$[a]_R = \{b \in A \mid aRb\}$$

若没有歧义, 我们将  $[a]_R$  简记为  $[a]$ 。

等价类这个概念在数学各分支中随处可见。例如, 在考虑不定积分时, 如果  $F' = f$ , 则我们会写

$$\int f(x) dx = F(x) + C$$

等式右侧实际上表示的是和  $F$  等价<sup>6</sup>的一类函数, 而并非单个函数。

**例 3.41**  $R$  为  $\mathbb{Z}$  上的模 3 等价关系, 则

$$\begin{aligned}[0]_R &= \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\} \\ [1]_R &= \{\dots, -8, -5, -2, 1, 4, 7, \dots\} \\ [2]_R &= \{\dots, -7, -4, -1, 2, 5, 8, \dots\}\end{aligned}$$

注意到, 若  $i \neq j$ , 则  $[i]_R \cap [j]_R = \emptyset$ , 并且  $[0]_R \cup [1]_R \cup [2]_R = \mathbb{Z}$ 。

**定理 3.42**  $R$  是  $A$  上的等价关系,  $a, b \in A$ 。

1.  $a \in [a]_R$ ;

---

<sup>6</sup> $F$  和  $G$  等价, 如果  $F' = G'$

2.  $aRb$  当且仅当  $[a]_R = [b]_R$ ;
3. 若  $[a]_R \cap [b]_R \neq \emptyset$ , 则  $[a]_R = [b]_R$ 。

第(3)条见习题 3.9。

**定义 3.43**  $P \subseteq \mathcal{P}(A)$  是  $A$  的一个划分, 如果

- $\emptyset \notin P$ ;
- $\forall a \in P \forall b \in P (a \neq b \rightarrow a \cap b = \emptyset)$ ;
- $A = \bigcup_{a \in P} a$ 。

$P$  中的元素称为 划分块。

**例 3.44** 在例 3.41 中,  $\{[0]_R, [1]_R, [2]_R\}$  为  $\mathbb{Z}$  的一个划分。

**定理 3.45** 若  $R$  为  $A \neq \emptyset$  上的一个等价关系, 则

$$\{[a]_R : a \in A\}$$

为  $A$  的一个划分。

**证明** 由定义直接验证: 各等价类非空 (因  $a \in [a]_R$ ); 两两不交 (定理 3.42); 并集为  $A$ 。□

划分在数学各分支中十分常见, 通常借助等价关系作为商引入:

**定义 3.46** 若  $R$  为  $A \neq \emptyset$  上的一个等价关系,  $A$  在  $R$  下的商集为

$$A/R = \{[a]_R : a \in A\}$$

讨论等价类  $[a]_R$  时, 我们关注什么元素和  $a$  是“一样的”。讨论  $A/R$  时, 则把关注点放在元素之间不同的性质上。

**定理 3.47** 若  $P$  为  $A \neq \emptyset$  的一个划分, 定义  $x \sim y$  如果

$$\exists a \in P (x \in a \wedge y \in a)$$

则  $P = A/\sim$ 。

由此定理 3.45 和定理 3.47 知, 划分和等价关系有一个一一对应。两者本质上是同一件事:

**定理 3.48** 集合  $A \neq \emptyset$  的等价关系和划分有一一对应。

**证明** 令

$$\mathbf{E} = \{R \mid R \text{ 为 } A \text{ 上的等价关系}\}$$

$$\mathbf{P} = \{P \mid P \text{ 为 } A \text{ 上的划分}\}$$

定义  $f: \mathbf{E} \rightarrow \mathbf{P}$  满足

$$f(R) = A/R$$

我们验证  $f$  为双射: (单射) 若  $R_1 \neq R_2$ , 则存在  $a, b$  满足  $aR_1b$  但  $\neg aR_2b$ 。因此,  $b \in [a]_{R_1}$  但  $b \notin [a]_{R_2}$ 。即, 在划分  $f(R_1)$  中,  $a, b$  在同一个划分块中, 而在  $f(R_2)$  中,  $a, b$  不在同一个划分块中。所以,  $f(R_1) \neq f(R_2)$ 。(满射) 令  $P$  为一个划分,  $\sim$  由定理 3.47 给出, 则  $f(\sim) = P$ 。单射的另一写法见习题 3.10。□

**例 3.49** 考虑  $A = \{1, 2, 3\}$  上的所有等价关系。

等价关系把“无法区分”做成一类; 偏序则把“可比较的大小”做成序。

### 3.8 偏序关系

**定义 3.50**  $R$  是  $A$  上的偏序关系, 如果  $R$  是自反的、反对称的、传递的。为了可读性, 我们有时会将  $R$  写作  $\leq$ , 并且我们会定义  $a < b$  如果  $a \leq b \wedge a \neq b$ 。

**例 3.51**  $\mathbb{Q}$  上的“小于等于”是偏序关系, 但“小于”不是。 $\mathcal{P}(A)$  上的包含关系是偏序关系。

若  $R$  是  $A$  上的偏序关系, 则称  $(A, R)$  为偏序集。用一阶语言  $\mathcal{L} = \{R\}$  写出自反、反对称、传递三条, 其模型即偏序集。例如,  $(\mathbb{Z}, \leq)$  是偏序集,  $(\mathbb{N}, |)$  是偏序集, 其中  $a|b$  表示  $a$  整除  $b$ 。

一个偏序集中有一些特殊的点:

**定义 3.52**  $(A, \leq)$  是一个偏序集,  $B \subseteq A$ 。  $x \in B$  是  $B$  的

1. 极小元 (minimal element), 如果  $\neg \exists y \in B (y < x)$ ;
2. 极大元 (maximal element), 如果  $\neg \exists y \in B (x < y)$ ;
3. 最小元 (minimum element), 如果  $\forall y \in B (x \leq y)$ ;
4. 最大元 (maximum element), 如果  $\forall y \in B (y \leq x)$ 。

$y \in A$  是  $B$  的

1. 上界 (upper bound), 如果  $\forall x \in B (x \leq y)$ ;
2. 下界 (lower bound), 如果  $\forall x \in B (y \leq x)$ ;
3. 上确界 (supremum), 如果  $y$  是  $B$  的上界, 且对  $B$  的任意上界  $z$  有  $y \leq z$ ;
4. 下确界 (infimum), 如果  $y$  是  $B$  的下界, 且对  $B$  的任意下界  $z$  有  $z \leq y$ 。

最小元是极小元, 最大元是极大元。极大元是最大元吗? 上界/上确界一定存在吗?

**定义 3.53** 若  $(A, \leq)$  是偏序集, 并且额外满足  $\forall x \forall y (x \leq y \vee y \leq x)$ , 则称  $(A, \leq)$  为全序集。

$(\mathbb{Z}, \leq)$  是全序集,  $(\mathbb{N}, |)$  不是全序集。

**定理 3.54** 若  $(A, \leq)$  是全序集,  $B \subseteq A$  的极小 (大) 元, 如果存在, 是最小 (大) 元。

**证明** 设  $x$  为  $B$  的极小元。假设它不是最小元, 则存在  $y \in B$ ,  $x \not\leq y$ 。由于  $(A, \leq)$  是全序集,  $y < x$ 。与  $x$  的极小性矛盾。  $\square$

**例 3.55** 对  $(0, 1] \subseteq \mathbb{R}$  考察定义 3.52; 对  $\{x \mid x^2 < 2\} \subseteq \mathbb{Q}$  考察定义 3.52。

有穷偏序可用盖住关系画成图, 信息与原偏序相同。

### 3.9 哈斯图

**定义 3.56**  $(A, \leq)$  为一个偏序集, 如果  $x < y$  并且  $\forall z (x \leq z \leq y \rightarrow x = z \vee y = z)$ , 则我们称  $y$  盖住  $x$ 。令

$$COV(A) = \{\langle x, y \rangle \in A \times A \mid y \text{ 盖住 } x\}$$

若  $x < y$  但  $y$  没有盖住  $x$ , 则存在  $z$  满足  $x < z < y$ 。若  $(A, \leq)$  为一个偏序集, 我们可以从  $COV(A)$  得到  $(A, \leq)$  的所有信息:

**定理 3.57** 若  $(A, \leq)$  为一个 (有穷) 偏序集, 则  $x < y$  当且仅当存在  $n \geq 2$ , 存在  $x = x_1, x_2, \dots, x_n = y$  满足  $\langle x_i, x_{i+1} \rangle \in COV(A)$ 。

**证明**  $(\Rightarrow)$  令  $z_0 = x$ 。假设我们已经定义了  $z_n$ 。

- (1) 若  $z_n$  盖住  $x$ , 则令  $x_2 = z_n$ ;
- (2) 若不然, 则存在  $z_{n+1}$  满足  $x < z_{n+1} < z_n$ 。

由于  $A$  是有穷集合, 一定存在一个  $n$ , 情况 (1) 发生。我们得到  $\langle x_1, x_2 \rangle \in COV(A)$ 。若  $x_2 = y$ , 则我们找到了序列; 若  $x_2 < y$ , 我们重复之前的步骤, 寻找  $x_3$  盖住  $x_2$ 。以此类推。

( $\Leftarrow$ ) 由传递性,  $x = x_1 < x_n = y$ 。

□

**定义 3.58** 若  $(A, \leq)$  为一个偏序集, 我们称有向图  $G = (A, COV(A))$  为哈斯图。

见习题 3.12。

### 3.10 习题

**习题 3.1** 计算  $\mathcal{P}(\mathcal{P}(\{1, 2\}))$  及  $\mathcal{P}(\{1, 2\}) \times \{1, 2\}$ 。

**习题 3.2** 判断题 (若为假, 举例说明):

1.  $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$
2.  $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$
3.  $A \setminus (B \cup C) = (A \setminus B) \setminus C$
4.  $(A \cup B \cup C) \setminus (A \cup B) = C$
5.  $(A \cup B) \setminus (B \cup C) = A \setminus C$
6.  $A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$

**习题 3.3** 判断:  $A \setminus B = B \setminus A$  当且仅当  $A = B$ 。若正确, 则证明; 若不正确, 举例说明。

**习题 3.4** 若  $X \times X = Y \times Y$ , 则  $X = Y$ 。

**习题 3.5** 若  $X \times Y = X \times Z$  且  $X \neq \emptyset$ , 则  $Y = Z$ 。

**习题 3.6** 考虑  $A = \{0, 1, 2, 3, 4, 5, 6\}$  上的关系  $R = \{\langle x, y \rangle \mid x < y \vee x \text{ 是质数}\}$ 。写出关系矩阵, 画出关系图。

**习题 3.7** 若  $R, S$  是  $A$  上的二元关系, 并且  $R, S$  是自反的、对称的、传递的。证明  $R \cap S$  也是。

**习题 3.8** 找出一个  $A = \{a, b, c\}$  上的关系  $R$  满足对称性、反自反性, 但不满足传递性。写出它的关系矩阵、画出关系图。

**习题 3.9** 设  $R$  是  $A$  上的等价关系,  $a, b \in A$ 。若  $[a]_R \cap [b]_R \neq \emptyset$ , 则  $[a]_R = [b]_R$ 。

**习题 3.10**  $R$  和  $S$  是  $A$  上的两个等价关系。(不要用反证) 证明: 若  $A/R = A/S$ , 则  $R = S$ 。注: 这题说明定理 3.48 的函数  $f$  为单射。

**习题 3.11**  $A = \{1, 2, 3\}$ ,  $R = \{\langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle 3, 1 \rangle, \langle 1, 1 \rangle, \langle 2, 2 \rangle, \langle 3, 3 \rangle\}$ 。  $R$  是否为偏序关系? 是否存在一个偏序关系  $S$  满足  $R \subseteq S$ ?

**习题 3.12**  $A = \{1, 2, 3, 4, 6, 8, 12\}$ ,  $R$  为  $A$  上的整除关系, 即  $xRy$  当且仅当  $x|y$ 。

1. 画出关系  $R$  的哈斯图。
2. 写出极小点、极大点、最小点、最大点。

## 习题提示

1.1 错、错、对、对、对、对、对。

1.2

1. 正确。
2. 不正确。

1.3

1. 正确。
2. 不正确。

1.4

1. 不正确。
2. 不正确。

1.5 注意到  $\neg p \models p \downarrow p$  以及  $p \wedge q \models \neg p \downarrow \neg q$ , 因此我们可以用  $\downarrow$  表示  $\neg$  和  $\wedge$ 。而  $\{\neg, \wedge\}$  为全功能集, 因此  $\{\downarrow\}$  为全功能集。

1.6  $\neg$  不能诱导二元布尔函数。

考虑由  $\wedge$  或者  $\wedge, \vee$  构成的句子。若每个变元赋值为 1 时, 这类公式的取值为 1。因此, 布尔函数  $G = 0$  无法被这类公式诱导 (即, 这类公式无法表达永假式)。

1.7 由真值表可以验证:  $A + (A \leftrightarrow A) \models \neg A$ , 因此, 我们可以表示  $\neg$ 。由于  $\{\wedge, \neg\}$  为全功能集, 所以  $\{\wedge, \leftrightarrow, +\}$  为全功能集。

$\wedge, \leftrightarrow$  不是全功能集: 若每个变元赋值为 1 时, 这类公式只能取值为 1。

$\wedge, +$  不是全功能集: 若每个变元赋值为 0 时, 这类公式只能取值为 0。

$\leftrightarrow, +$  不是全功能集: 定义

$$S(\alpha, n) = \{v \in \{0, 1\}^n \mid \bar{v}(\alpha) = 1\}$$

其中我们要求  $\alpha$  涉及的变元在  $A_1, A_2, \dots, A_n$  中。

断言若  $\alpha$  涉及的变元在  $A_1, A_2, \dots, A_n$  中, 则  $S(\alpha, n+1)$  为偶数。

给定赋值  $v \in \{0, 1\}^{n+1}$ , 定义  $v^*$  满足  $v^*(A_i) = v(A_i)$  ( $i \leq n$ ) 并且  $v^*(A_{n+1}) \neq v(A_{n+1})$ 。则  $v^* \neq v$ , 并且

$$v(\alpha) = v^*(\alpha)$$

即,  $v$  满足  $\alpha$  当且仅当  $v^*$  满足  $\alpha$  (满足  $\alpha$  的赋值是成双出现的)。所以  $S(\alpha, n+1)$  为偶数。

断言对  $n \geq 2$ ,  $S(\alpha, n)$  为偶数。

固定  $n \geq 2$ , 我们对公式  $\alpha$  (涉及的变元在  $A_1, \dots, A_n$  中) 的复杂度做归纳: 首先,  $S(A_i, n)$  ( $i \leq n$ ) 为偶数。现在, 我们假设  $S(\alpha, n)$  和  $S(\beta, n)$  均为偶数, 我们证明  $S(\alpha \leftrightarrow \beta, n)$  及  $S(\alpha + \beta, n)$  为偶数。我们考虑  $X_{ij} = \{v \in \{0, 1\}^n \mid \bar{v}(\alpha) = i \text{ 且 } \bar{v}(\beta) = j\}$ ,  $i, j \in \{0, 1\}$ 。

- 设  $|X_{00}| = a, |X_{10}| = b, |X_{01}| = c, |X_{11}| = d$
- 则  $a + c = 2^n - |S(\alpha, n)|, b + d = |S(\alpha, n)|, a + b = 2^n - |S(\beta, n)|, c + d = |S(\beta, n)|$  均是偶数。
- $2a + b + c$  是偶数, 因此  $b + c$  是偶数。所以  $a + d = 2^n - (b + c)$  是偶数。
- 因此  $|S(\alpha \leftrightarrow \beta, n)| = a + d, |S(\alpha + \beta, n)| = b + c$  都是偶数。

由归纳得证。

由于  $|S(A \rightarrow B, 2)| = 3$ , 所以  $A \rightarrow B$  无法用  $\leftrightarrow$  和  $+$  表示。

1.8 简单合取式: ①, ②, ③; 简单析取式: ②, ④; 合取范式: ①, ②, ③, ④; 析取范式: ①, ②, ③, ④; 极小项: ③; 极大项: ④; 主合取范式: ④; 主析取范式: ③。

1.9  $A \vee \neg B \vee C$

1.10  $A \wedge B \wedge \neg C \wedge D$

1.11 由真值表知 (略), 该公式的成真赋值为

000, 001, 010, 100, 110

分别对应自然数

0, 1, 2, 3, 6

因此, 主析取范式为

$$m_0 \vee m_1 \vee m_2 \vee m_3 \vee m_6$$

主合取范式为

$$M_4 \wedge M_5 \wedge M_7$$

1.12  $E(A, B, C)$  的成假赋值为

000, 001, 010, 100

(0 比 1 多的序列), 对应的自然数分别为

0, 1, 2, 4

因此, 主合取范式为

$$M_0 \wedge M_1 \wedge M_2 \wedge M_4$$

主析取范式为

$$m_3 \vee m_5 \vee m_6 \vee m_7$$

### 1.13

1. 利用反证法, 记  $\Sigma = \{\neg(P \wedge \neg Q), \neg Q \vee R, \neg R\}$ 。我们证明  $\Sigma \cup \{P\}$  不相容:

- (a)  $\neg(P \wedge \neg Q)$  已知
- (b)  $\neg(P \wedge \neg Q) \rightarrow P \rightarrow Q$  永真 (德摩根)
- (c)  $P \rightarrow Q$  1,2, MP
- (d)  $P$  已知
- (e)  $Q$  3,4,MP
- (f)  $\neg Q \vee R$
- (g)  $(\neg Q \vee R) \rightarrow (Q \rightarrow R)$  永真
- (h)  $Q \rightarrow R$  6,7,MP
- (i)  $R$  5,8,MP

由此知  $\Sigma \cup \{P\} \vdash R, \neg R$ 。所以  $\Sigma \vdash \neg P$ 。

2. 我们只需证明  $\Sigma = \{P \rightarrow Q \rightarrow S, Q, P \vee \neg R, R\} \vdash S$ :

- (a)  $P \vee \neg R$  (已知)
- (b)  $(P \vee \neg R) \rightarrow (R \rightarrow P)$  (永真)
- (c)  $R \rightarrow P$  (1,2,MP)
- (d)  $R$  (已知)
- (e)  $P$  (3,4,MP)
- (f)  $P \rightarrow Q \rightarrow S$  (已知)
- (g)  $Q \rightarrow S$  (5,6,MP)
- (h)  $Q$  (已知)
- (i)  $S$  (7,8,MP)

3. 我们只需证明  $\Sigma = \{P \rightarrow Q, P\} \vdash P \wedge Q$ :

- (a)  $P \rightarrow Q$  (已知)
- (b)  $\star P$  (已知)
- (c)  $\star Q$  (1,2,MP)
- (d)  $P \wedge Q$  (2,3,合取)

4. (a)  $T$  (由已知  $T \wedge R$ )

- (b)  $S \leftrightarrow T$  (已知)
- (c)  $(S \leftrightarrow T) \rightarrow (T \rightarrow S)$  (永真)
- (d)  $T \rightarrow S$  (2,3,MP)
- (e)  $\star S$  (1,4,MP)
- (f)  $Q \leftrightarrow S$  (已知)

- (g)  $(Q \leftrightarrow S) \rightarrow (S \rightarrow Q)$  (永真)  
 (h)  $S \rightarrow Q$  (6,7,MP)  
 (i)  $\star Q$  (5,8,MP)  
 (j)  $Q \rightarrow P$  (已知)  
 (k)  $\star P$  (9,10,MP)  
 (l)  $\star R$  (已知  $T \wedge R$ )  
 (m)  $P \wedge Q \wedge S \wedge R$  (由 5,9,11,12)
5. 令  $\Sigma = \{(P \wedge Q) \rightarrow R, \neg R \vee S, \neg S, P\}$ , 我们证明  $\Sigma \cup \{Q\}$  不相容:
- (a)  $P$  (已知)  
 (b)  $Q$  (已知)  
 (c)  $P \wedge Q$  (1,2, 合取)  
 (d)  $(P \wedge Q) \rightarrow R$  (已知)  
 (e)  $R$  (3,4,MP)  
 (f)  $\neg R \vee S$  (已知)  
 (g)  $(\neg R \vee S) \rightarrow (R \rightarrow S)$  (永真)  
 (h)  $R \rightarrow S$  (5,6,MP)  
 (i)  $S$  (7,8,MP)  
 (j)  $\neg S$  (已知)  
 (k)  $S \wedge \neg S$  (8,9, 合取)
- 所以  $\Sigma \cup \{Q\}$  不相容, 因此,  $\Sigma \vdash \neg Q$ 。

## 2.1

- $\exists x \forall y (y \neq x \rightarrow y < x)$
- $\exists x \forall y (y \neq x \rightarrow x < y)$
- $\exists x \exists y (x < y \wedge x \not> y \wedge x \neq y)$

## 2.2

- $\forall x (x \neq 0 \rightarrow \exists y (x \times y = 1))$
- $\forall x \exists y (x + y = 0)$
- $\forall x (x + 0 = x)$
- $\forall x (x \times 1 = x \wedge 1 \times x = x)$
- $\forall x \forall y (x + y = y + x)$
- $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$
- $\forall x \forall y (x \times y = y \times x)$
- $\forall x \forall y \forall z (x \times (y \times z) = (x \times y) \times z)$
- $\forall x \forall y \forall z (x \times (y + z) = (x \times y) + (x \times z))$

## 2.4

$$\forall x (P(x, y) \wedge \exists y Q(x, y))$$

其中黑色  $y$  是自由变元, 蓝色  $y$  被  $\exists y$  约束, 红色  $x$  被  $\forall x$  约束。

2.5 任取结构  $M$  和赋值  $s$  满足  $M \models \forall x (\alpha \rightarrow \beta), \forall x \alpha[s]$ , 我们想要证明  $M \models \forall x \beta[s]$ : 任取  $m \in M$ , 我们都有

1.  $M \models \alpha \rightarrow \beta[s_x^m]$
2.  $M \models \alpha[s_x^m]$

由 1 的定义, 我们知  $M \models \neg \alpha[s_x^m]$  或  $M \models \beta[s_x^m]$ 。再由 2 我们得到  $M \models \beta[s_x^m]$ 。由于  $m$  的任意性, 得

$$M \models \forall x \beta[s]$$

综上,  $\forall x (\alpha \rightarrow \beta), \forall x \alpha \vdash \forall x \beta$ 。

2.6 取任意结构  $M$  和赋值  $s$  满足  $M \models \alpha[s]$ 。由于  $x$  不是  $\alpha$  的自由变量, 因此  $s(x)$  的取值不影响  $\alpha$  的真假。确切的说, 任取  $m \in M$ , 我们有  $M \models \alpha[s_x^m]$ 。由于  $m$  的任意性, 我们得到

$$M \models \forall x \alpha$$

2.7

$$\exists x_1 \exists x_2 \exists x_3 \forall y [( \bigwedge_{1 \leq i < j \leq 3} x_i \neq x_j ) \wedge (y = x_1 \vee y = x_2 \vee y = x_3)]$$

2.8  $\forall x \exists y (y < x)$ 2.9  $M_1$  中为真: 1, 3;  $M_2$  中为真: 1, 3, 4。

2.10

- 取任意结构  $M$  和赋值  $s$  满足  $M \models \forall x \alpha \vee \forall x \beta[s]$ , 则

$$M \models \forall x \alpha[s] \text{ 或 } M \models \forall x \beta[s]$$

不妨假设  $M \models \forall x \alpha[s]$ , 则对任意  $m \in M$ ,  $M \models \alpha[s_x^m]$ , 因此, 由定义得  $M \models \alpha \vee \beta[s_x^m]$ 。由于  $m$  的任意性得,

$$M \models \forall x (\alpha \vee \beta)[s]$$

右边不蕴涵左边: 取自然数结构  $\mathbb{N}$ ,  $\alpha$  为  $\exists y (y + y = x) (x \text{ 为偶数})$ ,  $\beta$  为  $\exists y (y + y + 1 = x) (x \text{ 为奇数})$ , 则  $\mathbb{N} \models \forall x (\alpha \vee \beta)$ , 但我们既没有  $M \models \forall x \alpha$  也没有  $M \models \forall x \beta$ 。因此,  $M \not\models \forall x \alpha \vee \forall x \beta$ 。

- 提示: 用奇数偶数的例子可以说明不等值。

2.11 分别作等值演算

- $\exists x F(x) \vee \forall y G(x, y)$
- $\exists z F(z) \vee \forall y G(x, y)$
- $\exists z \forall y (F(z) \vee G(x, y))$
- $\exists x \neg F(x, y) \wedge \forall y \neg G(x, y)$
- $\exists u \neg F(u, y) \wedge \forall v \neg G(x, v)$
- $\exists u \forall v (\neg F(u, y) \wedge \neg G(x, v))$
- $\forall z F(z) \vee \exists y G(x, y)$
- $\forall z \exists y (F(z) \vee G(x, y))$

3.1

$$\begin{aligned} \mathcal{P}(\{1, 2\}) &= \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \\ \mathcal{P}(\mathcal{P}(\{1, 2\})) &= \{\emptyset, \\ &\quad \{\emptyset, \{1\}\}, \{\{2\}, \{1, 2\}\}, \\ &\quad \{\emptyset, \{1\}\}, \{\emptyset, \{2\}\}, \{\emptyset, \{1, 2\}\}, \{\{1\}, \{2\}\}, \{\{1\}, \{1, 2\}\}, \{\{2\}, \{1, 2\}\}, \\ &\quad \{\emptyset, \{1\}, \{2\}\}, \{\emptyset, \{1\}, \{1, 2\}\}, \{\emptyset, \{1, 2\}, \{2\}\}, \{\{1\}, \{2\}, \{1, 2\}\}, \\ &\quad \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}\} \\ \mathcal{P}(\{1, 2\}) \times \{1, 2\} &= \{(\emptyset, 1), (\emptyset, 2), (\{1\}, 1), (\{1\}, 2), (\{2\}, 1), (\{2\}, 2), (\{1, 2\}, 1), (\{1, 2\}, 2)\} \end{aligned}$$

3.2 真的有 1, 2, 3, 6。

4 的反例: 令  $A = \{1\}, B = \emptyset, C = \{1, 2\}$ , 则左边为  $\{2\}$ , 不等于  $C$ 。5 的反例: 令  $A = \{1\}, B = \{1\}, C = \emptyset$ , 则左边为  $\emptyset$ , 右边为  $\{1\}$ 。

3.3 正确。

 $(\Leftarrow)$  此时  $A \setminus B = \emptyset = B \setminus A$ 。

$(\Rightarrow)$  任取  $a \in A$ 。若  $a \in A \cap B$ , 则  $a \in B$ ; 若  $a \in A \setminus B = B \setminus A$ , 则  $a \in B$ 。由  $a$  的任意性知,  $A \subseteq B$ 。同理可证  $B \subseteq A$ 。因此  $A = B$ 。

3.4 若  $X = \emptyset$ , 则  $Y \times Y = X \times X = \emptyset$ 。因此  $Y = \emptyset = X$ 。

若  $X \neq \emptyset$ , 任取  $x \in X$ 。由于  $\langle x, x \rangle \in X \times X = Y \times Y$ , 得到  $x \in Y$ 。因此  $X \subseteq Y$ 。同理可得  $Y \subseteq X$ 。因此,  $X = Y$ 。

3.5 取  $x \in X$ 。任取  $a \in Y$ 。则  $\langle x, a \rangle \in X \times Y = X \times Z$ , 因此,  $a \in Z$ 。因此,  $Y \subseteq Z$ 。同理可证  $Z \subseteq Y$ 。因此,  $Y = Z$ 。

3.6

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

关系图略。

3.7 记  $T = R \cap S$ 。

(自反) 任取  $x \in A$ 。  $\langle x, x \rangle \in R$  并且  $\langle x, x \rangle \in S$ 。因此,  $\langle x, x \rangle \in R \cap S$ 。即,  $xTx$ 。

(对称) 若  $xTy$ 。则  $\langle x, y \rangle \in R$  并且  $\langle x, y \rangle \in S$ 。由  $R, S$  的对称性知,  $\langle y, x \rangle \in R \cap S = T$ 。即,  $yTx$ 。

(传递) 若  $xTy, yTz$ , 则  $\langle x, y \rangle, \langle y, z \rangle \in R \cap S$ 。由传递性,  $\langle x, z \rangle \in R \cap S = T$ 。即,  $xTz$ 。

3.8

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

关系图略。

该关系有  $bRa$  且  $aRb$ 。但该关系没有  $bRb$ 。因此, 不满足传递性。

由关系矩阵易知, 该关系满足对称性和反自反性。

3.9 取  $c \in [a]_R \cap [b]_R$ , 则有  $aRc$  且  $bRc$ 。由于对称性, 有  $cRb$ , 由传递性有  $aRb$ 。因此,  $[a]_R = [b]_R$ 。

3.10  $(R \subseteq S)$  取  $\langle a, b \rangle \in R$ , 即  $aRb$ 。由于  $A/R = A/S$ , 存在  $c$  满足

$$[a]_R = [b]_R = [c]_S$$

因此,  $cSa$  和  $cSb$ 。由  $S$  的对称性知,  $aSc$ 。由传递性知,  $aSb$ 。即,  $\langle a, b \rangle \in S$ 。

$(S \subseteq R)$  同理。

因此  $R = S$ 。

3.11 不满足传递性。

不存在。因为  $S$  若满足传递性, 则由  $1S2, 2S3$  得  $1S3$ 。由于同时又有  $3S1$ , 与反对称性矛盾。

3.12 (1) 哈斯图略。盖住关系为 1 盖住无更小元; 2, 3, 4 盖住 1; 6 盖住 2, 3; 8 盖住 4; 12 盖住 4, 6。

(2) 极小点为 1。最小点为 1。极大点为 8 和 12。最大点不存在。