信息安全数学基础

（内部教材）

院系：计算机科学与技术学院
教师：韩 琦

版本：2023秋_v_20230910

第一部分

数理逻辑

第 1 章　数理逻辑

本章我们介绍数理逻辑中的两个最基本的问题：命题逻辑和谓词逻辑。逻辑学(logic)是由古希腊学者亚里士多德创建的，是探索、阐述和确立有效推理原则的学科。传统的逻辑学用自然语言表示各种命题形式和推理形式，但是自然语言常常具有多义性，因此并不适合精确的表示命题和推理。而数理逻辑则是用数学的方法来研究关于推理、证明等问题的学科，以其特有的人工符号来书写逻辑法则，突出体现了方便、精确的优势。

经典命题逻辑和一阶谓词逻辑在计算机科学中应用最为广泛，也是数理逻辑中最成熟的部分，而命题逻辑是数理逻辑的最基础部分，谓词逻辑是在它的基础上发展起来的。首先我们介绍一下经典命题逻辑。

1.1 经典命题逻辑

命题逻辑(propositional logic)是数理逻辑的基础，以命题为研究对象，研究基于命题的符号逻辑体系及推理规律。我们的课程主要介绍以下几个问题：

1. 简单命题与复合命题：什么是命题，命题联结词及其含义；
2. 命题公式与赋值：命题逻辑公式的归纳定义，命题公式的真值表；
3. 等值演算：命题公式的等值赋值，重要的等值式；
4. 命题公式的范式：析取范式与合取范式；
5. 命题演算系统：使用命题逻辑公式进行推理的形式系统。

1.1.1 简单命题与复合命题

在经典命题逻辑中，**命题**(proposition)是可以判断真假的陈述句。命题必须为陈述句，不能为疑问句、祈使句、感叹句等，例如：

- 2大于1；
- $\sqrt{3}$是无理数；
- 有两条腿、直立行走的是人。

而下面的句子不是命题：

- 大海啊，全是水！

- 当时你的车速只有70公里/小时？
- 上天赐我们一支真正的国家队吧！

但是，要注意！不是所有的陈述句都是命题，无法判断其真假的陈述句也不是命题：

- 我正在说谎；
- $x+y>10$。

那些我们现在无法判断其真假的陈述句，但是只要它具有唯一的真假值，就也是命题，比如：

- 2012年有大灾难；
- 我35岁的时候能买得起劳斯莱斯；
- 玛雅文明毁于殷商的远洋舰队。

经典命题逻辑不区分现在已经确定为真，还是将来可能确定为真这种情况，时态逻辑处理与时间有关的真值问题；经典命题逻辑也不区分是在技术上可以确定为真，还是现在的技术条件下不可以确定为真的这种情况。

如果命题的真值为真，则称为真命题，否则称为假命题。下面介绍几个基本概念：

命题常量：

命题符号p代表命题常量，则意味着它是某个具体命题的符号化；

命题变量：

命题符号p代表命题变量，则意味着它可指代任何具体命题。

kai 一般地，如果没有特殊说明，命题符号p、q等是命题变量。

简单命题与复合命题：

不能分成更简单的陈述句的命题为简单命题(或叫原子命题)，否则称为复合命题。

复合命题使用命题联结词联结简单命题而来，命题联结词如表??所示：

上述定义中的非(negation)、合取(conjunction)、析取(disjunction)、蕴含(implication)和等价(equivalence)是命题逻辑中的术语，而引号中给出的复合命题是自然语言中的典型用法。可以看出，命题逻辑中符号化形式的复合命题在自然语言中有许多种表达方法，自然语言多义性的特点可见一斑。

复合命题与简单命题之间的真值关系可以用表??给出，其中0代表假，1代表真。

表 1-1 联结词

联结词	符 号	称 谓	读 法
非	$\neg$	否定	$\neg p$读作“非p”
与	$\wedge$	合取	$p\wedge q$读作“p且q”
或	$\vee$	析取	$p\vee q$读作“p或q”
如果$\cdots$，那么$\cdots$	$\rightarrow$	蕴含	$p\rightarrow q$读作“p蕴含q”或者“如果p则q”
当且仅当	$\leftrightarrow$	等价	$p\leftrightarrow$读作“p与q等价”或者“p当且仅当q”

表 1-2 复合命题真值表

p	q	$\neg p$	$p\wedge q$	$p\vee q$	$p\rightarrow q$	$p\leftrightarrow q$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

逻辑联结词也称为逻辑运算符，规定优先级的顺序为$\neg$、$\wedge$、$\vee$、$\rightarrow$、$\leftrightarrow$，若有括号时，先进行括号内运算。例如：

$$p\rightarrow(q\vee\neg p)\wedge(q\vee r)\leftrightarrow\neg q$$

的运算顺序为：

1. $\neg p$和$\neg q$；
2. $q\vee\neg p$和$q\vee r$；
3. $(q\vee\neg p)\wedge(q\vee r)$；
4. $\rightarrow$；
5. $\leftrightarrow$。

再举一个简单的例子，来看一下自然语言中的命题和逻辑运算符如何转换：

例 1.1 设p：小明聪明，q：小明用功。

1. 小明既聪明又用功；
2. 小明虽然聪明，但不用功；
3. 小明不但聪明，而且用功；
4. 小明不是不聪明，而是不用功。

解： 若用p表示“小明聪明”，q表示“小明用功”，则上述命题表达式分别如下：

1. $p \wedge q$；
2. $p \wedge \neg q$；
3. $p \wedge q$；
4. $\neg(\neg p) \wedge \neg q$。

1.1.2 命题逻辑公式

定义 1.1 (**命题逻辑公式**) 命题逻辑公式(propositional logic formula)由以下子句归纳定义：

1. 命题常量或命题变量是命题逻辑公式，称为命题逻辑公式的原子项；
2. 如果A、B是命题逻辑公式，则$(\neg A)$、$(A \wedge B)$、$(A \vee B)$、$(A \rightarrow B)$和$A \leftrightarrow B$也是命题逻辑公式；
3. 所有的命题逻辑公式都通过1.和2.得到。

定理 1.1 设R是某个性质，如果有：

1. 对于所有的原子项p，都满足性质R；
2. 如果对任意的公式A和B都满足性质R，就有$(\neg A)$、$(A \wedge B)$、$(A \vee B)$、$(A \rightarrow B)$和$A \leftrightarrow B$也满足性质R。

那么，所有的公式A就都满足性质R。

任意命题逻辑公式A具有下列6种形式之一，且只具有其中一种形式：

1. A为原子项
2. $(\neg A)$
3. $(A \wedge B)$
4. $(A \vee B)$
5. $(A \rightarrow B)$
6. $(A \leftrightarrow B)$

定义 1.2 对命题公式的一次真值赋值t是从所有命题变量所组成的集合倒集合$\{0,1\}$的函数。

定义 1.3 命题公式A在真值赋值$t:U\rightarrow\{0,1\}$下的真实$t(A)$递归定义如下：

1. 如果命题公式A是命题常量p，则如果p为真，$t(A)=1$，否则$t(A)=0$；
2. 如果命题公式A是一个命题变量p，则$t(A)=t(p)$；
3. 若$t(A)=0$则$t(\neg A)=1$，否则$t(\neg A)=0$；
4. 若$t(A)=t(B)=1$，则$t(A\wedge B)=1$，否则$t(A\wedge B)=0$；
5. 若$t(A)=t(B)=0$，则$t(A\wedge B)=0$，否则$t(A\wedge B)=1$；
6. 若$t(A)=0$或者$t(B)=1$，则$t(A\rightarrow B)=1$，否则$t(A\rightarrow B)=0$；
7. 若$t(A)=t(B)$，则$t(A\leftrightarrow B)=1$，否则$t(A\leftrightarrow B)=0$。

定义 1.4 如果命题公式A在任意的真值赋值函数$t:U\rightarrow\{0,1\}$下的真值$t(A)$都为1，则称命题公式A为永真式(tautology)(或称重言式)；如果命题公式A在任意的真值赋值函数下的真值都为0，则称A为矛盾式(contradiction)；如果A不是矛盾式，则称为可满足式。

定义 1.5 使用符号Σ来表示一组命题公式所构成的集合，定义Σ在真值赋值函数$t:U\rightarrow\{0,1\}$下的真值$t(\Sigma)$为：$t(\Sigma)=1$当且仅当Σ中任意公式A有$t(A)=1$，否则定义$t(\Sigma)=0$。说Σ是可满足的，如果存在某个真值赋值函数t使得$t(\Sigma)=1$，这时称t满足Σ。

设Σ是一组命题公式的集合，说命题公式A是以Σ为前提的永真式，如果满足对任意满足Σ的真值赋值函数t都有$t(A)=1$，这时记为$\Sigma\models A$.

如果Σ为空集，则$\Phi\models A$表示A为永真式。

1.1.3 等值演算

定义 1.6 当$\Sigma=\{A_1,A_2,\cdots,A_n\}$时，也记$\Sigma\models A$为$A_1,A_2,\cdots,A_n\models A$。如果有$A\models B$且$B\models A$，则称命题公式$A$ 与B等值，记为$A\Leftrightarrow B$。

于是，显然有下面的定理：

定理 1.2 $A\Leftrightarrow B$当且仅当$A\leftrightarrow B$是永真的。

设A、B、C是任意的命题公式，使用真值表不难证明下面逻辑等价式：

1. 双重否定律：$A \Leftrightarrow (\neg(\neg A))$

2. 等幂律：$A \Leftrightarrow (A \wedge A)$，$A \Leftrightarrow (A \vee A)$

3. 交换律：$(A \vee B) \Leftrightarrow (B \vee A)$，$(A \wedge B) \Leftrightarrow (B \wedge A)$

4. 结合律：$((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C))$，$((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))$

5. 分配律：$(A \vee (B \wedge C)) \Leftrightarrow (A \vee B) \wedge (A \vee C))$，$(A \wedge (B \vee C)) \Leftrightarrow (A \wedge B) \vee (A \wedge C))$

6. 德摩根律：$(\neg(A \vee B)) \Leftrightarrow ((\neg A) \wedge (\neg B))$，$(\neg(A \wedge B)) \Leftrightarrow ((\neg A) \vee (\neg B))$

7. 吸收律：$(A \vee (A \wedge B)) \Leftrightarrow A$，$(A \wedge (A \vee B)) \Leftrightarrow A$

8. 零律：$(A \vee 1) \Leftrightarrow 1$，$(A \wedge 0) \Leftrightarrow 0$

9. 同一律：$(A \vee 0) \Leftrightarrow A$，$(A \wedge 1) \Leftrightarrow A$

10. 排中律：$(A \vee (\neg A)) \Leftrightarrow 1$

11. 矛盾律：$(A \wedge (\neg A)) \Leftrightarrow 0$

12. 蕴涵等值律：$(A \rightarrow B) \Leftrightarrow ((\neg A) \vee B)$

13. 等价等值律：$(A \leftrightarrow B) \Leftrightarrow ((A \rightarrow B) \wedge (B \rightarrow A))$

14. 假言易位律：$(A \rightarrow B) \Leftrightarrow ((\neg B) \rightarrow (\neg A))$

15. 等价否定等值律：$(A \leftrightarrow B) \Leftrightarrow ((\neg A) \leftrightarrow (\neg B))$

16. 归谬论：$((A \rightarrow B) \wedge (A \rightarrow (\neg B))) \Leftrightarrow (\neg A)$

定理 1.3 (1) $A_1, A_2, \cdots, A_n \models A$当且仅当$\phi \models ((A_1 \wedge A_2 \wedge \cdots \wedge A_n) \rightarrow A)$；
(2) $A_1, A_2, \cdots, A_n \models A$当且仅当$\phi \models (A_1 \rightarrow (A_2 \rightarrow (\cdots (A_n \rightarrow A) \cdots)))$。

定理 1.4 设有$A \Leftrightarrow A'$和$B \Leftrightarrow B'$，则有：

1. $(\neg A) \Leftrightarrow (\neg A')$

2. $(A \wedge B) \Leftrightarrow (A' \wedge B')$

3. $(A \vee B) \Leftrightarrow (A' \vee B')$

4. $(A \rightarrow B) \Leftrightarrow (A' \rightarrow B')$

5. $(A \leftrightarrow B) \Leftrightarrow (A' \leftrightarrow B')$

定理 1.5 设有$B \Leftrightarrow C$，而A'是命题公式A通过使用C替换A中出现的某些B(不需要替换所有的B)而得到的命题公式，则有$A \Leftrightarrow A'$。

定义 1.7 如果命题公式A中只出现命题变量、命题常量、命题联接符号$\neg$、$\wedge$和$\vee$则称为限制性(命题)公式。定义：

1. 对于限制性公式A，将其中的命题联接符号$\wedge$换成$\vee$，命题联接符号$\vee$换成$\wedge$得到的公式称为A的对偶公式(dual formula)，记为A^{op}；

2. 对于限制性公式A，将其中出现的所有原子项(命题变量或命题常量)p换成$\neg p$得到的公式称为A的内否式，记为$A^{\neg}$。

定理 1.6 设公式A、B都是限制性公式，有：

1. $(A^{op})^{op} \equiv A$，$(A^{\neg})^{\neg} \equiv A$
2. $(A \vee B)^{op} \equiv A^{op} \wedge B^{op}$，$(A \vee B)^{\neg} \equiv A^{\neg} \vee B^{\neg}$
3. $(A \wedge B)^{op} \equiv A^{op} \vee B^{op}$，$(A \wedge B)^{\neg} \equiv A^{\neg} \wedge B^{\neg}$
4. $(A^{op})^{\neg} \equiv (A^{\neg})^{op}$

定理 1.7 设公式A是任意的限制性公式，有

1. $(\neg A)^{op} \Leftrightarrow \neg(A^{op})$，$(\neg A)^{\neg} \Leftrightarrow \neg(A^{\neg})$
2. $(A^{op})^{\neg} \Leftrightarrow \neg A$

推论 1.8 设公式A和B都是限制性公式，有$A \Leftrightarrow B$则$(A^{op})^{\neg} \Leftrightarrow (B^{op})^{\neg}$。

1.1.4 命题公式的范式

定义 1.9 由有限个简单合取式构成的析取式称为析取范式(disjunctive normal form)，由有限个简单析取式构成的合取式称为合区范式(conjunctive normal form)。析取范式和合取范式统称为范式(normal form)。一个析取范式是矛盾式当且仅当它的每个简单合取式都是矛盾式。一个合区范式是永真式当且仅当它的每个简单析取式都是永真式。

定理 1.8 任意命题公式都存在与之等值的析取范式与合区范式。

1.1.5 命题演算系统

定义 1.10 命题演算系统(system of propositional calculus)P定义如下：

1. P的符号表包括：

(a) 命题变元：小写英文字母并可加下标。

(b) 联结词：$\neg$、$\rightarrow$。

(c) 辅助符号：(,)(圆括号)。

2. P的公式归纳定义如下：

(a) 命题变元是公式。

(b) 若A是公式，则$(\neg A)$也是公式。

(c) 若A和B是公式，则$(A \to B)$也是公式。

(d) 所有公式都是通过有限次使用1、2和3得到。

3. P的公理模式有如下3个：

(a) **肯定前件律**：$(A \to (B \to A))$

(b) **分配律**：$((A \to (B \to C))) \to ((A \to B) \to (A \to C))$

(c) **逆否定律**：$(((\neg A) \to (\neg B)) \to (B \to A))$

4. P的规律只有一条：

(a) **分离规则**：由A和$(A \to B)$可得到B

定义 1.11 命题演算系统P中的证明是由P中公式组成的一个序列：$A_1, A_2, \cdots, A_n$使得对每个$i(1 \le i \le n)$，下列两个条件之一成立：

1. A_i是公理，或者

2. A_i是由上述序列中A_i之前的某两个公式$A_j, A_k(1 \le j, k \le i)$应用分离规则得到。此时$A_1, A_2, \cdots, A_n$称为$A_n$的一个证明，而$A_n$称为$P$的一个内定理，记为$\vdash A_n$。

定理 1.9 (传递规则T_r) 设A、B、C是P中的3个公式，若$\vdash A \to B$，且$\vdash B \to C$，则$\vdash A \to C$。

定义 1.12 设Σ是P中的一个公式集，称P中的公式序列：$A_1, A_2, \cdots, A_n$为前提Σ下推出A_n的一个证明，如果对每个$i(1 \le i \le n)$，下列3个条件之一成立：

1. A_i是公理，或者

2. $A_i \in \Sigma$，或者

3. A_i是由上述序列中A_i之前的某两个公式$A_j, A_k(1 \le j, k \le i$应用分离规则得到。此时记为$\Sigma \vdash A_n$。

定理 1.10 (演绎定理) 设Σ是P中的公式集，A和B是P中的两个公式，若$\Sigma \cup \{A\} \vdash B$，则$\Sigma \vdash A \to B$。

定理 1.11 (演绎定理的逆定理) 设Σ是P中的公式集，A和B是P中的两个公式，若$\Sigma \vdash A \to B$，则$\Sigma \cup \{A\} \vdash B$。

由以上两个定理得到：

推论 1.13 $\{A_1, A_2, \cdots, A_n\}$当且仅当$\vdash (A_1 \to (A_2 \to \cdots \to (A_n \to A) \cdots))$。

定理 1.12 设Σ是P中的公式集，$A_1, A_2, \cdots, A_n$为P中的公式，若有$\Sigma \vdash A_1, \Sigma \vdash A_2, \cdots, \Sigma \vdash A_n$，且$A_1, A_2, \cdots, A_n \vdash A$，则$\Sigma \vdash A$。

定理 1.13 合取的引入和消除规则：

1. **合取的引入**：$A, B \vdash A \wedge B$
2. **合取的消除**：$A \wedge B \vdash A, B$(这代表$A \wedge B \vdash A$及$A \wedge B \vdash B$)

定理 1.14 析取的引入和消除规则：

1. **析取的引入**：$A \vdash A \vee B, A \vdash B \vee A$
2. **析取的消除**：$A \to B, C \to B, A \vee C \vdash B$

定理 1.15 对于P的任意一个公式A，若有$\vdash A$，则A是一个永真式。

定理 1.16 不存在P的一个公式A，使得$\vdash A$和$\vdash (\neg A)$都成立。

定理 1.17 若A是P的永真式，则有$\vdash A$。

1.2 经典一阶逻辑

命题逻辑的基本研究单位是原子命题。在命题逻辑中，原子命题是不能再分割的了，这对研究命题间的关系而言是比较适合的。但是，在进一步研究时就会发现，命题逻辑这种工具是非常不充分的。其主要原因就在于这种推理中需要对原子命题作进一步分解，在命题间具有必然的内在逻辑关系，只有对这种内在逻辑联系深入研究后，才能解决形式逻辑中的一些推理问题。一阶逻辑(first-order logic)正是为此目的，他对原子命题进行进一步分解，并在此基础上建立起了一个完整体系，一阶逻辑又称为谓词逻辑(predicate logic)。

1.2.1 基本概念

一阶逻辑中，命题被分解为个体和谓词两部分。**个体**(individuals)是指可独立存在的客体，可以是一个具体的事物，也可以是一个抽象的概念。**谓词**(predication)是用来刻画个体的性质及事物关系的词。为了描述对个体所进行的某种变换，引入所谓**函词**的概念。函词与谓词的区别在于，函词作用在个体上，而产生另一个个体，而谓词作用在个体上产生的是一个命题。

个体常项是表示具体或特定的个体的个体词，**个体变项**是表示抽象或泛指的个体词。个体变项的取值范围称为**个体域**，当个体域不同时，一阶逻辑公

式的含义不同。为了使公式有一致的含义，可引入一个**全总域**，表示宇宙间所有个体所组成的域。在某些情况下，全总域也可指所讨论的问题范围内的所有个体。

1.2.2 一阶逻辑公式及解释

一阶逻辑语言的符号包括：

1. **个体常项**：通常用排在前面的小写字母表示，$a, b, c, \cdots, a_i, b_i, c_i, \cdots$；
2. **个体变项**：通常用排在后面的小写字母表示，$x, y, z, \cdots, x_i, y_i, z_i, \cdots$；
3. **函数符号**：通常用排在中间的小写字母表示，$f, g, h, \cdots, f_i, g_i, h_i, \cdots$；
4. **谓词符号**：通常用排在中间的大写字母表示，$F, G, H, \cdots, F_i, G_i, H_i, \cdots$；
5. **量词符号**：全称量词$\forall$、存在量词$\exists$；
6. **联接符号**：$\neg$、$\wedge$、$\vee$、$\leftrightarrow$、$\rightarrow$；
7. **辅助符号**：(、)、,(逗号)。

一阶逻辑中的逻辑符号应用于任何问题时都是通用的、不变的，而其中的非逻辑符号则在不同的应用问题中有所不同，可以变化，因此一阶逻辑语言的表达能力非常强，它可通过采用不同的非逻辑符号来增强自己的表达能力。

定义 1.14 一阶逻辑语言的项(term)递归定义如下：

1. 个体常项和个体变项是项。
2. 若$f(x_1, x_2, \cdots, x_n)$是n元函数，$t_1, t_2, \cdots, t_n$是n个项，则$f(t_1, t_2, \cdots, t_n)$是项。
3. 一阶逻辑语言的所有项都通过有限次使用上述步骤生成。

定义 1.15 一阶逻辑语言的合式公式(well-formed formula)递归定义如下：

1. 若$F(x_1, x_2, \cdots, x_n)$是n元谓词，$t_1, t_2, \cdots, t_n$是n个项，则$F(t_1, t_2, \cdots, t_n)$是合式公式，此类合式公式称为原子公式。
2. 若A、B是合式公式，则$(\neg A), (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B)$也是合式公式。
3. 若A是合式公式，则$(\forall x)A, (\exists x)A$也是合式公式。
4. 一阶逻辑语言的所有公式都通过有限次使用上述步骤生成。

通常r, s, t, r_i, s_i, t_i表示项，而用$A, B, C, \cdots, A_i, B_i, C_i, \cdots$表示合式公式。称公式$(\forall x)A$中的$A$为量词$(\forall x)$的辖域(scope)，称公式$(\exists x)A$中$A$为量词$(\exists x)$的

辖域。称变元x在公式A中的某处出现是约束出现，如果该出现处于量词$(\forall x)$或$(\exists x)$的辖域内，或者就是量词中x。若x在公式A中的某处出现不是约束出现，则此出现称为自由出现。

设变元x在公式A中出现，如果x在A中的所有出现都是约束出现，则称x为A的约束变元(bounded variable)，否则称x为A的自由变元(free variable)。

变元x在公式A中可同时有约束出现和自由出现两种情况，而只有当x的所有出现都是约束出现时，称x为A的约束变元。

为了明确起见，通常再用字母$A, B, C, \cdots$表示一阶逻辑公式时，同时列出该公式中的自由变元，而写成$A(x_1, x_2, \cdots, x_n)$等，表示公式A中的所有自由变元皆在$x_1, x_2, \cdots, x_n$中。一阶逻辑中，存在如下约束变元换名规则和自由变元替换规则：

R-FL1(换名规则)对于公式$(\forall x)A$或$(\exists x)A$，设变元y不在A中出现，则将其中$(\forall x)$或$(\exists x)$改为$(\forall y)$或$(\exists y)$，且将A中出现的所有x都改成y，得到公式$(\forall y)A$或$(\exists y)A$与原公式等价。

R-FL2(替换原则)对于公式$A(x)$，设y不在A中出现，将其中所有自由出现的x改为y，得到公式$A(y)$与原公式等价。

1.2.3 一阶逻辑的等值演算与前束范式

设A和B是一阶逻辑中任意的两个公式，若$A \leftrightarrow B$是永真式，则称A与B等值，记为$A \Leftrightarrow B$，称$A \Leftrightarrow B$为等值式。下面定理给出与量词无关、一阶逻辑特有的一些等值式：

E-FL1(消除量词)在有限个体域$D = \{a_1, z_2, \cdots, a_n\}$中：

1. $(\forall x)A(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \cdots \wedge A(a_n)$
2. $(\exists x)A(x) \Leftrightarrow A(a_1) \vee A(a_2) \vee \cdots \vee A(a_n)$

E-FL1(量词否定等值式)

1. $\neg(\forall x A(x)) \Leftrightarrow \exists x(\neg A(x))$
2. $\neg(\exists x A(x)) \Leftrightarrow \forall x(\neg A(x))$

E-FL1(收缩与扩张等值式)下述等值式中，变元x不在B中出现：

1. $\forall x(A(x) \vee B) \Leftrightarrow (\forall x A(x)) \vee B$
2. $\forall x(A(x) \wedge B) \Leftrightarrow (\forall x A(x)) \wedge B$
3. $\forall x(A(x) \to B) \Leftrightarrow (\exists x A(x)) \to B$
4. $\forall x(B \to A(x)) \Leftrightarrow B \to (\forall x A(x))$

5. $\exists x(A(x) \vee B) \Leftrightarrow (\exists x A(x)) \vee B$
6. $\exists x(A(x) \wedge B) \Leftrightarrow (\exists x A(x)) \wedge B$
7. $\exists x(A(x) \to B) \Leftrightarrow (\forall x A(x)) \to B$
8. $\exists x(B \to A(x)) \Leftrightarrow B \to (\exists x A(x))$

E-FL1(量词分配等值式)

1. $(\forall x(A(x) \wedge B(x)) \Leftrightarrow (\forall x A(x)) \wedge (\forall x B(x))$
2. $(\exists x(A(x) \vee B(x)) \Leftrightarrow (\exists x A(x)) \vee (\exists x B(x))$

E-FL1(量词顺序变换等值式)

1. $\forall x \forall y(A(x,y) \Leftrightarrow \forall y \forall x(A(x,y)$
2. $\exists x \exists y(A(x,y) \Leftrightarrow \exists y \exists x(A(x,y)$

设A为一阶逻辑公式，若A具有如下形式：$Q_1x_1Q_2x_2\cdots Q_nx_nB$，则称$A$为前束范式(prenex normal form)。其中$Q_i(1 \le i \le n)$是$\forall$或$\exists$，B为不含量词的公式。

定理 1.18 对于任意的一阶逻辑公式A，都存在与之等值的前束范式。

1.2.4 一阶逻辑的推理理论

一阶逻辑的推理形式与命题逻辑类同：

定义 1.16 称蕴涵式$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \to B$为推理的形式结构，$A_1, A_2, \cdots, A_k$为推理的前提，$B$为推理的结论。若$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \to B$为永真式，则称从前提$A_1, A_2, \cdots, A_k$推出结论$B$的推理正确(或说有效)，$B$是$A_1, A_2, \cdots, A_k$的逻辑结论或称有效结论，否则称推理不正确。若从前提$A_1, A_2, \cdots, A_k$推出结论B的推理正确，则记为$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow B$。

定义 1.17 一个描述推理过程的一阶公式序列$A_1, A_2, \cdots, A_n$，其中的每个一阶公式或者是已知的前提，或者是由某些前提应用推理规则得到的结论，满足这样条件的公式序列$A_1, A_2, \cdots, A_n$称为结论A_n的证明。

通过对命题逻辑公式进行替换，一阶逻辑的推理可使用命题逻辑的推理规则有3条：

- R-FL3(前提引入规则) 在证明的任何步骤都可以引入已知的前提
- R-FL4(结论引入规则)在证明的任何步骤都可以引入这次已经得到的结论作为后续证明的前提

- R-FL5(置换规则)在证明的任何步骤上，一阶公式中的任何子公式都可用与之等值的公式置换，得到证明的公式序列的另一公式。

使用一阶逻辑公式进行推理还有其他一些推理规则，这些规则建立在下面一些推理定律上，推理定律是一阶逻辑的一些永真蕴涵式，重要的推理定律如下：

- T-FL1(附加律)：$A \Rightarrow (A \vee B)$
- T-FL2(化简律)：$(A \wedge B) \Rightarrow A, (A \wedge B) \Rightarrow B$
- T-FL3(假言推理)：$A \to B \wedge A \Rightarrow B$
- T-FL4(拒取式)：$A \to B \wedge \neg B \Rightarrow \neg A$
- T-FL5(析取三段论)：$(A \vee B) \wedge \neg B \Rightarrow A$
- T-FL6(假言三段论)：$(A \to B) \wedge (B \to C) \Rightarrow (A \to C)$
- T-FL7(等价三段论)：$(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$
- T-FL8(构造性二难)：$(A \to B) \wedge (C \to D) \wedge (A \vee C) \Rightarrow (B \vee D)$

定理 1.19 $(A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge A) \Rightarrow B$当且仅当$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow A \to B$

定理 1.20 $(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow B$当且仅当$\neg(A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B)$是永真式，或者说$(A_1 \wedge A_2 \wedge \cdots \wedge A_k) \Rightarrow B$当且仅当$\neg(A_1 \wedge A_2 \wedge \cdots \wedge A_k \wedge \neg B)$是矛盾式。

在一阶逻辑中，可使用上述推理定律的替换示例来进行推理，此外，一阶逻辑中还有如下特有的推理定律：

- T-FL9：$(\forall x A(x)) \vee (\forall x B(x)) \Rightarrow \forall x(A(x) \vee B(x))$
- T-FL10：$\exists x(A(x) \vee B(x)) \Rightarrow (\exists x A(x)) \vee (\exists x B(x))$
- T-FL11：$(\forall x(A(x) \to B(x)) \Rightarrow (\forall x A(x)) \to (\forall x B(x))$
- T-FL12：$\forall x(A(x) \to B(x)) \Rightarrow (\exists x A(x)) \to (\exists x B(x))$
- T-FL8(构造性二难)：$(A \to B) \wedge (C \to D) \wedge (A \vee C) \Rightarrow (B \vee D)$

R-UI(全称量词消除规则)：

- (i) $\forall x A(x) \Rightarrow A(y)$
- (ii) $\forall x A(x) \Rightarrow A(c)$

成立的条件如下：

- (1) x是$A(x)$的自由变元；
- (2) 在(i)中，y为不在$A(x)$中约束出现的变元，y可以在$A(x)$中自由出现，也可在证明序列中前面的公式中出现；

- (3)在(ii)中，c为任意的个体常项，可以是证明序列中前面公式所指定的个体常项。

R-UG(全称量词引入规则)：

$$A(y) \Rightarrow \forall x A(x)$$

成立的条件如下：

- (1) y是$A(y)$中自由出现；
- (2) 替换y的x要选择在$A(y)$中不出现的变元符号。

R-EG(存在量词引入规则)：

$$A(c) \Rightarrow \exists x A(x)$$

成立的条件如下：

- (1) c是$A(c)$中是特定的个体常项；
- (2) 替换c的x要选择在$A(c)$中不出现的变元符号。

R-EI(存在量词消除规则)：

$$\exists x A(x) \Rightarrow A(c)$$

成立的条件如下：

- (1) c是特定的个体常项，c不能在前面的公式序列中出现
- (2) c不在$A(x)$中出现
- (3) $A(x)$中自由出现的个体变元只有x