离 散 数 学

--数理逻辑

第三章：推理与证明技术

2025年11月6日 星期四

3.1 本章内容

1 命题逻辑的推理理论

2 谓词逻辑的推理理论

3 数学归纳法的使用

4 CP规则相关证明

3.2 命题逻辑的推理理论

概念

描述问题的句子

判断

对概念的肯定与否定的判断

推理

从一个或多个前提推出结论的思维过程

认识世界的渐进过程

推理的有效性和结论的真实性

有效的推理不一定产生真实的结论；而产生真实结论的推理过程未必是有效的。有效的推理中可能包含为“假”的前提，而无效的推理却可能得到为“真”的结论 。

所谓推理有效，指的是它的结论是它前提的合乎逻辑的结果。也即，如果它的前提都为真，那么所得的结论也必然为真，而并不是要求前提或结论一定为真或为假，如果推理是有效的话，那么不可能它的前提都为真时，而它的结论为假。

3.2.1　推理的基本概念和推理形式

定义3.2.0 设G,H是公式，对任意解释I，如果I满足G，那么I满足H，则称H是G的逻辑结果(或称G蕴涵H)，记为$G \Rightarrow H$，此时称G为前提，H为结论。

判定定理

定理3.2.0 设G,H是公式，H是G的逻辑结果当且仅当G→H为永真公式。

证明： “⇒”若G⇒H，但G→H不是永真公式。于是，必存在一个解释I，使得G→H为假，即在解释I下，G为真，而H为假，这与G⇒H矛盾，故G→H是永真公式。

“⇐”若G→H是永真式，但G⇒H不成立，故存在G,H的一个解释I，使得G为真，而H为假，从而在解释I下，G→H为假，这与G→H是永真公式矛盾，所以G⇒H。

推广

定义3.2.1 设$G_1, G_2, \cdots, G_n$, H是公式，称H是$G_1, G_2, \cdots, G_n$的逻辑结果($G_1, G_2, \cdots, G_n$共同蕴涵H)，当且仅当H是$G_1 \wedge G_2 \wedge \cdots \wedge G_n$的逻辑结果(logic conclusion)。记为$G_1, G_2, \cdots, G_n \Rightarrow H$，此时称$G_1, G_2, \cdots, G_n \Rightarrow H$为有效的(efficacious)，否则称为无效的(inefficacious)。$G_1, G_2, \cdots, G_n$称为一组前提(Premise)，有时用集合Γ来表示，记$\Gamma=\{G_1, G_2, \cdots, G_n\}$。H称为结论(conclusion)。又称H是前提集合Γ的逻辑结果。记为$\Gamma \Rightarrow H$。

判定定理

定理3.2.1 公式H是前提集合$\Gamma=\{G_1, G_2, \cdots, G_n\}$的逻辑结果当且仅当$G_1\wedge G_2\wedge\cdots\wedge G_n\rightarrow H$为永真公式。

证明： 略。

“⇒”与“→”的不同

1. “→”仅是一般的蕴涵联结词，G→H的结果仍是一个公式，而“⇒”却描述了两个公式G，H之间的一种逻辑蕴涵关系，G ⇒ H的“结果”，是非命题公式；

2. 用计算机来判断G ⇒ H是办不到的。然而计算机却可“计算”公式G→H是否为永真公式。

3.2.2 判断有效结论的常用方法

要求

$\Gamma = \{G_1, G_2, \ldots, G_n\}$

$\Gamma \Rightarrow H$

也就是

$G_1 \wedge G_2 \wedge \ldots \wedge G_n \rightarrow H$

为永真公式

因而

真值表技术、演绎法和间接证明方法

1、真值表技术

设$P_1, P_2, \cdots, P_n$是出现在前提$G_1, G_2, \cdots, G_n$和结论H中的一切命题变元，如果将$P_1, P_2, \cdots, P_n$中所有可能的解释及$G_1, G_2, \cdots, G_n$, H的对应真值结果都列在一个表中，根据“→”的定义，则有判断方法如下：

1. 对所有$G_1, G_2, \cdots, G_n$都具有真值T的行(表示前提为真的行),如果在每一个这样的行中，H也具有真值T，则H是$G_1, G_2, \cdots, G_n$的逻辑结果。
2. 对所有H具有真值为F的行(表示结论为假的行),如果在每一个这样的行中，$G_1, G_2, \cdots, G_n$中至少有一个公式的真值为F(前提也为假),则H是$G_1, G_2, \cdots, G_n$的逻辑结果。

例3.2.1

判断下列H是否是前提G_1, G_2的逻辑结果

(1)　H：Q；　　G_1：P；G_2：P→Q；　是

(2)　H：┐P；　　G_1：P→Q；G_2：┐Q；　是

(3)　H：Q；　　G_1：┐P；G_2：P→Q。　否

解

(1)

P	Q	G_1	G_2	H
0	0	0	1	0
0	1	0	1	1
1	0	1	0	0
1	1	1	1	1

(2)

P	Q	G_1	G_2	H
0	0	1	1	1
0	1	1	0	1
1	0	0	1	0
1	1	1	0	0

(3)

P	Q	G_1	G_2	H
0	0	1	1	0
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

2 推理定律

设G，H，I，J是任意的命题公式，则有：

1）I_1：$G \wedge H \Rightarrow G$ （简化规则）

I_2：$G \wedge H \Rightarrow H$

2）I_3：$G \Rightarrow G \vee H$ （添加规则）

I_4：$H \Rightarrow G \vee H$

3）I_5：$\neg G \Rightarrow G \rightarrow H$

I_6：$H \Rightarrow G \rightarrow H$

4）I_7：$\neg (G \rightarrow H) \Rightarrow G$

I_8：$\neg (G \rightarrow H) \Rightarrow \neg H$

5）I_9：$G, H \Rightarrow G \wedge H$

2　推理定律(续)

6) I_{10}: $\neg G,\ G \vee H \Rightarrow H$ （选言三段论）

I_{11}: $\neg G,\ G\,\overline{\vee}\,H \Rightarrow H$

7) I_{12}: $G,\ G \to H \Rightarrow H$ （分离规则）

8) I_{13}: $\neg H,\ G \to H \Rightarrow \neg G$ （否定后件式）

9) I_{14}: $G \to H,\ H \to I \Rightarrow G \to I$ （假言三段论）

10) I_{15}: $G \vee H,\ G \to I,\ H \to I \Rightarrow I$ （二难推论）

例子

1)、前提：

1. 如果明天天晴，我们准备外出旅游。 $P \rightarrow Q$

2. 明天的确天晴。 P

结论：我们外出旅游。 Q

可描述为：$P \rightarrow Q$，$P \Rightarrow Q$ （分离规则）

2)、前提：

1. 如果一个人是单身汉，则他不幸福。 $P \rightarrow Q$

2. 如果一个人不幸福，则他死得早。 $Q \rightarrow R$

结论：单身汉死得早。 $P \rightarrow R$

可描述为：$P \rightarrow Q$，$Q \rightarrow R \Rightarrow P \rightarrow R$ （假言三段论）

例子(续1)

3)、某女子在某日晚归家途中被杀害，据多方调查确证，凶手必为王某或陈某，但后又查证，作案之晚王某在工厂值夜班，没有外出，根据上述案情可得前提：

1. 凶手为王某或陈某 $P \vee Q$
2. 如果王某是凶手，则他在作案当晚必外出 $P \rightarrow R$
3. 王某案发之晚并未外出。 $\neg R$

结论：陈某是凶手。 Q

则可描述为：$P \rightarrow R, \neg R \Rightarrow \neg P$ （否定后件式）

$P \vee Q, \neg P \Rightarrow Q$ （选言三段论）

例子(续2)

4)、前提：

1. 如果某同学为省二级以上运动员，则他将被大学录取。 $P \rightarrow R$
2. 如果某同学高考总分在560分以上，则将被大学录取。 $Q \rightarrow R$
3. 某同学高考总分在560分以上或者是省二级运动员。 $P \vee Q$

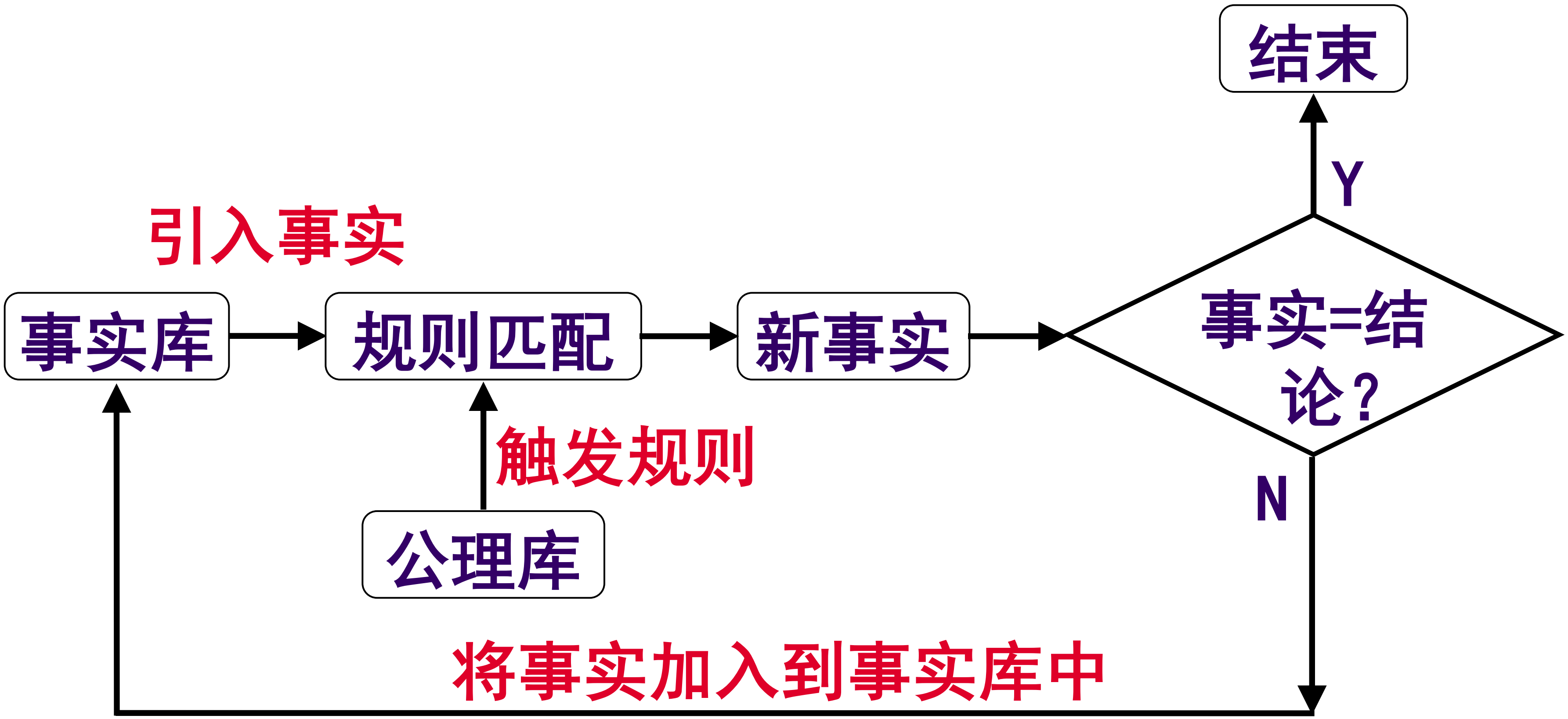
结论：该同学被大学录取。 R

则上述例子可描述为：

$P \vee Q$，$P \rightarrow R$，$Q \rightarrow R \Rightarrow R$ （二难推论）

3　演绎法

演绎法是从前提(假设)出发，依据公认的推理规则和推理定律，推导出一个结论来。



演绎的定义

定义3.2.2

从前提集合Γ推出结论H的一个演绎是构造命题公式的一个有限序列：

$$H_1, H_2, \cdots\cdots, H_n$$

其中，H_i或者是Γ中的某个前提，或者是前面的某些H_j（$j<i$）的有效结论，并且H_n就是H，则称公式H为该演绎的有效结论，或者称从前提Γ能够演绎出结论H来。

推理规则

① 规则P（称为前提引用规则）：在推导的过程中，可随时引入前提集合中的任意一个前提；

② 规则T（逻辑结果引用规则）：在推导的过程中，可以随时引入公式S，该公式S是由其前的一个或多个公式推导出来的逻辑结果。

③ 规则CP（附加前提规则）：如果能从给定的前提集合Γ与公式P推导出S，则能从此前提集合Γ推导出P→S。

$(\Gamma \wedge P) \Rightarrow S$ 等价于 $\Gamma \Rightarrow (P \rightarrow S)$，

$(Q \wedge P) \rightarrow S = Q \rightarrow (P \rightarrow S)$

例3.2.2

设前提Γ={$P\vee Q$，$P\leftrightarrow R$，$Q\rightarrow S$}，$G=S\vee R$。证明Γ$\Rightarrow$G。

证明1：

(1)	$P\vee Q$	P
(2)	$\neg P\rightarrow Q$	T, (1), E
(3)	$Q\rightarrow S$	P
(4)	$\neg P\rightarrow S$	T, (2), (3), I
(5)	$\neg S\rightarrow P$	T, (4), E
(6)	$P\leftrightarrow R$	P
(7)	$(P\rightarrow R)\wedge(R\rightarrow P)$	T, (6), E
(8)	$P\rightarrow R$	T, (7), I
(9)	$\neg S\rightarrow R$	T, (5), (8), I
(10)	$S\vee R$	T, (9), E

例3.31(续)

证明2:

(1)	$\neg S$	P(附加)
(2)	$Q\rightarrow S$	P
(3)	$\neg Q$	T, (1), (2), I
(4)	$P\vee Q$	P
(5)	P	T, (3), (4), I
(6)	$P\leftrightarrow R$	P
(7)	$(P\rightarrow R)\wedge(R\rightarrow P)$	T, (6), E
(8)	$P\rightarrow R$	T, (7), I
(9)	R	T, (5), (8), I
(10)	$\neg S\rightarrow R$	CP, (1), (9)
(11)	$S\vee R$	T, (10), E

例3.2.3

设$\Gamma=\{P\to(Q\to S), \neg R\vee P, Q\}$，$G=R\to S$。

证明：$\Gamma\Rightarrow G$。

证：

(1)	R	P(附加)
(2)	$\neg R\vee P$	P
(3)	P	T,(1),(2), I
(4)	$P\to(Q\to S)$	P
(5)	$Q\to S$	T,(3),(4), I
(6)	Q	P
(7)	S	T,(5),(6), I
(8)	$R\to S$	CP,(1),(7)

4　间接证明法（反证法）

前面使用过的一些证明方法都是正向推理。但在数学领域中，经常会遇到一些问题，当采用正向推理时很难从前提为真推出结论为真。

P⇒Q等价于¬Q⇒¬P，因此，为了间接地证明P⇒Q，可以假设Q为假(¬Q)，然后证明P为假(¬P)。

例3.2.4

设n是一个整数，证明：如果n^2是奇数，那么n是奇数。

证明 设n是偶数，则$n=2k$，这里k是一个整数。于是有：

$$n^2=(2k)^2=4k^2=2(2k^2)$$

所以n^2是偶数。

因而证明了若n是偶数，则n^2是偶数，它是已知命题的逆否式。因此，证明了所给的命题。

定义3.2.3

假设$G_1, G_2, \cdots, G_n$是一组命题公式，$P_1, P_2, \cdots, P_n$是出现在其中的一切命题变元，若有解释I使$G_1 \wedge G_2 \wedge \cdots \wedge G_n$取值为“真”，则称公式$G_1, G_2, \cdots, G_n$

$G_1 \wedge G_2 \wedge \cdots \wedge G_n$是矛盾式当且仅当

$$G_1 \wedge G_2 \wedge \cdots \wedge G_n \Rightarrow R \wedge \neg R,$$

其中，R可为任意公式，$R \wedge \neg R$为一矛盾式。

间接证明方法

将结论的否定加入到前提集合中构成一组新的前提，然后证明这组新的前提集合是不相容的，即蕴涵一个矛盾式。

$$G_1, G_2, \cdots, G_n, \neg H \Rightarrow R \wedge \neg R$$

定理3.2.2 设命题公式集合$\{G_1, G_2, \cdots, G_n\}$是一致的，于是从前提集合$\{G_1, G_2, \cdots, G_n\}$出发可以逻辑地推出公式H的充要条件是从前提集合$\{G_1, G_2, \cdots, G_n, \neg H\}$出发，可以逻辑地推出一个矛盾（永假）式来。

例3.2.5

证明不存在有理数P/q其平方为2，即证明$\sqrt{2}$是无理数。

证明　对某两个整数P和q，假设$(P/q)^2=2$成立，并且P和q没有公因子。如果原来选择的P、q具有公因子，则可以用与它相等的无公因子的P、q来取代它。

于是$P^2=2q^2$，所以P^2是偶数，这就推出P是偶数，因为一个奇数的平方是奇数。

因此存在某个整数n使得$P＝2n$成立。

例3.2.5(续)

因此

$$2q^2 = P^2 = (2n)^2 = 4n^2,$$

即有$q^2=2n^2$，所以q^2是偶数，从而q是偶数，于是得到P和q都是偶数，故它们有一个公因子2，这与假设相矛盾。

因此结论成立。

例3.2.6

用反证法证明二难推论

$$P \vee Q,\quad P \rightarrow R,\quad Q \rightarrow R \Rightarrow R$$

证明：

(1)	$P \rightarrow R$	P
(2)	$\neg R$	P(附加)
(3)	$\neg P$	T, (1), (2), I
(4)	$Q \rightarrow R$	P
(5)	$\neg Q$	T, (2), (4), I
(6)	$P \vee Q$	P
(7)	P	T, (5), (6), I
(8)	$P \wedge \neg P$	T, (3), (7), I

三种证明方法之间的关系

$G_1, G_2, \cdots, G_n, \neg H \Rightarrow R \wedge \neg R$ 反证法

$\overset{CP}{\Leftrightarrow}$ $G_1, G_2, \cdots, G_n \Rightarrow \neg H \to (R \wedge \neg R)$ CP规则证明法

$\Leftrightarrow$ $G_1, G_2, \cdots, G_n \Rightarrow \neg\neg H \vee (R \wedge \neg R)$

$\Leftrightarrow$ $G_1, G_2, \cdots, G_n \Rightarrow H$ 直接证明法

3.2.3 命题逻辑推理的难点

1. 弄清楚几种推理方法的区别与联系，对于命题逻辑推理而言，任何一个问题的推理，都可以采取三种推理方法中的任何一种来证明，针对不同的问题选用不同的推理方法。

2. 一般而言，对于结论是蕴涵式或析取式的，大多可以采取带CP规则的直接证明方法。

3.2.4　命题逻辑推理的应用

例3.2.7 符号化下面的语句，并用演绎法证明结论是否有效。

　　或者明天下午是天晴，或者是下雨；如果明天下午是天晴，则我将去看电影；如果我去看电影，我就不看书。结论：如果我看书，则天在下雨。

设 P：明天下午天晴；　　Q：明天下午下雨；

R：明天下午去看电影；S：明天下午看书。

则上述命题可符号化为：

$$P \overline{\vee} Q,\ P \rightarrow R,\ R \rightarrow \neg S \Rightarrow S \rightarrow Q。$$

证明

$P \overline{\vee} Q$， $P \rightarrow R$， $R \rightarrow \neg S \Rightarrow S \rightarrow Q$。

（1） S	P（附加）
（2） $R \rightarrow \neg S$	P
（3） $\neg R$	T，(1)，(2)，I
（4） $P \rightarrow R$	P
（5） $\neg P$	T，(3)，(4)，I
（6） $P \overline{\vee} Q$	P
（7） Q	T，(4)，(7)，I

例3.2.8

如果马会飞或羊吃草，则母鸡就会是飞鸟；如果母鸡是飞鸟，那么烤熟的鸭子还会跑；烤熟的鸭子不会跑。结论：所以羊不吃草。

分析：令P：马会飞；　　Q：羊吃草；

R：母鸡是飞鸟；

S：烤熟的鸭子还会跑。

符号化上述语句为：

$\Gamma=\{P\vee Q\rightarrow R,\ R\rightarrow S,\ \neg S\}$，　$G=\neg Q$

证明$\Gamma\Rightarrow G$。

例3.2.8 证明

$P \vee Q \rightarrow R,\ R \rightarrow S,\ \neg S \Rightarrow \neg Q$

(1)	$\neg S$	P
(2)	$R \rightarrow S$	P
(3)	$\neg R$	T, (1), (2), I
(4)	$P \vee Q \rightarrow R$	P
(5)	$\neg (P \vee Q)$	T, (3), (4), I
(6)	$\neg P \wedge \neg Q$	T, (5), E
(7)	$\neg Q$	T, (6), I

例3.2.9

一个公安人员审查一件盗窃案，已知的事实如下：

A或B盗窃了x；若A盗窃了x，则作案时间不能发生在午夜前；若B证词正确，则在午夜时屋里灯光未灭；若B证词不正确，则作案时间发生在午夜前；午夜时屋里灯光灭了。结论：B盗窃了x。

设 P：A盗窃了x；　　Q：B盗窃了x；

R：作案时间发生在午夜前；　S：B证词正确；

T：在午夜时屋里灯光未灭。　则上述命题可符号化为：

$$P\vee Q,\ P\rightarrow\neg R,\ S\rightarrow T,\ \neg S\rightarrow R,\ \neg T \Rightarrow Q$$

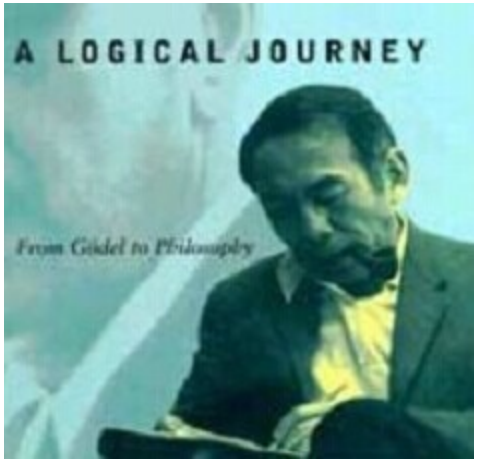
例3.2.9（续）

证明　采用**直接证明**方法

$P \vee Q,\ P \rightarrow \neg R,\ S \rightarrow T,\ \neg S \rightarrow R,\ \neg T \Rightarrow Q$

(1)	$\neg T$	P
(2)	$S \rightarrow T$	P
(3)	$\neg S$	T, (1), (2), I
(4)	$\neg S \rightarrow R$	P
(5)	R	T, (3), (4), I
(6)	$P \rightarrow \neg R$	P
(7)	$\neg P$	T, (5), (6), I
(8)	$P \vee Q$	P
(9)	Q	T, (7), (8), I

数理逻辑学家王浩与Stephen Cook



王浩（近代数理逻辑学家）

播报 编辑 讨论 上传视频

王浩（1921年5月20日—1995年5月13日）数理逻辑学家。祖籍山东省德州市齐河县，生于山东省济南市。1939年毕业于现山东省济南第一中学，进入西南联大数学系学习，师从金岳霖先生。1943年获学士学位后又入清华大学研究生院哲学部学习，1945年以《论经验知识的基础》的论文获硕士学位。王浩在中学时代就对哲学有兴趣，念初中时他在父亲的建议下阅读过恩格斯的著作《反杜林论》和《路德维希·费尔巴哈与德国古典哲学的终结》。1946年，王浩前往美国哈佛大学，在那里见到了当代美国著名哲学家、逻辑学家奎因（W.V.Quine），并随即开始学习他创立的形式公理系统。两年时间即获哈佛大学哲学博士学位。在哈佛短暂教学之后赴苏黎世与贝奈斯（Paul Bernays）一起工作。1954-1956年，在牛津大学任第二届约翰-洛克讲座主讲，又任逻辑及数理哲学高级教职，主持数学基础讨论班。1961-1967年，任哈佛大学教授。1967-1991年，任洛克菲勒大学逻辑学教授。20世纪50年代初被选为美国科学院院士，后又被选为不列颠科学院外国院士。1983年，被国际人工智能联合会授予第一届"数学定理机械证明里程碑奖"，以表彰他在数学定理机械证明研究领域中所作的开创性贡献。著有《数理逻辑概论》、《从数学到哲学》、《哥德尔》、《超越分析哲学》等专著。

库克本科就读于密歇根大学，一开始学的是工程，但后来数学教授鼓励他改学了数学。他本科毕业后在哈佛大学读研究生，想学代数。但那时已经在哈佛读研究生的科巴姆影响了他。库克和王浩很聊得来，就选定王浩做博士导师，并于1966年获得博士学位。

库克在1971年证明了命题逻辑的可满足问题(Satisfiability，SAT)是NP完全的，这是第一个NP完全问题。这个证明现在有标准的教科书式呈现方式，基本思路是：首先证明SAT属于NP类，这很简单，只要能够说明任何SAT问题是多项式可验证就可以了。另一方面比较难：要证明所有的NP问题都可以归约到SAT。库克的办法是用命题逻辑来描述非确定图灵机多项式时间运行的所有可能状态。也恰是因为库克用了命题逻辑，于是他的论文题目和定理证明相关。

3.3 谓词逻辑的推理理论

3.3.1 谓词演算的演绎与推理

定义3.3.1 设G_1, G_2, …, G_n, H是公式，称H是G_1, G_2, …, G_n的逻辑结果($G_1, G_2, \cdots, G_n$共同蕴涵H)，当且仅当H 是$G_1 \wedge G_2 \wedge \cdots \wedge G_n$的逻辑结果(logic conclusion)。记为$G_1, G_2, \cdots, G_n \Rightarrow H$，此时称$G_1, G_2, \cdots, G_n \Rightarrow H$为有效的(efficacious)，否则称为无效的（inefficacious）。$G_1, G_2, \cdots, G_n$称为一组前提(Premise)，有时用集合Γ来表示，记$\Gamma = \{G_1, G_2, \cdots, G_n\}$。H称为结论(conclusion)。又称H是前提集合的逻辑结果。记为$\Gamma \Rightarrow H$。

定理3.3.1

公式H是前提集合 $\Gamma=\{G_1, G_2, \cdots, G_n\}$ 的逻辑结果当且仅当 $G_1 \wedge G_2 \wedge \cdots \wedge G_n \rightarrow H$ 为有效公式。

一、推理规律

（1） I_{16}: $(\forall x)G(x) \Rightarrow (\exists x)G(x)$；

（2） I_{17}: $(\forall x)G(x) \vee (\forall x)H(x)$

$\Rightarrow (\forall x)(G(x) \vee H(x))$；

右式弱于左式，反向不成立

E_{35}: $(\forall x)G(x) \vee (\forall x)H(x)$

$=(\forall x)(\forall y)(G(x) \vee H(y))$；

右式与左式等价，反向成立

一、推理规律

（1） I_{16}: $(\forall x)G(x) \Rightarrow (\exists x)G(x)$；

（2） I_{17}: $(\forall x)G(x) \vee (\forall x)H(x)$

$\Rightarrow (\forall x)(G(x) \vee H(x))$；

I_{18}: $(\exists x)(G(x) \wedge H(x))$

$\Rightarrow (\exists x)G(x) \wedge (\exists x)H(x)$；

E_{34}: $(\exists x)(G(x) \vee H(x))$

$= (\exists x)G(x) \vee (\exists x)H(x)$；

$(\exists x)(G(x) \vee H(x))$

$\Rightarrow (\exists x)G(x) \vee (\exists x)H(x)$；

一、推理规律

（1） I_{16}： $(\forall x)G(x) \Rightarrow (\exists x)G(x)$；

（2） I_{17}： $(\forall x)G(x) \vee (\forall x)H(x)$

$$\Rightarrow (\forall x)(G(x) \vee H(x))；$$

I_{18}： $(\exists x)(G(x) \wedge H(x))$

$$\Rightarrow (\exists x)G(x) \wedge (\exists x)H(x)；$$

（3） I_{19}： $(\forall x)(G(x) \rightarrow H(x))$

$$\Rightarrow (\forall x)G(x) \rightarrow (\forall x)H(x)；$$

I_{20}： $(\forall x)(G(x) \rightarrow H(x))$

$$\Rightarrow (\exists x)G(x) \rightarrow (\exists x)H(x)。$$

推理规律（续）

（4） I_{21}： $(\exists x)(\forall y)G(x, y) \Rightarrow (\forall y)(\exists x)G(x, y)$；

I_{22}： $(\forall x)(\forall y)G(x, y) \Rightarrow (\exists y)(\forall x)G(x, y)$；

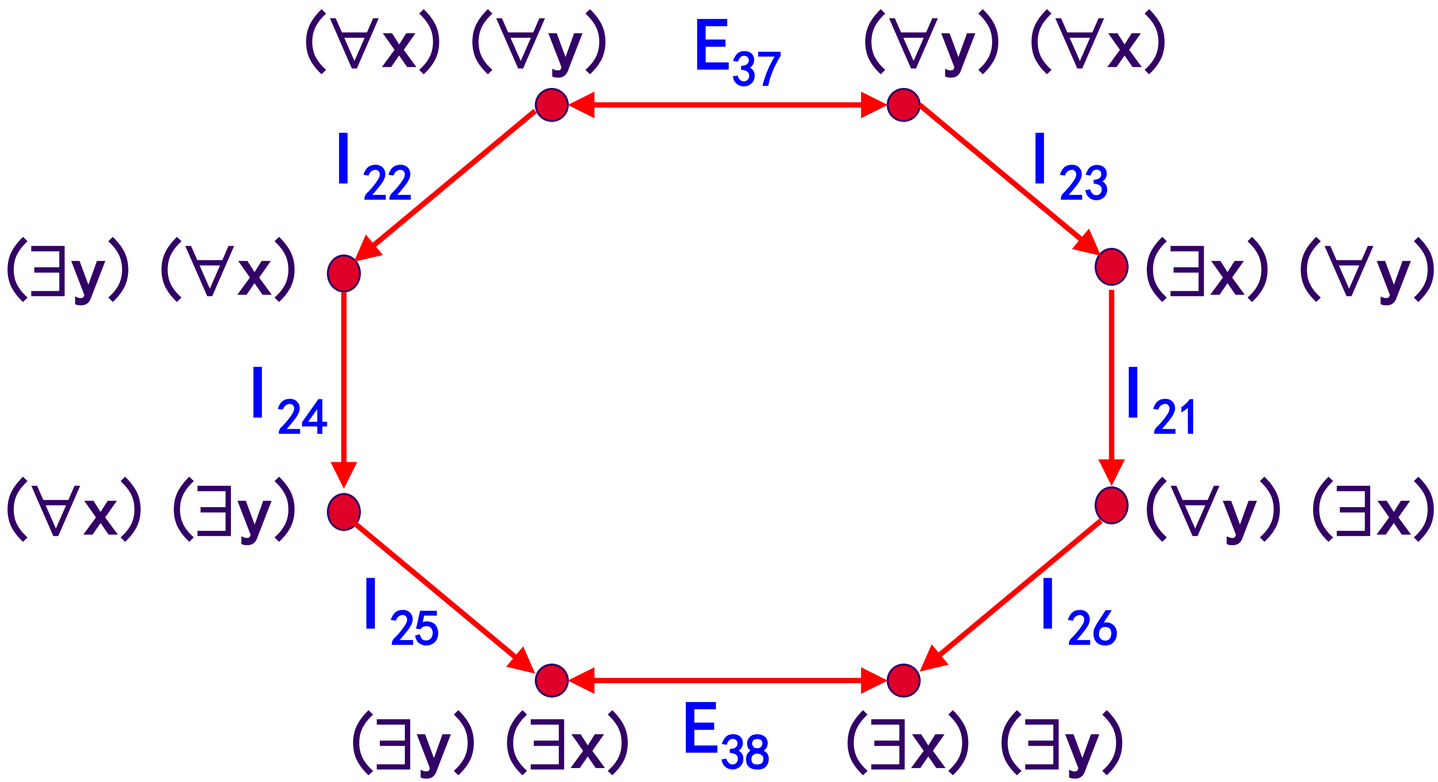
I_{23}： $(\forall y)(\forall x)G(x, y) \Rightarrow (\exists x)(\forall y)G(x, y)$；

I_{24}： $(\exists y)(\forall x)G(x, y) \Rightarrow (\forall x)(\exists y)G(x, y)$；

I_{25}： $(\forall x)(\exists y)G(x, y) \Rightarrow (\exists y)(\exists x)G(x, y)$；

I_{26}： $(\forall y)(\exists x)G(x, y) \Rightarrow (\exists x)(\exists y)G(x, y)$；

量词关系图



二、推理规则

1、US（全称特指规则，Universal SPecify）：

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

其中G(x)对y是自由的

推广：$(\forall x)G(x) \Rightarrow G(c)$

其中c为任 个体常量

2、ES（存在 则，Existential SPecify）：

在G(x)中，x不出现在量词

$(\forall y)$或$(\exists y)$

的辖域之内。

其 ；若G(x)中还有除x以外的自由变量时，则必须用这些变量的函数符号来取代。

推理规则（续）

3、UG（全称推广规则， Universal Generalize ）：

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

其中G(y)对x是自由的且G(y)中无自由变量x

4、EG（存在推广规则，Existential Generalize）：

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

其中G(c)对x是自由的且G(c)中无自由变量x

推广： $$G(y) \Rightarrow (\exists x)G(x)$$

其中G(y)对x是自由的且G(y)中无自由变量x

推理规则的正确使用(1)

例3.3.1 设实数集中，语句“不存在最大的实数”可符号化为：

$(\forall x)(\exists y)G(x, y)$。　　其中：$G(x, y)$：$y>x$。

推导1：

（1）$(\forall x)(\exists y)G(x, y)$　　P

注意：使用US规则来消去量词时，若选用变元y取代x，则要求在原公式中x不能出现在量词$(\forall y)$或$(\exists y)$的辖域之内。

（2）$(\exists y)G(z, y)$　　US,(1)

推理规则的正确使用（2）

推导2：

（1）$(\forall x)(\exists y)G(x, y)$　　P

（2）$(\exists y)G(z, y)$　　US,(1)

（3）$G(z, c)$　　ES,(2)

注意：使用ES规则来消去量词时， 若还有其它自由变元时，则必须用关于自由变元的函数符号来取代常量符号.

推理规则的正确使用（3）

推导3：

（1）$(\exists y)G(z, y)$　　P

（2）$(\forall y)(\exists y)G(y, y)$　　UG,(1)

分析：推导3是错误的。正确的推导如下：

注意：使用UG规则来添加量词时，若选用变元x取代y，则要求在原公式中y不能出现在量词$(\forall x)$或$(\exists x)$的辖域之内。

推理规则的正确使用（4）

推导4：

（1）G(x, c)　　　　　　P

（2）(∃x)G(x, x)　　　　EG,(2)

分析：推导4是错误的。正确的推导如下：

注意：使用EG规则来添加量词时，若选用变元x取代c，则要求在原公式中c不能出现在量词(∀x)或(∃x)的辖域之内且原公式中中无自由变量x。

判断

（1）	$(\forall x)(\exists y)G(x, y)$	P	
（2）	$(\exists y)G(z, y)$	US,(1)	对
（3）	$G(z, c)$	ES,(2)	错
（4）	$(\forall x)G(x, c)$	UG,(3)	对
（5）	$(\exists y) (\forall x)G(x, y)$	EG,(4)	对

3.3.2　谓词演算的综合推理方法

1. 推导过程中可以引用命题演算中的规则P 和规则T 。
2. 如果结论是以蕴涵形式(或析取形式)给出，我们还可以使用规则CP。
3. 若需消去量词，可以引用规则US和规则ES。
4. 当所要求的结论可能被定量时，此时可引用规则UG和规则EG将其量词加入。

谓词演算的综合推理方法（续1）

5. 证明时可采用如命题演算中的直接证明方法和间接证明方法。

6. 在推导过程中，对消去量词的公式或公式中不含量词的子公式，完全可以引用命题演算中的基本等价公式和基本蕴涵公式。

7. 在推导过程中，对含有量词的公式可以引用谓词中的基本等价公式和基本蕴涵公式。

例3.3.1

证明苏格拉底三段论："所有的人都是要死的；苏格拉底是人。所以苏格拉底是要死的。"

解：设H(x)：x是人；M(x)：x是要死的；

s：苏格拉底。 则符号化为

(4)错了！

$(\forall x)(H(x)\rightarrow M(x))$，$H(s)$

证明：	(1)	$(\forall x)(H(x)\rightarrow M(x))$	P
	(2)	$H(s)\rightarrow M(s)$	US,(1)
	(3)	$H(s)$	P
	(4)	$M(s)$	T,(2),(3),I

例3.3.2

证明 $(\forall x)(P(x)\rightarrow Q(x))$，$(\exists x)P(x)\Rightarrow(\exists x)Q(x)$

有下面的推导：

(5)错了！

(1)	$(\forall x)(P(x)\rightarrow Q($	
(2)	$P(x)\rightarrow Q(x)$	US, (1)
(3)	$(\exists x)P(x)$	P
(4)	$P(c)$	ES, (3)
(5)	$Q(c)$	T, (2), (4), I
(6)	$(\exists x)Q(x)$	EG, (5)

例3.3.2（２）

推导可修改为：

(1)	$(\forall x)(P(x)\rightarrow Q(x))$	P
(2)	$P(c)\rightarrow Q(c)$	US, (1)
(3)	$(\exists x)P(x)$	P
(4)	$P(c)$	ES, (3)
(5)	$Q(c)$	T, (2), (4), I
(6)	$(\exists x)Q(x)$	EG, (5)

例3.3.2(3)

请看推导：

正确！

(1)	$(\exists x)P(x)$	P
(2)	$P(c)$	ES, (1)
(3)	$(\forall x)(P(x)\rightarrow Q(x))$	P
(4)	$P(c)\rightarrow Q(c)$	US, (3)
(5)	$Q(c)$	T, (2), (4), I
(6)	$(\exists x)Q(x)$	EG, (5)

例3.3.3

证明 $(\exists x)(P(x)\wedge Q(x)) \Rightarrow (\exists x)P(x)\wedge(\exists x)Q(x)$

证明：

1)	$(\exists x)(P(x)\wedge Q(x))$	P
2)	$P(c)\wedge Q(c)$	ES, 1)
3)	$P(c)$	T, 2), I
4)	$Q(c)$	T, 2), I
5)	$(\exists x)P(x)$	EG, 3)
6)	$(\exists x)Q(x)$	EG, 4)
7)	$(\exists x)P(x)\wedge(\exists x)Q(x)$	T, 5), 6), I

例3.3.3(续1)

请看上述推论的逆推导：

(5)错了！

1)	$(\exists x)P(x)\wedge(\exists x)Q(x$	
2)	$(\exists x)P(x)$	T, 1), I
3)	$P(c)$	ES, 2)
4)	$(\exists x)Q(x)$	T, 1), I
5)	$Q(c)$	ES, 4)
6)	$P(c)\wedge Q(c)$	T, 3), 4), I
7)	$(\exists x)(P(x)\wedge Q(x))$	EG, 6)

证明 $(\exists x)P(x) \wedge (\exists x)Q(x) \Rightarrow (\exists x)(P(x) \wedge Q(x))$

例3.3.3(续2)

正确地推导：

1)	$(\exists x)P(x) \wedge (\exists x)Q(x)$	P
2)	$(\exists x)P(x)$	T, 1), I
3)	$P(c)$	ES, 2)
4)	$(\exists x)Q(x)$	T, 1), I
5)	$Q(b)$	ES, 4)
6)	$P(c) \wedge Q(b)$	T, 3), 4), I
7)	$(\exists y)(P(c) \wedge Q(y))$	EG, 6)
8)	$(\exists x)(\exists y)(P(x) \wedge Q(y))$	EG, 7)

例3.3.4

证明$(\forall x)(P(x)\vee Q(x)) \Rightarrow (\forall x)P(x)\vee(\exists x)Q(x)$

证明(采用反证法)：

1)	$\neg((\forall x)P(x)\vee(\exists x)Q(x))$	P(附加)
2)	$\neg(\forall x)P(x)\wedge\neg(\exists x)Q(x)$	T, 1), E
3)	$\neg(\forall x)P(x)$	T, 2), I
4)	$\neg(\exists x)Q(x)$	T, 2), I
5)	$(\exists x)\neg P(x)$	T, 3), E
6)	$\neg P(c)$	ES, 5)

例3.3.4

7)	$(\forall x)\neg Q(x)$	T, 4), E
8)	$\neg Q(c)$	US, 7)
9)	$\neg P(c)\wedge\neg Q(c)$	T, 6), 8), I
10)	$\neg(P(c)\vee Q(c))$	T, 9), E
11)	$(\forall x)(P(x)\vee Q(x))$	P
12)	$(P(c)\vee Q(c))$	US, 11)
13)	$\neg(P(c)\vee Q(c))\wedge(P(c)\vee Q(c))$	T, 10), 12)

3.3.3 谓词逻辑推理的难点

1. 在推导过程中，如既要使用规则US又要使用规则ES消去公式中的量词，而且选用的个体是同一个符号，则必须先先使用规则ES，再使用规则US。然后再使用命题演算中的推理规则，最后使用规则UG或规则EG引入量词，得到所要的结论。
2. 如一个变量是用规则ES消去量词，对该变量在添加量词时，则只能使用规则EG，而不能使用规则UG；如使用规则US消去量词，对该变量在添加量词时，则可使用规则EG和规则UG。

谓词逻辑推理的难点（续）

3. 如有两个含有存在量词的公式，当用规则ES消去量词时，不能选用同样的一个常量符号来取代两个公式中的变元，而应用不同的常量符号来取代它们。
4. 在用规则US和规则ES消去量词、用规则UG和规则EG添加量词时，此量词必须位于整个公式的最前端，并且它的辖域为其后的整个公式。
5. 在添加量词(∀x)、(∃x)时，所选用的x不能在公式G(y)或G(c)中自由出现且G(y)或G(c)对x是自由的。

3.3.4 谓词逻辑推理的应用

例3.3.5 每个喜欢步行的人都不喜欢坐汽车；每个人或者喜欢坐汽车或者喜欢骑自行车；有的人不喜欢骑自行车。因而有的人不喜欢步行。

设：H(x)：x是人；　　　P(x)：x喜欢坐汽车；

Q(x)：x喜欢骑自行车；　R(x)：x喜欢步行。

则上述语句可符号化为：

$(\forall x)(H(x)\wedge R(x)\rightarrow\neg P(x))$,

$(\forall x)(H(x)\rightarrow P(x)\vee Q(x))$,

$(\exists x)(H(x)\wedge\neg Q(x)) \quad \Rightarrow \quad (\exists x)(H(x)\wedge\neg R(x))$

例3.3.5证明

(1) $(\exists x)(H(x)\wedge\neg Q(x))$ P

(2) $H(c)\wedge\neg Q(c)$ ES,(1)

(3) $H(c)$ T,(2),I

(4) $\neg Q(c)$ T,(2),I

(5) $(\forall x)(H(x)\rightarrow P(x)\vee Q(x))$ P

(6) $H(c)\rightarrow P(c)\vee Q(c)$ US,(5)

(7) $P(c)\vee Q(c)$ T,(3),(6),I

(8) $P(c)$ T,(4),(7),I

例3.3.5（续）

(9) $(\forall x)(H(x)\wedge R(x)\rightarrow\neg P(x))$	P
(10) $H(c)\wedge R(c)\rightarrow\neg P(c)$	US,(9)
(11) $\neg(H(c)\wedge R(c))$	T,(8),(10),I
(12) $\neg H(c)\vee\neg R(c)$	T,(11),E
(13) $\neg R(c)$	T,(3),(12),I
(14) $H(c)\wedge\neg R(c)$	T,(3),(13),I
(15) $(\exists x)(H(x)\wedge\neg R(x))$	EG,(14)

例3.3.5

每个喜欢步行的人都不喜欢坐汽车；每个人或者喜欢坐汽车或者喜欢骑自行车；有的人不喜欢骑自行车。因而有的人不喜欢步行。

设：个体域D＝{人}；　　P(x)：人x喜欢坐汽车；

Q(x)：人x喜欢骑自行车；

R(x)：人x喜欢步行。

则上述语句可符号化为：

$$(\forall x)(R(x)\rightarrow\neg P(x)),\quad (\forall x)(P(x)\vee Q(x)),$$

$$(\exists x)(\neg Q(x)) \Rightarrow (\exists x)(\neg R(x))$$

证明

(1)	$(\exists x)(\neg Q(x))$	P
(2)	$\neg Q(c)$	ES,(1)
(3)	$(\forall x)(P(x) \vee Q(x))$	P
(4)	$P(c) \vee Q(c)$	US,(3)
(5)	$P(c)$	T,(2),(4),I
(6)	$(\forall x)(R(x) \rightarrow \neg P(x))$	P
(7)	$R(c) \rightarrow \neg P(c)$	US,(6)
(8)	$\neg R(c)$	T,(5),(7),I
(9)	$(\exists x)\neg R(x)$	EG,(8)

例3.3.6 ：

证明下述论断的正确性：

所有的哺乳动物都是脊椎动物；并非所有的哺乳动物都是胎生动物；故有些脊椎动物不是胎生的。

解：设谓词如下：

P(x)：x是哺乳动物；

Q(x)：x是脊椎动物；

R(x)：x是胎生动物。

则有：

$$(\forall x)(P(x)\rightarrow Q(x)),\quad \neg(\forall x)(P(x)\rightarrow R(x))$$

$$\Rightarrow (\exists x)(Q(x)\wedge\neg R(x))$$

请看下面推导：

1)	$\neg(\forall x)(P(x)\to R(x))$	P
2)	$\neg(P(x)\to R(x))$	US,1)
3)	$\neg(\neg P(x)\vee R(x))$	T,2),E
4)	$(P(x)\wedge\neg R(x))$	T,3),E
5)	$P(x)$	T,4),I
6)	$\neg R(x)$	T,4),I
7)	$(\forall x)(P(x)\to Q(x))$	P
8)	$P(x)\to Q(x)$	US,7)
9)	$Q(x)$	T,(5),(8),I
10)	$Q(x)\wedge\neg R(x)$	T,6),9),I
11)	$(\exists x)(Q(x)\wedge\neg R(x))$	EG,10)
12)	$(\forall x)(Q(x)\wedge\neg R(x))$	UG,10)

证明：

1) $\neg(\forall x)(P(x)\rightarrow R(x))$ P
2) $(\exists x)\neg(\neg P(x)\vee R(x))$ T,1),E
3) $\neg(\neg P(c)\vee R(c))$ ES,2)
4) $(P(c)\wedge\neg R(c))$ T,3),E
5) $P(c)$ T,4),I
6) $\neg R(c)$ T,4),I
7) $(\forall x)(P(x)\rightarrow Q(x))$ P
8) $P(c)\rightarrow Q(c)$ US,7)
9) $Q(c)$ T,5),8),I
10) $Q(c)\wedge\neg R(c)$ T,6),9),I
11) $(\exists x)(Q(x)\wedge\neg R(x))$ EG,10)

例3.3.7

证明下列论断的正确性：

有些孩子相信所有的大人；任何一个孩子都不相信骗子；所以，大人都不是骗子。

解：设谓词如下：

S(x)：x是孩子　　T(x)：x是大人

P(x)：x是骗子　　L(x,y)：x相信y

则可符号化为：

$$(\exists x)(S(x)\land(\forall y)(T(y)\to L(x,y))),$$

$$(\forall x)(\forall y)((S(x)\land P(y))\to\neg L(x,y))$$

$$\Rightarrow\quad(\forall x)(T(x)\to\neg P(x))$$

证明:

1) $(\exists x)(S(x)\wedge(\forall y)(T(y)\rightarrow L(x,y)))$ P

2) $S(c)\wedge(\forall y)(T(y)\rightarrow L(c,y))$ ES,1)

3) $S(c)$ T,2),I

4) $(\forall y)(T(y)\rightarrow L(c,y))$ T,2),I

5) $T(x)\rightarrow L(c,x)$ US,4)

6) $(\forall x)(\forall y)((S(x)\wedge P(y))\rightarrow\neg L(x,y))$ P

7) $(\forall y)((S(c)\wedge P(y))\rightarrow\neg L(c,y))$ US,6)

8) $(S(c)\wedge P(x))\rightarrow\neg L(c,x)$ US,7)

证明：

9) $S(c)\rightarrow(P(x)\rightarrow\neg L(c,x))$ T,8),E

10) $P(x)\rightarrow\neg L(c,x)$ T,3),8),E

11) $L(c,x)\rightarrow\neg P(x)$ T,10),E

12) $T(x)\rightarrow\neg P(x)$ T,5),11),E

13) $(\forall x)(T(x)\rightarrow\neg P(x))$ UG,12)

例3.3.8

现有一智力测验题目(水容器问题)：设有两个分别能盛7升与5升的水容器，开始时两个容器均空，允许对容器做三种操作：

（1）容器倒满水，

（2）将容器中的水倒光，

（3）从一个容器倒水至另一容器，使一个容器倒光或另一容器倒满。

最后要求能使大容器(能盛7升的容器)中有4升水，并求其操作过程。

解决方案

（0）开始时两个容器均空
（1）容器倒满水，
（2）将容器中的水倒光，
（3）从一容器倒水至另一容器，使一个容器倒光或另一容器倒满。

令S(x, y)表示大容器装x升水，小容器装y升水

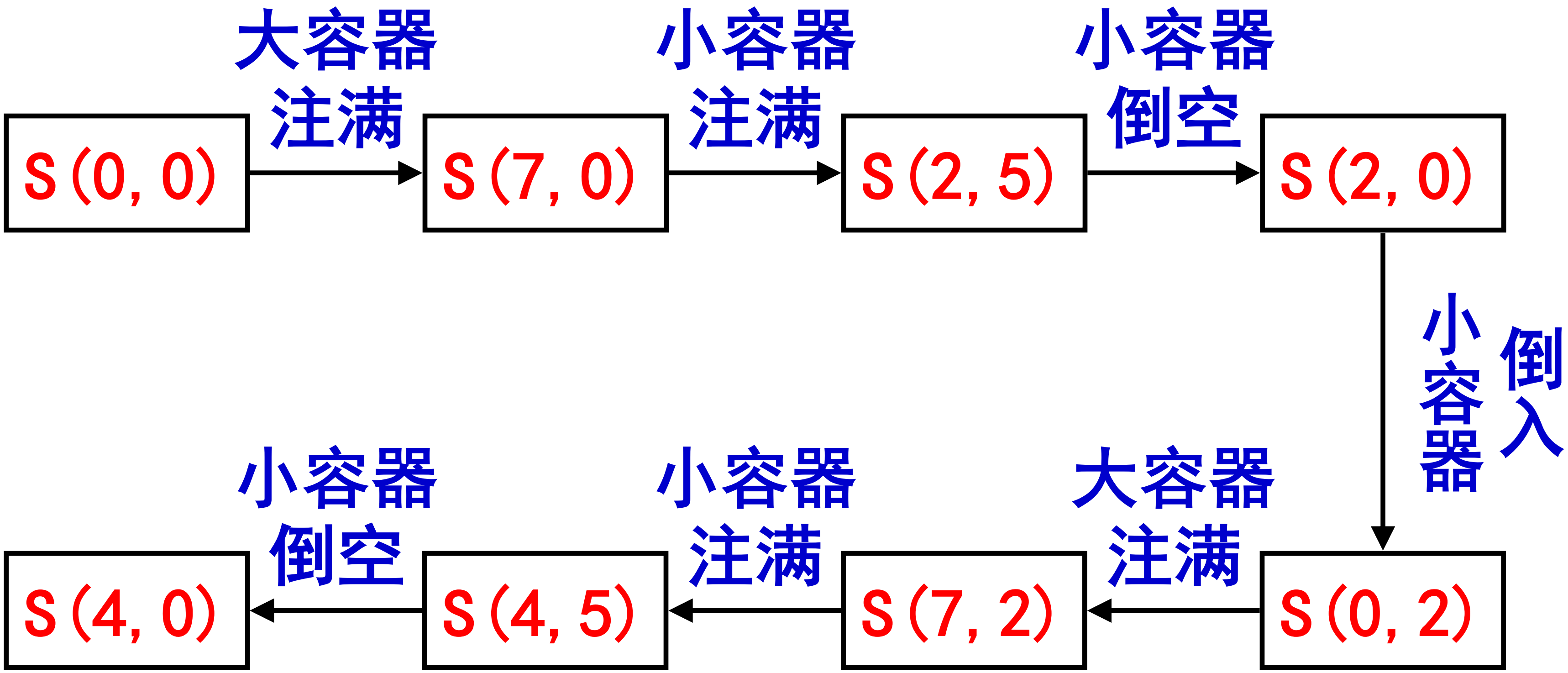
（0）S(0, 0)

（1）$(\forall x)(\forall y)(S(x, y)\rightarrow S(7, y))$或$(\forall x)(\forall y)(S(x, y)\rightarrow S(x, 5))$

（2）$(\forall x)(\forall y)(S(x, y)\rightarrow S(x, 0))$或$(\forall x)(\forall y)(S(x, y)\rightarrow S(0, y))$

（3）$(\forall x)(\forall y)(\exists z)(S(x, y)\rightarrow S(z, 5))$或
$(\forall x)(\forall y)(\exists z)(S(x, y)\rightarrow S(0, z))$或
$(\forall x)(\forall y)(\exists z)(S(x, y)\rightarrow S(7, z))$或
$(\forall x)(\forall y)(\exists z)(S(x, y)\rightarrow S(z, 0))$

解决方案



S(0,0)
大容器注满
S(7,0)
小容器注满
S(2,5)
小容器倒空
S(2,0)
小容器倒入
S(0,2)
大容器注满
S(7,2)
小容器注满
S(4,5)
小容器倒空
S(4,0)

证明

（1）$S(0, 0)$	P
（2）$(\forall x)(\forall y)(S(x, y)\rightarrow S(7, y))$	P
（3）$(\forall y)(S(0, y)\rightarrow S(7, y))$	US,(2)
（4）$S(0, 0)\rightarrow S(7, 0)$	US ,(3)
（5）$S(7, 0)$	T,(1),(4).I
（6）$(\forall x)(\forall y)(\exists z)(S(x, y)\rightarrow S(z, 5))$	P
（7）$(\forall y)(\exists z)(S(7, y)\rightarrow S(z, 5))$	US,(6)
（8）$(\exists z)(S(7, 0)\rightarrow S(z, 5))$	US,(7)
（9）$S(7, 0)\rightarrow S(2, 5)$	ES,(8)

证明

（10）	$S(2, 5)$	T,(5),(9),I
（11）	$(\forall x)(\forall y)(S(x, y) \rightarrow S(x, 0))$	P
（12）	$(\forall y)(S(2, y) \rightarrow S(2, 0))$	US,(11)
（13）	$S(2, 5) \rightarrow S(2, 0)$	US,(12)
（14）	$S(2, 0)$	T,(10),(13),I
（15）	$(\forall x)(\forall y)(\exists z)(S(x, y) \rightarrow S(0, z))$	P
（16）	$(\forall y)(\exists z)(S(2, y) \rightarrow S(0, z))$	US,(15)
（17）	$(\exists z)(S(2, 0) \rightarrow S(0, z))$	US,(16)

证明（续）

（18）	$(S(2, 0) \rightarrow S(0, 2))$	ES,(17)
（19）	$S(0, 2)$	T,(14),(18),I
（20）	$(\forall x)(\forall y)(S(x, y) \rightarrow S(7, y))$	P
（21）	$(\forall y)(S(0, y) \rightarrow S(7, y))$	US,(20)
（22）	$(S(0, 2) \rightarrow S(7, 2))$	US,(21)
（23）	$S(7, 2)$	T,(19),(22),I
（24）	$(\forall x)(\forall y)(\exists z)(S(x, y) \rightarrow S(z, 5))$	P
（25）	$(\forall y)(\exists z)(S(7, y) \rightarrow S(z, 5))$	US,(24)
（26）	$(\exists z)(S(7, 2) \rightarrow S(z, 5))$	US,(25)

证明（续）

（27）	$S(7, 2) \rightarrow S(4, 5)$	ES,(26)
（28）	$S(4, 5)$	T,(23),(27),I
（29）	$(\forall x)(\forall y)(S(x, y) \rightarrow S(x, 0))$	P
（30）	$(\forall y)(S(4, y) \rightarrow S(4, 0))$	US,(29)
（31）	$S(4, 5) \rightarrow S(4, 0)$	US,(30)
（32）	$S(4, 0)$	T,(30),(33),I

3.4 数学归纳法

3.4.1 数学归纳法原理

假设要证明的命题能写成形式:

$\forall n \geq n_0$，有$P(n)$

其中n_0是某个固定的整数,

即：希望证明对所有的整数$n \geq n_0$都有$P(n)$为真。

数学归纳法原理

假设

1）验证$n=n_0$，有$P(n_0)$为真；　　　　(归纳基础)

2）假设对于$n=k(k\geq n_0)$，有$P(k)$为真；(归纳假设)

3）证明$n=k+1$，有$P(k+1)$为真。　　　　(归纳结论)

结论 对所有的整数$n\geq n_0$，都有$P(n)$为真。

谓词表示：

$$(\exists n_0)(P(n_0)\wedge(\forall n)((n=k)\wedge P(k)\rightarrow P(k+1))=1$$

强形式数学归纳法原理

假设

1） 验证$n=n_0$、n_0+1，有$P(n_0)$、 $P(n_0+1)$为真；（归纳基础）

2）假设对于$n\leqslant k(k\geqslant n_0)$，有$P(n)$为真； （归纳假设）

3）证明$n=k+1$，有$P(k+1)$为真。 （归纳结论）

结论 对所有的整数$n\geqslant n_0$，都有$P(n)$为真。

谓词表示：

$$(\exists n_0)(P(n_0)\land P(n_0+1)\land(\forall n)((n\leq k)\land P(n)\rightarrow P(k+1))=1$$

例3.4.1

用数学归纳法证明：

对所有n≥1，有$1+2+3+\cdots+n=\dfrac{n(n+1)}{2}$

证明 **归纳基础验证**

$1=\dfrac{1(1+1)}{2}$ 显然P(1)真值为1；

归纳假设假定 对于n=k(k≥1)，有P(k)为真，即有

$1+2+3+\cdots+k=\dfrac{k(k+1)}{2}$；

例3.4.1证明

归纳结论证明　对于n＝k＋1，有P(k+1)为真

$$1+2+3+\cdots+k+(k+1)$$

$$=\frac{k(k+1)}{2}+(k+1)$$

$$=(k+1)(\frac{k}{2}+1)=\frac{(k+1)(k+2)}{2}=\frac{(k+1)((k+1)+1)}{2}$$

由数学归纳法原理得到，P(n)对所有n≥1为真。

例3.4.2

对每个正整数$n\geq 1$，能惟一地写成 $p_1^{a_1}p_2^{a_2}...p_s^{a_s}$，其中$P_i$是素数且满足$P_1<P_2<\cdots<P_s$。

分析 设$P(n)$： $n=p_1^{a_1}p_2^{a_2}...p_s^{a_s}$； 由于素数一定是大于等于2的正整数，因此，$n_0=2$。

例3.4.2

证明 归纳基础验证

因为$2=2^1$，$3=3^1$，所以P(2)、P(3)为真；

归纳假设假定

对$n\le k$的所有正整数，都有P(n)为真，即

$$n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$$

例3.4.2(续)

归纳结论证明 对n＝k＋1，需分两种情况讨论：

（1） 如果n本身就是一个素数，则k＋1＝$(k+1)^1$，即P(k+1)为真；

（2） 如果n不是一个素数，则k＋1＝lm，其中2≤l≤k，2≤m≤k，此时由归纳假设有

$$l = p_1^{b_1} p_2^{b_2} \cdots p_s^{b_s},$$

$$m = p_1^{c_1} p_2^{c_2} \cdots p_s^{c_s}$$

其中，$P_1, P_2, \cdots, P_s$是素数，且是包含l、m中全部分解因子， b_i、c_i≥0的自然数，

例3.4.2(续)

为此有

$$k+1=lm=p_1^{b_1}p_2^{b_2}...p_s^{b_s}\ p_1^{c_1}p_2^{c_2}...p_s^{c_s}$$

$$=p_1^{b_1+c_1}p_2^{b_2+c_2}...p_s^{b_s+c_s}=\ p_1^{a_1}p_2^{a_2}...p_s^{a_s}$$

由于$P_1, P_2, \cdots, P_s$是素数，所以k+1能分解成素数的积，又因为l和m的因子分解是惟一的，所以k＋1的因子分解也是惟一的，所以P(k+1)是真的。由数学归纳法原理得到，P(n)对所有n≥1为真。

3.4.2　数学归纳法应用

例3.4.3 用数学归纳法证明下列伪码程序的计算结果是两个正整数的最大公因子。其中伪码程序为：

```
FUNCTION  GCD(X, Y)
   1. WHILE (X≠Y)
        a. IF (X>Y) THEN
            1. X←X-Y
        b. ELSE
          1. Y←Y-X
     2. RETURN(X)
END OF FUNCTION GCD
```

证明

归纳基础验证　因为在循环开始之前存在变量值X_0＝X，Y_0＝Y，因此，P(0)是命题GCD(X_0，Y_0)＝GCD(X, Y)，显然命题为真；

归纳假设假定　设P(k)是命题GCD(X_k，Y_k)＝GCD(X, Y)为真；

证明(续)

归纳结论证明 首先考虑P(k＋1)的左边，即$GCD(X_{k+1}, Y_{k+1})$。在通过k＋1次循环后，

或者$X_{k+1}=X_k$和$Y_{k+1}=Y_k-X_k$；

或者$X_{k+1}=X_k-Y_k$和$Y_{k+1}=Y_k$；

则由整数的基本性质知，$P(k+1)=GCD(X_{k+1}, Y_{k+1})=GCD(X_k, Y_k)=GCD(X, Y)$。

根据数学归纳法知：对所有n≥0，有P(n)为真。为此，该伪码程序输出的结果必是两个正整数的最大公因子。

铺瓦问题

例3.4.4 一个直角三正方形，是一个由三个正方形组成的对象，如图1所示。如果我们从n×n(n为2的幂)正方形的板中去掉一个正方形，则余下的图形可用直角三正方形来铺成，如图2。此处的铺成是用直角三正方形正好覆盖全图的图形，每个直角三正方形不能有重叠，也不许超出图形之外。我们缺少一个正方形的板称为一个缺方板，把此问题称为铺瓦问题。

直角三正方形

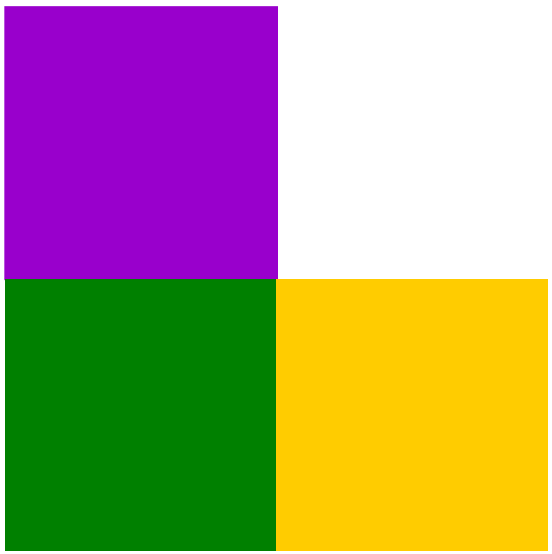


图1

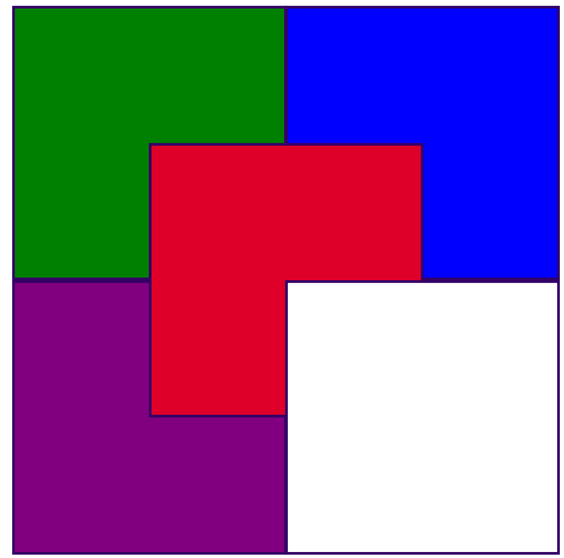


图2

证明

归纳基础验证　如k＝1，2×2缺方板本身就是一个直角三正方形。因此可由三正方形铺成；

归纳假设假定　设我们可以把$2^k \times 2^k$的缺方板用直角三正方形铺成；

证明(续)

归纳结论证明部分　对于$2^{k+1}\times 2^{k+1}$的缺方板问题，我们可以将其分成四个$2^k\times 2^k$的板，如图所示。旋转此板，使缺少的正方形在左上的四分之一中。由归纳假设，此左上的$2^k\times 2^k$缺方板可由直角三正方形铺成，把一个直角三正方形T放在中间，则另外三个四分之一都是$2^k\times 2^k$的缺方板。由归纳假设，它们的铺瓦问题都是可以解决的。于是$2^{k+1}\times 2^{k+1}$的缺方板可由直角三正方形铺成。

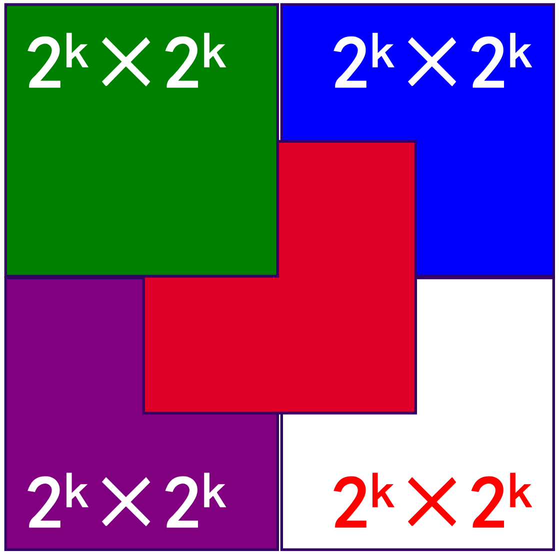


图3

由数学归纳法知，对任何的n，n×n正方形的铺瓦问题都是可以铺成的。

3.5 按定义证明方法 （CP规则证明）

在离散数学中，我们大量的定义描述都是用蕴涵型“$P \rightarrow Q$”的方式来描述的。

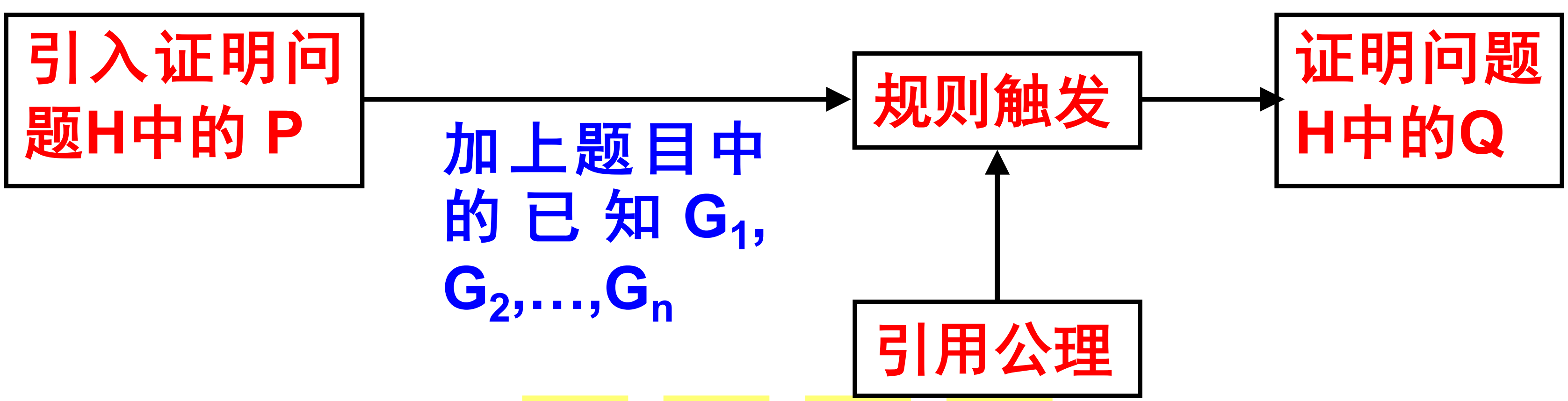
如集合中子集的包含关系的定义描述为：

$$A \subseteq B \Leftrightarrow (\forall a)(a \in A \rightarrow a \in B)$$

3.5.1 按定义证明方法原理

设有一组前提(或叫做已知条件)为$\Gamma=\{G_1,G_2,\ldots,G_n\}$，证明问题$H = P\rightarrow Q$，则利用CP规则的证明方式，将证明问题H中的前提P作为附加前提，加入到前提集合当中，构成一组新前提$\Gamma'=\{G_1,G_2,\ldots,G_n,P\}$，此时，证明这组新前提$\Gamma' \Rightarrow Q$，即有

$$\Gamma \Rightarrow H \overset{\text{CP}}{\Longleftrightarrow} \Gamma' \Rightarrow Q$$



3.5.2 按定义证明方法应用

例3.5.1 设A、B是两个任意集合，证明

$A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$，其中P(X)表示集合X的幂集（所有子集的集合）

证明 （1）必要性“$\Rightarrow$”：

对任意$x \in P(A)$，则$x \subseteq A$, 由于$A \subseteq B$，所以$x \subseteq B$，即有$x \in P(B)$。由CP规则知：

$$P(A) \subseteq P(B)。$$

即 $A \subseteq B \Rightarrow P(A) \subseteq P(B)$

例3.5.1(续)

（2）充分性“$\Leftarrow$”：

对任意$x\in A$，则$\{x\}\in P(A)$，由于$P(A)\subseteq P(B)$，所以$\{x\}\in P(B)$，即有$x\in B$。由CP规则知：

$$A\subseteq B。$$

即 $P(A)\subseteq P(B)\Rightarrow A\subseteq B$。

原式得证。

例3.5.2

如果A $\subseteq$ B，则A∪B＝B且A∩B＝A

证明两个集合相等，即是证明两个集合相互包含，请学生自证。