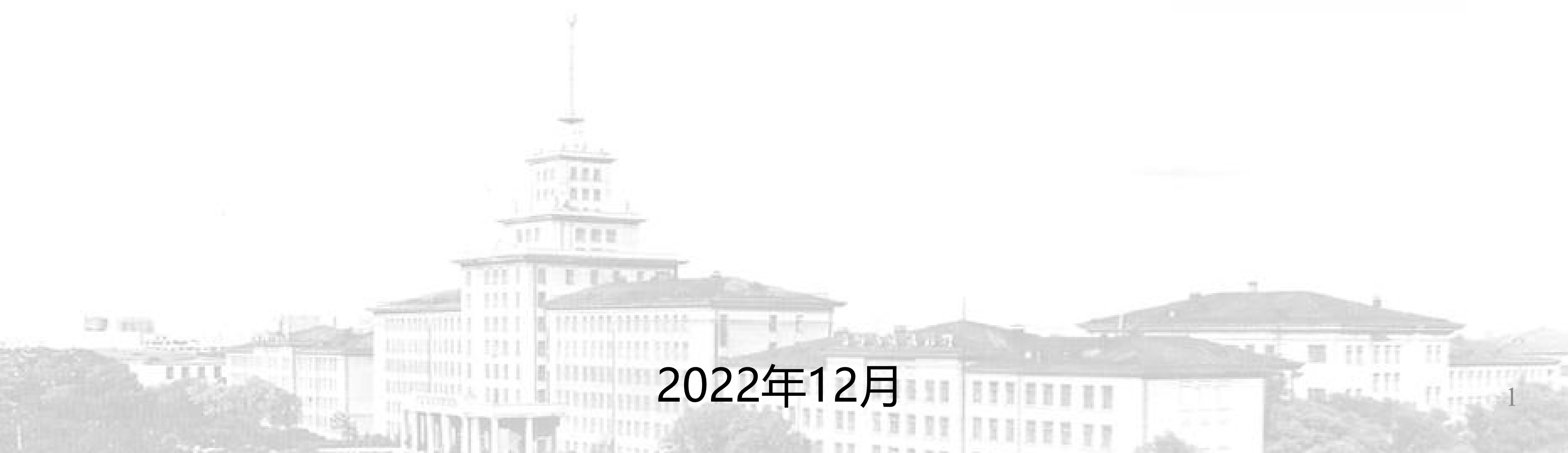
第10讲 命题演算形式系统-基本定理30-34及演绎定理

授课教师：蒋琳
e-mail: zoeljiang@hit.edu.cn

哈尔滨工业大学（深圳）计算机科学与技术学院



2022年12月

推理部分

公理集合:

（1） A_1: $A \to (B \to A)$

（2） A_2: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

（3） A_3: $(\neg A \to \neg B) \to (B \to A)$

推理规则或分离规则（Modus Ponens）：

若有A和$A \to B$成立，则必有结论B成立，可形式化表示为:

$$r_{mp}: \frac{A,\ A \to B}{B}$$

证明

证明的定义: 称下列公式序列为公式A 在PC 中的一个证明:

$$A_1, A_2, \cdots, A_m (= A)$$

如果对任意的 $i \in \{1,2,\cdots,m\}$，A_i 或者是PC中的公理，或者是 $A_j (j < i)$，或者$A_j, A_k (j, k < i)$用分离规则导出的。**其中A_m就是公式A。**

注释： A_i 只能是以下三种中的其一:

（1）PC中的公理或已知定理;

（2）序列$A_1, A_2, \cdots, A_{i-1}$中的某一个;

（3）序列$A_1, A_2, \cdots, A_{i-1}$中某两个用分离规则导出的。

基本定理

定理1：$\vdash_{PC} A \to A$ ($A \to A$是PC中的一个定理)√

定理2：如果$\vdash_{PC} A \to (B \to C)$，那么$\vdash_{PC} B \to (A \to C)$ （前件互换定理）√

定理3：$\vdash (A \to (B \to C)) \to (B \to (A \to C))$ 定理（2）的另一种形式 √

定理4：$\vdash (B \to C) \to ((A \to B) \to (A \to C))$（加前件定理）√

定理5：$\vdash (A \to B) \to ((B \to C) \to (A \to C))$（加后件定理）√

定理6：$\vdash \neg A \to (A \to B)$√

定理7：$\vdash A \to (\neg A \to B)$√

定理8：如果$\vdash (A \to B)$，$\vdash (B \to C)$，那么$\vdash (A \to C)$（三段论定理）√

定理9. $\vdash (\neg A \to A) \to A$ （反证法）√

定理10. $\vdash \neg\neg A \to A$√

定理11. $\vdash (A \to \neg A) \to \neg A$ （反证法）√

定理12. $\vdash A \to \neg\neg A$√

基本定理

定理13：$\vdash (A \to B) \to (\neg B \to \neg A)$ （公理A_3的逆命题）√

定理14：$\vdash (\neg A \to B) \to (\neg B \to A)$ √

定理15：$\vdash (A \to \neg B) \to (B \to \neg A)$ √

定理16：$\vdash (\neg A \to B) \to ((\neg A \to \neg B) \to A)$ （反证法）√

定理17：$\vdash (A \to B) \to ((A \to \neg B) \to \neg A)$√

定理18：$\vdash \neg A \to C$，$\vdash B \to C$当且仅当$\vdash (A \to B) \to C$√

定理19：$\vdash A \to A \vee B$，其中，$A \vee B$定义为$\neg A \to B$，也即√

$$A \to A \vee B \Leftrightarrow A \to (\neg A \to B)$$ (等价于定理7)

定理20：$\vdash A \to B \vee A$，其中，$A \vee B$定义为$\neg A \to B$，也即√

$$A \to B \vee A \Leftrightarrow A \to (\neg B \to A)$$ (等价于公理1)

定理21：如果$\vdash P \to Q$, 且$\vdash R \to S$, 则$\vdash (Q \to R) \to (P \to S)$√

定理22：$\vdash (A \to C) \to ((B \to C) \to ((A \vee B) \to C))$ 也即√

$$(A \to C) \to ((B \to C) \to ((\neg A \to B) \to C))$$ （二难推理）

基本定理

定理23： $\vdash A \wedge B \rightarrow C$ 当且仅当 $\vdash A \rightarrow (B \rightarrow C)$ √

定理24： $\vdash A \wedge B \rightarrow A$ √

定理25： $\vdash A \wedge B \rightarrow B$ √

定理26： $\vdash A \rightarrow (B \rightarrow (A \wedge B))$ √

定理27： $\vdash (A \rightarrow B) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B \wedge C))$ √

定理28： $\vdash A \vee B \leftrightarrow B \vee A$ √

定理29： $\vdash A \wedge B \leftrightarrow B \wedge A$ √

PC系统的结合律

定理30：$\vdash (A \vee B) \vee C \leftrightarrow A \vee (B \vee C)$

定理31：$\vdash (A \wedge B) \wedge C \leftrightarrow A \wedge (B \wedge C)$

注：只证明定理30，定理31类似。

$A \vee B \Leftrightarrow \neg A \to B$

PC系统的结合律

定理30：$\vdash (\neg(\neg A \to B) \to C) \to (\neg A \to (\neg B \to C))$

$\vdash (\neg A \to (\neg B \to C)) \to (\neg(\neg A \to B) \to C)$

证明： （1）$(\neg(\neg A \to B) \to C) \to (\neg C \to (\neg A \to B))$ 定理14

（2）$(\neg C \to (\neg A \to B)) \to (\neg A \to (\neg C \to B))$ 前件互换定理3

（3）$(\neg C \to B) \to (\neg B \to C)$ 定理14

（4）$((\neg C \to B) \to (\neg B \to C)) \to (\neg A \to ((\neg C \to B) \to (\neg B \to C)))$ 公理1

（5）$\neg A \to ((\neg C \to B) \to (\neg B \to C))$ （3）和（4）用rmp分离规则

（6）$(\neg A \to ((\neg C \to B) \to (\neg B \to C))) \to ((\neg A \to (\neg C \to B)) \to (\neg A \to (\neg B \to C)))$公理2

（7）$((\neg C \to B) \to (\neg B \to C)) \to$

$((\neg A \to (\neg C \to B)) \to (\neg A \to (\neg B \to C)))$ **(4)** 和 **(6)** 用三段论定理8

（8）$(\neg A \to (\neg C \to B)) \to (\neg A \to (\neg B \to C))$ （3）和（7）用rmp分离规则

（9）$(\neg C \to (\neg A \to B)) \to (\neg A \to (\neg B \to C))$ **(2)** 和 **(8)** 用三段论定理8

（10）$(\neg(\neg A \to B) \to C) \to (\neg A \to (\neg B \to C))$ （1）和（9）用三段论定理8

PC系统的结合律

定理30：$\vdash (\neg(\neg A \to B) \to C) \to (\neg A \to (\neg B \to C))$

$\vdash (\neg A \to (\neg B \to C)) \to (\neg(\neg A \to B) \to C)$

证明：

定理18：$\vdash \neg A \to C$，$\vdash B \to C$当且仅当$\vdash (A \to B) \to C$

(1) $B \to (\neg A \to B)$ 公理1

(2) $(B \to (\neg A \to B)) \to (\neg(\neg A \to B) \to \neg B)$ 定理13

(3) $\neg(\neg A \to B) \to \neg B$ （1）和（2）用rmp分离规则

(4) $(\neg(\neg A \to B) \to \neg B) \to$

$((\neg B \to C) \to (\neg(\neg A \to B) \to C))$ 加后件定理5

(5) $(\neg B \to C) \to (\neg(\neg A \to B) \to C)$ （3）和（4）用rmp分离规则

(6) $A \to (\neg A \to B)$ 定理7

(7) $(A \to (\neg A \to B)) \to (\neg(\neg A \to B) \to \neg A)$ 定理13

(8) $\neg(\neg A \to B) \to \neg A$ （6）和（7）用rmp分离规则

(9) $\neg A \to (A \to C)$ 定理6

(10) $\neg(\neg A \to B) \to (A \to C)$ （8）和（9）用三段论定理8

(11) $A \to (\neg(\neg A \to B) \to C)$ （10）用前件互换定理2

(12) $\neg\neg A \to A$ 定理10

(13) $\neg\neg A \to (\neg(\neg A \to B) \to C)$ （12）和（11）用三段论定理8

(14) $(\neg A \to (\neg B \to C)) \to (\neg(\neg A \to B) \to C)$ 由（13）和（5）用定理18

PC系统的吸收律

定理32：$\vdash A \land (A \lor B) \leftrightarrow A$

定理33：$\vdash A \lor (A \land B) \leftrightarrow A$

注：只证明定理32，定理33类似。定理32定义式为：

$$\neg(A \to \neg(\neg A \to B)) \leftrightarrow A$$

PC系统的吸收律

定理32：$\neg(A \to \neg(\neg A \to B)) \leftrightarrow A$

证明思路：

$$\neg(A \to \neg(\neg A \to B)) \leftrightarrow A$$

$$\neg(A \to \neg(\neg A \to B)) \to A$$

定理14

$$\neg A \to (A \to \neg(\neg A \to B))$$

定理6

$$A \to \neg(A \to \neg(\neg A \to B))$$

定理15

$$(A \to \neg(\neg A \to B)) \to \neg A$$

定理18

$$\neg(\neg A \to B) \to \neg A$$

公理3

$$A \to (\neg A \to B)$$

定理7

$$\neg A \to \neg A$$

定理1

PC系统的吸收律

定理32：$\vdash \neg(A \rightarrow \neg(\neg A \rightarrow B)) \rightarrow A$

$$\vdash A \rightarrow \neg(A \rightarrow \neg(\neg A \rightarrow B))$$

证明：

（1）$\neg A \rightarrow (A \rightarrow \neg(\neg A \rightarrow B))$ 定理6

（2）$(\neg A \rightarrow (A \rightarrow \neg(\neg A \rightarrow B))) \rightarrow$

$(\neg(A \rightarrow \neg(\neg A \rightarrow B)) \rightarrow A)$ 定理14

（3）$\neg(A \rightarrow \neg(\neg A \rightarrow B)) \rightarrow A$ （1）和（2）用rmp分离规则

PC系统的吸收律

定理32：$\vdash \neg(A \to \neg(\neg A \to B)) \to A$

$\vdash A \to \neg(A \to \neg(\neg A \to B))$

证明：

定理18：$\vdash \neg A \to C$， $\vdash B \to C$当且仅当$\vdash (A \to B) \to C$

(1) $\neg A \to \neg A$ 定理1

(2) $A \to (\neg A \to B)$ 定理7

(3) $(A \to (\neg A \to B)) \to (\neg(\neg A \to B) \to \neg A)$ 定理13

(4) $\neg(\neg A \to B) \to \neg A$ （2）和（3）用rmp分离规则

(5) $(A \to \neg(\neg A \to B)) \to \neg A$ 由（1）和（4）用定理18

(6) $((A \to \neg(\neg A \to B)) \to \neg A) \to$

$(A \to \neg(A \to \neg(\neg A \to B)))$ 定理15

(7) $A \to \neg(A \to \neg(\neg A \to B))$ （5）和（6）用rmp分离规则

PC系统的分配律

定理34：$\vdash A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$

定理35：$\vdash A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$

注：只证明定理34，定理35类似。

PC系统的分配律

定理34：$\vdash A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$

证明思路： $A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$

$$\downarrow$$

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

定理10 $\downarrow$

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

先证 $\downarrow$

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

前件互换定理2 $\downarrow$

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

公理3 $\downarrow$

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

定理27

$$\Updownarrow$$

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

定理27：$\vdash (A \rightarrow B) \rightarrow ((A \rightarrow C) \rightarrow (A \rightarrow B \wedge C))$

PC系统的分配律

定理34：$\vdash A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$

证明： （1）$(A \to \neg B) \to ((A \to \neg C) \to (A \to \neg B \wedge \neg C))$ 定理27

（2）$(A \to \neg B) \to ((A \to \neg C) \to (A \to \neg(\neg B \to C)))$ 定理27

（3）$(A \to (\neg A \to B)) \to (\neg(\neg A \to B) \to \neg A)$ 定理13

（4）$\neg(\neg A \to B) \to \neg A$ （2）和（3）用rmp分离规则

（5）$(A \to \neg(\neg A \to B)) \to \neg A$ 由（1）和（4）用定理18

（6）$((A \to \neg(\neg A \to B)) \to \neg A) \to$

$(A \to \neg(A \to \neg(\neg A \to B)))$ 定理15

（7）$A \to \neg(A \to \neg(\neg A \to B))$ （5）和（6）用rmp分离规则

定理27：$\vdash (A \to B) \to ((A \to C) \to (A \to B \wedge C))$

$A \wedge B$定义为$\neg(A \to \neg B)$

PC系统的分配律

定理34：$\vdash A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$

证明思路：

$$A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$$

$$\downarrow$$

$$\neg(A \to \neg(\neg B \to C)) \leftrightarrow (\neg\neg(A \to \neg B) \to \neg(A \to \neg C))$$

定理10 $\downarrow$

$$\neg(A \to \neg(\neg B \to C)) \leftrightarrow ((A \to \neg B) \to \neg(A \to \neg C))$$

再证 $\downarrow$

$$((A \to \neg B) \to \neg(A \to \neg C)) \to \neg(A \to \neg(\neg B \to C))$$

定理18

$$\neg(A \to \neg B) \to \neg(A \to \neg(\neg B \to C))$$

公理3 $\downarrow$

$$(A \to \neg(\neg B \to C)) \to (A \to \neg B)$$

逆用加前件定理4 $\downarrow$

$$\neg(\neg B \to C) \to \neg B$$

公理3 $\downarrow$

$$B \to (\neg B \to C)$$

定理7

$$\neg(A \to \neg C) \to \neg(A \to \neg(\neg B \to C))$$

公理3 $\downarrow$

$$(A \to \neg(\neg B \to C)) \to (A \to \neg C)$$

逆用加前件定理4 $\downarrow$

$$\neg(\neg B \to C) \to \neg C$$

公理3 $\downarrow$

$$C \to (\neg B \to C)$$

公理1

演绎

演绎的定义： 设Γ为PC的公式集合，称以下公式序列为公式A的一个以Γ为前提在PC中的演绎：

$$A_1, A_2, \cdots, A_m (= A)$$

如果对任意的 $i \in \{1,2,\cdots,m\}$，A_i**或者是 Γ 的成员，**或者是PC中的公理，或者是$A_j(j < i)$，或者$A_j, A_k(j,k < i)$用分离规则导出的。其中 A_m就是公式A。

证明的定义： 称下列公式序列为公式A在PC中的一个证明：

$$A_1, A_2, \cdots, A_m (= A)$$

如果对任意的 $i \in \{1,2,\cdots,m\}$，A_i 或者是PC中的公理，或者是$A_j(j < i)$，或者$A_j, A_k(j,k < i)$用分离规则导出的。**其中A_m就是公式A。**

演绎结果

演绎结果： 称A是前提Γ在PC 中的演绎结果，记为$\Gamma \vdash_{PC} A$，如果公式A有一个以Γ为前提在PC 中的演绎。

- 如果$\Gamma = \{B\}$，则用$B \vdash_{PC} A$表示$\Gamma \vdash_{PC} A$；（**去掉了{}**）
- 如果$B \vdash_{PC} A$并且$A \vdash_{PC} B$，则记为 $A \vdash\dashv B$ （A B 相互演绎）。

注释：若$\Gamma \vdash_{PC} A$，则有$A_1, A_2, \cdots, A_m (= A)$

（1）若$\Gamma = \phi$（空集），$\Gamma \vdash_{PC} A$即$\phi \vdash_{PC} A$，那么$\vdash_{PC} A$，即演绎退化为证明。

（2）若$A \in \Gamma$，则必有$\Gamma \vdash_{PC} A$（此时的序列是A），

（3）$\{A\} \vdash_{PC} A$，$\{A, B, C\} \vdash_{PC} A$，$\{A, B, C\} \vdash_{PC} B$，$\{A, B, C\} \vdash_{PC} C$ 。

演绎定理

演绎定理： 对PC中的任意公式集合Γ和公式A, B, $\Gamma \cup \{A\} \vdash_{\mathrm{PC}} B$当且仅当$\Gamma \vdash_{\mathrm{PC}} A \to B$。

充分性： 已知$\Gamma \vdash A \to B$，往证$\Gamma \cup \{A\} \vdash B$。

证明：

- 因为$\Gamma \vdash A \to B$，则有演绎序列 $A_1, A_2, \cdots, A_m\ (= A \to B)$。
- 在此序列中加上公式$A_{m+1} = A, A_{m+2} = B$得到一个以$\Gamma \cup \{A\}$为前提对B的演绎过程。

$$\Gamma; A \stackrel{\text{def}}{=} \Gamma \cup \{A\}$$
$$\Gamma; A, B, C \stackrel{\text{def}}{=} \Gamma \cup \{A, B, C\}$$

演绎定理

必要性： 已知$\Gamma \cup \{A\} \vdash_{\mathrm{PC}} B$，往证$\Gamma \vdash_{\mathrm{PC}} A \to B$。

证明：对$\Gamma \cup \{A\} \vdash_{\mathrm{PC}} B$的演绎序列的长度$l$用第二数学归纳法

（1）当$l = 1$时，序列中只有B。那么B或是公理或是假设中的元素即$B \in \Gamma \cup \{A\}$，即为如下可能：

（1）B为公理；（2）$B \in \Gamma$；（3）$B = A$

- 对（1）有B公理，$B \to (A \to B)$公理1，$A \to B$分离规则，构成了一个**证明**，则$\Gamma \vdash \mathrm{A} \to B$
- 对（2）有B前提，$B \to (A \to B)$公理1，$A \to B$分离规则，构成了一个**演绎序列**，则$\Gamma \vdash A \to B$
- 对（3）由$A = B$知$\vdash A \to A(= B)$定理1，则$\Gamma \vdash A \to B$

（2）假设当演绎序列的长度比l小时结论成立。

（3）则长度为l时，演绎序列为$A_1, A_2, \cdots$，$A_{m=l}(= B)$。观察B（4种可能）：

- 如果B为公理或者为$\Gamma \cup \{A\}$中的元素，可仿照$l = 1$的情形证明结论完全正确。
- 如果$B = A_j\,(j < l)$，则由于$\Gamma \cup \{A\} \vdash A_j$，由于$j < l$知$\Gamma \vdash A \to A_j$，即$\Gamma \vdash A \to B$。
- 如果B为$A_j, A_k(j, k < l)$用分离规则导出，不妨设$A_k = A_j \to B$，由$\Gamma \cup \{A\} \vdash A_j$，$\Gamma \cup \{A\} \vdash A_j \to B$，根据（2）知$\Gamma \vdash A \to A_j$，$\Gamma \vdash A \to (A_j \to B)$。此两序列加上公式$(A \to (A_j \to B)) \to ((A \to A_j) \to (A \to B))$（公理2）并用分离规则得$(A \to A_j) \to (A \to B)$，再使用分离规则得$A \to B$，这样一个公式序列是一个以$\Gamma$为前提对$A \to B$的一个演绎过程。从而$\Gamma \vdash A \to B$。

演绎定理的应用

例1 $\vdash (A \to (B \to C)) \to ((C \to D) \to (A \to (B \to D)))$

证明思路：

- 只需证 $(A \to (B \to C)) \vdash ((C \to D) \to (A \to (B \to D)))$
- 只需证 $A \to (B \to C), C \to D \vdash A \to (B \to D)$
- 只需证 $A \to (B \to C), C \to D, A \vdash B \to D$
- 只需证 $A \to (B \to C), C \to D, A, B \vdash D$

证明：使用演绎定理进行证明

(1) A 假设
(2) B 假设
(3) $C \to D$ 假设
(4) $A \to (B \to C)$ 假设
(5) $B \to C$ （1）和（4）用分离规则
(6) C （2）和（5）用分离规则
(7) D （6）和（3）用分离规则
(8) $A \to (B \to C), C \to D, A, B \vdash D$
(9) $A \to (B \to C), C \to D, A \vdash B \to D$
(10) $A \to (B \to C), C \to D \vdash A \to (B \to D)$
(11) $(A \to (B \to C)) \vdash ((C \to D) \to (A \to (B \to D)))$
(12) $\vdash (A \to (B \to C)) \to ((C \to D) \to (A \to (B \to D)))$

这一块要加上！

演绎定理：对PC中的任意公式集合Γ和公式A, B, $\Gamma \cup \{A\} \vdash_{PC} B$当且仅当$\Gamma \vdash_{PC} A \to B$。

演绎定理应用

例2：$\vdash ((A \to B) \to (A \to C)) \to (A \to (B \to C))$

证明思路：

- 只需证 $(A \to B) \to (A \to C) \vdash A \to (B \to C)$
- 只需证 $(A \to B) \to (A \to C)$, $A \vdash (B \to C)$
- 只需证 $(A \to B) \to (A \to C), A$, $B \vdash C$

证明：使用演绎定理进行证明

演绎定理： 对PC中的任意公式集合Γ和公式A, B, $\Gamma \cup \{A\} \vdash_{PC} B$当且仅当$\Gamma \vdash_{PC} A \to B$。

(1) A 假设

(2) B 假设

(3) $(A \to B) \to (A \to C)$ 假设

(4) $B \to (A \to B)$ 公理1

(5) $B \to (A \to C)$ （4）和（3）用三段论定理8

(6) $A \to C$ （2）和（5）用rmp分离规则

(7) C （1）和（6）用rmp分离规则

(8) $(A \to B) \to (A \to C), A,\ B \vdash C$

(9) $(A \to B) \to (A \to C), A \vdash (B \to C)$

(10) $(A \to B) \to (A \to C) \vdash A \to (B \to C)$

(11) $\vdash ((A \to B) \to (A \to C)) \to (A \to (B \to C))$

这一块要加上！