经典命题逻辑公理系统定理证明算法设计

杜国平 [1, 2]

（1. 南京大学哲学系 210093；2.南京航空航天大学计算机系 210016）

内容提要：本文利用演绎定理的证明思路给出了一个由演绎证明构造公理证明的一般程序，并增加了一条简化命令，使该程序既严格又具有实际可操作性。

关键词： 演绎证明 公理证明 程序

中图分类号：B81 **文献标识码：A**

在经典命题逻辑常见的公理系统中，仅仅从公理和推理规则出发进行定理的形式证明一般没有能行的程序，对于初学者而言是比较困难的。但是，在经典命题逻辑公理系统中，演绎定理成立，而使用演绎定理来构造定理的形式证明是比较简单的。实际上，演绎定理的证明过程已经表明：有了一个使用演绎定理的形式证明（简称为演绎证明），就可以构造出仅仅从公理和推理规则出发的形式证明（简称为公理证明）。本文拟对由演绎证明构造公理证明的具体算法和技巧进行一些探讨。

为了说明的方便，我们取如下的命题逻辑公理系统 PC 来进行讨论。

系统 PC 由如下三条公理模式和一条推理规则构成：

公理模式为：

$(Ax1)\ \ A \to (B \to A)$
$(Ax2)\ \ (A \to (B \to C)) \to ((A \to B) \to (B \to C))$
$(Ax3)\ \ (\neg A \to B) \to ((\neg A \to \neg B) \to A)$

推理规则即分离规则（Modus ponens）：由 A 和 $A \to B$ 可以推出 B。简记为 MP。

在系统 PC 中显然可以证明：

演绎定理 (DT)：如果 Σ， $A + B$，那么 $\Sigma + A \to B$。

因为任一证明序列都是有限长的，因此，演绎证明中需要引入的假设也是有限的。所以我们只考虑假设集 Σ 为有限集的情况，令 $\Sigma = \{A_1, A_2, \mathrm{L}, A_{m-1}, A_m\}$。

假设有一个 $\Sigma \cup \{A_0\} + B$ 的演绎证明，该证明的公式序列为：$C_1, C_2, \mathrm{L}, C_n = B$。那么我们可按照下述程序构造出一个 $\Sigma + A_0 \to B$ 的演绎证明。

收稿日期：2004-11-25；
作者简介：杜国平，1965 **年生，男，汉族，江苏盱眙人，南京大学副教授。**
基金项目：国家社科基金项目（02CZX008**）；南京大学引进人才基金项目；南京大学笆川青年教育基金项目。**
联系方式：210093 **南京大学哲学系** Email: dgpnju@126.com **电话：**025-83597161

[1] 如果 $A_0 \to C_n$ 是公理或者 $A_0 \to C_n \in \Sigma$，则执行如下子程序[1']，即直接写入：

$A_0 \to C_n$

[2] 如果 C_n 是公理，则执行如下子程序[2']：

C_n
$C_n \to (A_0 \to C_n)$
$A_0 \to C_n$

[3] 如果 C_n 是 A_0，则执行如下子程序[3']：

$A_0 \to ((B \to A_0) \to A_0)$
$(A_0 \to ((B \to A_0) \to A_0)) \to ((A_0 \to (B \to A_0)) \to (A_0 \to A_0))$
$(A_0 \to (B \to A_0)) \to (A_0 \to A_0)$
$A_0 \to (B \to A_0)$
$A_0 \to A_0$

[4] 如果 $C_n = A_k \in \Sigma$，$k \in \{1, 2, \mathrm{L}, m\}$，则执行如下子程序[4']：

A_k
$A_k \to (A_0 \to A_k)$
$A_0 \to A_k$

[5] 如果 C_n 是由 C_i，$C_j (= C_i \to C_n)$ $(i, j \in \{1, 2, \mathrm{L}, n-1\})$ 经使用分离规则而得到，则对 C_j 执行如下子程序[5']：

$(A_0 \to (C_i \to C_n)) \to ((A_0 \to C_i) \to (A_0 \to C_n))$
$(A_0 \to C_i) \to (A_0 \to C_n)$
$A_0 \to C_n$

[6] 对[4]中出现的 C_i，C_j 重复执行程序[1]～[6]。

[7] 若程序全部进入[1]～[4]，则执行完[1']～[4']，程序终止。

对 $\Sigma + A_0 \to B$ 反复使用上述程序 m 次之后，就可以得到一个 $+ A_m \to (A_{m-1} \to \mathrm{L} \to (A_1 \to (A_0 \to B))\mathrm{L})$ 的公理证明。

例 1　在系统 PC 中构造定理 $+ ((A \to B) \to C) \to (B \to C)$ 的公理证明。

首先，我们构造一个 $((A \to B) \to C),\ B + C$ 的演绎证明。

证明1'：

1	$(A \to B) \to C$	假设
2	B	假设
3	$B \to (A \to B)$	$(Ax1)$
4	$A \to B$	2、3 MP
5	C	1、4 MP

其次，由 $(A \to B) \to C$，$B + C$ 的演绎证明构造 $(A \to B) \to C + B \to C$ 的演绎证明。

1、这可以通过回溯检查逐步完成。证明1' 的第 5 行为 C，进入程序[1]检查 $B \to C$，发现它既不是公理也不属于假设集 $\{((A \to B) \to C)\}$；进入程序[2]～[5]发现 C 由第 1、4 行 $(A \to B) \to C$ 和 $A \to B$ 分离而得。因此，执行子程序[5']：

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

2、进入程序[6]，对$(A \to B) \to C$和$A \to B$执行程序[1]～[6]。

3、进入程序[1]，检查$B \to ((A \to B) \to C)$，发现它既不是公理也不属于假设集$\{((A \to B) \to C)\}$；进入程序[2]～[5]发现$(A \to B) \to C$属于假设集$\{((A \to B) \to C)\}$。因此，执行子程序[4']：

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

4、进入程序[1]，检查$B \to (A \to B)$，发现它是公理。因此，执行子程序[1']：

$B \to (A \to B)$

5、程序已经全部进入[1]～[4]，并且已经执行完子程序[1']～[4']，因此程序终止。

所以我们得到一个$(A \to B) \to C + B \to C$的演绎证明。

证明1"：

1	$(A \to B) \to C$	假设
2	$((A \to B) \to C) \to (B \to ((A \to B) \to C))$	$(Ax1)$
3	$B \to ((A \to B) \to C)$	1、2 MP
4	$B \to (A \to B)$	$(Ax1)$
5	$(B \to ((A \to B) \to C)) \to ((B \to (A \to B)) \to (B \to C))$	$(Ax2)$
6	$(B \to (A \to B)) \to (B \to C)$	3、5 MP
7	$B \to C$	4、6 MP

再次，由$(A \to B) \to C + B \to C$的演绎证明构造+ $((A \to B) \to C) \to (B \to C)$的公理证明。

1、进入程序[1] 检查$((A \to B) \to C) \to (B \to C)$，发现它不是公理（此时，因为假设集是空集，所以它也当然不属于假设集）；进入程序[2]～[5]发现$B \to C$由第 4、6 行$B \to (A \to B)$和$(B \to (A \to B)) \to (B \to C)$分离而得。因此，执行子程序[5']：

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

2、进入程序[6]，对$B \to (A \to B)$和$(B \to (A \to B)) \to (B \to C)$执行程序[1]～[6]。

3、进入程序[1]，检查$((A \to B) \to C) \to (B \to (A \to B))$，发现它不是公理；进入程序[2]～[5]发现$B \to (A \to B)$是公理。因此，执行子程序[2']：

$B \to (A \to B)$

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

4、进入程序[1] 检查$((A \to B) \to C) \to ((B \to (A \to B)) \to (B \to C))$，发现它不是公理 进入程序[2]～[5]发现$(B \to (A \to B)) \to (B \to C)$由第 3、5 行 $B \to ((A \to B) \to C)$ 和 $(B \to ((A \to B) \to C)) \to ((B \to (A \to B)) \to (B \to C))$ 分离而得。因此，执行子程序[5']：

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

5、进入程序[6]，对 $B \to ((A \to B) \to C)$ 和 $(B \to ((A \to B) \to C)) \to ((B \to (A \to B)) \to (B \to C))$ 执行程序[1]～[6]。

6、进入程序[1]，检查$((A \to B) \to C) \to (B \to ((A \to B) \to C))$，发现它是公理。因此，执行子程序[1']：

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

7、进入程序[1]，检查 $((A \to B) \to C) \to ((B \to ((A \to B) \to C)) \to ((B \to (A \to B)) \to (B \to C)))$，发现它不是公理；进入程序[2]～[5]发现 $(B \to ((A \to B) \to C)) \to ((B \to (A \to B)) \to (B \to C))$ 是公理。因此，执行子程序[2']：

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

8、程序已经全部进入[1]～[4]，并且已经执行完子程序[1']～[4']，因此程序终止。

这样我们就得到一个+ $((A \to B) \to C) \to (B \to C)$ 的公理证明。

证明1'''：

1 $((A \to B) \to C)) \to (B \to ((A \to B) \to C))$ $(Ax1)$
2 $(B \to ((A \to B) \to C)) \to ((B \to (A \to B)) \to (B \to C))$ $(Ax2)$
3 $((B \to ((A \to B) \to C)) \to ((B \to (A \to B)) \to (B \to C)))$
$\to (((A \to B) \to C) \to ((B \to ((A \to B) \to C))$
$\to ((B \to (A \to B)) \to (B \to C))))$ $(Ax1)$
4 $((A \to B) \to C) \to ((B \to ((A \to B) \to C))$
$\to ((B \to (A \to B)) \to (B \to C)))$ 2、3 MP
5 $(((A \to B) \to C) \to ((B \to ((A \to B) \to C)) \to ((B \to (A \to B)) \to (B \to C))))$
$\to ((((A \to B) \to C)) \to (B \to ((A \to B) \to C)))$
$\to (((A \to B) \to C) \to ((B \to (A \to B)) \to (B \to C))))$ $(Ax2)$

6 $(((A\to B)\to C))\to(B\to((A\to B)\to C)))$
$\to(((A\to B)\to C)\to((B\to(A\to B))\to(B\to C))))$ 4、5 MP

7 $((A\to B)\to C)\to((B\to(A\to B))\to(B\to C)))$ 1、6 MP

8 $(((A\to B)\to C)\to((B\to(A\to B))\to(B\to C))))$
$\to((((A\to B)\to C)\to(B\to(A\to B)))$
$\to(((A\to B)\to C)\to(B\to C)))$ $(Ax2)$

9 $(((A\to B)\to C)\to(B\to(A\to B)))$
$\to(((A\to B)\to C)\to(B\to C))$ 7、8 MP

10 $B\to(A\to B))$ $(Ax1)$

11 $(B\to(A\to B)))$
$\to(((A\to B)\to C)\to(B\to(A\to B)))$ $(Ax1)$

12 $((A\to B)\to C)\to(B\to(A\to B))$ 10、11 MP

13 $((A\to B)\to C)\to(B\to C)$ 9、12 MP

构造程序的[2]~[7]**也可以构成一个独立的公理证明构造程序，这是演绎定理的证明中显示出来的，但该程序很繁琐。程序**[1]**是一个简化程序，它的加入，可以使构造程序大为简化，尽管它多了一条程序命令。但是这样就增加了该程序的实际可操作性。**

参考文献：

[1] 宋文坚. 逻辑学[M]. 人民出版社,1998. P86-92.

[2] 陆钟万. 面向计算机科学的数理逻辑[M]. 科学出版社,2002. P86-92.

[3] 周礼全. 逻辑百科辞典[M]. 四川教育出版社,1994. P685.

[4] A.G.Hamilton. Logic for Mathematicians[M]. 清华大学出版社,2003. P32-34.

[5] 张清宇 郭世铭 李小五. 哲学逻辑研究[M]. 社会科学文献出版社,1997.

The Arithmetic Design for Theorem Proving in the Axiom System of Classical Propositional Logic

Du Guo-ping[1,2]

(1.Nanjing University. Nanjing 210093,China; 2.Nanjing University of Aeronautics and Astronautics, Nanjing 210016,China)

Abstract: The article uses the proving of deduction theorem to give general program of construction theorem proving, and adding a piece of simplification command. The program is gotten strict and exercisable.

Key words: deduction prove; axiom prove; program