

Natural Deduction & C/DNF

Wang-Zhou Dai

命题逻辑的推理

1. 通过重言等价性来化简逻辑公式，用真值表证明；
2. 利用公理化系统，如希尔伯特式推演系统 \mathcal{L}
 - 三条公理：
 - (a) L1: $\alpha \rightarrow (\beta \rightarrow \alpha)$
 - (b) L2: $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow ((\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \gamma))$
 - (c) L3: $(\neg\beta \rightarrow \neg\alpha) \rightarrow ((\neg\beta \rightarrow \alpha) \rightarrow \beta)$
 - 一条推理规则：分离规则 $\{\alpha, \alpha \rightarrow \beta\} \vdash \beta$
3. 本课程主要讲一种更符合直觉的“自然推演系统”（Gerhard Gentzen, 1909-1945）：
 - 在本课程的作业和考试中，我们都使用 Stanisław Jaśkowski (1906—1965) 提出的自然推演记法。

自然推演

例：用自然推演证明： $\vdash ((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma)$

证：

Jaśkowski style:

1.	$(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma)$	assumption
2.	$\alpha \rightarrow \beta$	$\wedge e_1$ I
3.	α	assumption
4.	β	$\rightarrow e$ 2,3
5.	$\beta \rightarrow \gamma$	$\wedge e_2$ I
6.	γ	$\rightarrow e$ 4,5
7.	$\alpha \rightarrow \gamma$	$\rightarrow i$ 3,6
8.	$((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma)$	$\rightarrow i$ 1,7

Q.E.D.

Gentzen style

证明公式的有穷集合 $\Gamma = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ ，即 $\alpha_1 \vee \alpha_2 \vee \dots \vee \alpha_n$ 。这里用 Γ, α 表示 $\Gamma \cup \{\alpha\}$ 。

公理：

$$\Gamma, A_i, \neg A_i$$

或规则 (\vee):

$$\frac{\Gamma, \alpha_i}{\Gamma, (\alpha_0 \vee \alpha_1)}, \quad i = 0, 1$$

或规则推论 (\vee'):

$$\frac{\Gamma, \alpha_0, \alpha_1}{\Gamma, (\alpha_0 \vee \alpha_1)}$$

与规则 (\wedge):

$$\frac{\Gamma, \alpha_0 \quad \Gamma, \alpha_1}{\Gamma, (\alpha_0 \wedge \alpha_1)}$$

切割规则 (cut):

$$\frac{\Gamma, \alpha \quad \Gamma, \neg \alpha}{\Gamma}$$

为方便书写更清晰的证明过程, 还可添加一个转写规则 (rw):

$$\frac{\{a, b, c\}}{\{a, b\}, c}$$

例子

例 1 的 Gentzen 证明树写法:

根据逻辑等价规则重写目标公式:

$$(\alpha \wedge \neg \beta) \vee (\beta \wedge \neg \gamma) \vee (\neg \alpha \vee \gamma)$$

开始构造第一个析取枝, 使用规则 (\wedge):

$$\frac{\{\beta, \gamma, \neg \alpha\}, \alpha \quad \{\beta, \gamma, \neg \alpha\}, \neg \beta}{\{\beta, \gamma, \neg \alpha\}, (\alpha \wedge \neg \beta)}$$

将结果转写 (rw):

$$\{\gamma, \neg \alpha, (\alpha \wedge \neg \beta)\}, \beta$$

继续构造第二个析取枝, 使用规则 (\wedge):

$$\frac{\{\gamma, \neg \alpha, (\alpha \wedge \neg \beta)\}, \beta \quad \{\gamma, \neg \alpha, (\alpha \wedge \neg \beta)\}, \neg \gamma}{\{\gamma, \neg \alpha, (\alpha \wedge \neg \beta)\}, \beta \wedge \neg \gamma}$$

继续构造第三个析取枝, 使用规则 (\vee'):

$$\frac{\{(\alpha \wedge \neg \beta), (\beta \wedge \neg \gamma)\}, \gamma, \neg \alpha}{\{(\alpha \wedge \neg \beta), (\beta \wedge \neg \gamma)\}, (\gamma \vee \neg \alpha)}$$

Gentzen style:

$$\frac{\frac{\frac{\{\beta, \gamma\}, \alpha, \neg \alpha}{\{\beta, \gamma, \neg \alpha\}, \alpha} (rw) \quad \frac{\{\neg \alpha, \gamma\}, \beta, \neg \beta}{\{\beta, \gamma, \neg \alpha\}, \neg \beta} (rw)}{\frac{\{\gamma, \neg \alpha, \beta\}, \alpha \wedge \neg \beta}{\{\gamma, \neg \alpha, \alpha \wedge \neg \beta\}, \beta} (rw)} (\wedge) \quad \frac{\{\neg \alpha, \alpha \wedge \neg \beta\}, \gamma, \neg \gamma}{\{\gamma, \neg \alpha, \alpha \wedge \neg \beta\}, \neg \gamma} (rw)}{\frac{\{\gamma, \neg \alpha, \alpha \wedge \neg \beta\}, \beta \wedge \neg \gamma}{\{\alpha \wedge \neg \beta, \beta \wedge \neg \gamma\}, \neg \alpha, \gamma} (rw)} (\wedge) \quad \frac{\{\alpha \wedge \neg \beta, \beta \wedge \neg \gamma\}, \neg \alpha, \gamma}{\{\alpha \wedge \neg \beta, \beta \wedge \neg \gamma\}, \neg \alpha \vee \gamma} (\vee')} {\frac{\{(\alpha \wedge \neg \beta) \vee (\beta \wedge \neg \gamma) \vee (\neg \alpha \vee \gamma)\}}{\{(\alpha \wedge \neg \beta) \vee (\beta \wedge \neg \gamma) \vee (\neg \alpha \vee \gamma)\}} (rw)}$$

Q.E.D.

命题逻辑公式的范式

CNF 存在性的构造性证明:

引理 1: 每个布尔函数都可以由某合式公式导出

- 布尔函数: $f: \{0, 1\}^n \mapsto \{0, 1\}$
- 公式 $A(p_1, \dots, p_n)$ 导出函数: $A(x_1, \dots, x_n)$

证明：只需令

$$A(p_1, \dots, p_n) = \bigvee \{p_1^{x_1} \wedge p_2^{x_2} \wedge \dots \wedge p_n^{x_n} \mid (x_1, \dots, x_n) \in f^{-1}(1)\},$$

其中，我们约定逻辑文字的表示形式：

$$p^{-1} \equiv \neg p, p^1 \equiv p$$

例子：设 3 元布尔函数 $f: \{0, 1\}^3 \mapsto \{0, 1\}$ ，有 $f^{-1}(1) = \{(0, 0, 1), (1, 0, 0), (1, 1, 0)\}$ ，那么可得目标公式：

$$(\neg p_1 \wedge \neg p_2 \wedge p_3) \vee (p_1 \wedge \neg p_2 \wedge \neg p_3) \vee (p_1 \wedge p_2 \wedge \neg p_3)$$

定理 1：每个合式公式都重言等价于一个析取范式和合取范式。

证明：不失一般性，记该公式为 ϕ ，分情况讨论：

1. 若 ϕ 为矛盾式，其等价于 $(p_1 \wedge \neg p_1)$ ；
2. 若 ϕ 为非矛盾式，则其可满足。以 f 记 ϕ 导出的布尔函数，那么 $f^{-1}(1) \neq \emptyset$ 。根据引理 1，存在公式 ψ 可以导出 f ；且 ψ 是析取范式，因此原命题第一部分（DNF）得证。

关于 CNF 的证明部分略去。

主（合）析取范式的唯一性

由存在性，以及极小项、极大项的唯一性易证。