Proof Theory

枫聆

2022 年 4 月 22 日

目录

Basic Logic

Satisfiability of Sets of Formulas

Definition 1 If v is a valuation, this is, a mapping from the atoms to the set $\{t, f\}$.

Definition 2 [4] Let Σ denote a set of well-formed formulas and t a valuation. Define

$$\Sigma^t = \begin{cases} T & \text{if for each } \beta \in \Sigma, \beta^t = T \\ F & \text{otherwise} \end{cases}$$

When $\Sigma^t = T$, we say that t satisfies Σ. A set Σ is satisfiable iff there is some valuation t such that $\Sigma^t = T$.

Definition 3 Let Σ be a set of formulas, and let α be a formula, we say that

1. α is a logical consequence of Σ, or
2. Σ (semantically) entails α, or
3. $\Sigma \models \alpha$,

if and only if for all truth valuations t, if $\Sigma^t = T$ then also $\alpha^t = T$. We write $\Sigma \not\models \alpha$ for there exists a truth valuation t such that $\Sigma^t = T$ and $\alpha^t = F$.

Annotation 4 For example, $\Sigma = \{p_1, p_2, \cdots, p_n\}$ could be a set of premises and let α could be the conclusion that we want to derive.

Natural Deduction

Remark 5 Natural deduction is a kind of proof calculus in which logical reasoning is expressed by inference rules closely related to the "natural" way of reasoning.

Judgments and Propositions

Definition 6 A *judgment* is somthing we may know, this is, an object of knowledge. A judgment is *evident* if we in fact know it.

Annotation 7 "A is false" (see classical logic), "A is true at time t" (see temporal logic), "A is necessarily true" or "A is possibly true" (see modal logic), "the program M has type " (see programming languages and type theory), "A is achievable from the available resources" (see linear logic).

Introduction and Elimination

Definition 8 Inference rules that introduce a logical connective is the conclusion are known as *introduction rules*. i.e., to conclude "A and B *true*" for propositions A and B, one requires evidence for "A *true*" and B *true*. As an inference rule:

$$\frac{A\ true \quad B\ true}{A \wedge B\ true}\ \wedge I$$

Here $\wedge I$ stands for "conjunction introduction".

Annotation 9 实际上面的 inference rule 的 general form 应该是

$$\frac{A\ prog \quad B\ prog \quad A\ true \quad B\ true}{A \wedge B\ true}\ \wedge I$$

这里才能帮助后面的 $\vDash$ make sense.

Definition 10 Inference rules that describe how to deconstruct information about a compound proposition into information about its consitiuents are elimination rules. i.e., from $A \wedge B$ *true*, we can conclude A *true* and B *true*:

$$\frac{A \wedge B\ true}{A\ true}\ \wedge E_L \qquad \frac{A \wedge B\ true}{B\ true}\ \wedge E_R$$

Annotation 11 The meaning of conjunction is determinded by its *verifications*.

Hypothetical Derivations

Definition 12 A *hypothetical judgment* is $J_1, \cdots, J_n \vdash J$, where judgments $J_1, \cdots, J_n$ are unproved assumptions, and the judgment J is the conclusion. A *hypothetical deduction*(derivation) for $J_1, \cdots, J_n \vdash J$ has the form

$$\begin{array}{c} J_1 \quad \cdots \quad J_n \\ \vdots \\ J \end{array}$$

which means J is derivable from $J_1, \cdots, J_n$.

Annotation 13 上面的 $J_1, \cdots, J_2$ 都可以替换成关于 J_i 的一个 hypothetical derivation.

Definition 14 In the natural deduction calculus, an assumption is discharged when the conclusion of an inference does not depend on it, although one of the premises of the inference does[1].

Annotation 15 Once the appropriate rules have been completed, these are known as discharged assumptions, and are not included in the pool of assumptions on which the conclusion of the rule depends[3].

Annotation 16 hypothetical derivation 要求最后的 conclusion 依赖的 poof of assumptions 不是空的.

Theorem 17 Deduction theorem

$$T, P \vdash Q \iff T \vdash P \to Q$$

.

Annotation 18 在 deduction theorem 中我们注意到第一个 hypothetical judgment 里面的 antecedent Q 被去掉了，在第二个 hypothetical judgment 的 succedent 里面作为一个 implication 的 antecedent 出现了，这里我们就可以说 assumption Q is discharged，即现在的 conclusion 已经不依赖它了. 那么我们是如何构造 deduction theorem 里面的 implication 的呢？下面接着看

Definition 19 (implication) If B is true under the assumption that A is true, formly written $A \supset B$. The corresponed introduction and elimination rule as follow

$$\dfrac{\dfrac{\overline{A\ true}^{\,u}}{\begin{array}{c}\vdots\\ B\ true\end{array}}}{A \supset B\ true} \supset I^u \qquad \dfrac{A \supset B \quad A\ true}{B\ true} \supset E$$

Annotation 20 Why indexed u In the introduction rule, the antecedent named u is discharged in the conclusion. This is a mechanism for delimiting the scope of the hypothesis: its sole reason for existence is to establish "$B\ true$"; it cannot be used for any other purpose, and in particular, it cannot be used below the introduction.

上面这段话出自 natural deduction 的 wiki，这个 $u$scope 了 assumption $A\ true$ 的开端，因为 $A \supset B$ 并不依赖 $A\ true$, 它描述只是 if $A\ true$ then $B\ true$. 同时最后的 introduction rule 会将这个 assumption $A\ true$ discharged 掉，表示 scope 在这里已经结束了. 而 implication rule 会将上述 derivation 直接总结得到一个结论，即

$$A \vdash B \Rightarrow \cdot \vdash A \to B.$$

Example 21 Considering the following proof of $A \supset (B \supset (A \wedge B))$

$$\dfrac{\dfrac{\dfrac{\overline{A\ true}^{\,u} \quad \overline{B\ true}^{\,w}}{A \wedge B\ true} \wedge I}{B \supset (A \wedge B)\ true} I^{w}}{A \supset (B \supset (A \wedge B))\ true} I^{u}.$$

这整个 derivation 不是 hypothetical 的，因为两个 assumptions $A\ true$ 和 $B\ true$ 都已经被 discharged，因此它实际上一个 complete proof!

Definition 22 (disjunction) The elimination rule for disjunction:

$$\dfrac{A \vee B\ true \quad \begin{matrix} \overline{A\ true}^{\,u} \\ \vdots \\ C\ true \end{matrix} \quad \begin{matrix} \overline{B\ true}^{\,w} \\ \vdots \\ C\ true \end{matrix}}{C\ true} \vee E^{u,w}$$

both assumption u, w are discharged at the disjunction elimination rule.

Definition 23 The falsehood elimination rule:

$$\dfrac{\perp\ true}{C\ true} \perp E$$

Annotation 24 falsehood elimination 的意义在哪? 首先你应该主要到一个特殊等价命题 $A \vee \perp = A$，从 $\vee$ 的 introduction rule 来看这意味 $\perp\ true \vdash A\ true$，由于 A 是任意的，因此我们得到了 $\perp\ true \vdash C\ true$.

Harmony

Definition 25 Local soundness shows that the elimination rules are not strong: no matter how we apply eliminations rules to the result of an introduction we cannot gain any new information.

Definition 26 Local completeness shows that the elimination rules are not weak: there is alwayws a way to apply elimination rules so that we can reconstitute a proof of the original proposition from the the results by apply intruduction ruls.

Annotation 27 local soundness 告诉你通过 elimination 压缩得到的东西不会比你已经知道的东西强 (not strong), 而 local completeness 告诉你合并通过 elimination 压缩得到的东西会得到全部你知道的信息.

Definition 28 Given two deduction of same judgment, we use the notion

$$\begin{array}{c}\mathcal{D}\\ A\ true\end{array} \Longrightarrow_R \begin{array}{c}\mathcal{D}'\\ A\ true\end{array}$$

for the local reduction of a deduction $\mathcal{D}$ to another deduction D' of same judgement $A\ true$. Simliarly, we have local expansion

$$\begin{array}{c}\mathcal{D}'\\ A\ true\end{array} \Longrightarrow_E \begin{array}{c}\mathcal{D}\\ A\ true\end{array}$$

Definition 29 (substitution Principle) If

$$\begin{array}{c}\overline{A\ true}\ u\\ \mathcal{E}\\ C\ true\end{array}$$

is a hypothetical proof of $\mathcal{C}\ true$ under the undischarged hypothesis $A\ true$ labelled u, and

$$\begin{array}{c}\mathcal{D}\\ A\ true\end{array}$$

is a proof of $A\ true$ then

$$\begin{array}{c}\dfrac{\mathcal{D}}{A\ true}\ u\\ \mathcal{E}\\ C\ true\end{array}$$

is our notation for substituting $\mathcal{D}$ for all uses of the hypothesis labelled u in $\mathcal{E}$. This deduction, also sometime written as $[\mathcal{D}/u]\mathcal{E}$ no longer depends on u.

Example 30 If given a elimination rule of disjunction as follow

$$\frac{A \vee B\ true}{A\ true}\ \vee E_L$$

The rule a little bit stronger, since we would not be able to reduce

$$\dfrac{\dfrac{B\ true}{A \vee B\ true}\ \vee I_R}{A\ true}\ \vee E_L$$

As u can see it's not local soundness.

Verifications and Uses

Definition 31 a verification should be a proof that only analyzes the consitituents of a proposition.

Annotation 32 natural deduction 实际上像 constructive logic 或者 intuitive logic, 不像 classic logic, 例如 Proposition $A \vee (A \supset B)$ 在 classic logic 就是正确的，因为我们 A 和 B 都需要给定是 true/false tag, 但是在 natural deduction 里面我们好像没有办法来处理. 更甚，如果我们要证明一个 B 是 accpeted in natural deduction, 你可能首先需要证明 $A \supset B$ 和 B 都是 accepted，就需要根据其结构 bottom-up 来做 derivation.

Definition 33 Writing $A\uparrow$ for the judgment "A has a verification". Naturally, this should mean that A is true, and that the evidence for that has a special form.

Definition 34 Writing $A\downarrow$ for the judgment "A may be used". $A\downarrow$ should be the case when either A *true* is a hypothesis, or A is deduced from a hypothesis via elimination rules.

Definition 35 For conjunction.

$$\frac{A\uparrow \quad B\uparrow}{A \wedge B\uparrow} \wedge I \qquad \frac{A \wedge B\downarrow}{A\downarrow} \wedge E_L \qquad \frac{A \wedge B\downarrow}{B\downarrow} \wedge E_R$$

Definition 36 For implication

$$\frac{\begin{array}{c}\overline{A\downarrow}^{\,u} \\ \vdots \\ B\uparrow\end{array}}{A \supset B\uparrow} \supset^u \qquad \frac{A \supset B\downarrow \quad A\uparrow}{B\downarrow} \supset E$$

implication introduction rule 里面的 $B\uparrow$ 表示没看懂，因为这里的 B 显然是来自 elimination 的结果. 为什么 implication elimination 里面需要 $A\uparrow$ 呢?

Example 37

$$\frac{\dfrac{\overline{A \wedge B\ true}^{\,u}}{A\ true} \wedge E_L}{(A \wedge B) \supset A\ true} \supset I^u$$

Definition 38 For disjunction

$$\frac{A\uparrow}{A \vee B\uparrow} \vee I_L \qquad \frac{B\uparrow}{A \vee B\uparrow} \vee I_R \qquad \frac{A \vee B\downarrow \quad \begin{array}{c}\overline{A\uparrow}^{\,u} \\ \vdots \\ C\uparrow\end{array} \quad \begin{array}{c}\overline{B\downarrow}^{\,w} \\ \vdots \\ C\uparrow\end{array}}{C\uparrow} \vee E^{u,w}$$

Definition 39 For truth and falsehood.

$$\frac{}{\top\uparrow}\ \top I \qquad \frac{\bot\downarrow}{C\uparrow}\ \bot E$$

Annotation 40 $\bot\downarrow$ signifies a contradiction from our hypotheses.

Definition 41 For atomic propositions.

$$\frac{P\downarrow}{P\uparrow}\ \downarrow\uparrow.$$

Annotation 42 对于 atomic props，我们只能对它赋予一个 property，没有关于它的 verification. 因此上述的规则是在进行一个转换，只要我们 assumption 了关于它的一个 property，就默认它已经被 verified.

Soundness and Completeness of Natural Deduction

Definition 43 [5]Soundness of natural deduction means that the conclusion of proof is always a logical consequence of the premises. That is

$$\text{If } \Sigma \vdash \alpha, \text{then } \Sigma \vDash \alpha.$$

Definition 44 Completeness of natural deduction means that all logical consequences in propositional logic are provable in natural deduction. That is,

$$\text{If } \Sigma \vDash \alpha, \text{then } \Sigma \vdash \alpha.$$

Annotation 45 其中 $\Sigma \vdash \alpha$，表示存在一个以 Σ 作为 premise 得到 conclusion 为 α 的 proof. 而 $\Sigma \vDash \alpha$，就考虑两端的 proposition 加上 truth-falsehood 了，即如 $\Sigma^t = True$ 则有 $\alpha^t = True$.

对于 soundness 的证明，我们需要根据 α 的结构来做归纳，而后再考虑赋予其 true/false 来考虑. 这里记录一下对于结构归纳它是怎样对应一般归纳法命题 $P(n)$ 结构上，这里的 n 应该对应 α 的 bottom-up derivation 里面的 maximum depth of line.

而对于 completeness 的证明，相对来说会复杂一点. 我们需要下面 3 个 lemma. 有一个疑问不引入 negation 是不是还说明不了 completeness?

Lemma 46 If $\Sigma \vDash \beta$, then

$$\emptyset \vDash (\alpha_0 \to (\alpha_1 \to (\cdots \to (\alpha_n \to \beta) \cdots)).$$

Lemma 47 For any well-form formula γ containing atoms $p_1, p_2, \cdots, p_n$ and any valuation t, we have

1. If $\gamma^t = True$ then $\widehat{p}_1, \widehat{p}_2, \cdots, \widehat{p}_n \vdash \gamma$;

2. If $\gamma^t = False$ then $\widehat{p}_1, \widehat{p}_2, \cdots, \widehat{p}_n \vdash \neg\gamma$;

where defines $\widehat{p}_i$ as follow

$$\widehat{p}_i = \begin{cases} p_i & \text{if } p_i^t = True \\ \neg p_i & \text{if } p_i^t = False \end{cases}$$

Example 48 若 $\gamma = p \to q$，我们可以构造一个真值表

p	q	$p \to q$	Claim
T	T	T	$p, q \vdash p \to q$
T	F	F	$p, \neg q \vdash \neg(p \to q)$
F	T	T	$\neg p, q \vdash p \to q$
F	F	T	$\neg p, \neg q \vdash p \to q$

那么上面的 claims 是怎么来的呢？我们可以来分别证明，对于第一行

$$\cfrac{\cfrac{\cfrac{}{p\ \mathit{true}}u \qquad q\ \mathit{true}}{q\ \mathit{true}}}{p \to q\ \mathit{true}}u$$

感觉有点奇怪，这里需要用到 vars inference rule，这里相对于对 $q \vdash p \to q$ 的 weaken premise. 对于第二行

$$\cfrac{\cfrac{\cfrac{\cfrac{}{p \to q\ \mathit{true}}u \qquad p\ \mathit{true}}{q} \qquad \neg q\ \mathit{true}}{\bot}}{\neg(p \to q)\ \mathit{true}}u$$

对于第三行

$$\cfrac{\cfrac{\cfrac{\cfrac{}{p\ \mathit{true}}u \qquad \neg p\ \mathit{true}}{\bot}}{q\ \mathit{true}}}{p \to q\ \mathit{true}}u$$

对于第四行，和第三行类似. 可以看的出来这个 lemma 非常深刻，只要将 atoms 调整为在当前 valuation 下都是 true 的命题，结论再对应调整，就可以构造一个对应的 proof.

Lemma 49 For any well-formed formula γ, if $\emptyset \vDash \gamma$, then $\emptyset \vdash \gamma$.

Annotation 50 Lemma 49一句话概况就是 tautologies are provable. 其证明过程可以用 Lemma 47来说明. 现在 γ 是一个 tautology，那么对于所有的 valuation 都有 $\gamma^t = \mathit{true}$，这有什么用呢？这里还需要引入另外一种 tautology $p \vee \neg p$，配合 emilination rule of vee，即

$$\cfrac{(p_1 \vee \neg p_1) \quad (p_2 \vee \neg p_2) \quad \cdots \quad (p_n \vee \neg p_n) \qquad \begin{array}{c} \cfrac{\overline{p_1} \quad \cdots \quad \overline{p_n}}{} \\ \vdots \\ \gamma \end{array} \qquad \cdots \qquad \begin{array}{c} \cfrac{\overline{\neg p_1} \quad \cdots \quad \overline{\neg p_n}}{} \\ \vdots \\ \gamma \end{array}}{\gamma}$$

这里需要考虑有 2^n 个 cases，每一个对应一种 valuation，又因为 γ 是 tautology，因此最后的 conclusion 也都是 γ.

Lemma 51 If $\emptyset \vdash (\alpha_0 \to (\alpha_1 \to (\cdots \to (\alpha_n \to \beta)\cdots))$, then $\{\alpha_0, \alpha_1, \cdots, \alpha_n\} \vdash \beta$, that is, $\Sigma \vdash \beta$.

Notational Definition

Definition 52 A notational definition gives the meaning of the general form of a proposition in terms of another proposition whose meaning has already been defined.

Example 53 We can define logical equivalence, written $A \equiv B$ as

$$(A \supset B) \wedge (B \supset A).$$

Example 54 We can define negation $\neg A$ as

$$\neg A = (A \supset \perp) \Longrightarrow \dfrac{\begin{matrix} A \\ \vdots \\ \perp \end{matrix}}{\neg A}\ \neg I$$

We also can give the introduction rule of falsehood.

$$\frac{\neg A \quad A}{\perp}\ \perp I$$

so $\perp$ actually means any contradictions. moreover double negation is coming.

Annotation 55 notaional definition 可以看做用已有的东西构造出一些东西. 与之对应的是我们可以直接符号化的给出某个新的定义，称之为 symbolic definition.

Derived Rules of Inference

Example 56

$$\frac{A \supset B \; true \quad B \supset C \; true}{A \supset C \; true}$$

is a derived rule of inference. Its derivation is the following:

$$\dfrac{\dfrac{B \supset C \; true \quad \dfrac{A \supset B \; true \quad \dfrac{}{A \; true}\, u}{B \; true} \supset E}{C \; true} \supset E}{A \supset C \; true} \supset I^u$$

Annotation 57 关于 derivation 的推导这里有一些 strategies 在里面

- 使用 introduction rule 从下至上，即我们想要什么;
- 使用 elimination rule 从上至下，即我们知道什么.

Example 58 Modus tollens(这玩意不就是逆否命题)

$$\frac{A \to B \quad \neg B}{\neg A} \; MT.$$

Curry-Howard Conrrespondence

Definition 59 Curry-Howard correspondence is between the natural deduction and simply-typed λ-calculus at three levels

- propositions are types;
- proofs are programs; and
- simplification of proofs is evaluation of programs.

That is

Types	Propositions
Unit types (1)	Truth ($\top$)
Product type ($\times$)	Conjunction ($\wedge$)
Union type ($+$)	Disjunction ($\vee$)
Function type ($\rightarrow$)	Implication ($\supset$)
Void types (0)	False ($\perp$)

Every typing rule has a correspondence with a deduction rule.

Example 60 The typing derivation of the term $\lambda a.\ \lambda b.\ \langle a, b\rangle$ can be seen as a deduction tree proving $A \supset B \supset A \wedge B$.

$$\dfrac{\dfrac{\dfrac{\dfrac{a : A \in \Gamma}{\Gamma \vdash a : A}\,var \quad \dfrac{b : B \in \Gamma}{\Gamma \vdash b : B}\,var}{\Gamma \vdash \langle a, b\rangle : A \times B}\,pair}{\Gamma \vdash \lambda y : B.\ \langle a, y\rangle : B \rightarrow A \times B}\,abs}{\Gamma \vdash \lambda x : A.\ \lambda y : B.\ \langle x, y\rangle : A \rightarrow B \rightarrow A \times B}\,abs \quad \Longleftrightarrow \quad \dfrac{\dfrac{\dfrac{\overline{A\ true}\,u \quad \overline{B\ true}\,w}{A \wedge B\ true}\,\wedge \wedge I}{B \supset A \wedge B\ true}\,\supset I^{w}}{A \supset B \supset A \wedge B\ true}\,\supset I^{u}$$

Annotation 61 从上面例子中看的出来，the inference rule of natural deduction 缺点什么，我也可以给原本每个 inference rule 都加上 the annotation for proof terms. [6] 那么这里 $M : A$ 有两种解释:

1. M is proof term for proposition A;
2. M is a program of type A.

这样解释 Curry-Howard ismorphism 或许方便一点. 让 proof terms make sense: 我们有"if $M : A$ then $A\ true$", 反过来"if $A\ true$ then $M : A$". 例如我们可以将 the proof term of $A \wedge B\ true$ 看做一个 pair 包含两个 subterm, 一个关于 $A\ true$ 和另一个关于 $B\ true$.

$$\frac{M : A \quad N : B}{\langle M, N\rangle : A \wedge B}\,\wedge I$$

那么 the elimination rule of conjunction 对应一个 natural projection.

$$\frac{M : A \wedge B}{\pi_1 M : A} \wedge E_L \quad \frac{M : A \wedge B}{\pi_2 M : B} \wedge E_R$$

Example 62 通过 Curry-Howard isomorphism 我们可以将我们想要证明的 judgment 转换到 type system 中，你会看到非常的便利! 例如

$$(A \supset (B \wedge C)) \supset (A \supset B) \wedge (A \supset C) \; true$$

等价于

$$\lambda x.\ \langle \lambda y.\ \pi_1(x\ y), \lambda y.\ \pi_2(x\ y) \rangle : (A \to B \times C) \to (A \to B) \times (A \to C)$$

一个 implication 被转换成了对应的 abstraction，此时我们肯定会想如果给一个 false proposition 是不是就转不了? 例如

$$(A \supset B) \supset (B \supset A)$$

显然我们无法在现有 type system 构造出一个合理的 abstraction 使得 $(A \to B) \to (B \to A)$.

迎面走来的问题是: 给定一个 proposition true, 是否有其他的 term with type 和它对应呢? 显然是有的，

$$\lambda z.\ \lambda x.\ \langle \lambda y.\ \pi_1(x\ y), \lambda y.\ \pi_2(x\ y) \rangle\ z'$$

那这是不是违反 Curry-Howard isomorphsim 了呢? 其实并不是，这里的对应是指 proof terms 和 deduction of proposition true, 显然 deduction 变了，对应的 proof terms 也要变.

参考文献

[1] John Slaney. The Logic Notes. http://users.cecs.anu.edu.au/~jks/LogicNotes/

[2] The relation between deduction theorem and discharged. https://math.stackexchange.com/questions/3527285/what-does-discharging-an-assumption-mean-in-natural-deduction

[3] Definition:Discharged Assumption. https://proofwiki.org/wiki/Definition:Discharged_Assumption

[4] Propositional Logic: Semantics. https://cs.uwaterloo.ca/~cbruni/CS245Resources/lectures/2018_Fall/05_Propositional_Logic_Semantics_Continued_post.pdf

[5] Propositional Logic: Soundness and Completeness for Natural Deduction. https://cs.uwaterloo.ca/~cbruni/CS245Resources/lectures/2018_Fall/09_Propositional_Logic_Natural_Deduction_Soundness_and_Completeness_post.pdf

[6] Lecture Notes on Proofs as Programs. http://www.cs.cmu.edu/~fp/courses/15816-s10/lectures/02-pap.pdf