Proof Theory

枫聆

2022 年 4 月 29 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.

Classic Propositional Modal Logic

Definition 5 [8]Let Σ be a set of propositional letters or atomic propositions. The set $F_P(\Sigma)$ of formulas of classical propositional modal logic is the smallest set with:

1. If $A \in \Sigma$ is a propositional letter, then $A \in F_P(\Sigma)$;
2. If $\phi, \psi \in F_P(\Sigma)$, then $\neg\phi, (\phi \wedge \psi), (\phi \vee \psi), (\phi \to \psi) \in F_P(\Sigma)$;
3. If $\phi \in F_P(\Sigma)$, then $(\Box\phi), (\Diamond\phi) \in F_P(\Sigma)$.

Definition 6 Let $\mathcal{S}$ be a system of modal logic, this is $F_P(\Sigma)$ with a set of axioms and rules. If axioms and rules as follow

$$\text{all propostional tautologies} \qquad \text{(P)}$$

$$\Box(\phi \to \psi) \to (\Box\phi \to \Box\psi) \qquad \text{(Kripke axiom)}$$

$$\Box\phi \to \phi \qquad \text{(T)}$$

$$\Box\phi \to \Box\Box\phi \qquad \text{(4)}$$

$$\frac{\phi \quad \phi \to \psi}{\psi} \qquad \text{(modus ponens)}$$

$$\frac{\phi}{\Box\phi} \qquad \text{(Gödel)}$$

We call it modal logic $\mathcal{S}4$.

Annotation 7 Kriple axiom 原本的形式应为

$$\Box\phi \wedge \Box(\phi \to \psi) \to \Box\psi$$

上面是它经常用的等价形式. Axiom T 是指若 ϕ is necessary, 那么 ϕ is true. Axiom 4 是指 ϕ is necessary, 那么命题"ϕ is necessary" is necessary, 有点别扭，举个形象的例子如果 box 是指某个人知道某件事，假设我知道 A *true*, 那么我肯定知道我知道 A *true*. 最后一个叫 Gödel translation, 它将 intuitionistic logic 里面的 formulas 转换到 modal logic 里面.

Definition 8 Let $\mathcal{S}$ be a system of modal logic. For a formula ψ and a set of formulas Φ, we write $\Phi \vdash_{\mathcal{S}} \psi$ and say that ψ can be derived from Φ(or is provable from Φ), iff there is a proof of ψ that uses only the formulas of Φ and the axioms and proof rules of $\mathcal{S}$. That is, we define $\Phi \vdash_{\mathcal{S}} \psi$ inductively as:

$$\Phi \vdash_{\mathcal{S}} \psi$$

iff $\psi \in \Phi$ or there is an instance

$$\frac{\phi_1 \quad \cdots \quad \phi_n}{\psi}$$

of a proof rule of $\mathcal{S}$ with conclusion ψ and some number $n \geq 0$ of premises such that for all $i = 1, 2, \cdots, n$, the premises ϕ_i is derivable, i.e:

$$\Phi \vdash_{\mathcal{S}} \phi_i$$

When the case $n = 0$ corresponds to axioms.

Annotation 9 现在以 $\Box$ 表示 provable 的视角来看待前面提到的 axioms. 首先是

$$\Box(\phi \to \psi) \to (\Box\phi \to \Box\psi) \quad \text{(Kripke axiom)}$$

若 $\phi \to \psi$ is provable 且 ϕ is provable, 那么则 ψ is provable.

$$\Box\phi \to \phi \quad \text{(T)}$$

若 ϕ is provable, 那么 ϕ should be true.

$$\Box\phi \to \Box\Box\phi \quad (4)$$

若 ϕ is provable, 那么 ϕ should be provably provable, 也就是我们肯定知道存在一个 proof.

$$\frac{\phi}{\Box\phi} \quad \text{(Gödel)}$$

若 ϕ is proven, 那么 ϕ should be provable.

Definition 10 A Kripke frame (W, ρ) consists of a non-empty set W and a relation $\rho \subseteq W \times W$ on worlds. The element of W are called possible worlds and ρ is called accessibility relation.

Definition 11 A Kripke structure $K = (W, \rho, v)$ consists of Kripke frame (W, ρ) and a mapping $v : W \to \Sigma \to \{true, false\}$ that assigns truth-values to all the propositional letters in all worlds.

Definition 12 Given a Kriple structure $K = (W, \rho, v)$, the interpretation $\vDash$ of modal formulas in worlds s is defined as

- $K, s \vDash A$ iff $v(s)(A) = true$;
- $K, s \vDash \phi \wedge \psi$ iff $K, s \vDash \phi$ and $K, s \vDash \psi$;
- $K, s \vDash \phi \vee \psi$ iff $K, s \vDash \phi$ or $K, s \vDash \psi$;
- $K, s \vDash \neg\phi$ iff it is not the case that $K, s \vDash \phi$;

- $K, s \models \Box\phi$ iff $K, t \models \phi$ for all worlds t with $s\rho t$;
- $K, s \models \Diamond\phi$ iff $K, t \models \phi$ for some worlds t with $s\rho t$.

Annotation 13 最后两个关于 modality $\Box$ 和 $\Diamond$ 定义是最重要的，它们借助 accessible possible world 来 make sense. 可以通过它们的 nesting 形式来描述更长的路径即 $\Box\Box, \Diamond\Diamond, \Box\Diamond$.

Definition 14 Given a Kripke structure $K = (W, \rho, v)$, formula ϕ is vaild in K, written $K \models \phi$, iff $K, s \models \phi$ for all worlds $s \in W$.

Definition 15 (local consequence) Let ψ be a formula and Φ a set of formulas. Then we write $\Phi \models_l \psi$ if and only if, for each Kripke structure $K = (W, \rho, v)$ and each world $s \in W$, we have $K, s \models \Phi$ implies $K, s \models \psi$.

Definition 16 (global consequence) Let ψ be a formula and Φ a set of formulas. Then we write $\Phi \models_g \psi$ if and only if, for each Kripke structure $K = (W, \rho, v)$, if for all world $s \in W : K, s \models \Phi$, then for all world $s \in W : K, s \models \psi$.

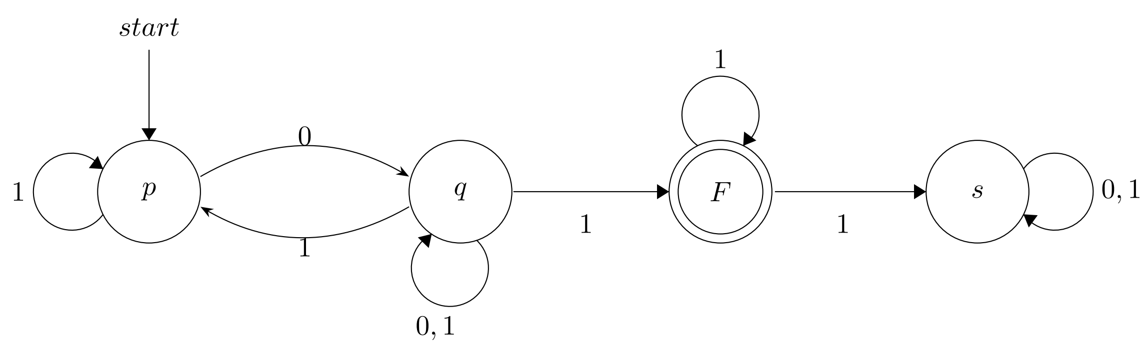
Annotation 17 local consequence 和 global consequence 的区别就是 assumption 是在某个 world 里面还是在所有的 worlds 里面.

Definition 18 A formula ϕ is vaild or a tautology, iff $\emptyset \models_l \phi$, which we write $\models \phi$. A set of formulas Φ is called satisifable, iff there is a Kripke structure K and a world s with $K, s \models \Phi$.

Lemma 19 (local deduction theorem) For formulas ϕ, ψ we have

$$\phi \models_l \psi \iff \models_l \phi \to \psi.$$

Annotation 20 (view of finite automata) 对于 Kripke frame 的第一反应应该是 finite automata, 但是对于一个给定的 finite automata 我们还需要一些额外的说明. 例如



每一个 state 里面存在一个 proposition，它表示这个 proposition is hold at this state，自然地 states 就变成了 possible worlds. state 现在可以接受多个输入 $\{0,1\}$，那么这里就表示我们有两个 relations ρ_0 和 ρ_1，对应我们需要两个 pair 来构建不同的 modality $(\Box_0, \Diamond_0)$ 和 $(\Box_1, \Diamond_1)$，它们都是用于描述某个 state 的 successor. 因此这里可以对应上一个 Kripke structure, 对上图我们可以列举几个 vaild formula.

$$
\begin{aligned}
&K \vDash \neg\Diamond_0 F && \text{does not end with 0}\\
&K \vDash p \to \Diamond_0 p && p \text{ has a 1-loop}\\
&K \vDash \Diamond_0\ true && \text{never stuck with input 0}\\
&K \vDash \Diamond_1\ true && \text{never stuck with input 1}
\end{aligned}
$$

再看一个稍微复杂一点

$$K \vDash F \to \Diamond_0(\neg\Diamond_0 F \wedge \neg\Diamond_1 F)$$

它意思如果某个状态 σ 下 F is hold, 那么 σ accept 0 的 successors $\{s_i\}$ 中每个 s_i 的 successors 都无法 hold F, 显然这是成立的.

Definition 21 A system $\mathcal{S}$ of proof rules and axioms of modal logic is sound iff, for all formulas ψ and all sets of formulas Φ:

$$\Phi \vdash_S \psi \text{ implies } \Phi \vDash_g \psi$$

Annotation 22 上述 soundness 实际在建立关于 axiomatic modal logic 和 semantic modal logic 之间的一座桥，这座桥需要每一个 axiom make sense.

Lemma 23 Kripke axiom $\Box(\phi \to \psi) \to (\Box\phi \to \Box\psi)$ is sound.

Proof 首先给定任意一个 Kripke structure K. 我们需要证明

$$K, s \vDash \Box(\phi \to \psi) \to (\Box\phi \to \Box\psi).$$

因此假设其前提

$$
\begin{aligned}
&K, s \vDash \Box(\phi \to \psi)\\
&K, s \vDash \Box\phi
\end{aligned}
$$

那么对应所有满足 $s\rho t$ 的 successor t, 都有

$$
\begin{aligned}
&K, t \vDash \phi \to \psi\\
&K, t \vDash \phi
\end{aligned}
$$

自然地这里有 $K, t \vDash \psi$，于是 $K, s \vDash \Diamond\psi$. Q. E. D.

Lemma 24 Gödel Rule $\dfrac{\phi}{\Box\phi}$ is sound.

Lemma 25 A Kripke frame (W, ρ) is reflexive, that ρ is reflexive, if and only if $K, s \vDash \Box q \to q$ for all Kripke structures $K = (W, \rho, v)$.

Proof (⇒) 若 (W, ρ) is reflexive, 这是显然的.

(⇐) 若 $K, s \vDash \Box q \to q$ for all Kripke structures $K = (W, \rho, v)$. 假设存在一个 r such that $(r, r) \notin \rho$, 构造一个比较巧妙地 valuation v

$$v(s)(q) = \begin{cases} true & \text{if } r\rho s \\ false & \text{otherwise} \end{cases}$$

那么显然有 $K, r \vDash \Box q$，根据前提这里有 $K, r \vDash q$，而根据 valuation 这里就 r 存在一个 successor 是它自己，即 (r, r) 与假设矛盾. Q. E. D.

Lemma 26 A Kriple frame (W, ρ) is transitive, that ρ is transitive, if and only if $K, s \vDash \Box q \to \Box\Box q$ for all Kripke structures $K = (W, \rho, v)$.

Proof (⇒) 若 (W, ρ) is transitive, 给定 $K, s \vDash \Box q$，对于 s 的任意一个 successor $t(s\rho t)$ 则有 $K, t \vDash p$，进一步对 t 的任意一个 successor $r(t\rho r)$，考虑 transitive $s\rho r$，那么有 $K, r \vDash p$. 由于 t 和 r 的任意性，因此 $K, s \vDash \Box\Box p$.

(⇐) 若 Kriple frame 满足对任意的 valuation v 都有 $K, s \vDash \Box q \to \Box\Box q$. 假设 (W, ρ) 不是 transitive，那么存在 $r_1, r_2, r_3 \in W$ such that $r_1 \rho r_2, r_2 \rho r_3$ and $(r_1, r_3) \notin \rho$. 构造一个 valuation v

$$v(s)(q) = \begin{cases} true & \text{if } r_0\rho s \\ false & \text{otherwise} \end{cases}$$

那么 $K, r_0 \vDash \Box q$，但是因为 $(r_0, r_3) \notin \rho$，因此 $K, r_0 \nvDash \Box\Box q$，和假设前提矛盾了. Q. E. D.

Annotation 27 这座需要两边的支撑一样高，给定特定 axiomatic modal logic, 我们得到找到与之对应的 semantic modal logic，我们的手法就是 sketch it from basic Kripke frame. 当我们尝试构造了一部分之后，我们需要让其 make sense，上述 lemma 利用 formula 来 characterize 是一个不错的选择.

Definition 28 (characterization)Let C be a class of Kripke frames and ϕ a formula in modal logic. Formula ϕ characterizes C, if for every Kripke frame (W, ρ):

$$(W, \rho) \in C \text{ iff for each } v : K, s \vDash \phi \text{ holds for } K = (W, \rho, v).$$

Theorem 29 (soundness of $\mathcal{S}4$)The Kriple proof rules for $\mathcal{S}4$ are sound for the class of reflexive and transitive frames.

Theorem 30 The conjunction of the following two multimodal formulas

$$\Box_a p \to (p \land \Box_a \Box_b p)$$
$$\Box_a(p \to \Box_b p) \to (p \to \Box_a p)$$

characterizest the class of all multimodal kripke frames (W, ρ_a, ρ_b) such that ρ_a is the reflxive, transitive closure of ρ_b.

Proof (⇐) 如果 $(W, \rho_a, \rho_b)$is Kripke frame where ρ_a is the reflexive, transitive closure of ρ_b. 对于一个 formula 只要注意到 $\Box_a\Box_a p \to \Box_a\Box_b p$ 即可，可以从需要考虑的 successors 数量来证明. 对于第二个 formula，我有点不太确定，因为 $p \to \Box_b p$ 和 $p \to \Box_a p$ 在 K 里面都是 vaild. Q. E. D.

Natural Deduction

Remark 31 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 32 A *judgment* is somthing we may know, this is, an object of knowledge. A judgment is *evident* if we in fact know it.

Annotation 33 "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 34 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 35 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 36 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 37 The meaning of conjunction is determinded by its *verifications*.

Hypothetical Derivations

Definition 38 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

$$\begin{array}{ccc} J_1 & \cdots & J_n \\ & \vdots & \\ & J & \end{array}$$

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

Annotation 39 上面的 $J_1, \cdots, J_2$ 都可以替换成关于 J_i 的一个 hypothetical derivation.

Definition 40 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 41 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 42 hypothetical derivation 要求最后的 conclusion 依赖的 poof of assumptions 不是空的.

Theorem 43 Deduction theorem

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

.

Annotation 44 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 45 (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

$$\dfrac{\dfrac{}{A\ true}\,u \atop {\vdots \atop B\ true}}{A \supset B\ true} \supset I^u \qquad \dfrac{A \supset B \quad A\ true}{B\ true} \supset E$$

Annotation 46 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 47 Considering the following proof of $A \supset (B \supset (A \wedge B))$

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

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 48 (disjunction) The elimination rule for disjunction:

$$\cfrac{A \vee B\ true \quad \begin{array}{c}\overline{A\ true}^{\,u} \\ \vdots \\ C\ true\end{array} \quad \begin{array}{c}\overline{B\ true}^{\,w} \\ \vdots \\ C\ true\end{array}}{C\ true} \vee E^{u,w}$$

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

Definition 49 The falsehood elimination rule:

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

Annotation 50 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 51 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 52 Local completeness shows that the elimination rules are not weak: there is always 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 53 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 54 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 55 (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 56 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 57 a verification should be a proof that only analyzes the consitituents of a proposition.

Annotation 58 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 59 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 60 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.

Annotation 61 上述两个 definitions 里面隐藏着非常重要但有点不正式的结论:If A has a vertification then A true, 反之依然. 后面我们将形式化地证明它们.

Definition 62 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 63 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 64

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

Definition 65 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 66 For truth and falsehood.

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

Annotation 67 $\perp\downarrow$ signifies a contradiction from our hypotheses.

Definition 68 For atomic propositions.

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

Annotation 69 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 assume 了关于它的一个 property，就默认它已经被 verified.

Soundness and Completeness of Natural Deduction

Definition 70 [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 71 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 72 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 73 If $\Sigma = \{\alpha_0, \alpha_1, \cdots, \cdots, \alpha_n\}$ and $\Sigma \vDash \beta$, then

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

Annotation 74 Deduction theorem 体现的淋漓尽致，将 β 完美转换成了一个 tautology.

Lemma 75 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 76 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

$$\dfrac{\dfrac{\overline{p\ true}^{\,u} \quad q\ true}{q\ true}}{p \to q\ true}\,u$$

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

$$\dfrac{\dfrac{\dfrac{\overline{p \to q\ true}^{\,u} \quad p\ true}{q} \quad \neg q\ true}{\bot}}{\neg(p \to q)\ true}\,u$$

对于第三行

$$\dfrac{\dfrac{\dfrac{\overline{p\ true}^{\,u} \quad \neg p\ true}{\bot}}{q\ true}}{p \to q\ true}\,u$$

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

Annotation 78 Lemma 77一句话概况就是 tautologies are provable. 其证明过程可以用 Lemma 75来说明. 现在 γ 是一个 tautology，那么对于所有的 valuation 都有 $\gamma^t = true$，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

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

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 79 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 80 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 81 We can define logical equivalence, written $A \equiv B$ as

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

Example 82 We can define negation $\neg A$ as

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

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 83 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 84

$$\frac{A \supset B\ \mathit{true} \qquad B \supset C\ \mathit{true}}{A \supset C\ \mathit{true}}$$

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

$$\dfrac{\dfrac{B \supset C\ \mathit{true} \qquad \dfrac{A \supset B\ \mathit{true} \qquad \dfrac{}{A\ \mathit{true}}\,u}{B\ \mathit{true}}\supset E}{C\ \mathit{true}}\supset E}{A \supset C\ \mathit{true}}\supset I^u$$

Annotation 85 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 86 Modus tollens(这玩意不就是逆否命题)

$$\frac{A \to B \qquad \neg B}{\neg A}\ MT.$$

Curry-Howard Conrrespondence

Definition 87 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 ($\bot$)

Every typing rule has a correspondence with a deduction rule.

Example 88 The typing derivation of the term $\lambda a.\ \lambda b.\ \langle a, b\rangle$ can be seen as a deduction tree proving $A \supset B \supset A \wedge B$.

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

Annotation 89 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 $B\ true$.

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

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 90 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.

More Delicate

Validity

Definition 91 A *valid* if $\bullet \vdash A$ *true* where $\bullet$ is emphasizing that there are no truth hypotheses(different from $\cdot$ that represents empty collection of hypotheses), and we call $\bullet \vdash A$ *true* is categorical judgement. Written ΔA for reflecting the notion of validity as a proposition.

Annotation 92 其中 $\Box A$ 表示一个 proposition claimed A is vaild, 因此 $\Box A$ *true* 表示这个 proposition 成立. 那么关于它的 introduction rule 是什么？很自然地由 A *valid* 的 definition 有

$$\frac{\bullet \vdash A\ \mathit{true}}{\Gamma \vdash \Box A\ \mathit{true}}\ \Box I$$

那么它的 elimination rule 又是什么呢？第一次尝试

$$\frac{\Gamma \vdash \Box A\ \mathit{true}}{\bullet \vdash A\ \mathit{true}}\ \Box E$$

看起来是 local soundness，通过它得到的 infos 还行. 但是实际上有问题

$$\frac{\overline{\Box A\ \mathit{true} \vdash \Box A\ \mathit{true}}}{\bullet \vdash A\ \mathit{true}}\ \Box E$$

这等于我们可以 no assumption 推出所有 proposition 都是 valid，因此这个 elimination rule 有点太强了. 那么我们考虑让它弱一点，第二次尝试

$$\frac{\Gamma \vdash \Box A\ \mathit{true}}{\Gamma \vdash A\ \mathit{true}}\ \Box E$$

这里确实是 local soundness，但却不是 local completeness

$$\cfrac{\cfrac{\Gamma \vdash \Box A\ \mathit{true}}{\Gamma \vdash A\ \mathit{true}}\ \Box E}{\Gamma \vdash \Box A\ \mathit{true}}\ ?$$

我们得改变一下思路，如果 A *vaild*，那么其他 premise 包含 A *vaild* 的 judgement 那么实际上都是可以去掉 A *vaild*，但也仅仅局限以此，这才是 emilination 故事的主线.

Definition 93 Then general judgement form

$$\underbrace{u_1 :: B_1\ \mathit{vaild}, \cdots, u_k :: B_k\ \mathit{vaild}}_{\Delta}; \underbrace{x_1 : A_1\ \mathit{true}, \cdots, x_n : A_n\ \mathit{true}}_{\Gamma} \vdash C\ \mathit{true}$$

Definition 94 The introduction rule and elimination rule of A *vaild* as follow

$$\frac{\Delta;\bullet\vdash A\ true}{\Delta;\Gamma\vdash\Box A\ true}\Box I\qquad\frac{\Delta;\Gamma\vdash\Box A\ true\quad\Delta,u::A\ vaild;\Gamma\vdash C\ true}{\Delta;\Gamma\vdash C\ true}\Box E$$

Theorem 95 Local soundness and local completeness of above introduction and elimination rule are held

Annotation 96 可以看到 emilination rule 变成了 substitution，而不是从单纯从本身要得到什么，后面会看见更多这样的东西.

Example 97 Proof of $\cdot;\cdot\vdash\Box A\supset A$.

$$\cfrac{\cfrac{\cfrac{}{\cdot;x:\Box A\ true\vdash\Box A\ true}x\quad\cfrac{}{u::A\ vaild;x:\Box A\ true\vdash A\ true}u}{\cdot;x:\Box A\ true}\Box E^u}{\cdot;\cdot\vdash(\Box A\supset A)\ true}\supset I^x$$

Box is Powerful

Definition 98 $\Box$ is $\Box$.

Definition 99 A term box$M$ means M is a quated source expression such that there are not any free variables x.

Definition 100 And $\Box A$ is necessity modality.

Possibility

Definition 101 We use $\Diamond A$ for possibility modality.

Annotation 102 $\Diamond A$ 就是一个 claim A is possible 的命题. 通常在 classic modal logic 里面我们定义 A is possible if its negation is not necessary, that is $\Diamond A = \neg\Box\neg A$. 但是这种手法在现在我们讨论的 intuitionistic logic 无法奏效，我们希望的是有一个直观的 introduction rule 来得到它，也就是我们需要一些 explicit evidences，一开始就它的 negation 那显然是做不到的.

Definition 103 [7]The definition of possiblity.

$$\frac{\Delta, \Gamma \vdash A\ true}{\Delta, \Gamma \vdash A\ poss}\ poss$$

Definition 104 The introduction and emilination rule of possiblity.

$$\frac{\Delta; \Gamma \vdash A\ poss}{\Delta; \Gamma \vdash \Diamond A\ true}\ \Diamond I \qquad \frac{\Delta; \Gamma \vdash \Diamond A\ true \quad \Delta; x : A\ true \vdash C\ poss}{\Delta; \Gamma \vdash C\ poss}\ \Diamond E$$

Annotation 105 注意这里的 emilination rule 里面的第二个 premise 中的 hypothesis 只有 $A\ true$，即我们 under assumption $A\ true$, we conclude $C\ poss$.

Theorem 106 Local soundness and completeness are held.

Annotation 107 td; 对上述 inference rule 的理解.

Example 108 Proof of $\Box(A \supset B) \supset \Diamond A \supset \Diamond B$.

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-natu

[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

[7] Computational Interpretations of Modalities
http://www.cs.cmu.edu/~fp/courses/15816-s10/lectures/04-compmodal.pdf

[8] Classic Modal Logic
http://www.cs.cmu.edu/~fp/courses/15816-s10/lectures/05-pml.pdf