Proof Theory

枫聆

2022 年 5 月 4 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

$$\text{all propostional tautologies} \tag{P}$$

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

$$\Box\phi \to \phi \tag{T}$$

$$\Box\phi \to \Box\Box\phi \tag{4}$$

$$\frac{\phi \quad \phi \to \psi}{\psi} \tag{modus ponens}$$

$$\frac{\phi}{\Box\phi} \tag{Gödel}$$

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 $K, s \vDash \phi$;

- $K, s \vDash \Box\phi$ iff $K, t \vDash \phi$ for all worlds t with $s\rho t$;
- $K, s \vDash \Diamond\phi$ iff $K, t \vDash \phi$ 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 $K \vDash \phi$, iff $K, s \vDash \phi$ for all worlds $s \in W$.

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

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

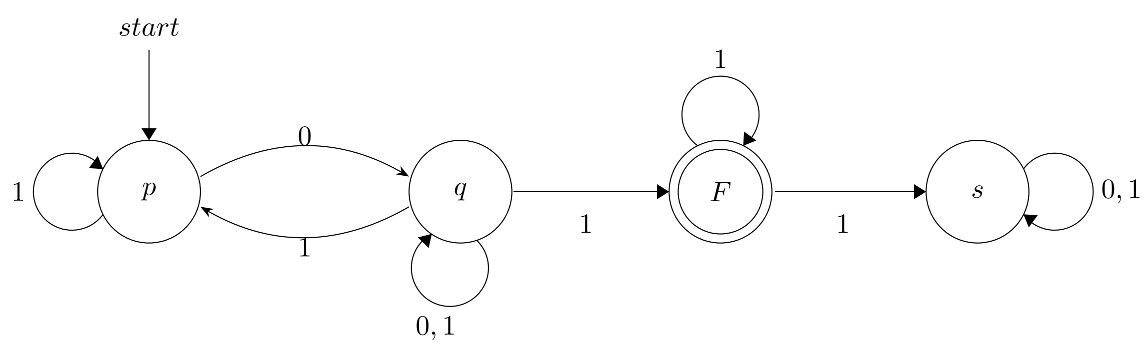
Annotation 17 local consequence 和 global consequence 的区别就是 assumption 是在某个 world 里面还是在所有的 worlds 里面.

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

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

$$\phi \vDash_l \psi \iff \vDash_l \phi \to \psi.$$

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.

Proof 注意这里的结论是建立在 global assumption 上的，即 $K, s \vDash \phi$ for any $s \in W$，证明过程是显然的. Q. E. D.

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

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

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, 先给一个思考图

$$\begin{tikzcd}
 & & w_i \arrow[r, "b:w_i\rho_b w_{i+1}"] & w_{i+1} \arrow[dr, dashed, "b*"] & \\
s \arrow[r, "s\rho_b^* t"] \arrow[urr, bend left, "s\rho_b^* w_i"] & t : p \to \Box_b p \text{ and } p \arrow[ur, dashed, "b*"] \arrow[rrr, "t\rho_b^* r"] & & & r
\end{tikzcd}$$

这里 $\rho_a = \rho_b^*$. 这里证明手法是

$$\Box_a (p \to \Box_b p) \to \Box_a (p \to \Box_a p) \text{ and } \Box_a (p \to \Box_a p) \to (p \to \Box_a p)$$

最重要是证明第一个 implication，第二个 implication 是前面已经证明过的 reflexive. 对于第一个 implication 它描述的是首先给出前提 $(1)\Box_a (p \to \Box_b p)$ 即 $s\rho_b^* t$. 然后我们想要将 t 中 $p \to \Box p$ 扩展至 $p \to \Box_b^* p$，因此再给一个假设前提 t holds p，我们来考察 $\Box_b^* p$ 是否成立即 $t\rho_b^* r$. 这里我们需要分解 $t\rho_b^* r$ 使其为 $w_i \rho_b w_{i+1}$ for all $i < n$，其中 $w_0 = t$ 和 $w_n = r$. 利用数学归纳法证明 $K, w_i \vdash p$，这里就不详细描述了，和后面一个证明过程类似，但是说明几点: $(1) s\rho_b^* w_i$ 送来了 $p \to \Box_b p$ (2) 假设前提保证了 $K, w_i \vDash p$. 因此 $K, w_{i+1} \vDash p$.

(⇒) 如果 $(W, \rho_a, \rho_b)$is Kripke frame such that above formulas are vaild in it for any valuation v. 我们得证明 $\rho_a = \rho_b^*$. 这种证明两个集合相等的手法，还是用两边证.

先证$\rho_a \subseteq \rho_b^*$. 取任意的 $(s, t) \in \rho_a$，我们得证明 $(s, t) \in \rho_b^*$. 还是构造一个特殊的 valuation

$$v(w)(q) = \begin{cases} true & \text{if } (s, w) \in \rho_b^* \\ false & \text{otherwise} \end{cases}$$

我们的思路是首先证明第二个 formula 的前提 (1) $\Box_a (p \to \Box_b p)$，从而得到对应的 conclusion (2) $(p \to \Box_a p)$，由给定的 v 结合 ρ_b^* 的 reflexive 性质，自然地有 $K, s \vDash p$，在使用一下 (2) 得到 $K, t \vDash p$, 这样就有 $(s, t) \in \rho_b^*$. 证明 (1) 思路是依然是假设前提: 给定 $s\rho_a w$ 且 $K, w \vDash p$，实际上 $(s, w) \in \rho_b^*$. 考虑下面的思考过程

$$\begin{tikzcd}
s \arrow[r, "a:s\rho_b^* w"] \arrow[rr, bend left, "s\rho_b^* w'"] & w : p \arrow[r, "b:w\rho_b^* w'"] & w'
\end{tikzcd}$$

另外又给了一个 w' 满足 $w\rho_b w'$，再根据 ρ_b^* 的 transitive 得到 $s\rho_b^* w'$，从而 $K, w' \vDash p$.

再证$\rho_a \supseteq \rho_b^*$. 取任意的 $(s,t) \in \rho_b^*$，我们要证明 $(s,t) \in \rho_a$. 依然构造一个类似的 valuation

$$v(w)(q) = \begin{cases} true & \text{if } (s,w) \in \rho_a \\ false & \text{otherwise} \end{cases}$$

我们的思路: 由于我们构造地特别的 v 有 $K, s \vDash \Box_a p$, 借助命题中的第一个 formula 得到对应的 conclusion (1) $K, s \vDash p \wedge \Box_a \Box_b p$. 考虑下面的思考过程

$$\begin{tikzcd}
 & w_i : p \arrow[r, "b:w_i\rho_b w_{i+1}"] & w_{i+1} : p \arrow[dr, dashed, bend left] & \\
s : p \arrow[ur, dashed, bend left] \arrow[rrr, "s\rho_b^* t"] & & & t : p
\end{tikzcd}$$

我们考虑将 $s\rho_b^* t$ 拆开，设 $w_i \rho_b w_{i+1}$ for all $i < n$，其中 $w_0 = s$ 和 $w_n = t$，这是可以做到的，考虑 closure 的构造过程. 再用一下数学归纳法证明 $K, w_i \vDash p$，在 $i = 0$ 显然是成立的，假设 w_i 成立，那么根据 v 即有 $s\rho_a w_i$，再利用一下 (1) 可以得到 $K, w_i \vDash \Box_b p$，因此 $K, w_{i+1} \vDash p$. 最终 $K, t \vDash p$，那么 $(s,t) \in \rho_a$. Q. E. D.

Annotation 31 回顾上面的证明手法，我们如果想要刻画两个 possible worlds 是否存在某种关系，例如 $(r,t) \overset{?}{\in} \rho$，我们可以额外借助一个 formula p 和 valuation v，仅使得所有 w 满足 $r\rho w$ 都 hold p. 这样如果我们能利用额外和 p 相关的条件间接证明 t holds p, 那么就可以证明 $s \to t$. 我们应该意识到 relations 是 Kripke frame 固有的性质，与 valuation 无关因此这里我们可以任意的定义它.

Natural Deduction

Remark 32 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 33 A *judgment* is somthing we may know, this is, an object of knowledge. A judgment is *evident* if we in fact know it.

Annotation 34 "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 35 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 36 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 $\models$ make sense.

Definition 37 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 38 The meaning of conjunction is determinded by its *verifications*.

Hypothetical Derivations

Definition 39 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 40 上面的 $J_1, \cdots, J_2$ 都可以替换成关于 J_i 的一个 hypothetical derivation.

Definition 41 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 42 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 43 hypothetical derivation 要求最后的 conclusion 依赖的 poof of assumptions 不是空的.

Theorem 44 Deduction theorem

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

.

Annotation 45 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 46 (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

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

Annotation 47 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 48 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 49 (disjunction) The elimination rule for disjunction:

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

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

Definition 50 The falsehood elimination rule:

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

Annotation 51 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 52 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 53 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 54 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 55 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 56 (substitution Principle) If

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

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 57 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 58 a verification should be a proof that only analyzes the consitituents of a proposition.

Annotation 59 [9] 在 natural deduction 中由于 local reduction 的存在，可能会让一个证明过程变得非常的冗余，例如在证明 conjunction commutativity

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{A \wedge B\ true}^{\,u}}{A\ true}\wedge E_1 \quad \dfrac{\overline{A \wedge B\ true}^{\,u}}{B\ true}\wedge E_2}{A \wedge B\ true}\wedge I}{B\ true}\wedge E_2 \quad \dfrac{\overline{A \wedge B\ true}^{\,u}}{A\ true}\wedge E_1}{\dfrac{B \wedge A\ true}{(A \wedge B) \supset (B \wedge A)\ true}\supset I^u}\wedge I$$

其中左上角的 local reduction 显然是冗余的. 这样对于谈论某个具体 proposition 的 proof 时就会出现问题, 因为 the shape of proof is not decidable. 同时我们也希望未来能够设计出一个 tool 用于 deviates proofs automatically, 也就是 search proof automatically. 因此从 natural deduction 上诞生了一个新的 calculus，它会在 syntax level 上来施加一些限制，借此限制 the shape of proof. 最后我们将证明这个 calculus 引入的 restrictions 不会产生 side-effect.

Definition 60 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 61 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 62 我觉得下述两种理解方式更为明确易懂

- $A \uparrow$ denotes that we are searching for a verfication of A;
- $A \downarrow$ denotes that we are allowed to use A.

Annotation 63 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 64 For conjunction.

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

Definition 65 For implication

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

Annotation 66 (why implication) In order to have a verification of $A \supset B$, we need a proof of B and we are given an assumption A to work with. Therefore, we will need a verification of B and we are allowed to use A.

When using an implication statement in a proof, we need to show that the antecedent holds, so we need a verification of it. Only then we are allowed to use the consequent.

Example 67

$$\dfrac{\dfrac{(A \supset A) \supset B\ ? \quad \dfrac{\dfrac{A\ ?}{A\ ?}}{A \supset A\ ?}}{B\ ?}}{((A \supset A) \supset B) \supset B \uparrow}$$

Example 68

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

那么它对应上 verification 和 use

$$\dfrac{\dfrac{A \wedge B \downarrow}{A \downarrow}\wedge E_L}{(A \wedge B) \supset A\ ?}\supset I^u$$

一切都非常奇怪，这个 verification 和 use 到底是怎样对应 truth？从前面两个例子都可以清晰地感觉到一个阻力，即

$$\begin{array}{c} A \downarrow \\ ??? \\ A \uparrow \end{array}$$

就是当我们在 use A 的时候，实际上存在一个 A has a verification.

Definition 69 For disjunction

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

Definition 70 For truth and falsehood.

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

Annotation 71 $\bot\downarrow$ signifies a contradiction from our hypotheses.

Annotation 72 the elimination rule of disjunction and falsehood 里面出现 conclusion $C \uparrow$ 也很奇怪，为什么不是 $C \downarrow$?

Definition 73 For atomic propositions.

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

Annotation 74 当引入上述的 arrow switch 之后我们可以回答前面的种种问题了. 首先是 example 67，假设其中的 A, B 都是 atomic proposition，则

$$\cfrac{\cfrac{}{(A\supset A)\supset B\ \downarrow}\,w \qquad \cfrac{\cfrac{\cfrac{}{A\ \downarrow}\,u}{A\ \uparrow}\downarrow\uparrow}{A\supset A\ \uparrow}\supset I^u}{\cfrac{\cfrac{B\ \downarrow}{B\uparrow}\downarrow\uparrow}{((A\supset A)\supset B)\supset B\uparrow}\supset I^w}$$

同时如果将 implication emilination 的 premise 换成 $A\downarrow$，在找 $A\supset A\downarrow$ 的 proof 时就被卡住了. example 68类似. 那么有一个很自然的问题这个 arrow switch 能不能推广到任意的 propositions 上呢？本质上是没有问题的，例如

$$\cfrac{A\supset A\downarrow \qquad \cfrac{\cfrac{}{A\ \downarrow}\,u}{A\uparrow}\downarrow\uparrow}{\cfrac{\cfrac{A\downarrow}{A\uparrow}\downarrow\uparrow}{A\supset A\uparrow}\supset I^u}$$

但是这样的语法又会使得 proof search space 变大，并不符合我们的初衷，因此我们只将 arrow switch 放在的了 atomic proposition 上，这样做的后果你也可以看到，需要将 connectives 都展开.

再来思考另外一种 arrow switch

$$\frac{F\downarrow}{F\uparrow}\uparrow\downarrow$$

这个人在本质上也是没有问题的，当我们有一个关于 F 的 verification，我们当然可以 use it. 但是引入它同样会造成我们的 proof search space，就像 classical logic 中的 tautologies，我们可以在任何 proof 中使用它，但是有时候是没有意义的. 同在 emilinotation rule of disjunction and falsehood 中的 conclusion 中我们都是使用的 verification，而不是 use，也是为了防止后续使得我们的 proof 变得复杂.

Theorem 75 (Global Soundness) If $A\uparrow$ and $\begin{array}{c}A\downarrow\\ \vdots\\ C\uparrow\end{array}$ then $C\uparrow$

Annotation 76 Global Soundness 意味着如果 if the verification formula of C under the verification formula A，那么在 C 中使用 A，并不会得到任何其他 new informations.

Theorem 77 (Global Completeness) If $A\downarrow$, then $A\uparrow$.

Annotation 78 Global completeness 意味着如果我们确定 formula A 在某种情况下可以使用，那么在相同的 assumptions 下我们可以推导出一个关于它的 verification. 这在前面关于 $\downarrow\uparrow$ 转换规则的 annotation 中已经见识过一个特殊例子了.

Notational Definition

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

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

Example 81 We can define negation $\neg A$ as

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

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 82 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.

Soundness and Completeness of Native Natural Deduction

Definition 83 [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 84 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 85 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 86 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 87 Deduction theorem 体现的淋漓尽致，将 β 完美转换成了一个 tautology.

Lemma 88 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 89 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

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

对于第三行

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

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

Annotation 91 Lemma 90一句话概况就是 tautologies are provable. 其证明过程可以用 Lemma 88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

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

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 92 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, $\Sigma \vdash \beta$.

Derived Rules of Inference

Example 93

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

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 94 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 95 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 96 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 ($\to$)	Implication ($\supset$)
Void types (0)	False ($\perp$)

Every typing rule has a correspondence with a deduction rule.

Example 97 The typing derivation of the term $\lambda a.\ \lambda b.\ \langle a, b\rangle$ can be seen as a deduction tree proving $A \supset B \supset A \wedge B$.

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

Annotation 98 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 99 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

Natural Deduction in Sequent Nation

Definition 100 A sequent is a pariticular form of hypothetical judgement

$$A_1, \cdots, A_n \vdash C.$$

where $A_1, \cdots, A_n$ and C are well-defined formulas.

Definition 101 The correspondence between natural deduction and natural deduction in sequent nation.

$\dfrac{A\ true \quad B\ true}{A \wedge B\ true} \wedge I$	$\dfrac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge I$
$\dfrac{A \wedge B\ true}{A\ true} \wedge E_1 \quad \dfrac{A \wedge B\ true}{B\ true} \wedge E_2$	$\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge E_1 \quad \dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge E_2$
$\dfrac{A\ true}{A \vee B\ true} \vee I_1 \quad \dfrac{B\ true}{A \vee B\ true} \vee I_2$	$\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee I_1 \quad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee I_2$
$\dfrac{A \vee B\ true \quad \begin{matrix}\overline{A\ true}^{\,u} \\ \vdots \\ C\ true\end{matrix} \quad \begin{matrix}\overline{B\ true}^{\,w} \\ \vdots \\ C\ true\end{matrix}}{C\ true} \vee E^{u,w}$	$\dfrac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C} \vee E$
$\dfrac{\begin{matrix}\overline{A\ true}^{\,u} \\ \vdots \\ B\ true\end{matrix}}{A \supset B\ true} \supset I^u$	$\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B} \supset I$
$\dfrac{A \supset B\ true \quad A\ true}{B\ true} \supset E$	$\dfrac{\Gamma \vdash A \supset B \quad \Gamma \vdash A}{\Gamma \vdash B} \supset E$
$\dfrac{}{\top\ true} \top I$	$\dfrac{}{\Gamma \vdash \top} \top I$
$\dfrac{\perp\ true}{C\ true} \perp E$	$\dfrac{\Gamma \vdash \perp}{\Gamma \vdash C} \perp E$
Hypothesis discharging	$\dfrac{}{\Gamma, A \vdash A}\ hyp$
Substitution	$\dfrac{\Gamma, A \vdash C \quad \Gamma \vdash A}{\Gamma \vdash C}\ subst$

Annotation 102 (detail of correspondence) 其中 Γ 是一个 set of formulas，它可以是 empty set. 思考上述 sequent 形式下的 natural deduction，我们应该用 bottom-up 的视角来观察. 试想我们在没有 additional assumptions 证明一个 formulas，在最开始 Γ 应该是 empty 的，随着我们不断 apply 上述规则过程中将不断的填充 Γ. 那么什么时候证明算接结束了呢？在 natural deduction 中我们从下往上使用 introduction rules，并添加相应的 assumptions，再从上往下使用 emilination rules，直到它们在中途相遇，这时候我们的证明就结束了，当证明结束的时候，此时所有的 assumptions 都应该被 discharge 了，这个操作对应到 sequent 形式下就是上述 hyp rule，在利用 sequent 构造 proof 的时候，总是以 hyp rule 结束的.

显然 sequent 提供了一种收集 assumptions 的方式，使得 assumptions 和需要证明的 formula 总是在一个 level，一旦某个 assumption 建立之后，以此往后的证明过程中这个 assumption 都是 visible 的.

Example 103 A proof in sequent form.

$$\dfrac{\dfrac{\dfrac{}{A \supset B, (A \wedge C) \vdash A \supset B}\,hyp \quad \dfrac{\dfrac{}{A \supset B, (A \wedge C) \vdash A \wedge C}\,hyp}{A \supset B, (A \wedge C) \vdash A}\,\wedge E_1}{A \supset B, (A \wedge C) \vdash B}\,\supset E \quad \dfrac{\dfrac{}{A \supset B, (A \wedge C) \vdash A \wedge C}\,hyp}{A \supset B, (A \wedge C) \vdash C}\,\wedge E_2}{\dfrac{A \supset B, (A \wedge C) \vdash (B \wedge C)}{\dfrac{A \supset B \vdash (A \wedge C) \supset (B \wedge C)}{\vdash (A \supset B) \supset ((A \wedge C) \supset (B \wedge C))}\,\supset I}\,\supset I}\,\wedge I$$

Definition 104 We say a rule is admissible if all proofs using the rule can be transformed into proofs that do not use the rule.

Lemma 105 The *subst* rule is admissible.

PROOF 我们可以将其替换为等价的形式

$$\dfrac{\Gamma, A \vdash C \quad \Gamma \vdash A}{\Gamma \vdash C}\,subst \quad \rightsquigarrow \quad \dfrac{\dfrac{\Gamma, A \vdash C}{\Gamma \vdash A \supset C}\,\supset I \quad \Gamma \vdash A}{\Gamma \vdash C}\,\supset E$$

Sequent Calculus

Definition 106 A sequent is a pariticular form of hypothetical judgement

$$A_1\ left, \cdots, A_n\ left \vdash C\ right.$$

where $A\ left$ corresponds to a proposition that can be used ($A \downarrow$) and $C\ right$ corresponds to a proposition we have to verify ($C \uparrow$). The right rules decompose C in analogy with introduction rules from the perspective of "bottom-up", while the left rule decompose one of the hypotheses, in analogy with elimination rules, but "upside-down".

Definition 107 引入上述 sequent 及其 inferences 是为了正式地说明 proof search, 即从 conclusion 到 premises 的 derivations.

Definition 108 The initial rule

$$\frac{}{\Gamma, P\ left \vdash P\ right}\ init$$

where P is atomic proposition.

Definition 109 The left rules and right rules

$\dfrac{\Gamma, A \wedge B\ left, A\ left \vdash C\ right}{\Gamma, A \wedge B\ left \vdash C\ right}\ \wedge L_1$ $\dfrac{\Gamma, A \wedge B\ left, B\ left \vdash C\ right}{\Gamma, A \wedge B\ left \vdash C\ right}\ \wedge L_2$	$\dfrac{\Gamma \vdash A\ right \quad \Gamma \vdash B\ right}{\Gamma \vdash A \wedge B\ right}\ \wedge R$
$\dfrac{\Gamma, A \supset B\ left \vdash A\ right \quad \Gamma, A \supset B\ left, B\ left \vdash C\ right}{\Gamma, A \supset B\ left \vdash C\ right}\ \supset L$	$\dfrac{\Gamma, A\ left \vdash B\ right}{\Gamma \vdash A\ left \supset B\ right}\ \supset R$
$\dfrac{\Gamma, A \vee B\ left, A\ left \vdash C\ right \quad \Gamma, A \vee B\ left, B\ left \vdash C\ right}{\Gamma, A \vee B\ left \vdash C\ right}\ \vee L$	$\dfrac{A\ right}{\Gamma \vdash A \vee B\ right}\ \vee R_1$ $\dfrac{B\ right}{\Gamma \vdash A \vee B\ right}\ \vee R_2$
	$\dfrac{}{\Gamma \vdash \top\ right}\ \top R$
$\dfrac{\Gamma, \perp\ left}{C\ right}\ \perp L$	

Annotation 110 The above rules we can use $\Gamma \Rightarrow A$ instead of them.

Annotation 111 这里 frank 给出的 left rules 怪怪的，因为 conclusion 里面的 assumptions 依然出现在了 primises 里面，这让人很奇怪，虽然不影响其正确性. frank 对此的意见是这只是一种 weakening 操作，同时他想表达一个”monotonicity of hypotheses” 的概念: 在 bottom-up 形式下的 proof 中一旦建立某个 assumption，那么它在后续的构造过程中同样 available.

我的感觉是 left rules 应该和 right rules 一样，right rules 在 simplify conclusion，而 left rules 也应该去 simplify hypotheses. 这里 simplify 是指去掉 formula 里面存在的 connectives.

Example 112 The proof in sequent calculus.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \supset B, (A \wedge C), A \Rightarrow A}\,init}{A \supset B, (A \wedge C) \Rightarrow A}\,\wedge L_1 \qquad \dfrac{}{A \supset B, (A \wedge C), B \Rightarrow B}\,init}{A \supset B, (A \wedge C) \Rightarrow B}\,\supset L \qquad \dfrac{\dfrac{}{A \supset B, (A \wedge C), C \Rightarrow C}\,init}{A \supset B, (A \wedge C) \Rightarrow C}\,\wedge L_2}{\dfrac{A \supset B, (A \wedge C) \Rightarrow (B \wedge C)}{\dfrac{A \supset B \Rightarrow (A \wedge C) \supset (B \wedge C)}{\Rightarrow (A \supset B) \supset ((A \wedge C) \supset (B \wedge C))}\,\supset R}\,\supset R}\,\wedge R$$

Theorem 113 (from verifications to sequent calculus) Given hypotheses $\Gamma = (A_1 \uparrow, \cdots, A_n \uparrow)$, it correpsonds to $\widehat{\Gamma} = (A_1\ left, \cdots, A_n\ left)$. Then we have

1. If $\Gamma \vdash C \uparrow$ then $\widehat{\Gamma} \vdash C\ right$;
2. If $\Gamma \vdash A \downarrow$ and $\widehat{\Gamma}, A\ left \vdash C\ right$ then $\widehat{\Gamma} \vdash C\ right$.

Proof 这里需要对 $\Gamma \vdash C \uparrow$ 和 $\Gamma \vdash A \downarrow$ 做 mutual induction. 记录几个 representative cases.

Case 1 若

$$\frac{\Gamma, C_1 \downarrow \vdash C_2 \uparrow}{\Gamma \vdash C_1 \supset C_2 \uparrow} \supset I$$

则

(1)	$\widehat{\Gamma}, C_1\ left \vdash C_2\ right$	hyp.1 from premise1
(2)	$\widehat{\Gamma} \vdash C_1 \supset C_2\ right$	$\supset R$. (1)

Case 2 若

$$\frac{\Gamma \vdash P \downarrow}{\Gamma \vdash P \uparrow} \downarrow\uparrow$$

则

(1)	$\widehat{\Gamma}, P\ left \vdash P\ right$	*init*
(2)	$\widehat{\Gamma} \vdash P\ right$	hyp.2 from premise1

Case 3 若

$$\frac{\Gamma \vdash A_1 \supset A_2 \downarrow \quad \Gamma \vdash A_1 \uparrow}{\Gamma \vdash A_2 \downarrow} \supset E$$

则

(1)	$\widehat{\Gamma}, A_2\ left \vdash C\ right$	assumption
(2)	$\widehat{\Gamma}, A_1 \supset A_2\ left, A_2\ left \vdash C\ right$	weakening(1)
(3)	$\widehat{\Gamma} \vdash A_2\ right$	hyp.1 from premise1
(4)	$\widehat{\Gamma}, A_1 \supset A_2\ left \vdash A_2\ right$	weakening(3)
(5)	$\widehat{\Gamma}, A_1 \supset A_2\ left \vdash C\ right$	$\supset L(2)(4)$
(6)	$\widehat{\Gamma} \vdash C\ right$	hyp.1 from premise2

Case 4 若

$$\frac{}{\Gamma', A \downarrow \vdash A \downarrow} hyp$$

则

(1)	$\widehat{\Gamma}, A\ left, A\ left \vdash C\ right$	assumption
(2)	$\widehat{\Gamma}, A\ left \vdash C\ right$	contraction(1)

Theorem 114 (substitution of uses) If $\Gamma \vdash A \downarrow$. Then

1. if $\Gamma, A \downarrow \vdash B \downarrow$ then $\Gamma \vdash B \downarrow$, and
2. if $\Gamma, A \downarrow \vdash C \uparrow$ then $\Gamma \vdash C \uparrow$,

Proof 这里需要对 $\Gamma, A \downarrow \vdash B \downarrow$ 和 $\Gamma, A \downarrow \vdash C \uparrow$ 做 mutual induction. 还是列举几个代表性的 cases.

Case 1 Base case

$$\frac{}{\top \uparrow} \top I$$

根据假设 $A \downarrow \vdash \top \uparrow$，这里显然有 $\vdash \top \uparrow$.

Case 2 若

$$\frac{\Gamma' \vdash C \supset B \downarrow \quad \Gamma' \vdash C \uparrow}{\Gamma' \vdash B \downarrow} \supset E$$

其中 $\Gamma' = (\Gamma, A \downarrow)$. 那么

(1)	$\Gamma \vdash A \downarrow$	assumption
(2)	$\Gamma \vdash C \supset B \downarrow$	hyp.1
(3)	$\Gamma \vdash C \uparrow$	hyp.2
(4)	$\Gamma \vdash B \downarrow$	$\supset E(3)(4)$

Theorem 115 (from sequent calculus to verifications) If $\widehat{\Gamma} \vdash C\ right$ then $\Gamma \vdash C \downarrow$.

Definition 116 (another of substitution) The rule of cut

$$\frac{\Gamma \vdash A\ right \quad \Gamma, A\ left \vdash C\ right}{\Gamma \vdash C\ right}\ cut$$

Annotation 117 注意 *cut* rule 是在用 the vertification of A 去替换 the use of A，这和前面 substitution of uses 是不太一样的.

Theorem 118 (admissibility of cut) If $\Gamma \vdash A\ right$ and $\Gamma, A\ left \vdash C\ right$ then $\Gamma \vdash C\ right$.

Definition 119 (generalization of *init* rule) The rule of identity

$$\frac{}{\Gamma, A\ left \vdash A\ right}\ id$$

Theorem 120 (admissibility of identity) $\Gamma, A\ left \vdash A\ right$ fir arbitrary propositions A and contexts Γ.

Theorem 121 (truth and verification) $A\ true$ iff $A \uparrow$.

Validity

Definition 122 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 123 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

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

那么它的 elimination rule 又是什么呢？第一次尝试

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

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

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

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

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

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

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

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 124 Then general judgement form

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

Definition 125 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 126 Local soundness and local completeness of above introduction and elimination rule are held

Annotation 127 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 128 Proof of $\cdot;\cdot \vdash \Box A \supset A$.

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

Box is Powerful

Definition 129 $\Box$ is $\Box$.

Definition 130 A term box$M$ means M is a quated source expression such that there are not any free variables x.

Definition 131 And $\Box A$ is necessity modality.

Possibility

Definition 132 We use $\Diamond A$ for possibility modality.

Annotation 133 $\Diamond A$ 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 134 [7]The definition of possiblity.

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

Definition 135 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 136 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 137 Local soundness and completeness are held.

Annotation 138 td; 对上述 inference rule 的理解.

Example 139 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

[9] Verifications and uses
https://web2.qatar.cmu.edu/cs/15317/lectures/06-verifications.pdf