

Midterm Exam on **Nov. 27th.** (Week 8)

Curry-Howard Correspondence

Intuitionistic Logic

Let us consider the following proposition and proof.

Proposition. There is an irrational a such that a^b is rational for an irrational b .

Proof. Let us consider a number $\sqrt{2}^{\sqrt{2}}$. If $\sqrt{2}^{\sqrt{2}}$ is irrational, then take $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$.

If $\sqrt{2}^{\sqrt{2}}$ is rational, then take $a = \sqrt{2}$ and $b = \sqrt{2}$.

This proof is correct in the *classical* logic, but does not exactly give us those a and b . In other words, the proof is *not constructive*. In contrast, we can prove the proposition by taking $a = \sqrt{2}$ and $b = 2 \log 3$ (in this case $a^b = 3$). This proof is *constructive* in the sense that we have constructed this concrete pair of a and b .

The *intuitionistic logic*, very roughly speaking, is a (sort of) logic that allows only constructive proofs: $P \vee Q$ has a proof only when we have a proof of P or a proof of Q ., and $\exists x.P(x)$ has a proof only when we find a concrete a such that $P(a)$ holds. This is quite different from the classical logic, in which we can prove $P \vee \neg P$ without proving P or $\neg P$. Notice that we used the fact that $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational in the above proof.

Minimal (Propositional) Logic

Here, the set of propositional formulas is defined as follows.

$$A ::= P \mid A_1 \Rightarrow A_2 \mid A_1 \wedge A_2 \mid A_1 \vee A_2$$

Sometimes, we consider a special propositional letter \perp .

We will give a set of deduction rules for the minimal logic, a negation-free fragment of intuitionistic propositional logic, in the natural deduction style. The judgment $\Delta \vdash A$ explicitly includes the assumptions as Δ : which is read that under a set Δ of assumptions A holds.

$$\begin{array}{c} \frac{A \in \Delta}{\Delta \vdash A} \text{Ax} \quad \frac{\Delta \cup \{A_1\} \vdash A_2}{\Delta \vdash A_1 \Rightarrow A_2} \Rightarrow\text{-I} \quad \frac{\Delta \vdash A_1 \Rightarrow A_2 \quad \Delta \vdash A_1}{\Delta \vdash A_2} \Rightarrow\text{-E} \\ \\ \frac{\Delta \vdash A_1 \quad \Delta \vdash A_2}{\Delta \vdash A_1 \wedge A_2} \wedge\text{-I} \quad \frac{\Delta \vdash A_1 \wedge A_2}{\Delta \vdash A_1} \wedge\text{-E}_1 \quad \frac{\Delta \vdash A_1 \wedge A_2}{\Delta \vdash A_2} \wedge\text{-E}_2 \\ \\ \frac{\Delta \vdash A_1}{\Delta \vdash A_1 \vee A_2} \vee\text{-I}_1 \quad \frac{\Delta \vdash A_2}{\Delta \vdash A_1 \vee A_2} \vee\text{-I}_2 \quad \frac{\Delta \vdash A_1 \vee A_2 \quad \Delta \cup \{A_1\} \vdash A' \quad \Delta \cup \{A_2\} \vdash A'}{\Delta \vdash A'} \vee\text{-E} \end{array}$$

We say that A is *provable* under assumptions Δ if $\Delta \vdash A$ is derivable (i.e., there is a derivation tree whose root concludes $\Delta \vdash A$), and especially when $\Delta = \emptyset$, we just say that A is *provable*. Some examples of deducible formula are $((P \Rightarrow Q) \wedge P) \Rightarrow Q$ and $(P \wedge Q) \Rightarrow (Q \wedge P)$. A derivation tree in a proof system is sometimes called a *proof tree*.

Exercise. Write proof trees for $((P \Rightarrow Q) \wedge P) \Rightarrow Q$ and $(P \wedge Q) \Rightarrow (Q \wedge P)$. □

Exercise. Write a proof tree for $((P \Rightarrow Q) \Rightarrow P) \wedge (P \Rightarrow (P \Rightarrow Q)) \Rightarrow Q$. □

Adding the following rule, we will obtain a proof system of the *intuitionistic propositional logic*.

$$\frac{\Delta \vdash \perp}{\Delta \vdash A} \perp\text{-E}$$

The rule is sometimes called *ex falso quodlibet* (“from falsehood, anything”). Then, negation $\neg A$ is given as a shorthand for $A \Rightarrow \perp$. Check that $\Delta \vdash A$ and $\Delta \vdash A \Rightarrow \perp$ implies $\Delta \vdash \perp$, and $\Delta, A \vdash \perp$ implies $\Delta \vdash A \Rightarrow \perp$.

Adding *either* one of the following rules to the proof system of the intuitionistic propositional logic, we will obtain a proof system for the *classical propositional logic*.

$$\frac{\Delta \vdash (A \Rightarrow \perp) \Rightarrow \perp}{\Delta \vdash A} \text{DNE} \quad \frac{}{\Delta \vdash A \vee (A \Rightarrow \perp)} \text{EM} \quad \frac{\Delta \cup \{A \Rightarrow \perp\} \vdash \perp}{\Delta \vdash A} \text{PBC}$$

The system is known to be sound and complete; i.e., A is provable if and only if A is a tautology. Also, it is known that A is provable in the classical logic if and only if $\neg\neg A$ is provable in the intuitionistic logic.

Exercise. Write a proof tree of $((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$ in the classical propositional logic.

Curry-Howard Correspondence

We define the function $\phi(-)$ from types to propositional formulas as follows.

$$\begin{aligned} \phi(P) &= P && (P \text{ is a base type}) \\ \phi(\tau_1 \rightarrow \tau_2) &= \phi(\tau_1) \Rightarrow \phi(\tau_2) \\ \phi(\tau_1 \times \tau_2) &= \phi(\tau_1) \wedge \phi(\tau_2) \\ \phi(\tau_1 + \tau_2) &= \phi(\tau_1) \vee \phi(\tau_2) \end{aligned}$$

Clearly, $\phi(-)$ is a bijection. Also, we define the function $\text{erase}(-)$ as follows.

$$\text{erase}(\Gamma) = \{\phi(\tau) \mid (x, \tau) \in \Gamma\}$$

Then, we have a following theorem.

Theorem (Curry-Howard Correspondence).

- For any Γ, M and τ , $\Gamma \vdash M : \tau$ implies $\text{erase}(\Gamma) \vdash \phi(\tau)$.
- For any Δ and A , there exist Γ and M such that $\Delta \vdash A$ implies $\Gamma \vdash M : \phi^{-1}(A)$, and $\Delta = \text{erase}(\Gamma)$.

We do not show the complete proof (that can be done by induction on the derivations), but show intuition underlying the proof by writing corresponding typing/deduction rules side by side, as follows.

$$\begin{array}{c}
\frac{(x, \tau) \in \Gamma}{\Gamma \vdash x : \tau} \text{T-VAR} \qquad \frac{A \in \Delta}{\Delta \vdash A} \text{AX} \\
\frac{\Gamma \uplus \{x \mapsto \tau_1\} \vdash M : \tau_2}{\Gamma \vdash \lambda x.M : \tau_1 \rightarrow \tau_2} \text{T-ABS} \qquad \frac{\Delta \cup \{A_1\} \vdash A_2}{\Delta \vdash A_1 \rightarrow A_2} \Rightarrow\text{-I} \\
\frac{\Gamma \vdash M : \tau_1 \rightarrow \tau_2 \quad \Gamma \vdash N : \tau_1}{\Gamma \vdash M N : \tau_2} \text{T-APP} \qquad \frac{\Delta \vdash A_1 \Rightarrow A_2 \quad \Delta \vdash A_1}{\Delta \vdash A_2} \Rightarrow\text{-E} \\
\frac{\Gamma \vdash M : \tau_1 \quad \Gamma \vdash N : \tau_2}{\Gamma \vdash (M, N) : \tau_1 \times \tau_2} \text{T-PAIR} \qquad \frac{\Delta \vdash A_1 \quad \Delta \vdash A_2}{\Delta \vdash A_1 \wedge A_2} \wedge\text{-I} \\
\frac{\Gamma \vdash M : \tau_1 \times \tau_2}{\Gamma \vdash \pi_1 M : \tau_1} \text{T-FST} \qquad \frac{\Delta \vdash A_1 \wedge A_2}{\Delta \vdash A_1} \wedge\text{-E}_1 \\
\frac{\Gamma \vdash M : \tau_1 \times \tau_2}{\Gamma \vdash \pi_2 M : \tau_2} \text{T-SND} \qquad \frac{\Delta \vdash A_1 \wedge A_2}{\Delta \vdash A_2} \wedge\text{-E}_2 \\
\frac{\Gamma \vdash M : \tau_1}{\Gamma \vdash \text{lnL } M : \tau_1 + \tau_2} \text{T-LEFT} \qquad \frac{\Delta \vdash A_1}{\Delta \vdash A_1 \vee A_2} \vee\text{-I}_1 \\
\frac{\Gamma \vdash M : \tau_2}{\Gamma \vdash \text{lnR } M : \tau_1 + \tau_2} \text{T-RIGHT} \qquad \frac{\Delta \vdash A_2}{\Delta \vdash A_1 \vee A_2} \vee\text{-I}_2 \\
\frac{\Gamma \vdash M : \tau_1 + \tau_2 \quad \Gamma \uplus \{x \mapsto \tau_1\} \vdash N_1 : \tau' \quad \Gamma \uplus \{y \mapsto \tau_2\} \vdash N_2 : \tau'}{\Gamma \vdash \text{case } M \text{ of } (x.N_1) (y.N_2) : \tau'} \text{T-CASE} \qquad \frac{\Delta \vdash A_1 \vee A_2 \quad \Delta \cup \{A_1\} \vdash A' \quad \Delta \cup \{A_2\} \vdash A'}{\Delta \vdash A'} \vee\text{-E}
\end{array}$$

In this sense, a λ -term represents a proof in the minimal logic. Such a term representing a proof is sometimes called a *proof term*.

Exercise. Give λ -terms of the types $((P \rightarrow Q) \times P) \rightarrow Q$ and $(P \times Q) \rightarrow (Q \times P)$, where P and Q are some base types. Show their typing derivations. \square

Exercise. Give a λ -term of the type $((P \rightarrow Q) \rightarrow P) \wedge (P \rightarrow (P \rightarrow Q)) \rightarrow Q$, where P and Q are some base types. Show its typing derivation. \square

Exercise. Give a λ -term of the type $((P + (P \rightarrow R)) \rightarrow R) \rightarrow R$, where P and R are some types. Show its typing derivation. \square

Consistency via Curry-Howard

Definition (Consistency). We call a proof system *consistent* if \perp is not provable in the system. \square

Theorem. The minimal logic is consistent.

Proof. Suppose that $\emptyset \vdash \perp$. Then, by Curry-Howard correspondence, we have a term M such that $\emptyset \vdash M : \perp$. (That is, the simply-typed λ -calculus is a model of the minimal logic.) By the subject

reduction property and strong normalization, we have a value V such that $\emptyset \vdash V : \perp$. Then, we perform case analysis of the form of V to show that V cannot have type \perp for each case.

If V has the form of $\lambda x.V'$ for some V' . Its type must have the form of $\tau_1 \rightarrow \tau_2$, which cannot be \perp . Similar discussions apply to the cases $V = (V_1, V_2)$, $V = \text{InL } V'$, and $V = \text{InR } V'$. Then, we consider the case where $V = W$ for a neutral term W . However, it is easy to show that $\text{FV}(W) \neq \emptyset$ and W cannot have any type under the empty type environment. \square

In the proof, subject reduction and strong normalization play very important roles in showing consistency. Generally speaking, these two properties are important in a proof calculus based on Curry-Howard correspondence, such as the calculus of construction and the Martin-Löf type theory. Both are (quite big) extension of the simply-typed λ -calculus, and underlie proof assistants Coq and Agda, respectively.

FYI: Simply-Typed λ -Calculus for Intuitionistic Propositional Logic with Negation

We add following construct to the simply-typed λ -calculus with pairs and sums.

$$M, N ::= \dots \mid \text{error } M$$

Accordingly, we add \perp to the set of types. Its reduction rules are given by:

$$\frac{}{(\text{error } M) N \longrightarrow \text{error } M} \quad \frac{}{\pi_i (\text{error } M) \longrightarrow \text{error } M}$$

$$\frac{}{\text{case } (\text{error } M) \text{ of } (x.N_1) (y.N_2) \longrightarrow \text{error } M} \quad \frac{}{\text{error } (\text{error } M) \longrightarrow \text{error } M}$$

alongside with

$$\frac{M \longrightarrow M'}{\text{error } M \longrightarrow \text{error } M'}$$

Intuitively, error propagates the “exception” that something wrong has happened.

We also extend the set of values.

$$V ::= \dots \mid \text{error } W$$

The typing rule for **error** is designed as a correspondent to the rule \perp -E.

$$\frac{\Gamma \vdash M : \perp}{\Gamma \vdash \text{error } M : \tau} \text{T-ERROR}$$

Still we have many important properties, including subject reduction, progress, and strong normalization. Also, check that there is no value that has type \perp under the empty type environment.

Exercise. Give a λ -term of type $((P \rightarrow Q) \rightarrow P) \rightarrow ((P \rightarrow \perp) \rightarrow \perp)$. Show its typing derivation.

FYI: Kripke Model of Intuitionistic Logic

In the classical logic, a proposition is either true or false. However, in the intuitionistic logic, things are not that simple; there is a proposition A such that A is not provable whereas $\neg A$ leads to contradiction (i.e., $\neg\neg A$ is provable). So, what does a proposition in the intuitionistic logic represent?

Curry-Howard correspondence suggests that a proposition A represents a set of proofs for A : a proof for $A_1 \wedge A_2$ is a pair of proofs for A_1 and A_2 respectively, a proof for $A_1 \vee A_2$ is either a left-tagged proof of A_1 or a right-tagged proof of A_2 , and a proof for $A_1 \Rightarrow A_2$ is a function that maps a proof of A_1 to a proof of A_2 . This view of propositions is known as the *BHK* interpretation, which clarify the constructive nature of the intuitionistic logic.

Here, we introduce another model of the intuitionistic propositional logic called the Kripke model.

Definition (Kripke model). A Kripke model is a triple (W, \preceq, \Vdash) of a non-empty set W , a partial-order \preceq on W , and binary relation \Vdash between W and propositional formulas, satisfying the following conditions for any $w \in W$ and any propositions A_1 and A_2 .

- if $w \preceq w'$, $w \Vdash P$ implies $w' \Vdash P$ for any propositional letter P .
- $w \Vdash A_1 \wedge A_2$ if and only if $w \Vdash A_1$ and $w \Vdash A_2$.
- $w \Vdash A_1 \vee A_2$ if and only if either $w \Vdash A_1$ or $w \Vdash A_2$.
- $w \Vdash A_1 \Rightarrow A_2$ if and only if $w' \Vdash A_2$ for any w' such that $w \preceq w'$ and $w' \Vdash A_1$.
- $w \Vdash \perp$ does not hold for any $w \in W$. □

Elements of W are sometimes called *world*. Intuitively, $w \preceq w'$ means that w' is a future of w , and $w \Vdash A$ means that we *know* that A holds at world w . The first line says that, once we know that P holds, we also know that P holds in any future. The condition of $w \Vdash A_1 \Rightarrow A_2$ means that if we know that A_1 holds now or in some future, A_2 must hold from this point. Notice that, for any world w , we have that $w \Vdash \neg A$ if and only if $w' \not\Vdash A$ for any world w' such that $w \preceq w'$. In other words, A does not hold neither now nor in the future. We omit the last line if we consider the minimal logic instead of the full intuitionistic propositional logic.

Sometimes, for a Kripke model $\mathcal{M} = (W, \preceq, \Vdash)$, we write $\mathcal{M}, w \Vdash A$ to clarify the model we consider. For a Kripke model $\mathcal{M} = (W, \preceq, \Vdash)$, we write $\mathcal{M}, w \Vdash \Delta$ if $\mathcal{M}, w \Vdash A$ for all $A \in \Delta$. Also, we write $\Delta \Vdash A$ if for every Kripke model $\mathcal{M} = (W, \preceq, \Vdash)$ and world $w \in W$, $\mathcal{M}, w \Vdash \Delta$ implies $\mathcal{M}, w \Vdash A$.

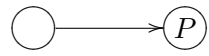
It is known that the proof system of the intuitionistic propositional logic is sound and complete with respect to the Kripke model.

Theorem. $\Delta \vdash A$ if and only if $\Delta \Vdash A$. □

Model theory is sometimes useful to show that a certain proposition is not provable.

Example(s). We show that $\not\vdash ((P \Rightarrow \perp) \Rightarrow \perp) \Rightarrow P$ by giving a concrete model $\mathcal{M} = (W, \preceq, \Vdash)$ such that $w \not\Vdash ((P \Rightarrow \perp) \Rightarrow \perp) \Rightarrow P$ for some $w \in W$. To give such a model, there must be a world such that $w \Vdash ((P \Rightarrow \perp) \Rightarrow \perp)$ but not $w \Vdash P$. The former condition means that for any

world w' with $w \preceq w'$, there is some w'' such that $w' \preceq w''$ and $w'' \Vdash P$. That is, P necessarily holds, but P is not required to be true now. Thus, $\mathcal{M} = (\{w_1, w_2\}, \{(w_1, w_2)\}^*, \{(w_2, P)\})$ is such a model because $w_1 \Vdash (P \Rightarrow \perp) \Rightarrow \perp$ holds but $w_1 \nVdash P$ does not. We can illustrate this model as follows.



Here, a world is represented by a circle labeled by the propositional letters that hold in the world.

□