Intuitionistic Propositional Logic

CIS700 — Fall 2023

Kris Micinski

Natural Deduction is a logical reasoning system which defines an explicit syntactic notion of proofs at the same time as the propositions they inhabit (prove).

This mindset is closely related to the notion of type-checking a program, wherein subexpressions types are surmised and compositional rules allow you to combine subexpressions in a well-typed manner.

In natural deduction, we say “the following rules are the **only** ways in which a proof of a logical statement may be built.”

To say something is true **is the same as** having a ***syntactic, materialized*** proof for it

My lecture very closely follows Frank Pfenning's notes from his various classes, I will link these notes in the Google Group.

I am not a researcher in type theory (not my branch of PL!), so I will defer to expert expositions when necessary.

“Intuitionistic logic, sometimes more generally called constructive logic, refers to systems of symbolic logic that differ from the systems used for classical logic by more closely mirroring the notion of constructive proof. — Wikipedia”

Intuitionism is the notion of identifying a **true statement** with a **symbolic proof of that statement**

Last lecture, we talked about a model (i.e., set)-theoretic perspective, mapping variables to values. This has issues in handling higher-order objects (Russel’s paradox) which do not crop up in the propositional setting—but the study of higher-order logic (wherein one can quantify over propositions) motivated the study of **intuitionistic type theory**

Introduction and Elimination Forms

I will present what Pfenning's notes call the "verificationalist" approach (Gentzen-style systems), which define the meaning of each connective in the logic via orthogonal rules. In classical logic, we typically construe connectives as *encodings* into a minimal form (e.g., CNF/DNF). This pushes reasoning into a set-theoretic interpretation.

Specifically problematic for computers: explicitly representing an interpretation (e.g., as a set) may be either (a) intractable or (b) impossible due to infiniteness.

By contrast, Gentzen-style intuitionism dictates that when we discuss the meaning of a connective, we completely define a set of **formation rules**.
These rules break down into two broad categories:

- **Introduction Forms** — a connective **appears new** in a conclusion
- **Elimination Forms** — a connective is **consumed** and disappears in the conclusion

The **introduction** form for and ($\wedge$) is a proof schema which tells us how we can introduce $\wedge$ s into a conclusion.

$$\wedge\mathbf{I}\ \frac{P\ \text{True} \quad Q\ \text{True}}{P \wedge Q\ \text{True}}$$

There are two **elimination** forms for $\wedge$: the **first** eliminator selects the left item (discarding the second), and the **second** eliminator selects the right (discarding the left)

$$\wedge\mathbf{E1}\ \frac{P \wedge Q\ \text{True}}{P\ \text{True}} \qquad \wedge\mathbf{E2}\ \frac{P \wedge Q\ \text{True}}{Q\ \text{True}}$$

A crucial problem — the need for premises

Let's say we want to write proofs of true statements involving ∧. This is the kind of thing we should be able to do now that we've defined the introduction and elimination forms for ∧.

Unfortunately, this doesn't work. Look at this:

$$\dfrac{\dfrac{A \wedge (B \wedge C) \text{ True}}{(B \wedge C) \text{ True}}\ \wedge\mathbf{E2}}{B \text{ True}}\ \wedge\mathbf{E1}$$

The **reasoning** here works, but following this reasoning allows us to conclude that an arbitrary proposition is true. Obviously, there are some false statements (A ∧ ¬A), so there **must** be a problem!

A crucial problem — the need for premises

This is **not** a proof, it is a suppositional line of reasoning! We have **assumed** that $A \wedge (B \wedge C)$ True, and used that to derive B True

Intuitionistic logic gives **names** to assumptions. We will reject this as a "proof" because the hypothesis is not explicitly introduced. We will do this by introducing them into an **environment**, which allows naming hypotheses

Hypotheses get introduced (and **named**) by the introduction of ⇒.

To prove A ⇒ B, we assume A (by introducing it as a named hypothesis, which may then be referenced) and showing B:

Named hypothesis u

$$\cfrac{\cfrac{}{A \text{ True}}\,u \\ \cdots \\ B \text{ True}}{A \Rightarrow B \text{ True}}\,\Rightarrow\!\mathrm{I}^{u}$$

Intuitively, <u>if nothing is above the line, then the previous proposition is taken as an axiom</u> (i.e., assumed true).

Thus, this **incorrect proof** is broken because it **assumes** A, without correctly accounting for *how* doing so is justified!

$$\dfrac{\dfrac{}{A \text{ True}} \quad \cdots \quad B \text{ True}}{A \Rightarrow B \text{ True}} \Rightarrow\!\mathbf{I}^{u}$$

Intuitively, <u>if nothing is above the line, then the previous proposition is taken as an axiom</u> (i.e., assumed true).

Thus, this **incorrect proof** is broken because it **assumes** A, without correctly accounting for *how* doing so is justified!

$$
\cfrac{\cfrac{}{A \text{ True}}\,u \quad \cdots \quad B \text{ True}}{A \Rightarrow B \text{ True}} \Rightarrow\!\mathbf{I}^{u}
$$

The fix is to ensure the introduction point is explicitly named

Notice that implicitly, we are assuming that, in checking a valid proof, the assumption truly *is* in scope, by looking higher up in the term

$$\cfrac{\cfrac{}{A \text{ True}}\,u \\ \cdots \\ B \text{ True}}{A \Rightarrow B \text{ True}}\Rightarrow\!\mathbf{I}^{\mathbf{u}}$$

The **eliminator** for ⇒ is modus ponens

$$\frac{A \Rightarrow B \text{ True} \quad A \text{ True}}{B \text{ True}} \Rightarrow\!\mathbf{E}$$

"If I have a proof of A ⇒ B, and a proof of A, I can apply ⇒E to obtain a proof of B."

So far, we have defined a set of rules, or **proof schemas**, which tell us how to construct each intermediate step of the proof. To actually build proofs, we have to chain these rules together.

$$\wedge\mathbf{I}\ \frac{P\ \text{True} \quad Q\ \text{True}}{P \wedge Q\ \text{True}} \qquad \wedge\mathbf{E1}\ \frac{P \wedge Q\ \text{True}}{P\ \text{True}} \qquad \wedge\mathbf{E2}\ \frac{P \wedge Q\ \text{True}}{Q\ \text{True}}$$

$$\dfrac{\dfrac{}{A\ \text{True}}\,u \\ \cdots \\ B\ \text{True}}{A \Rightarrow B\ \text{True}}\,\Rightarrow\mathbf{I}^{\mathbf{u}} \qquad \frac{A \Rightarrow B\ \text{True} \quad A\ \text{True}}{B\ \text{True}}\,\Rightarrow\mathbf{E}$$

You can build proofs by either:

- **Forward reasoning** — start at the assumptions, grow to conclusion
- **Backward reasoning** — start by writing a statement, build the proof from the bottom to the top

$$\wedge\mathbf{I}\ \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}} \qquad \wedge\mathbf{E1}\ \frac{P \wedge Q \text{ True}}{P \text{ True}} \qquad \wedge\mathbf{E2}\ \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\cfrac{\cfrac{}{A \text{ True}}\ u \\ \cdots \\ B \text{ True}}{A \Rightarrow B \text{ True}}\ \Rightarrow\mathbf{I}^{\mathbf{u}} \qquad \frac{A \Rightarrow B \text{ True} \quad A \text{ True}}{B \text{ True}}\ \Rightarrow\mathbf{E}$$

It is more natural to employ backwards (suppositional) reasoning, and eventually "closing off" each branch of the proof with an assumption.

Let's try some examples

$$\wedge\mathbf{I}\ \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}} \qquad \wedge\mathbf{E1}\ \frac{P \wedge Q \text{ True}}{P \text{ True}} \qquad \wedge\mathbf{E2}\ \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\frac{\dfrac{}{A \text{ True}}\,u \atop {\cdots \atop B \text{ True}}}{A \Rightarrow B \text{ True}}\ \Rightarrow\mathbf{I}^{\mathbf{u}} \qquad \frac{A \Rightarrow B \text{ True} \quad A \text{ True}}{B \text{ True}}\ \Rightarrow\mathbf{E}$$

$$\wedge\textbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\textbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\wedge\textbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

Step 1: write statement below line

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \Rightarrow\!\textbf{E}$$

$$\frac{}{A \text{ True}}\ u$$

$$\dots$$

$$\frac{B \text{ True}}{A \Rightarrow B \text{ True}}\ \Rightarrow\!\textbf{I}^{\textbf{u}}$$

$$\frac{\dots}{(A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}$$

$$\wedge\textbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\textbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\wedge\textbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \boldsymbol{\Rightarrow}\textbf{E}$$

$$\frac{\dfrac{}{A \text{ True}}\,u \qquad \begin{matrix} \cdots \\ B \text{ True}\end{matrix}}{A \Rightarrow B \text{ True}}\ \boldsymbol{\Rightarrow}\textbf{I}^{\textbf{u}}$$

Step 2: in this case, we must apply the $\Rightarrow\mathrm{I}^{\mathrm{u}}$ rule—

no other rule will "fit"

$$\frac{\begin{matrix}\dfrac{}{(A \Rightarrow B \wedge C)}\,\mathrm{u} \\ \cdots \\ \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)\end{matrix}}{(A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\ \Rightarrow\mathrm{I}^{\mathrm{u}}$$

$$\wedge\mathbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\mathbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\wedge\mathbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}} \Rightarrow\mathbf{E}$$

$$\frac{\dfrac{}{A \text{ True}}\, u \quad \cdots \quad B \text{ True}}{A \Rightarrow B \text{ True}} \Rightarrow\mathbf{I}^u$$

Step 2: now what do we apply? The "…" is the unfinished portion of the proof, so we make progress on the proximate proposition before it—in this case, we need ∧ in the conclusion, so we apply ∧I

Notice how ∧I "splits" the proof, forcing us to prove two "subgoals" — u factors across subgoals

Subgoal 1 / **Subgoal 2**

$$\dfrac{\dfrac{\dfrac{}{A \Rightarrow B \wedge C}\, u \quad \cdots \quad A \Rightarrow B \qquad \dfrac{}{A \Rightarrow B \wedge C}\, u \quad \cdots \quad A \Rightarrow C}{\big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)} \wedge\mathrm{I}}{(A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)} \Rightarrow\mathrm{I}^u$$

$$\wedge\mathbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\mathbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\wedge\mathbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

Let's focus in on just subgoal 1 for a bit—subgoal 2 is symmetric, so once we've proven subgoal 1 we can use similar reasoning to solve subgoal 2

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \Rightarrow\!\mathbf{E}$$

$$\frac{\dfrac{}{A \text{ True}}\,u \quad \begin{matrix}\cdots \\ B \text{ True}\end{matrix}}{A \Rightarrow B \text{ True}}\ \Rightarrow\!\mathbf{I}^{\mathbf{u}}$$

Subgoal 1

$$\frac{\dfrac{}{A \Rightarrow B \wedge C}\,u \quad \cdots}{A \Rightarrow B}$$

This subgoal says: "Assuming A ⇒ B ∧ C, show A ⇒ B."

Again, we need to introduce ⇒, so we assume A (introducing a new assumption w) and prove B

$$\wedge\mathbf{E1}\ \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\mathbf{E2}\ \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\wedge\mathbf{I}\ \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \mathbf{\Rightarrow E}$$

$$\frac{\dfrac{}{A \text{ True}}\ u \quad \cdots \quad B \text{ True}}{A \Rightarrow B \text{ True}}\ \mathbf{\Rightarrow I^{u}}$$

So we apply ⇒E to obtain B ∧ C…

$$\frac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B \wedge C}\ u \quad \dfrac{}{A}\ w}{B \wedge C}\ \Rightarrow\text{E} \quad \cdots}{B}}{A \Rightarrow B}\ \Rightarrow\text{I}^{w}$$

$$\wedge\textbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\textbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\wedge\textbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \mathbf{\Rightarrow E}$$

$$\cfrac{\cfrac{}{A \text{ True}}\, u \quad \cdots \quad B \text{ True}}{A \Rightarrow B \text{ True}}\ \mathbf{\Rightarrow I^u}$$

Note, I am taking a shortcut, really it is more like…

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A \Rightarrow B \wedge C}\,u}{A}\,w}{A \Rightarrow B \wedge C} \qquad \cfrac{\cfrac{\cfrac{}{A \Rightarrow B \wedge C}\,u}{A}\,w}{A}}{B \wedge C}\,\Rightarrow\text{E}}{\cdots}}{\cfrac{B}{A \Rightarrow B}\,\Rightarrow\text{I}^w}$$

Next, we can use the ∧E1 eliminator to obtain just B

$$\wedge\mathbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\mathbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}} \qquad \wedge\mathbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad\qquad A \text{ True}}{B \text{ True}}\ \mathbf{\Rightarrow E}$$

$$\begin{array}{c l}
\hline & u \\
A \text{ True} & \\
\cdots & \\
B \text{ True} & \\
\hline A \Rightarrow B \text{ True} & \mathbf{\Rightarrow I^{u}}
\end{array}$$

$$\begin{array}{c l}
\hline & u \\
A \Rightarrow B \wedge C & \\
\hline & w \\
A & \\
\hline & \Rightarrow\text{E} \\
B \wedge C & \\
\hline & \wedge\mathbf{E1} \\
B & \\
\cdots & \\
\hline B & \\
\hline A \Rightarrow B & \Rightarrow\text{I}^{w}
\end{array}$$

$$\wedge\mathbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

Indeed, now we are **done** with this subgoal

$$\wedge\mathbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\wedge\mathbf{I}\quad \frac{P \text{ True} \qquad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B \wedge C}\, u}{A}\, w}{B \wedge C}\, \Rightarrow\text{E}}{B}\, \wedge\text{E1}}{A \Rightarrow B}\, \Rightarrow\text{I}^w$$

$$\frac{A \Rightarrow B \text{ True} \qquad\qquad A \text{ True}}{B \text{ True}}\ \Rightarrow\mathbf{E}$$

$$\frac{\begin{array}{c} \overline{}\ u \\ A \text{ True} \\ \cdots \\ B \text{ True} \end{array}}{A \Rightarrow B \text{ True}}\ \Rightarrow\mathbf{I}^{\mathbf{u}}$$

$$\wedge\mathbf{E1}\ \frac{P \wedge Q \text{ True}}{P \text{ True}} \qquad \wedge\mathbf{E2}\ \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

Now, we substitute our proof of the subgoal into the larger proof we're working on…

$$\wedge\mathbf{I}\ \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \mathbf{\Rightarrow E}$$

$$\cfrac{\overline{A \text{ True}}^{\,u} \\ \cdots \\ B \text{ True}}{A \Rightarrow B \text{ True}}\ \mathbf{\Rightarrow I^u}$$

Subgoal 1

Subgoal 2

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A \Rightarrow B \wedge C}\,u \qquad \cfrac{}{A}\,w}{B \wedge C}\,\Rightarrow E}{B}\,\wedge E1}{A \Rightarrow B}\,\Rightarrow I^w \qquad \cfrac{\cfrac{}{A \Rightarrow B \wedge C}\,u \\ \cdots \\ A \Rightarrow C}{}}{\cfrac{\big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}{(A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\,\Rightarrow I^u}\,\wedge I$$

$$\wedge\mathbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\mathbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

To get the proof of the second, we use the eliminator ∧E2 instead

$$\wedge\mathbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \Rightarrow\mathbf{E}$$

$$\cfrac{\cfrac{}{A \text{ True}}\,u \\ \cdots \\ B \text{ True}}{A \Rightarrow B \text{ True}}\ \Rightarrow\mathbf{I}^u$$

Subgoal 1 **Subgoal 2**

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A \Rightarrow B \wedge C}\,u \quad \cfrac{}{A}\,w}{B \wedge C}\,\Rightarrow\mathrm{E}}{B}\,\wedge\mathrm{E1}}{A \Rightarrow B}\,\Rightarrow\mathrm{I}^w \qquad \cfrac{\cfrac{\cfrac{\cfrac{}{A \Rightarrow B \wedge C}\,u \quad \cfrac{}{A}\,w}{B \wedge C}\,\Rightarrow\mathrm{E}}{C}\,\wedge\mathrm{E2}}{A \Rightarrow C}\,\Rightarrow\mathrm{I}^w}{\big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\,\wedge\mathrm{I}}{(A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\,\Rightarrow\mathrm{I}^u$$

$$\wedge\mathbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}}$$

$$\wedge\mathbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\wedge\mathbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \Rightarrow\mathbf{E}$$

$$\cfrac{\cfrac{}{A \text{ True}}\, u \\ \cdots \\ B \text{ True}}{A \Rightarrow B \text{ True}}\ \Rightarrow\mathbf{I}^{u}$$

Both of our subgoals are done—our proof is **complete**

Subgoal 1

Subgoal 2

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A \Rightarrow B \wedge C}\,u \quad \cfrac{}{A}\,w}{B \wedge C}\,\Rightarrow\text{E}}{B}\,\wedge\text{E1}}{A \Rightarrow B}\,\Rightarrow\text{I}^{w} \qquad \cfrac{\cfrac{\cfrac{\cfrac{}{A \Rightarrow B \wedge C}\,u \quad \cfrac{}{A}\,w}{B \wedge C}\,\Rightarrow\text{E}}{C}\,\wedge\text{E2}}{A \Rightarrow C}\,\Rightarrow\text{I}^{w}}{\big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\,\wedge\mathbf{I}}{(A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\,\Rightarrow\text{I}^{u}$$

So far, we've seen conjunction and implication. Adding **disjunction** is not too hard. If you have A, you can prove A ∨ B (and similar for B), leading to two natural introduction rules

$$\wedge\mathbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}} \qquad \wedge\mathbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}}$$

$$\vee\mathbf{I1}\quad \frac{P \text{ True}}{P \vee Q \text{ True}} \qquad \vee\mathbf{I2}\quad \frac{Q \text{ True}}{P \vee Q \text{ True}}$$

Notice how the **introduction** rules for ∨ mirror the *elimination* rules for ∧

To **eliminate** an ∨ is roughly analogous to reasoning suppositionally by cases. If we have A ∨ B, we can use it to prove C by (a) assuming A and proving C and (b) assuming B and proving C

$$\vee E^{uw}\ \dfrac{A \vee B \text{ True} \qquad \begin{array}{c} \overline{A \text{ True}}^{\,u} \\ \cdots \\ C \text{ True} \end{array} \qquad \begin{array}{c} \overline{B \text{ True}}^{\,w} \\ \cdots \\ C \text{ True} \end{array}}{C \text{ True}}$$

Notice that u is available **only** in the first subgoal, and w is **only** available in the right. Intuitively, this is because we know that either A or B is true—but not (necessarily) both. If we assume A, we do not get B, and vice-versa

So far, we've done nearly everything, the only remaining rules handle negation…

$$\wedge\mathbf{E1}\ \frac{P \wedge Q \text{ True}}{P \text{ True}} \qquad \wedge\mathbf{E2}\ \frac{P \wedge Q \text{ True}}{Q \text{ True}} \qquad \wedge\mathbf{I}\ \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\vee\mathbf{I1}\ \frac{P \text{ True}}{P \vee Q \text{ True}} \qquad \vee\mathbf{I2}\ \frac{Q \text{ True}}{P \vee Q \text{ True}} \qquad \vee\mathbf{E}^{uw}\ \frac{A \vee B \text{ True} \quad \begin{array}{c} \overline{A \text{ True}}^{\,u} \\ \cdots \\ C \text{ True} \end{array} \quad \begin{array}{c} \overline{B \text{ True}}^{\,w} \\ \cdots \\ C \text{ True} \end{array}}{C \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \mathbf{\Rightarrow E} \qquad \frac{\begin{array}{c} \overline{A \text{ True}}^{\,u} \\ \cdots \\ B \text{ True} \end{array}}{A \Rightarrow B \text{ True}}\ \mathbf{\Rightarrow I}^{u}$$

In classical logic, we admit the excluded middle: everything is either true or false. In intuitionistic logic, “being true” means “having a proof.”

Thus, for a proposition to be false ($\perp$), it must have no proof.

To implement this we (a) provide **no introduction forms** for $\perp$ and (b) provide a single *elimination* rule

The elimination rule for $\perp$ says that if we assume $\perp$, we can prove anything

$$\frac{\perp}{P\ \text{True}}\ \perp\mathbf{E}$$

This rule is justified because we can't actually **construct** $\perp$ without assuming a contradiction. But <u>if we can show that our assumptions lead to a contradiction</u>, we can prove anything.

Q: If we can't construct $\perp$, how is it possibly of any use to us? A: The elimination rule for $\perp$ allows us to show that our assumptions lead to a contradiction (in latin, *reductio ad absurdum*), and can then be used to prove anything.

Also: intuitionism regards $\neg P$ as $P \Rightarrow \perp$. Intuitively this means: if we want to prove $\neg P$, we must assume P and then show that ***anything*** can be proven

$$\frac{\perp}{P \text{ True}}\ \perp\mathbf{E}$$

$\neg P$ is sugar for $P \Rightarrow \perp$

Let's see how $\perp$ and $\neg$ show up in intuitionistic logic by looking at a proof of a theorem we all intuitively know must be a contradiction:

$\neg(P \wedge \neg P)$

Intuitively, this says: "If we assume $P \wedge \neg P$, we can prove anything."

Intuitively, we can make progress by forward reasoning, harvesting the data from $\wedge$

$$
\begin{array}{c}
\dfrac{\dfrac{\dfrac{}{(P \wedge (P \Rightarrow \bot))}\,u}{P}\,\wedge E1}{(P \Rightarrow \bot)}\,\wedge E2 \\
\hline
\cdots \\
\dfrac{\bot}{(P \wedge (P \Rightarrow \bot)) \Rightarrow \bot}\,\Rightarrow I^{u}
\end{array}
$$

To finish the proof, we just use the eliminator for $\Rightarrow$ with our assumption P

Now our proof is complete!

$$
\dfrac{\dfrac{\dfrac{\dfrac{\overline{\quad (P \land (P \Rightarrow \bot)) \quad}\, u}{P}\, \land E1}{(P \Rightarrow \bot)}\, \land E2}{\bot}\, \Rightarrow E}{(P \land (P \Rightarrow \bot)) \Rightarrow \bot}\, \Rightarrow I^{u}
$$

Our **complete** set of rules for IPL (intuitionistic propositional logic)

$$\wedge\mathbf{E1}\quad \frac{P \wedge Q \text{ True}}{P \text{ True}} \qquad \wedge\mathbf{E2}\quad \frac{P \wedge Q \text{ True}}{Q \text{ True}} \qquad \wedge\mathbf{I}\quad \frac{P \text{ True} \quad Q \text{ True}}{P \wedge Q \text{ True}}$$

$$\vee\mathbf{I1}\quad \frac{P \text{ True}}{P \vee Q \text{ True}} \qquad \vee\mathbf{I2}\quad \frac{Q \text{ True}}{P \vee Q \text{ True}} \qquad \vee\mathbf{E}^{\mathbf{uw}}\quad \frac{A \vee B \text{ True} \quad \begin{matrix} \overline{A \text{ True}}^{\,u} \\ \cdots \\ C \text{ True} \end{matrix} \quad \begin{matrix} \overline{B \text{ True}}^{\,w} \\ \cdots \\ C \text{ True} \end{matrix}}{C \text{ True}}$$

$$\frac{A \Rightarrow B \text{ True} \qquad A \text{ True}}{B \text{ True}}\ \mathbf{\Rightarrow E} \qquad \frac{\begin{matrix} \overline{A \text{ True}}^{\,u} \\ \cdots \\ B \text{ True} \end{matrix}}{A \Rightarrow B \text{ True}}\ \mathbf{\Rightarrow I^{u}}$$

$$\frac{\bot}{P \text{ True}}\ \bot\mathbf{E}$$

¬P is sugar for P ⇒ ⊥

Now we will ask ourselves: how do convince ourselves that our proofs are "correct?" In our setting, this reduces to checking that **all usages of assumptions are *in scope* at the point they are used**

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B \wedge C}\,u}{A}\,w}{B \wedge C}\Rightarrow\mathrm{E}}{B}\wedge\mathrm{E1}}{A \Rightarrow B}\Rightarrow\mathrm{I}^{w} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B \wedge C}\,u}{A}\,w}{B \wedge C}\Rightarrow\mathrm{E}}{C}\wedge\mathrm{E2}}{A \Rightarrow C}\Rightarrow\mathrm{I}^{w}}{\dfrac{\big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}{(A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\Rightarrow\mathrm{I}^{u}}\wedge\mathrm{I}
$$

Now we will ask ourselves: how do convince ourselves that our proofs are "correct?" In our setting, this reduces to checking that **all usages of assumptions are *in scope* at the point they are used**

Essentially, this means that our proof checking is reduced to **reachability**

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{A \Rightarrow B \land C}\,u
}{A}\,w
}{B \land C}\,{\Rightarrow}\mathrm{E}
}{B}\,{\land}\mathrm{E1}
}{A \Rightarrow B}\,{\Rightarrow}\mathrm{I}^{w}
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{A \Rightarrow B \land C}\,u
}{A}\,w
}{B \land C}\,{\Rightarrow}\mathrm{E}
}{C}\,{\land}\mathrm{E2}
}{A \Rightarrow C}\,{\Rightarrow}\mathrm{I}^{w}
}{
\dfrac{\big((A \Rightarrow B) \land (A \Rightarrow C)\big)}{(A \Rightarrow B \land C) \Rightarrow \big((A \Rightarrow B) \land (A \Rightarrow C)\big)}\,{\Rightarrow}\mathrm{I}^{u}
}\,{\land}\mathrm{I}
$$

We can only call something a “proof” if we check that every assumption is introduced correctly.

The following example (from Pfenning) illustrates why we **must** do this “scope checking” for assumptions

u is referenced **incorrectly** here, is **not** in scope

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A\ \mathsf{True}}\,u}{(A \Rightarrow A)\ \mathsf{True}}\,{\Rightarrow}\mathsf{I}^{u} \qquad \dfrac{}{A\ \mathsf{True}}\,u}{(A \Rightarrow A) \wedge A\ \mathsf{True}}}{A\ \mathsf{True}}$$

The “turnstile” syntax

This “scope checking” is something that we require as a last step to deem a proof acceptable. We have been implicitly doing it throughout lecture. There is an alternative presentation which allows us to materialize a set of *assumptions* via an algebraically-constructed *“environment”*

We will modify our system to allow judgements to be *conditional tautologies* (often called “sequents”) and written like so:

$$\Gamma \vdash P$$

Which reads “under the assumptions Γ, we may derive P.”

Porting our old rules into this new **sequent** style

∧E1 $$\frac{\Gamma \vdash P \wedge Q}{\Gamma \vdash P}$$

∧E2 $$\frac{\Gamma \vdash P \wedge Q}{\Gamma \vdash Q}$$

∧I $$\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q}$$

∨I1 $$\frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q}$$

∨I2 $$\frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q}$$

∨E $$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$$ **⇒E**

$$\frac{\Gamma, A \vdash B}{\Gamma, A \Rightarrow B}$$ **⇒I**

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash P}$$ **⊥E**

¬P is sugar for P ⇒ ⊥

Many of the rules simply propagate the environment, however it is worth focusing in on the rules where the environment is extended—these are rules where new assumptions are introduced into scope

Sequent Style Rules

$$\vee\mathbf{E}\ \frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$\frac{\Gamma, A \vdash B}{\Gamma, A \Rightarrow B}\ \Rightarrow\mathbf{I}$$

Previous Formulation…

$$\vee\mathbf{E}^{uw}\ \frac{A \vee B \text{ True} \qquad \begin{array}{c} \overline{A \text{ True}}^{\,u} \\ \cdots \\ C \text{ True} \end{array} \qquad \begin{array}{c} \overline{B \text{ True}}^{\,w} \\ \cdots \\ C \text{ True} \end{array}}{C \text{ True}}$$

$$\frac{\begin{array}{c} \overline{A \text{ True}}^{\,u} \\ \cdots \\ B \text{ True} \end{array}}{A \Rightarrow B \text{ True}}\ \Rightarrow\mathbf{I}^{u}$$

The sequent style allows us to make a ***local*** change to the set of assumptions, rather than delaying “scope checking” to the *end*

We also need an **assumption** rule (which lets us find assumptions in Γ)

$$\textbf{Assumption}\ \frac{}{\Gamma, P \vdash P}$$

$$\wedge\textbf{E1}\ \frac{\Gamma \vdash P \wedge Q}{\Gamma \vdash P} \qquad \wedge\textbf{E2}\ \frac{\Gamma \vdash P \wedge Q}{\Gamma \vdash Q} \qquad \wedge\textbf{I}\ \frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q}$$

$$\vee\textbf{I1}\ \frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q} \qquad \vee\textbf{I2}\ \frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q} \qquad \vee\textbf{E}\ \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \Rightarrow\!\textbf{E} \qquad \frac{\Gamma, A \vdash B}{\Gamma, A \Rightarrow B}\ \Rightarrow\!\textbf{I}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash P}\ \bot\textbf{E}$$

¬P is sugar for P ⇒ ⊥

Also, the **order** of assumptions in Γ is irrelevant—this seems obvious to humans, but formally we also need **structural** rules which enable reordering

$$\textbf{Assumption}\ \frac{}{\Gamma, P \vdash P}$$

$$\wedge\textbf{E1}\ \frac{\Gamma \vdash P \wedge Q}{\Gamma \vdash P} \qquad \wedge\textbf{E2}\ \frac{\Gamma \vdash P \wedge Q}{\Gamma \vdash Q} \qquad \wedge\textbf{I}\ \frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q}$$

$$\vee\textbf{I1}\ \frac{\Gamma \vdash P}{\Gamma \vdash P \vee Q} \qquad \vee\textbf{I2}\ \frac{\Gamma \vdash Q}{\Gamma \vdash P \vee Q} \qquad \vee\textbf{E}\ \frac{\Gamma \vdash A \vee B \quad \Gamma, A \vdash C \quad \Gamma, B \vdash C}{\Gamma \vdash C}$$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ \Rightarrow\!\textbf{E} \qquad \frac{\Gamma, A \vdash B}{\Gamma, A \Rightarrow B}\ \Rightarrow\!\textbf{I}$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash P}\ \bot\textbf{E}$$

¬P is sugar for P ⇒ ⊥

Let’s redo our previous proof in this new sequent-based style

(The previous style and the sequent style are isomorphic)

$$
\dfrac{
  \dfrac{
    \dfrac{
      \dfrac{\dfrac{}{(A \Rightarrow B \wedge C), A \vdash A \Rightarrow B \wedge C}\;\text{Assm} \qquad \dfrac{}{(A \Rightarrow B \wedge C), A \vdash A}\;\text{Assm}}{(A \Rightarrow B \wedge C), A \vdash B \wedge C}\;{\Rightarrow}\text{E}
    }{(A \Rightarrow B \wedge C), A \vdash B}\;{\wedge}\text{E1}
  }{(A \Rightarrow B \wedge C) \vdash A \Rightarrow B}\;{\Rightarrow}\text{I}
  \qquad
  \dfrac{
    \dfrac{
      \dfrac{\dfrac{}{(A \Rightarrow B \wedge C), A \vdash A \Rightarrow B \wedge C}\;\text{Assm} \qquad \dfrac{}{(A \Rightarrow B \wedge C), A \vdash A}\;\text{Assm}}{(A \Rightarrow B \wedge C), A \vdash B \wedge C}\;{\Rightarrow}\text{E}
    }{(A \Rightarrow B \wedge C), A \vdash C}\;{\wedge}\text{E2}
  }{(A \Rightarrow B \wedge C) \vdash A \Rightarrow C}\;{\Rightarrow}\text{I}
}{
  \dfrac{(A \Rightarrow B \wedge C) \vdash \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}{\vdash (A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\;{\Rightarrow}\text{I}
}\;{\wedge}\text{I}
$$

The new style makes assumptions **explicitly manifest** (i.e., *materialized*)

(Assumptions are tracked and extended *on-the-fly* rather than a reachability-based check at the end!)

$$\text{Assm}\ \dfrac{}{(A \Rightarrow B \wedge C), A \vdash A \Rightarrow B \wedge C} \qquad \dfrac{}{(A \Rightarrow B \wedge C), A \vdash A \Rightarrow B \wedge C}\ \text{Assm}$$

$$\text{Assm}\ \dfrac{}{(A \Rightarrow B \wedge C), A \vdash A} \qquad \dfrac{}{(A \Rightarrow B \wedge C), A \vdash A}\ \text{Assm}$$

$$\Rightarrow\text{E}\ \dfrac{(A \Rightarrow B \wedge C), A \vdash A \Rightarrow B \wedge C \quad (A \Rightarrow B \wedge C), A \vdash A}{(A \Rightarrow B \wedge C), A \vdash B \wedge C} \qquad \dfrac{(A \Rightarrow B \wedge C), A \vdash A \Rightarrow B \wedge C \quad (A \Rightarrow B \wedge C), A \vdash A}{(A \Rightarrow B \wedge C), A \vdash B \wedge C}\ \Rightarrow\text{E}$$

$$\wedge\text{E1}\ \dfrac{(A \Rightarrow B \wedge C), A \vdash B \wedge C}{(A \Rightarrow B \wedge C), A \vdash B} \qquad \dfrac{(A \Rightarrow B \wedge C), A \vdash B \wedge C}{(A \Rightarrow B \wedge C), A \vdash C}\ \wedge\text{E2}$$

$$\Rightarrow\text{I}\ \dfrac{(A \Rightarrow B \wedge C), A \vdash B}{(A \Rightarrow B \wedge C) \vdash A \Rightarrow B} \qquad \dfrac{(A \Rightarrow B \wedge C), A \vdash C}{(A \Rightarrow B \wedge C) \vdash A \Rightarrow C}\ \Rightarrow\text{I}$$

$$\dfrac{(A \Rightarrow B \wedge C) \vdash A \Rightarrow B \qquad (A \Rightarrow B \wedge C) \vdash A \Rightarrow C}{(A \Rightarrow B \wedge C) \vdash \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\ \wedge\text{I}$$

$$\dfrac{(A \Rightarrow B \wedge C) \vdash \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}{\vdash (A \Rightarrow B \wedge C) \Rightarrow \big((A \Rightarrow B) \wedge (A \Rightarrow C)\big)}\ \Rightarrow\text{I}$$

Also, look at this fragment of the proof, this is an example of us assuming that we can reorder assumptions at will

$$\dfrac{}{(A \Rightarrow B \wedge C), A \vdash A \Rightarrow B \wedge C}\ \text{Assm}$$

Notice that it's not **quite** the assumption rule — P is on the front rather than the end

$$\text{Assumption}\ \dfrac{}{\Gamma, P \vdash P}$$

Also, look at this fragment of the proof, this is an example of us assuming that we can reorder assumptions at will

$$\text{Assm}\ \frac{}{(A \Rightarrow B \land C), A \vdash A \Rightarrow B \land C}$$

Some **sub-structural** logics treat assumptions like resources, popular examples are *linear logic* (assumptions must be used exactly once) or *affine logic* (assumptions may be used at most once); these logics can reason about resource usage (e.g., files always closed after opened)

$$\textbf{Assumption}\ \frac{}{\Gamma, P \vdash P}$$

The Curry-Howard Isomorphism

Intuitively, the Curry-Howard Isomorphism is the notion that proof terms in intuitionistic logics are equivalent to (isomorphic to) terms (i.e., expressions, *programs*) in a suitable type theory

This means that every well-typed program (in the Simply-Typed λ calculus) is a proof of a theorem in IPL, and **vice-versa** (every proof of a theorem in IPL can be read computationally as a term in the Simply-Typed λ calculus)

Every ***program*** (in a language with a consistent & sound type theory) may be read as a ***proof*** (of the theorem corresponding to the propositional analogue of the type inhabited by the term). Every ***proof*** may be read as a ***program***.

So what is the programming language that corresponds to the natural-deduction-style rules we gave for IPL?

Answer: a minimal functional language with functions ($\rightarrow$ types, the analogue of $\Rightarrow$), pairs (product types, $A \times B$—the analogue of $A \wedge B$), sums ($A + B$—the analogue of $A \vee B$), along with a collection of primitive types (e.g., Int, Bool, etc…).

CHI vs. IPL

The key idea is to realize that the typing derivation for STLC **precisely mirrors** the deductive rules of IPL

$$\frac{x \mapsto t \in \Gamma}{\Gamma \vdash x : t} \ \textbf{Var}$$

$$\textbf{Assumption} \ \frac{}{\Gamma, P \vdash P}$$

$$\frac{\Gamma \vdash e : t \to t' \quad \Gamma \vdash e' : t}{\Gamma \vdash (e\ e') : t'} \ \textbf{App}$$

$$\textbf{⇒E} \ \frac{\Gamma \vdash \phi \Rightarrow \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma, \{x \mapsto t\} \vdash e : t'}{\Gamma \vdash (\lambda\, (x : t)\ e) : t \to t'} \ \textbf{Lam}$$

$$\textbf{⇒I} \ \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi}$$

This means that every proof tree for STLC can be **trivially-mapped** to a proof tree in IPL. I.e., if `(e : t)` is typeable in STLC, the theorem `t` holds in IPL by construction of the proof built using this mapping

$$\frac{x \mapsto t \in \Gamma}{\Gamma \vdash x : t} \textbf{ Var}$$

$$\textbf{Assumption } \frac{}{\Gamma, P \vdash P}$$

$$\frac{\Gamma \vdash e : t \to t' \quad \Gamma \vdash e' : t}{\Gamma \vdash (e\ e') : t'} \textbf{ App}$$

$$\Rightarrow\textbf{E } \frac{\Gamma \vdash \phi \Rightarrow \psi \quad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

$$\frac{\Gamma, \{x \mapsto t\} \vdash e : t'}{\Gamma \vdash (\lambda\,(x : t)\ e) : t \to t'} \textbf{ Lam}$$

$$\Rightarrow\textbf{I } \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \Rightarrow \psi}$$

We will talk more about Typed Lambda Calculi (i.e., the programming embodiment of constructive logics) later on in the course if students are interested—it would be easy to fill a whole course on this, but much work in automated reasoning exploits classical logic and the excluded middle.

Next we will look at DPLL and algorithms for SAT.

History, as I understand it (and some links / references)

- First accounts of intuitionism by Brouwer (see http://thatmarcusfamily.org/philosophy/Course_Websites/Readings/Brouwer%20-%20Intuitionism%20and%20Formalism.pdf)
- 1960s-1970s: Per Martin-Löf gives several series of lectures on intuitionistic type theory which were highly influential (https://www.cs.cmu.edu/~crary/819-f09/Martin-Lof80.pdf)
- Type theory within PL has since become lore, explored by meany famous folks (Harper, Pfenning, Milner, Coquand, Pierce, …). Type theories inspired a wide array of systems from AUTOMATH, Mizar, HOL, Coq, Lean, Idris, Agda, …
- These systems enable such feats as **certified programming** (proof-carrying code)
- Each of these systems builds upon the foundational ideas, proximately influenced by Martin-Löf's type theory