Constructive Logic (15-317), Spring 2020
Recitation 1: An introduction to natural deduction (2020-01-15)
André Platzer et al

1 Why another logic?

Around a century ago, some people became intrigued about the way we reason and get conclusions from assumptions, particularly in the field of mathematics[1]. There were (and still are) many discussions on what constitutes a "correct" reasoning, which steps can one take without compromising an argument, and what it means for something to be true. But one thing that people usually accept fairly naturally is that, for every proposition A, either A holds or $\neg A$ holds. This is the so-called law of excluded middle. Given this principle, a proof that it is not the case that $\neg A$ (i.e., a proof of $\neg\neg A$) can be considered as evidence for A (if the disjunction is true and we know that one disjunct does not hold, then the other one **must** be true). This principle is the core of proofs by contradiction where, to prove a statement, you assume the contrary of the statement and arrive at an impossible situation. Another proof that relies heavily on the law of excluded middle is the following.

Theorem 1. *There exist two irrational numbers x and y such that x^y is a rational number.*

Proof. Take the number $\sqrt{2}^{\sqrt{2}}$. We do not know if this is a rational or irrational number, but the law of excluded middle tells us it must be one or the other.
Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Then choose $x = y = \sqrt{2}$ and the theorem holds.
Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Then choose $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Therefore $x^y = 2$ and the theorem also holds. □

In this proof, we know that the numbers x and y "exist," but we don't have any way of computing them! Some were not happy about this situation, and they decided to come up with new rules for the game. They were the constructivists (or intuitionists). They decided that, in their logic, the truth of a judgment is solely determined by an evidence (or proof) of **that** judgment. Not a negation of its negation, not the judgment painted in blue, but the judgment. It can be thought of as a *proof-centered* logic. In such a logic, we cannot say "either A holds or $\neg A$ holds" unless we have a proof of one or the other. It turns out that proofs become really interesting and informative, and can even be interpreted as algorithms (spoiler alert!). Mathematically, constructive proofs represent the construction of objects (hence the name)[2]. A real constructive proof of the theorem above would actually show how to obtain values for x and y which satisfy the property.

In this class, we'll explore different formal systems which capture aspects of constructive reasoning. By making these ideas formal, we'll be able to analyze the structure of proofs, discover their computational content, show that principles like the axiom $A \vee \neg A$ are or are not justified, and determine how to effectively search for proofs.

2 The System of Natural Deduction

In order to build proofs we need to use a *proof calculus*[3]. There are many proof calculi with widely varying notations, but the ones we will encounter can all be characterized either as *natural deduction* or *sequent calculus*. We'll be starting with the former, but both share the same building blocks: *propositions*, *judgments*, and *inference rules*.

First and foremost, we have the notion of *judgment*. A judgment is simply an assertion. For example, we could define a judgment form M *nat* which asserts that M is a natural number. Then 4 *nat* and Cat *nat* are both judgments, although only one of them can be made evident. We can define judgments that make assertions about any sort of thing, but in natural deduction we will be judging *propositions*.

A proposition is a logical statement like $\top$, $A \wedge B$, or $A \vee C \supset B$ built up from *connectives* (like $\top$, $\wedge$ and $\supset$). In natural deduction, we make assertions about propositions with the judgment A *true*, which asserts (unsurprisingly) that the proposition A is a true statement. In the future, we will see other judgments which describe propositions,

[1] For a nice and fun account of the history of logic, I absolutely recommend Logicomix.
[2] Actually, there is a whole field named *constructive mathematics* trying to express all mathematics in terms of constructive proofs.
[3] Around here, a "calculus" is just a system for calculating, the differential and integral calculi being the most well-known examples.

such as A *false*. (As André mentioned, we might also consider A *prop* to be a judgment, which asserts that A is a proposition.)

Now that we can write down the judgment $A\ \mathit{true}$, we want to be able to establish that the judgment is in fact *evident*, that is, to give a justification that it holds. For this we introduce the notion of a *proof*. To start with, we specify a collection of *inference rules*, a set of basic reasoning principles from which proofs are constructed. These are analogous to the *axioms* of classical mathematical logic. (In the natural deduction setting, the word *axiom* usually refers to an inference rule with zero premises, such as $\top I$.) For example, we have the rules for the connective $\wedge$:

$$\frac{A\ \mathit{true} \qquad B\ \mathit{true}}{A \wedge B\ \mathit{true}}\wedge I \qquad \frac{A \wedge B\ \mathit{true}}{A\ \mathit{true}}\wedge E_1 \qquad \frac{A \wedge B\ \mathit{true}}{B\ \mathit{true}}\wedge E_2$$

An inference rule consists of a set of *premise* judgments and a single *conclusion* judgment, along with a label:

$$\begin{array}{r} \text{Premises} \longrightarrow \\ \text{Conclusion} \longrightarrow \end{array} \quad \frac{A\ \mathit{true} \qquad B\ \mathit{true}}{A \wedge B\ \mathit{true}}\wedge I \quad \longleftarrow \text{Label}$$

This rule can be read as "from $A\ \mathit{true}$ and $B\ \mathit{true}$, conclude $A \wedge B\ \mathit{true}$". The letters A and B are *schema variables*: they can replaced with anything and the rule is still valid. For example,

$$\frac{\bot\ \mathit{true} \qquad \text{the moon is green}\ \mathit{true}}{\bot \wedge \text{the moon is green}\ \mathit{true}}\wedge I$$

is a valid instance of the $\wedge I$ rule.

In general, each connective comes with *introduction* and *elimination* rules: the introduction rules are used to establish the truth of a proposition using that connective, while the elimination rules are used to derive facts *from* such a proposition. In the case of the connective $\wedge$, $\wedge I$ is an introduction rule ("from $A\ \mathit{true}$ and $B\ \mathit{true}$, conclude $A \wedge B\ \mathit{true}$"), while $\wedge E_1$ ("from $A \wedge B\ \mathit{true}$, conclude $A\ \mathit{true}$") and $\wedge E_2$ ("from $A \wedge B\ \mathit{true}$ conclude $B\ \mathit{true}$") are elimination rules. The rules for $\wedge$ match our intuition about the meaning of $\wedge$:

> $A \wedge B\ \mathit{true}$ is provable iff[4] $A\ \mathit{true}$ is provable and $B\ \mathit{true}$ is provable.

Note the proof-centered meaning explanation! In the case of $\wedge$, this is uncontroversial, but we will see that claiming

> $A \vee B\ \mathit{true}$ is provable iff either $A\ \mathit{true}$ is provable or $B\ \mathit{true}$ is provable.

has interesting consequences.

Observe also that the introduction and elimination rules "fit together:" since we put in $A\ \mathit{true}$ and $B\ \mathit{true}$ to get $A \wedge B\ \mathit{true}$ (via $\wedge I$), this is exactly what we can get out (via $\wedge E_1$ and $\wedge E_2$). We will make this idea of "fitting together" more precise soon.

Inference rules may introduce *assumptions*, for example in the introduction rule $\supset I$ for implication:

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

Here, the premise of the $\supset I$ rule is a *hypothetical judgment*, a judgment in the presence of hypotheses. To assert the hypothetical judgment

$$\begin{array}{c} A\ \mathit{true} \\ \vdots \\ B\ \mathit{true} \end{array}$$

is to assert that $B\ \mathit{true}$ holds supposing that $A\ \mathit{true}$ holds. (This hypothetical judgment can be written more compactly as $A\ \mathit{true} \vdash B\ \mathit{true}$.) In the $\supset I$ rule, we use the label u to name the assumption $A\ \mathit{true}$. Once we start construct ing proofs from inference rules, we will use the label u to mark where that assumption is used.

As a general design principle, we try to mention only one connective in a particular rule. When we want to define a connective in terms of others, we simply define it as shorthand, rather than by giving rules. For example,

[4] "if and only if"

we define $\neg A$ to mean $A \supset \bot$. By doing this, we avoid cluttering our system with redundant constructs, and we can be sure that none of our connectives are circularly defined in terms of each other. Moreover, this makes the system more *modular*, in the sense that we can study connectives in isolation or in various combinations.

Finally, we build *proofs* (or *proof trees*) by composing inference rules. For example, we can prove $A \supset A \wedge A\ \mathit{true}$ and $A \wedge A \supset A\ \mathit{true}$:

$$\dfrac{\overline{A\ \mathit{true}}^{\,u}}{A \supset A\ \mathit{true}}\supset I^u \qquad\qquad \dfrac{\dfrac{\overline{A\ \mathit{true}}^{\,v} \qquad \overline{A\ \mathit{true}}^{\,v}}{A \wedge A\ \mathit{true}}\wedge I}{A \supset A \wedge A\ \mathit{true}}\supset I^v$$

Notice that assumptions can be used more than once (they can also be used zero times!). We know that these proofs are complete because there are no floating assumptions left over: every judgment in the tree is justified either by an inference rule or by an assumption. (In our notation, this is the same as saying every judgment has a line on top.) In contrast, here is an incomplete proof of $B \supset B \wedge C\ \mathit{true}$:

$$\dfrac{\dfrac{\overline{B\ \mathit{true}}^{\,x} \qquad C\ \mathit{true}}{B \wedge C\ \mathit{true}}\wedge I}{B \supset B \wedge C\ \mathit{true}}\supset I^x$$

This proof is incomplete because the assumption $C\ \mathit{true}$ is unjustified. (It is, however, a complete proof of the *hypothetical* judgment $C\ \mathit{true} \vdash B \supset B \wedge C\ \mathit{true}$.)

There can be different proofs of the same judgment. For example, these are two proofs of $A \wedge A \supset A\ \mathit{true}$:

$$\dfrac{\dfrac{\overline{A \wedge A\ \mathit{true}}^{\,w}}{A\ \mathit{true}}\wedge E_1}{A \wedge A \supset A\ \mathit{true}}\supset I^w \qquad\qquad \dfrac{\dfrac{\overline{A \wedge A\ \mathit{true}}^{\,w}}{A\ \mathit{true}}\wedge E_2}{A \wedge A \supset A\ \mathit{true}}\supset I^w$$

Here we begin to see the importance of labeling our inference rules: without labels, we wouldn't be able to distinguish the two proofs. Likewise, here we have two proofs that $A \supset (A \supset A)\ \mathit{true}$, which are distinguishable only by assumption labels:

$$\dfrac{\dfrac{\overline{A\ \mathit{true}}^{\,u}}{A \supset A\ \mathit{true}}\supset I^v}{A \supset (A \supset A)\ \mathit{true}}\supset I^u \qquad\qquad \dfrac{\dfrac{\overline{A\ \mathit{true}}^{\,v}}{A \supset A\ \mathit{true}}\supset I^v}{A \supset (A \supset A)\ \mathit{true}}\supset I^u$$

Our reasons for distinguishing these will become more clear as we explore the computational aspects of constructive logic.

This calculus is called "natural deduction" because (according to its inventor, Gerhard Gentzen) it is the "natural" way of proving things, as opposed to earlier axiomatic systems. Indeed, looking at the intuitive meanings of connectives, the rules come rather naturally. For some purposes, however, such as proof search and unprovability results, there are better options, which we will see later on.

3 Installing Tutch

For this first section of the class, we will be using the Tutch proof checker to formulate and verify natural deductive proofs. A syntax guide and explanation can be found in the online documentation. Some examples can also be found on the course webpage.

The webpage has instructions for installing tutch locally, if that is desired. However, most will find it easier to use the tutch installation available on CMU's andrew linux clusters, which can be found at the location `/afs/andrew/course/15/317/bin/tutch`. You may want to add `/afs/andrew/course/15/317/bin` to your `PATH`, as it allows you to use the `tutch` command directly, along with some other software we will be using later in the semester. Alternatively, you can run the command `/afs/andrew/course/15/317/317setup` if you are using a bash shell (if you don't know whether you're using bash, you are).

Exercises

Self-absorbed

Question: Prove $A \supset A$ *true*.

$$\cfrac{\cfrac{}{A\ \mathit{true}}\,u}{A \supset A\ \mathit{true}}\,{\supset}I^u$$

Maybe one is better than two

Question: Prove $A \wedge B \supset B$ *true*.

$$\cfrac{\cfrac{\cfrac{}{A \wedge B\ \mathit{true}}\,u}{B\ \mathit{true}}\,{\wedge}E_2}{A \wedge B \supset B\ \mathit{true}}\,{\supset}I^u$$

Some logical connectives too need to get to work

Question: Prove $A \wedge B \supset B \wedge A$ *true*.

$$\cfrac{\cfrac{\cfrac{\cfrac{}{A \wedge B\ \mathit{true}}\,u}{B\ \mathit{true}}\,{\wedge}E_2 \qquad \cfrac{\cfrac{}{A \wedge B\ \mathit{true}}\,u}{A\ \mathit{true}}\,{\wedge}E_1}{B \wedge A\ \mathit{true}}\,{\wedge}I}{A \wedge B \supset B \wedge A\ \mathit{true}}\,{\supset}I^u$$

A game

Question: Prove $A \wedge (A \supset B) \supset B$ *true*.

$$\cfrac{\cfrac{\cfrac{\cfrac{}{A \wedge (A \supset B)\ \mathit{true}}\,u}{A \supset B\ \mathit{true}}\,{\wedge}E_2 \qquad \cfrac{\cfrac{}{A \wedge (A \supset B)\ \mathit{true}}\,u}{A\ \mathit{true}}\,{\wedge}E_1}{B\ \mathit{true}}\,{\supset}E}{A \wedge (A \supset B) \supset B\ \mathit{true}}\,{\supset}I^u$$

Just passing through

Question: Prove $A \wedge (A \supset B) \wedge (B \supset C) \supset C$ *true*.

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{A \wedge (A \supset B) \wedge (B \supset C)\ \mathit{true}}\,u}{(A \supset B) \wedge (B \supset C)\ \mathit{true}}\,{\wedge}E_2}{B \supset C\ \mathit{true}}\,{\wedge}E_2 \qquad \cfrac{\cfrac{\cfrac{\cfrac{}{A \wedge (A \supset B) \wedge (B \supset C)\ \mathit{true}}\,u}{(A \supset B) \wedge (B \supset C)\ \mathit{true}}\,{\wedge}E_2}{A \supset B\ \mathit{true}}\,{\wedge}E_1 \qquad \cfrac{\cfrac{}{A \wedge (A \supset B) \wedge (B \supset C)\ \mathit{true}}\,u}{A\ \mathit{true}}\,{\wedge}E_1}{B\ \mathit{true}}\,{\supset}E}{C\ \mathit{true}}\,{\supset}E}{A \wedge (A \supset B) \wedge (B \supset C) \supset C\ \mathit{true}}\,{\supset}I^u$$

Begone!

Question: Prove $A \supset (B \supset A)$ *true*.

$$\cfrac{\cfrac{\cfrac{}{A\ \mathit{true}}\,u}{B \supset A\ \mathit{true}}\,{\supset}I^v}{A \supset (B \supset A)\ \mathit{true}}\,{\supset}I^u$$