

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 mathematics¹. 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. \square

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 $M \text{ nat}$ 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 $A \text{ true}$, which asserts (unsurprisingly) that the proposition A is a true statement. In the future, we will see other judgments which describe propositions,

¹For a nice and fun account of the history of logic, I absolutely recommend Logicomix.

²Actually, there is a whole field named *constructive mathematics* trying to express all mathematics in terms of constructive proofs.

³Around 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 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 :

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

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

$$\begin{array}{l} \text{Premises} \rightarrow \\ \text{Conclusion} \rightarrow \end{array} \frac{A \text{ true} \quad B \text{ true}}{A \wedge B \text{ true}} \wedge I \quad \leftarrow \text{Label}$$

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

$$\frac{\perp \text{ true} \quad \text{the moon is green true}}{\perp \wedge \text{the moon is green true}} \wedge I$$

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 true and B true, conclude $A \wedge B$ true”), while $\wedge E_1$ (“from $A \wedge B$ true, conclude A true”) and $\wedge E_2$ (“from $A \wedge B$ true conclude B true”) are elimination rules. The rules for \wedge match our intuition about the meaning of \wedge :

$A \wedge B$ true is provable iff⁴ A true is provable and B true is provable.

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

$A \vee B$ true is provable iff either A true is provable or B true is provable.

has interesting consequences.

Observe also that the introduction and elimination rules “fit together:” since we put in A true and B true to get $A \wedge B$ 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:

$$\frac{\frac{\frac{}{A \text{ true}} u \quad \vdots \quad B \text{ true}}{A \supset B \text{ true}} \supset I^u}{A \supset B \text{ true}} \supset E \quad \frac{A \supset B \text{ true} \quad A \text{ true}}{B \text{ true}} \supset E$$

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

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

is to assert that B true holds supposing that A true holds. (This hypothetical judgment can be written more compactly as $A \text{ true} \vdash B \text{ true}$.) In the $\supset I$ rule, we use the label u to name the assumption A true. Once we start constructing 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 $A \supset \perp$. 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 $A \supset A \wedge A$ *true* and $A \wedge A \supset A$ *true*:

$$\frac{\overline{A \text{ true}}^u}{A \supset A \text{ true}} \supset I^u \qquad \frac{\overline{A \text{ true}}^v \quad \overline{A \text{ true}}^v \quad \wedge I}{A \wedge A \text{ true}} \supset I^v$$

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 $B \supset B \wedge C$ *true*:

$$\frac{\overline{B \text{ true}}^x \quad C \text{ true} \quad \wedge I}{B \wedge C \text{ true}} \supset I^x$$

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

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

$$\frac{\overline{A \wedge A \text{ true}}^w \quad \wedge E_1}{A \text{ true}} \supset I^w \qquad \frac{\overline{A \wedge A \text{ true}}^w \quad \wedge E_2}{A \text{ true}} \supset I^w$$

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 $A \supset (A \supset A)$ *true*, which are distinguishable only by assumption labels:

$$\frac{\overline{A \text{ true}}^u \quad \supset I^v}{A \supset A \text{ true}} \supset I^u \qquad \frac{\overline{A \text{ true}}^v \quad \supset I^v}{A \supset A \text{ true}} \supset I^u$$

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 Proof Trees in SML

You will have to write proof trees for your homework in SML for easy autograding. The provided homework infrastructure allows you to print your proofs in the SMLNJ repl so that you may easily view your work. Below are some proof trees and their corresponding SML representations. We will also provide a web tool which allows you to input the lines of your proof, and gives an output of the SML code to represent it, since writing the code can get tedious. It is, however, good to understand how the proofs are represented in code regardless.

The last line in a coded proof should be the original judgment you are proving. When applying an inference rule, you use a dashed line followed by the name of the rule. The premises for a rule are represented by a list of judgments, each of which should have its own proof. The list of judgments precedes the dashed line and rule name, while the conclusion follows it. The list of judgments can be empty.

Note that \wedge in SML represents \wedge and $>$ represents \supset for these proof trees.

Self-absorbed

Question: Prove $A \supset A$ true.

$$\frac{\overline{A \text{ true}}^u}{A \supset A \text{ true}} \supset I^u$$

```
val taskA : proof =
[
  []
  ----- Hyp "u"
  tru A
]
----- ImpI "u"
tru A > B
```

Each judgment J in the proof tree takes the form tru J.

The dashed lines can be anywhere between 2 and 10 dashes long. The rule names that come after the dashed lines must be written as they are in these examples (for example, you may not use "Hypothesis" instead of "Hyp"). The rule names relevant to the first homework are:

- And introduction: AndI
- And elimination: AndE1 and AndE2
- Implication introduction: Hyp and ImpI
- Implication elimination: ImpE

On the homework, you would run `Out.print_proof HomeworkX.taskA` to view a clear version of your proof tree.

```
----- hyp_u
  A true
----- >I_u
A > A true
```

Maybe one is better than two

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

$$\frac{\frac{\overline{A \wedge B \text{ true}}^u}{B \text{ true}} \wedge E_2}{A \wedge B \supset B \text{ true}} \supset I^u$$

```
val taskB : proof =
[
  [
    [
      ----- Hyp "u"
      tru A ^ B
    ]
    ----- AndE2
    tru B
  ]
  ----- ImpI "u"
  tru A ^ B > B
```

Some logical connectives too need to get to work

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

$$\frac{\frac{\overline{A \wedge B \text{ true}}^u}{B \text{ true}} \wedge E_2 \quad \frac{\overline{A \wedge B \text{ true}}^u}{A \text{ true}} \wedge E_1}{\frac{B \wedge A \text{ true}}{A \wedge B \supset B \wedge A \text{ true}} \supset I^u} \wedge I$$

```
val taskC : proof =
[
  [
    [
      [
        [
          ----- Hyp "u"
          tru A ^ B
        ]
        ----- AndE2
        tru B,
        [
          [
            [
              ----- Hyp "u"
              tru A ^ B
            ]
            ----- AndE1
            tru A
          ]
          ----- AndI
          tru B ^ A
        ]
        ----- ImpI "u"
        tru A ^ B > B ^ A
      ]
    ]
  ]
```

You *may* find it neater to format the proof as follows:

```
val taskC : proof =
let
  val hyp_of_u =
    []
    ----- Hyp "u"
    tru A ^ B
in
  [
    [
      [hyp_of_u]
      ----- AndE2
      tru B,
      [hyp_of_u]
      ----- AndE1
      tru A
    ]
    ----- AndI
    tru B ^ A
  ]
  ----- ImpI "u"
  tru A ^ B > B ^ A
end
```

Here, in the use of the AndI rule, you see that with rules which contain more than one premise, the list of proofs of the premises contains more than one item.

Just passing through

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

$$\frac{\frac{\frac{A \wedge (A \supset B) \wedge (B \supset C) \text{ true}}{(A \supset B) \wedge (B \supset C) \text{ true}} \wedge E_2 \quad u}{B \supset C \text{ true}} \wedge E_2 \quad \frac{\frac{\frac{A \wedge (A \supset B) \wedge (B \supset C) \text{ true}}{(A \supset B) \wedge (B \supset C) \text{ true}} \wedge E_2 \quad u}{A \supset B \text{ true}} \wedge E_1}{B \text{ true}} \supset E \quad \frac{A \wedge (A \supset B) \wedge (B \supset C) \text{ true}}{A \text{ true}} \wedge E_1}{C \text{ true}} \supset E}{A \wedge (A \supset B) \wedge (B \supset C) \supset C \text{ true}} \supset I^u$$

```

val taskD : proof =
let
  val hyp_of_u =
    []
    ----- Hyp "u"
    tru A ^ (A > B) ^ (B > C)
  val sec1 =
    [hyp_of_u]
    ----- AndE2
    tru (A > B) ^ (B > C)
  val sec2 =
    [hyp_of_u]
    ----- AndE1
    tru A
in
  [
    [
      [sec1]
      ----- AndE2
      tru B > C,
      [
        [sec1]
        ----- AndE1
        tru A > B,
        sec2
      ]
      ----- ImpE
      tru B
    ]
    ----- ImpE
    tru C
  ]
  ----- ImpI "u"
  tru A ^ (A > B) ^ (B > C) > C
end

```

Begone!

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

$$\frac{\frac{\overline{A \text{ true}}^u}{B \supset A \text{ true}} \supset I^v}{A \supset (B \supset A) \text{ true}} \supset I^u$$

```
val taskE : proof =
  [
    [
      []
      ----- Hyp "u"
      tru A
    ]
    ----- ImpI "v"
    tru B > A
  ]
  ----- ImpI "u"
  tru A > (B > A)
```