

Logic and Formal Verification

Lecture notes

Jeremy Avigad

Version: June, 2009

Contents

1	Propositional logic	1
1.1	Natural deduction	1
1.2	Some propositional validities	5
1.3	Exercices	8
1.4	Using Isabelle	9
1.5	Exercices	11
1.6	A completeness proof	11
2	First-order logic	13
2.1	Quantifiers in natural deduction	13
2.2	Some first-order validities	14
2.3	Exercices	15
2.4	Quantifiers in Isabelle	16
2.5	Exercices	16
2.6	Equality and Isabelle's simplifier	17
2.7	First-order theories	18
2.8	Using Isabelle's automated tools	18
2.9	Exercices	19
2.10	Completeness for first-order logic	19
3	The natural numbers	21
3.1	Induction and recursion on the natural numbers	21
3.2	Exercices	23
3.3	The natural numbers in Isabelle	24
3.4	Exercices	25

Chapter 1

Propositional logic

1.1 Natural deduction

In this workshop, I will assume that you are familiar with the syntax and semantics of propositional and first-order logic. In other words, I will assume that you are able to read and write expressions in propositional and first-order logic, and understand what they mean. Henceforth, by “logic,” I mean classical logic.

In discussing propositional logic, I will take p, q, r, \dots to range over propositional variables, and $\varphi, \psi, \theta, \dots$ to range over formulas. It is common to take the basic connectives to be $\wedge, \vee, \rightarrow, \perp$. Additional connectives $\neg, \leftrightarrow, \top$ can be defined by

- $\neg\varphi \equiv \varphi \rightarrow \perp$
- $\top \equiv \neg\perp$
- $(\varphi \leftrightarrow \psi) \equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

In fact, in classical propositional logic, there is redundancy even in the original list: you can get by, for example, with \rightarrow and \perp alone.

I assume that you are familiar with truth-table semantics. A propositional formula φ is said to be *valid*, or a *tautology*, if φ is true under every assignment. This is written $\models \varphi$. More generally, if Γ is a set of formulas and φ is a formula, Γ *entails* φ , written $\Gamma \models \varphi$, if φ is true under every truth assignment that makes every formula in Γ true. For example, computing truth tables shows that the following hold:

- $\models p \wedge q \rightarrow q \vee r$

- $\{q, p \wedge r\} \models q \wedge r$

I will work through these examples in class.

The purpose of a proof system is to provide a system of rules which is sufficient to verify all valid formulas and entailments. We will use a system of *natural deduction*, due to Gerhard Gentzen. In this system, the basic object is a proof of a formula from some hypotheses; the rules of the system enable us to construct complex proofs from simpler ones. Rules are associated to each connective, characterizing its proper usage. In particular, for each logical connective we wish to have *introduction rules*, which tells us what is needed to justify an assertion involving this connective; and *elimination rules*, which tell what we may legitimately infer from such an assertion. For example, here are the rules for conjunction:

$$\frac{\varphi \quad \psi}{\varphi \wedge \psi} \wedge I \qquad \frac{\varphi \wedge \psi}{\varphi} \wedge E_1 \qquad \frac{\varphi \wedge \psi}{\psi} \wedge E_2$$

A key feature of natural deduction is that the notion of a proof from *hypotheses* is central, with the understanding that hypotheses can not only be introduced but also “cancelled” during a proof. So one should read the introduction rule for \wedge as follows: given a proof of φ from some hypotheses, and a proof of ψ from hypotheses, one obtains a proof of $\varphi \wedge \psi$ from the union of the two sets of hypotheses. The first elimination rule for \wedge says that given a proof of $\varphi \wedge \psi$ from some hypotheses, one obtains a proof of φ from the same set of hypotheses. These are the rules for implication:

$$\frac{\overline{\varphi} \quad \vdots \quad \psi}{\varphi \rightarrow \psi} \rightarrow I \qquad \frac{\varphi \rightarrow \psi \quad \varphi}{\psi} \rightarrow E$$

The introduction rule is the interesting one, since it involves cancelling a hypothesis. Informally, it says that in order to prove $\varphi \rightarrow \psi$, it suffices to assume φ and conclude ψ . The three dots suggest a proof of ψ in which the assumption φ can be used any number of times. In concluding $\varphi \rightarrow \psi$, this assumption is made explicit. In the resulting proof, then, φ is no longer an assumption; it has been “cancelled.” More precisely, then, the introduction rule for \rightarrow should be read as follows: given a proof of ψ from some hypotheses, which may include φ , one obtains a proof of $\varphi \rightarrow \psi$, from the same set of hypotheses *except* for the fact that φ may be cancelled.

The rules for disjunction are as follows:

$$\frac{\varphi}{\varphi \vee \psi} \vee I_1 \quad \frac{\psi}{\varphi \vee \psi} \vee I_2 \quad \frac{\begin{array}{c} \overline{\varphi} \quad \overline{\psi} \\ \vdots \quad \vdots \\ \varphi \vee \psi \quad \theta \quad \theta \end{array}}{\theta} \vee E$$

While the introduction rules are clear, the elimination rule may seem confusing. On reflection, however, it can be seen to model the natural process of proving θ from $\varphi \vee \psi$ by branching on cases: “Suppose $\varphi \vee \psi$. Case 1: φ holds. ... and θ follows. Case 2: ψ holds. ... and θ follows. Either way, we have θ .” Notice that in the resulting inference, the hypotheses φ and ψ are cancelled.

Finally, we add one last rule, *reductio ad absurdum*.

$$\frac{\begin{array}{c} \overline{\neg\varphi} \\ \vdots \\ \perp \end{array}}{\varphi}$$

This is the only rule that is not intuitionistically valid. (For intuitionistic logic, one replaces this rule with a weak rule, *ex falso sequitur quodlibet*, allowing us to derive any conclusion from \perp .)

Remembering that $\neg\varphi$ abbreviates $\varphi \rightarrow \perp$, the natural introduction and elimination rules for negation follow from the corresponding rules for implication:

$$\frac{\begin{array}{c} \overline{\varphi} \\ \vdots \\ \perp \end{array}}{\neg\varphi} \neg I \quad \frac{\begin{array}{c} \overline{\neg\varphi} \quad \varphi \\ \perp \end{array}}{\neg\varphi} \neg E$$

Similarly, we have the following derived rules for \leftrightarrow :

$$\frac{\begin{array}{c} \overline{\varphi} \quad \overline{\psi} \\ \vdots \quad \vdots \\ \psi \quad \varphi \end{array}}{\varphi \leftrightarrow \psi} \leftrightarrow I \quad \frac{\varphi \leftrightarrow \psi \quad \varphi}{\psi} \leftrightarrow E_1 \quad \frac{\varphi \leftrightarrow \psi \quad \psi}{\varphi} \leftrightarrow E_2$$

Don't confuse *reductio ad absurdum* with negation introduction (the former is not valid in intuitionistic logic, whereas the latter is). Of course, we need to have a rule with no hypotheses to get started. Here it is:

φ

This is called the *assumption rule*, and has a trivial reading: we can always prove φ , assuming φ as a hypothesis. The fact that this is an open hypothesis will be clear diagrammatically, because there is no line over φ ; if and when this hypothesis is cancelled, we put a line over it.

Reading a natural deduction proof can be difficult because hypotheses are introduced and cancelled at various times. In particular, it is useful to know at which points in a proof particular hypotheses have been cancelled. This information is conveyed by labelling the hypothesis and the point that it is cancelled with a letter x, y, z, \dots . For example, the following is a proof of $\psi \rightarrow (\varphi \wedge \psi)$ from hypothesis φ :

$$\frac{\varphi \quad \overline{\psi}^x}{\varphi \wedge \psi} \quad \frac{\varphi \wedge \psi}{\psi \rightarrow \varphi \wedge \psi} x$$

One more instance of \rightarrow I yields a proof of $\varphi \rightarrow (\psi \rightarrow \varphi \wedge \psi)$:

$$\frac{\frac{\overline{\varphi}^y \quad \overline{\psi}^x}{\varphi \wedge \psi} \quad \frac{\varphi \wedge \psi}{\psi \rightarrow \varphi \wedge \psi} x}{\varphi \rightarrow (\psi \rightarrow \varphi \wedge \psi)} y$$

There is some legalistic fine print associated with the implication introduction rule (similar considerations apply to disjunction elimination as well). Properly stated, the rule should be read as follows: “Given ψ , you may conclude $\varphi \rightarrow \psi$. Furthermore, if φ occurs as a hypothesis, you may cancel any instances of this hypothesis.” Note that you do not *need* the hypothesis φ to conclude $\varphi \rightarrow \psi$; if you know ψ outright, you know $\varphi \rightarrow \psi$. We need this flexibility, for example, to derive the first schema in our axiomatic proof systems:

$$\frac{\overline{\psi}^x}{\varphi \rightarrow \psi} \quad \frac{\varphi \rightarrow \psi}{\psi \rightarrow (\varphi \rightarrow \psi)} x$$

Furthermore, nothing is harmed if we leave some of the hypotheses open when we could have cancelled them; again, this only weakens the proof. With this convention in mind, note that the *ex falso* rule can be viewed as a special case of double-negation elimination.

It will be helpful to have a description of natural deduction that keeps track of the open hypotheses at each stage of the proof. A pair (Γ, φ) , where

Γ is a finite set of formulas and φ is a propositional formula, will formally be called a *sequent*, and will be written $\Gamma \Rightarrow \varphi$. Intuitively, this sequent should be read as the assertion that we have established φ from hypotheses in Γ . If Γ is a set of formulas and ψ is a formula, it is convenient to write Γ, ψ for $\Gamma \cup \{\psi\}$; and, more generally, it is convenient to leave off curly braces when listing the elements of a finite set. With this new mode of presentation, the natural deduction rules are expressed as follows:

$$\begin{array}{c}
 \frac{}{\Gamma, \varphi \Rightarrow \varphi} \text{Assumption} \\
 \\
 \frac{\Gamma \Rightarrow \varphi \quad \Gamma \Rightarrow \psi}{\Gamma \Rightarrow \varphi \wedge \psi} \wedge\text{I} \qquad \frac{\Gamma \Rightarrow \varphi_0 \wedge \varphi_1}{\Gamma \Rightarrow \varphi_i} \wedge\text{E}_i \\
 \\
 \frac{\Gamma \Rightarrow \varphi_i}{\Gamma \Rightarrow \varphi_0 \vee \varphi_1} \vee\text{I}_i \qquad \frac{\Gamma \Rightarrow \varphi \vee \psi \quad \Gamma, \varphi \Rightarrow \theta \quad \Gamma, \psi \Rightarrow \theta}{\Gamma \Rightarrow \theta} \vee\text{E} \\
 \\
 \frac{\Gamma, \varphi \Rightarrow \psi}{\Gamma \Rightarrow \varphi \rightarrow \psi} \rightarrow\text{I} \qquad \frac{\Gamma \Rightarrow \varphi \rightarrow \psi \quad \Gamma \Rightarrow \varphi}{\Gamma \Rightarrow \psi} \rightarrow\text{E} \\
 \\
 \frac{\Gamma, \neg\varphi \Rightarrow \perp}{\Gamma \Rightarrow \varphi} \text{RAA}
 \end{array}$$

One can show that if it is possible to prove $\Gamma \Rightarrow \varphi$ then it is possible to prove $\Gamma \cup \Delta \Rightarrow \varphi$ for any set Δ . This is known as “weakening” the set of hypotheses. In practice, it is more convenient to fold weakening into the rules by allowing any subset of Γ in the hypotheses. For example, the following proof tree witnesses $\vdash \varphi \rightarrow (\psi \rightarrow \varphi \wedge \psi)$:

$$\frac{\frac{\frac{\frac{}{\varphi \Rightarrow \varphi} \text{Ax} \quad \frac{}{\psi \Rightarrow \psi} \text{Ax}}{\varphi, \psi \Rightarrow \varphi \wedge \psi} \wedge\text{I}}{\varphi \Rightarrow \psi \rightarrow \varphi \wedge \psi} \rightarrow\text{I}}{\Rightarrow \varphi \rightarrow (\psi \rightarrow \varphi \wedge \psi)} \rightarrow\text{I}$$

1.2 Some propositional validities

Here are some propositional validities:

1. Commutativity of \wedge : $\varphi \wedge \psi \leftrightarrow \psi \wedge \varphi$
2. Commutativity of \vee : $\varphi \vee \psi \leftrightarrow \psi \vee \varphi$

3. Associativity of \wedge : $(\varphi \wedge \psi) \wedge \theta \leftrightarrow \varphi \wedge (\psi \wedge \theta)$
4. Associativity of \vee : $(\varphi \vee \psi) \vee \theta \leftrightarrow \varphi \vee (\psi \vee \theta)$
5. Distributivity of \wedge over \vee : $\varphi \wedge (\psi \vee \theta) \leftrightarrow (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$
6. Distributivity of \vee over \wedge : $\varphi \vee (\psi \wedge \theta) \leftrightarrow (\varphi \vee \psi) \wedge (\varphi \vee \theta)$
7. $(\varphi \rightarrow (\psi \rightarrow \theta)) \leftrightarrow (\varphi \wedge \psi \rightarrow \theta)$.
8. $(\varphi \rightarrow \psi) \rightarrow ((\psi \rightarrow \theta) \rightarrow (\varphi \rightarrow \theta))$
9. $((\varphi \vee \psi) \rightarrow \theta) \leftrightarrow (\varphi \rightarrow \theta) \wedge (\psi \rightarrow \theta)$
10. $\neg(\varphi \vee \psi) \leftrightarrow \neg\varphi \wedge \neg\psi$
11. $\neg(\varphi \wedge \psi) \leftrightarrow \neg\varphi \vee \neg\psi$
12. $\neg(\varphi \wedge \neg\varphi)$
13. $\neg(\varphi \rightarrow \psi) \leftrightarrow \varphi \wedge \neg\psi$
14. $\neg\varphi \rightarrow (\varphi \rightarrow \psi)$
15. $(\neg\varphi \vee \psi) \leftrightarrow (\varphi \rightarrow \psi)$
16. $\varphi \vee \perp \leftrightarrow \varphi$
17. $\varphi \wedge \perp \leftrightarrow \perp$
18. $\varphi \vee \neg\varphi$
19. $\neg(\varphi \leftrightarrow \neg\varphi)$
20. $(\varphi \rightarrow \psi) \leftrightarrow (\neg\psi \rightarrow \neg\varphi)$
21. $(\varphi \rightarrow \theta \vee \eta) \rightarrow ((\varphi \rightarrow \theta) \vee (\varphi \rightarrow \eta))$
22. $((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$

There is a simple heuristic for searching for proofs: work backwards from the goal using introduction rules, and work forwards from the hypothesis using elimination rules, until all the pieces come together. For example, here is a proof of the forward direction of (5):

$$\frac{\frac{\frac{\overline{\varphi \wedge (\psi \vee \sigma)}^y}{\psi \vee \sigma}}{\overline{\varphi \wedge (\psi \vee \sigma)}^y} \quad \frac{\frac{\frac{\overline{\varphi \wedge (\psi \vee \sigma)}^y}{\varphi} \quad \overline{\psi}^x}{\varphi \wedge \psi} \quad \frac{\frac{\overline{\varphi \wedge (\psi \vee \sigma)}^y}{\varphi} \quad \overline{\sigma}^x}{\varphi \wedge \sigma}}{(\varphi \wedge \psi) \vee (\varphi \wedge \sigma)} \quad \frac{\frac{\overline{\varphi \wedge (\psi \vee \sigma)}^y}{\varphi \wedge \psi} \quad \frac{\overline{\varphi \wedge (\psi \vee \sigma)}^y}{\varphi \wedge \sigma}}{(\varphi \wedge \psi) \vee (\varphi \wedge \sigma)}^x}{(\varphi \wedge (\psi \vee \sigma)) \rightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \sigma))}^y$$

Here is a proof of the forward direction of (7):

$$\frac{\frac{\overline{\varphi \rightarrow (\psi \rightarrow \theta)}^y}{\psi \rightarrow \theta} \quad \frac{\frac{\overline{\varphi \wedge \psi}^x}{\varphi} \quad \overline{\psi}^x}{\varphi \wedge \psi}}{\frac{\overline{\theta}}{\varphi \wedge \psi \rightarrow \theta}^x} \quad \frac{\overline{\varphi \wedge \psi}^x}{\psi}}{(\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow (\varphi \wedge \psi \rightarrow \theta)}^y$$

Here is a proof of the forward direction of (10):

$$\frac{\frac{\overline{\neg(\varphi \vee \psi)}^z}{\neg\varphi}^x \quad \frac{\overline{\neg(\varphi \vee \psi)}^z}{\varphi \vee \psi} \quad \frac{\overline{\neg(\varphi \vee \psi)}^z}{\varphi \vee \psi} \quad \frac{\overline{\psi}^y}{\varphi \vee \psi}}{\frac{\perp}{\neg\varphi}^x \quad \frac{\perp}{\neg\psi}^y} \quad \frac{\overline{\neg(\varphi \vee \psi)}^z}{\neg\varphi \wedge \neg\psi}}{\frac{\perp}{\neg(\varphi \vee \psi)}^z} \quad \frac{\perp}{\neg(\varphi \vee \psi)}^z$$

An extended heuristic is often needed to find proofs in classical logic. When all else fails, try a proof by contradiction: assume the negation of your goal, and aim for a contradiction.

For example, here is a proof of the law of the excluded middle:

$$\frac{\frac{\overline{\neg(\varphi \vee \neg\varphi)}^y}{\neg\varphi}^x \quad \frac{\overline{\neg(\varphi \vee \neg\varphi)}^y}{\varphi \vee \neg\varphi}}{\frac{\perp}{\neg\varphi}^x \quad \frac{\perp}{\neg(\varphi \vee \neg\varphi)}^x} \quad \frac{\perp}{\varphi \vee \neg\varphi}^y$$

Here is a proof of double-negation elimination:

$$\frac{\frac{\overline{\neg\neg\varphi}^y}{\neg\neg\varphi} \quad \overline{\neg\varphi}^x}{\frac{\perp}{\varphi}^x \quad (RAA)} \quad \frac{\perp}{\neg\neg\varphi \rightarrow \varphi}^y$$

Here are a couple additional examples of proofs:

$$\frac{\frac{\frac{\overline{\varphi} \ x \quad \overline{\neg\varphi} \ y}{\perp}}{\psi} \quad \overline{\psi} \ x}{\varphi \vee \psi} \ z}{\frac{\frac{\psi}{\neg\varphi \rightarrow \psi} \ y}{\varphi \vee \psi \rightarrow (\neg\varphi \rightarrow \psi)}} \ z$$

$$\frac{\frac{\overline{\neg(\varphi \wedge \neg\psi)} \ z \quad \frac{\overline{\varphi} \ y \quad \overline{\neg\psi} \ x}{\varphi \wedge \neg\psi}}{\frac{\perp}{\psi} \ x \text{ (RAA)}}}{\frac{\frac{\psi}{\varphi \rightarrow \psi} \ y}{\neg(\varphi \wedge \neg\psi) \rightarrow (\varphi \rightarrow \psi)}} \ z$$

1.3 Exercises

To get used to natural deduction, try finding natural-deduction proofs of any or all of the following.

1. $(\varphi \rightarrow (\psi \rightarrow \theta)) \rightarrow (\varphi \wedge \psi \rightarrow \theta)$.
2. $(\varphi \vee \psi) \vee \theta \rightarrow \varphi \vee (\psi \vee \theta)$
3. $\neg(\varphi \rightarrow \psi) \rightarrow \neg\psi$
4. $\neg(\varphi \rightarrow \psi) \rightarrow \varphi$
5. $(\neg\varphi \vee \psi) \leftrightarrow (\varphi \rightarrow \psi)$
6. $(\varphi \rightarrow \psi) \vee (\psi \rightarrow \varphi)$
7. $((\varphi \rightarrow \psi) \rightarrow \varphi) \rightarrow \varphi$
8. $\neg(\varphi \leftrightarrow \neg\varphi)$.

For more practice, you can use try to prove any of the validities in the last section.

1.4 Using Isabelle

Now let's start experimenting with Isabelle. If you are sitting at one of the machines in the clusters, you should log on to your Andrew account, and start a terminal console within the Xwindows environment. Then type `isabelle emacs` to start the system.

At this stage, you should consult all the following as references:

- The Isabelle tutorial, especially Sections 5.1–5.8, on propositional logic.
- The slides and exercises from the Brucker et al. course.
- The list of propositional rules on the “Propositional Logic” exercise.
- The list of ASCII equivalents for logical symbols in Isabelle.
- Henry Towsner’s useful “cheat sheet” of Isabelle commands.

In class, I will discuss:

- The Isabelle interface, the structure of an Isabelle theory, and Isabelle syntax.
- The propositional rules.
- The difference between `rule`, `frule`, `drule`, and `erule`.

I will also through some examples in class.

Roughly, use the “rule” tactic to apply an introduction rule to the conclusion of a sequent. For example, suppose your goal is the conclusion of the introduction rule for “and”:

$$\frac{\Gamma \Rightarrow \varphi \quad \Gamma \Rightarrow \psi}{\Gamma \Rightarrow \varphi \wedge \psi}$$

Typing the command `apply (rule conjI)` reduces that goal to the two subgoals corresponding to the hypotheses. Similarly, `apply (rule impI)` allows you to prove an implication by assuming the hypothesis and deriving the conclusion:

$$\frac{\Gamma, \varphi \Rightarrow \psi}{\Gamma \Rightarrow \varphi \rightarrow \psi}$$

Generally speaking, the “rule” tactic is used to run an introduction rule backwards, reducing the task of proving the conclusion to the task of proving the hypotheses.

In the other direction, the “frule” tactic allows you to work forwards from hypotheses. For example, `apply (frule conjunct1)` runs the following rule in reverse:

$$\frac{\Gamma, \varphi \wedge \psi, \varphi \Rightarrow \theta}{\Gamma, \varphi \wedge \psi \Rightarrow \theta}$$

Similarly, the command `apply (frule conjunct2)` extracts ψ :

$$\frac{\Gamma, \varphi \wedge \psi, \psi \Rightarrow \theta}{\Gamma, \varphi \wedge \psi \Rightarrow \theta}$$

In other words, these rule “unpack” a hypothesis so you can use it. The command `apply (drule ...)` does the same thing, except it deletes the hypothesis afterwards, eliminating clutter. (The “d” stands for “destruct.”)

The final variant of the rule tactic, “erule,” is probably the most confusing. The “e” stands for “elimination.” Try this variant when you want to use a hypothesis, but the use of the hypothesis involves more than simply “working forwards.” For example, the command `apply (erule disjE)` runs the following rule in reverse:

$$\frac{\Gamma, \varphi \Rightarrow \theta \quad \Gamma, \psi \Rightarrow \theta}{\Gamma, \varphi \vee \psi \Rightarrow \theta}$$

This is a “proof” by cases: to prove θ from the assumption $\varphi \vee \psi$, first show that θ follows from φ , and then show that it follows from ψ .

The rules for using an implication in a hypothesis can be confusing. The command `apply (erule impE)` runs the following rule in reverse:

$$\frac{\Gamma \Rightarrow \varphi \quad \Gamma, \psi \Rightarrow \theta}{\Gamma, \varphi \rightarrow \psi \Rightarrow \theta}$$

This enables you to make use of a hypothesis $\varphi \rightarrow \psi$; after applying the rule, you then only need to prove φ , after which you can use ψ as a hypothesis. You can also experiment with the rule “mp” (for “modus ponens”), which has a different behavior.

Working with propositional rules is fun, but it can get tedious after a while. The good news is that Isabelle can handle propositional logic automatically, without working up a sweat: any propositionally valid sequent can be verified using the tactics `auto` or `blast`. But the low-level rules are useful in more complex settings, when you have to do fine-tuned manipulation by hand; so it pays to get used to them.

1.5 Exercises

Now it is time for you to try it out! You can practice on any of the propositional validities in the sections above. You can find solutions to all of the following in the Brucker et al. exercises:

- $A \rightarrow (B \rightarrow A)$
- $A \wedge B \rightarrow B \wedge A$
- $A \wedge B \rightarrow B \vee A$
- $A \vee B \rightarrow B \vee A$
- $A \wedge (B \wedge C) \rightarrow A \wedge C$
- $(A \rightarrow B \rightarrow C) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$
- $(A \wedge B) \vee C \rightarrow (A \vee C) \wedge (B \vee C)$
- $(\neg Q \rightarrow P) \rightarrow P \vee Q$
- $\neg P \vee P$
- $((A \rightarrow B) \rightarrow A) \rightarrow A$

You can also try the “Propositional logic” set from the Isabelle/HOL exercises.

1.6 A completeness proof

By now you may be convinced that Isabelle’s rules will allow you to verify any propositional tautology. But how do you know that this is the case? This is exactly what a *completeness* proof is supposed to establish.

Here I will briefly sketch a proof that any valid sequent is provable, or, equivalently, that if a sequent is not valid, there is a truth assignment that makes the hypotheses true but the conclusion false. First, verify that Isabelle’s rules are enough to show that any sequent $\Gamma \Rightarrow \varphi$ is equivalent to $\Gamma, \neg\varphi \Rightarrow \perp$, and $\Gamma \Rightarrow \neg\varphi$ is equivalent to $\Gamma, \varphi \Rightarrow \perp$. In other words, we can use Isabelle’s rules to go back and forth between the sequents in each pair. Since Isabelle can also show that $\neg\neg\varphi$ is equivalent to φ , we never have to deal with more than one negation at the top level. And the previous observation means that we can always remove a negation by moving it to the other side of the sequent.

The strategy behind the proof of completeness is to show that we can unwrap all the other connectives until we are reduced to sequents that have only propositional variables, negations of propositional variables, \perp , and \top . But then it is easy to see that if such a sequent is not provable by the “assumption” rule, it is not valid.

The following rules let us “unwrap” a connective on the right side of a sequent:

$$\frac{\Gamma \Rightarrow \varphi \quad \Gamma \Rightarrow \psi}{\Gamma \Rightarrow \varphi \wedge \psi}$$

$$\frac{\Gamma, \neg\varphi, \neg\psi \Rightarrow \perp}{\Gamma \Rightarrow \varphi \vee \psi}$$

$$\frac{\Gamma, \varphi \Rightarrow \psi}{\Gamma \Rightarrow \varphi \rightarrow \psi}$$

In other words, in each case Isabelle’s rules allow us to derive the conclusion from the hypotheses, and if the conclusion is not valid, then one of the hypothesis is necessary invalid as well. The following rules to the same for connectives on the left:

$$\frac{\Gamma, \varphi, \psi \Rightarrow \theta}{\Gamma, \varphi \wedge \psi \Rightarrow \theta}$$

$$\frac{\Gamma, \varphi \Rightarrow \theta \quad \Gamma, \psi \Rightarrow \theta}{\Gamma, \varphi \vee \psi \Rightarrow \theta}$$

$$\frac{\Gamma, \neg\varphi \Rightarrow \theta \quad \Gamma, \psi \Rightarrow \theta}{\Gamma, \varphi \rightarrow \psi \Rightarrow \theta}$$

We need only iterate this unwrapping, moving formulas from side to side of the sequent as necessary, until all the connectives other than negation have been eliminated. In fact, this is how tactics like `auto` and `blast` achieve completeness.

Chapter 2

First-order logic

2.1 Quantifiers in natural deduction

As a model for mathematical reasoning, propositional logic is too limited. First-order logic does much better in that respect. One specifies a first-order *language* by giving a list of function and relation symbols of various arities. These determine a set of *terms*, that is, syntactic expressions that name elements in an intended domain interpretation, and *formulas*, that is, expressions that make assertions about that domain. In class, I will discuss the syntax of first-order logic briefly, and the notion of free and bound variables. Hopefully, this will be review for most of you.

First, some notation. If φ is any formula, t is a term, and x is a variable, $\varphi[t/x]$ denotes the result of substituting t for x in φ . Such a substitution causes problems when one of the variables of t is captured by a bound variable in φ , so let us adopt the convention that when I write $\varphi[t/x]$, I mean that this is not one of those “bad” substitutions. It is often convenient to introduce a formula is “ $\varphi(x)$ ”, after which $\varphi(t)$ abbreviates $\varphi[t/x]$.

To extend our systems of natural deduction to first-order logic, add the following rules:

$$\frac{\varphi}{\forall y \varphi[y/x]} \forall I \qquad \frac{\forall x \varphi}{\varphi[t/x]} \forall E$$

where in the introduction rule, we require that x is not free in any open hypothesis, corresponding to the eigenvalue condition above; and we assume that y is not a free variable of φ , unless $y = x$. Similarly, we have the rules for the existential quantifier:

$$\frac{\frac{\varphi[t/x]}{\exists y \varphi} \exists I}{\frac{\frac{\overline{\varphi[x/y]}}{\vdots} \psi}{\exists y \varphi} \exists E} \psi \exists E$$

where again, in the elimination rule, we assume that x is not free in ψ or any hypothesis other than $\varphi[x/y]$, and x is not free in φ unless $x = y$. The elimination rule exhibits a pattern of reasoning that is similar to that of disjunction elimination: to show that ψ holds on assumption $\exists x \varphi$, let y be an “arbitrary” object satisfying $\varphi[y/x]$, and show that ψ follows. Note that the universal introduction and existential elimination rules allow you to rename the quantified variable.

In sequent form, the natural deduction rules are expressed as follows:

$$\frac{\Gamma \Rightarrow \varphi}{\Gamma \Rightarrow \forall y \varphi[y/x]} \forall I \qquad \frac{\Gamma \Rightarrow \forall x \varphi}{\Gamma \Rightarrow \varphi[t/x]} \forall E$$

$$\frac{\Gamma \Rightarrow \varphi[t/x]}{\Gamma \Rightarrow \exists x \varphi} \exists I \qquad \frac{\Gamma \Rightarrow \exists y \varphi[y/x] \quad \Gamma, \varphi \Rightarrow \psi}{\Gamma \Rightarrow \psi} \exists E$$

with the same restrictions above.

2.2 Some first-order validities

Once again, let’s consider some valid formulas, and examples of proofs.

1. $\forall x \varphi \leftrightarrow \varphi$ if x is not free in φ
2. $\exists x \varphi \leftrightarrow \varphi$ if x is not free in φ
3. $\forall x (\varphi \wedge \psi) \leftrightarrow \forall x \varphi \wedge \forall x \psi$
4. $\exists x (\varphi \wedge \psi) \leftrightarrow \exists x \varphi \wedge \psi$ if x is not free in ψ
5. $\exists x (\varphi \vee \psi) \leftrightarrow \exists x \varphi \vee \exists x \psi$
6. $\forall x (\varphi \vee \psi) \leftrightarrow \forall x \varphi \vee \psi$ if x is not free in ψ
7. $\forall x (\varphi \rightarrow \psi) \leftrightarrow (\exists x \varphi \rightarrow \psi)$ if x is not free in ψ
8. $\exists x (\varphi \rightarrow \psi) \leftrightarrow (\forall x \varphi \rightarrow \psi)$ if x is not free in ψ
9. $\forall x (\varphi \rightarrow \psi) \leftrightarrow (\varphi \rightarrow \forall x \psi)$ if x is not free in φ

10. $\exists x (\varphi \rightarrow \psi) \leftrightarrow (\varphi \rightarrow \exists x \psi)$ if x is not free in ψ
11. $\exists x \varphi \leftrightarrow \neg \forall x \neg \varphi$
12. $\forall x \varphi \leftrightarrow \neg \exists x \neg \varphi$

For example, assuming x is not free in ψ , here is a proof of the forward direction of (4):

$$\frac{\frac{\frac{\overline{\varphi \wedge \psi}^x}{\varphi}}{\exists x \varphi} \quad \frac{\overline{\varphi \wedge \psi}^x}{\psi}}{\exists x (\varphi \wedge \psi)} \quad \frac{\overline{\varphi \wedge \psi}^x}{\psi}}{\exists x \varphi \wedge \psi} \quad x}{\frac{\exists x \varphi \wedge \psi}{\exists x (\varphi \wedge \psi) \rightarrow \exists x \varphi \wedge \psi} \quad y} \quad y$$

Here is proof of the converse direction:

$$\frac{\frac{\overline{\exists x \varphi \wedge \psi}^y}{\exists x \varphi} \quad \frac{\overline{\varphi}^x \quad \frac{\overline{\exists x \varphi \wedge \psi}^y}{\psi}}{\varphi \wedge \psi}}{\exists x (\varphi \wedge \psi)} \quad x}{\frac{\exists x (\varphi \wedge \psi)}{\exists x \varphi \wedge \psi \rightarrow \exists x (\varphi \wedge \psi)} \quad y} \quad y$$

2.3 Exercises

1. Try to give some examples of what can go wrong when eigenvariable conditions in the quantifier rules are violated.
2. Prove the following equivalence:

$$\exists x (\varphi \rightarrow \psi) \leftrightarrow (\forall x \varphi \rightarrow \psi)$$

assuming x is not free in ψ . One direction is difficult, in that it requires classical logic.

3. Here are some more examples to try:

- (a) $\forall x (\varphi \rightarrow \psi) \rightarrow (\forall x \varphi \rightarrow \forall x \psi)$
- (b) $\forall x \varphi \rightarrow \exists x \varphi$

- (c) $\exists x \varphi \leftrightarrow \neg \forall x \neg \varphi$
- (d) $(\varphi \rightarrow \exists x \psi) \leftrightarrow \exists x (\varphi \rightarrow \psi)$, if x is not free in φ (independence of premise)
4. Suppose I tell you that, in a town, there is a (male) barber that shaves all and only the men who do not shave themselves. Formalize this claim, and show, in minimal logic, that it implies a contradiction.
 5. Prove some of the other validities in the last section.

2.4 Quantifiers in Isabelle

At this point, you should refer to:

- Section 5.9 in the tutorial.
- The corresponding lectures and exercises in the Brucker et al. course.

In class, I will discuss:

- Isabelle syntax for relation and quantifiers. For example, note that one writes Pxy instead of $P(x, y)$, and in an expression like $\forall x. Px \vee Qx$ the quantifier is given the widest scope possible.
- Isabelle's type system. For example, the annotation $(x : \text{nat})$ indicates that x ranges over natural numbers; different constants in an expression can have different types, and Isabelle is good at inferring types implicitly from the context.
- Isabelle's quantifier rules (including the variants that let you choose an explicit instantiation for terms).

I will present some examples of proofs.

2.5 Exercises

As suggested in the tutorial, try proving $\exists x . P \wedge Q(x) \Rightarrow P \wedge (\exists x . Q(x))$ in Isabelle. Note that here I am switching to Isabelle syntax for quantifiers, as described in the previous section.

The following exercises are all worked out in the Brucker et al. course:

1. $(\forall x. Px) \rightarrow (\exists x. Px)$

2. $(\forall x. Px) \vee (\forall x. Qx) \rightarrow (\forall x. Px \vee Qx)$
3. $((\forall x. Px) \wedge (\forall x. Qx)) \leftrightarrow (\forall x. Px \wedge Qx)$
4. $(\exists x. \forall y. Pxy) \rightarrow (\forall y. \exists x. Pxy)$
5. $(\exists x. P(fx)) \rightarrow (\exists x. Px)$
6. $(\forall x. A \rightarrow Bx) \leftrightarrow (A \rightarrow \forall x. Bx)$

Can you prove the converse direction to 2?

Do also the “Predicate Logic” and “Rich Grandfather” problem sets in the Isabelle/HOL exercises.

2.6 Equality and Isabelle's simplifier

The nature of the equality relation has traditionally posed a host of philosophical and logical puzzles, but at least in the context of first-order logic, the appropriate treatment is straightforward. First, we need to express that equality is an *equivalence relation*, namely, it is reflexive, symmetric, and transitive; and second, we need to express that it is a *congruence* with respect to the function and relation symbols in the language. In systems of natural deduction, this amounts to the following rules:

$$\frac{}{t = t} \quad \frac{s = t}{t = s} \quad \frac{r = s \quad s = t}{r = t}$$

$$\frac{\bar{s} = \bar{t}}{f(\bar{s}) = f(\bar{t})} \quad \frac{\bar{s} = \bar{t} \quad R(\bar{s})}{R(\bar{t})}$$

From these, one can derive the more general rules for arbitrary terms and formulas:

$$\frac{\bar{r} = \bar{s}}{t(\bar{r}) = t(\bar{s})}$$

and

$$\frac{\bar{s} = \bar{t} \quad \theta(\bar{s})}{\theta(\bar{t})}$$

For pragmatic purposes, it is more useful to include these generalizations among the basic rules.

Dealing with equality in the context of a proof assistant can be painful. At this stage, you should consult Section 5.8 in the tutorial. In class, I will discuss Isabelle's equality rules (most notably **subst** and **ssubst**, as well as **trans**), as well as the *subst* tactic, which make it possible to carry out calculations “by hand.” I will do some examples.

2.7 First-order theories

There are two ways first-order logic can be used:

- To reason about a particular structure, like the natural numbers, the real numbers, the universe of sets, etc.
- To reason about a class of structures, like groups, rings, linear orders, and so on.

Note that there is no *theoretical* difference between the two: in either case, one writes down some axioms and reasons about their consequences. In class, I will discuss first-order axiomatizations of the following:

- Orderings (partial orders, linear orders, and so on).
- Algebraic structures, like groups, rings, and fields.
- The natural numbers.
- The real numbers.

In Isabelle/HOL, one can reason about such axiomatic structures by defining an “axiomatic type class.” I will explain how this works. If you go to the Isabelle/HOL theory on the web, you can find, for example, various orderings axiomatized in the file “Orderings”, and you can various algebraic structures axiomatized in “OrderedGroup” and “Ring-and-Field”.

Note that in ordinary mathematics, we do much more than, say, prove first-order consequences of the group axioms. We often want to reason about subsets of a group, or functions from one group to another, or functions from a group to the natural numbers, and so on. In fact, Isabelle/HOL is good at this sort of thing. “HOL” stands for “higher-order logic.” This means that whenever we have domains A and B , we can also reason about the domain $A \Rightarrow B$ of all functions from A to B , the domain *set* A of all subsets of A , and more. But we will have to come back to that later; in the exercises below, we will focus on first-order consequences of our axioms.

2.8 Using Isabelle’s automated tools

Soon we will want to move on to bigger and better things, and let Isabelle’s automated tools handle piddling logical inferences. These, and other tricks of the trade, are discussed at the end of Chapter 5 of the tutorial, as well as the beginning of Chapter 3. In class, I will discuss some of the automated tools, including:

- The simplifier: `simp`
- The automated reasoner: `auto`, `blast`, and relatives
- Linear arithmetic: `arith`

I will also discuss some useful tricks of the trade, including:

- `insert`
- `subgoal-tac`
- The “find theorems” command.

2.9 Exercises

Once again, an exercise from Brucker et al.: prove

$$s(s(s(s\ zero))) = four \wedge P\ zero \wedge (\forall x. Px \rightarrow P(s(s\ x))) \rightarrow P\ four.$$

Do this by hand, using the explicit rules for propositional logic and equality, and `subgoal-tac`. Then try `auto`!

Prove that in any commutative ring (axiomatic class `comm-ring` in Isabelle), the following holds:

$$(x + y) * (x + y) = x * x + x * y + x * y + y * y$$

First, try doing this by hand, using explicit equality rules. Then try it using the simplifier and `ring-simps`. Do the same for the identity:

$$(-x) * (-y) = xy.$$

2.10 Completeness for first-order logic

Recall that when it came to propositional logic, we had a notion of what it means for a formula to be true under a particular truth assignment to its variables; we were then able to say that a formula is *valid* if and only if it is true under all truth assignments. When it comes to first-order logic, instead of truth assignments, we speak of *models*. A first-order sentence is then said to be *valid* if it is true in all models. The notion of entailment lifts to first-order logic in a similar way. Just as for propositional logic, one can show that Isabelle’s first-order rules are complete.

In contrast to first-order logic, however, there is no algorithm that will decide whether or not a given sentence is valid. There is a “semi-decision procedure”: given a sentence, one can search systematically for a proof in a first-order deductive calculus. If the sentence is valid, the search will terminate; but there is no general method for detecting when one should give up, in situations when the sentence turns out to be invalid. This means, in particular, that Isabelle’s automated tools can sometimes fall into infinite searches, in which case, you need to terminate them by hand.

Chapter 3

The natural numbers

3.1 Induction and recursion on the natural numbers

Let N be the set of natural numbers, with least element 0, and let $s(x) = x + 1$ be the successor function. From a foundational standpoint, $(N, 0, s)$ is characterized uniquely, up to isomorphism, by the following clauses:

- $0 \neq s(x)$ for any x in N .
- For every x and y in N , if $x \neq y$, then $s(x) \neq s(y)$. In other words, s is *injective*.
- If A is any subset of N with the property that 0 is in A and whenever x is in A then $s(x)$ is in A , then $A = N$.

The last clauses can be reformulated as the principle of induction:

Suppose $P(x)$ is any property of natural numbers, such that P holds of 0, and for every x , $P(x)$ implies $P(s(x))$. Then every P holds of every natural number.

This principle can be used to justify definitions by *primitive recursion*:

Let X be any set, a be any element of X , and let g be any function from X to X . Then there is a unique function $f : N \rightarrow X$ satisfying the following two clauses:

- $f(0) = a$
- $f(s(x)) = g(f(x))$ for every x in N .

For example, one can define addition with the following two clauses:

$$\begin{aligned}x + 0 &= x \\x + s(y) &= s(x + y)\end{aligned}$$

Having done so, one can define multiplication using the following two clauses:

$$\begin{aligned}x \cdot 0 &= 0 \\x \cdot s(y) &= x \cdot y + x\end{aligned}$$

One can also define a predecessor function by

$$\begin{aligned}p(0) &= 0 \\p(s(x)) &= x.\end{aligned}$$

With these definitions and the induction principle, and can prove all the following identities:

1. $x \neq 0 \rightarrow s(p(x)) = x$
2. $0 + x = x$
3. $1 + x = s(x)$, where 1 is defined to be $s(0)$
4. $0 \cdot x = 0$
5. $1 \cdot x = x$
6. $(x + y) + z = x + (y + z)$
7. $x + y = y + x$
8. $(xy)z = x(yz)$
9. $xy = yx$
10. $x(y + z) = xy + xz$

You can find proofs in the excerpt from Stewart and Tall; I will go over some of them in class. One can proceed to define $<$, truncated subtraction, exponentiation, factorial, and so, and show they they have the desired properties. One can then define divisibility, greatest common divisor, primality, and more.

The remarkable thing is that everything traces back to the principle of induction and definition by recursion. In practice, it is useful to justify a more flexible form of induction:

Let P be any property of natural numbers. To show that $P(x)$ holds for every x , it suffices to show that for every x , if P holds of every number smaller than x , then P holds of x as well.

It is also useful to have a more flexible form of recursion:

Let X be any set, let m be any function from X to N that assigns a “measure” to each element of x . Then one can define a function f from X to any set Y by specifying $f(x)$ in terms of the value of f on elements having a smaller measure.

I will give two examples in class: fibonacci numbers, and the gcd function.

3.2 Exercises

Most of the exercises that follow are taken from the excerpt from Stewart and Tall.

Prove the properties of addition and multiplication above. Define exponentiation recursively, and prove the following:

- $x^{y+z} = x^y x^z$
- $x^{yz} = (x^y)^z$
- $(xy)^z = x^z y^z$

Note that exponentiation x^y makes sense, more generally, when x is any element of an ordered ring and y is any natural number.

Prove the following identities by induction:

- $1 + 2 + \dots + n = \frac{1}{2}n(n + 1)$
- $1^2 + 2^2 + \dots + n^2 = \frac{1}{6}n(n + 1)(2n + 1)$
- $1^3 + 2^3 + \dots + n^3 = \frac{1}{4}n^2(n + 1)^2$
- $1 + 3 + 5 + \dots + (2n - 1) = n^2$

Define the factorial function in the usual way, and define

$$\binom{n}{r} = \frac{n!}{(n-r)!r!}$$

This is the number of ways of choosing r elements out of n . Show that

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{r} = \binom{n}{n-r}$$

and

$$\binom{n}{r} + \binom{n}{r-1} = \binom{n+1}{r}$$

Using the last equality, prove the *binomial theorem*: for every a and b ,

$$(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i}$$

Note that this makes sense, more generally, for elements a and b in any commutative ring. Show also

- $1 \cdot 1! + 2 \cdot 2! + \dots + n \cdot n! = (n+1)! - 1$
- $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$
- $\binom{n}{1} + 2\binom{n}{2} + \dots + n\binom{n}{n} = 2^{n-1}n$

Here is a tricky one. Define the Fibonacci numbers by

$$F_0 = F_1 = 1, F_{n+2} = F_{n+1} + F_n.$$

In 1680, Gian Domenico Cassini published the identity

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^{n+1}.$$

Prove this by induction.

More identities involving $\binom{n}{r}$ and Fibonacci numbers can be found in Graham, Knuth, and Patashnik's book, *Concrete Mathematics*.

3.3 The natural numbers in Isabelle

You should not be surprised to learn that Isabelle/HOL includes an axiomatic development of the natural numbers, which allows you to perform proofs by induction and to define functions by recursion. I will discuss this in class. You can also consult Sections 2.5 and 3.5., and the slides on the natural numbers in the Brucker et al. lectures.

When it comes to proving things by induction, Isabelle's automated tools, `auto`, `simp`, and `arith` can be quite powerful. You can even use Isabelle as a desk calculator; try stating the "theorem" $12345 * 6789 = ?x$ and applying `simp`.

3.4 Exercises

Starting with `Suc` only, in Isabelle, give primitive recursive definitions of the functions

- $plus(x, y) = x + y$
- $mult(x, y) = x * y$
- $exp(x, y) = x^y$

For example, here are definitions of *plus*, and the predecessor function:

```
theory Temp
imports Main
begin

consts
  pred :: "nat => nat"
  plus :: "nat => nat => nat"

primrec
  pred_0:   "pred 0 = 0"
  pred_Suc: "pred (Suc x) = x"

primrec
  plus_0:   "plus x 0 = x"
  plus_Suc: "plus x (Suc y) = Suc (plus x y)"
```

The corresponding definitions of *mult* and *exp* are left to you. Note that you can refer to the defining clauses by name; so, for example, you can simplify with the theorem `plus_0`.

Now use induction to verify their basic properties. Of course, the Isabelle libraries already contain definitions of `+` and `*`; this exercise will give you a sense of how their properties were verified by those who designed the library.

For the next few exercises, use the ordinary built-in functions on the natural numbers to verify the summation identities in Section 3.2. (It's much simpler if you multiply through to get equivalent identities without the division symbol.) Most of the calculations can be done automatically; it helps to use `ring-simps` to simplify expressions, as well as `power2-eq-square` and `power3-eq-cube` to expand squares and cubes, respectively.

Use the Isabelle `fun` mechanism to define the sequence of Fibonacci numbers, as a function from the natural numbers to the integers:

```
fun fib :: "nat => int"
where
  "fib 0 = 1"
| "fib (Suc 0) = 1"
| "fib (Suc (Suc n)) = fib (Suc n) + fib n"
```

Then verify Cassini's identity, from the last section:

```
theorem "fib (Suc (Suc n)) * fib n - (fib (Suc n))^2 = (-1)^n"
```

You can find notation for finite sums in the file `FiniteSet`, and definitions of the binomial coefficients in the file `Binomial`. Try then formalizing the various exercises in the section before last.

Also, try the “Power, Sum” and “Magical Methods” problem sets in the Isabelle/HOL Exercises.