Logic for Computer Science - Week 5
Natural Deduction

Ștefan Ciobâcă

November 30, 2017

1 An Alternative View of Implication and Double Implication

So far, we have understood $\varphi \rightarrow \varphi'$ as a shorthand of $\neg\varphi \vee \varphi'$. However, there is an alternative view that is equally correct.

In the alternative view, we note that the set PL of propositional formulae depends on a set C of connectives. Our definition so far was that the set of connectives is $C = \{\vee, \wedge, \neg\}$.

The alternative definition is that there exist several logics PL_C, where $C \subseteq \{\vee, \wedge, \neg, \rightarrow, \leftrightarrow, \bot, \top\}$. The new connectives $\bot$ and $\top$ are nullary connectives, in that they do not take any arguments ($\neg$ is unary, the other are binary). In fact, $\bot$ is a formula that is false in any truth assignment and $\top$ is a formula that is true in any truth assignment.

Definition 1.1. *Let $C \subseteq \{\vee, \wedge, \neg, \rightarrow, \leftrightarrow, \bot, \top\}$ be a set of logical connectives. The set PL_C of propositional formulae with connectives in C is the only set of strings that:*

1. *(Base case) $A \subseteq PL_C$ (any propositional variable is a formula);*
2. *(Inductive case) if $\varphi, \varphi' \in PL_C$, then:*
   (a) *if $\neg \in C$, then $\neg\varphi \in PL_C$;*
   (b) *if $\vee \in C$, then $(\varphi_1 \vee \varphi_2) \in PL_C$;*
   (c) *if $\wedge \in C$, then $(\varphi_1 \wedge \varphi_2) \in PL_C$;*
   (d) *if $\rightarrow \in C$, then $(\varphi_1 \rightarrow \varphi_2) \in PL_C$;*
   (e) *if $\leftrightarrow \in C$, then $(\varphi_1 \leftrightarrow \varphi_2) \in PL_C$;*
   (f) *if $\bot \in C$, then $\bot \in PL_C$;*
   (g) *if $\top \in C$, then $\top \in PL_C$;*
3. *(Minimality Condition) No other string belongs to PL_C.*

We adopt the previous rules regarding brackets. All existing definitions (truth assignment, satisfiability, equivalence, etc) can be carried over easily to the new definition of formulae. Note that $\hat{\tau}(\varphi \to \varphi') = \overline{\hat{\tau}\Big(\varphi\Big)} + \hat{\tau}\varphi'$, $\hat{\tau}\Big(\bot\Big) = 0$ and $\hat{\tau}\Big(\top\Big) = 1$ for any truth assignment τ and any formulae $\varphi, \varphi' \in PL_C$.

We retrieve our previous definition of PL by setting $C = \{\neg, \wedge, \vee\}$. That is, $PL = PL_{\{\neg,\wedge,\vee\}}$.

Definition 1.2. *A set C of connectives is adequate if for any formula $\varphi \in PL$, there exists a formula $\varphi' \in PL_C$ such that $\varphi \equiv \varphi'$.*

For example, $C = \{\vee, \neg\}$ is adequate, since we can get rid of $\wedge$ using the equivalence $\neg(\varphi_1 \wedge \varphi_2) \equiv \neg\varphi_1 \vee \neg\varphi_2$.

The set $C = \{\wedge, \neg\}$ is also adequate.

However, the set $C = \{\wedge, \vee\}$ is not adequate, since there is no formula $\varphi \in PL_C$ equivalent to $\neg p$.

Exercise 1.1. *Show that $C = \{\to, \bot\}$ is adequate (hint: show that any connective can be expressed using just $\to$ and $\bot$).*

2 Natural Deduction

Natural deduction is our first example of proof system. Proof systems are abundent in theoretical computer science and it is important to get a good understanding of them.

2.1 Motivation

Suppose you had to show that $p \vee q, \neg p \models q$. You could proceed as follows: suppose τ is a truth assignment such that $\hat{\tau}\Big(p \vee q\Big) = 1$ and that $\hat{\tau}\Big(\neg p\Big) = 1$. We show that $\hat{\tau}\Big(q\Big) = 1$. But $1 = \hat{\tau}\Big(\neg p\Big) = \overline{\hat{\tau}\Big(p\Big)}$ and so $\hat{\tau}\Big(o\Big) = 0$. We also have that $1 = \hat{\tau}\Big(p \vee q\Big) = \hat{\tau}\Big(p\Big) + \hat{\tau}\Big(q\Big) = 0 + \hat{\tau}\Big(q\Big) = \hat{\tau}\Big(q\Big)$. Therefore $\hat{\tau}\Big(q\Big) = 1$, what we had to show. The problem with such a proof is that a human being can check it in principle. Could we have proof checkable by computers? We could, and natural deduction is such an example.

2.2 Inference Rules

Definition 2.1. *A proof system is a set of inference rules.*

Definition 2.2. *An inference rule is of the form:*

$$\textsc{Name}\ \frac{\textit{Hypothesis 1} \qquad \ldots \qquad \textit{Hypothesis n}}{\textit{Conclusion}},$$

where to the left of the line we have the rule name, above the line there are several (0, 1 or more) hypotheses and under the line is the conclusion. The hypotheses and conclusion are usually formulae.

2.3 Rules for $\wedge$

There are several inference rules for each connective. The simplest inferece rules are for $\wedge$:

$$\wedge i\ \frac{\varphi_1 \qquad \varphi_2}{\varphi_1 \wedge \varphi_2} \qquad \wedge e1\ \frac{\varphi_1 \wedge \varphi_2}{\varphi_1} \qquad \wedge e2\ \frac{\varphi_1 \wedge \varphi_2}{\varphi_2}$$

The first rule tells us intuitively that if we know φ_1 to be true and φ_2 to be true (i.e., if the hypotheses are true), then we also know the formula $\varphi_1 \wedge \varphi_2$ to be true (i.e., the conclusion is also true). The name of the inference rule is $\wedge i$, read as "$\wedge$ introduction". The name "introduction" refers to the fact that $\wedge$ appears in the conclusion, but not the hypotheses.

The second rule tells us intuitively that if we know the formula $\varphi_1 \wedge \varphi_2$ to be true, then we also know φ_1 to be true. This is the first elimination rule for $\wedge$, hence the name $\wedge e1$. "Elimination" comes from the fact that $\wedge$ appears in the hypotheses, but not the conclusion. The second elimination rule for $\wedge$ is similar.

But what do we do with inference rules?

2.4 Formal Proofs

Definition 2.3. *A* <u>*formal proof*</u> *of φ starting with $\varphi_1, \ldots, \varphi_n$ is a sequence of formulae $\psi_1, \psi_2, \ldots, \psi_m$ such that for all $1 \leq i \leq m$:*

1. *$\psi_i \in \{\varphi_1, \ldots, \varphi_n\}$, or,*
2. *ψ_i is the conclusion of an inference rule whose hypotheses can be found among $\psi_1, \ldots, \psi_{i-1}$,*

and such that $\psi_n = \varphi$.

For example, we have that $(p \wedge q) \wedge r, p \wedge q, r, q, r \wedge q$ is a formal proof of $r \wedge q$ from $(p \wedge q) \wedge r$. However, it helps to organize the formal proof as follows:

1. $(p \wedge q) \wedge r$; (premiss)
2. $p \wedge q$; ($\wedge e1$, 1)
3. r; ($\wedge e2$, 1)
4. q; ($\wedge e2$, 2)
5. $r \wedge q$. ($\wedge i$, 3, 4)

As written, the formal proof has, in addition to the list of formulae in it, the name of the inference rule applied and the lines at which the hypotheses of the inference rule can be found.

Here is another formal proof of $(p \vee q) \wedge r$ from $p \vee q$ and $r \wedge p$:

1. $p \vee q$; (premiss)
2. $r \wedge p$; (premiss)
3. r; ($\wedge e1$, 2)
4. $(p \vee q) \wedge r$. ($\wedge i$, 1, 3)

Exercise 2.1. *Give a formal proof of* $p \wedge r$ *from* $(q \wedge r) \wedge q$ *and* $q \wedge q$.

2.5 Sequents

Definition 2.4. *A* sequent *is a tuple* $\varphi_1, \ldots, \varphi_n, \varphi$ *of formulae, written as* $\varphi_1, \ldots, \varphi_n \vdash \varphi$. *The symbol* $\vdash$ *is read as "turnstyle".*

See google images for "turnstyle": `https://www.google.com/search?hl=en&site=imghp&tbm=isch&source=hp&q=turnstyle`.

The name sequent is the wrong English translation of the word "Sequenz" from an early paper on logic in German. It should have been "sequence", but the wrong translation stuck and it has become an integral concept of logic today.

Definition 2.5. *A* sequent $\varphi_1, \ldots, \varphi_n \vdash \varphi$ *is valid if there exists a formal proof of* φ *from* $\varphi_1, \ldots, \varphi_n$.

For example, we have already seen that $(p \wedge q) \wedge r \vdash q \wedge r$ and that $p \vee q, r \wedge p \vdash (p \vee q) \wedge r$ are valid sequents. Note the graphical resemblance of sequents to logical consequence, but recall that they mean two different things.

2.6 More Inference Rules

Inference rules for natural deduction come in two flavours: elimination rules and introduction rules. Each logical connective usually has an introduction rule and an elimination rule, but this is not strictly required (for example, $\wedge$ has two elimination rules).

Here are the introduction rules for $\vee$:

$$\vee i1\ \frac{\varphi_1}{\varphi_1 \vee \varphi_2} \qquad \vee i2\ \frac{\varphi_2}{\varphi_1 \vee \varphi_2}$$

We will see the elimination rule for $\vee$ later, as it is more complicated.

Let us see an example that makes use of the new rules, by giving a formal proof of the sequent $p \wedge q \vdash (r \vee q) \vee (r \wedge p)$:

1. $p \wedge q$; (premiss)

2. q; $(\wedge e2,\ 1)$

3. $r \vee q$; $(\vee i2,\ 2)$

4. $(r \vee q) \vee (r \wedge p)$. $(\vee i1,\ 3)$

Exercise 2.2. *Prove the validity of the sequent* $p \wedge q, r \vdash p \wedge (r \vee r')$.

2.7 Elimination of Implication

The rule for eliminating implication is the following:

$$\rightarrow e\ \frac{\varphi_1 \rightarrow \varphi_2 \qquad \varphi_1}{\varphi_2}$$

In fact, this rule goes back to antiquity and is so famous that it has a latin name: modus ponens.

Here is an example of the rule in practice:

1. $p \rightarrow r \wedge q$; (premiss)

2. $p \wedge r$; (premiss)

3. p; $(\wedge e1,\ 2)$

4. $r \wedge q$; $(\rightarrow e,\ 1,\ 3)$

5. q. $(\wedge e2,\ 4)$

The above is a proof of the sequent $p \rightarrow r \wedge q, p \wedge r \vdash q$.

2.8 Rules for Double Negation

There are two rules that play a special role:

$$\neg\neg i\ \frac{\varphi}{\neg\neg\varphi} \qquad\qquad \neg\neg e\ \frac{\neg\neg\varphi}{\varphi}$$

These rules allow to eliminate and respectively introduce double negation freely.

Here is a formal proof of the sequent $(p \wedge q) \wedge \neg\neg r \vdash \neg\neg(\neg\neg p \wedge r)$ that makes use of the new inference rules:

1. $(p \wedge q) \wedge \neg\neg r$; (premiss)

2. $\neg\neg r$; $(\wedge e2,\ 1)$

3. $p \wedge q$; $(\wedge e1,\ 1)$

4. p; $(\wedge e1,\ 3)$

5. $\neg\neg p$; $(\neg\neg i,\ 4)$

6. r; $(\neg\neg e,\ 2)$

7. $\neg\neg p \wedge r$; $(\wedge i,\ 5,\ 6)$

8. $\neg\neg(\neg\neg p \wedge r)$. $(\neg\neg i,\ 7)$

We will see later that in fact the $\neg\neg i$ is derivable, and that the rule $\neg\neg e$ is derivable, is we allow for the law of excluded middle (and vice-versa).

2.9 The Rule for Introducing Implication

What would be a good rule for the introduction of the implication?

If up to the present moment the hypotheses of the rules were all formulae, we will now allow hypotheses that are formal proofs themselves:

$$\to i\ \frac{\boxed{\begin{array}{c}\varphi_1\\ \vdots\\ \varphi_2\end{array}}}{\varphi_1 \to \varphi_2}$$

The hypotheses that must be formal proofs will be placed in a box. In the rule above, there is only one hypothesis, namely a formal proof. The formal proof must start from φ_1, which is called an assumption (similar to premisses) and must end with φ_2. If we can produce such a formal proof of φ_2 from φ_1, then the inference rule $\to i$ allows to conclude $\varphi_1 \to \varphi_2$.

Here is an example of a formal proof of the sequent $\mathtt{p} \to \mathtt{q}, \mathtt{q} \to \mathtt{r} \vdash \mathtt{p} \to \mathtt{r}$ that makes use of $\to i$:

1.	$\mathtt{p} \to \mathtt{q}$	premiss
2.	$\mathtt{q} \to \mathtt{r}$	premiss
3.	$\mathtt{p}$	assumption
4.	$\mathtt{q}$	$\to e$, 1, 3
5.	$\mathtt{r}$	$\to e$, 2, 4
6.	$\mathtt{p} \to \mathtt{r}$	$\to i$, 3–5

Note that inside the box (the subproof) we may use the assumption and any outer premiss. However, it is not allowed to use, outside of the box, formulae that are derived within the box, except as prescribed by the inference rules. For example, the following formal proof is wrong:

1.	$\mathtt{p} \to \mathtt{q}$	premiss
2.	$\mathtt{q} \to \mathtt{r}$	premiss
3.	$\mathtt{p}$	assumption
4.	$\mathtt{q}$	$\to e$, 1, 3
5.	$\mathtt{r}$	$\to e$, 2, 4
6.	$\cancel{\mathtt{p} \wedge \mathtt{q}}$	WRONG APPLICATION OF $\wedge i$, 3,4

We may also have nested boxes. Here is a formal proof of $\mathtt{p} \wedge \mathtt{q} \to \mathtt{r} \vdash \mathtt{p} \to (\mathtt{q} \to \mathtt{r})$:

1.	$\mathtt{p} \wedge \mathtt{q} \to \mathtt{r}$	premiss
2.	$\mathtt{p}$	assumption
3.	$\mathtt{q}$	assumption
4.	$\mathtt{p} \wedge \mathtt{q}$	$\wedge i$, 2, 3
5.	$\mathtt{r}$	$\to e$, 1, 4
6.	$\mathtt{q} \to \mathtt{r}$	$\to i$, 3–5
7.	$\mathtt{p} \to (\mathtt{q} \to \mathtt{r})$	$\to i$, 2,6

Exercise 2.3. *Give a formal proof of* $\mathtt{p} \to (\mathtt{q} \to \mathtt{r}) \vdash \mathtt{p} \wedge \mathtt{q} \to \mathtt{r}$.

2.10 The Rule for Eliminating Disjunction

Here is the rule $\vee e$:

$$\vee e \; \frac{\varphi_1 \vee \varphi_2 \qquad \boxed{\begin{matrix}\varphi_1 \\ \vdots \\ \varphi\end{matrix}} \qquad \boxed{\begin{matrix}\varphi_2 \\ \vdots \\ \varphi\end{matrix}}}{\varphi}$$

Similarly to the rule for introducing introduction, it has other proofs as hypotheses. The intuition behind the rule is the following: suppose you hold that $\varphi_1 \vee \varphi_2$ is true. That means that φ_1 is true or φ_2 is true, but you do not know which one. You make a formal proof of φ from φ_1 and a formal proof of φ from φ_2. Then, no matter which of φ_1 or φ_2 holds, you are guaranteed that φ holds.

Here is a formal proof of $(\mathtt{p} \vee \mathtt{q}) \wedge \mathtt{r} \vdash (\mathtt{p} \wedge \mathtt{r}) \vee (\mathtt{q} \wedge \mathtt{r})$ that makes use of the new rule:

1.	$(\mathtt{p} \lor \mathtt{q}) \land \mathtt{r}$	premiss
2.	$\mathtt{p} \lor \mathtt{q}$	$\land e1$
3.	$\mathtt{r}$	$\land e2$
4.	$\mathtt{p}$	assumption
5.	$\mathtt{p} \land \mathtt{r}$	$\land i$, 3, 4
6.	$(\mathtt{p} \land \mathtt{r}) \lor (\mathtt{q} \land \mathtt{r})$	$\lor i1$, 5
7.	$\mathtt{q}$	assumption
8.	$\mathtt{q} \land \mathtt{r}$	$\land i$, 7, 3
9.	$(\mathtt{p} \land \mathtt{r}) \lor (\mathtt{q} \land \mathtt{r})$	$\lor i2$, 8
10.	$(\mathtt{p} \land \mathtt{r}) \lor (\mathtt{q} \land \mathtt{r})$	$\lor e$, 2,4–6,7–9

2.11 The Rules for Negation and $\bot$

Here are the rules for introducing and eliminating negation:

$$\neg i \, \frac{\boxed{\begin{array}{c}\varphi \\ \vdots \\ \bot\end{array}}}{\neg\varphi} \qquad\qquad \neg e \, \frac{\varphi \qquad \neg\varphi}{\bot}$$

Let us start with the intuition behind the rule for eliminating $\neg$. If you hold both φ and $\neg\varphi$, you also hold $\bot$. Recall that $\bot$ is a formula that is false in any truth assignment. But it is impossible to hold $\bot$. Of course, but it may be useful in a proof. It play the role of a contradiction.

The rule for introducing $\neg$ also makes use of $\bot$: suppose you want to prove $\neg\varphi$ holds. You assume φ and derive a contradiction, that is you make a formal proof of $\bot$ starting from φ.

Here is a formal proof of $\neg p \vdash \neg(p \land q)$ making use of the rules above:

1.	$\neg\mathtt{p}$	premiss
2.	$\mathtt{p} \land \mathtt{q}$	assumption
3.	$\mathtt{p}$	$\land e1$, 2
4.	$\bot$	$\neg e$, 3, 1
5.	$\neg(\mathtt{p} \land \mathtt{q})$	$\neg i$, 2–4

There is another rule, for eliminating $\bot$: it tells us that if we hold $\bot$, then we hold any other formula as well (e.g., if we hold $1 = 2$, we also hold $10 = 15$):

$$\bot e \, \frac{\bot}{\varphi}$$

Here is an example of its use (a proof of the sequent $\mathtt{p} \land \neg\mathtt{q} \vdash \mathtt{q} \land \neg\mathtt{q}$):

1.	$\mathtt{p} \wedge \neg\mathtt{p}$	premiss
2.	$\mathtt{p}$	$\wedge e1$, 1
3.	$\neg\mathtt{p}$	$\wedge e2$, 1
4.	$\bot$	$\neg e$, 2, 3
5.	$\mathtt{q} \wedge \neg\mathtt{q}$	$\bot e$, 4

2.12 The Copy Rule

There is one more rule needed for technical reasons:

$$\textsc{copy}\ \frac{\varphi}{\varphi}$$

The rule says that if you hold φ, then you hold φ. Here is an example of a formal proof of $\vdash \mathtt{p} \to (\mathtt{q} \to \mathtt{p})$ where we need it:

1.	$\mathtt{p}$	assumption
2.	$\mathtt{q}$	assumption
3.	$\mathtt{p}$	copy, 1
4.	$\mathtt{q} \to \mathtt{p}$	$\to i$, 2–3
5.	$\mathtt{p} \to (\mathtt{q} \to \mathtt{p})$	$\to i$, 1–4

We may use this rule to copy within a subproof another formula that is in scope.

3 Derived Rules

Here is an inference rule called modus tollens:

$$\text{MT}\ \frac{\varphi_1 \to \varphi_2 \qquad \neg\varphi_2}{\neg\varphi_1}$$

And here is a formal proof of $\mathtt{p} \to \mathtt{q} \vdash \neg\mathtt{q} \to \neg\mathtt{p}$ that makes use of the new rule:

1.	$\mathtt{p} \to \mathtt{q}$	premiss
2.	$\neg\mathtt{q}$	assumption
3.	$\neg\mathtt{p}$	MT, 1, 2
4.	$\neg\mathtt{q} \to \neg\mathtt{p}$	$\to i$, 2–3

However, we do not need the rule, because we can simulate it by applications of other rules. We can show that for any φ_1, φ_2, there exists a formal proof of $\varphi_1 \to \varphi_2, \neg\varphi_2 \vdash \neg\varphi_1$:

1.	$\varphi_1 \to \varphi_2$	premiss
2.	$\neg\varphi_2$	premiss
3.	φ_1	assumption
4.	φ_2	$\to e$, 1, 3
5.	$\bot$	$\neg e$, 4, 2
6.	$\neg\varphi_1$	$\neg i$, 3–5

Such a rule that can be simulated by applications of other rules is called a derived rule.

Exercise 3.1. *Show that the rule for introducing $\neg\neg$ is derivable.*

Exercise 3.2. *Show that the law of excluded middle is derivable:*

$$\text{LEM}\ \frac{}{\varphi \vee \neg\varphi}$$

Exercise 3.3. *Show that the rule $\neg\neg e$ is derivable using the LEM (i.e. you may use LEM, but not $\neg\neg e$).*

4 Soundness and Completeness

A (good) proof system needs to have two important properties:

1. anything it proves must be true;
2. it can prove anything that is true.

The first property is called soundness and the second property is called completeness. Natural deduction has both:

Theorem 4.1 (Soundness of Natural Deduction)**.** *If there is a formal proof of the sequent*

$$\varphi_1, \ldots, \varphi_n \vdash \varphi,$$

then

$$\varphi_1, \ldots, \varphi_n \models \varphi.$$

That is, if a sequent can be derived syntactically using the inference rules of natural deduction, then the corresponding logical consequence holds as well.

Theorem 4.2 (Completeness of Natural Deduction)**.** *If $\varphi_1, \ldots, \varphi_n \models \varphi$, then there is a formal proof of the sequent*

$$\varphi_1, \ldots, \varphi_n \vdash \varphi.$$

In fact, the theorems above mean that $\vdash$ and $\models$ are interchangable, even if they have different definitions.

Exercise 4.1. *We write $\varphi_1 \dashv\vdash \varphi_2$ if there are formal proofs of both $\varphi_1 \vdash \varphi_2$ and $\varphi_2 \vdash \varphi_1$.*

Prove, using the soundness and completeness theorems, that $\varphi_1 \dashv\vdash \varphi_2$ if and only if $\varphi_1 \equiv \varphi_2$.

5 Summary of Inference Rules

Base rules:

$$\wedge i \ \frac{\varphi_1 \qquad \varphi_2}{\varphi_1 \wedge \varphi_2} \qquad\qquad \wedge e1 \ \frac{\varphi_1 \wedge \varphi_2}{\varphi_1} \qquad\qquad \wedge e2 \ \frac{\varphi_1 \wedge \varphi_2}{\varphi_2}$$

$$\vee i1 \ \frac{\varphi_1}{\varphi_1 \vee \varphi_2} \qquad\qquad \vee i2 \ \frac{\varphi_2}{\varphi_1 \vee \varphi_2} \qquad\qquad \to e \ \frac{\varphi_1 \to \varphi_2 \qquad \varphi_1}{\varphi_2}$$

$$\neg\neg e \ \frac{\neg\neg\varphi}{\varphi} \qquad\qquad \to i \ \frac{\boxed{\begin{array}{c}\varphi_1\\ \vdots \\ \varphi_2\end{array}}}{\varphi_1 \to \varphi_2} \qquad\qquad \vee e \ \frac{\varphi_1 \vee \varphi_2 \qquad \boxed{\begin{array}{c}\varphi_1\\ \vdots \\ \varphi\end{array}} \qquad \boxed{\begin{array}{c}\varphi_2\\ \vdots \\ \varphi\end{array}}}{\varphi}$$

$$\neg i \ \frac{\boxed{\begin{array}{c}\varphi\\ \vdots \ \ c \\ \bot\end{array}}}{\neg\varphi} \qquad\qquad \neg e \ \frac{\varphi \qquad \neg\varphi}{\bot} \qquad\qquad \bot e \ \frac{\bot}{\varphi} \qquad\qquad \text{COPY} \ \frac{\varphi}{\varphi}$$

Derived rules:

$$\neg\neg i \ \frac{\varphi}{\neg\neg\varphi} \qquad\qquad \text{LEM} \ \frac{}{\varphi \vee \neg\varphi} \qquad\qquad \text{MT} \ \frac{\varphi_1 \to \varphi_2 \qquad \neg\varphi_2}{\neg\varphi_1}$$

Exercise 5.1. *Prove that Proof By Contradiction (PBC) is a derived rule:*

$$\text{PBC} \ \frac{\boxed{\begin{array}{c}\neg\varphi\\ \vdots \\ \bot\end{array}}}{\varphi}$$