PROGRAM
PROOF

Samuel MIMRAM

- For $\varepsilon/2 > 0$:
    - because $2 > 0$, this amounts to show $(\varepsilon/2) \times 2 > 0 \times 2$,
    - which, by usual identities, amounts to show $\varepsilon > 0$,
    - which is an hypothesis.
- For $\forall x.|x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon$:
    - suppose given x, we have to show: $|x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon$,
    - suppose that $|x| < \varepsilon/2$ holds, we have to show: $|2x| < \varepsilon$,
    - since $2 > 0$, this amounts to show: $|2x|/2 < \varepsilon/2$,
    - which, by usual identities, amounts to show: $|x| < \varepsilon/2$,
    - which is an hypothesis.

Now that we have decomposed the proof in very small steps, it seems possible to give a list of all the generic rules that we are allowed to apply in a reasoning. We will do so and will introduce a convenient formalism and notations, so that the above proof will be noted as:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varepsilon > 0 \vdash \varepsilon > 0}}{\varepsilon > 0 \vdash (\varepsilon/2) \times 2 > 0 \times 2}}{\varepsilon > 0 \vdash \varepsilon/2 > 0} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |x| < \varepsilon/2}}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |2x|/2 < \varepsilon/2}}{\varepsilon > 0, |x| < \varepsilon/2 \vdash |2x| < \varepsilon}}{\varepsilon > 0 \vdash |x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \forall x.|x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \varepsilon/2 > 0 \wedge \forall x.|x| < \varepsilon/2 \Rightarrow |2x| < \varepsilon}}{\varepsilon > 0 \vdash \exists \eta.(\eta > 0 \wedge \forall x.|x| < \eta \Rightarrow |2x| < \varepsilon)}}{\vdash \varepsilon > 0 \Rightarrow \exists \eta.(\eta > 0 \wedge \forall x.|x| < \eta \Rightarrow |2x| < \varepsilon)}}{\vdash \forall \varepsilon.(\varepsilon > 0 \Rightarrow \exists \eta.(\eta > 0 \wedge \forall x.|x| < \eta \Rightarrow |2x| < \varepsilon))}$$

(when read from bottom to top, you should be able to see the precise correspondence with the previous description of the proof).

2.1.4 Properties of the logical system. Once we have formalized our logical system we should do some sanity checks. The first requirement is that it should be *consistent*: there is at least one formula A which is not provable (otherwise, the system would be entirely pointless). The second requirement is that typechecking should be decidable: there should be an algorithm which checks whether a proof is a valid proof or not. In contrast, the question of deciding whether a formula is provable or not will not be decidable in general and we do not expect to have an algorithm for that.

2.2 Natural deduction

Natural deduction is the first formalism for proofs that we will study. It was introduced by Gentzen [Gen35]. We first present the intuitionistic version.

2.2.1 Formulas. We suppose fixed a countably infinite set $\mathcal{X}$ of *propositional variables*. The set $\mathcal{A}$ of *formulas* or *propositions* is generated by the following grammar

$$A, B ::= X \mid A \Rightarrow B \mid A \wedge B \mid \top \mid A \vee B \mid \bot \mid \neg A$$

where X denotes a propositional variable (in $\mathcal{X}$) and A and B denote propositions. They are respectively read as a propositional variable, *implication*, *conjunction*, *truth*, *disjunction*, *falsity* and *negation*. By convention, $\neg$ binds the most tightly, then $\wedge$, then $\vee$, then $\Rightarrow$:

$$\neg A \vee B \wedge C \Rightarrow D \qquad \text{reads as} \qquad ((\neg A) \vee (B \wedge C)) \Rightarrow D$$

Moreover, all binary connectives are implicitly bracketed on the right:

$$A_1 \wedge A_2 \wedge A_3 \Rightarrow B \Rightarrow C \qquad \text{reads as} \qquad (A_1 \wedge (A_2 \wedge A_3)) \Rightarrow (B \Rightarrow C)$$

This is particularly important for $\Rightarrow$, for the connectives $\wedge$ and $\vee$ the other convention could be chosen with almost no impact. We sometimes write $A \Leftrightarrow B$ for $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

A *subformula* of a formula A is a formula occurring in A. The set of subformulas of A can formally be defined by induction on A by

$$\begin{aligned} \operatorname{Sub}(X) &= \{X\} & \operatorname{Sub}(A \Rightarrow B) &= \{A \Rightarrow B\} \cup \operatorname{Sub}(A) \cup \operatorname{Sub}(B) \\ \operatorname{Sub}(\top) &= \{\top\} & \operatorname{Sub}(A \wedge B) &= \{A \wedge B\} \cup \operatorname{Sub}(A) \cup \operatorname{Sub}(B) \\ \operatorname{Sub}(\bot) &= \{\bot\} & \operatorname{Sub}(A \vee B) &= \{A \vee B\} \cup \operatorname{Sub}(A) \cup \operatorname{Sub}(B) \\ & & \operatorname{Sub}(\neg A) &= \{\neg A\} \cup \operatorname{Sub}(A) \end{aligned}$$

2.2.2 Sequents. A *context*

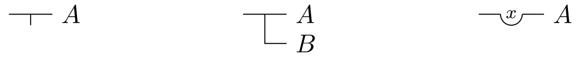
$$\Gamma = A_1, \ldots, A_n$$

is a list of propositions. A *sequent*, or *judgment*, is a pair

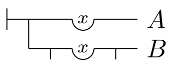
$$\Gamma \vdash A$$

consisting of a context Γ and a variable A. Such a sequent should be read as "under the hypothesis in Γ, I can prove A" or "supposing that I can prove the propositions in Γ, I can prove A". The comma in a context can thus be read as a "meta" conjunction (the logical conjunction being $\wedge$) and the sign $\vdash$ as a "meta" implication (the logical implication being $\Rightarrow$).

Remark 2.2.2.1. The notation derives from Frege's *Begriffsschrift* [Fre79], an axiomatization of first-order logic based on a graphical notation, in which logical connectives are noted by using wires of particular shapes: the formulas $\neg A$, $A \Rightarrow B$ and $\forall x.A$ are respectively written



In this system, given a proposition noted —— A , the notation $\vdash$—— A means that A is provable. The assertion that $(\forall x.A) \Rightarrow (\exists x.B)$ is provable would for instance be written



(in classical logic, the formula $\exists x.B$ is equivalent to $\neg\forall x.\neg B$). The symbol $\vdash$ used in sequents, as well as the symbol $\neg$ for negation, originate from there.

$$\frac{}{\Gamma, A, \Gamma' \vdash A}\,(\mathrm{ax})$$

$$\frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,(\Rightarrow_{\mathrm{E}}) \qquad\qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\mathrm{I}})$$

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\,(\wedge^{\mathrm{l}}_{\mathrm{E}}) \quad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\,(\wedge^{\mathrm{r}}_{\mathrm{E}}) \qquad\qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\,(\wedge_{\mathrm{I}})$$

$$\frac{}{\Gamma \vdash \top}\,(\top_{\mathrm{I}})$$

$$\frac{\Gamma \vdash A \vee B \qquad \Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma \vdash C}\,(\vee_{\mathrm{E}}) \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\,(\vee^{\mathrm{l}}_{\mathrm{I}}) \quad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\,(\vee^{\mathrm{r}}_{\mathrm{I}})$$

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\,(\bot_{\mathrm{E}})$$

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,(\neg_{\mathrm{E}}) \qquad\qquad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,(\neg_{\mathrm{I}})$$

Figure 2.1: NJ: rules of intuitionistic natural deduction.

2.2.3 Inference rules. An *inference rule*, noted

$$\frac{\Gamma_1 \vdash A_1 \qquad \ldots \qquad \Gamma_n \vdash A_n}{\Gamma \vdash A} \tag{2.1}$$

consists of n sequents $\Gamma_i \vdash A_i$, called the *premises* of the rule, and a sequent $\Gamma \vdash A$, called the *conclusion* of the rule. We sometimes identify the rules by a name given to them, which is written on the right of the rule. Some rules also come with external hypothesis on the formulas occurring in the premises: those are called *side conditions*. There are two ways to read an inference rule:

- the *deductive* way, from top to bottom: from a proof for each of the premises $\Gamma_i \vdash A_i$ we can deduce $\Gamma \vdash A$,
- the *inductive* or *proof search* way, from bottom to top: if we want to prove $\Gamma \vdash A$ by that inference rule we need to prove all the premises $\Gamma_i \vdash A_i$.

Both are valid ways of thinking about proofs, but one might be more natural than the other one depending on the application.

2.2.4 Intuitionistic natural deduction. The rules for *intuitionistic natural deductions* are shown in figure 2.1, the resulting system often being called NJ (N for natural deduction and J for intuitionistic). Apart from the *axiom* rule (ax), each rule is specific to a connective and the rules can be classified in two families depending on whether this connective appears in the conclusion or in the premises:

- the *elimination rules* allow the use of a formula with a given connective (which is in the formula in the leftmost premise, called the *principal premise*),
- the *introduction rules* construct a formula with a given connective.

In figure 2.1, the elimination (resp. introduction) rules are figured on the left (resp. right) and bear names of the form $(\ldots_{\mathrm{E}})$ (resp. $(\ldots_{\mathrm{I}})$).

The axiom rule allows the use of a formula in the context Γ: supposing that a formula A holds, we can certainly prove it. This rule is the only one to really make use of the context: when read from the bottom to top, all the other rules either propagate the context or add hypothesis to it, but never inspect it.

The introduction rules are the most easy to understand: they allow proving a formula with a given logical connective from the proofs of the immediate subformulas. For instance, $(\wedge_{\mathrm{I}})$ states that from a proof of A and a proof of B, we can construct a proof of $A \wedge B$. Similarly, the rule $(\Rightarrow_{\mathrm{I}})$ follows the usual reasoning principle for implication: if, after supposing that A holds, we can show B, then $A \Rightarrow B$ holds.

In contrast, the elimination rules allow the use of a connective. For instance, the rule $(\Rightarrow_{\mathrm{E}})$, which is traditionally called *modus ponens* or *detachment rule*, says that if A implies B and A holds then certainly B must hold. The rule $(\vee_{\mathrm{E}})$ is more subtle and corresponds to a case analysis: if we can prove $A \vee B$ then, intuitively, we can prove A or we can prove B. If in both cases we can deduce C then C must hold. The elimination rule $(\bot_{\mathrm{E}})$ is sometimes called *ex falso quodlibet* or the *explosion principle*: it states that if we can prove false then the whole logic collapses, and we can prove anything.

We can notice that there is no elimination rule for $\top$ (knowing that $\top$ is true does not bring any new information), and no introduction rule for $\bot$ (we do not expect that there is a way to prove falsity). There are two elimination rules for $\wedge$ which are respectively called *left* and *right* rules, and similarly there are two introduction rules for $\vee$.

2.2.5 Proofs. The set of *proofs* (or *derivations*) is the smallest set such that given proofs π_i of the sequent $\Gamma_i \vdash A_i$, for $1 \leqslant i \leqslant n$, and an inference rule of the form (2.1) there is a proof of $\Gamma \vdash A$, often noted in the form of a tree as

$$\frac{\dfrac{\pi_1}{\Gamma_1 \vdash A_1} \quad \ldots \quad \dfrac{\pi_n}{\Gamma_n \vdash A_n}}{\Gamma \vdash A}$$

A sequent $\Gamma \vdash A$ is *provable* (or *derivable*) when it is the conclusion of a proof. A formula A is *provable* when it is provable without hypothesis, i.e. when the sequent $\vdash A$ is provable.

Example 2.2.5.1. The formula $(A \wedge B) \Rightarrow (A \vee B)$ is provable (for any formulas A and B):

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A \wedge B \vdash A \wedge B}\,(\mathrm{ax})}{A \wedge B \vdash A}\,(\wedge_{\mathrm{E}})}{A \wedge B \vdash A \vee B}\,(\vee_{\mathrm{I}}^{\mathrm{l}})}{\vdash A \wedge B \Rightarrow A \vee B}\,(\Rightarrow_{\mathrm{I}})$$

Example 2.2.5.2. The formula $(A \vee B) \Rightarrow (B \vee A)$ is provable:

$$\dfrac{\dfrac{\dfrac{}{A \vee B \vdash A \vee B}\;(\text{ax}) \qquad \dfrac{\dfrac{}{A \vee B, A \vdash A}\;(\text{ax})}{A \vee B, A \vdash B \vee A}\;(\vee_{\text{I}}^{\text{r}}) \qquad \dfrac{\dfrac{}{A \vee B, B \vdash B}\;(\text{ax})}{A \vee B, B \vdash B \vee A}\;(\vee_{\text{I}}^{\text{l}})}{A \vee B \vdash B \vee A}\;(\vee_{\text{E}})}{\vdash A \vee B \Rightarrow B \vee A}\;(\Rightarrow_{\text{I}})$$

Example 2.2.5.3. The formula $A \Rightarrow \neg\neg A$ is provable:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A, \neg A \vdash \neg A}\;(\text{ax}) \qquad \dfrac{}{A, \neg A \vdash A}\;(\text{ax})}{A, \neg A \vdash \bot}\;(\neg_{\text{E}})}{A \vdash \neg\neg A}\;(\neg_{\text{I}})}{\vdash A \Rightarrow \neg\neg A}\;(\Rightarrow_{\text{I}})$$

Example 2.2.5.4. The formula $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$ is provable:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow B, \neg B, A \vdash \neg B}\;(\text{ax}) \qquad \dfrac{\dfrac{}{A \Rightarrow B, \neg B, A \vdash A \Rightarrow B}\;(\text{ax}) \qquad \dfrac{}{A \Rightarrow B, \neg B, A \vdash A}\;(\text{ax})}{A \Rightarrow B, \neg B, A \vdash B}\;(\Rightarrow_{\text{E}})}{A \Rightarrow B, \neg B, A \vdash \bot}\;(\neg_{\text{E}})}{A \Rightarrow B, \neg B \vdash \neg A}\;(\neg_{\text{I}})}{A \Rightarrow B \vdash \neg B \Rightarrow \neg A}\;(\Rightarrow_{\text{I}})}{\vdash (A \Rightarrow B) \Rightarrow \neg B \Rightarrow \neg A}\;(\Rightarrow_{\text{I}})$$

Example 2.2.5.5. The formula $(\neg A \vee B) \Rightarrow (A \Rightarrow B)$ is provable:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg A \vee B, A \vdash \neg A \vee B}\;(\text{ax}) \qquad \dfrac{\dfrac{}{\neg A \vee B, A, \neg A \vdash \neg A}\;(\text{ax}) \qquad \dfrac{}{\neg A \vee B, A, \neg A \vdash A}\;(\text{ax})}{\neg A \vee B, A, \neg A \vdash B}\;(\neg_{\text{E}}) \qquad \dfrac{}{\neg A \vee B, A, B \vdash B}\;(\text{ax})}{\neg A \vee B, A \vdash B}\;(\vee_{\text{E}})}{\neg A \vee B \vdash A \Rightarrow B}\;(\Rightarrow_{\text{I}})}{\vdash (\neg A \vee B) \Rightarrow (A \Rightarrow B)}\;(\Rightarrow_{\text{I}})$$

Other typical provable formulas are

– $\wedge$ and $\top$ satisfy the axioms of idempotent commutative monoids:

$$\begin{array}{rl} (A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C) & \qquad A \wedge B \Leftrightarrow B \wedge A \\ \top \wedge A \Leftrightarrow A \Leftrightarrow A \wedge \top & \qquad A \wedge A \Leftrightarrow A \end{array}$$

– $\vee$ and $\bot$ satisfy the axioms of idempotent commutative monoids

– $\wedge$ distributes over $\vee$ and conversely:

$$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$$

– $\Rightarrow$ is reflexive and transitive

$$A \Rightarrow A \qquad\qquad (A \Rightarrow B) \Rightarrow (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$$

– curryfication:

$$((A \wedge B) \Rightarrow C) \Leftrightarrow (A \Rightarrow (B \Rightarrow C))$$

– usual reasoning structures with latin names, such as

$$\begin{array}{rl}
(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A) & \text{(modus tollens)} \\
(A \vee B) \Rightarrow (\neg A \Rightarrow B) & \text{(modus tollendo ponens)} \\
\neg(A \wedge B) \Rightarrow (A \Rightarrow \neg B) & \text{(modus ponendo tolens)}
\end{array}$$

Reasoning on proofs. In this formalism, the proofs are defined inductively and therefore we can reason by induction on them, which is often useful. Precisely, the induction principle on proofs is the following one:

Theorem 2.2.5.6 (Induction on proofs). Suppose given a predicate $P(\pi)$ on proofs π. Suppose moreover that for every rule of figure 2.1 and every proof π ending with this rule

$$\pi \quad = \quad \frac{\dfrac{\pi_1}{\Gamma_1 \vdash A_1} \quad \ldots \quad \dfrac{\pi_n}{\Gamma_n \vdash A_n}}{\Gamma \vdash A}$$

if $P(\pi_i)$ holds for every index i, with $1 \leqslant i \leqslant n$, then $P(\pi)$ also holds. Then $P(\pi)$ holds for every proof π.

2.2.6 Fragments. A *fragment* of intuitionistic logic is a system obtained by restricting to formulas containing certain connectives and rules concerning these connectives. By convention, the axiom rule (ax) is present in every fragment. For instance, the *implicational fragment* of intuitionistic logic is obtained by restricting to implication: formulas are generated by the grammar

$$A, B ::= X \mid A \Rightarrow B$$

and the rules are

$$\frac{}{\Gamma, A, \Gamma' \vdash A}\,(\text{ax}) \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}\,(\Rightarrow_{\text{E}}) \qquad \frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\text{I}})$$

The *cartesian fragment* is obtained by restricting to product and implication. Another useful fragment is *minimal logic* obtained by considering formulas without $\bot$, and thus removing the rule ($\bot_{\text{E}}$).

2.2.7 Admissible rules. A rule is *admissible* when, whenever the premises are provable, the conclusion is also provable. An important point here is that the way the proof of the conclusion is constructed might depend on the proofs of the premises, and not only on the fact that we know that the premises are provable.

Structural rules. We begin by showing that the *structural rules* are admissible. Those rules are named in this way because they concern the structure of the logical proofs, as opposed to the particular connectives we are considering for formulas. They express some resource management possibilities for the hypothesis in sequents: we can permute, merge and weaken them, see section 2.2.10.

A first admissible rule is the weakening rule, which states that whenever one can prove a formula with some hypothesis, we can still prove it with more hypothesis. The proof with more hypothesis is “weaker” in the sense that it apply in less cases (since more hypothesis have to be satisfied).

Proposition 2.2.7.1 (Weakening). The *weakening rule*

$$\frac{\Gamma,\Gamma'\vdash B}{\Gamma,A,\Gamma'\vdash B}\ (\text{wk})$$

is admissible.

Proof. By induction on the proof of the hypothesis $\Gamma,\Gamma'\vdash B$.

- If the proof is of the form

  $$\frac{}{\Gamma,\Gamma'\vdash B}\ (\text{ax})$$

  with B occurring in Γ or Γ', then we conclude with

  $$\frac{}{\Gamma,A,\Gamma'\vdash B}\ (\text{ax})$$

- If the proof is of the form

  $$\frac{\dfrac{\pi_1}{\Gamma,\Gamma'\vdash B\Rightarrow C}\qquad\dfrac{\pi_2}{\Gamma,\Gamma'\vdash B}}{\Gamma,\Gamma'\vdash C}\ (\Rightarrow_{\text{E}})$$

  then we conclude with

  $$\frac{\dfrac{\pi_1'}{\Gamma,A,\Gamma'\vdash B\Rightarrow C}\qquad\dfrac{\pi_2'}{\Gamma,A,\Gamma'\vdash B}}{\Gamma,A,\Gamma'\vdash C}\ (\Rightarrow_{\text{E}})$$

  where π_1' and π_2' are respectively obtained from π_1 and π_2 by induction hypothesis:

  $$\pi_1'=\frac{\dfrac{\pi_1}{\Gamma,\Gamma'\vdash B\Rightarrow C}}{\Gamma,A,\Gamma'\vdash B\Rightarrow C}\ (\text{wk})\qquad\qquad \pi_2'=\frac{\dfrac{\pi_2}{\Gamma,\Gamma'\vdash B}}{\Gamma,A,\Gamma'\vdash B}\ (\text{wk})$$

- If the proof is of the from

  $$\frac{\dfrac{\pi}{\Gamma,\Gamma',B\vdash C}}{\Gamma,\Gamma'\vdash B\Rightarrow C}\ (\Rightarrow_{\text{I}})$$

  then we conclude with

  $$\frac{\dfrac{\pi'}{\Gamma,A,\Gamma',B\vdash C}}{\Gamma,A,\Gamma'\vdash B\Rightarrow C}\ (\Rightarrow_{\text{I}})$$

  where π' is obtained from π by induction hypothesis.

- Other cases are similar. □

Also admissible is the exchange rule, which states that we can reorder hypothesis in the contexts:

Proposition 2.2.7.2 (Exchange). The *exchange rule*

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C}\ (\text{xch})$$

is admissible.

Proof. By induction on the proof of the hypothesis $\Gamma, A, B, \Gamma' \vdash C$. □

Given a proof π of some sequent, we often write $w(\pi)$ for a proof obtained by weakening. Another admissible rule is contraction, which states that if we can prove a formula with two occurrences of a hypothesis, we can also prove it with one occurrence.

Proposition 2.2.7.3 (Contraction). The *contraction rule*

$$\frac{\Gamma, A, A, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\ (\text{contr})$$

is admissible.

Proof. By induction on the proof of the hypothesis $\Gamma, A, A, \Gamma' \vdash B$. □

We can also formalize the fact that knowing $\top$ does not bring information, what we call here *truth strengthening* (we are not aware of a standard terminology for this one):

Proposition 2.2.7.4 (Truth strengthening). The following rule is admissible:

$$\frac{\Gamma, \top, \Gamma' \vdash A}{\Gamma, \Gamma' \vdash A}\ (\text{tstr})$$

Proof. By induction on the proof of the hypothesis $\Gamma, \top, \Gamma' \vdash A$, the only “subtle” case being that we have to transform

$$\frac{}{\Gamma, \top, \Gamma' \vdash \top}\ (\text{ax}) \qquad \text{into} \qquad \frac{}{\Gamma, \Gamma' \vdash \top}\ (\top_\text{I})$$

□

The cut rule. A most important admissible rule is the cut rule, which states that if we can prove a formula B using a hypothesis A (thought of as a lemma used in the proof) and we can prove the hypothesis A, then we can directly prove the formula B.

Theorem 2.2.7.5 (Cut). The *cut rule*

$$\frac{\Gamma \vdash A \qquad \Gamma, A, \Gamma' \vdash B}{\Gamma, \Gamma' \vdash B}\ (\text{cut})$$

is admissible.

Proof. For simplicity, we restrict to the case where Γ' is the empty context, which is not an important limitation because the exchange rule is admissible. The cut rule can be derived from the rules of implication by

$$\frac{\Gamma \vdash A \qquad \dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B}\,(\Rightarrow_{\mathrm{I}})}{\Gamma \vdash B}\,(\Rightarrow_{\mathrm{E}})$$

□

We will see in section 2.3.2 that the above proof is not satisfactory and will provide another one, which brings much more information about the dynamics of the proofs.

Admissible rules via implication. Many rules can be proved to be admissible by eliminating provable implications:

Lemma 2.2.7.6. Suppose that the formula $A \Rightarrow B$ is provable. Then the rule

$$\frac{\Gamma \vdash A}{\Gamma \vdash B}$$

is admissible.

Proof. We have

$$\frac{\Gamma \vdash A \qquad \dfrac{\dfrac{\vdots}{\vdash A \Rightarrow B}}{\Gamma \vdash A \Rightarrow B}\,(\mathrm{wk})}{\Gamma \vdash B}\,(\Rightarrow_{\mathrm{E}})$$

□

For instance, we have seen in example 2.2.5.4 that the implication

$$(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$$

is provable. We immediately deduce:

Lemma 2.2.7.7 (Modus tollens). The following two variants of the *modus tollens rule*

$$\frac{\Gamma \vdash A \Rightarrow B}{\Gamma \vdash \neg B \Rightarrow \neg A} \qquad\qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash \neg B}{\Gamma \vdash \neg A}$$

are admissible.

2.2.8 Definable connectives. A logical connective is *definable* when it can be expressed from other connectives in such a way that replacing the connective by its expression and removing the associated logical rules preserves provability.

Lemma 2.2.8.1. Negation is definable as $\neg A = A \Rightarrow \bot$.

Proof. The introduction and elimination rules of $\neg$ are derivable by

$$\frac{\Gamma, A \vdash \bot}{\Gamma \vdash \neg A}\,(\neg_{\mathrm{I}}) \quad \rightsquigarrow \quad \frac{\Gamma, A \vdash \bot}{\Gamma \vdash A \Rightarrow \bot}\,(\Rightarrow_{\mathrm{I}})$$

$$\frac{\Gamma \vdash \neg A \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,(\neg_{\mathrm{E}}) \quad \rightsquigarrow \quad \frac{\Gamma \vdash A \Rightarrow \bot \qquad \Gamma \vdash A}{\Gamma \vdash \bot}\,(\Rightarrow_{\mathrm{E}})$$

from which it follows that, given a provable formula A, the formula A' obtained from A by changing all connectives $\neg-$ into $- \Rightarrow \bot$ is provable, without using $(\neg_{\mathrm{E}})$ and $(\neg_{\mathrm{I}})$. Conversely, suppose given a formula A, such that the transformed formula A' is provable. We have to show that A is also provable, which is more subtle. In the proof of A', for each subproof of the form

$$\frac{\pi}{\Gamma \vdash B \Rightarrow \bot}$$

where the conclusion $B \Rightarrow \bot$ corresponds to the presence of $\neg B$ as a subformula of A, we can transform the proof as follows:

$$\cfrac{\cfrac{\cfrac{\cfrac{\pi}{\Gamma \vdash B \Rightarrow \bot}}{\Gamma, B \vdash B \Rightarrow \bot}\,(\text{wk}) \qquad \cfrac{}{\Gamma, B \vdash B}\,(\text{ax})}{\Gamma, B \vdash \bot}\,(\Rightarrow_{\mathrm{E}})}{\Gamma \vdash \neg B}\,(\neg_{\mathrm{I}})$$

Applying this transformation enough times, we can transform the proof of A' into a proof of A. A variant of this proof is given in corollary 2.2.9.2. □

Lemma 2.2.8.2. Truth is definable as $A \Rightarrow A$, for any provable formula A not involving $\top$. For instance: $\top = (\bot \Rightarrow \bot)$.

Remark 2.2.8.3. In intuitionistic logic, contrarily to what we expect from the usual de Morgan formulas, the implication is not definable as

$$A \Rightarrow B = \neg A \vee B$$

see sections 2.3.5 and 2.5.1.

2.2.9 Equivalence. We could have added to the syntax of our formulas an *equivalence* connective $\Leftrightarrow$ with associated rules

$$\frac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash A \Rightarrow B}\,(\Leftrightarrow^{\mathrm{l}}_{\mathrm{I}}) \qquad \frac{\Gamma \vdash A \Leftrightarrow B}{\Gamma \vdash B \Rightarrow A}\,(\Leftrightarrow^{\mathrm{r}}_{\mathrm{I}}) \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash B \Rightarrow A}{\Gamma \vdash A \Leftrightarrow B}\,(\Leftrightarrow_{\mathrm{E}})$$

It would have been definable as

$$A \Leftrightarrow B = (A \Rightarrow B) \wedge (B \Rightarrow A)$$

Two formulas A and B are *equivalent* when $A \Leftrightarrow B$ is provable. This notion of equivalence relates in the expected way to provability:

Lemma 2.2.9.1. If A and B are equivalent then, for every context Γ, $\Gamma \vdash A$ is provable if and only if $\Gamma \vdash B$ is provable.

Proof. Immediate application of lemma 2.2.7.6. □

In this way, we can give a variant of the proof of lemma 2.2.8.1:

Corollary 2.2.9.2. Negation is definable as $\neg A = (A \Rightarrow \bot)$.

Proof. We have $\neg A \Leftrightarrow (A \Rightarrow \bot)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg A, A \vdash \neg A}\,(\text{ax}) \qquad \dfrac{}{\neg A, A \vdash A}\,(\text{ax})}{\neg A, A \vdash \bot}\,(\neg_\text{E})}{\neg A \vdash A \Rightarrow \bot}\,(\Rightarrow_\text{I})}{\vdash \neg A \Rightarrow A \Rightarrow \bot}\,(\Rightarrow_\text{I}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{A \Rightarrow \bot, A \vdash A \Rightarrow \bot}\,(\text{ax}) \qquad \dfrac{}{A \Rightarrow \bot, A \vdash A}\,(\text{ax})}{A \Rightarrow \bot, A \vdash \bot}\,(\Rightarrow_\text{E})}{A \Rightarrow \bot \vdash \neg A}\,(\neg_\text{I})}{\vdash (A \Rightarrow \bot) \Rightarrow \neg A}\,(\Rightarrow_\text{I})}{\vdash \neg A \Leftrightarrow (A \Rightarrow \bot)}\,(\Leftrightarrow_\text{E})$$

and we conclude using lemma 2.2.9.1. □

2.2.10 Structural rules. The rules of exchange, contraction, weakening and truth strengthening are often called *structural rules*:

$$\frac{\Gamma, A, B, \Gamma' \vdash C}{\Gamma, B, A, \Gamma' \vdash C}\,(\text{xch}) \qquad \frac{\Gamma, A, A, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\,(\text{contr})$$

$$\frac{\Gamma, \Gamma' \vdash B}{\Gamma, A, \Gamma' \vdash B}\,(\text{wk}) \qquad \frac{\Gamma, \top, \Gamma' \vdash A}{\Gamma, \Gamma' \vdash A}\,(\text{tstr})$$

We have seen in section 2.2.7 that they are admissible in our system.

Contexts as sets. The rules of exchange and contraction allow to think of contexts as sets (rather than lists) of formulas, because a set is a list "up to permutation and duplication of its elements". More precisely, given a set $\mathcal{A}$, we write $\mathcal{P}(\mathcal{A})$ for the set of subsets of $\mathcal{A}$, and $\mathcal{A}^*$ for the set of lists over $\mathcal{A}$. We define an equivalence relation $\sim$ on $\mathcal{A}^*$ as the smallest equivalence relation such that

$$\Gamma, A, B, \Delta \sim \Gamma, B, A, \Delta \qquad\qquad \Gamma, A, A, \Delta \sim \Gamma, A, \Delta$$

Lemma 2.2.10.1. The function $f : \mathcal{A}^* \to \mathcal{P}(\mathcal{A})$ which to a list associates its set of elements is surjective. Moreover, given $\Gamma, \Delta \in \mathcal{A}^*$, we have $f(\Gamma) = f(\Delta)$ if and only if $\Gamma \sim \Delta$.

We could therefore have directly defined contexts to be sets of formulas, as is sometimes done, but this would be really unsatisfactory. Namely, a formula A in a context can be thought of as some kind of hypothesis which is to be proved by an auxiliary lemma and we might have twice the same formula A, but proved by different means: in this case, we would like to be able to refer to a particular instance of A (which is proved in a particular way), and we cannot do this if we have a set of hypothesis. For instance, there are intuitively two proofs of $A \Rightarrow A \Rightarrow A$: the one which uses the left A to prove A and the one which uses the right one (this will become even more striking with the Curry-Howard correspondence, see remark 4.1.7.2). However, with contexts as sets, both are the same:

$$\dfrac{\dfrac{\dfrac{}{A \vdash A}\,(\text{ax})}{A \vdash A \Rightarrow A}\,(\Rightarrow_\text{I})}{\vdash A \Rightarrow A \Rightarrow A}\,(\Rightarrow_\text{I})$$

A less harmful simplification which is sometimes done is to quotient by exchange only (and not contraction), in which case the contexts become multisets, see appendix A.3.5. We will refrain from doing that here as well.

Variants of the proof system. The structural rules are usually taken as “real” (as opposed to admissible) rules of the proof system. Here, we have carefully chosen the formulation of rules, so that they are admissible, but it would not hold anymore if we had used subtle variants instead. For instance, if we replace the axiom rule by

$$\frac{}{\Gamma, A \vdash A}\ (\text{ax}) \qquad \text{or} \qquad \frac{}{A \vdash A}\ (\text{ax})$$

or replace the introduction rule for conjunction by

$$\frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma, \Delta \vdash A \land B}\ (\land_{\text{I}})$$

the structural rules are not all admissible anymore. The fine study of the structure behind this lead Girard to introduce *linear logic* [Gir87].

2.2.11 Substitution. Given formulas A and B and a variable X, we write

$$A[B/X]$$

for the *substitution* of X by B in A, i.e. the formula A where all the occurrences of X have been replaced by B. More generally, a *substitution* for A is a function which to every variable X occurring in A assigns a formula $\sigma(X)$ and we also write

$$A[\sigma]$$

for the formula A where every variable X has been replaced by $\sigma(X)$. Similarly, given a context $\Gamma = A_1, \ldots, A_n$, we define

$$\Gamma[\sigma] = A_1[\sigma], \ldots, A_n[\sigma]$$

We often write

$$[A_1/X_1, \ldots, A_n/X_n]$$

for the substitution σ such that $\sigma(X_i) = A_i$ and $\sigma(X) = X$ for X different from each X_i. It satisfies

$$A[A_1/X_1, \ldots, A_n/X_n] = A[A_1/X_1] \ldots [A_n/X_n]$$

We always suppose that, for a substitution σ, the set

$$\{X \in \mathcal{X} \mid \sigma(X) \neq X\}$$

is finite so that the substitution can be represented as the list of images of elements of this set. Provable formulas are closed under substitution:

Proposition 2.2.11.1. Given a provable sequent $\Gamma \vdash A$ and a substitution σ, the sequent $\Gamma[\sigma] \vdash A[\sigma]$ is also provable.

Proof. By induction on the proof of $\Gamma \vdash A$. □